Post-Quantum Lattice-Based Secure Reconciliation Enabled Key Agreement Protocol for IoT

Dharminder Dharminder, Challa Bhageeratha Reddy, Ashok Kumar Das, *Senior Member, IEEE*, Youngho Park, *Member, IEEE*, and Sajjad Shaukat Jamal

***Abstract*—The authenticated key agreement is one of the major security services that can be used to secure an Internet of Things (IoT) environment, where the devices collect the data and the data is then aggregated at the cloud server, and then a user needs to access the data stored at the server(s) securely. For this purpose, after a mutual authentication performed between a user and the accessed server, a session key needs to be established among them for secure communication. In this article, we design an efficient lattice-based authenticated key exchange protocol using ring-based version of learning with errors assumption for the IoT-enabled smart devices. The proposed protocol is basically a key exchange that uses the reconciliation mechanism. The detailed security analysis under the standard model has been performed along with the informal security analysis to show that the proposed protocol is robust against different attacks. We then simulate the proposed protocol under the NS-3 simulator to measure the network performance parameters like network throughput and latency. A comparative analysis shows that the proposed protocol has superior security, less computational cost, and comparable communication cost when compered these parameters with the other competing schemes.**

***Index Terms*—Authentication and key agreement, Internet of Things (IoT), lattice-based cryptography, security, simulation.**

I. Introduction

THE Internet of Things (IoT) has dramatically revolutionized many different fields. It enables the sensors to measure with more accuracy in an online healthcare application. It also improves the quality of multimedia content transferred through IoT objects. It has been observed that the wireless communication is used in IoT applications and it suffers various risks where the users/devices are vulnerable to the privacy, security, and control of data being circulated over the public network.

Upsurge growth in a wireless communication network has been witnessed in smart living standards, which necessitates the usage of low-cost IoT devices. Almost any smart device user is keen about his/her user privacy when using data on Internet platforms, such as mail, broadcast, and so on. The breach of confidentiality and anonymity of smart device users in a wireless network are all dependent on the provision of user anonymity, authentication, and confidentiality. If a device is hacked and the hacker recovers the saved credentials, user anonymity is important in wireless communication.

IoT-based devices have recently become increasingly common in the development of communication technologies. IoT devices, such as cellphones, tablets, and personal digital assistants, can handly integrate to the cloud server with ease. Security and privacy have become more primary concerns as this data transmission process takes place over an open wireless channel. The most prevalent cryptographic system is now an authentication protocol for IoT devices, which provides secure connection between devices and servers.

Several cryptographic techniques have emerged lately to ensure that all extant smart device end-users in a wireless system can transferring data in a secure manner. Many authentication and session key agreement scheme architectures, on the other hand, are based on hard problem number theoretic. Shor's algorithms [1], [2] pose a severe security threat to these schemes. The concept of a lattice-based cryptosystem, which was first suggested in the 18th century by mathematicians, such as Lagrange, Gauss, and later Minkowski, could be beneficial in overcoming these security difficulties in smart device authentication and session key agreement. For creating a new cryptographic primitive, Ajtai [3] made a progress by inventing a tool. In the advent of quantum computation, contribute to a better understanding of grid problem and their interactions to cryptography. Post-quantum cryptography is made much easier and more efficient by using lattice architectures. Their security is built on a worst-case scenario. Other known cryptographic hard problems, such as factorization and discrete logarithm issues, are predicated on some average-case assumption, such as discrete logarithm problem (DLP). Authentication protocols for IoT devices are typically based on number theoretic hard problems. Although, with the advent of the quantum age, new attacks will be launched against them, posing a major danger

Manuscript received 18 July 2022; revised 23 September 2022; accepted 9 October 2022. Date of publication 12 October 2022; date of current version 24 January 2023. This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant 2020R1I1A3058605; in part by the Blockchain Project under the Ripple Centre of Excellence (CoE) Scheme, CoE in Blockchain, IIIT Hyderabad, India, under Grant IIIT/R&D Office/Internal Projects/Ripple/2021-22/009; and in part by the Deanship of Scientific Research at King Khalid University under Grant R.G.P. 2/86/43. *(Corresponding authors: Ashok Kumar Das; Youngho Park.)*

Dharminder Dharminder and Challa Bhageeratha Reddy are with the Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Chennai 601 103, India (e-mail: c_dharminder@ch.amrita.edu; ch.en.u4cys20009@ch.students.amrita.edu).

Ashok Kumar Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology Hyderabad, Hyderabad 500 032, India (e-mail: iitkgp.akdas@gmail.com).

Youngho Park is with the School of Electronics Engineering, Kyungpook National University, Daegu 41566, South Korea (e-mail: parkyh@knu.ac.kr).

Sajjad Shaukat Jamal is with the Department of Mathematics, College of Science, King Khalid University, Abha 62529, Saudi Arabia (e-mail: shussain@kku.edu.sa).

Digital Object Identifier 10.1109/JIOT.2022.3213990

to established approaches. Any probabilistic polynomial time (PPT) opponent can breach the classic mathematical assumption using the Shor algorithms. As a result, post-quantum cryptography, which can withstand quantum computer attacks, has emerged as a new dimension in encryption.

The National Institute of Standards and Technology (NIST) had started a program in 2016 with the goal of developing and evaluating new cryptographic primitives to withstand quantum assaults. There are various known approaches for dealing with these problems. All of these strategies, however, are no longer applicable in the presence of a quantum computer. Ideal lattices are a subset of lattices that are useful for generating "efficient cryptographic primitives with some additional algebraic structure for quantum computer attack resistance." The lattice-based cryptographic hard assumptions can withstand quantum assaults effectively. The shortest vector problem (SVP), short integer solution (SIS), closest vector problem (CVP), and "ring learning mistake" are all names for the hard assumption of the ring learning with error (RLWE).

Key management, authentication, access control, and intrusion detection are the important security services in wireless sensor networks and IoT [4], [5], [6], [7], [8], [9]. When compared to traditional cryptographic systems, ideal lattice-based cryptographic systems [10] have reduced processing costs. First, an ideal lattice and RLWE protocols [10], [11] are presented, and it is demonstrated that it is as challenging as other worst-case hard problems on ideal lattices. Zhang et al. [11] developed an authenticated key exchange system for the perfect lattice, which is theoretically straightforward and resembles "Diffie–Hellman (DH)-based protocols like HMQV (CRYPTO'05)" [12] and "optimal authenticated key exchange" OAKE (ACM CCS'13) [13], which is a high-performance secure DH protocol. Alkim et al. [14] originally proposed a post-quantum key exchange mechanism. Ding et al. [15] went to describe a key exchange and authentication mechanism based on ring learning with an error issue. Furthermore, Ding et al. [16] provided security against post-quantum attacks, where the RLWE-based key exchange can provide a strong security with a small key size.

Taking inspiration from Fluhrer [17], Ding et al. [18] introduced the idea of signal leakage attack for RLWE-key exchange reusing public/private keys. In this idea, an adversary analysis the output of the signal function, and he recovers the private key by establishing multiple sessions with the honest party. The main advantage of this idea is its applicability when the session key is established using least significant bits of approximately equal bit lengths.

The number of steps required is $2q$ to retrieve the private key of the server, where q is the prime modulus. In the next year 2018, Ding et al. [19] introduced on the advantage of this attack is less number of steps required to retrieve the private key of an honest party. The original signal leakage attack requires $2q$ steps, but the improved signal leakage attack requires $q + c$ steps, where c is some constant. Therefore, the signal leakage attack is as follows. At first, the honest party does not add the errors f_s during the computation of secret key sk_s. The adversary sets his private key $r_i = 0$ where the corresponding public value is a constant. The public value takes the form $x_i = a.r_i + 2f_i$, where a is an element of the ring. The number of steps to retrieve the private key can be reduced to $(q/2) + 4$ for the simplified case.

For the quantum world, Ding et al. [16] developed a high-entropy and key exchange protocol based on RLWE over a public channel. However, their protocol [16] suffers from signal leakage attack. For mobile devices, Feng et al. [20] developed an anonymous authenticated key exchange system. They also compared their technique with others and provided security proofs in the random oracle model. Using the lattice hard problem, Islam [21] devised an authentication technique for the post-quantum era. But, this protocol can not resist signal leakage attack [19]. Dharminder and Chandran [22] suggested a lattice-based mobile device authentication system based on the RLWE problem. Unfortunately, their protocol suffers from both signal leakage attack and incorrect verification during the key exchange phase. Rana and Mishra [23] proposed a post-quantum key exchange protocol using the ring version of learning with error (LWE) assumption for IoT-enabled smart devices. However, they observed that the protocol [23] suffers some errors during authenticated key agreement.

A. Research Gap and Contributions

Based on the literature, it becomes essential to understand the advanced threats if a quantum computer comes in to existence. The most of authentication protocols based on number theoretic assumptions like RSA/discrete logarithm are vulnerable to quantum attacks due to Shor's algorithm. Although, there are many post-quantum secure authentication protocols, but they have their own drawbacks. For example, the protocols [20], [21], [22] can not resist signal leakage attack as explained in [19], and the protocol [23] is mathematically incorrect. It is analyzed that the protocol cannot establish authenticated key because of an error factor added in the hashing with reconciliation. Therefore, we aim to propose a new authenticated key agreement protocol for IoT smart devices. The proposed design is based ring version of the ideal-based key exchange for IoT devices. The proposed design possesses provably security. The formal security analysis and comparative performance ensure its security and efficiency as well.

B. Paper Outline

In Section II, we discuss some basic knowledge of lattice-based RLWE problem and state the proposed assumptions. The system models, including the network and threat models are discussed in Section III. In Section IV, we state various phases related to our authentication scheme. Section V-A demonstrates the proof of the proposed scheme. In Section V, we discuss the security analysis of our scheme against various threats. In Section VI, we do a comparative performance analysis of the proposed scheme with some other relevant authentication schemes. In Section VII, we provide the simulation results using the widely accepted discrete event network simulator, NS-3. Finally, Section VIII concludes this article.

II. Preliminaries

The design has been simplified in short notations, symbols, and definitions in this part of the present lattice-based technique [24]. Lattices are very good sources of quantum-safe cryptographic assumptions, and resistance toward the quantum attacks in modern cryptography. The constructions based on lattices have received good enough mathematical security proofs. The security of lattice-based cryptographic algorithms is based on the hard assumptions, such as finding integer short vector/short independent vectors in an n-dimensional Euclidean space $\mathbb{R}^n$ as shown in [25], where $\mathbb{R}$ denotes the set of reals.

