Quantum Resistant Lattice-Based Access Control Scheme for UAV-Assisted Internet-of-Drones Applications

Basudeb Bera, Ashok Kumar Das, *Senior Member, IEEE*, and Biplab Sikdar, *Fellow, IEEE*

***Abstract*—The proliferation of Uncrewed Aerial Vehicle (UAV) networks and their numerous benefits in critical scenarios, UAV become crucial for Internet of Drones (IoD) operations. However, due to their communication methods, such as the micro-air-vehicle communication (MAVlink) protocol, wireless connections, and potentially insecure Internet channels, UAV networks are highly vulnerable to potentially lethal attacks. To overcome such issues, public key cryptographic techniques relying on integer factorization problem (IFP) and discrete logarithm problems (DLP) have been used form decades. However, with the significant advancements in quantum computing and adaptation of Shor's algorithm such cryptographic techniques based on IFP and DLP become insecure today and vulnerable to quantum attacks, which demand new ways of thinking about security. In this paper, we propose a quantum-secure access control protocol for UAV-based IoD applications, and its primary focus is on preserving user anonymity. A comprehensive security analysis validates the accuracy, security, and resilience against various active and passive attacks in both classical and quantum scenarios. A thorough formal security verification using the Scyther automated software validation tool to showcases the robustness of the proposed scheme. Furthermore, a real-time testbed experiment on Raspberry Pi 4 devices to assess the computational overhead of various cryptographic primitives demonstrates its practicality. Lastly, a detailed comparative performance evaluation, including authentication accuracy, performance under unknown attacks with existing related schemes illustrates its scalability and efficiency in real-world applications.**

***Index Terms*—Post-quantum security, access control, Ring Learning with Errors (RLWE), Internet of Drones (IoD), random oracle model, Scyther.**

I. Introduction

AN UNCREWED Aerial Vehicle (UAV) commonly known as a drone, is a building block of the Internet of Drones (IoD) network. These aircraft are remotely controlled, operates with minimum human interaction, and accesses airspace through mostly wireless communication system. The range of UAV applications are rapidly increasing, encompassing various uses from military operations to commercial applications. The growth of these UAVs are relies on there flexibility, cost-effectiveness, and ease of deployment [1]. The utilization of drones will significantly increase in the coming years. Based to the Federal Aviation Administration (FAA) report the commercial drone fleet encompasses drones operated for business purposes and it is anticipated to grow to approximately 828,000 by 2024 in USA. In parallel, the recreational drone fleet in personal used, it is projected to expand to approximately 1.48 million in USA by 2024 [2], [3].

Due to the significant proliferation of UAV networks and adaptation in tough terrains, such as border surveillance systems, wildlife monitoring systems, and disaster management systems, drones become potential key components for building blocks for sensitive drone operations due to their intelligence, surveillance, and reconnaissance in nature [4]. In IoD networks, drones commonly utilize wireless media as communication technologies, such as Bluetooth, Wi-Fi, or cellular networks, for communicating with other network components, including drones, ground control stations (GCSs), or user devices. However, these communication channels are mostly insecure. In addition, with the limited access to the IoD network, synchronization of heterogeneous data using drones and execution of critical operations within the network become challenging tasks in such cases. The UAV-based applications are used for time-sensitive missions, such as disaster management and battlefield surveillance systems. Due to their adaptation of insecure communication methods, they become vulnerable to interception or eavesdropping attacks by malicious persons. Moreover, drones operate with constrained resources, including limited computation power, low memory capacity, and less battery life, posing challenges for integrating complex security protocols. In addition, drones operate in hostile environments where they are susceptible to various attacks, such as Denial of Service (DoS) attacks, jamming, eavesdropping, hijacking, spoofing attacks, configuration and file tampering, and physical capture attacks [5]. Therefore, the drone faces challenges related to privacy, safety, and security for transmitting confidential, private, and classified information utilizing the communication protocols, like the MAVlink protocol, insecure Internet connections, or may have design security flaws [4]. The UAV networks also face notable challenges related

Received 5 May 2025; revised 25 August 2025; accepted 14 October 2025. Date of publication 17 October 2025; date of current version 4 February 2026. This research was supported in part by A*STAR, CISCO Systems (USA) Pte. Ltd and in part by the National University of Singapore under its Cisco-NUS Accelerated Digital Economy Corporate Laboratory under Grant I21001E0002. Recommended for acceptance by M. N. Aman. *(Corresponding authors: Basudeb Bera; Ashok Kumar Das.)*

Basudeb Bera and Biplab Sikdar are with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583 (e-mail: b.bera26@nus.edu.sg; bsikdar@nus.edu.sg).

Ashok Kumar Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India (e-mail: iitkgp.akdas@gmail.com).

This article has supplementary downloadable material available at https://doi.org/10.1109/TMC.2025.3622654, provided by the authors.

to data tampering and unauthorized access, as discussed by Golam et al. [6], along with potential security threats identified by Jacobsen et al. [7].

To overcome these security issues, various cryptographic methods adopted, including an elliptic curve Diffie-Hellman problem (ECDHP)-based authentication scheme to secure UAV communication in "flying ad-hoc networks (FANET)" [8], an attribute-based encryption (ABE) model to ensure data security in battlefields [9], a secure data aggregation and authentication models for resisting machine learning-based poisoning attacks [10] in IoD network, and authentication and access control mechanisms for UAV communication systems [11], [12]. However, most of these security measures are relies on computational hardness problem, such as integer factorization problem (IFP), discrete logarithm problems (DLP), and elliptic curve discrete logarithm problems (ECDLP).

It is worth noticing that the communications in a UAV network face various issues related to privacy, safety, and security. Furthermore, design vulnerabilities and security flaws increase these issues [4]. To overcome these security issues, traditional cryptographic techniques relying on IFP and DLP have been employed for decades for high-performance data sharing and identity verification in UAV networks. For example, ECDHP-based authentication scheme proposed in [8], ABE model for battlefields security in [9], access control and key agreement scheme in [13], and authentication and key agreement in [14] among others. However, with the significant evolution in quantum computing and adaptation of Shor's algorithm [15], [16], these public key cryptosystems become vulnerable to quantum attacks, and urgent consideration of alternatives to mitigate these quantum threats is needed. In contrast, cryptographic schemes, such as quantum key distribution, lattice-based protocols, multivariate polynomials, code-based cryptography, and hash-based cryptographic techniques, are considered secure against quantum attacks. Among these, lattice-based cryptography stands out as the most prominent security framework for quantum secure authentication and key agreement (AKE) protocols to resist quantum attacks [17].

Therefore, we propose a quantum-resistant lattice-based access control protocol for UAV communication to resist quantum threats. This scheme also provides robust security by not only resisting quantum attacks, such as quantum side-channel attacks [18], and quantum lattice reduction attacks [19], [20], but also providing security against known and unknown classical attacks.

The major contributions of this work are as follows:

- *Enhanced security features:* The proposed scheme provides a quantum-secure access control model relying on lattice-based ring learning with errors (RLWE) for anonymous drone communication system. It enhances the security measure for sharing a secure session keys utilizing both long-term and short-term secrets by resisting various attacks, including "Ephemeral Secret Leakage (ESL)" attacks under the "Canetti and Krawczyk (CK) adversary threat model" [21].
- *Innovative aspects:* The proposed scheme represents new dimensions in quantum-secure access control by integrating a fuzzy model for biometric data for drone applications. This preserves user anonymity and untraceability. Novel parameter selection enhances key agreement strategies and ensures security that remains unbreakable even with quantum computers. Both formal and informal comprehensive security analyses show its correctness, ensure validity, and resist against various attacks in both quantum and classical scenarios.
- *Technical advantages:* The proposed scheme demonstrates the technical advantages compared with existing works through comparative analysis, performance evaluations, authentication times, security and functionality features, scalability, applicability, and efficiency in real-world applications.
- *Experimental validation:* A real-time testbed experiment on Raspberry Pi 4 (model B) and laptop devices equipped with the cryptography 37.0.2 library is conducted to assess the computational overhead of various cryptographic primitives along with energy consumption. These experimental results enhance the technical advantages claimed in our proposed scheme. The security verification using widely-adopted verification tools like Scyther and Tamarin validates against known classical and advanced attacks.

The rest of the paper is organized as follows. Section II presents a comprehensive literature survey concerning access control and authentication schemes in IoT-based drone applications. Section III highlights the fundamental mathematical concept used in the proposed scheme, whereas Section IV presents the various phases of the proposed scheme. In Section V, we provide a detailed security analysis under Real-Or-Random (ROR) model and Section VI presents security verification using Scyther tool and Tamarin prover tool. A real-time testbed experiments highlights in Section VII, while Section VIII conducts an extensive comparative analysis of our QRAC-UAV scheme along with other relevant existing schemes. Finally, Section IX offers concluding remarks on our proposed scheme.

II. Related Works

In 2019, Feng et al. [22] proposed a lattice-based authentication scheme for mobile devices, which provides security against some known attacks. Unfortunately, their model is vulnerable to spoofing and signal leakage attacks and fails to support user anonymity [23]. In 2020, Ever [24] suggested a robust security model for UAV communication, where mobile sinks and drones share a link. Their scheme allows mutual authentication and session key agreement and reduces communication overhead. However, their scheme is vulnerable to various attacks, such as quantum attacks and ephemeral secret leakage (ESL) attacks under the CK adversary threat model. In addition, this scheme does not offer anonymity, dynamic node addition, and increased complexity in managing authentication protocols in highly dynamic and large-scale drone networks. In 2021, Dabra et al. [25] proposed an authentication protocol relying on passwords and lattice-based cryptography. This scheme supports user anonymity; however, it fails to maintain untraceability, and it is vulnerable to replay attacks. In 2022, Ding et al. [26] revealed that their scheme is susceptible to signal leakage attacks when the master key is reused. In 2021, Islam and Basu [27]

proposed a password and lattice-based user AKE protocol for mobile communication. This scheme resists quantum attacks and maintains lightweight computational requirements. Although this scheme resists attacks like replay, offline/online password guessing, and man-in-the-middle (MiTM) attacks, it exposes users' real identities over the public channel; as a result, it fails to offer user anonymity and untraceability property.

In 2021, Zhang et al. [28] proposed a three-factor authentication scheme based on password, biometrics, and smart devices for UAV communication networks. This scheme achieves communication efficiency utilizing BPV-FourQ and an ECC technique, making it suitable for resource-constrained IoD environments. Unfortunately, this scheme cannot resist replay attacks and fails to offer user anonymity [29]. In addition, this scheme is vulnerable to quantum attacks. In 2021, Chang et al. [30] designed a three-factor authentication protocol for IoT communications comprising a password, biometrics, and a smart device. This scheme achieves user anonymity and offers mutual authentication and session key agreement. Although it is lightweight and suitable for resource-constrained IoT devices, it is vulnerable to replay, privileged insider, and quantum attacks, as well as ESL attacks under the CK adversary model. In 2022, Feng et al. [31] designed a blockchain-based authentication for cross-domain communication in drone networks. This scheme offers a decentralized trust management system and ensures transparency, immutability, and security. However, this scheme requires high computational and storage costs for blockchain operations and faces challenges for resource-limited drones. In addition, this scheme is vulnerable to ESL attacks under the CK-adversary model. In 2023, Irshad et al. [32] suggested a software-defined networking (SDN)-based access control for industrial Internet of Things (IIoT) and cyber-physical systems (CPS). This scheme ensures dynamic, flexible, and scalable security for managing industrial networks and resists unauthorized access and insider attacks. However, this scheme fails to resist quantum attacks, requires huge computational and communication costs, and faces a single-point failure issue.

