AI-Enabled Adversarial Attacks Resistant Post-Quantum Secure Authentication Protocol for Consumer Applications

Prithwi Bagchi, Basudeb Bera, Sayan Rakshit, Ashok Kumar Das, *Senior Member, IEEE*, Sujit Biswas, *Senior Member, IEEE*, Mohammad Kamrul Hasan, *Senior Member, IEEE*, Biplab Sikdar, *Fellow, IEEE*

***Abstract*—The rapid adoption of Artificial Intelligence (AI) in consumer applications has significantly improved automation and user experiences. However, it has introduced emerging security challenges, particularly AI-driven adversarial attacks. Conventional cryptographic mechanisms are increasingly susceptible to these attacks and to the growing risks associated with quantum computing. To mitigate these challenges, this paper presents an AI-enabled, adversarial attack-resistant, post-quantum secure authentication protocol designed for consumer applications. The proposed protocol combines post-quantum lattice-based cryptographic techniques to provide strong and adaptive user authentication against evolving threats. Comprehensive formal security analysis and experimental evaluations confirm that the protocol effectively mitigates quantum and adversarial attacks, including classical attacks, while maintaining comparable computational and communication overhead with the existing competing authentication schemes. As a result, the proposed scheme becomes ideal for resource-constrained consumer environments, such as smart devices, Internet of Things (IoT) systems, and mobile platforms. Finally, an experimental investigation on radio frequency fingerprinting for consumer devices is conducted using an AI-driven model called TinyMLP, and our model achieves $\approx 97\%$ authentication accuracy by resisting adversarial attacks.**

***Index Terms*—Consumer applications, adversarial machine learning attacks, post-quantum authentication, key agreement, security.**

(Corresponding authors: Mohammad Kamrul Hasan, Sujit Biswas; and Ashok Kumar Das).

This work has been supported by the Universiti Kebangsaan Malaysia, Under Research Grant Scheme No. DIP 2024-033.

Prithwi Bagchi is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India (e-mail: prithwi.bagchi@research.iiit.ac.in).

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).

Sayan Rakshit is with the Centre of Studies in Resources Engineering, Indian Institute of Technology Bombay, Mumbai 400076, India (e-mail: sayan1by2@gmail.com)

Ashok Kumar Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India, and also with the Department of Computer Science and Engineering, College of Informatics, Korea University, 145 Anam-ro, Seongbuk-gu, Seoul 02841, South Korea (e-mail: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in).

Sujit Biswas is with the Department of Computer Science, City St. George's, University of London, London EC1V 0HB, United Kingdom. (e-mail: sujit.biswas@citystgeorges.ac.uk).

Mohammad Kamrul Hasan is with the Centre for Cyber Security, University Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia. (e-mail: mkhasan@ukm.edu.my).

I. Introduction

In the field of AI-based cryptosystems, Adversarial Machine Learning (AML) has become a significant and expanding threat. Developers and cybersecurity specialists are becoming increasingly concerned about AML-based attacks as AI and Machine Learning (ML) models are incorporated into a wider range of sectors. ML-driven systems are necessary for critical industries, such as consumer device-based smart home systems. Any vulnerability in these systems could have catastrophic repercussions and pose serious safety risks.

Recent advancements in NLP and CV [1], [2] have positioned trained classifiers as essential components in many critical security applications. As a result, ensuring the security of the ML models has become more crucial. Specifically, improving resilience to maliciously constructed inputs has emerged as a primary design objective for contemporary ML systems. Even though trained models are generally good at identifying valid inputs, existing studies [3] have shown that an adversary can subtly alter inputs to make the model provide inaccurate or deceptive results. Therefore, it is important, from a security perspective, to create an efficient mechanism against AML attacks and to assist businesses in using ML models securely. As of right now, there doesn't seem to be comprehensive research in the literature that provides a thorough examination of AML attacks, their various forms, their outcomes, security testing tools, and mitigation techniques. It is still quite difficult to comprehend assaults on the automatically generated data produced by ML models due to their intricate architectures.

Attempts to coerce an AI system into carrying out unexpected tasks, such as generating inaccurate or deceptive outputs, are known as adversarial attacks. Malicious actors carry out AML attacks with the intention of making an ML model fail. All phases of the model lifecycle are susceptible to these attacks, including before training, during testing, and even after the model has been put into use in a real-world setting. Adversaries typically create adversarial sample inputs that are purposefully altered to result in misclassification in order to execute an AML attack. These attacks can be either targeted or untargeted. They can take many different forms, such as evasion, poisoning, and privacy attacks. An adversary may generate an input in a targeted attack with the express purpose of forcing the AI system to carry out a certain action,

such as installing malware or crashing the system. On the other hand, an untargeted attack seeks to cause widespread interference, including making the system incorrectly identify noises, images, or other inputs.

To mitigate AI-enabled adversarial attacks, we aim to design a post-quantum secure authentication protocol that is targeted for consumer applications. The proposed scheme not only resists classical attacks, including replay, impersonation, man-in-the-middle, ephemeral secret leakage (ESL), privileged-insider, and physical consumer devices capture attacks, but it also resists lattice reduction attacks, along with quantum attacks. The performance analysis shows that the proposed scheme is reasonable in terms of communication and computational overheads as compared with other competing authentication schemes in the literature.

II. Related Work

Authors in [4] suggested a cost-effective IoT architecture that utilizes Wi-Fi-enabled control boards constructed with Espressif microcontrollers, which interface seamlessly with smart devices and standard home automation servers. A Raspberry Pi serves as the automation server in their configuration, and ESP-based modules control IoT functionalities. On the other hand, for improved processing and analysis, the Jetson Nano developer kit makes it possible to incorporate deep learning methods, such as long short-term memory (LSTM) models and convolutional neural networks (CNN), into this mechanism [4].

Qiuyun *et al.* [5] developed a framework for smart homes that makes use of Internet-based services. In their method, users may safely and remotely connect with their home systems, which use an IFTTT-enabled home gateway that serves as a command controller and security manager. Additionally, the model ensures that user registration only takes place within the authorized person's visible range. A PUF-based authentication technique that guarantees user anonymity and resilience to various security threats was introduced by CHO *et al.* [6]. The Burrows-Abadi-Needham logic (also known as the BAN logic) was used to confirm the scheme's accuracy in mutual authentication and key agreement, and AVISPA simulations were used to assess the security resilience of this proposed mechanism [6].

Nimmy *et al.* [7] presented a simple, privacy-preserving remote authentication mechanism for smart home settings using Photo Response Non-Uniformity (PRNU) to protect against smart home attacks, such as smartphone capture and phishing attacks. This mechanism [7] is optimized for IoT devices with limited resources and uses geometric secret sharing for mutual authentication. A Raspberry Pi prototype was used to evaluate energy efficiency, and the 'Automated Validation of Internet Security Protocols and Applications (AVISPA)' tool was used to verify the security of the proposed scheme [7]. PRNU's ability to uniquely identify user devices was validated by experiments using 100 facial photos from 10 smartphones. For smart home networks, Wazid *et al.* designed a three-party remote user authentication protocol that uses AES$-$128 in CBC mode to ensure secure communication. The widely-known AVISPA tool was used to formally verify the security of their proposed mechanism [8]. The widely used NS-2 simulation provides a practical illustration of this suggested scheme. By lowering expenses, increasing comfort, and guaranteeing security for mobile users, smart homes seek to enhance automation. However, they are susceptible to assaults such as message interception, alteration, or deletion due to insecure communication pathways. Therefore, for dependable smart home services, secure and lightweight authentication procedures are essential. ALAM, a lightweight, anonymous authentication system for SDN-enabled smart homes, was proposed by Iqbal *et al.* [9]. However, Yu *et al.* [10] showed that the scheme proposed by Iqbal *et al.* [9] does not guarantee user anonymity and mutual authentication and is susceptible to impersonation, MITM, and session key leak attacks. An attacker can calculate session keys by using credentials that have been taken from a mobile device.

Yu *et al.* [10] later suggested fixes to address these security flaws. The time efficiency, processing delay, cost, complexity, and security needs of users are not met by the current SHA technique. This proposed STeSh framework [11] uses dataset features for user face recognition in order to overcome the above issues. A dual-level authentication procedure that combines speech verification and face recognition ensures the resilience of this scheme [11]. This system [11] also uses MAC address verification to reduce time delays caused by unnecessary load activations. A secure, privacy-preserving, and energy-efficient communication protocol was presented by Song *et al.* [12] for smart home systems (SHSs), which include sensors, home appliances, RFID tags, a central controller, and user interfaces. Their proposed scheme [12] uses symmetric encryption with secret keys produced by chaotic systems to ensure the security of data transfer.

TABLE I: Comparison of State-of-the-Art Authentication Schemes

Scheme	Resource Efficient	Security Assumptions	Quantum-Safe	Consumer Application	AI-Enabled Adversarial Attacks
[13]	✓	Ring-LWE	✓	✓	✗
[14]	✓	TLS 1.3	✓	✓	✗
[15]	✗	QKD	✓	✓	✗
[7]	✓	ECC	✗	✓	✗
[8]	✗	AES-CBC (128 bits)	✗	✓	✗
[9]	✗	Symmetric Key & Hash function-based	✗	✓	✗
[11]	✓	Symmetric Key & Hash function-based	✗	✓	✗
[12]	✓	Hash function-based	✗	✓	✗
Proposed	✓	Ring-LWE	✓	✓	✓

Existing authentication schemes for IoT and consumer applications predominantly rely on classical or post-quantum cryptographic techniques (PQC), primarily optimizing efficiency and lightweight performance. For instance, PQCAIE [13] integrates PQC with TLS 1.3 for secure healthcare systems but remains confined to classical communication models and fails to address adversarial threats. Similarly, lattice-based lightweight authentication and hybrid encryption schemes [14] enhance quantum resistance and computational efficiency; however, they do not consider AI-driven adversarial attacks or adaptive security mechanisms. More recently, QKD-based frameworks for decentralized biometric authentication provide quantum-secure key exchange, yet they largely overlook ad-

versarial robustness and practical deployment constraints [15]. Table I presents a comparative analysis of existing schemes, highlighting these limitations. To the best of our knowledge, no existing work simultaneously addresses post-quantum security, adversarial resilience, and lightweight deployment. In contrast, our proposed scheme uniquely integrates these dimensions into a unified authentication framework for next-generation consumer environments.