A. Basics of RLWE

This section focuses to discuss the background of the ring version of LWE and its few fundamental assumptions. We demonstrate some of mathematical hard assumptions to prove both security and correctness of the proposed design.

Consider $q > 2$ is an odd prime number, $\mathbb{R}$ denotes the set of reals, and $\mathbb{Z}$ denotes the set of all integers. Suppose $\mathbb{Z}[x]$ and $\mathbb{Z}_q[x]$ denote two different rings of polynomials over $\mathbb{Z}$ and $\mathbb{Z}_q$, respectively. We have considered two different rings of polynomials $R = (\mathbb{Z}[x]/(x^n + 1))$ and $R_q = (\mathbb{Z}_q[x]/(x^n + 1))$. An arbitrary element chosen from the ring of polynomials is denoted by $c = c_0 + c_1x + c_2x^2 + c_3x^2 + \cdots + c_{n-1}.x^{n-1} \in R$. The Euclidean length/norm computed by $||c|| = \sqrt{{c_0}^2 + {c_1}^2 + {c_2}^2 + \cdots + {c_{n-1}}^2}$ and the infinity norm/length L_∞ is $||c_\infty|| = \max\{c_0, c_1, c_2, c_3, \ldots, c_{n-1}\}$. Let $\beta > 0$ be a real number and χ_β be the Gaussian over R_q.

Lemma 1 [11]: If we consider two ring elements c and d from the ring R, the following relations hold:

$$c \cdot d \leq \sqrt{n} \cdot ||c|| \cdot ||d||$$
$$||c \cdot d||_\infty \leq n \cdot ||c|| \cdot ||d||.$$

Lemma 2 [19]: Let $\beta > 0$ be a real number such that $\beta = \omega\sqrt{\log(n)}$, then the probability $\Pr_{c \leftarrow \chi_\beta}[\, ||c|| > \beta\sqrt{n}\,] \leq 2^{-n+1}$.

Consider that the mid portion of $\mathbb{Z}_q = \{-((q-1)/2), \ldots, ((q-1)/2)\}$ is denoted by M, which is defined $M = \{-\lfloor (q/4) \rfloor, \ldots, \lfloor (q/4) \rfloor\}$. The characteristic map Cha consists the complements of the set $M \ \forall \ x \in \mathbb{Z}_q$, where

$$\text{Cha}(x) = \begin{cases} 0, & \text{if } x \in M \\ 1, & \text{otherwise.} \end{cases}$$

The auxiliary mod function is denoted as follows:

$$\text{Mod}_2 : \mathbb{Z}_q \times \{0, 1\} \rightarrow \{0, 1\}$$

and defined by

$$\text{Mod}_2(a, b) = \left(a + b \cdot \frac{q-1}{2} \pmod q \right) \pmod 2$$

where $a \in \mathbb{Z}_q$ and b is corresponding to the output of characteristic map of a satisfying $b = \text{Cha}(a)$.

Lemma 3 [19]: Let $q > 2$ be a large prime, and two random elements c and e of the finite ring R_q, where e follows the inequality $|e| < (q/8)$. Then, the modular mapping $\text{Mod}_2(c, \text{Cha}(c)) = \text{Mod}_2(\omega, \text{Cha}(c))$ satisfies $\omega = c + 2e$.

We now discuss two functions Cha and Mod_2 over the finite ring R_q. Let "$c = c_0 + c_1.x + c_2.x^2 + c_3.x^2 + \cdots + c_{n-1}.x^{n-1} \in R$," where $c = (c_0, c_1, c_2, c_3, \ldots, c_{n-1})$ denotes a tuple. If $u = \{u_0, u_1, u_2, \ldots, u_{n-1}\} \in \{0, 1\}^n$ is a random vector, a relation between two functions is defined by $\text{Cha}\{c\} = (\text{Cha}\{c_0\}, \text{Cha}\{c_1\}, \text{Cha}\{c_3\}, \ldots, \text{Cha}(c_{n-1}))$, and $\text{Mod}_2(c, u) = (\text{Mod}_2(c_0, u_0), \text{Mod}_2(c_1, u_2), \text{Mod}_2(c_2, u_2), \ldots, \text{Mod}_2(c_{n-1}, u_{n-1}))$.

B. Assumptions

In the following, we discuss some assumptions, and terminologies based on the ideal generated lattices.

1) *RLWE:* The RLWE is a mathematical assumption A_{s,χ_β} possessing uniform distribution $(c, c.s + e) \in R_q \times R_q$, such that $c, s \leftarrow R_q$ are random and the small error $e \leftarrow \chi_\beta$ is chosen independently from c. The ring-based LWE, $\text{RLWE}_{q,\alpha}$ is hard to distinguish A_{s,χ_β} for any PPTs adversary from uniform distribution followed on $R_q \times R_q$.
2) *Pairing With Errors (PWE):* The mapping described by $\psi(y, s) = \text{Mod}_2(y \cdot s, \text{Cha}(y \cdot s))$, such that y and s are two members of R_q. Then, the PWE assumption is to compute $\psi(y, s)$, if $c, y, z \in R_q$ are known and $z = c \cdot s + 2 \cdot e$ such that $s, e \in \chi_\beta$ are unknown.
3) *Decision PWEs (DPWE):* The decision version of the PWE assumption is to distinguish $k = y.s + 2e'$ and $z = c.s + 2.e$, such that $s,\ e',\ e \in \chi_\beta$ are secret or (k, z) follows uniform distribution on $R_q \times R_q$ [24].

III. System Models

This section explains both the network and adversary models that are essential to design and analysis of the proposed scheme in this article.

A. Network Model

An IoT-based network model considered for the proposed scheme is shown in Fig. 1. There are various IoT applications, such as smart home, smart agriculture, smart healthcare, and so on. In each application, IoT smart devices are deployed to monitor the surrounding information and send their nearby gateway node. In turn, the gateway nodes send the aggregated data to the cloud server(s) via the base station. For security reasons, the sensing information must be securely sent to the gateway nodes and the aggregated data needs to be securely sent to the cloud server(s). Now, assume that there is a user who wants to access the stored data at the cloud server(s). However, before granting access to the data by an accessed cloud server, a mutual authentication needs to be executed among the user and the server to confirm that there are legitimate, and after the successful mutual authentication a session key needs to be established among them for future secure transmission of the accessed data. This is done by designing a new lattice-based authenticated key agreement scheme in the IoT scenario.

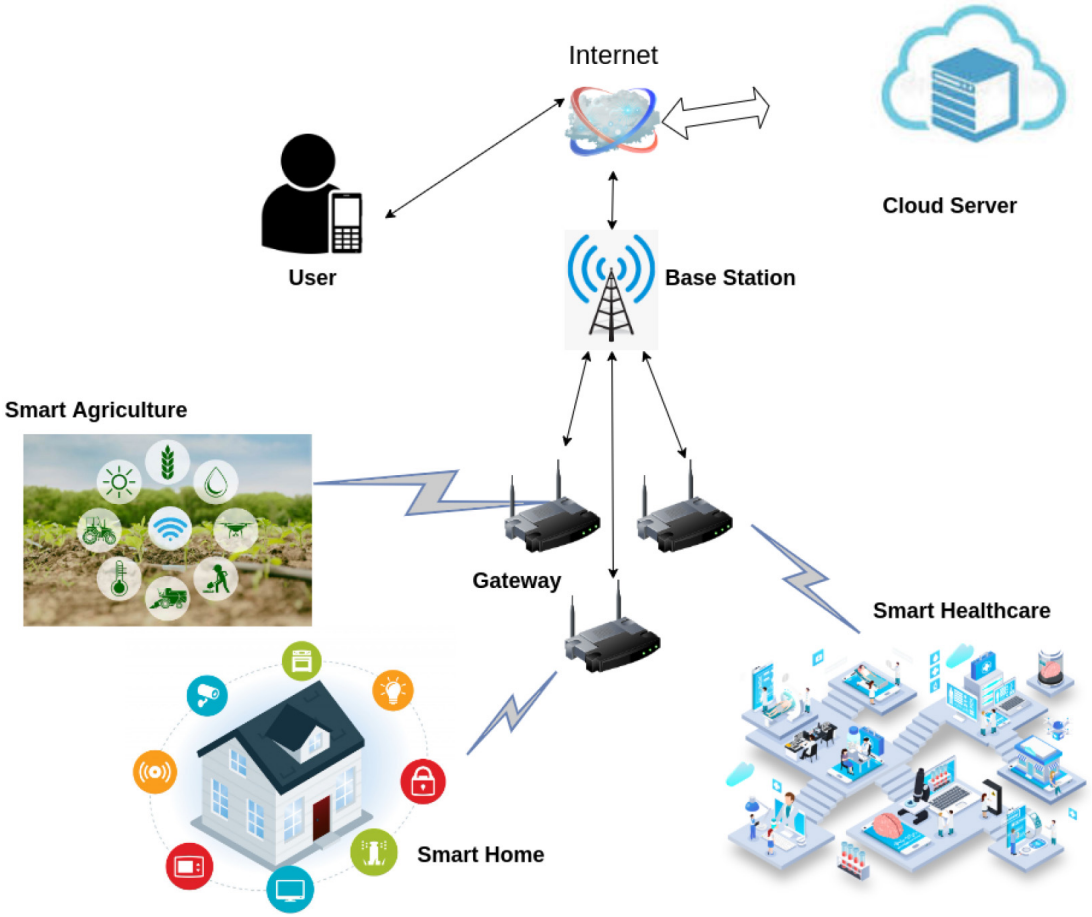

Fig. 1. IoT-based network model for proposed design.

B. Threat Model

We assume that a PPT adversary $\Im_{Ad}$, can launch both the traditional number theoretic and quantum attacks. For example, some traditional attacks include "replay attack," "man-in-the-middle attack," "unlinkability attack," "offline dictionary attack" in case of password-based schemes, and "ephemeral secret leakage (ESL) attack." Quantum attacks may include "signal leakage attack" for RLWE-key exchange protocols.

In this threat model, we adopt the following three widely recognized models as in [8].