In 2023, Mishra et al. [33] designed an RLWE-based communication scheme for IoD networks that resists quantum attacks. This scheme resists unauthorized access and offers secure transmissions within IoD environments. However, this scheme requires high communication costs, making it impractical for real-time resource-constrained applications. In addition, it fails to preserve anonymity and untraceability properties. In 2023, Rewal et al. [23] developed a lattice-based key agreement protocol for mobile communication that resists quantum attacks. This scheme offers forward secrecy and ensures long-term session key security. However, this scheme reveals users' real identities over the communication channel; as a result, it fails to preserve user anonymity and untraceability. In 2023, Ayub et al. [34] developed an ECC-based authentication protocol for smart grid applications. Unfortunately, this scheme is vulnerable to ESL attacks under the CK-adversary model and quantum attacks. In 2023, Hu et al. [35] designed an ECC-based authentication protocol for IoT applications. However, their protocol fails to resist denial-of-service (DoS) attacks and does not ensure anonymity. Moreover, after compromising a third party's secret information, an adversary can expose all data associated with the session key, and as a result, it is vulnerable to insider privilege and MiTM attacks [36].

Safkhani et al. [37] proposed an ECC-based authentication model for smart grid applications, where the user is equipped with a secure and reliable PUF function for secure message exchanges. However, utilizing an ECC-based model, this scheme is vulnerable to quantum attacks in the post-quantum era. Chaudhary et al. [38] designed an AKE protocol for IoT applications, where they establish a session key between users via a server relying on RLWE lattice-based hardness and a hash function. Unfortunately, their scheme is vulnerable to replay attacks and needs high computation and communication costs, making it impractical in real-world scenarios. In 2024, another AKE scheme is designed by Chaudhary et al. [39] for mobile users based on the same RLWE-hardness and a cryptographic hash function. However, their scheme also fails to resist replay attacks and incurs significant computation and communication overheads. In 2024, Ahmad and Jagatheswari [40] proposed an RLWE-based AKE protocol for IoT-based medical applications in the post-quantum era. In their scheme, the user and sensor node shared a session key by sharing their real identities over the communication channel. Thus, their scheme fails to resist anonymity and untraceability properties and is vulnerable to replay attacks.

TABLE I
USED NOTATIONS AND THERE DESCRIPTION

Notation	Description
U, DR, RA	A user, drone, and registration authority
ID, ID_i	Identity of U and DR_i
pw, Bio	Password and biometric data of U
$Cha(\cdot), Mod_2(\cdot)$	Characteristic and modular function
$s \in \chi_\gamma$	Master secret key for RA from discrete Gaussian distribution χ_γ with a standard deviation of γ
n, p	A security parameter (power of 2, i.e., $n = 2^l, l > 0$ and odd large prime
$\mathbb{Z}$	Set of all integers
$\mathbb{Z}_p$	A finite field of prime order p, $\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$
$x \in \mathbb{Z}_p$	User's secret key
$x^n + 1$	An irreducible ($2n$-th cyclotomic polynomial) over $\mathbb{Z}$ of degree n
R, R_p	Polynomial rings: $\frac{\mathbb{Z}(x)}{<x^n+1>}$ and $\frac{\mathbb{Z}_p(x)}{<x^n+1>}$
$h(.)$	One way hash function
TS_i	i^{th} timestamp
ΔT	Maximum message transmission delay
SK, SKV	A session key and its verifier

III. MATHEMATICAL PRELIMINARIES

In this section, we discus mathematical preliminaries related to RLWE problems and the notations and their meaning are presented in Table I.

A. Ring Learning With Error

Let $\mathbb{Z}$ be the set of all integers and $n \in \mathbb{Z}$ be a security parameter with a power of 2, that is, $n = 2^l, l > 0$. Also, let $\mathbb{Z}[x]$ and $\mathbb{Z}_p[x]$ be the ring of polynomials over $\mathbb{Z}$ and $\mathbb{Z}_p$, respectively, where the coefficients of all polynomials in $\mathbb{Z}_p[x]$ are reduced to modulo p, and $p \in \mathbb{Z}$ be a large prime number. We define a polynomial ring R as $R = \frac{\mathbb{Z}[x]}{<x^n+1>}$, where $(x^n + 1)$

is an $2n$th cyclotomic polynomial (irreducible polynomial) over $\mathbb{Z}$, and similarly, $R_p = \frac{\mathbb{Z}_p[x]}{<x^n+1>}$, where each coefficient of the polynomial ring R_p is reduced modulo p.

Any element $b \in R$ express as $b = b_0 + b_1 \cdot x + b_2 \cdot x^2 + \cdots + b_{n-1} \cdot x^{n-1}$, then the norms L_2 and L_∞ can be defined as $||b|| = \sqrt{b_0^2 + b_1^2 + \cdots + b_{n-1}^2}$ and $||b||_\infty = \max\{|b_i|\}_{i=1}^{n-1}$. Let χ_γ be a discrete Gaussian distribution [41] over R_p, where $\gamma > 0$ is a real number and represents the standard deviation of χ_γ.

Lemma 1: Let $\mathbf{a}, \mathbf{b} \in R$ be any arbitrary elements. Then, they satisfy the inequality $||\mathbf{a}.\mathbf{b}||_\infty \leq n||\mathbf{a}||_\infty||\mathbf{b}||_\infty$ and $||\mathbf{a}.\mathbf{b}||_2 \leq \sqrt{n}||\mathbf{a}||_2||\mathbf{b}||_2$ [42], where l_2 norm and l_∞ norm are defined for a vector $\mathbf{x} \in R$ as $||\mathbf{x}||_2 = \sqrt{\sum_i |x_i|^2}$ and $||\mathbf{x}||_\infty = \max_i |x_i|$, respectively.

Proof: For further details regarding the proof of Lemma 1, please refer to [42] and [43].

Lemma 2: For $\gamma = \omega(\sqrt{log_2 n})$ be any positive real number and $\alpha = \gamma\sqrt{n}$, the inequality $Pr_{r \leftarrow \chi_\gamma}[||r|| > \alpha] \leq \frac{2}{2^n}$ holds [41], where $Pr[E]$ denotes the probability of an event E.

Proof: The proof for Lemma 2 can be found in [41] and [43].

Let ${\mathbb{Z}_p}^* = \{-\lfloor \frac{p}{4} \rfloor, \ldots, \lfloor \frac{p}{4} \rfloor\}$ be a subset of $\mathbb{Z}_p = \{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\}$. Let x be a variable which varies in the set $\mathbb{Z}_p$. Then, a characteristic function $Cha(\cdot)$ can be defined as:

$$Cha(x) = \begin{cases} 0, \text{if} & x \in {\mathbb{Z}_p}^* \\ 1, \text{if} & x \notin {\mathbb{Z}_p}^* \end{cases}. \tag{1}$$

The modular function $Mod_2 : \mathbb{Z}_p \times \{0,1\} \rightarrow \{0,1\}$ is defined as $Mod_2(a,b) = (a + b.\frac{(p-1)}{2}) \pmod p \pmod 2$, where $a \in \mathbb{Z}_p$ and $b = Cha(b)$ [42], [44]. The function Mod_2 satisfies Lemma 3.

Lemma 3: Let x, y be any two arbitrary elements of R_p, where p is an odd prime and $|y| < \frac{p}{8}$. If $d = x + 2.y$ and $e = Cha(x)$, then $Mod_2(x,e) = Mod_2(d,e)$ holds.

Proof: The details proof of Lemma 3 is provided in [42].

The functions $Cha(\cdot)$ and $Mod_2(\cdot)$ can be expanded to apply to the ring R_p using the following approach. Given an element $b = b_0 + b_1 \cdot x + b_2 \cdot x^2 + \cdots + b_{n-1} \cdot x^{n-1} \in R$ can be present into a vector form as $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})$. Therefore, for any vector $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) \in \{0,1\}^n$, we can define the two function $Cha(\cdot)$ and $Mod_2(\cdot)$ as $Cha(\mathbf{b}) = (Cha(b_0), Cha(b_1), \ldots, Cha(b_{n-1}))$ and $Mod_2(\mathbf{b}, \mathbf{a}) = (Mod_2(b_0, a_0), Mod_2 b_1, a_1, \ldots, Mod_2(b_{n-1}, a_{n-1})$, respectively.

The RLWE problem states that for a given polynomial and the number of given polynomial pairs $(x, y = x.s + e) \in R_p \times R_p$, it is hard to find the unknown polynomials $s, e \in R_p$ chosen from Gaussian distribution.

Definition 1 (Ring Learning With Error (RLWE)). Let $A_{s,\chi_\gamma} = (x, y)$ be a sample from $R_p \times R_p$, x be chosen uniformly from R_p and $y = x.s + e$, where $s, e \leftarrow \chi_\gamma$ are chosen uniformly. The $RLWE(p, \gamma)$ problem states that it is hard to distinguish the elements of A_{s,χ_γ} from the uniform distribution on $R_p \times R_p$ in polynomial time by the adversary [43].

Definition 2 (Pairing with Error (PWE) Problem). For a function $f : R_p \times R_p \rightarrow \{0,1\}$, where $f(x,s) = Mod_2(x.s, Cha(x.s))$, the objective of the PWE is to determine $f(x,s)$ for the unknown values of $s, e \in \chi_\gamma$, given $x, y, a \in R_p$, where $y = a.s + 2.e$ [22].

Definition 3 (Decision Pairing with Error (DPWE) Problem). Given the values of $a, b, c, d \in R_p$, the goal of the DPWE is to determine whether (a, c) is uniformly random in $R_p \times R_p$, where $a = b.s + 2.e$ and $c = d.s + 2.e'$, with the unknown values of $s, e, e' \in \chi_\gamma$ [22], [43].

The RLWE problems can be effectively reduced to the following problems with the condition that if the PWE problem in Definition 2 or DPWE problem in Definition 3 can be solved efficiently in polynomial time, then any quantum computer can also solve the RLWE problem in polynomial time.

B. Biometrics and Fuzzy Extractor

Biometric data and user passwords can form the basis for access control in Internet of Drones systems, where these credentials are employed to authenticate a user's identity. To achieve this, a fuzzy extractor function is employed. This function generates a uniformly random string known as the biometric secret, along with a public parameter, using the biometric template. The process adheres to a predefined error tolerance value denoted as e_t [45], [46].

Definition 4 (Fuzzy extractor): A fuzzy extractor F_e is represented as a tuple $(\mathcal{B}, m, l, e_t, \epsilon)$, where $\mathcal{B}$ denotes the metric space, m signifies the min-entropy of a distribution on $\mathcal{B}$, l represents the number of bits in the biometric secret σ, and ϵ refer to the statistical difference between two given probability distributions, specifically $< \sigma, \tau >$ and $< U_l, \tau >$ with $l = m - 2\log(\frac{1}{\epsilon}) + O(1)$. Here, U_l denotes the uniform distribution on l-bit binary strings. The F_e consists of the following two algorithms, namely $Gen(\cdot)$ and $Rep(\cdot)$:

- $Gen(\cdot)$*:* This is a probabilistic algorithm that accepts an original biometric data $Bio \in \mathcal{B}$ as input and generates a biometric secret key $\sigma \in \{0,1\}^l$ along with a public reproduction parameter τ as its outputs, that is, $Gen(Bio) = \{\sigma, \tau\}$.
- $Rep(\cdot)$*:* This is a deterministic reproduction algorithm that takes noisy biometric data $Bio' \in \mathcal{B}$ and the public reproduction parameter τ as input. It then reproduces (recovers) the biometric secret key σ. Specifically, $Rep(Bio', \tau) = \sigma$ with the condition: the Hamming distance $HD(Bio, Bio') \leq e_t$ is satisfied.