III. System Model

A. Network Model

A Key Generation Center (KGC), serving as the trusted authority, several gateway nodes (GWNs), a collection of cloud servers $\{CS_i; i \in [l]\}$, numerous smart home applications, and a large number of consumer devices (DVs) dispersed throughout these applications, make up the network architecture in the suggested framework, which is illustrated in Fig. 1. The TA oversees the registration procedure for each CSs, every consumer device across the various smart home applications, and each gateway node. The entire procedure of registration is conducted offline. All CSs, GWNs, and DVs can be deployed to their assigned operational regions after the registration procedure is completed. In a specific smart home application, particularly the j^{th} smart home application, the i^{th} consumer device, $DV_{i,j}$, and its corresponding registered gateway node, GWN_j, undergo a mutual authentication process. To enable private communication, $DV_{i,j}$ and GWN_j both generate a quantum-secure session key. Subsequently, GWN_j communicates with the k^{th} cloud server, CS_k, using the known quantum-safe secret session key that connects them. After collecting data from their respective zones, $DV_{i,j}$ encrypts it with the lattice-based authentication key and sends it to the GWN_j. The GWN_j receives the encrypted data, uses the timestamp mechanism to confirm that it is current, decrypts it, selects a fresh timestamp, re-encrypts it using the fresh timestamp and the authenticated session key generated between GWN_j and CS_k, and then sends it to the CS_k. The data is processed as test data for ML-based prediction after the cloud server CS_k verifies its integrity. Adversarial attack scenarios are also included in the model, in which a malicious party tries to alter the lattice-encrypted data by adding noise or perturbations.

B. Threat Model

According to the suggested framework, the smart devices (DVs) use a communication channel to transmit real-time sensor data to their associated gateway nodes (GWNs). This data transmission occurs across a public channel that is either wired or wireless. Due to the inherent insecurity of public channels, each consumer device (DV) uses a pre-established secret key, known as the session key, to share smart home information with its corresponding GWN. Using the session key for a secure connection once more, the GWNs then send the private smart home data to their related cloud servers (CSs) via the same kind of public channel. Subsequently, this sensitive data might be compromised and exploited by an

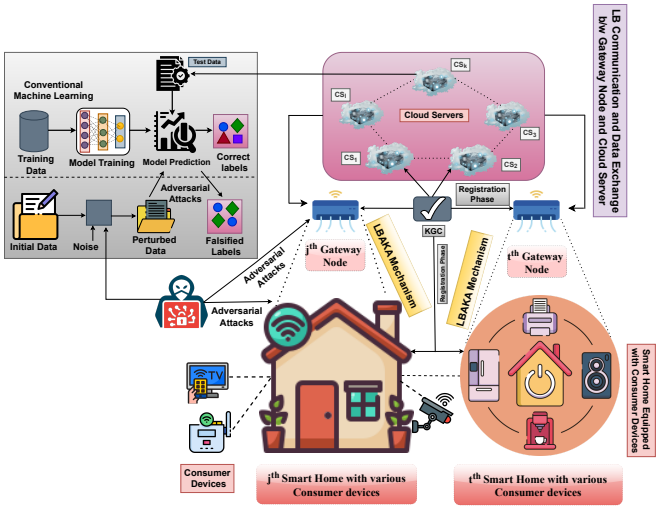

Fig. 1: Network model incorporating adversarial attacks (Adapted from [16]).

adversary $\mathcal{A}$ if these session keys are not immune to quantum computing attacks.

In this work, we develop and examine the process of building a session key across an unsecured communication channel by utilizing several existing security models. These models include the Dolev-Yao (DY) model [17], the Canetti-Krawczyk (CK) model [18], and the extended Canetti-Krawczyk (eCK) model [19], [20]. A different viewpoint on how an attacker can try to undermine secure communication is offered by each of these frameworks. The DY-threat model [17] allows an adversary, say $\mathcal{A}$, to possess total control over the communication channel, allowing the adversary to intercept, change, replay, insert, or obstruct any communicated message. In contrast to the DY model, the CK threat model [18] accounts for enhanced adversarial knowledge, including session-state revelation, session-key disclosure, and the capacity to engage with numerous protocol instances. The eCK-adversarial model [19], [20] allows the attacker $\mathcal{A}$ to acquire particular combinations of long-term private keys and temporary session secrets while maintaining the security of the generated session key during concealed sessions.

The CK-adversary model offers several important advantages over the DY model for analyzing the authenticated key exchange (AKE) protocols. The CK-adversary model allows session-state reveal, session-key leakage, as well as corruption queries. It then defines session freshness and indistinguishability of session keys. Additionally, it typically ensures stronger security, like "resistance to key compromise impersonation (KCI)" attack, "forward secrecy" and "session key indistinguishability", as compared to the DY-model. On the other side, the eCK-adversary model allows an adversary to reveal ephemeral (session-specific) secret keys in addition to long-term private keys. Moreover, the eCK-model provides stronger resilience against KCI attacks. Consequently, integrating the DY, CK, and eCK threat models facilitates a thorough security assessment of the proposed authentication scheme.

We also take into account the possibility of quantum-based

attacks by the adversary $\mathcal{A}$ during data exchanges between various entities. In addition to the risks of remote communication, we consider the potential for $\mathcal{A}$ to physically compromise a device, which would allow for quantum-powered side-channel attacks, such as power analysis attacks [21], [22], to retrieve the secret credentials from the device's memory. Furthermore, it is presumed that $\mathcal{A}$ can execute a quantum lattice reduction attack to recover the secret session keys [23].

IV. Mathematical Preliminaries

$\mathbb{N}$ signifies the set of positive integers and takes $\alpha \in \mathbb{N}$ into account. $n = 2^\alpha \in \mathbb{N}$ is defined. For the given positive integer n, we select a sufficiently large prime number q that satisfies the condition $q \equiv 1 \pmod{2n}$. The value of $\mathbb{Z}_q = \{-\frac{q-1}{2}, \cdots, \frac{q-1}{2}\}$ represents the equivalent finite field. Consider the ideal $< x^n + 1 >$ represented by an irreducible polynomial $x^n + 1$. $R = \mathbb{Z}[x]/ < x^n + 1 >$ is an expression for the polynomial ring, where $R = \{M(x) : M(x) = \sum_{u=0}^{n-1} D_u x^u : \forall u \in \{0, 1, \cdots, n-1\}, D_u \in \mathbb{Z}\}$, and the set of all integers is denoted by $\mathbb{Z}$. In the same way, a finite ring is defined as $R_q = \mathbb{Z}_q[x]/ < x^n+1 >= \{K(x) : K(x) = \sum_{u=0}^{n-1} N_u x^u : \forall u \in \{0, 1, \cdots, n-1\}, N_u \in \mathbb{Z}_q\}$.

We take into consideration a positive integer $d \leq (q-1)/2$ with the constraint $0 < d < \sqrt{q}$. Define $R_{q,d}$ as a subset of R_q, where $R_{q,d} = \{K(x) : K(x) = \sum_{u=0}^{n-1} N_u x^u : \forall u \in \{0, 1, \cdots, n-1\}, N_u \in [-d, d]\}$. For $p \geq 1$, $||K(x)||_p = \sqrt[p]{\sum_{u=0}^{n-1} |N_u|^p}$ gives the l_p norm, and $||K(x)||_\infty = \max\{|N_u|; u \in [n-1] \cup \{0\}\}$ gives the sup-norm of a polynomial $K(x) = (N_0, N_1 \cdots, N_{n-1})$. Moreover, considering β to be a fixed positive parameter, let χ_β be a discrete Gaussian distribution over R_q.

Lemma 1. *Let the two polynomials $K_1(x)$ and $K_2(x)$ be members of $\in R_q$. The following disparities are true: $||K_1(x).K_2(x)|| \leq \sqrt{n}.||K_1(x)||.||K_2(x)||$ and $||K_1(x).K_2(x)||_\infty \leq n.||K_1(x)||_\infty.||K_2(x)||_\infty$ [24].*

Lemma 2. *Given $\beta = w(\sqrt{\log n}) \in R^+$, $Pr_{\alpha \leftarrow \chi_\beta}[||\alpha|| > \beta.\sqrt{n}] \leq 2^{-(n-1)}$ holds [25], where $Pr[E]$ stands for the probability of a random event E' in which $0 \leq Pr[E] \leq 1$.*

Characteristic function: A subset $L = \{-\lfloor \frac{q}{4} \rfloor, \cdots, \lfloor \frac{q}{4} \rfloor\}$ of $\mathbb{Z}_q$ is considered, as is the set $\mathbb{Z}_q = \{-\frac{q-1}{2}, \cdots, \frac{q-1}{2}\}$. The definition of Cha, the characteristic function, is as follows [24]: $Cha(x) = \begin{cases} 0 & \text{if } x \in L, \\ 1 & \text{if } x \notin L. \end{cases}$ The auxiliary modular function $Mod_2 : \mathbb{Z}_q \times \{0, 1\} \rightarrow \{0, 1\}$ is also defined as $Mod_2(\zeta, x) = (\zeta + x.\frac{q-1}{2}) \pmod{q} \pmod 2$, where $\zeta \in \mathbb{Z}_q$ and $x = Cha(\zeta)$. The function Mod_2 satisfies Lemma 3.

Lemma 3. *Let q be a large prime integer, and let there be two polynomials $a, e \in R_q$, such that $|e| < \frac{q}{8}$ and $b = a + 2.e$. Then it is true that $Mod_2(b, Cha(a)) = Mod_2(a, Cha(a))$, [24].*

Now, $a \in R_q$ can be represented as $a = (a_0, a_1, \cdots, a_{n-1})$. If $x = (x_0, x_1, \cdots, x_{n-1}) \in \{0, 1\}^n$, $Cha(a) = (Cha(a_0), Cha(a_1), \cdots, Cha(a_{n-1}))$ and $Mod_2(a, x) = (Mod_2(a_0, x_0), Mod_2(a_1, x_1), \cdots, Mod_2(a_{n-1}, x_{n-1}))$ [24].

Ring Learning with Errors (Ring-LWE): Originating from the standard Learning With Errors (LWE) problem [26], Ring-LWE is a fundamental security pillar of lattice-based cryptosystems. The computational difficulty of addressing the Ring-LWE problem is the primary determinant of overall security in contemporary lattice-based cryptographic systems [27]. The following is a definition of the Ring-LWE problem. Choose a polynomial $a \in R_q$ with a maximum degree of $n-1$ and another polynomial $s \in_R R_q$, which is randomly chosen and has a degree of no more than $n-1$. Given an error distribution χ over R, the Ring-LWE distribution $D_{s,\chi}$ produces pairings of the form $(a, a \cdot s + e \bmod (x^n + 1)) \in R_q \times R_q$. The error term e is chosen at random based on χ. Given a collection of samples $a_i \in R_q$ and corresponding error terms e_i, let's assume that each e_i is selected separately from the error distribution χ for all $i \in [m]$ with $m \geq n$. Recovery of the secret $s \in_R R_q$ from the set of m instances $\{(a_i, a_i \cdot s + e_i \bmod (x^n+1)); i \in [m]\}$ is the problem. Here, s is sampled uniformly from R_q. It is computationally difficult to solve this problem because the Ring-LWE assumption reduces to the "Shortest Independent Vectors Problem (SIVP)" over ideal lattices [26], [28].