1) *Honest-But-Curious Adversary Model:* This is considered as a passive adversarial model [26]. Under this model, the adversary $\Im_{Ad}$ may behave as an authorized entity and follow the specified protocol. $\Im_{Ad}$ can eavesdrop all the transmitted data among the corrupted entities in a network.
2) *Dolev–Yao Threat Model:* The Dolev–Yao threat model (known as DY model) [27] allows $\Im_{Ad}$ not only can eavesdrop the messages, but can also modify, insert and delete information during the communication among the involved entities.
3) *Canetti and Krawczyk's Model:* The Canetti and Krawczyk's model (CK-adversary model) [28] is currently a *de facto* threat model. Under the "CK-adversary model," $\Im_{Ad}$ can compromise the "secret credentials shared between two communicating involved entities. This may result to compromise the past or future established session keys between the communicating entities in the IoT environment by means of compromising the "session states and session keys." This model suggests that the session key construction should rely on both the "short-term (temporal) secrets" and "long-term (permanent) secrets" to avoid the ESL attack.

Due to a hostile environment, all the IoT smart devices can not be monitored in 24 × 7. Thus, some IoT smart devices may be physically compromised by $\Im_{Ad}$ and dynamic smart devices addition should be allowed in the IoT environment as in [29] and [30]. Moreover, the gateway nodes can be put under a physical locking system [31] to avoid physical capture. In addition, the cloud servers are considered as semi-trusted and also responsible for users registration.

IV. Proposed Lattice-Based Authenticated Key Agreement Scheme

In the proposed design, we describe a novel post-quantum secure reconciliation-based authenticated key agreement protocol using lattice. The proposed protocol can be divided into four phases: 1) "set-up phase;" 2) "user registration phase;" 3) "user login and authentication phase;" and 4) "user

TABLE I
SYMBOLS AND THEIR DESCRIPTIONS

Notations	Descriptions
U_i	i^{th} user
MD_i	U_i's smart (mobile) device)
S_j	j^{th} cloud server
Cha	Characteristic mapping
$\Im_{Ad}$	Probabilistic polynomial time (PPT) adversary
Mod_2	Auxiliary modular mapping
ID_{U_i}	Identity of U_i
SK	Session key shared between U_i and S_j
PW_i	U_i's chosen (sufficiently strong) password
x	Master secret key of server, S_j
α_{U_i}	Random secret generated by U_i
T_1, T_2	Current timestamps
ΔT	"Maximum transmission delay" associated with a message
q	A sufficiently large prime
R_q	Finite ring
$x \leftarrow S$	x is randomly chosen from the set S
χ_β	Discrete Gaussian for error distribution
$h(\cdot)$	Collision-resistance hash function
$\oplus$	Bitwise exclusive-OR (XOR)
$\|\|$	String concatenation

password change phase." A brief explanation behind these phases is given in the following.

1) The "setup phase" executed by a cloud server helps in fixing all the system-related parameters like public parameters and the secret key of a cloud server.
2) In the "user registration phase," a user requires to register to a cloud server for accessing the services securely.
3) The "user login and authentication phase" helps a user to login to an accessed cloud server using his/her mobile device and then to establish a session key between the login user and the accessed cloud server after a mutual authentication process.
4) For security reasons, it is a typical procedure that a registered user to be allowed to change/update his/her current password locally without contacting further the registered cloud server. This will help to reduce extra communication and computational overheads incurred during the "user password change phase."

Note that the user registration process is only one time. Hence, the registration process can be done via a secure channel (for instance, via person).

Since the proposed scheme will use of the current system timestamps in order to safeguard replay attack, all the communicating involved entities, like users and cloud servers, will be synchronized with their clocks. This is a broadly accepted assumption used in designing various existing authentication and access control mechanisms under different networking scenarios [29], [30], [32], [33], [34], [35]. The list of symbols and their descriptions are tabulated in Table I that are utilized for describing and also analyzing the proposed scheme.

A. Setup Phase

In this part of the proposed design, all the servers run the set-up algorithm. Thus, a server S_j needs to execute the following steps.

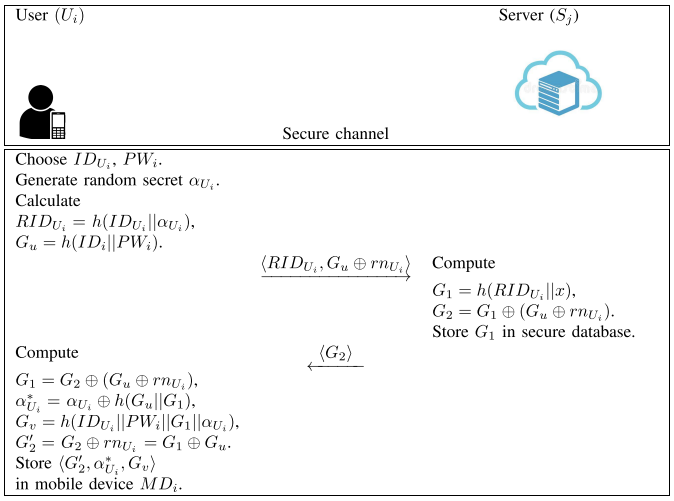

Fig. 2. Brief illustration of user registration phase.

1) The server S_j chooses $c \leftarrow R_q$ and it takes discrete Gaussian χ_β for the error distribution.
2) The server S_j chooses a positive integer of the form: $n = 2^k$ with $k > 0$ being an integer, and an odd prime q such that $q \pmod{2n} = 1$.
3) The server S_j chooses two arbitrary numbers $x, e \leftarrow \chi_\beta$, and it computes the public key as $P_i = \alpha \cdot x + 2 \cdot e$.
4) The server S_j chooses a "collision resistant one-way hash function $h : \{0,1\}^* \rightarrow \{0,1\}^l$ that gives a fixed length output of l bits."
5) The server S_j then puts the public parameters $\{n, q, c, \chi_\beta, P_i, h(\cdot)\}$ in a public directory and it keeps x as a master secret key.

B. User Registration Phase

Suppose a user U_i is willing to register under a cloud server S_j for accessing the services. The following steps are then needed.

1) U_i inputs his/her identity ID_{U_i} and a chosen password PW_i. U_i generates a random secret α_{U_i} and computes the pseudo-identity $\mathrm{RID}_{U_i} = h(\mathrm{ID}_{U_i}||\alpha_{U_i})$ and $G_u = h(\mathrm{ID}_{U_i}||\mathrm{PW}_i)$. Next, U_i sends the registration request $\langle \mathrm{RID}_{U_i}, G_u \oplus rn_{U_i} \rangle$ to the corresponding server S_j via secure channel by generating another random secret rn_{U_i}.
2) S_j computes the value $G_1 = h(\mathrm{RID}_{U_i}||x)$ using its own master secret key x and $G_2 = G_1 \oplus (G_u \oplus rn_{U_i})$. S_j then keeps G_1 in its own storage and sends the registration reply $\langle G_2 \rangle$ to the intended user U_i via secure channel.
3) Once U_i receives $\langle G_2 \rangle$, he/she computes $G_1 = G_2 \oplus (G_u \oplus rn_{U_i})$, $\alpha^*_{U_i} = \alpha_{U_i} \oplus h(G_u||G_1)$, $G_v = h(\mathrm{ID}_{U_i}||\mathrm{PW}_i||G_1||\alpha_{U_i})$ and $G'_2 = G_2 \oplus rn_{U_i} = G_1 \oplus G_u$, and stores $\langle G'_2, \alpha^*_{U_i}, G_v \rangle$ in his/her mobile device MD_i.

The overall user registration phase is briefed in Fig. 2.

C. User Login and Authentication Phase

In this part, we illustrate each of the following steps used to perform authentication between the user U_i and the accessed server S_j, respectively. The user login and authentication phase is also summarized in Fig. 3.

1) U_i provides the inputs, like the registered identity ID_{U_i} and password PW_i. The mobile device MD_i of U_i then computes the value $G_u = h(\mathrm{ID}_{U_i}||\mathrm{PW}_i)$, $G_1{}' = G_2 \oplus G_u$, $\alpha_{U_i} = \alpha^*_{U_i} \oplus h(G_u||G'_1)$, $\mathrm{RID}_{U_i} = h(\mathrm{ID}_{U_i}||\alpha_{U_i})$, and $G'_v = h(\mathrm{ID}_{U_i}||\mathrm{PW}_i||G'_1||\alpha_{U_i})$. Next, if the verification $G_v{}' = ?G_v$ holds, the user U_i is authenticated and the entered identity ID_{U_i} and password PW_i are valid; otherwise, the login phase is aborted.
2) After completing the successful login procedure, MD_i generates random samples $r_i, f_i \leftarrow \chi_\beta$, and computes the values $X_u = c \cdot r_i + 2 \cdot f_i$, and $K_u = r_i \cdot P_i$. This scheme applies the characteristic function to compute $C_u = \mathrm{Cha}(K_u)$, and it also uses the modular function to compute $M_u = \mathrm{Mod}_2(K_u, C_u)$. Next, it generates the current timestamp T_1, and finds the values $G_3 = \mathrm{RID}_{U_i} \oplus h(M_u \oplus X_u)$ and $G_w = h(G_3||X_u||M_u||\mathrm{RID}_{U_i}||T_1)$. Finally, U_i transfers the authentication request message $\langle X_u, G_w, G_3, C_u, T_1\rangle$ to the server S_j via a public channel.
3) After receiving the message $\langle X_u, G_w, G_3, C_u, T_1\rangle$ from U_i at time T_1^*, the server S_j verifies the "validity of the received timestamp T_1 by the condition: $|T_1 - T_1^*| < \Delta T$, where ΔT represents the maximum transmission delay associated with a message." If the timestamp is valid, the next phase is executed; otherwise, the phase is aborted.
4) S_j computes $K_u{}' = x \cdot X_u$, $M_u{}' = \mathrm{Mod}_2(K'_u, C_u)$, $\mathrm{RID}_{U_i} = G_3 \oplus h(M'_u \oplus X_u)$, and $G_w{}^* = h(G_3||X_u||M_u{}'||\mathrm{RID}_{U_i}||T_1)$. It verifies the correctness of the equation: $G_w{}^* = G_w$. If it verifies correctly, the user U_i is authenticated by the server S_j. The server S_j generates random samples $r_s, f_s \leftarrow \chi_\beta$, and finds the values $X_s = c \cdot r_s + 2 \cdot f_s$, $K_s = r_s \cdot X_u$, $C_s = \mathrm{Cha}(K_s)$, and $M_s = \mathrm{Mod}_2(K_s, C_s)$. Next, it generates the current timestamp T_2 and applies the stored value G_1 to compute the session key shared with the user U_i as $\mathrm{SK} = (G_1||X_u||X_s||M_u||M_s||T_1||T_2)$, and a verification factor on SK as $G_z = h(\mathrm{SK}\ ||G_1\ ||X_s\ ||M_s\ ||M_u\ ||T_2)$. Finally, the server S_j sends the authentication reply message $\langle G_z, C_s, X_s, T_2\rangle$ to the user U_i via an open channel.
5) After obtaining the message $\langle G_z, C_s, X_s, T_2\rangle$ from the server S_j at time T_2^*, MDi of the user U_i verifies the "validity of the received timestamp T_2 by the condition: $|T_2 - T_2^*| < \Delta T$." If the timestamp is invalid, the phase is aborted. Otherwise, MD_i computes $K_s{}' = r_i \cdot X_s$, $M_s{}' = \mathrm{Mod}_2(K_s{}', C_s)$, the session key shared with the server S_j as $\mathrm{SK}' = h(G_1\ ||X_u\ ||X_s\ ||M_u\ ||M'_s\ ||T_1||T_2)$ and the verification factor on SK$'$ as $G_z{}' = h(\mathrm{SK}'\ ||G_1\ ||X_s\ ||M'_s\ ||M_u||T_2)$. If the verification: $G'_z = ?G_z$ is correct, the server S_j is authenticated by the user U_i. Thus, the user U_i establishes the correct session key SK$'$ (= SK) with the server S_j because the "mutual authentication between U_i and S_j" is satisfied.