If we measure the "Hamming distance between the original biometric template Bio and the current biometric template Bio'" and find it to be d, and if the number of bits in the input biometric is b, then we can establish $e_t = \frac{d}{b}$. The advantage of an adversary in successfully guessing the biometric secret key $\sigma \in \{0,1\}^l$ is approximately $\frac{1}{2^l}$ [46].

IV. Proposed QRAC-UAV Scheme

In this section, we elaborate various phases of the proposed "**Q**uantum **R**esistant lattice-based **A**ccess **C**ontrol scheme for **UAV**-assisted Internet-of-drones applications," called as **QRAC-UAV**.

Fig. 1. Network model for QRAC-UAV.

A. System Model

This section presents a system model combing with a network and an adversary model for the proposed QRAC-UAV scheme.

1) Network Model: In this scheme, we assume a generalized network model of UAV applications, where drones are deployed to deliver various packages and medicines in a smart city, hospitals and emergency services, and also play a key role in firefighting to control fires in wildlife monitoring systems. In each scenario, the drones are building blocks operated by the respective authorities. The network model of the proposed scheme is presented in Fig. 1, where we consider the network components to be fully trusted authorities (RA), users (U) equipped with smart drone controllers (SDC), and drones (DR). The RA is responsible for registering U and DRs through a secure channel or via offline before their deployment in their respective functioning zones. In this model, SDC possesses sufficient computational power for lattice-based operations. After completing the registration process, they can communicate through wireless media. We also assume U and DR establish a secure session key through the wireless channel prior to exchanging information.

2) Adversary Model: In this proposed scheme, network components, like DRs and U, communicate and share sensitive information over the wireless public channel. Since the public channel is not secure enough, this raises the security challenges. Therefore, we consider various widely-adopted adversary models, such as Dolev-Yao (DY) [47], Canetti and Krawczyk (CK) [21], and the extended CK-adversary (eCK) models [48], [49].

• *DY and CK adversary models:* According to the DY adversary model, an adversary $\mathcal{A}$ can have the ability to eavesdrop on the communicated messages and manipulate, delete, or insert fake content into the communication channel. Whereas, under the CK-adversary model, $\mathcal{A}$ has enhanced capacities for compromising the communication channels. As a result, $\mathcal{A}$ can not only delete, modify, or insert malicious content but also compromise a session state and then reveal the short-term and long-term secret credentials that are used to build a session key in that session. In addition, $\mathcal{A}$ is also capable of launching a dictionary attack to guess (offline/online) the U's passwords that are used to log in to the local device.

• *eCK adversary model:* The extended CK-adversary (eCK) adversary model is a variation of the Canetti-Krawczyk (CK) adversary model. According to the eCK model, $\mathcal{A}$ may possess additional capabilities compared to the traditional CK model, such as $\mathcal{A}$ can control the entire network and can re-route, change, and drop messages as it sees fit. These supplementary capabilities may include the active execution of possible query sequences (for example, a session key reveal query on a specific session ID, say sid), which compromise the session's freshness. Under this eCK model, $\mathcal{A}$ is allowed to create a sequence of queries, eventually performs a $Test(sid)$ query, receives a value C, and after some time later, $\mathcal{A}$ has to guess whether C was the correct session key or a random value. After revealing both the long-term and short-term secrets, $\mathcal{A}$ reveals the session key of sid (or its corresponding session sid^*).

• *Quantum adversary attacks:* We also consider that the DRs can operate hostile environment, where $\mathcal{A}$ can physically capture the DRs using any of the techniques: 1) shoot it down with a gun, 2) use anti-drone drones, and 3) use net-firing anti-drone guns [50]. Next, $\mathcal{A}$ can launch quantum computer power side-channel attacks, such as power analysis attacks [18], [51] and then extract all stored information from the compromised DR's non-tamper-proof memory. Additionally, $\mathcal{A}$ can have the capacity to launch a quantum lattice reduction attack for recovering a short vector for secret session keys [52].

B. Detailed Decription of Various Phases

1) Initial Setup Phase: In this phase, the RA sets the some initial parameters using the following steps:

Step 1: The RA selects a large odd prime number p and an integer $n \in \mathbb{Z}_p$, such that $p \pmod{2n} \equiv 1$.

Step 2: Next, the RA picks a discrete Gaussian distribution with a standard deviation of γ, denoted as χ_γ and the RA defines a ring $R_p = \frac{\mathbb{Z}_p[v]}{v^n+1}$, where $p > 16\gamma^2 n^{3/2}$.

Step 3: The RA selects $a \in R_p$ and randomly samples $s \leftarrow \chi_\gamma$ as its own master secret key. The RA also defines a hash function $h : \{0,1\}^* \rightarrow \{0,1\}^{l_b}$, where l_b is a fixed hash output length. Here, the hash function $h(\cdot)$ is considered as SHA-256, since it is post quantum secure (for more details, please see ETSI White Paper No. 8 [53]).

Step 4: The RA picks a one-way hash function, say H_1, whose input can be any random string of fixed length l and whose output is an element in χ_γ, defined as $H_1 : \{0,1\}^l \rightarrow \chi_\gamma$. This is a random oracle and its outputs are sampled from χ_γ [54].

Step 5: Finally, the RA publishes the parameters $\{n, p, a, \chi_\gamma, h(\cdot), H_1\}$ and retains s as the master secret key.

2) Registration Phase: In this phase, the RA registers U and DR via offline or through a secure channel with the following steps:

- *User Registration Phase:* A user U registers a smart drone controller SDC with the RA as follows:
  * *UReg1:* User U picks a password pw, a unique identity ID, and a biometric data Bio using the biometric sensor installed on the SDC. U then generates a random number $x \in \mathbb{Z}_p$, a biometric secret σ, and a public reproduction parameter τ using the fuzzy extractor probabilistic generation function $Gen(\cdot)$ [45] as $Gen(Bio) = \{\sigma, \tau\}$. Next,

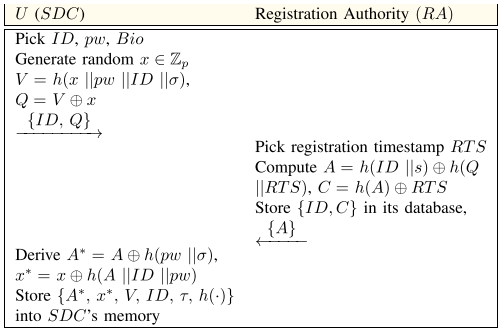

Fig. 2. Summary of the user registration phase.

U computes $V = h(x \,||pw\, ||ID\, ||\sigma)$ and $Q = V \oplus x$. U sends the registration request with $\{ID, Q\}$ to the RA.

* *UReg2:* The RA computes $A = h(ID\ ||s) \oplus h(Q\ ||RTS)$ and $C = h(A) \oplus RTS$, where RTS is registration timestamp. The RA then sends the registration credential $\{A\}$ to U through the same channel and stores $\{ID, C\}$ in its database.

* *UReg3:* Next, U calculates $A^* = A \oplus h(pw\ ||\sigma)$, $x^* = x \oplus h(A\ ||ID\ ||pw)$, and stores $\{A^*, x^*, V, ID, \tau, h(\cdot)\}$ in their SDC's memory. Fig. 2 presents a summary of this phase.

- *Drone Registration Phase:* DR registration is done with the RA by the following steps:

  * *DReg1:* The RA selects a unique and distinct real identity ID_i, a temporary identity TID_i, and a registration timestamp RTS_i. The RA randomly samples $y_i \leftarrow \chi_\gamma$. The RA computes $D = h(ID_i\ ||s\ ||y_i\ ||RTS_i)$ and stores the information $\{TID_i,\ ID_i,\ D,\ h(ID)\}$ in the DR's memory.

  * *DReg2:* The RA then deletes the DR's secrets y_i and D from its memory, adds ID_i to its own database, and sends the values $\{TID_i, ID_i\}$ to the user.

3) Login and Access Control Phase (LACP): LACP is executed by the following steps:

LACP1: User U first enters their password say pw', unique identity ID, and current biometric, say Bio'. U then derives the biometric secret key σ' using Bio' and τ by the reproduction function $Rep(\cdot)$ [45] as $\sigma' = Rep(Bio', \tau)$ with the condition that $HD(Bio', Bio) \leq et$, where $HD(\cdot)$ denotes the "Hamming distance between the registered biometric template Bio and the current biometric template Bio'," and e_t is the pre-defined error tolerance threshold value. Next, U computes $A' = A^* \oplus h(pw'\ ||\sigma')$, $x' = x^* \oplus h(A'\ ||ID\ ||pw')$ and the verification factor V' as $V' = h(x\ ||pw'\ ||ID\ ||\sigma')$. U verifies the condition: $V' = V$. If it is verified, entered password, identity, and biometric data all are correct, that is, $(pw = pw',\ \sigma = \sigma',\ x = x')$. Then, U is allowed to log in to the SDC. Next U execute Algorithm 1 to construct a session key between DR_i.

LACP2: Next, U selects r_c and f_c from χ_γ, generates a fresh timestamp TS_1, and computes $x_c = a.r_c + 2.f_c$. Next, U computes $x'_c = x_c + H_1(TS_1\ ||h(ID)\ ||ID_i)$, $M_c = (h(ID)||\ ID_i) \oplus h(V\ ||r_c\ ||TS_1\ ||ID\ ||x)$, and $T_c = h(M_c\ ||TID_i\ ||TS_1\ ||x_c)$. U constructs an access control request message $msg_1 = \{T_c,\ M_c,\ TS_1,\ x'_c,\ TID_i\}$ and sends it to the associated drone DR_i over the public channel.

LACP2: DR_i receives the message msg_1 from U at timestamp TS_1^* and executes Algorithm 2 to construct the session key. DR_i first verifies its freshness using the condition: $|TS_1^* - TS_1| < \Delta T$, where ΔT is the "maximum message transmission delay" within the network. If this condition is met, DR_i derives $x_c = x'_c - H_1(TS_1\ ||h(ID)\ ||ID_i)$ and calculates $T'_c = h(M_c\ ||TID_i\ ||TS_1\ ||x_c)$. Then DR_i verifies $T'_c = T_c$, if it is verified, DR_i considers that $h(ID)$ has been verified, as it is hidden into M_c. DR_i then derives $h(V\ ||r_c\ ||TS_1\ ||ID\ ||x) = M_c \oplus (h(ID)||\ ID_i)$. Next, DR_i selects randoms r_i and f_i from χ_γ, generates a fresh timestamp TS_2, and computes $x_i = a.r_i + 2.f_i$ and $x'_i = x_i + H_1(TS_2\ ||h(ID)\ ||ID_i)$. Next DR_i calculates $t_i = x_c.r_i$, $w_i = Cha(t_i)$, $u_i = Mod_2(t_i, w_i)$, $w'_i = w_i \oplus h(TS_2\ ||h(ID)\ ||ID_i)$, and $M_i = h(D\ ||r_i\ ||ID_i) \oplus h(TID_i\ ||ID_i\ ||u_i\ ||TS_2)$. After that, DR_i generates a session key SK as $SK = h(h(V\ ||r_c\ ||TS_1\ ||ID\ ||x)\ ||u_i\ ||h(D\ ||r_i\ ||ID_i)\ ||TS_2\ ||TS_1)$ and a session key verifier SKV as $SKV = h(SK\ ||TID_i\ ||M_i\ ||TS_2\ ||TS_1\ ||w_i\ ||x_i\ ||x_c)$. DR_i then builds a reply message msg_2 as $msg_2 = \{SKV,\ x'_i,\ M_i,\ TS_2,\ w'_i\}$ and sends it to U via the public channel.