TABLE II: Used notations and their descriptions

Notation	Description
$DV_{i,j}$, GWN_j, CS_k	i^{th} consumer device in the j^{th} smart home, j^{th} gateway node, and k^{th} cloud server
ID_X	Identity of an entity X
KGC	Key Generation Center (Trusted Authority).
$Cha(\cdot)$, $Mod_2(\cdot)$	Characteristic and modular functions
n, q	A security parameter (power of 2), with $n = 2^\lambda, \lambda > 0$, and an odd large prime such that $q \equiv 1 \pmod{2n}$
$\mathbb{Z}$	Set of all integers
$\mathbb{Z}_q$	A finite field of prime order q, $\mathbb{Z}_q = \{0, 1, 2, \cdots, q-1\}$
$x^n + 1$	An irreducible ($2n$-th cyclotomic) polynomial over $\mathbb{Z}$ of degree n
R, R_q	Polynomial rings: $\frac{\mathbb{Z}[x]}{<x^n+1>}$ and $\frac{\mathbb{Z}_q[x]}{<x^n+1>}$
$R_{q,1}$	A subset of R_q such that each coefficients of every polynomial is in $\{-1, 0, 1\}$
$H_1(.)$	One-way cryptographic hash function from $\{0,1\}^*$ to $R_{q,1}$
$H(.)$	One-way cryptographic hash function from $\{0,1\}^*$ to $\{0,1\}^b$, where b is a fixed length.
msk	Secret key $(sk_1, sk_2) \in_{ur} R_{q,1} \times R_{q,1}$ of KGC
mpk, a	Public key of KGC, A polynomial in R_q
TS_1	Timestamp generated by $DV_{i,j}$
TS_2	Timestamp chosen by GWN_j
ΔT	Maximum message transmission delay
$SK_{X,Y}$	A session key between entities X and Y
$TID_{DV_{i,j}}$	Temporary Identity of $DV_{i,j}$ chosen by KGC
MK_X	Secret positive integer chosen from $\mathbb{Z}$ by KGC for the entity X
$(sk^1_{DV_{i,j}}, sk^2_{DV_{i,j}})$, $pk_{DV_{i,j}}$	Secret keys and public key of $DV_{i,j}$ generated by KGC
PR	Secret positive integer chosen by KGC for GWN_j and CS_k
$(sk_{GWN_j,1}, sk_{GWN_j,2})$	Secret keys of GWN_j produced by KGC
pk_{GWN_j}	Public keys of GWN_j generated by KGC

V. Proposed Scheme

The proposed authentication scheme (2PA-AKA-QS-CD) is based on the computational difficulty of the Ring-LWE problem. The hardness assumption of the Ring-LWE problem is fundamental because it provides the proposed scheme's stronger security against both classical and quantum attacks.

Moreover, it assures that deriving secret keys from the available public parameters remains computationally infeasible with the help of a quantum computing facility. As a result, this assumption provides us with strong resistance to various attacks, like key recovery and impersonation, while also supporting post-quantum security. Thus, it makes the authentication scheme robust for future cryptographic applications as well.

Based on the Ring-LWE framework, we provide 2PA-AKA-QS-CD, an effective two-party authentication method. This protocol is designed for smart home settings where DV, gateway nodes, cloud servers, a big-data analytics center, and a fully trusted authority known as the KGC interact. Table II offers a thorough explanation of the notations used in this scheme. The three main stages of the overall framework are as follows: (A) System Initialization Phase; (B) Registration Phase, which includes enrolling DV in different smart home applications, as well as their corresponding gateway nodes and cloud servers; and (C) Mutual Authentication Phase.

A. System Initialization Phase

The KGC uses the following stages to carry out this algorithm:

- KGC selects a pair of polynomials randomly as the master secret key $msk = (sk_1, sk_2) \in_{ur} R_{q,1} \times R_{q,1}$ and chooses a polynomial $a \in_r R_q$. Then KGC computes the associated master public key as $mpk = a.sk_1 + sk_2 \pmod{x^n + 1}$.
- Then KGC selects a one-way collision resistant cryptographic hash function H, publishes the public parameters as $pp = \{mpk, H, H_1, a\}$, and keeps the msk secret.

B. Registration Phase

All the DV that will be deployed in each smart home, together with their $GWNs$ respective cloud servers connected to the gateway node, must be registered by the KGC. The following steps are used KGC to execute this algorithm:

1) Registration of the i^{th} consumer device $DV_{i,j}$ in the j^{th} smart home: Consider the i^{th} smart DV in the j^{th} smart home that is identified by the symbol $DV_{i,j}$. The following is a description of the registration process for the $DV_{i,j}$:

- KGC selects a unique identity $ID_{DV_{i,j}}$, a temporary identity $TID_{DV_{i,j}}$, a positive integer $MK_{DV_{i,j}} \in \mathbb{Z}$, and then generates the associated secret keys for $DV_{i,j}$.
- KGC computes the secret keys $sk^1_{DV_{i,j}} = H_1(ID_{DV_{i,j}} || sk_1 || MK_{DV_{i,j}} || sk_2 || TID_{DV_{i,j}})$, $sk^2_{DV_{i,j}} = H_1(sk_1 || ID_{DV_{i,j}} || TID_{DV_{i,j}} || sk_2 || MK_{DV_{i,j}})$, and the associated public key $pk_{DV_{i,j}} = a.sk^1_{DV_{i,j}} + 2.sk^2_{DV_{i,j}} \pmod{x^n + 1}$.
- Then, KGC installs the credentials as $\{(sk^1_{DV_{i,j}}, sk^2_{DV_{i,j}}), MK_{DV_{i,j}}, ID_{DV_{i,j}}, pk_{DV_{i,j}}, TID_{DV_{i,j}}\}$ in the memory of $DV_{i,j}$ and publishes $pk_{DV_{i,j}}$.
- For security reasons, TA deletes $\{(sk^1_{DV_{i,j}}, sk^2_{DV_{i,j}}, ID_{DV_{i,j}}, MK_{DV_{i,j}}, pk_{DV_{i,j}}\}$ from its database and keeps $\{TID_{DV_{i,j}}\}$ until the equivalent gateway node GWN_j has finished registering.

2) Registration of the j^{th} Gateway Node GWN_j: Consider the associated gateway node for the j^{th} smart home, denoted by the symbol GWN_j. An explanation of the GWN_j registration procedure is provided below:

- To register the gateway node GWN_j associated with the j^{th} hospital, KGC selects the identity ID_{GWN_j} of GWN_j, along with two positive integers $MK_{GWN_j}, PR \in_r \mathbb{Z}$, and then creates a pair of secret polynomials $(sk_{GWN_j,1}, sk_{GWN_j,2}) = (H_1(ID_{GWN_j} || sk_1 || sk_2 || MK_{GWN_j}), H_1(sk_2 || ID_{GWN_j} || MK_{GWN_j} || sk_1))$. Subsequently, KGC evaluates the corresponding public key $pk_{GWN_j} = a.sk_{GWN_j,1} + 2.sk_{GWN_j,1} \pmod{x^n+1}$ of GWN_j, and the hash value $A_{GWN_j} = H(ID_{GWN_j} || MK_{GWN_j} || sk_{GWN_j,1} || sk_{GWN_j,2})$.
- KGC stored the subsequent entities $\{(sk_{GWN_j,1}, sk_{GWN_j,2}), ID_{GWN_j}, PR, MK_{GWN_j}, pk_{GWN_j}, A_{GWN_j}, \{TID_{DV_{i,j}}; i \in [N]\}\}$ in the memory of GWN_j and published the public keys $\{pk_{GWN_j}\}$. It is considered that the gateway node, such as GWN_j, is under the physical locking mechanism system.
- Finally, KGC removes $\{\{TID_{DV_{i,j}}; i \in [N]\}, (sk_{GWN_j,1}, sk_{GWN_j,2}), MK_{GWN_j}, pk_{GWN_j}\}$ from his memory and keeps $\{ID_{GWN_j}, PR, A_{GWN_j}\}$ until the session key between the cloud server and the gateway nodes has been established.

3) Registration of the k^{th} Cloud Server CS_k:

- The k^{th} cloud server, CS_k, is registered by KGC by choosing a unique identity ID_{CS_k}, a positive integer $MK_{CS_k} \in_r \mathbb{Z}$, and generating $A_{CS_k} = H(ID_{CS_k} || MK_{CS_k})$ for CS_k. Subsequently, in the memory of CS_k, KGC saved the secret credential $\{A_{CS_k}, A_{GWN_j}, ID_{CS_k}, ID_{GWN_j}, PR\}$.

Finally, at the end of the registration phase, KGC stored $\{ID_{CS_k}, A_{CS_k}\}$ secretly in the memory of GWN_j and deleted $\{A_{GWN_j}, ID_{GWN_j}\}$, and $\{A_{CS_k}, ID_{CS_k}, PR, MK_{CS_k}\}$. Finally, GWN_j and CS_k both generate the secret communication key $Sk_{GWN_j,CS_k} = H(A_{GWN_j} || ID_{GWN_j} || PR || A_{CS_k} || ID_{CS_k})$.

C. Authentication Phase between $DV_{i,j}$ and GWN_j

During this phase, the following actions are taken in order to create a session key between the $DV_{i,j}$ and GWN_j.

**Step 1.* $DV_{i,j}$ selects a pair of random secrets $r_{DV_{i,j}}, f_{DV_{i,j}} \in_{ur} \chi_\beta$ and picks a fresh timestamp TS_1. Then $DV_{i,j}$ computes the subsequent operations.

**Step 2.* $DV_{i,j}$ executes $g_{DV_{i,j}} = a.r_{DV_{i,j}} + 2.f_{DV_{i,j}} \pmod{x^n + 1}$, $w_{DV_{i,j}} = (sk^1_{DV_{i,j}} + r_{DV_{i,j}}).pk_{GWN_j} \pmod{x^n + 1}$, $\delta_{DV_{i,j}} = Cha(w_{DV_{i,j}})$, $Y_{DV_{i,j}} = Mod_2(w_{DV_{i,j}}, \delta_{DV_{i,j}})$, $C_{DV_{i,j}} = H(f_{DV_{i,j}} || MK_{DV_{i,j}} || sk^2_{DV_{i,j}})$, $R_{DV_{i,j}} = H(TS_1 || \delta_{DV_{i,j}} || Y_{DV_{i,j}})$, $J_{DV_{i,j}} = R_{DV_{i,j}} \oplus C_{DV_{i,j}}$, and computes the masked identity $ID^*_{DV_{i,j}} = ID_{DV_{i,j}} \oplus H(C_{DV_{i,j}} || TS_1)$, and $G_{DV_{i,j}} = H(TID_{DV_{i,j}} || R_{DV_{i,j}} || TS_1 || C_{DV_{i,j}} || ID_{DV_{i,j}})$.

