Sādhanā (2021) 46:84
https://doi.org/10.1007/s12046-021-01607-2

Lattice-based key agreement protocol under ring-LWE problem for IoT-enabled smart devices

SAURABH RANA[1,*] and DHEERENDRA MISHRA[2]

[1]Department of Mathematics, Chandigarh University, Mohali 140413, India
[2]Department of Mathematics, Maulana Azad National Institute of Technology, Bhopal 462003, India
e-mail: saurabhranapsm@gmail.com

MS received 11 February 2020; revised 11 January 2021; accepted 12 March 2021

Abstract. Advances in communication technologies along with the availability of Internet and Internet of Things (IoT) devices enable users to acquire various services over the Internet. However, IoT devices are prone to attacks on the open communication channel. Many authenticated key agreement schemes have been introduced in the last decades to improve security, where most of the schemes are based on the classical number-theoretic assumptions. Unfortunately, Shor's algorithm provides the mechanism to solve the existing number-theory-based problems such as discrete logarithm, integer factorization, etc. As a result, the hard problems based on number theory could be solved very efficiently on a quantum computer using Shor's algorithm. Therefore, the design of a protocol is required that can resist all known attacks by quantum computers. To address the security issues raised by Shor's algorithm, we propose a lattice-based key agreement protocol under ring learning with errors (RLWE). Security analysis of the proposed protocol is also presented, where both informal security and formal security analyses are followed. The analysis of security clearly indicates that the proposed scheme is provably secure under a random oracle model. In addition we study the performance of the proposed scheme, which shows the enhancement in terms of performance.

Keywords. Lattice based cryptography; ring learning with errors; IoT; authentication; security.

1. Introduction

The Internet of Things (IoT) enables smart devices to revolutionize the multimedia content distribution system. Multimedia content can be easily transferred through IoT objects without any content quality degradation and human intervention. However, all the communication between IoT devices is performed in the open public network.

Nowadays precursive growth in a wireless communication network has been observed in smart living standard, which invokes the use of low-cost IoT devices. Each smart device user has a concern about his privacy and security during the access of data on online platforms. The privacy of smart device users in a wireless network depends on the support of user's anonymity, authentication, and confidentiality. In wireless communication, user anonymity plays a significant role if the device is hacked and hackers retrieve stored credentials.

Of late, IoT-based devices are playing a ubiquitous role in developing communication technologies for common users. As communication among the users or devices takes place over the public channel, the security and privacy are emerging as major issues. An authentication protocol for IoT devices is provided to secure communication between devices and servers, which is currently the most popular cryptographic system.

In recent years several cryptographic protocols have been developed to obtain privacy-preserving communication among smart device users in the network system, where most of the authentication and session key agreement architectures are basis of number-theory-based hard problems [1–4]. These schemes face serious security threats due to Shor's algorithm. To get rid of these security challenges in authentication and session key agreement protocols for smart devices, the design of lattice-based cryptosystems is required as lattice-based cryptosystems are potential candidates to resist existing quantum attacks. It was initially introduced in the 18th century by mathematicians such as Lagrange, Gauss, and later Minkowski. In 1996, Ajtai [5] presented the breakthrough in this field by discovering the tool to construct new cryptographic primitives.

In an era of quantum cryptography, it is pertinent to understand the complexity of lattice problems and their relation to cryptography. Lattice structures are applied for post-quantum cryptography with great simplicity and efficiency. There security is based on a worst-case hard problem. The other existing cryptographic hard problems are based on some average-case assumptions such as

*For correspondence
Published online: 22 April 2021

integer factorization problem (IFP) and discrete logarithm problem (DLP). Authentication protocols developed for IoT devices are mostly based on number-theoretic hard problems. However the coming quantum era will bring new attacks on them, which will be a serious threat to these existing methodologies. The Shor algorithm [6, 7] proves that any probabilistic polynomial time (PPT) adversary can break the classical mathematical assumption. Therefore the new dimension in cryptography has been developing as post-quantum cryptography, which can resist quantum computer attacks.

In 2016, NIST established a program whose aim was to develop and evaluate new cryptographic primitives for resisting quantum attacks. There are several existing techniques to handle these issues. However, all these methods are not valid if the quantum computer comes into the picture. Ideal lattices are a special class of lattices, which are suitable and most sought after technique for constructing efficient cryptographic primitives with some additional algebraic structure for quantum computer attack resistance. The lattice-based cryptographic hard assumptions are capable of resisting the quantum attacks efficiently. The ideal-lattice-based cryptographic systems obtain low computational costs as compared with classical cryptographic systems. Lyubashevsky *et al* [8] introduced an ideal lattice and ring learning with errors (RLWE) for the first time. Zhang *et al* [9] introduce an authenticated key exchange protocol for the ideal lattice, which is conceptually simple and has similarities to the Diffie–Hellman-based protocols such as HMQV (CRYPTO 2005) and OAKE (CCS 2013). Alkim *et al* [10] give an initial idea of post-quantum key exchange protocol. Later, Ding *et al* [11] introduce the key exchange and authentication protocol using RLWE problem. RLWE-based key exchange has high security with minimum key size against post-quantum attacks. Ding *et al* [12] proposed a high-entropy and key exchange protocol on RLWE over a public channel for the quantum world. Feng *et al* [13] introduced an anonymous key exchange protocol for mobile devices. They also give security proof of their scheme in the random oracle model and compare to other ones. Islam [14] designs an authentication scheme for post-quantum environment using lattice hard problem. Recently, Dharminder and Chandran [15] proposed the lattice-based authentication scheme using RLWE problem for mobile devices.