D. User Password Change Phase

To update the password of a registered user U_i locally without further contacting the respective registered server S_j, U_i proceeds with the following steps. Note that the credentials $\langle G'_2, \alpha^*_{U_i}, G_v\rangle$ are already stored in U_i's mobile device MD_i.

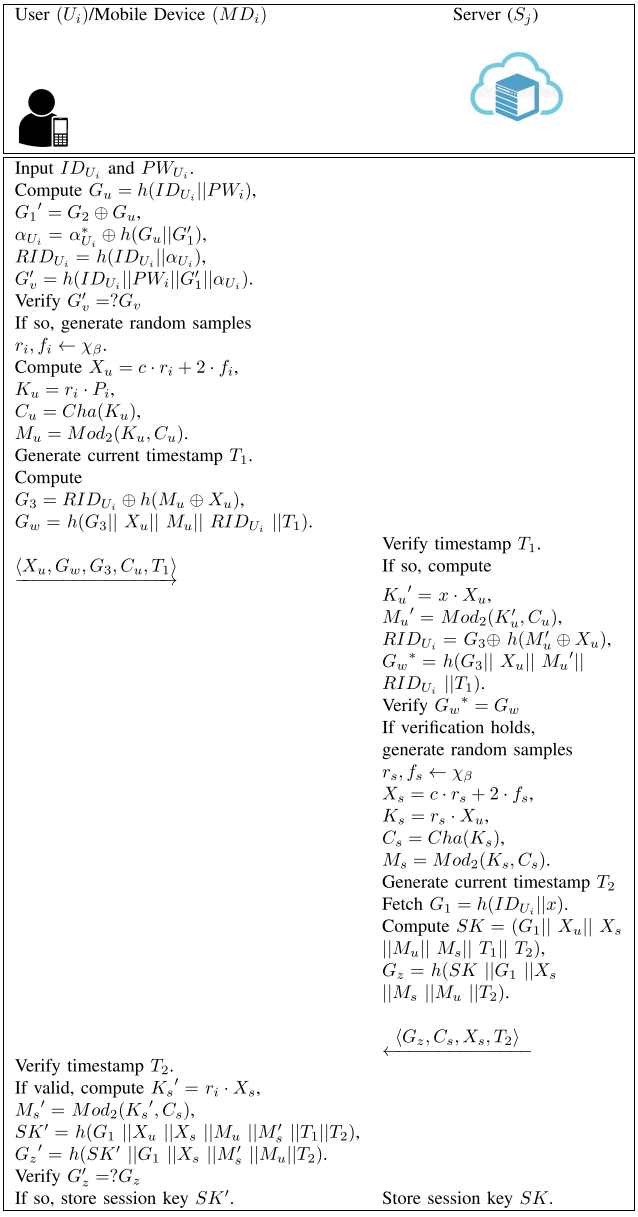

Fig. 3. Brief illustration of user login and authentication phase.

1) U_i provides the inputs, like the current registered identity ID_{U_i} and password PW_i. The mobile device MD_i of U_i computes $G_u = h(\mathrm{ID}_{U_i}\ ||\mathrm{PW}_i)$, $G_1{}' = G_2 \oplus G_u$, $\alpha_{U_i} = \alpha^*_{U_i}\ \oplus h(G_u\ ||G'_1)$, $\mathrm{RID}_{U_i} = h(\mathrm{ID}_{U_i}\ ||\alpha_{U_i})$, and $G'_v = h(\mathrm{ID}_{U_i}||\mathrm{PW}_i\ ||G'_1\ ||\alpha_{U_i})$. If the verification $G_v{}' = ?G_v$ holds, the user U_i is authenticated by MD_i and the entered identity ID_{U_i} and password PW_i are treated as valid; otherwise, this phase is aborted.
2) MD_i asks the user U_i to input new password. Assume that U_i chooses a new password PW_i^n. MD_i then calculates $G_u^n = h(\mathrm{ID}_{U_i}\ ||\mathrm{PW}_i^n)$, $\alpha^n_{U_i} = \alpha_{U_i} \oplus\ h(G_u^n||G'_1)$, $G_v^n = h(\mathrm{ID}_{U_i}\ ||\mathrm{PW}_i^n\ ||G'_1\ ||\alpha_{U_i})$ and $G_2^n = = G'_1 \oplus G_u^n$.
3) Finally, MD_i replaces the old credentials $\langle G'_2, \alpha^*_{U_i}, G_v\rangle$ with the new credentials $\langle G_2^n, \alpha^n_{U_i}, G_v^n\rangle$ in his/her mobile device MD_i.

User (U_i)	Mobile Device (MD_i)
Input present identity ID_{U_i} and password PW_i.	
	Calculate $G_u = h(ID_{U_i} \|\|PW_i)$, $G_1{}' = G_2 \oplus G_u$, $\alpha_{U_i} = \alpha^*_{U_i} \oplus h(G_u \|\|G'_1)$, $RID_{U_i} = h(ID_{U_i} \|\|\alpha_{U_i})$, $G'_v = h(ID_{U_i}\|\| PW_i \|\|G'_1 \|\|\alpha_{U_i})$. Check $G_v{}' = ?G_v$ If it holds, U_i is authenticated by MD_i. Ask U_i to input new password.
Input new password PW_i^n.	
	Compute $G_u^n = h(ID_{U_i} \|\|PW_i^n)$, $\alpha^n_{U_i} = \alpha_{U_i} \oplus h(G_u^n\|\| G'_1)$, $G_v^n = h(ID_{U_i} \|\|PW_i^n \|\|G'_1 \|\|\alpha_{U_i})$, $G_2^n = = G'_1 \oplus G_u^n$. Update $\langle G'_2, \alpha^*_{U_i}, G_v\rangle$ by computed $\langle G_2^n, \alpha^n_{U_i}, G_v^n\rangle$ in its memory.

Fig. 4. Summary of user password change phase.

The brief illustration of the user password phase is provided in Fig. 4.

V. Security Analysis

The security analysis is made in this proposed method to accomplish the important security prerequisites pertaining to this proposal through both the formal and informal security methods.

A. Mutual Authentication Correctness

Both the user U_i and the server S_j authenticate each other by performing the following calculations for verification of K_u and K_s. Note that

$$\begin{aligned} K_u &= r_i \cdot P_i \\ &= r_i \cdot (c \cdot x + 2 \cdot e) \\ &= c \cdot r_i \cdot x + 2 \cdot e \cdot r_i. \end{aligned} \tag{1}$$

Then

$$\begin{aligned} K_u{}' &= x \cdot X_u \\ &= (c \cdot r_i + 2 \cdot f_i) \cdot x \\ &= c \cdot r_i \cdot x + 2 \cdot f_i \cdot x. \end{aligned} \tag{2}$$

From (1) and (2), it follows that:

$$K_u = K_u{}' + 2(r_i \cdot e - f_i \cdot x). \tag{3}$$

By using Lemmas 1 and 2, we have

$$\begin{aligned} |r_i \cdot e - f_i \cdot x| &\le |r_i \cdot e| + |f_i \cdot x| \\ &\le \sqrt{n} \cdot ||r_i|| \cdot ||e|| + \sqrt{n} \cdot ||f_i|| \cdot ||x|| \\ &< \sqrt{n} \cdot \beta\sqrt{n} \cdot \beta\sqrt{n} + \sqrt{n} \cdot \beta\sqrt{n} \cdot \beta\sqrt{n} \\ &= 2 \cdot \beta^2 \cdot n^{\frac{3}{2}}. \end{aligned} \tag{4}$$

Lemma 2 implies $\beta = \omega\sqrt{\log n}$ and$n << q$. As a result, from (4), it follows that:

$$|r_i \cdot e - f_i \cdot x| < 2 \cdot \beta^2 . n^{\frac{3}{2}} < \frac{q}{8}. \tag{5}$$

Finally, by following Lemma 3, from (3) and (5), we obtain:

$$\begin{aligned} M_u &= \text{Mod}_2(K_u, C_u) \\ &= \text{Mod}_2\big(K_u{}', C_u\big) \\ &= M_u.{}' \end{aligned} \tag{6}$$

Similarly, it is also easy to verify that $M_s = M'_s$. This means that the message authentication is successful.

B. Formal Security Analysis

In this section, we have worked on the security of the proposed protocol. We have shown that the proposed reconciliation-based authenticated key exchange is provably secure under RLWEs assumption. In the first part, we have discussed the security model, and in the second part, we have proved the security of the proposed design under the discussed security model. Before proving Theorem 1, we consider the following.