**Step 3.* Next, $DV_{i,j}$ transmits the set of messages $\langle g_{DV_{i,j}}, TID_{DV_{i,j}}, ID^*_{DV_{i,j}}, \delta_{DV_{i,j}}, J_{DV_{i,j}}, G_{DV_{i,j}}, TS_1\rangle$ to GWN_j via the open channel.

Step 3. When GWN_j receives the authentication request at time TS_1^*, it verifies the timestamp validation by checking if $|TS_1^* - TS_1| < \Delta T$, where ΔT represents the "maximum transmission delay for a received message." The following are calculated by GWN_j, if it is valid.

Step 4. GWN_j executes $w'_{DV_{i,j}} = (g_{DV_{i,j}} + pk_{DV_{i,j}}).sk_{GWN_j,1} \pmod{x^n+1}$, $Y'_{DV_{i,j}} = Mod_2(w'_{DV_{i,j}}, \delta_{DV_{i,j}})$, $R'_{DV_{i,j}} = H(TS_1 || \delta_{DV_{i,j}} || Y'_{DV_{i,j}})$, $J_{DV_{i,j}} \oplus R'_{DV_{i,j}} = C'_{DV_{i,j}}$, and retrieves $ID'_{DV_{i,j}} = ID^*_{DV_{i,j}} \oplus H(C_{DV_{i,j}} || TS_1)$, then $G'_{DV_{i,j}} = H(TID_{DV_{i,j}} || R'_{DV_{i,j}} || TS_1 || C'_{DV_{i,j}} || ID'_{DV_{i,j}})$, and verifies whether $G'_{DV_{i,j}} = G_{DV_{i,j}}$ holds or not. If not, then this phase is aborted.

Step 5. Otherwise, GWN_j selects a fresh timestamp TS_2, two polynomials $r_{GWN_j}, f_{GWN_j} \in_{ur} \chi_\beta$, then computes the following : $g_{GWN_j} = a.r_{GWN_j} + 2.f_{GWN_j} \pmod{x^n+1}$, $w_{GWN_j} = (r_{GWN_j} + sk_{GWN_j,1}).pk_{DV_{i,j}} \pmod{x^n+1}$, $\delta_{GWN_j} = Cha(w_{GWN_j})$, $\delta^*_{GWN_j} = \delta_{GWN_j} \oplus H(C_{DV_{i,j}} || TS_1)$ and $Y_{GWN_j} = Mod_2(w_{GWN_j}, \delta_{GWN_j})$.

Step 6. After that, GWN_j executes $VH_{GWN_j} = H(MK_{GWN_j} || TS_2 || Y_{GWN_j} || sk_{GWN_j,2} || ID_{GWN_j})$, $Z_{GWN_j} = H(C_{DV_{i,j}} || TS_2 || Y_{GWN_j}) \oplus VH_{GWN_j}$, and the secret session key $Sk_{DV_{i,j},GWN_j} = H(TS_2 || VH_{GWN_j} || C_{DV_{i,j}} || Y_{GWN_j} || ID_{DV_{i,j}})$.

Step 7. Now GWN_j selects a new temporary identity $TID^{new}_{DV_{i,j}}$ of $DV_{i,j}$, and computes $TID^*_{DV_{i,j}} = H(Sk_{DV_{i,j},GWN_j} || TS_2 || ID_{DV_{i,j}}) \oplus TID^{new}_{DV_{i,j}}$, as well as $SKV_{DV_{i,j},GWN_{i,j}} = H(TID^{new}_{DV_{i,j}} || Sk_{DV_{i,j},GWN_j} || TS_2 || ID_{DV_{i,j}} || VH_{GWN_j})$, then sends the authentication reply $\langle TID^*_{DV_{i,j}}, g_{GWN_j}, \delta^*_{GWN_j}, Z_{GWN_j}, SKV_{DV_{i,j},GWN_{i,j}}, TS_2 \rangle$ to $DV_{i,j}$ over a public channel.

Step 8. The user $DV_{i,j}$ confirms the timestamp's freshness by ensuring that $|TS_2^* - TS_2| < \Delta T$ occurs after receiving the authentication response at time TS_2^*. $DV_{i,j}$ proceeds with the next computational steps if this condition is met, indicating a valid timestamp.

Step 9. The $DV_{i,j}$ first executes $\delta_{GWN_j} = \delta^*_{GWN_j} \oplus H(C_{DV_{i,j}} || TS_1)$, then computes $w'_{GWN_j} = (g_{GWN_j} + pk_{GWN_j}).sk^1_{DV_{i,j}}$, and $Y'_{GWN_j} = Mod_2(w'_{GWN_j}, \delta_{GWN_j})$. Now $DV_{i,j}$ executes $H(C_{DV_{i,j}} || TS_2 || Y'_{GWN_j})$, and $Z_{GWN_j} \oplus H(C_{DV_{i,j}} || TS_2 || Y'_{GWN_j}) = VH'_{GWN_j}$. Subsequently, $DV_{i,j}$ regenerates the secret session key $SK'_{GWN_j,DV_{i,j}} = H(TS_2 || VH'_{GWN_j} || C_{DV_{i,j}} || Y'_{GWN_j} || ID_{DV_{i,j}})$, and $TID^*_{DV_{i,j}} \oplus H(SK'_{GWN_j,DV_{i,j}} || TS_2 || ID_{DV_{i,j}}) = (TID^{new}_{DV_{i,j}})^*$, and $SKV'_{DV_{i,j},GWN_{i,j}} = H((TID^{new}_{DV_{i,j}})^* || SK'_{GWN_j,DV_{i,j}} || TS_2 || ID_{DV_{i,j}} || VH'_{GWN_j})$. In the event that $SKV'_{DV_{i,j},GWN_{i,j}} = SKV_{DV_{i,j},GWN_{i,j}}$, then both $DV_{i,j}$ and GWN_j save the same session key $Sk_{DV_{i,j},GWN_j} (= SK_{GWN_j,DV_{i,j}})$ for their subsequent private conversations. Finally, $DV_{i,j}$ stored $TID^{new}_{DV_{i,j}}$ as the new temporary identity.

D. Secure Interaction between GWN_j and CS_k

These steps include the following actions:

Step 1. After the session key between $DV_{i,j}$ and GWN_j is established, $DV_{i,j}$, which contains private data designated as m_i, is combined with the current timestamp TS_3. With the session key SK_{DV_i,GWN_j}, $DV_{i,j}$ then uses the lattice-based encryption method $Enc(\cdot)$ to encrypt the data $(m_i||TS_3)$. Afterwards, $DV_{i,j}$ transmits $\{Enc_{SK_{DV_i,GWN_j}}(m_i||TS_3), TS_3\}$ to GWN_j.

Step 2. When $Enc_{SK_{DV_i,GWN_j}}(m_i||TS_3)$ is received from $DV_{i,j}$, GWN_j first confirms that TS_3 is fresh. Following confirmation that the timestamp is current, GWN_j computes $Dec_{SK_{DV_i,GWN_j}}(Enc_{SK_{DV_i,GWN_j}}(m_i||TS_3))$ using the lattice-based decryption technique $Dec(\cdot)$, which yields m_i and TS_3. Afterward, GWN_j verifies that the received timestamp and the decrypted TS_3 match accurately. GWN_j discards m_i if there are any discrepancies.

Step 3. GWN creates a new timestamp TS_4 and encrypts m_i using a Sk_{GWN_j,CS_k}, yielding $Enc_{Sk_{GWN_j,CS_k}}(m_i|| TS_4)$ then $\{Enc_{Sk_{GWN_j,CS_k}}(m_i|| TS_4), TS_4\}$ are sent to CS_k.

Step 4. Following receipt of the encrypted message and timestamp $Enc_{Sk_{GWN_j,CS_k}}(m_i||TS_4), TS_4$, CS_k applies $Dec_{Sk_{GWN_j,CS_k}}(Enc_{Sk_{GWN_j,CS_k}}(m_i||TS_4))$ to retrieve m_i and TS_4 first. After that, CS_k compares TS_4 to the received timestamp to confirm its correctness. m_i is discarded in the event that the timestamps do not coincide. If not, CS_k sends $Enc_{Sk_{GWN_j,CS_k}}(m_i||TS_4)$ for model prediction analysis on the test data to produce label predictions.

VI. Security Analysis

A. Formal Security Analysis

The formal security analysis of the proposed Ring-LWE-based authentication mechanism is provided in this section. The details of the security model and formal security proof are provided in the supplementary material.

Definition 1. *The occurrence in which the adversary $\mathcal{A}$ correctly determines the bit b following a coin toss is represented by $Succ(\mathcal{A})$. $Pr(Succ(\mathcal{A}))$ indicates the probability that this event will occur. The probability that the adversary will successfully breach the semantic security of protocol $\mathcal{P}$ in the Ring-LWE-based anonymous authentication framework for smart consumer devices in a smart home setting, as opposed to a random guess, is $Adv_{\mathcal{P}}(\mathcal{A}) = |Pr(Succ(\mathcal{A})) - 1/2|$. An authentication protocol $\mathcal{P}$ is deemed secure if the adversary's advantage, represented by $Adv_{\mathcal{P}}(\mathcal{A})$, remains insignificant.*

In Theorem 1, we demonstrate that our scheme achieves semantic security against an adversary within the random oracle model, ensuring the secure derivation of the session key between a consumer device and its associated gateway node, as well as the session key between the gateway node and the cloud server.

In this scheme, hash, execute, and send query counts are represented by q_h, q_e, and q_s, respectively, in the proposed mechanism. An adversary can mount an attack by issuing these queries to the random oracle.