LACP3: After receiving message msg_2 from DR_i at timestamp TS_2^*, U verifies its freshness using the condition: $|TS_2^* - TS_2| < \Delta T$. If this condition is satisfied, U derives $x_i = x'_i - H_1(TS_2\ ||h(ID)\ ||ID_i)$ and $w_i = w'_i \oplus h(TS_2\ ||h(ID)\ ||ID_i)$. Next, U computes $t'_i = x_i.r_c$, $u'_i = Mod_2(t'_i, w_i)$, and derives $h(D\ ||r_i\ ||ID_i) = M_i \oplus h(TID_i\ ||ID_i\ ||u'_i\ ||TS_2)$. Next, U constructs the session key SK' as $SK' = h(h(V\ ||r_c\ ||TS_1\ ||ID\ ||x)\ ||u'_i\ ||h(D\ ||r_i\ ||ID_i)\ ||TS_2\ ||TS_1)$ and the session key verifier SKV' as $SKV' = h(SK'\ ||TID_i\ ||M_i\ ||TS_2\ ||TS_1\ ||w_i\ ||x_i\ ||x_c)$. U then checks whether the condition $SKV' = SKV$ is valid. If it is validated, U believes that they have established the same session key $SK'(= SK)$. U proceeds by selecting a new timestamp TS_3 and a new temporary identity TID_N. U derives $TID_N^* = TID_N \oplus h(SK'\ ||TS_3\ ||TID_i)$, generates an acknowledgment $ACK = h(TID_N\ ||SK'\ ||TS_3\ ||TS_2)$, and constructs the acknowledgment message $msg_3 = \{ACK, TID_N^*, TS_3\}$. U updates TID_i corresponding to the real identity ID_i with the new one, TID_N, in the SDC's memory. Finally, U sends the acknowledgment message $msg_3 = \{ACK, TID_N^*, TS_3\}$ to DR_i through the public channel.

LACP4: Next, DR_i receives the message msg_3 from U at timestamp TS_3^* and verifies its freshness using the condition: $|TS_3^* - TS_3| < \Delta T$. If it is satisfied, DR_i derives $TID_N = TID_N^* \oplus h(SK\ ||TS_3\ ||TID_i)$, calculates $ACK' = h(TID_N\ ||SK\ ||TS_3\ ||TS_2)$, and checks whether $ACK' = ACK$. If it is verified, DR_i also believes that they both established the same session key $SK(= SK')$ and then updates TID_i with the new TID_N in its memory. The summary of this phase is shown in Algorithms 1 and 2.

A detailed flowchart of the proposed scheme is presented in Fig. 3.

Algorithm 1: U's Session key Construction.

procedure USESSIONKEY($ID, (ID_i, TID_i), A^*, x^*, V, \Delta T$)
  $r_c, f_c \leftarrow \chi_\gamma$, timestamp TS_1
  $x_c = a.r_c + 2.f_c$
  $x_c' = x_c + H_1(TS_1 ||h(ID) ||ID_i)$
  $M_c = (h(ID)||ID_i) \oplus h(V||r_c||TS_1||ID||x)$,
  $T_c = h(M_c||TIDhown_i||TS_1||x_c)$
  $msg_1 \leftarrow \{T_c, M_c, TS_1, x_c', TID_i\}$, send it to DR_i
  Receive msg_2 at TS_2^* from the DR_i
  if $|TS_2^* - TS_2| < \Delta T$ **then**
    $x_i = x_i' - H_1(TS_2 ||h(ID) ||ID_i)$
    $w_i = w_i' \oplus h(TS_2 ||h(ID) ||ID_i)$
    $t_i' = x_i.r_c$, $u_i' = Mod_2(t_i', w_i)$
    $h(D||r_i||ID_i) = M_i \oplus h(TID_i||ID_i||u_i'||TS_2)$
    $SK' = h(h(V||r_c||TS_1||ID||x)||u_i'$
    $||h(D||r_i||ID_i)||TS_2||TS_1)$
    $SKV' = h(SK'||TID_i||M_i||TS_2||TS_1||w_i||x_i||x_c)$
    if $SKV' = SKV$ **then**
      Pick new TID_N, timestamp TS_3
      $TID_N^* = TID_N \oplus h(SK'||TS_3||TID_i)$
      $ACK = h(TID_N||SK'||TS_3||TS_2)$
      $msg_3 \leftarrow \{ACK, TID_N^*, TS_3\}$, send it to DR_i
    else
      exit
    end if
    return (SK', TID_N)
  else
    return *exit*
  end if
end procedure

Algorithm 2: DR_i's Session Key Construction.

procedure DRSESSIONKEY($ID_i, TID_i, D, h(ID), \Delta T$)
  Receive msg_1 at TS_1^* from U
  if $|TS_1^* - TS_1| < \Delta T$ **then**
    $x_c = x_c' - H_1(TS_1 ||h(ID) ||ID_i)$
    $T_c' = h(M_c ||TID_i ||TS_1 ||x_c)$
    if $T_c' = T_c$ **then**
      $h(V||r_c||TS_1||ID||x) = M_c \oplus (h(ID)||ID_i)$
      $r_i, f_i \leftarrow \chi_\gamma$
      Pick fresh timestamp TS_2
      $x_i = a.r_i + 2.f_i$, $t_i = x_c.r_i$
      $x_i' = x_i + H_1(TS_2 ||h(ID) ||ID_i)$
      $w_i = Cha(t_i)$, $u_i = Mod_2(t_i, w_i)$
      $w_i' = w_i \oplus h(TS_2 ||h(ID) ||ID_i)$
      $M_i = h(D||r_i||ID_i) \oplus h(TID_i||ID_i||u_i||TS_2)$
      $SK = h(h(V||r_c||TS_1||ID||x)||u_i$
      $||h(D||r_i||ID_i)||TS_2||TS_1)$
      $SKV = h(SK||TID_i||M_i||TS_2||TS_1||w_i||x_i||x_c)$
      $msg_2 \leftarrow \{SKV, x_i', M_i, TS_2, w_i'\}$
      Send msg_2 to U and then wait
      Receive msg_3 at TS_3^* from U
      if $|TS_3^* - TS_3| < \Delta T$ **then**
        $TID_N = TID_N^* \oplus h(SK||TS_3||TID_i)$
        $ACK' = h(TID_N||SK||TS_3||TS_2)$
        if $ACK' = ACK$ **then**
          $TID_i \leftarrow TID_N$
          return (SK, TID_N)
        else
          exit
        end if
      else
        exit
      end if
    else
      exit
    end if
  else
    exit
  end if
end procedure

4) Password and Biometric Update Phase: To change or update user old password (pw_o) along with their biometric data (Bio_o), U needs to execute the following steps:

PBUP1: User U enters their ID, old password pw_o, and old biometric data Bio_o. U then calculates the biometric secret key σ_o corresponding to the inputs Bio_o and τ using $Rep(\cdot)$ function as $\sigma_o = Rep(Bio_o, \tau)$ with the condition: $HD(Bio_o, Bio) \leq e_t$, where $HD(\cdot)$ denotes the "Hamming distance between the registered biometric template Bio and the current biometric template Bio_o," and e_t is the predefined error tolerance threshold value. U then computes $A_o = A^* \oplus h(pw_o ||\sigma_o)$, $x = x^* \oplus h(A_o ||ID ||pw_o)$, $V_o = h(x ||pw_o ||ID ||\sigma_o)$, and verifies the condition: $V_o = V$. If it is verified, U successfully logs in to the SDC.

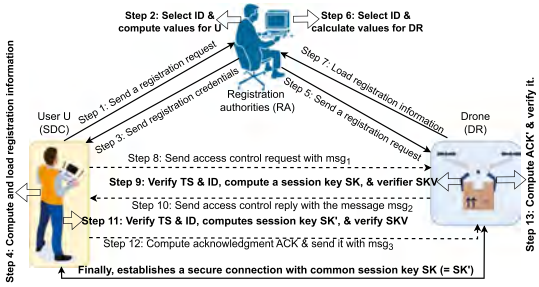

Fig. 3. A flowchart of the proposed scheme.

PBUP2: Next, U enters a new password (pw_n) and a biometric template (Bio_n), and then generates the biometric secret σ_n and the "public reproduction parameter τ_n" using the $Gen(\cdot)$ function as $Gen(Bio_n) = \{\sigma_n, \tau_n\}$. Next, U calculates $V_n = h(x ||pw_n ||ID ||\sigma_n)$ and $Q_n = V_n \oplus x$. U sends the password and biometric update request with $\{ID, Q_n, h(A_o)\}$ to the RA.

PBUP3: The RA checks the identity ID. If it exists, the RA derives $RTS = C \oplus h(A_o)$, computes $A_n = h(ID ||s) \oplus h(Q_n ||RTS)$, and $C_n = h(A_n) \oplus RTS$. RA then sends the credential A_n to U, stores $\{ID, C_n\}$ in its memory, and deletes A_n from its memory.

PBUP4: Next, U calculates $A_n^* = A_n \oplus h(pw_n ||\sigma_n)$, $x_n^* = x \oplus h(A_n ||ID ||pw_n)$, and stores $\{A_n^*, x_n^*, V_n, ID, \tau_n, h(\cdot)\}$ into their SDC's memory.

5) Dynamic Drone Addition Phase: A new drone (DR_d) can be added through the following process:

DDA1: The RA selects a unique and distinct real identity ID_d, a temporal identity TID_d, and a registration timestamp RTS_d. Then, the RA randomly selects samples y_d from χ_γ and computes $D_d = h(ID_d ||s ||y_d ||RTS_d)$. Subsequently, it loads the information $\{TID_d, ID_d, D_d, h(ID)\}$ into the memory of DR_d.

DDA2: The RA proceeds to delete the secrets y_d and D_d related to DR_d from its own memory. It also stores ID_d in its database and sends the values $\{TID_d, ID_d\}$ to the user.

V. SECURITY ANALYSIS

In this section, we provide both formal and informal security analyses of the proposed scheme, which proves that the proposed scheme resists a range of active and passive classical as well as quantum attacks.

A. Proof of Correctness

Claim: The established session key $SK'(= SK)$ between a drone DR_i and user U remains the same.