1.1 *Our contribution*

It is clear from the literature that it is necessary to understand future threats if a quantum computer comes into the picture. In quantum computer era, most of the existing security protocols will not be able to resist quantum attack as number-theory-based hard problems can be efficiently solved on quantum computer using Shor's algorithm. From the last few years, many researchers contributed in a different aspect to restrict quantum attack.

To overcome this issue, we propose a lattice-based key agreement protocol under RLWE problem for IoT devices. The main aim of RLWE problem is to separate noisy ring multiplications from uniform distributions, such as distinguishing $(c, c \cdot x + e)$, where c, x, and e are uniformly randomized from the ring and $'\cdot'$ is a multiplication operation on the ring. The proposed scheme has following merits:

- The proposed scheme provides the ideal-lattice-based key agreement protocol under the RLWE problem for IoT devices.
- The proposed system is provably secure under the RLWE hard assumption.
- Security analysis shows that it is secure against known security threats.
- The comparative study of performance shows that it is efficient in term of computation and communication overhead.

In Section 2, we discuss some basic information about lattice-based RLWE problem and state the assumptions. In Section 3, we state the phases of our proposed authentication scheme. The next section demonstrates the security analysis of the proposed scheme. In Section 4.1, we present a security analysis of the proposed scheme under RLWE hard problem and successfully shows that no polynomial-time adversary can solve this problem. In Section 5, we do a performance analysis of the proposed scheme. Section 6 concludes the paper.

2. Preliminaries

In this section, we briefly review current lattice-based techniques as described in [16]. Lattice provides resistance against the quantum and post-quantum attack in modern cryptography. These assembly languages enable good mathematical security proofs. Security of lattice depends on the hard problems in n-dimensional Euclidean space R^n. In addition, we will discuss lattice-based cryptosystems worst-case hard assumptions of security [17].

2.1 *Basics of RLWE*

In this phase, we discuss background of RLWE with some basic assumptions and system architecture (figure 1). For the security concern of proposed scheme, we describe some mathematical hard problems.

Let q be an odd prime number; $q > 2$. $\mathbb{R}$ and $\mathbb{Z}$ denote the set of real numbers and integers, respectively. $\mathbb{Z}[x]$ and $\mathbb{Z}_q[x]$ denote a ring of polynomial over $\mathbb{Z}$ and $\mathbb{Z}_q$,

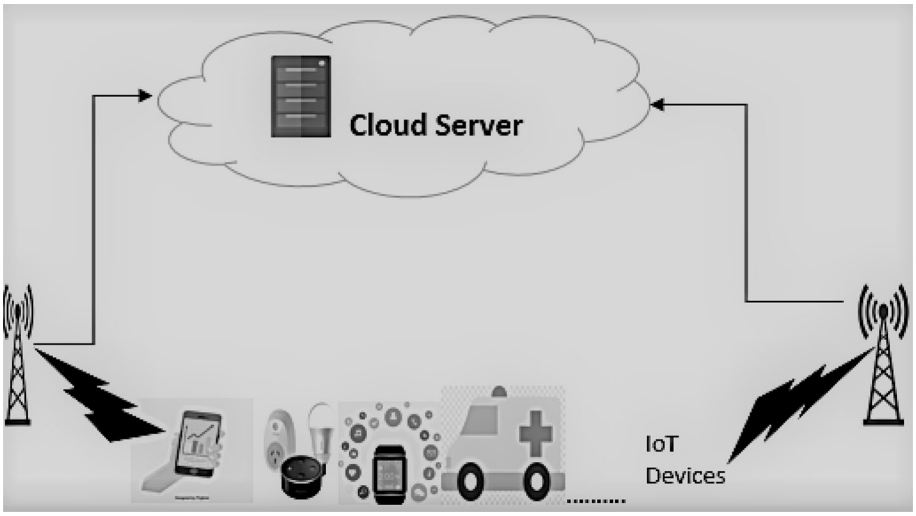

Figure 1. A typical architecture of IoT-enabled environment.

separately. We consider a polynomial ring $R = \frac{\mathbb{Z}[x]}{x^n+1}$ and $R_q = \frac{\mathbb{Z}_q[x]}{x^n+1}$. Any element of polynomial ring $c = c_0 + c_1x + c_2x^2 + c_3x^2 + \cdots\cdots\cdots + c_{n-1}x^{n-1} \in R$. The Euclidean norm is defined as $||c|| = \sqrt{c_0{}^2 + c_1{}^2 + c_2{}^2 + \cdots + c_{n-1}{}^2}$ and L_∞ norm is defined as $||c_\infty|| = max\{c_0, c_1, c_2, c_3, \ldots, c_{n-1}\}$. Let β be a given positive real number and gaussian discrete distribution be denoted by χ_β over R_q.