Theorem 1. *Let q denote the order of the ring R_q, while $Adv^{RLWE}_{\mathcal{A}}(t)$ represents the probability advantage of an adversary in compromising the RLWE scheme, respectively, within a time bound t. In addition, let q_h, q_e, and q_s represent the numbers of hash, execute, and transmit queries caused by a probabilistic adversary $\mathcal{A}$ that operates in*

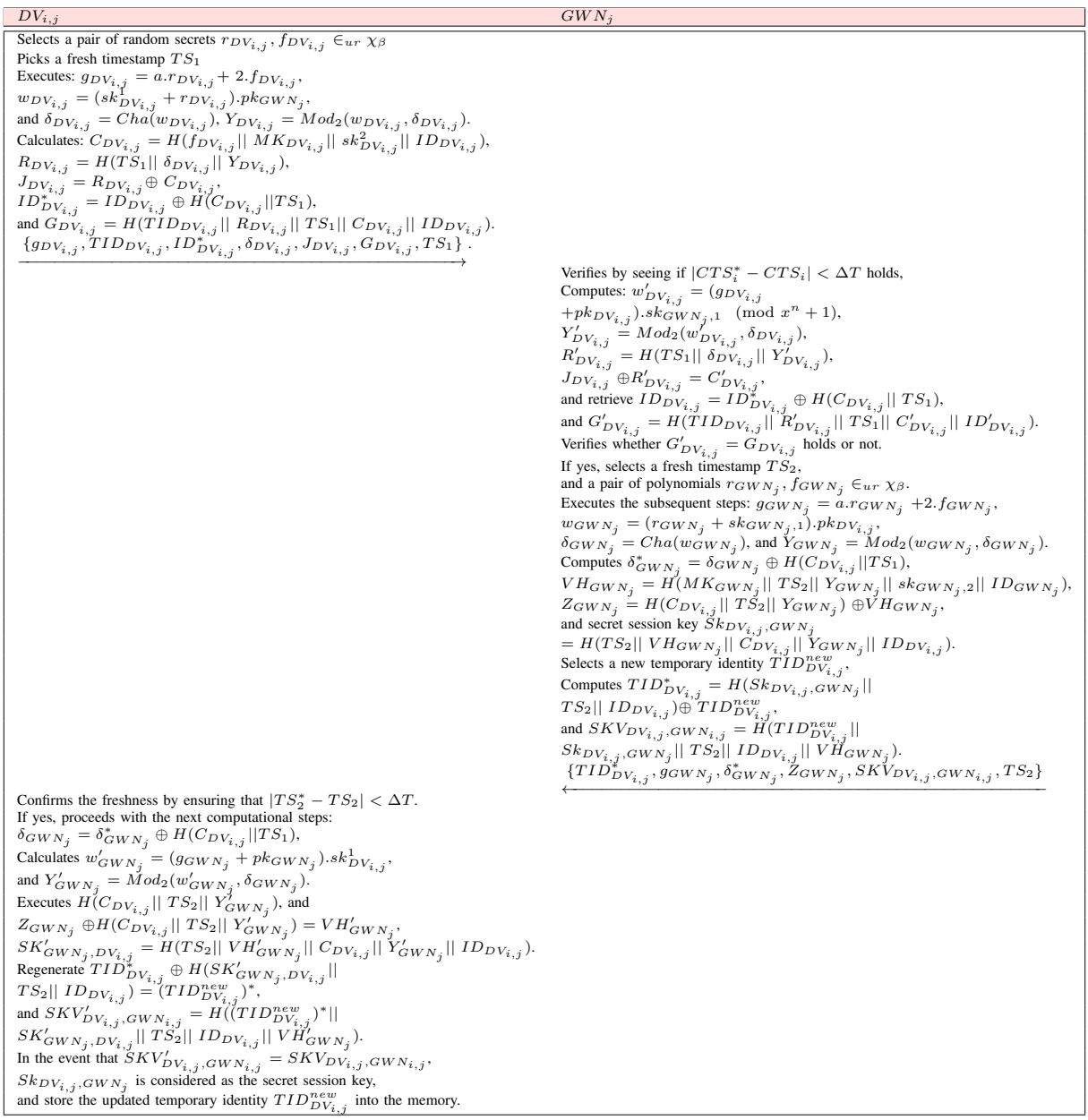

Fig. 2: Summary of the authentication phase.

PPT. The adversary's advantage in attempting to obtain the session keys that are shared between a consumer device and its corresponding gateway node, as well as the gateway node and its associated cloud server, represented as $Adv^{2PA-AKA-QS-CD}_{\mathcal{A}}(t)$*, under these circumstances, is expressed as* $Adv^{2PA-ITS-RingLWE}_{\mathcal{A}}(t) \leq O(\frac{q_h^2}{2^t}) + \frac{(q_e+q_s^2)}{q} + (q_e + q_s).Adv^{RLWE}_{\mathcal{A}}(t)$.

B. Informal (Heuristics) Security Analysis

As mentioned in Propositions 1–10, we show that the suggested authentication method (2PA-AKA-QS-CD) is resistant to a number of possible attacks. The additional material contains a thorough verification of these claims. The detailed security proofs of the propositions are provided in the supplementary material.

Proposition 1. *2PA-AKA-QS-CD is resistant to replay attacks.*

Proposition 2. *2PA-AKA-QS-CD is protected against man-in-the-middle attacks.*

Proposition 3. *2PA-AKA-QS-CD is robust against impersonation attacks.*

Proposition 4. *2PA-AKA-QS-CD is protected from privileged insider attacks.*

Proposition 5. *2PA-AKA-QS-CD is robust against attacks that involve the physical capture of a smart consumer device.*

Proposition 6. *Anonymity and untraceability are preserved in 2PA-AKA-QS-CD.*

Proposition 7. *2PA-AKA-QS-CD is resilient against lattice*

reduction attacks.

Proposition 8. *2PA-AKA-QS-CD is resistant to quantum hybrid attacks.*

Proposition 9. *2PA-AKA-QS-CD is resistant to quantum search attacks.*

Proposition 10. *2PA-AKA-QS-CD is resistant to data poisoning attacks.*

Remark 1. *The proposed authentication scheme is based on the Ring-LWE (RLWE) assumption, which is an average-case lattice problem with exponential time complexity, reduced from a worst-case lattice problem called the ideal shortest independent vector problem (SIVP). Since "the Ideal Shortest Independent Vector Problem (Id-SIVP)" is NP-hard, it is impossible to break the RLWE hardness assumption. RLWE-based cryptosystem is a widely used hardness assumption that ensures security against various quantum attacks, such as Grover's search attack, lattice reduction attack, and quantum hybrid attack. As a result, the rapid development of quantum computing requires continued evaluation of fundamental cryptographic primitives. Under such a scenario, the modular design of the proposed scheme allows for the integration of newly developed quantum-safe algorithms as they become available.*

VII. TestBed Experiment

In this section, we perform a testbed experiment and investigate the execution times for cryptographic primitives using the Cryptography 37.0.2 library. The script was written in the Python programming language. The experiment was performed under two scenarios, such as scenario 1: here we consider the GWN_j configuration with Ubuntu 22.04 LTS, featuring 16 GB 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 256 GB SSD; and scenario 2: considered as the $DV_{i,j}$ configuration 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.

Let T_h, T_g, T_{sm}, T_{pm}, T_{pa}, and T_{cha} represent the required execution time (in milliseconds) for the one-way hash function using Secure Hash Algorithm (SHA-256) algorithm, sampling from χ_β, a component-wise scalar multiplication in R_q, a component-wise polynomial multiplication in R_q, a component-wise polynomial addition in R_q and "the characteristic function in R_q, respectively. We considered the average execution time over 1,000 instances for each primitive, and the result is shown in Table III. For the energy consumption costs, Table IV displays the results of the cost required by each primitive.

VIII. Performance Analysis

In this section, we compare the proposed scheme with the existing related schemes of Mishra et al. [29], Cui et al. [30], Rewal et al. [31], Khalid et al. [32], Chaudhary et al. [33], and Ahmad and Jagatheswari [34].

TABLE III: Average execution times (in ms) of cryptographic primitives

Operation	DV/Smart device	GWN/Server
T_h	0.174898	0.020801
T_g	0.020998	0.004416
T_{sm}	0.018785	0.004067
T_{pm}	1.5712	0.159847
T_{pa}	0.067424	0.006628
T_{cha}	0.291955	0.035375

TABLE IV: Average energy consumption costs (in mJ) of cryptographic primitives

Primitives	DV/Smart device	GWN/Server
T_h	3.12193	0.3713
T_g	0.37481	0.078834
T_{sm}	0.33530	0.072595
T_{pm}	28.0459	2.85327
T_{pa}	1.20352	0.11831
T_{cha}	5.21139	0.631437

A. Communication Costs Comparison

Here, we assume that the hash sizes of outputs using SHA-256 are 256 bits, random nonces are 160 bits, identities are 160 bits, timestamps are 32 bits, elements in R_q are 4096 bits, and cha and the signal function are 1 bit each. In the proposed scheme, two messages are communicated over the public channels, such as message 1: $\{g_{DV_{i,j}}, TID_{DV_{i,j}}, ID^*_{DV_{i,j}}, \delta_{DV_{i,j}}, J_{DV_{i,j}}, G_{DV_{i,j}}, TS_1\}$, which requires (4096 + 256 + 256 + 1 + 256 + 256 + 32) = 5153 bits, and message 2: $\{TID^*_{DV_{i,j}}, g_{GWN_j}, \delta^*_{GWN_j}, Z_{GWN_j}, SKV_{DV_{i,j},GWN_{i,j}}, TS_2\}$, which requires (256 + 4096 + 256 + 256 + 256 + 32) = 5152 bits, respectively. The total of both messages needs 10306 bits. The comparison of the communication costs is shown in Table V, and the results show that the proposed scheme requires lower communication costs compared to the related schemes, except the scheme of Khalid et al. [32]. However, it is noteworthy that Khalid et al. [32] scheme does not fulfill all the security features and attributes, such as failing to maintain untraceability, dynamic node addition, and being vulnerable to key reuse attacks.

TABLE V: Comparative analysis on communication costs

Scheme	No. of messages	Total cost (in bits)
Mishra et al. [29]	3	14018
Cui et al. [30]	4	26977
Rewal et al. [31]	4	18626
Khalid et al. [32]	3	5696
Chaudhary et al. [33]	5	19490
Ahmad and Jagatheswari [34]	4	18210
Proposed scheme	2	10305

B. Computation Costs Comparison

For computational costs calculation, we used testbed experimental results for cryptographic primitives displayed in Table III. In the proposed scheme, $DV_{i,j}$ incurs a computational cost of $8T_h + 2T_g + T_{sm} + 3T_{pm} + 3T_{pa} + T_{cha} \approx 6.6677$ ms, and GWN_j needs costs of $9T_h + 2T_g + T_{sm} + 3T_{pm} + 3T_{pa} + T_{cha} \approx 0.73490$ ms. The comparison of communication costs is presented in Table VI, and it is worth noticing that the proposed scheme requires lower computation costs compared to schemes of Mishra et al. [29], Rewal et al. [31], and Ahmad

and Jagatheswari [34]. Although the proposed scheme incurs a little more cost than that of Cui et al. [30] and Khalid et al. [32], these schemes are vulnerable to key reuse attacks and fail to achieve untraceability properties.