Proof: In this proposed protocol, if $u_i \neq u_i'$, U and DR_i cannot establish the same session key $SK'(= SK)$. However, if we can prove that $u_i = u_i'$, it would establish the correctness

of the session key. This can be prove through the following equations:

$$t_i = x_c.r_i = a.r_c.r_i + 2.f_c.r_i, \tag{2}$$

$$t_i' = x_i.r_c = a.r_i.r_c + 2.f_i.r_c. \tag{3}$$

After subtracting (3) from (2), we have

$$t_i - t_i' = 2.(f_c.r_i - f_i.r_c). \tag{4}$$

From Lemma 1, we have

$$\begin{aligned} ||f_c.r_i - f_i.r_c|| &\leq ||f_c.r_i|| + ||f_i.r_c|| \\ &< \sqrt{n}||f_c||_2.||r_i||_2 + \sqrt{n}||f_i||_2.||r_c||_2 \\ &< \sqrt{n}.\gamma^2.n + \sqrt{n}.\gamma^2.n \\ &= 2.\gamma^2.n^{3/2} \\ &< p/8; \quad \text{where} \quad p > 16\gamma^2 n^{3/2}. \end{aligned} \tag{5}$$

Using Lemma 3, we conclude that

$$\begin{aligned} u_i' &= Mod_2(t_i', w_i) = Mod_2(t_i', Cha(t_i)) \\ &= Mod_2(t_i, Cha(t_i)) = u_i. \end{aligned} \tag{6}$$

Therefore, using (6), we obtain: $SK = h(h(V||\ r_c||TS_1\ ||ID\ ||x)\ ||u_i\ ||h(D\ ||r_i\ ||ID_i)\ ||TS_2\ ||TS_1) = h(h(V\ ||r_c\ ||TS_1\ ||ID\ ||x)\ ||u_i'\ ||h(D\ ||r_i\ ||ID_i)\ ||TS_2\ ||TS_1) = SK'$.

B. Formal Security Analysis Under Real-Or-Random (ROR) Model

In this section, we have adopted the widely recognized Real-Or-Random (ROR) oracle model [55] for providing the security of the session key $SK(= SK')$ between a SDC and a DR_i. The semantic security of the proposed QRAC-UAV scheme is defined in Definition 5 and the advantage of $\mathcal{A}$ for breaking the session key security is mentioned in Theorem 1 (for more details, please see the supplementary material). The adversary $\mathcal{A}$ is permitted to execute all the queries outlined below. According to [56], all participants, including $\mathcal{A}$, have access to a collision-resistant one-way cryptographic hash function denoted as $h(\cdot)$, which can be considered equivalent to a random oracle denoted as $\mathcal{H}$. For details, please see the supplementary material.

Definition 5 (Semantic security): Let $S(\mathcal{A})$ denote an event, such that $\mathcal{A}$ can correctly guesses a bit b', equivalent to the bit b selected in the $Test$ oracle query, and let $Pr(S)$ denotes the probability of $S(\mathcal{A})$. Therefore, the advantage of $\mathcal{A}$, denoted as $Adv_{\mathcal{A}}^{QRAC-UAV}(t)$, for breaking the semantic security of QRAC-UAV within a polynomial time t is defined as the absolute probability of a random guess: $Adv_{\mathcal{A}}^{QRAC-UAV}(t) = |2Pr[S] - 1|$.

The proposed QRAC-UAV scheme achieves semantic security if: a) Σ_i^P and its partner consistently reach an *accept* state and compute the same session key, and b) the advantage $Adv_{\mathcal{A}}^{QRAC-UAV}(t)$ remains negligible (ϵ) for any probabilistic polynomial time-bounded adversary $\mathcal{A}$. Σ_i^P as the i^{th} instance of a participant denoted as P, where P can represent either U or DR.

Theorem 1. Let $Adv_{\mathcal{A}}^{QRAC-UAV}(t)$ denote the advantage of an adversary $\mathcal{A}$ for breaking the semantic security of the session key $SK\ (= SK')$ between U and DR_i in the proposed QRAC-UAV scheme within a polynomial time t. Then, $Adv_{\mathcal{A}}^{QRAC-UAV}(t) \leq \frac{Q_h^2}{|Hash|} + \frac{(Q_s+Q_e)^2}{|\chi_\gamma|} + 2(\max\{C'.Q_s^{s'}, \frac{Q_s}{2^l}\} + Adv_{\mathcal{A}}^{RLWE}(t))$, where $Hash$, Q_h, Q_e, Q_s, $|\chi_\gamma|$, l, and $Adv_{\mathcal{A}}^{RLWE}(t)$ are the range space of one-way collision-resistant hash function $h(\cdot)$, execute queries, send queries, range space of the discrete Gaussian distribution χ_γ, the number of bits in biometrics secret key σ, and advantage of breaking the RLWE problem in polynomial time t, respectively. The parameters C' and s' are the Zipf's parameters provided in [57].

Proof. For details, please see the supplementary material.

C. Informal Security Analysis

This section provides a security analysis of the proposed QRAC-UAV scheme, resists various active and passive attacks. The proofs of the Propositions 1–11 are provided in the supplementary material.

Proposition 1: QRAC-UAV is secure against replay attack.

Proposition 2: QRAC-UAV is resilient against Man in the Middle (MiTM) attack.

Proposition 3: QRAC-UAV is safe against drone impersonation attack.

Proposition 4: Stolen SDC device attack is protected by QRAC-UAV.

Proposition 5: QRAC-UAV is secure against offline/online password guessing attacks.

Proposition 6: Privileged-insider attack is protected in QRAC-UAV.

Proposition 7: QRAC-UAV is resilient against Ephemeral Secret Leakage (ESL) attack under the CK-adversary model.

Proposition 8: Both anonymity and untraceability are supported in QRAC-UAV.

Proposition 9: QRAC-UAV is safe against device physical capture attack.

Proposition 10: QRAC-UAV is secure against quantum lattice reduction attacks, including primal attack and dual attack.

Proposition 11: QRAC-UAV is secure against key reuse attacks.

VI. Formal Security Verification for QRAC-UAV Under Various Verification Tools

In this section, we provide security verification results utilizing state-of-the-art tools, like Tamarin Prover and Scyther to validate the security of the proposed scheme. The details of these tools and the results are also provided in the supplementary material.

A. Formal Security Verification Under Scyther Tool

In this section, we provide a security validation of the proposed QRAC-UAV scheme using Scyther tool.

Scyther is an automated verification tool for detecting any attacks of any security protocols [58], [59]. It ensures the termination and permits the validation of correctness under

Fig. 4. Simulation results using Scyther tool.

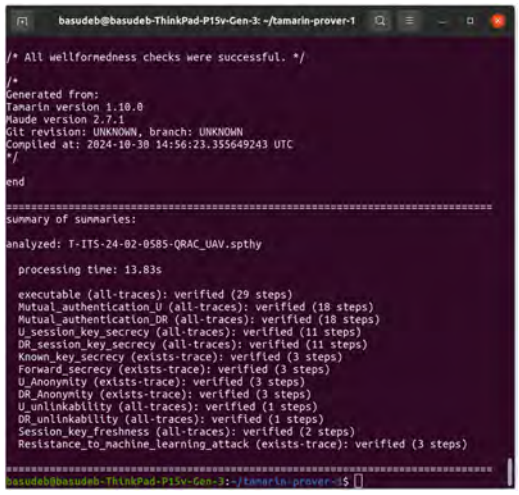

Fig. 5. Tamarin result of the proposed QRAC-UAV scheme.

unbounded number of sessions. It's user interface provides an analysis centered around classes of protocol behavior or potential attacks, rather than relying solely on individual attack traces. It works under predefined security threat models, such as the DY threat model, CK-adversary, eCK-adversary, among others, which eliminates the necessity for users to define adversary capabilities formally [60]. The details of this section can be found in Supplementary memorial.

The results presented in Fig. 4 confirmed that Scyther has not identified any attacks in the proposed scheme.

B. Formal Security Verification Under Tamarin Prover Tool

The Tamarin Prover is a tool for verifying security protocols that enables both attack discovery (falsification) and unbounded verification (proof). Security protocols can be defined using multiset rewriting models and can be analyzed for temporal first-order properties. This tool allows for modeling of number of equations for a cryptographic protocols by supporting various equational theories. The details of this result can be found in Supplementary memorial.

Tamarin uses *lemmas* to define the security properties of the protocol and it automatically generates verification results for these lemmas. If a **lemma** satisfies, which means it is **verified**; if not, it is marked as **falsified**. This tool also creates an attack graph for demonstrating the falsification of the verified property. For further details, readers are encouraged to refer the Tamarin tool manual https://tamarin-prover.com/.

Fig. 5 discloses the results of our analysis against the proposed QRAC-UAV protocol. From the perspectives of both the user **U** and the drone **DR**, the secrecy of the session key is maintained as the output of the result is **verified**. The mutual authentication is also successfully verified and ensured the freshness property. The results also indicates that the proposed scheme satisfies (**verified**) anonymity, forward secrecy, and unlinkability properties, that is, the attacker cannot find the session key or execute any known valid attacks.

VII. Experimental Setup and Results

In this section, we perform a practical testbed experiment using Raspberry Pi devices configured as either U or DR and a laptop considered as server platforms.

A. Testbed Experiment Using Raspberry PI

We have conducted timing measurements for various cryptographic operations utilizing the cryptography standard library, Cryptography 37.0.2. This library is widely acknowledged and provides Python developers to access of various cryptographic functionalities, such as symmetric encryption/decryption, one-way hash functions, key derivation, and more. Let T_h indicate the time required for computing a one-way hash function using Secure Hash Algorithm (SHA-256), T_{senc}/T_{sdec} are the time taken for Advanced Encryption Standard (AES) encryption and decryption operations, T_{eca}/T_{ecm} stand for the time required for elliptic curve point addition/ multiplication operations, T_{mtp} stand for the time taken to convert a message to elliptic curve point function, and T_{bp} indicate the time for bilinear pairing function.

For elliptic curve operations, we have considered a non-singular elliptic curve known as secp256r1 of the form $y^2 = x^3 + ax + b \pmod p$ (for more details, please refer to RFC5480). Each operation is performed 1000 iterations under the Raspberry PI configuration: Raspberry Pi 4 Model B configured with Raspberry Pi 4 Model B Rev 1.5, featuring a 64-bit Cortex-A72 processor clocked at 1800 MHz with 4 cores and 7.6 GB of RAM, running Ubuntu 20.04.6 LTS on an aarch64 architecture. Whereas, the server configured with Ubuntu 22.04 LTS, featuring 16GB of RAM and an Intel Core™ i7-9750H processor, CPU running at 2.60 GHz, equipped with 6 cores and 12 threads, operating on a 64-bit architecture with a 256GB SSD. We then calculated the maximum, minimum, and average execution times (in milliseconds) for each cryptographic primitives. We have taken the average times for each primitive and the results of these experiments are shown in Fig. 6 and

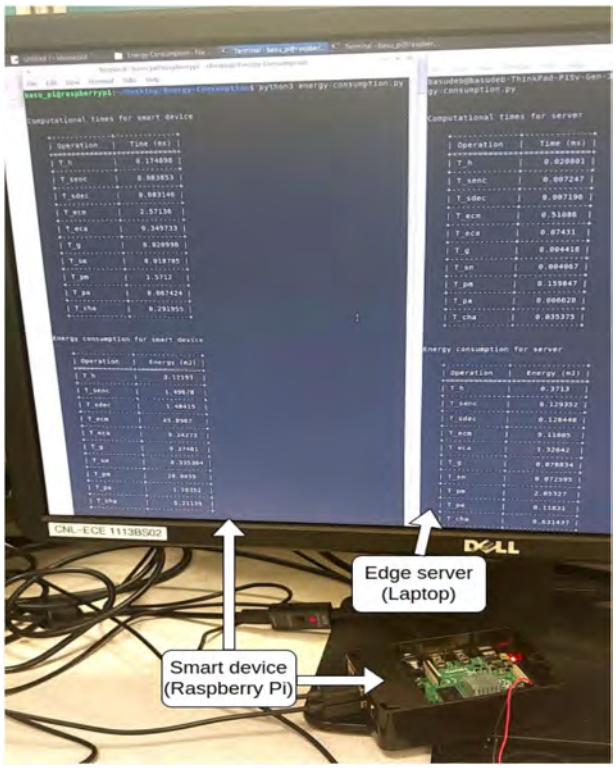

Fig. 6. Testbed results using Raspberry Pi as a smart device and server as a Laptop.