1) The user U_i chooses a secure and random password PW_i form predefined possible dictionary. The server S_j chooses its own secret x. The next step is registration phase, the user U_i keeps the value (G'_2, G_v) in the concerned smart device.
2) Let us consider an instances η for the ith user that is denoted by Π_i^η. Again, Let us consider an instance μ for the jth server S_j that is denoted by Π_j^μ. A particular consumer denoted by C belongs to the user U_i or the server S_j, and it is denoted in compact form $C \in (U_i, LS_j)$. We have also defined that a PPT adversary $\Im_{\text{Ad}}$ can see/deviate all the communication happening between U_i and S_j.
3) If $\Im_{\text{Ad}}$ communicates with Π_i^C, $\Im_{\text{Ad}}$ executes queries to the oracle. We have also assumed that the probabilistic adversary $\Im_{\text{Ad}}$ either steals device (σ) or gets the passwords using some alternative technology (ω). In the proposed design q_h, q_e, and q_s denotes hashing query, executes query, and sends query, respectively.

All the queries submitted is a good measurement of $\Im_{\text{Ad}}$, and $\Im_{\text{Ad}}$ is used as subroutine that can simulate various kind of attacks based on the proposed security model.

1) Two instances Π_σ^η and Π_ω^μ become partner if and only if they possesses a common session key with acceptance state.
2) The adversary $\text{succ}(\Im_{\text{Ad}})$ is taken as an event, and it tries to guess a correct bit c chosen during Test oracle queries. The adversary $\text{succ}(\Im_{\text{Ad}})$ gains the advantage $\Pr(S_j)$. In our design, the adversary $\Im_{\text{Ad}}$ gains the advantage in polynomial time t which is denoted by the difference given in the following:

$$\text{ADV}_{\Im_{\text{Ad}}}(t) = \left|\Pr(\text{succ}(\Im_{\text{Ad}})) - \frac{1}{2}\right|.$$

The semantic security of the proposed design depends upon Π_i^C and Π_j^C ends on acceptance state for the adversary and it generates common session key. The advantage gain by the $\text{ADV}_{\Im_{\text{Ad}}}(t)$ is arbitrary close to negligible.

To prove Theorem 1, we discuss below the difference lemma.

Lemma 4 (Difference Lemma): Let A, B, and C be three events such that they are defined in some probability distribution. If $A \wedge \neg^C \Leftrightarrow B \wedge \neg^C$, $|\Pr[A] - \Pr[B]| \leq \Pr[C]$, where $\Pr[X]$ denotes the probability of an event X.

Theorem 1: The security of the introduced protocol relies on the "RLWE assumption," and if the advantage gain by an adversary $\mathrm{ADV}_{\Im_{\mathrm{Ad}}}^{\mathrm{RLWE}}(t)$, then a PPT adversary $\Im_{\mathrm{Ad}}$ solves the RLWE assumption bounded time t is

$$\mathrm{ADV}_{\Im_{\mathrm{Ad}}}(t) \leq \frac{{q_h}^2}{2^l} + \frac{(q_e+q_s)^2}{q} + (q_e+q_s)\mathrm{ADV}_{\Im_{\mathrm{Ad}}}^{\mathrm{RLWE}}(t).$$

Proof: We have simulated the proposed protocol with a number of games that stimulates $\Im_{\mathrm{Ad}}$. We have denoted the games by the indexing $(0 \leq i \leq 4)$. The adversary $\Im_{\mathrm{Ad}}$ wins the only if he guesses the bit c in the test query. One of the events S_j happens, and its probability is defined by $\Pr(\mathrm{succ}(\Im_{\mathrm{Ad}}))$.

1) *G_0:* If someone tries to simulate the real attack on the proposed protocol in the random oracle, then we define the advantage

$$\mathrm{ADV}_{\Im_{\mathrm{Ad}}}(t) = \left|\Pr(\mathrm{succ}(\Im_{\mathrm{Ad}_0}) - \frac{1}{2}\right|.$$

Now, we can do further simplification as follows:

$$\begin{aligned}\mathrm{ADV}_{\Im_{\mathrm{Ad}}}(t) &= \Big|\Pr\big(\mathrm{succ}(\Im_{\mathrm{Ad}_0}) - \Pr\big(\mathrm{succ}(\Im_{\mathrm{Ad}_4}) \\ &\quad + \Pr\Big(\mathrm{succ}(\Im_{\mathrm{Ad}_4}) - \frac{1}{2}\Big| \\ &= \Big|\Pr\big(\mathrm{succ}(\Im_{\mathrm{Ad}_0})\big) - \Pr\big(\mathrm{succ}(\Im_{\mathrm{Ad}_4})\big) \\ &\quad + \Pr\big(\mathrm{succ}(\Im_{\mathrm{Ad}_3})\big) - \Pr\big(\mathrm{succ}(\Im_{\mathrm{Ad}_3})\big) \\ &\quad + \Pr\big(\mathrm{succ}(\Im_{\mathrm{Ad}_4})\big) - \frac{1}{2}\Big| \qquad (7) \\ &= \Big|\sum_{i=1}^{4} P_i + \Pr\Big(\mathrm{succ}(\Im_{\mathrm{Ad}_4}) - \frac{1}{2}\Big|.\end{aligned}$$

The values P_i denote the modulus of difference of probabilities of success for $\Im_{\mathrm{Ad}_{i-1}}$ and $\Im_{\mathrm{Ad}_i}$ such that $P_i = |\Pr(\Im_{\mathrm{Ad}_{i-1}}) - \Pr(\Im_{\mathrm{Ad}_i})|$.

2) *G_1:* The adversary $\Im_{\mathrm{Ad}}$ submits hashing queries those are simulated by the hashing list H_l. The table H_l is taken empty, and it is consisted of ordered pairs $(x,\ y)$ satisfying the relation $y = h(x)$ that is output of hashing. After obtaining the queries q_h, the oracle first searches it in H_l such that $q_s \in H_l$. If it exists, then it returns the related value, and otherwise it stores $(x, y) \in H_l$ for a random string $y \in \{0, 1\}^l$. All the concerned instances go through the executes, sends, reveals, corrupts, and tests queries phases. This simulation for the concerned game can be in-distinguish form from the earlier G_0

$$P_1 = |\Pr(\Im_{\mathrm{Ad}_0}) - \Pr(\Im_{\mathrm{Ad}_1})|. \qquad (8)$$

3) *G_2:* The game G_2 possesses same simulation execution as possessed by the game G_1, but it terminates the process whenever collision occur between messages (G_z, G_w) and (G_1, G_v). The advantage in terms of probabilities of collisions during queries to the oracle is given by at most $({q_h}^2/(2^l+1))$ and $(((q_e+q_s)^2)/q)$. The ordered pair (X_u, X_s) is chosen from standard Gaussian χ_β for standard deviation β. Then, we define the term P_2 as modulus of probabilities is at most as given below. It is worth noticing that P_2 is obtained by applying the difference lemma stated in Lemma 4

$$P_2 = |\Pr(\Im_{\mathrm{Ad}_1}) - \Pr(\Im_{\mathrm{Ad}_2})| \leq \frac{{q_h}^2}{2^{l+1}} + \frac{(q_e+q_s)^2}{q}. \qquad (9)$$

4) *G_3:* Here, we have assumed that the session key SK is revealed without the simulation of hashing oracles. In the given design, the value of the session key is $\mathrm{SK} = (G_1||X_u||X_s||M_u||M_s||T_1||T_2)$, where $M_u = \mathrm{Mod}_2(r_i.P_i, \mathrm{Cha}(K_u))$ and $M_s = \mathrm{Mod}_2(r_s X_u, \mathrm{Cha}(K_s))$. It is very impossible to find the solution of the RLWE assumption. But, if the adversary $\Im_{\mathrm{Ad}}$ correctly guesses SK, then the challenger solves the RLWE assumption. If we apply the difference lemma stated in Lemma 4, it follows that:

$$\begin{aligned}P_3 &= |\Pr(\Im_{\mathrm{Ad}_2}) - \Pr(\Im_{\mathrm{Ad}_3})| \\ &\leq (q_e+q_s)\mathrm{ADV}_{\Im_{\mathrm{Ad}}}^{\mathrm{RLWE}}(t). \qquad (10)\end{aligned}$$

5) *G_4:* In this particular game, if the adversary $\Im_{\mathrm{Ad}}$ submits hashing queries to the oracle with the inputs "G_1, X_u, X_s, M_u, M_s," the "probability of guessing a bit c in tests queries in hashing is at most $({q_h}^2/(2^l+1))$." By applying the difference lemma stated in Lemma 4 and the birthday paradox, it follows that:

$$P_4 = |\Pr(\Im_{\mathrm{Ad}_3}) - \Pr(\Im_{\mathrm{Ad}_4})| \leq \frac{{q_h}^2}{2^l+1}. \qquad (11)$$

Otherwise, $\Im_{\mathrm{Ad}}$ gains no advantage during the games played. The probability of getting SK from any random string

$$\Pr|\Pr(\Im_{\mathrm{Ad}_4})| = \frac{1}{2}. \qquad (12)$$

Now, by solving (7)–(12), it follows that:

$$\mathrm{ADV}_{\Im_{\mathrm{Ad}}}(t) \leq \frac{{q_h}^2}{2^l} + \frac{(q_e+q_s)^2}{q} + (q_e+q_s)\mathrm{ADV}_{\Im_{\mathrm{Ad}}}^{\mathrm{RLWE}}(t).$$

■

C. Informal Security Analysis

In this section, we discuss about informal security of the proposed design for ring version of the LWE assumption.

Proposition 1: The proposed scheme confirms user ambiguity and unlinkability toward polynomial time adversary.

Proof: To attain ambiguity and unlinkability of the projected method, triggers $\langle G_w, G_3, X_u, C_u\rangle$ information including user's dynamic identity G_3 in place of user's identity. G_3

masks the user's identity and delink any two information which is depicted as follows.

1) The adversary tries to get RID_{U_i} from the message G_3, and $h(K_u \oplus M_u \oplus X_u)$, then he needs to compute $G_3 = \mathrm{RID}_{U_i} \oplus h(M_u \oplus X_u)$.
2) To attain the values $h(M_u \oplus X_u)$, $X_u = c.r_i + 2.f_i$, $K_u = r_i.P_i$ and $C_u = \mathrm{Cha}(K_u)$, the adversary needs to compute $h(M_u \oplus X_u) \oplus G_3$.
3) To get ID_{U_i}, the adversary $\Im_{\mathrm{Ad}}$ needs to compute the values X_u, K_u that is not possible due to ring version of LWE assumption.
4) For each of session, both user and server sample random short values r_i, f_i from the Gaussian, and the user computes the value $X_u = c.r_i + 2.f_i$.
5) To compute the values r_i', f_i' with the help of information $\langle X_u', G_w', G_3', C_u' \rangle$, $h(M_u' \oplus X_u')$, one needs to compute $G_3' = \mathrm{RID}_{U_i} \oplus h(M_u' \oplus X_u')$ that is not possible due to anonymity.
6) The adversary needs M_u for computing the value $h(M_u' \oplus X_u')$ such that r_i, and f_i are known. ■

Proposition 2: The man-in-the-middle attack is not possible in the proposed design.