TABLE VI: Comparative analysis on computation costs

Scheme	DV/Smart device	Server/GWN
Mishra et al. [29]	$8T_h + 4T_g + 2T_{sm} +$ $3T_{pm} + 2T_{pa} + 2T_{cha}$ ≈ 10.0955 ms	$6T_h + T_{pm}$ ≈ 0.28465 ms
Cui et al. [30]	$5T_h + 3T_g + 2T_{sm} +$ $2T_{pm} + 2T_{pa}$ ≈ 4.2523 ms	$10T_h + 3T_g + 2T_{sm} +$ $2T_{pm} + 2T_{pa} + T_{cha}$ ≈ 0.59771 ms
Rewal et al. [31]	$8T_h + 4T_g + 2T_{sm} +$ $4T_{pm} + 2T_{pa} + T_{cha}$ ≈ 8.2323 ms	$6T_h$ ≈ 0.1248 ms
Khalid et al. [32]	$8T_h + 2T_g + T_{sm} +$ $2T_{pm} + T_{pa}$ ≈ 4.6697 ms	$7T_h + T_g$ ≈ 0.15002 ms
Chaudhary et al. [33]	$12T_h + 4T_g + 2T_{sm} +$ $4T_{pm} + 2T_{pa} + 4T_{cha}$ ≈ 6.6654 ms	$10T_h + T_g + 2T_{pm}$ ≈ 0.5321 ms
Ahmad and Jagatheswari [34]	$4T_h + 4T_g + 2T_{sm} +$ $4T_{pm} + 2T_{pa} + T_{cha}$ ≈ 7.5327 ms	$5T_h$ ≈ 0.10400 ms
Proposed scheme	$8T_h + 2T_g + T_{sm}$ $+3T_{pm} + 3T_{pa} + T_{cha}$ ≈ 6.6677 ms	$9T_h + 2T_g + T_{sm}$ $+3T_{pm} + 3T_{pa} + T_{cha}$ ≈ 0.73490 ms

C. Energy Consumption Costs Comparison

This section provides the energy consumption cost in millijoules (mJ) of the proposed scheme, along with the existing schemes. This cost is calculated based on the energy consumption required for establishing the session key between the device and the gateway node in the proposed scheme displayed in Fig. 2, which means the energy required for executing cryptographic primitives used by the devices and the gateway node for completion of the proposed protocol. Based on the testbed results displayed in Table IV, we use the energy cost for the primitives to calculate the final result. Table VII shows the results of the energy consumption costs of the proposed scheme along with compared schemes, and it is worth noticing that the proposed scheme requires 3983.7700 mJ for the smart device and 105.0813 mJ for the gateway node. It is calculated as $8T_h+2T_g+T_{sm}+3T_{pm}+3T_{pa}+T_{cha}+D_m\times E \approx 3983.7700$ mJ, where, $E = 0.7500$ mJ is an energy consumption costs for smart device requires for sending a single bit message with a transmission rate of 1 Mbps operating at 5.1 V and 3.5 A and D_m is the message sizes (in bits) transferred by the smart device. For the gateway powered at 250V and 3A, sending 1 bit with the same transmission rate, the energy required is ≈ 0.01785 mJ. Similarly, the energy consumption costs for the gateway node requires as 105.0813 mJ. It is worth noticing that the proposed scheme requires lower energy consumption costs compared to other existing schemes and shows efficiency in real-world applications.

D. Functionality and Security Attributes (FS) Comparison

Table VIII shows FS features of the proposed scheme along with other related schemes. It is noteworthy to mention that the proposed scheme supports all FS, whereas the compared scheme does not support all features, which proves the superiority of the proposed scheme.

TABLE VII: Comparative analysis on energy consumption costs (in mJ)

Scheme	Device	Gateway node
Mishra et al. [29]	6973.7046	93.6170
Cui et al. [30]	6555.9035	338.3417
Rewal et al. [31]	13732.4473	11.3670
Khalid et al. [32]	683.3556	90.0715
Chaudhary et al. [33]	7584.4774	179.7159
Ahmad and Jagatheswari [34]	10214.4595	233.1925
Proposed scheme	3983.7700	105.0813

TABLE VIII: Comparative analysis on various FS attributes

Attribute (FS)	[33]	[31]	[29]	[34]	[30]	[32]	Proposed scheme
FS_1	×	✓	✓	×	✓	✓	✓
FS_2	✓	✓	✓	✓	✓	✓	✓
FS_3	✓	✓	✓	✓	✓	✓	✓
FS_4	✓	✓	✓	✓	✓	✓	✓
FS_5	✓	✓	✓	✓	✓	✓	✓
FS_6	✓	✓	✓	✓	✓	✓	✓
FS_7	✓	✓	✓	✓	✓	✓	✓
FS_8	✓	×	×	×	✓	✓	✓
FS_9	✓	×	×	×	×	×	✓
FS_{10}	×	×	×	×	×	×	✓
FS_{11}	×	×	×	×	×	×	✓
FS_{12}	×	×	×	×	×	×	✓

FS_1: Replay attack; FS_2: MITM attack; FS_3: Mutual authentication; FS_4: Key Agreement; FS_5: Device impersonation attack; FS_6: Device physical capture attack; FS_7: ESL attack under the CK-adversary model; FS_8: Anonymity; FS_9: Untraceability; FS_{10}: Node addition phase; FS_{11}: Key reuse attacks; FS_{12}: Support AI for attack resistance.
✓: A scheme is secure, or it supports an attribute; ×: A scheme is insecure, or it does not support an attribute; N/A: means Not applicable in a scheme.

IX. Simulation Results and Discussions

This section presents an ML-based simulation study of the proposed scheme, along with a discussion of the results, with the implementation available at: https://github.com/SayanRakshit/TinyMLP/blob/main/TinyMLP.ipynb.

A. Model Architecture

We adopt a compact yet expressive two-layer Multi-Layer Perceptron (MLP) tailored for high-dimensional WiFi feature embeddings. Given an input sample $\mathbf{x} \in \mathbb{R}^{16384}$ extracted from the dataset, the model performs:

$$\begin{aligned} \mathbf{h} &= \mathrm{ReLU}(\mathbf{W}_1\mathbf{x} + \mathbf{b}_1), \quad \mathbf{W}_1 \in \mathbb{R}^{512\times 16384}, \\ \hat{\mathbf{y}} &= \mathrm{Softmax}(\mathbf{W}_2\mathbf{h} + \mathbf{b}_2), \quad \mathbf{W}_2 \in \mathbb{R}^{30\times 512}. \end{aligned} \tag{1}$$

This minimal yet efficient design consists of a single hidden representation layer followed by a linear classification head:

- **Input:** 16,384-dimensional feature vector;
- **Hidden:** 512 ReLU-activated neurons;
- **Output:** 30-way softmax classifier.

The proposed network comprises approximately 8.4×10^6 trainable parameters and requires only ~ 0.0168 GFLOPs per forward pass, achieving a strong balance between computational efficiency and representational power.

The total parameter count and FLOPs are computed as:

$$\text{Params} = (D \times H + H) + (H \times C + C), \tag{2}$$

$$\text{FLOPs} = 2 \times (D \times H + H \times C) \approx 1.68 \times 10^7, \tag{3}$$

where $D = 16384$, $H = 512$, and $C = 30$. This configuration ensures real-time operation even on resource-constrained edge hardware.

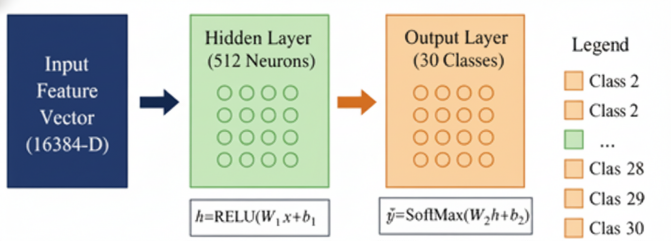

Fig. 3: Architecture diagram of the proposed **TinyMLP** model. The input WiFi feature vector (16,384-D) passes through a 512-neuron hidden layer (ReLU activation) and a 30-way softmax output.

B. Experimental Protocol

1) Dataset and Preprocessing: For experimental investigation, we utilize a LoRa radio frequency fingerprint benchmark dataset available at [35]. The dataset comprises $N = 15{,}000$ WiFi signal samples uniformly distributed across $C = 30$ device classes (500 samples per class). Each instance is represented by a 16,384-dimensional feature vector extracted from the physical-layer representation. Auxiliary metadata, such as Carrier Frequency Offset (CFO) and Received Signal Strength (RSS), are deliberately excluded to ensure modality independence.

A stratified per-class split is used to allocate 80% of samples for training and 20% for evaluation, preserving class uniformity. Feature standardization is applied online via streaming mean-variance normalization, computed incrementally to maintain memory efficiency on large datasets.

2) Training Setup: All experiments are implemented in PyTorch using the Adam optimizer with standard weight decay. The complete configuration is summarized in Table IX. To mitigate mild class imbalance, we employ a class-weighted cross-entropy loss with weights inversely proportional to class frequency.

TABLE IX: Training configuration and hyperparameters used for the proposed TinyMLP.

Parameter	Value
Optimizer	Adam
Learning rate	1×10^{-3}
Weight decay	1×10^{-4}
Batch size	512
Epochs	1000
Loss	Weighted cross-entropy
Activation	ReLU
Device	CUDA (single GPU)

3) Evaluation Metrics: We evaluate performance using both aggregate and class-wise metrics:

- Overall and per-class accuracy,
- Precision, recall, and F1-score (macro and micro averages),
- Confusion matrices (absolute and normalized),
- ROC analysis (micro, macro, and one-vs-rest),
- Inference latency and theoretical GFLOPs.

TABLE X: Per-class precision, recall, and F1-score for the proposed MLP-based router identification model. Each class has 100 test samples (total 3,000).

Class	Precision	Recall	F1-Score	Support
0	0.9899	0.9800	0.9849	100
1	1.0000	0.9700	0.9848	100
2	0.9794	0.9500	0.9645	100
3	0.9901	1.0000	0.9950	100
4	0.9700	0.9700	0.9700	100
5	1.0000	0.9900	0.9950	100
6	0.9340	0.9900	0.9612	100
7	0.9505	0.9600	0.9552	100
8	0.9505	0.9600	0.9552	100
9	0.9792	0.9400	0.9592	100
10	0.9500	0.9500	0.9500	100
11	1.0000	1.0000	1.0000	100
12	0.9802	0.9900	0.9851	100
13	0.9238	0.9700	0.9463	100
14	0.8151	0.9700	0.8858	100
15	1.0000	1.0000	1.0000	100
16	0.9604	0.9700	0.9652	100
17	0.9519	0.9900	0.9706	100
18	0.9600	0.7200	0.8229	100
19	0.9804	1.0000	0.9901	100
20	1.0000	0.9600	0.9796	100
21	0.9798	0.9700	0.9749	100
22	1.0000	1.0000	1.0000	100
23	0.9346	1.0000	0.9662	100
24	1.0000	0.9600	0.9796	100
25	0.9706	0.9900	0.9802	100
26	0.9604	0.9700	0.9652	100
27	1.0000	0.9800	0.9899	100
28	1.0000	0.9800	0.9899	100
29	1.0000	0.9900	0.9950	100
Accuracy			**0.9690**	3000
Macro Avg.	0.9704	0.9690	**0.9687**	3000
Weighted Avg.	0.9704	0.9690	**0.9687**	3000

TABLE XI: Inference performance and model complexity of the proposed TinyMLP on a single NVIDIA GPU.