TABLE II
AVERAGE COMPUTATION TIMES (IN MS) AND ENERGY CONSUMPTION (IN MJ) OF CRYPTOGRAPHIC PRIMITIVES

Primitives	Computation cost (in ms)		Energy consumption cost (in mJ)	
	Smart device	Server	Smart device	Server
T_h	0.1748	0.0208	3.1219	0.3713
T_{senc}	0.0838	0.0072	1.4967	0.1293
T_{sdec}	0.0831	0.0071	1.4841	0.1284
T_{ecm}	2.5713	0.5108	45.8987	9.1188
T_{eca}	0.3497	0.0743	6.2427	1.3264
T_{mtp}	7.7039	0.6627	–	–
T_{bp}	52.533	8.262	–	–
T_g	0.0209	0.0044	0.3748	0.0788
T_{sm}	0.0187	0.0040	0.3353	0.0725
T_{pm}	1.5712	0.1598	28.0459	2.8532
T_{pa}	0.0674	0.0066	1.2035	0.1183
T_{cha}	0.2919	0.0353	5.2113	0.6314

Table II. We observe that the Mod_2 operation in R_p is essentially performed as an AND operation, which taken negligible time and it is disregarded in the analysis.

In addition, for lattice-based operations, let T_g, T_{sm}, T_{pm}, T_{pa}, and T_{cha} indicate the computation times for a sampling from the discrete Gaussian distribution χ_γ; scalar multiplication in quotient rings of polynomials R_p; polynomial multiplication in R_p; polynomial addition in R_p; and characteristic function computation in R_p, respectively. We consider a polynomial ($\in R_p$) size to 4096 bits. We also measure the energy consumption costs (in mili joule (mJ)) for cryptographic primitives. For the smart device, energy usage is 5.1 V and 3.5 A, and the server's energy consumption is under a configuration of 250 V and 3 A. The experimental results are shown in Fig. 6 and Table II.

TABLE III
COMPARATIVE ASSESSMENT ON COMMUNICATION COST

Scheme	No. of messages	Total cost (in bits)
Mishra et al. [33]	3	14018
Rewal et al. [23]	4	18626
Islam and Basu [27]	8	19648
Chaudhary et al. [38]	5	19490
Safkhani et al. [37]	2	1728
Chaudhary et al. [39]	4	14851
Dabra et al. [25]	3	9122
Feng et al. [22]	3	8962
Zhang et al. [28]	4	9984
Chang et al. [30]	4	3712
Irshad et al. [32]	3	4320
Proposed (QRAC-UAV)	3	10240

Note: Here $\nu = 100$ is considered, where $|S| = \nu$ in Zhang et al. [28].

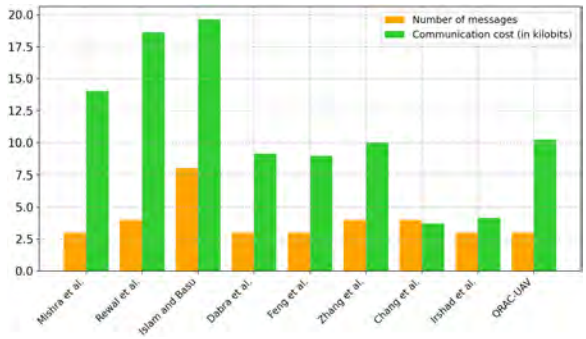

Fig. 7. Communication costs (in kilobits) along with number of messages.

VIII. COMPARATIVE COST EVALUATION

In this section, we conduct a comprehensive performance evaluation of the proposed QRAC-UAV scheme with other existing competing schemes. These schemes include those proposed by Mishra et al. [33], Rewal et al. [23], Islam and Basu [27], Dabra et al. [25], Feng et al. [22], Zhang et al. [28], Chang et al. [30], Ever [24], and Irshad et al. [32]. The comparative evaluation is based on communication costs, computation costs, energy consumption, authentication time, as well as security and functionality features.

A. Communication Cost Evaluation

To calculate communication cost, we assume random numbers are 160 bits, real or temporal identities are 160 bits, AES encryption/decryption key is 128 bits, timestamps are 32 bits, one-way hash function outputs (using the SHA-256) are 256 bits, elliptic curve points are 320 bits, elements in R_p are 4096 bits, and cha and w_i are 1 b each.

In the proposed QRAC-UAV, the access control phase is required the following three messages: $msg_1 = \{T_c, M_c, TS_1, x_c, TID_i\}$, $msg_2 = \{SKV, x_i, M_i, TS_2, w_i\}$, and $msg_3 = \{ACK, TID_N^*, TS_3\}$. These messages require (256 + 256 + 32 + 4096 + 160) = 4800 bits, (256 + 4096 + 256 + 32 + 256) = 4896 bits, and (256 + 256 + 32) = 544 bits, respectively, in total of 10240 bits. From Table III and Fig. 7, it is observed that the QRAC-UAV require significantly lower communication costs

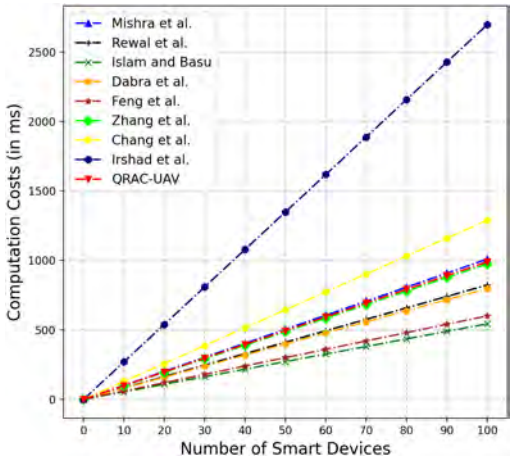

Fig. 8. Computation costs (in ms) versus the number of devices.

compared to the schemes of Mishra et al. [33], Rewal et al. [23], Islam and Basu [27], Chaudhary et al. [38], and Chaudhary et al. [39].

Although the proposed scheme incurs higher communication costs compared to those of Dabra et al. [25], Chang et al. [30], Irshad et al. [32], and Feng et al. [22], however, various critical security flaws has found in these schemes. Dabra et al.'s scheme is vulnerable to replay attacks, lacks support for untraceability, and has not been verified using security verification tools such as AVISPA, Scyther, or ProVerif, making it unreliable for real-world applications. Whereas, Chang et al.'s scheme is susceptible to "replay attacks", "ESL attacks under the CK-adversary model", and "privileged-insider attacks". Moreover, it does not support the dynamic device addition, which make it to scalability issues, and lacks of verification using AVISPA, Scyther, or ProVerif tools, and susceptible to quantum attacks. Irshad et al.'s scheme also lacks support for dynamic drone/device addition, making it impractical and unable to resist quantum attacks. In addition, Feng et al.'s scheme is vulnerable to replay attacks and lacks verification using AVISPA, Scyther, or ProVerif tools, which makes it impractical for real-world applications.

B. Computation Cost Evaluation

In computational cost calculation, we consider the access control phase described in Section IV-B3 and utilize the primitives values presented in Fig. 6 and Table II. In the proposed scheme, U incurs a computational cost of $8T_h + 4T_g + T_{sm} + 2T_{pm} + 3T_{pa} \approx 4.8453$ ms, while a drone DR requires computational cost of $8T_h + 3T_g + T_{sm} + 2T_{pm} + 2T_{pa} + T_{cha} \approx 5.0489$ ms. In total, they require computational cost of approximately $16T_h + 7T_g + 2T_{sm} + 4T_{pm} + 5T_{pa} + T_{cha} \approx 9.8942$ ms. Here, we consider the computation times for the primitive $H_1(\cdot)$ is similar to the time of T_g, that is, $T_{H_1} \approx T_g$, and the execution time for BPV and KDF functions in [28] is equivalent to the computation time for hash functions (T_h). It is worth noting that both Table IV and Fig. 8 indicate that our scheme incurs lower computational costs compared to Ever [24], Zhang et al. [28], Chang et al. [30], Mishra et al. [33], Safkhani et al. [37], and Irshad et al. [32]. It worth noticing that, the proposed scheme needs higher computational costs as compared to the scheme of Rewal et al. Islam and Basu, Dabra et al. and Feng et al. However, these scheme does not support all security requirement as mentioned in above. For example, Similarly, Islam and Basu fails to support user anonymity and untraceability properties, whereas Dabra et al. is vulnerable to replay attacks and lacks untraceability.

TABLE IV
COMPARATIVE ASSESSMENT ON COMPUTATION COST

Scheme	Mobile/U/IoT device	BS/Server
Mishra et al. [33]	$8T_h + 4T_g + 2T_{sm} + 5T_{pm} + 2T_{pa} + 2T_{cha} \approx 10.0940$ ms	$6T_h + T_{pm} \approx 0.2846$ ms
Rewal et al. [23]	$8T_h + 4T_g + 2T_{sm} + 2T_{pm} + 2T_{pa} + T_{cha} \approx 8.2309$ ms	$6T_h \approx 0.1248$ ms
Islam and Basu [27]	$12T_h + 4T_g + 2T_{sm} + 2T_{pm} + 2T_{pa} + 2T_{cha} \approx 5.4381$ ms	$6T_h \approx 0.1248$ ms
Dabra et al. [25]	$5T_h + 7T_g + 2T_{sm} + 4T_{pm} + 5T_{pa} + T_{cha} \approx 7.9714$ ms	$5T_h + 5T_g + 2T_{sm} + 5T_{pm} + 5T_{pa} + T_{cha} \approx 1.0013$ ms
Feng et al. [22]	$5T_h + 2T_g + T_{sm} + 3T_{pm} + T_{pa} + T_{cha} \approx 6.0074$ ms	$5T_h + 2T_g + T_{sm} + 3T_{pm} + T_{pa} + T_{cha} \approx 0.6381$ ms
Ever [24]	$9T_h + 2T_{bp} + 2T_{mtp} + 3T_{ecm} \approx 109.4970$ ms	$6T_h + 3T_{bp} + 2T_{mtp} + 3T_{ecm} \approx 27.7686$ ms
Zhang et al. [28]	$12T_h + 3T_{ecm} + T_{senc} + T_{sdec} \approx 9.7403$ ms	$7T_h + T_{ecm} + T_{senc} + T_{sdec} \approx 0.6707$ ms
Chang et al. [30]	$31T_h + 3T_{ecm} \approx 12.8946$ ms	–
Chaudhary et al. [38]	$12T_h + 4T_g + 2T_{sm} + 4T_{pm} + 2T_{pa} + 4T_{cha} \approx 8.9301$ ms	$10T_h + T_g + 2T_{pm} \approx 0.2204$ ms
Safkhani et al. [37]	$8T_h + 7T_{ecm} + T_{sdec} + T_{senc} \approx 19.0088$ ms	–
Chaudhary et al. [39]	$9T_h + 4T_g + 2T_{sm} + 4T_{pm} + 2T_{pa} + 2T_{cha} + T_{senc} \approx 8.4895$ ms	$8T_h + 2T_{pm} + T_{sdec} \approx 0.4931$ ms
Irshad et al. [32]	$20T_h + 9T_{ecm} + 3T_{eca} \approx 26.9725$ ms	$8T_h + 3T_{ecm} + 2T_{eca} + 2T_{senc}/T_{sdec} \approx 1.8617$ ms
Proposed (QRAC-UAV)	$17T_h + 7T_g + 2T_{sm} + 4T_{pm} + 5T_{pa} + T_{cha} \approx 9.8942$ ms	–