Proof: Suppose an adversary $\Im_{\mathrm{Ad}}$ is capturing all the messages communicated between S_j and U_i on the public channel.

1) $\Im_{\mathrm{Ad}}$ captures the user's message $\langle X_u, G_w, G_3, C_u \rangle$ from the public channel, and tries to gain some useful information.
2) The adversary $\Im_{\mathrm{Ad}}$ changes the message $\langle X_u, G_w, G_3, C_u \rangle$ by changing C_u with C_u^*, such that $C_u^* = r_i.P_i$ or random r_i. For this attempt, the adversary $\Im_{\mathrm{Ad}}$ needs to compute $K_u^* = r_i^* P$ that is not possible without the knowledge random samples r_i, f_i. As we know the user chooses random samples, and he computes $X_u = c.r_i + 2.f_i$ such that c is only known to S_j. Therefore, the adversary cannot get login.
3) If the adversary $\Im_{\mathrm{Ad}}$ intercepts $\langle X_u, G_w, G_3, C_u \rangle$ and restores it with previously sent messages. However, this attempt fails due to random samples r_i, f_i discussed above.

If the adversary $\Im_{\mathrm{Ad}}$ intercepts responder messages $\langle G_z, C_s, X_s \rangle$, he modifies and restores it.

1) If the adversary $\Im_{\mathrm{Ad}}$ modifies $\langle G_z, C_s, X_s \rangle$, and he replaces C_s with $C_s^* = \mathrm{Cha}(K_s)$, where K_s is generated $r_s.X_u$, then he needs $G_z = h(\mathrm{SK} \,||G_1\, ||X_s\, ||M_s\, ||M_u\, ||T_2)$ such that $M_u^* = \mathrm{Mod}_2(K_s, C_s)$, where $\mathrm{SK} = (G_1||X_u||X_s||M_u||M_s||T_1||T_2)$. The adversary cannot compute the session key SK without G_1, that is hidden with some operations with RID_{U_i}.
2) If the adversary $\Im_{\mathrm{Ad}}$ replaces $\langle G_z, C_s, X_s \rangle$ with another legal messages, then he needs to validate the condition $G_z = G_z'$. ■

Proposition 3: The proposed protocol achieves forward secrecy.

Proof: If the secret x of S_j leaked by any of the means, then the adversary $\Im_{\mathrm{Ad}}$ constructs session key $\mathrm{SK} = (G_1||X_u||X_s||M_u||M_s||T_1||T_2)$.

1) If the adversary $\Im_{\mathrm{Ad}}$ achieves G_2, G_v from the devices or earlier communicated messages.
2) To find $\mathrm{SK} = (G_1||X_u||X_s||M_u||M_s||T_1||T_2)$, he needs random samples for each sessions K_s, X_s, and r_i, f_i to compute SK.
3) To obtain RID_{U_i} from G_3, $\Im_{\mathrm{Ad}}$ needs $h(M_u \oplus X_u)$ as $G_3 = \mathrm{RID}_{U_i} \oplus h(M_u \oplus X_u)$.
4) To compute $h(M_u \oplus X_u)$, $\Im_{\mathrm{Ad}}$ needs $K_u' = r_i.P$ and $C_u' = \mathrm{Cha}(K_u)$.
5) $\Im_{\mathrm{Ad}}$ computes $h(M_u \oplus X_u)$ and $\mathrm{SK} = (G_1||X_u||X_s||M_u||M_s||T_1||T_2)$ using compromised master key x of the server. As $G_1 = h(\mathrm{ID}_{U_i}||x)$, he needs ID_{U_i}. ■

Proposition 4: The proposed schemes preserve the freshness of the established session key between a user U_i and its accessed server S_j.

Proof: The session key may be compromised if the same distribution is used again and again. But, the uniqueness of random samples ensures different keys for every new session. This property can ensure the freshness of the session key. ■

Proposition 5: The proposed scheme achieves the mutual authentication between a user U_i and its accessed server S_j.

Proof: The server S_j and the user U_i authenticate each other with the help of equations: $G_w = h(G_3||X_u||M_u||\mathrm{RID}_{U_i} \,||T_1)$ and $G_z = h(\mathrm{SK} \,||G_1\, ||X_s\, ||M_s\, ||M_u\, ||T_2)$, where the value of the session key is $\mathrm{SK} = (G_1||X_u||X_s||M_u||M_s||T_1||T_2)$. The user U_i computes G_w and G_z with the long-term secrets r_i, f_i. The server S_j retrieves RID_{U_i} with the help of $\mathrm{RID}_{U_i} = G_3 \oplus h(M_u' \oplus X_u)$, such that K_u, and M_u are random numbers that need to be computed. Therefore, the server S_j and the user U_j can verify themselves. ■

Proposition 6: The replay attack is resisted in the proposed scheme.

Proof: The replay attack happens when a third party gets the authenticated messages from an earlier session and he uses these messages in a fresh session playing the role of a legal user. In the designed protocol, the user takes random r_i, r_s and the server takes random f_i, f_s, respectively. In addition, all the communicated messages, namely, authentication request message $\langle X_u, G_w, G_3, C_u, T_1 \rangle$ and authentication reply message $\langle G_z, C_s, X_s, T_2 \rangle$, involve the current timestamps T_1 and T_2, respectively. The validation of the attached timestamps in the messages by the respective receiver will ensure whether a message is old and replayed one. This avoids the reply attack during verification. ■

Proposition 7: The impersonation attack is resisted in the proposed scheme.

Proof: In the proposed design, the adversary $\Im_{\mathrm{Ad}}$ is not capable of generating legal messages G_w and G_z. This is because of anonymity of the proposed protocol and the secret number K_u that contains a random number r_i. It helps to avoid the impersonation attack on messages traveling through a public channel. ■

Proposition 8: The proposed scheme is secure against offline password dictionary attack.

Proof: If an adversary gets the stored information $\langle G_2', \alpha_{U_i}^*, G_v \rangle$ inside the mobile device MD_i of a registered

TABLE II
COMMUNICATION AND STORAGE COMPARISON WITH CLASSICAL APPROACH

Item	Primitive	Length	Bit-size
Diffie-Hellman Storage	$g \in Z_\tau^*$	$\|\tau\|$	$\lambda' = \log \tau$
Diffie-Hellman Communication	$g^r, \tau(g^{rx_a}) \in Z_\tau^*$	$\|\tau\|$	$\lambda' = \log \tau$
Lattice based Storage	$E \in Z_\tau^{m \times n}$	$(m^2 + m).\tau$	$4\lambda \log^2 \lambda$ $(2\lambda \log \lambda + 1)$
Lattice based Communication	$z_j, \omega_j, \upsilon_j$	$3m\tau$	$12\lambda \log^2 \lambda$

user U_i, then he requires to compute the value G_u to guess the password PW_i. If the adversary does not know the identity ID_{U_i}, then it becomes impossible to verify U_i's identity. Therefore, it is not feasible to apply offline dictionary attack. ■

Proposition 9: The proposed scheme is secure against privileged-insider attack through stolen mobile device attack.

Proof: Suppose the adversary $\Im_{\text{Ad}}$ has attained the stolen mobile device MD_i of a legal registered user U_i. Additionally, assume that during the user registration phase, the adversary $\Im_{\text{Ad}}$ has the information $\langle \text{RID}_{U_i}, G_u \oplus rn_{U_i} \rangle$, where $\text{RID}_{U_i} = h(\text{ID}_{U_i} || \alpha_{U_i})$ and $G_u = h(\text{ID}_{U_i} || \text{PW}_i)$. Thus, using the extracted credentials $\langle G_2', \alpha_{U_i}^*, G_v \rangle$ stored in the mobile device MD_i, the adversary $\Im_{\text{Ad}}$ may try to guess a password. However, the guessed password verification can not be successful using G_u, G_2', and G_v because the secrets rn_{U_i}, α_{U_i}, ID_{U_i}, and $G_1 = h(\text{RID}_{U_i} || x)$ are unknown to the adversary $\Im_{\text{Ad}}$. This clearly shows that the privileged-insider attack through the stolen mobile device attack is not possible in the proposed design. ■

Proposition 10: The proposed scheme is secure against ESL attack.

Proof: In the proposed design, after mutual authentication, a user U_i establishes the session key shared with its accessed server S_j as $\text{SK}' = h(G_1 || X_u || X_s || M_u || M_s' || T_1 || T_2)$, and the server S_j establishes the same session key shared with U_i as $\text{SK} = (G_1 || X_u || X_s || M_u || M_s || T_1 || T_2)$. It is noted that the session key SK' (= SK) relies on two types of secrets: 1) short-term (temporal) secrets K_u and K_s and 2) long-term secret G_1 containing the master secret key x of the server S_j and RID_{U_i} of U_i. Now, with having both types of secrets, it is not possible to derive the session key by the adversary $\Im_{\text{Ad}}$. Moreover, due to chosen random samples, the session keys established in each session between U_i and S_j are distinct and unique. Therefore, according to the CK-adversary model described in the threat model (see Section III-B), the ESL attack is resisted in the proposed design. ■

VI. PERFORMANCE COMPARISON

This section describes two essential attributes: 1) computation and 2) communication costs of the corresponding proposed scheme and analysis on the performance with other related schemes. The existing scheme of Zhang et al. [11] performed a crucial role in selecting substitute of parameters in a lattice generated by an ideal. The descriptions of the proposed scheme's parameters taken into account are $n = 1024$ bits, Gaussian distribution $\log(\delta) = 17.01$, where q is an "odd prime" and δ is the "standard deviation."

The DH-based protocols take $|\tau| = \log(\tau)$ bits as in Table II that vary with the length of the parameter in binary representation, i.e., $\tau \approx 2^\lambda$, where λ is the security parameter to analyse the storage comparison between classical and post-quantum environment.