Metric	Value
Device	CUDA (single GPU)
Batch size	1
Parameters	8,404,510
FLOPs per sample	1.68×10^7
GFLOPs per sample	0.0168
Mean latency	0.153 ms
Median latency	0.151 ms
90th/95th percentile	0.159 ms / 0.171 ms
Throughput	6,535 samples/s

C. Computational Efficiency

We further analyze the inference efficiency of the proposed MLP model using a single NVIDIA GPU in `float32` precision. The network, comprising 8.40×10^6 parameters, performs only 1.68×10^7 floating-point operations (FLOPs) per forward pass (~ 0.0168 GFLOPs per sample). Latency profiling over 200 repeated runs (batch size 1) yields a mean inference time of 0.153 ms per sample ($\approx$ 6,535 samples/s throughput). The distribution of inference times remains highly stable, with median 0.151 ms and 90th/95th percentile latencies of 0.159 ms and 0.171 ms, respectively. These results confirm that the proposed TinyMLP achieves real-time performance while sustaining a 96.9% test accuracy, making it ideal for resource-efficient deployment on embedded and edge platforms.

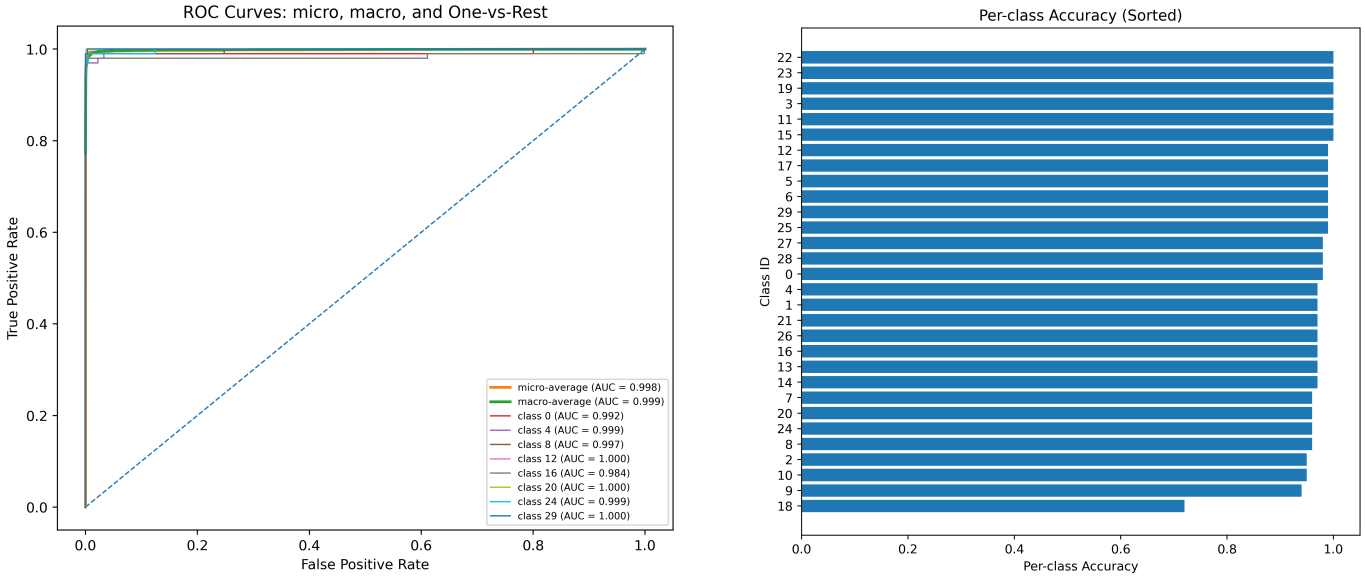

Fig. 4: Left: ROC curves showing micro/macro averages and selected one-vs-rest class curves on the test set. Right: Per-class accuracy distribution (each class contains 100 test samples).

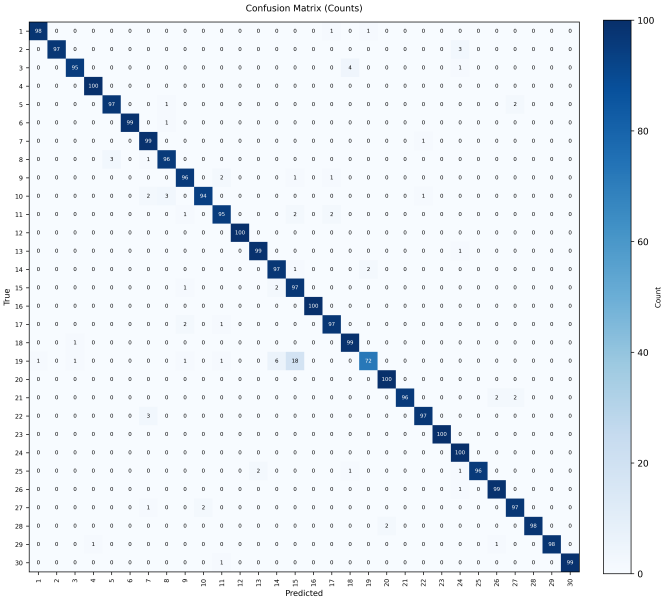

Fig. 5: Confusion matrix (absolute counts) for the proposed TinyMLP model. Rows denote ground truth and columns denote predictions.

D. Discussions

We presented a lightweight yet highly accurate MLP-based framework for device identification from WiFi signal representations. Despite the high-dimensional input space (16,384 features), the proposed TinyMLP efficiently maps data to 30 device classes using a single hidden layer. Comprehensive evaluations demonstrate strong classification performance (96.9% accuracy) coupled with low computational overhead (0.0168 GFLOPs, 0.153 ms latency). These results validate the effectiveness of simple, well-regularized architectures for high-dimensional wireless sensing and motivate future extensions toward hybrid signal semantic fusion and on-device adaptation. Such adaptation could, for instance, leverage incremental learning techniques [36] to adapt to new device types or environments without catastrophic forgetting, making them practical for communication systems.

X. Conclusion

In this paper, we propose a quantum-resistant authentication protocol for consumer electronic devices that resists adversarial attacks. A comprehensive performance analysis demonstrated the efficiency and feasibility of the proposed scheme. The formal security analysis using the RoR model proved the correctness of the proposed scheme, whereas the informal security analysis offered resistance against various potential active and passive classical, as well as quantum, threats. The session key is constructed relying on RLWE-hardness, which proves that the quantum secure key is further proof of communication. Real-time experiments for primitives using Raspberry Pi devices validated the scheme's efficiency and scalability. Finally, the ML model, called TinyMLP, was applied to matchmark radio frequency data for consumer devices and achieved $\approx 97\%$ accuracy, which makes the protocol practicable for real-world resource-constrained devices.

In the future, we would like to extend testbed evaluation to large-scale, real-world IoT deployments along with heterogeneous environments with diverse device capabilities. It should further validate scalability, robustness, and performance under practical constraints.

References

[1] S. Raza, M. Garg, D. J. Reji, S. R. Bashir, and C. Ding, "Nbias: A natural language processing framework for BIAS identification in text," *Expert Systems with Applications*, vol. 237, p. 121542, 2024.

[2] W. Wang, Z. Chen, X. Chen, J. Wu, X. Zhu, G. Zeng, P. Luo, T. Lu, J. Zhou, Y. Qiao, and J. Dai, "VisionLLM: Large Language Model is also an Open-Ended Decoder for Vision-Centric Tasks," 2023. [Online]. Available: https://arxiv.org/abs/2305.11175

[3] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards Deep Learning Models Resistant to Adversarial Attacks," 2019. [Online]. Available: https://arxiv.org/abs/1706.06083

[4] A. Gozuoglu, O. Ozgonenel, and C. Gezegin, "Design and Implementation of Controller Boards to Monitor and Control Home Appliances for Future Smart Homes," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 9, pp. 11 458–11 465, 2024.

[5] Q. Lyu, N. Zheng, H. Liu, C. Gao, S. Chen, and J. Liu, "Remotely Access My Smart Home in Private: An Anti-Tracking Authentication and Key Agreement Scheme," *IEEE Access*, vol. 7, pp. 41 835–41 851, 2019.

[6] Y. Cho, J. Oh, D. Kwon, S. Son, J. Lee, and Y. Park, "A Secure and Anonymous User Authentication Scheme for IoT-Enabled Smart Home Environments Using PUF," *IEEE Access*, vol. 10, pp. 101 330–101 346, 2022.

[7] K. Nimmy, S. Sankaran, K. Achuthan, and P. Calyam, "Lightweight and Privacy-Preserving Remote User Authentication for Smart Homes," *IEEE Access*, vol. 10, pp. 176–190, 2022.

[8] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 2, pp. 391–406, 2020.

[9] W. Iqbal, H. Abbas, P. Deng, J. Wan, B. Rauf, Y. Abbas, and I. Rashid, "ALAM: Anonymous Lightweight Authentication Mechanism for SDN-Enabled Smart Homes," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9622–9633, 2021.

[10] S. Yu, A. K. Das, and Y. Park, "Comments on "alam: Anonymous lightweight authentication mechanism for sdn enabled smart homes"," *IEEE Access*, vol. 9, pp. 49 154–49 159, 2021.

[11] S. K. Sahoo, S. K. Pattnaik, S. R. Samal, C. K. Nayak, J. K. Das, and V. Poulkov, "Stesh: Intelligent speech technology enabled smart home automation using iot," *Journal of Mobile Multimedia*, vol. 18, no. 6, pp. 1471–1496, 2022.

[12] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for iot applications in smart homes," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1844–1852, 2017.

[13] "Pqcaie: Post quantum cryptographic authentication scheme for iot-based e-health systems," *Internet of Things*, vol. 27, p. 101228, 2024.

[14] S. Kumari, M. Singh, R. Singh, and H. Tewari, "A post-quantum lattice based lightweight authentication and code-based hybrid encryption scheme for iot devices," *Computer Networks*, vol. 217, p. 109327, 2022.

[15] T. Qasim, V. A. Siris, I. Oosthuizen, M. Rajarajan, and S. Biswas, "Quantum secure biometric authentication in decentralised systems," in *2025 IEEE International Joint Conference on Biometrics (IJCB)*, 2025, pp. 1–9.

[16] S. Kusal, S. Patil, J. Choudrie, K. Kotecha, D. Vora, and I. Pappas, "A systematic review of applications of natural language processing and future challenges with special emphasis in text-based emotion detection," *Artificial Intelligence Review*, vol. 56, no. 12, pp. 15 129–15 215, 2023.