TABLE V
COMPARATIVE ANALYSIS ON AUTHENTICATION TIME AND STORAGE COST

Schemes	Authentication Time (in ms)		Storage Costs (in bits)
	Smart Device	Server	Smart Device
Mishra et al.	2.3824	0.2014	1344
Rewal et al.	5.6109	0.0832	1856
Islam and Basu	3.7478	0.1248	5088
Dabra et al.	7.9714	0.9805	416
Feng et al.	6.0074	0.6173	512
Zhang et al.	6.7239	0.5803	1536
Chang et al.	8.3498	–	1152
Irshad et al.	3.3659	1.7297	2240
Proposed scheme	2.5749	–	1248

C. Computation Efficiency Analysis

In this section, we examine the computational efficiency in terms of user/device authentication costs, similar to Cheng et al. [61], and it is calculated based on our experimental results described in Section VII-A. In addition, we also added storage costs for performing the execution of the protocol for computational efficiency calculation. The average authentication cost is calculated in milliseconds (ms), and it is measured relying on the time required for successful authentication of a device/user to the server. Table V displays the authentication costs and storage costs of the proposed scheme along with existing schemes.

TABLE VI
COMPARATIVE ANALYSIS ON ENERGY CONSUMPTION COST (IN MJ)

Primitives	Energy consumption cost (in mJ)	
	Smart device	Server
Mishra et al.	6973.7046	93.6170
Rewal et al.	13732.4473	11.3670
Islam and Basu	8017.0993	164.4486
Dabra et al.	3719.0665	95.5862
Feng et al.	3563.9971	89.0973
Zhang et al.	3850.1401	102.7965
Chang et al.	3018.4759	–
Irshad et al.	2582.255	60.6551
Proposed scheme	7856.6577	–

It is worth noticing that the proposed scheme requires an authentication cost for smart devices of 2.5749ms, which is smaller than all other schemes except Mishra et al. [33], and it proves the superiority of the proposed scheme in being lightweight in nature and more scalable. In addition, the proposed scheme requires less storage space, as 1248 bits for smart devices compared to other schemes, such as Mishra et al. Rewal et al. Islam and Basu, and others. The storage costs in bits are measured based on the bits needed to store the registration credentials during the registration phase by the respective server. Therefore, it is demonstrated that the proposed scheme is more efficient, scalable, and robust in terms of authentication and storage compared to existing schemes.

D. Energy Consumption Costs Analysis

The energy consumption cost is calculated based on the required energy cost (in mJ) for successful authentication, that is, the energy required to execute cryptographic primitives for successful authentication. Based on our testbed experiment described in Section VII-A, we compute the energy costs of the proposed scheme and other schemes as well. We use the similar approach to calculate it as described by Bera et al. [62], and Table VI shows the results. It is worth noticing that the proposed scheme requires 7856.6577 mJ for successful mutual authentication. It is calculated as $16T_h + 7T_g + 2T_{sm} + 4T_{pm} + 5T_{pa} + T_{cha} + T_m \times E \approx 16 \times 3.1219 + 7 \times 0.3748 + 2 \times 0.3353 + 4 \times 28.0459 + 5 \times 1.2035 + 5.2113 + 10240 \times 0.7500 \approx 7856.6577$ mJ. Similarly, we calculate the energy consumption for other schemes and it can be found in Table VI. Here, $E = 0.7500$ mJ is an energy consumption of a smart device to transmit a single bit with a transmission rate of 1Mbps operating at 5.1V and 3.5A and T_m is the total message transferred by the smart device.

E. Functionality and Security (FS) Attributes

Table VII demonstrated that the proposed QRAC-UAV scheme successfully fulfill all the essential security and functionality features and provided a strong security in access control for drone applications. In contrast, other existing solutions in the same domain fall short of achieving the desired level of security.

TABLE VII
COMPARATIVE ASSESSMENT ON VARIOUS FS ATTRIBUTES

Attribute	[33]	[23]	[27]	[25]	[22]	[24]	[28]	[30]	[32]	QRAC-UAV
FS_1	✓	✓	✓	×	×	✓	×	×	✓	✓
FS_2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
FS_3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
FS_4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
FS_5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
FS_6	✓	✓	✓	✓	✓	×	✓	×	✓	✓
FS_7	×	×	×	✓	✓	×	✓	✓	✓	✓
FS_8	×	×	×	×	✓	×	✓	✓	✓	✓
FS_9	✓	✓	✓	✓	✓	✓	✓	×	✓	✓
FS_{10}	✓	✓	✓	✓	✓	×	✓	×	✓	✓
FS_{11}	×	×	N/A	N/A	N/A	×	✓	×	×	✓
FS_{12}	×	×	×	×	×	×	×	×	✓	✓
FS_{13}	✓	✓	✓	✓	✓	×	×	×	×	✓

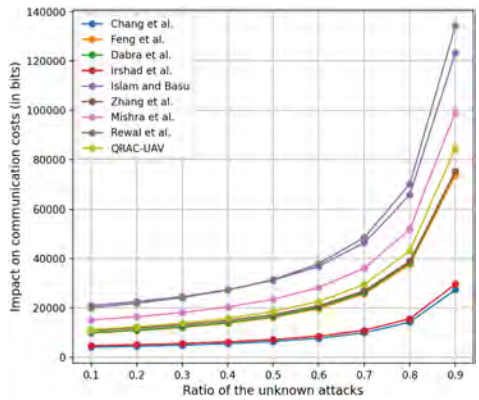

Fig. 9. Performance on communication costs under the unknown attacks.

F. Performance Analysis Under Unknown Attacks

Although we have discussed how the proposed scheme resists well-known active and passive attacks under both classical and quantum threats in Section V, there are some unidentified threats that can affect the performance of this scheme, and these attacks can occur unpredictably. Consequently, we evaluate the performance of the proposed scheme when it faces those unknown attacks, and we particularly focus on the effect on communication and computation overhead under unknown attacks. The effect can be calculated by the following equations:

$$Cost_{avg} = \frac{Cost_{fail} \times p_{fail} + Cost_{succ} \times p_{succ}}{p_{succ}}, \quad (7)$$

$$Cost_{fail} = \sum_{i=1}^{N} \frac{Cost_i}{N}. \quad (8)$$

In (7), $Cost_{avg}$ signifies the average communication/computation costs under unknown attacks, $Cost_{fail}$ signifies the communication/computation costs for an unsuccessful authentication under unknown attack and it can be derived from (8), and $Cost_{succ}$ signifies the communication/computation costs for successful authentication. p_{fail} represents the failure probability of an unknown attack in the protocol execution and p_{succ} is success probability, where $p_{succ} = 1 - p_{fail}$. N denotes the total number of messages in the authentication process and the probability of an unknown attack at Step i is $\frac{1}{N}$. $Cost_i$ signifies the cumulative communication/computation cost before an unknown attack occurs at Step i.

The performance results presented in Figs. 9 and 10 signify that the proposed protocol well perform compared to schemes

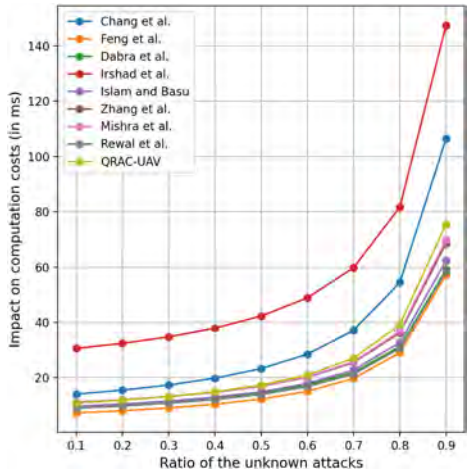

Fig. 10. Performance on computation costs under the unknown attacks.

of Mishra et al. [33], Rewal et al. [23], and Islam and Basu [27] under an unknown attack. This superiority stems from the fact that the proposed protocol incurs lower communication costs. However, the proposed protocol under-perform compared to Dabra et al. [25], Feng et al. [22], Zhang et al. [28], Chang et al. [30], and Irshad et al. [32], due to their lower communication costs requirement. Although these scheme does not fulfill the all security requirement as mentioned above. It is also noticing that, the proposed scheme exhibits superior performance compared to the schemes [30], [32], [33] under unknown attacks.

IX. Conclusion

In conclusion, we have proposed a quantum-secure access control framework for UAV-based IoD applications, where our primary goal was to maintain anonymous communication and safeguard a high-performance data-sharing platform. The proposed scheme offered a lightweight model for resource-constrained IoD devices and resisted various potential active and passive attacks in both classical and quantum scenarios. The security verification using state-of-the-art tools, like Scyther and Tamarin verified the proposed scheme's security, correctness, and robustness. A real-time testbed experiments on Raspberry Pi 4 devices highlighted the novelty of the proposed scheme, and the comprehensive performance analysis under unknown attacks, computational overhead, authentication time, and energy consumption confirmed its practicability, scalability, and efficiency for real-world applications.

Acknowledgment

The authors would like to thank the anonymous reviewers and associate editor for their valuable feedback on the paper.

References

[1] H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li, and J. Wei, "Survey on unmanned aerial vehicle networks: A cyber physical system perspective," *IEEE Commun. Surv. Tuts.*, vol. 22, no. 2, pp. 1027–1070, Second Quarter 2020.

[2] B. Bothwell, "Science & tech spotlight: Counter-drone technologies," 2022. Accessed: Sep. 2023. [Online]. Available: https://www.gao.gov/products/gao-22-105705

[3] M. Zolanvari, R. Jain, and T. Salman, "Potential data link candidates for civilian unmanned aircraft systems: A survey," *IEEE Commun. Surv. Tuts.*, vol. 22, no. 1, pp. 292–319, First Quarter 2020.

[4] V. U. Ihekoronye, S. O. Ajakwe, D. Kim, and J. M. Lee, "Hierarchical intrusion detection system for secured military drone network: A perspicacious approach," in *Proc. Mil. Commun. Conf.*, Rockville, MD, USA, 2022, pp. 336–341.

[5] A. D. Kaasen, G. Grov, F. Mancini, and M. Baksaas, "Towards data-driven autonomous cyber defence for military unmanned vehicles - threats & attacks," in *Proc. Mil. Commun. Conf.*, Rockville, MD, USA, 2022, pp. 861–866, doi: 10.1109/MILCOM55135.2022.10017692.

[6] M. Golam, R. Akter, R. Naufal, V.-S. Doan, J.-M. Lee, and D.-S. Kim, "Blockchain inspired intruder UAV localization using lightweight CNN for Internet of Battlefield Things," in *Proc. Mil. Commun. Conf.*, Rockville, MD, USA, 2022, pp. 342–349, doi: 10.1109/MILCOM55135.2022.10017795.