Various cryptographic operations have been described as follows. The notation t_δ stands for average cost used to sample from Gaussian χ_δ, t_{sm} is for average cost of single multiplication with scalar in Q_q, t_{om} is for average cost of single multiplication in Q_q, t_{am} is for cost of one multiplication and addition in Q_q, t_{ch} denotes cost for characteristics function, t_{h1} and t_{h2} denote the costs of the functions H_1 and H_2, respectively, used by Dabra et al. [36]. We have, $t_{h1} \approx 0.258 t_{am}$, $t_{h2} \approx 3.25 t_{am}$ [36] for server side and $t_{h1} \approx 0.185 t_{am}$, $t_{h2} \approx 4.3209 t_{am}$ [36] for user side. t_{mod} denotes mod function cost, where $t_{\text{mod}} \approx 3.30414 t_{am}$ [36] for user and $t_{\text{mod}} \approx 1.524 t_{am}$ [36] for sever. t_{ha} is the cost for hashing. The costs of each operation on server side are $t_{om} \approx 0.000307$, $t_{am} \approx 0.002549$, $t_\delta \approx 0.073503$, $t_{sm} \approx 0.000298$, $t_{ch} \approx 0.000689$, $t_{ha} \approx 0.01409$, $t_{h1} \approx 0.000657$, $t_{h2} \approx 0.00827$, and $t_{\text{mod}} \approx 0.003882$ microsecond (μs)., respectively. Each of the operations on the user side costs $t_{am} \approx 0.029505$, $t_{ch} \approx 0.035515$, $t_\delta \approx 0.561483$, $t_{sm} \approx 0.006655$, $t_{ha} \approx 0.180964$, $t_{h1} \approx 0.0054644$, $t_{h2} \approx 0.1274900$, $t_{om} \approx 0.0013052$, and $t_{\text{mod}} \approx 0.09749$ μs, respectively, [20], [23], [36].

The cost of each operation follows: 1) Lattice-crypto library and 2) Miracle libraries [github.com/miracl/MIRACL]. The implementation of related operations are performed on (server side) Dell PC, Windows-10, [c and c++] languages, operating-system with [3.4 GHz], 8-GB RAM, Intel's i-7, whereas on user end is on Samsung mobile 1.4 GHz, operating-systems 4.3, 1-GB RAM, processors Exnoys-4412, respectively [11], [20].

In the proposed protocol, user side executes five hashing, two sampling from the Gaussian distribution, two multiplication in Q_q, one addition and multiplication in Q_q, one scalar multiplication, one characteristic function, one characteristic function, two modulo functions, that is, in a total of $5t_{ha} + 2t_\delta + 2t_{om} + t_{am} + t_{sm} + t_{ch} + 2t_{\text{mod}}$. So, the execution cost for user side becomes 2.2970514 μs. Server side executes five hashing, two sampling from the Gaussian distribution, two multiplication in Q_q, one addition and multiplication, one scaler multiplication, two modulo functions, and one characteristic function, that is, a total of $5t_{ha} + 2t_\delta + 2t_{om} + t_{am} + t_{sm} + 2t_{\text{mod}} + t_{ch}$. Thus, the total cost for server side is 0.22937 μs. Therefore, the total execution time for the proposed protocol is 2.5264214 μs.

We now compare the computation costs (see Table III) of the proposed scheme with different classical protocols, such as Dabra et al. [36], Rana et al. [23], and Feng et al. [20] that are based on RLWE. In the protocol of Rana et al. a user needs execution time $7t_{ha} + 2t_\delta + 2t_{om} + t_{am} + t_{sm} + t_{ch} + t_{\text{mod}} \approx 2.5614894$ μs, where server needs $5t_{ha} + 2t_\delta + 2t_{om} + t_{am} + t_{sm} + t_{ch} + 2t_{\text{mod}} \approx 0.229367$ μs. In the scheme of Feng et al., a user needs $6t_{ha} + 2t_\delta + 2t_{om} + t_{am} +$

TABLE III
COMPARISON BETWEEN COMPUTATION AND COMMUNICATION COST

Scheme	User-side computation cost	server-side computation cost	Total computation cost (in microseconds)	Communication cost (in bits)
Rana *et al.*	$7t_{ha} + 2t_{\delta} + 2t_{om} + t_{am} + t_{sm} + t_{ch} + t_{mod}$	$5t_{ha} + 2t_{\delta} + 2t_{om} + t_{am} + t_{sm} + t_{ch} + 2t_{mod}$	2.7908594	9724
Feng *et al.*	$6t_{ha} + 2t_{\delta} + 2t_{om} + t_{am} + t_{sm} + t_{ch} + 2t_{mod}$	$5t_{ha} + 2t_{\delta} + 2t_{om} + t_{am} + t_{sm} + t_{ch} + 2t_{mod}$	2.7073854	9724
Dabra *et al.*	$5t_{ha} + 3t_{\delta} + t_{om} + 3t_{am} + 2t_{sm} + t_{ch} + 2t_{mod} + t_{h1} + 2t_{h2}$	$5t_{ha} + 3t_{\delta} + t_{om} + 3t_{am} + 2t_{sm} + t_{ch} + 2t_{mod} + t_{h1} + 2t_{h2}$	3.5084976	9726
Proposed	$5t_{ha} + 2t_{\delta} + 2t_{om} + t_{am} + t_{sm} + t_{ch} + 2t_{mod}$	$5t_{ha} + 2t_{\delta} + 2t_{om} + t_{am} + t_{sm} + t_{ch} + 2t_{mod}$	2.5264214	9790

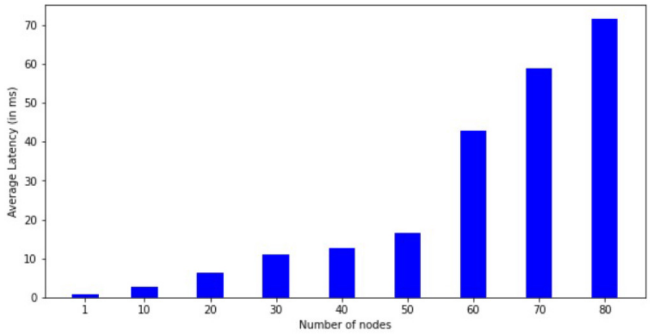

Fig. 5. Analysis on latency.

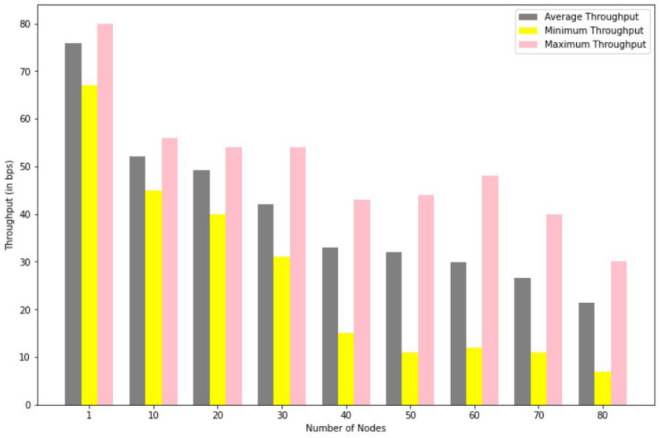

Fig. 6. Analysis on throughput.

$t_{sm} + t_{ch} + 2t_{\text{mod}} \approx 2.4780154$ μs execution time, whereas the server needs $5t_{ha} + 2t_{\delta} + 2t_{om} + t_{am} + t_{sm} + t_{ch} + 2t_{\text{mod}} \approx 0.22937$ μs computation cost. In the scheme of Dabra et al. [36] user spends $5t_{ha} + 3t_{\delta} + t_{om} + 3t_{am} + 2t_{sm} + t_{ch} + 2t_{\text{mod}} + t_{h1} + 2t_{h2} \approx 3.1833386$ μs where server spends $5t_{ha} + 3t_{\delta} + t_{om} + 3t_{am} + 2t_{sm} + t_{ch} + 2t_{\text{mod}} + t_{h1} + 2t_{h2} \approx 0.325159$ μs in computation.

To demonstrate the communication costs (see Table III) of different relevant protocols, a binary string of password, random secret, and identity are taken each of 64 bits, where the timestamp is taken as 32 bits. For hashing we use SHA-512 with the hash output of 512 bits, 256-bit symmetric key is considered for symmetric encryption/decryption (for example, Advanced Encryption Standard (AES-256) [37]), 256-bits chaotic map and an element from Q_q is taken as 4094 bits. One can notice that the communication costs of Rana et al., Feng et al., and Dabra et al. are 9724, 9724, and 9726 bits, respectively. Due to the larger key size, the proposed scheme requires a slightly higher cost of 9790 bits. This is because we are using the RLWE. However, one can justify communication overhead by considering the security against quantum computer attacks as none of existing schemes is secured against those attacks.

TABLE IV
SIMULATION PARAMETERS

Parameters	Description
Simulator	NS-3 3.35
Platform	Ubuntu 20.04.3 LTS
Simulation Area	$100m \times 100m$
Simulation Time	300 seconds
Wireless Protocol	IEEE 802.11p
Users	$1 - 60$

VII. SIMULATION STUDY

In this section, we use the widely used "Network Simulator (NS-3)" simulator to test the proposed system during the execution of the login and authentication phase in order to compute various network performance parameters. NS-3 is "a discrete-event network simulator for Internet system" [38].

A. Simulation Environment

The experiment was carried out by altering the number of nodes starting with one and testing up to 60 user nodes. The nodes have been spread across a 100×100 m^2 region. Table IV depicts the simulation environment and parameters configuration.

B. Simulation Results

1) Analysis on Latency: Latency is refers to the time a data packet takes to travel from its origin to destination. Fig. 5 illustrates the average latency of the proposed scheme. The analysis shows that the value of average latency grows with the number of nodes, because the proposed protocol requires more messages to convey and receive with more nodes.

2) Analysis on Throughput: Throughput is measured as the amount of information efficiently transferred to a certain destination during a particular time period. It determines the quantities of information successfully received by the sink node. Fig. 6 illustrates the average throughput, minimum throughput, and maximum throughput for the proposed

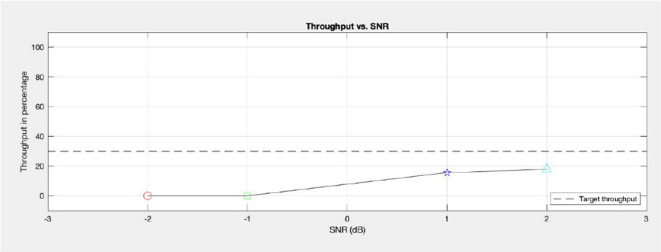

Fig. 7. Throughput versus SNR.