[17] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[18] R. Canetti and H. Krawczyk, "Universally Composable Notions of Key Exchange and Secure Channels," in *International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'02)*, Amsterdam, The Netherlands, 2002, pp. 337–351.

[19] A. Vangala, A. K. Das, A. Mitra, S. K. Das, and Y. Park, "Blockchain-Enabled Authenticated Key Agreement Scheme for Mobile Vehicles-Assisted Precision Agricultural IoT Networks," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 904–919, 2023.

[20] 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," *Information and Computation*, vol. 294, p. 105067, 2023.

[21] T. Messerges, E. Dabbish, and R. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[22] C. Xu, F. Erata, and J. Szefer, "Exploration of Quantum Computer Power Side-Channels," 2023. [Online]. Available: https://arxiv.org/abs/2304.03315

[23] Sauvik Bhattacharya and Oscar Garcia Morchon and Ronald Rietman and Ludo Tolhuizen, "spKEX: An optimized lattice-based key exchange," *IACR Cryptol. ePrint Arch.*, p. 709, 2017. [Online]. Available: http://eprint.iacr.org/2017/709

[24] Y. Huang, G. Xu, X. Song, and Y. Xu, "An Efficient RLWE-Based Privacy-Preserving Authentication Scheme Based on Edge Computing in Industrial Internet of Things," *IEEE Transactions on Services Computing*, vol. 17, no. 5, pp. 2012–2026, 2024.

[25] A. Bogdanov and L. Trevisan, "On Worst-Case to Average-Case Reductions for NP Problems," *SIAM Journal on Computing*, vol. 36, no. 4, pp. 1119–1159, 2006.

[26] P. Bagchi, R. Maheshwari, B. Bera, A. K. Das, Y. Park, P. Lorenz, and D. K. Y. Yau, "Public Blockchain-Envisioned Security Scheme Using Post Quantum Lattice-Based Aggregate Signature for Internet of Drones Applications," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 8, pp. 10 393–10 408, 2023.

[27] Z. Brakerski and V. Vaikuntanathan, "Fully homomorphic encryption from ring-LWE and security for key dependent messages," in *Annual cryptology conference*, Santa Barbara, CA, USA, 2011, pp. 505–524.

[28] J. Zhang, Z. Zhang, J. Ding, M. Snook, and O. Dagdelen, "Authenticated Key Exchange from Ideal Lattices," in *Advances in Cryptology - EUROCRYPT 2015*, Sofia, Bulgaria, 2015, pp. 719–751.

[29] D. Mishra, M. Singh, P. Rewal, K. Pursharthi, N. Kumar, A. Barnawi, and R. S. Rathore, "Quantum-Safe Secure and Authorized Communication Protocol for Internet of Drones," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 12, pp. 16 499–16 507, 2023.

[30] J. Cui, J. Liu, L. Wei, I. Bolodurina, J. Li, and H. Zhong, "Post-quantum Secure Authenticated Key Agreement Scheme for Vehicular Digital Twin," *IEEE Transactions on Mobile Computing*, pp. 1–16, 2025, doi: 10.1109/TMC.2025.3618752.

[31] P. Rewal, M. Singh, D. Mishra, K. Pursharthi, and A. Mishra, "Quantum-safe three-party lattice based authenticated key agreement protocol for mobile devices," *Journal of Information Security and Applications*, vol. 75, p. 103505, 2023.

[32] H. Khalid, S. Jahari Hashim, F. Hashim, W. Ameen Mahmoud Al-Jawher, M. Akmal Chaudhary, and H. H. M. Altarturi, "RAVEN: Robust Anonymous Vehicular End-to-End Encryption and Efficient Mutual Authentication for Post-Quantum Intelligent Transportation Systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 11, pp. 17 574–17 586, 2024.

[33] 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. 136 947–136 957, 2023.

[34] 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. 157 247–157 259, 2024.

[35] G. Shen, J. Zhang, A. Marshall, and J. R. Cavallaro, "Towards Scalable and Channel-Robust Radio Frequency Fingerprint Identification for LoRa," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 774–787, 2022.

[36] S. Rakshit, A. Mohanty, R. Chavhan, B. Banerjee, G. Roig, and S. Chaudhuri, "Frida–generative feature replay for incremental domain adaptation," *Computer Vision and Image Understanding*, vol. 217, p. 103367, 2022.

Prithwi Bagchi received the M.Sc. degree in Mathematics from Presidency University, Kolkata, India, and the Ph.D. degree in Computer Science and Engineering from International Institute of Information Technology (IIIT), Hyderabad, India. He is affiliated with the Center for Security, Theory and Algorithmic Research at IIIT, Hyderabad. His research interests include post-quantum cryptography, applied cryptography, and network security, with a focus on designing secure and efficient protocols for emerging computing environments.

Basudeb Bera received a Ph.D. degree in computer science and engineering from the International Institute of Information Technology, Hyderabad, India, in 2022. He also received his M.Sc. degree in mathematics and computing in 2014 from IIT (ISM) Dhanbad, India, and M.Tech. degree in computer science and data processing in 2017 from IIT Kharagpur, India. He is currently a post-doctoral fellow at the National University of Singapore (NUS), Singapore. He was also a post-doctoral fellow at the Singapore University of Technology & Design (SUTD), Singapore. His research interests are cryptography, communication and network security, IoT security, post-quantum security, and blockchain technology. He has published over 41 papers in international journals and conferences in his research areas.

Sayan Rakshit received the M.Sc. degree in mathematics with computer applications from the National Institute of Technology Durgapur, Durgapur, India, and the M.Tech. degree in computer science and data processing from the Indian Institute of Technology Kharagpur, Kharagpur, India, and the Ph.D. degree in computer vision from the Indian Institute of Technology Bombay, Mumbai, India. He is currently a researcher in artificial intelligence and computer vision based in Tokyo, Japan. His current research interests include computer vision, machine learning, domain adaptation, generative artificial intelligence, vision-language learning, autonomous perception, and robust visual understanding.

Ashok Kumar Das (Senior Member, IEEE) received a Ph.D. degree in computer science and engineering, an M.Tech. degree in computer science and data processing, and an M.Sc. degree in mathematics from IIT Kharagpur, India. He is currently a full professor with the Center for Security, Theory and Algorithmic Research, IIIT, Hyderabad, India. He is a distinguished adjunct professor at Korea University, Seoul, South Korea. He was also a visiting research professor with the Virginia Modelling, Analysis and Simulation Centre, Old Dominion University, Suffolk, VA 23435, USA. His research interests include cryptography, system and network security, blockchain, security in the IoT, Internet of Vehicles (IoV), Internet of Drones (IoD), smart grids, smart city, cloud/fog computing, intrusion detection, AI/ML security, and quantum and post-quantum cryptography. He has authored over 545 publications, including more than 470 journal papers. He is a Highly Cited Researcher (2022-23). He is/was on the editorial board of IEEE Transactions on Information Forensics and Security, IEEE Systems Journal, Journal of Network and Computer Applications (Elsevier), Computer Communications (Elsevier), International Journal of Communication Systems (Wiley), Journal of Cloud Computing (Springer), Cyber Security and Applications (Elsevier), Alexandria Engineering Journal (Elsevier), IET Communications, KSII Transactions on Internet and Information Systems, and International Journal of Communication Systems (Wiley). His Google Scholar h-index exceeds 100 with over 32,100 citations.

Sujit Biswas (Senior Member, IEEE) is a Senior Lecturer (Associate Professor) in Cybersecurity in the Department of Computer Science at City St. George's, University of London, U.K. He received the Ph.D. degree in Computer Science and Technology from Beijing Institute of Technology, China. He is also an Honorary Research Fellow at University College London, U.K. Previously, he was a Postdoctoral Research Fellow at Centre for Vision, Speech and Signal Processing (CVSSP), University of Surrey, and a Lecturer at University of East London. His research interests include Blockchain, Federated Learning, Distributed Consensus, and Privacy-preserving AI. He has published in leading journals such as IEEE Internet of Things Journal, IEEE Transactions on Big Data, IEEE Transactions on Services Computing, IEEE Transactions on Network and Service Management, IEEE TETCI, IEEE TNSE, and ACM Computing Surveys. He is an Associate Editor of IEEE Transactions on Consumer Electronics and serves on the editorial boards of Discover Computing, IET Blockchain, IET Computers & Digital Techniques, IET Biometrics, and MDPI Blockchain. He has also organised several special sessions and workshops at leading international venues and is actively involved in industry-academia collaborative research on trustworthy AI and blockchain-enabled systems.

Mohammad Kamrul Hasan (Senior Member, IEEE) is currently an Professor Madaya and the Head of the Network and Communication Technology Research Laboratory at the Cyber Security Center, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM). He is also appointed as a Distinguished Visiting Professor of Practice at the Faculty of Creative Industry, Universitas Teknologi Bandung (UTB), Indonesia, and serves as a Visiting Associate Professor at the Department of Computer Science and Engineering, Jain University, Bangalore, India. Dr. Kamrul received his Doctor of Philosophy (Ph.D.) and Master of Science (MSc) degrees in Electrical and Communication Engineering from the Faculty of Engineering, International Islamic University Malaysia, in 2016. His research interests span information-centric networks, wireless communication and networking, artificial intelligence, cyber-physical systems, smart vehicular networks, smart grids, and Industrial Internet of Things (IIoT). Dr Kamrul has been received national and International grants total amounting more than 1million Ringgit. He has been recognized as one of the top 2% of scientists for single and long career since 2022, and highly cited authors worldwide, based on rankings by Stanford University, Elsevier, and Web of Science. Dr. Kamrul has authored and co-authored over 230 indexed publications in high-impact journals and international conference proceedings. Dr. Kamrul is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), a signatory member of the Institution of Engineering and Technology (IET), and a member of the Internet Society. He is also a Certified Professional Technologist with the Board of Technologists Malaysia. In addition, he has actively contributed to numerous IEEE technical, training, and humanitarian programs in Malaysia. He serves the research community as a Guest Editor and Associate Editor for several leading publishers, including IEEE, Elsevier, Springer Nature, IET, MDPI, and Bentham Science.

Biplab Sikdar (Fellow, IEEE) received the B.Tech. degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He is a Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore, where he serves as the Vice Dean with the Faculty of Engineering. He was an Assistant Professor from 2001 to 2007 and an Associate Professor from 2007 to 2013 with the Department of Electrical, Computer, and Systems Engineering, Rensselaer Polytechnic Institute from 2001 to 2013. His research interests include IoT and cyber–physical system security, network security, and network performance evaluation. Dr. Sikdar served as an Associate Editor for the IEEE Transactions on Communications from 2007 to 2012 and an Associate Editor for the IEEE Transactions on Mobile Computing from 2014 to 2017. He is a member of Eta Kappa Nu and Tau Beta Pi.