[7] R. H. Jacobsen and A. Marandi, "Security threats analysis of the unmanned aerial vehicle system," in *Proc. Mil. Commun. Conf.*, San Diego, CA, USA, 2021, pp. 316–322, doi: 10.1109/MILCOM52596.2021.9652900.

[8] S. Safavat and D. B. Rawat, "Securing unmanned aerial vehicular networks using modified elliptic curve cryptography," in *Proc. Mil. Commun. Conf.*, San Diego, CA, USA, 2021, pp. 999–1004, doi: 10.1109/MILCOM52596.2021.9652982.

[9] S. Inshi, R. Chowdhury, H. Ould-Slimane, and C. Talhi, "Dynamic context-aware security in a tactical network using attribute-based encryption," in *Proc. Mil. Commun. Conf.*, Rockville, MD, USA, 2022, pp. 49–54, doi: 10.1109/MILCOM55135.2022.10017647.

[10] J. W. Stokes, P. England, and K. Kane, "Preventing machine learning poisoning attacks using authentication and provenance," in *Proc. Mil. Commun. Conf.*, San Diego, CA, USA, 2021, pp. 181–188, doi: 10.1109/MILCOM52596.2021.9653139.

[11] W. Li, X. Li, J. Gao, and H. Wang, "Design of secure authenticated key management protocol for cloud computing environments," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 3, pp. 1276–1290, May/Jun. 2021.

[12] C. Lin, D. He, X. Huang, N. Kumar, and K.-K. R. Choo, "BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 12, pp. 7408–7420, Dec. 2021.

[13] M. A. Khan et al., "An efficient and secure certificate-based access control and key agreement scheme for flying ad-hoc networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4839–4851, May 2021.

[14] J. Zhang, J. Cui, H. Zhong, I. Bolodurina, and L. Liu, "Intelligent drone-assisted anonymous authentication and key agreement for 5G/B5G vehicular ad-hoc networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 4, pp. 2982–2994, Fourth Quarter 2021.

[15] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, 1999.

[16] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Santa Fe, NM, USA, 1994, pp. 124–134.

[17] P. R. Babu, S. A. Kumar, A. G. Reddy, and A. K. Das, "Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges," *Comput. Sci. Rev.*, vol. 54, 2024, Art. no. 100676.

[18] C. Xu, F. Erata, and J. Szefer, "Exploration of quantum computer power side-channels," 2023. Accessed: Oct. 2023, doi: 10.48550/arXiv.2304.03315.

[19] J. Bos et al., "Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Vienna, Austria, 2016, pp. 1006–1018.

[20] P. Kirchner and P.-A. Fouque, "An improved BKW algorithm for LWE with applications to cryptography and lattices," in *Proc. Annu. Cryptol. Conf.*, Santa Barbara, CA, USA, 2015, pp. 43–62.

[21] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, Amsterdam, The Netherlands, 2002, pp. 337–351.

[22] Q. Feng, D. He, S. Zeadally, N. Kumar, and K. Liang, "Ideal lattice-based anonymous authentication protocol for mobile devices," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2775–2785, Sep. 2019.

[23] P. Rewal, M. Singh, D. Mishra, K. Pursharthi, and A. Mishra, "Quantum-safe three-party lattice based authenticated key agreement protocol for mobile devices," *J. Inf. Secur. Appl.*, vol. 75, 2023, Art. no. 103505.

[24] Y. K. Ever, "A secure authentication scheme framework for mobile-sinks used in the Internet of Drones applications," *Comput. Commun.*, vol. 155, pp. 143–149, 2020.

[25] V. Dabra, A. Bala, and S. Kumari, "LBA-PAKE: Lattice-based anonymous password authenticated key exchange for mobile devices," *IEEE Syst. J.*, vol. 15, no. 4, pp. 5067–5077, Dec. 2021.

[26] R. Ding, C. Cheng, and Y. Qin, "Further analysis and improvements of a lattice-based anonymous PAKE scheme," *IEEE Syst. J.*, vol. 16, no. 3, pp. 5035–5043, Sep. 2022.

[27] S. H. Islam and S. Basu, "PB-3PAKA: Password-based three-party authenticated key agreement protocol for mobile devices in post-quantum environments," *J. Inf. Secur. Appl.*, vol. 63, 2021, Art. no. 103026.

[28] N. Zhang, Q. Jiang, L. Li, X. Ma, and J. Ma, "An efficient three-factor remote user authentication protocol based on BPV-FourQ for Internet of Drones," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 3319–3332, 2021.

[29] Y. Park, D. Ryu, D. Kwon, and Y. Park, "Provably secure mutual authentication and key agreement scheme using PUF in Internet of Drones deployments," *Sensors*, vol. 23, no. 4, pp. 1–25, 2023.

[30] Y.-F. Chang, W.-L. Tai, P.-L. Hou, and K.-Y. Lai, "A secure three-factor anonymous user authentication scheme for Internet of Things environments," *Symmetry*, vol. 13, no. 7, pp. 1–17, 2021.

[31] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K.-K. R. Choo, "Blockchain-based cross-domain authentication for intelligent 5G-Enabled Internet of Drones," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6224–6238, Apr. 2022.

[32] A. Irshad, G. A. Mallah, M. Bilal, S. A. Chaudhry, M. Shafiq, and H. Song, "SUSIC: A secure user access control mechanism for SDN-enabled IIoT and cyber physical systems," *IEEE Internet Things J.*, vol. 10, no. 18, pp. 16504–16515, Sep. 2023, doi: 10.1109/JIOT.2023.3268474.

[33] D. Mishra et al., "Quantum-safe secure and authorized communication protocol for Internet of Drones," *IEEE Trans. Veh. Technol.*, vol. 72, no. 12, pp. 16499–16507, Dec. 2023, doi: 10.1109/TVT.2023.3292169.

[34] M. F. Ayub, X. Li, K. Mahmood, S. Shamshad, M. A. Saleem, and M. Omar, "Secure consumer-centric demand response management in resilient smart grid as industry 5.0 application with blockchain-based authentication," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 1370–1379, Feb. 2024, doi: 10.1109/TCE.2023.3320974.

[35] S. Hu et al., "Provably secure ECC-Based authentication and key agreement scheme for advanced metering infrastructure in the smart grid," *IEEE Trans. Ind. Informat.*, vol. 19, no. 4, pp. 5985–5994, Apr. 2023.

[36] H. Ma, C. Wang, G. Xu, Q. Cao, G. Xu, and L. Duan, "Anonymous authentication protocol based on physical unclonable function and elliptic curve cryptography for smart grid," *IEEE Syst. J.*, vol. 17, no. 4, pp. 6425–6436, Dec. 2023.

[37] M. Safkhani, S. Kumari, M. Shojafar, and S. Kumar, "An authentication and key agreement scheme for smart grid," *Peer-to-Peer Netw. Appl.*, vol. 15, no. 3, pp. 1595–1616, 2022.

[38] D. Chaudhary, U. Kumar, and K. Saleem, "A construction of three party post quantum secure authenticated key exchange using ring learning with errors and ECC cryptography," *IEEE Access*, vol. 11, pp. 136947–136957, 2023.

[39] D. Chaudhary, P. Ku mar Dadsena, A. Padmavathi, M. Mehedi Hassan, B. Fahad Alkhamees, and U. Kumar, "Anonymous quantum safe construction of three party authentication and key agreement protocol for mobile devices," *IEEE Access*, vol. 12, pp. 74572–74585, 2024.

[40] A. Ahmad and S. Jagatheswari, "Lattice-based three party authenticated key agreement scheme in medical IoT for post-quantum environment," *IEEE Access*, vol. 12, pp. 157247–157259, 2024.

[41] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," *SIAM J. Comput.*, vol. 37, no. 1, pp. 267–302, 2007.

[42] J. Zhang, Z. Zhang, J. Ding, M. Snook, and Ö. Dagdelen, "Authenticated key exchange from ideal lattices," in *Proc. 34th Annu. Int. Conf. Theory Appl. Cryptographic Techn.*, Sofia, Bulgaria, 2015, pp. 719–751.

[43] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn.*, French Riviera, 2010, pp. 1–23.

[44] J. Ding, S. Alsayigh, J. Lancrenon, S. Rv, and M. Snook, "Provably secure password authenticated key exchange based on RLWE for the post-quantum world," in *Proc. Cryptographers' Track RSA Conf.*, San Francisco, CA, USA, 2017, pp. 183–204.

[45] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn.*, Interlaken, Switzerland:Springer, 2004, pp. 523–540.

[46] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 9, pp. 1953–1966, Sep. 2015.

[47] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[48] R. M. Daniel, A. Thomas, E. B. Rajsingh, and S. Silas, "A strengthened eCK secure identity based authenticated key agreement protocol based on the standard CDH assumption," *Inf. Comput.*, vol. 294, 2023, Art. no. 105067.

[49] C. C. Zheng Wei, C. Chai Wen, and J. Alawatugoda, "Review on leakage resilient key exchange security models," *Int. J. Commun. Netw. Inf. Secur.*, vol. 11, no. 1, pp. 119–127, 2022.

[50] A. N. Khan, "How to disable a drone on your property," 2023. Accessed: Oct. 2023. [Online]. Available: https://flythatdrone.com/blog/how-to-disable-drone-on-your-property/

[51] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.

[52] S. Bhattacharya, Ó. García-Morchón, R. Rietman, and L. Tolhuizen, "spKEX: An optimized lattice-based key exchange," *IACR Cryptol. ePrint Arch.*, vol. 2017, pp. 1–25, 2017.

[53] Quantum safe cryptography and security, 2015. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

[54] J. Ding, P. Branco, and K. Schmitt, "Key exchange and authenticated key exchange with reusable keys based on RLWE assumption," *Cryptol. ePrint Arch.*, Paper 2019/665, 2019. Accessed: May 2025. [Online]. Available: https://eprint.iacr.org/2019/665

[55] M. Abdalla, P. A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. 8th Int. Workshop Theory Pract. Public Key Cryptography*, Les Diablerets, Switzerland, 2005, pp. 65–84.

[56] C. C. Chang and H. D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 357–366, Jan. 2016.

[57] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 11, pp. 2776–2791, Nov. 2017.

[58] C. Cremers, "The scyther tool," 2006. Accessed: Jun. 2023. [Online]. Available: https://people.cispa.io/cas.cremers/scyther/

[59] C. J. F. Cremers, "The Scyther tool: Verification, falsification, and analysis of security protocols," in *Proc. Int. Conf. Comput. Aided Verification*, Princeton, NJ, USA: Springer, 2008, pp. 414–418.

[60] J. Cao, M. Ma, Y. Fu, H. Li, and Y. Zhang, "CPPHA: Capability-based privacy-protection handover authentication mechanism for SDN-Based 5G HetNets," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 3, pp. 1182–1195, May/Jun. 2021.

[61] C. Cheng, Y. Qin, R. Lu, T. Jiang, and T. Takagi, "Batten down the hatches: Securing neighborhood area networks of smart grid in the quantum era," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6386–6395, Nov. 2019.

[62] B. Bera, R. P. Parameswarath, and B. Sikdar, "Fortifying the security of smart grid networks with post-quantum communication," *IEEE Trans. Smart Grid*, vol. 16, no. 6, pp. 5430–5445, Nov. 2025, doi: 10.1109/TSG.2025.3592991.