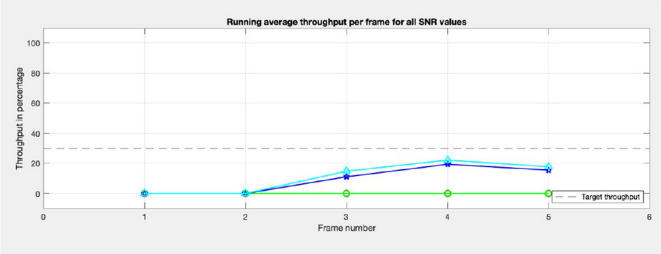

Fig. 8. Running average throughput per frame for all SNR values.

scheme. The analysis shows that when the number of nodes increases, the value of throughput also decreases.

3) Analysis on Signal-to-Noise Ratio: Fig. 7 shows the throughput *versus* signal-to-noise ratio (SNR) for the proposed scheme. Fig. 8 also shows the running average throughput per frame for all SNR values for the proposed scheme. It can be seen that the throughput increases with the increase in SNR, because whenever SNR increases, the transmission power at the origin and relays increases, resulting in an increase in average throughput.

VIII. Conclusion

We proposed a new lattice-based authenticated key exchange protocol using a ring-based version of LWEs assumption for IoT-enabled smart devices. This protocol is basically a reconciliation-based key exchange that uses the reconciliation-based key exchange mechanism. The proposed protocol is robust against various attacks that is shown through the formal and informal security evaluation. The proposed is efficient in computation as compared to the competing existing approaches. Moreover, the proposed scheme is also comparable in communication cost with the competing existing approaches. Finally, the proposed scheme is simulated using the NS-3 simulator to demonstrate the impact on various network parameters.

Acknowledgment

The authors thank the anonymous reviewers and the Associate Editor for providing constructive and generous feedback.

References

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

[2] 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.

[3] M. Ajtai, "Generating hard instances of lattice problems," in *Proc. ACM 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 99–108.

[4] A. K. Das, "A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks," *Int. J. Inf. Security*, vol. 11, no. 3, pp. 189–211, 2012.

[5] A. K. Das and B. Bruhadeshwar, "An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system," *J. Med. Syst.*, vol. 37, no. 5, pp. 1–17, 2013.

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

[7] S. Chatterjee and A. K. Das, "An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks," *Security Commun. Netw.*, vol. 8, no. 9, pp. 1752–1771, 2015.

[8] A. K. Das, S. Roy, E. Bandara, and S. Shetty, "Securing age of information (AoI)-enabled 5G smart warehouse using access control scheme," *IEEE Internet Things J.*, early access, Sep. 8, 2022, doi: 10.1109/JIOT.2022.3205245.

[9] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges," *IEEE Access*, vol. 8, pp. 3343–3363, 2020.

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

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

[12] H. Krawczyk, "HMQV: A high-performance secure Diffie–Hellman protocol," in *Proc. Adv. Cryptol. CRYPTO*, 2005, pp. 546–566.

[13] A. C.-C. Yao and Y. Zhao, "OAKE: A new family of implicitly authenticated Diffie–Hellman protocols," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, Berlin, Germany, 2013, pp. 1113–1128.

[14] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange—A new hope," in *Proc. 25th USENIX Security Symp. (USENIX Security)*, 2016, pp. 327–343.

[15] J. Ding, P. Branco, and K. Schmitt, "Key exchange and authenticated key exchange with reusable keys based on RLWE assumption," Cryptol. ePrint Archive, Rep. 2019/665, 2019.

[16] J. Ding, S. Alsayigh, J. Lancrenon, R. Saraswathy, and M. Snook, "Provably secure password authenticated key exchange based on RLWE for the post-quantum world," in *Proc. Cryptograph. Track RSA Conf.*, 2017, pp. 183–204.

[17] S. Fluhrer, "Cryptanalysis of ring-LWE based key exchange with key share reuse," Cryptol. ePrint Archive, Rep. 2016/085, 2016.

[18] J. Ding, S. Alsayigh, R. Saraswathy, S. Fluhrer, and X. Lin, "Leakage of signal function with reused keys in RLWE key exchange," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2017, pp. 1–6.

[19] J. Ding, S. Fluhrer, and S. Rv, "Complete attack on RLWE key exchange with reused keys, without signal leakage," in *Proc. Aust. Conf. Inf. Security Privacy*, 2018, pp. 467–486.

[20] 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. 2018.

[21] S. H. Islam, "Provably secure two-party authenticated key agreement protocol for post-quantum environments," *J. Inf. Security Appl.*, vol. 52, Jun. 2020, Art. no. 102468.

[22] D. Dharminder and K. P. Chandran, "LWESM: learning with error based secure communication in mobile devices using fuzzy extractor," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 10, pp. 4089–4100, 2020.

[23] S. Rana and D. Mishra, "Lattice-based key agreement protocol under ring-LWE problem for IoT-enabled smart devices," *Sādhanā*, vol. 46, no. 2, pp. 1–11, 2021.

[24] D. Micciancio and P. Mol, "Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions," in *Proc. Annu. Cryptol. Conf.*, 2011, pp. 465–484.

[25] D. Micciancio, "Generalized compact knapsacks, cyclic lattices, and efficient one-way functions," *Comput. Complexity*, vol. 16, no. 4, pp. 365–411, 2007.

[26] B. Narwal and A. K. Mohapatra, "A survey on security and authentication in wireless body area networks," *J. Syst. Archit.*, vol. 113, Feb. 2021, Art. no. 101883.
[27] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
[28] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, Amsterdam, The Netherlands, 2002, pp. 337–351.
[29] S. Challa et al., "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Elect. Eng.*, vol. 69, pp. 534–554, Jul. 2018.
[30] S. Mandal, B. Bera, A. K. Sutrala, A. K. Das, K.-K. R. Choo, and Y. Park, "Certificateless-signcryption-based three-factor user access control scheme for IoT environment," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3184–3197, Apr. 2020.
[31] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Trans. Depend. Secure Comput.*, vol. 17, no. 2, pp. 391–406, Mar./Apr. 2020.
[32] L. Wu, J. Wang, K. R. Choo, and D. He, "Secure key agreement and key protection for mobile device user authentication," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 319–330, Feb. 2019.
[33] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based Industrial Internet of Things deployment," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4900–4913, Dec. 2018.
[34] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of Drones environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, Jul. 2019.
[35] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of Drones deployment," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3572–3584, Apr. 2019.
[36] 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.
[37] "Advanced encryption standard (AES)," Nat. Inst. Stand. Technol., U.S. Dept. Commerce, Washingdon, DC, USA, Rep. FIPS PUB 197, Nov. 2001. Accessed: Jun. 2022. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[38] "ns-3 Network Simulator." 2022. Accessed: Jun. 2022. [Online]. Available: https://www.nsnam.org/

Dharminder Dharminder received the M.Sc. degree in mathematics and the M.Tech. degree in computer science and data processing from the Indian Institute of Technology Kharagpur, Kharagpur, India, in 2012 and 2015, respectively.

He is currently working as an Assistant Professor with the Department of Computer Science and Engineering, Amrita Vishwa Vidyapeetham, Chennai, India. His research interests are number theory, cryptography, post-quantum cryptography, and IoT security.

Challa Bhageeratha Reddy is currently pursuing the B.Tech. degree in cyber security with the Department of Computer Science and Engineering, Amrita Vishwa Vidyapeetham, Chennai, India.

His research interests are cryptography, post-quantum cryptography, and IoT security.

Ashok Kumar Das (Senior Member, IEEE) received the M.Sc. degree in mathematics, the M.Tech. degree in computer science and data processing, and the Ph.D. degree in computer science and engineering from the Indian Institute of Technology Kharagpur (IIT Kharagpur), Kharagpur, India, in 1998, 2000, and 2008, respectively.

He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology Hyderabad, Hyderabad, India. He also worked as a Visiting Faculty with the Virginia Modeling, Analysis, and Simulation Center, Old Dominion University, Suffolk, VA, USA. His Google Scholar H-index is 70 and i10-index is 202 with over 13 900 citations. His current research interests include cryptography, system, and network security, including security in smart grid, Internet of Things, Internet of Drones, Internet of Vehicles, cyber–physical systems and cloud computing, blockchain, and AI/ML security. He has authored over 320 papers in international journals and conferences in the above areas, including over 275 reputed journal papers.

Dr. Das was a recipient of the Institute Silver Medal from IIT Kharagpur. He was/is on the editorial board of IEEE SYSTEMS JOURNAL, *Journal of Network and Computer Applications* (Elsevier), *Computer Communications* (Elsevier), *Journal of Cloud Computing* (Springer), *Cyber Security and Applications* (Elsevier), *IET Communications*, *KSII Transactions on Internet and Information Systems*, and *International Journal of Internet Technology and Secured Transactions* (Inderscience). He also severed as one of the Technical Program Committee Chairs of the first International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, June 2019, International Conference on Applied Soft Computing and Communication Networks (ACN'20), October 2020, Chennai, India, and second International Congress on Blockchain and Applications (BLOCKCHAIN'20), L'Aquila, Italy, October 2020.

Youngho Park (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, South Korea, in 1989, 1991, and 1995, respectively.

He is currently a Professor with the School of Electronics Engineering, Kyungpook National University. From 1996 to 2008, he was a Professor with the School of Electronics and Electrical Engineering, Sangju National University, Sangju, South Korea. From 2003 to 2004, he was a Visiting Scholar with the School of Electrical Engineering and Computer Science, Oregon State University, Corvallis, OR, USA. His research interests include computer networks, multimedia, and information security.

Sajjad Shaukat Jamal received the Ph.D. degree in mathematics from Quaid-i-Azam University, Islamabad, Pakistan, in 2017.

He is currently working as an Assistant Professor with the Department of Mathematics, King Khalid University, Abha, Saudi Arabia. His research interests include number theory, cryptography, digital watermarking, steganography, information security, multimedia security, and blockchain technology. He has several journal papers in his research areas.