Lemma 1 *If c, d are any two elements of ring polynomial R, the following inequalities hold:*

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

Lemma 2 *For any positive real number β, where $\beta = \omega\sqrt{log(n)}$, the following inequality holds: $Pr_{c \leftarrow \chi_\beta}[||c|| > \beta\sqrt{n}] \leq 2^{-n+1}$.*

Let the middle set of $\mathbb{Z}_q = \{-\frac{q-1}{2} \cdots \frac{q-1}{2}\}$ be M, which is defined as $M = \{-\lfloor\frac{q}{4}\rfloor \ldots \lfloor\frac{q}{4}\rfloor\}$. The characteristic function (Cha) of the complement of set $M \; \forall \; x \in \mathbb{Z}_q$ is defined as

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

The auxiliary modular function is a map defined as follows:

$$Mod_2 : \mathbb{Z}_q \times \{0,1\} \rightarrow \{0,1\}$$
$$Mod_2(a,b) = (a + b \cdot \frac{q-1}{2}) \bmod q \bmod 2,$$

where $a \in \mathbb{Z}_q$ and b is a characteristic function of a such that $b = Cha(a)$.

Lemma 3 *Let q be an odd prime and c, e be any two element of R_q, where $|e| < \frac{q}{8}$. Then the modular function $Mod_2(c, Cha(c)) = Mod_2(\omega, Cha(c))$ is satisfied, where $\omega = c + 2e$.*

Both functions Cha and Mod_2 can be extended to the ring R_q by the following method. Let an element $c = c_0 + c_1.x + c_2.x^2 + c_3.x^2 + \cdots\cdots\cdots + c_{n-1}.x^{n-1} \in R$, where $c = (c_0, c_1, c_2, c_3, \ldots, c_{n-1})$ represents a vector. Then any arbitrary vector $u = u_0, u_1, u_2, \ldots, u_{n-1} \in \{0,1\}^n$ and the relations between the two defined functions are $Cha\{c\} = (Cha\{c_0\}, Cha\{c_1\}, Cha\{c_3\}, \ldots, Cha(c_{n-1}))$ and $Mod_2(c,u) = (Mod_2(c_0,u_0), Mod_2(c_1,u_2), \; Mod_2(c_2, u_2), \ldots, Mod_2(c_(n-1), u_(n-1)))$.

2.2 *Assumptions*

In this section, we briefly review the current lattice-based technique.

RLWE: RLWE has the assumption that A_{s,χ_β} is a uniformly distributed pair $(c, cs + e) \in R_q \times R_q$, where $c, s \leftarrow R_q$ are chosen uniformly random and $e \leftarrow \chi_\beta$ is independent of c. $RLWE_{q,\alpha}$ states that it is hard for any PPT adversary to distinguish A_{s,χ_β} from uniform distribution on $R_q \times R_q$ with only polynomially many samples.

Pairing with error (PWE): The function is defined as $\psi(y, s) = Mod_2(y \cdot s, Cha(y \cdot s))$, where y, s are two elements of R_q. The PWE problem is to compute $\psi(y, s)$ if $c, y, z \in R_q$ are given and z is defined as $z = c \cdot s + 2 \cdot e$ where $s, e \in \chi_\beta$ are unknown.

Decision pairing with errors (DPWE): The DPWE assumption is to determine $k = y.s + 2e'$ and $z = c.s + 2.e$, where $s, e', e \in \chi_\beta$ are unknown or (k, z) is uniformly random in $R_q \times R_q$ [16]. The lattice provides resistance against the quantum and post-quantum attack in modern cryptography. These assembly languages enable good mathematical security proofs. Security of lattice depends on the hard problems in n-dimensional Euclidean space R^n. In addition, the lattice-based cryptosystem's security has a feature of the worst-case hard assumption [17].

3. Proposed lattice-based authentication scheme

In this scheme we describe the proposed lattice-based authentication protocol, which comprises three phases.

3.1 *Setup phase*

In this phase, server S_j executes the following steps.

Step 1: S_j selects a random number $c \in R_q$ and discrete Gaussian distribution χ_β.

Step 2: S_j selects an integer n that is a power of 2 and an odd prime q satisfying $q \bmod 2n = 1$.

Step 3: S_j selects $x, e \leftarrow \chi_\beta$ randomly and drives the public key $P_i = c \cdot x + 2 \cdot e$.

Step 4: S_j selects a hash function defined as

$$h : \{0,1\}^* \rightarrow \{0,1\}^l,$$

where l is a fixed length output.

Step 5: S_j publishes $\{n, q, c, \chi_\beta, P_i, h\}$ in public domain and preserves the master key x confidentially.

3.2 *Registration phase*

Step 1: U_i gives the input as ID_{U_i} and PW_i. U_i computes $G_u = h(ID_{U_i}||PW_i)$. U_i sends $< ID_{U_i}, G_u >$ to S_j.

Step 2: S_j first verifies ID_{U_i}. Then it computes a $G_1 = h(ID_{U_i}||x)$, $G_2 = G_1 \oplus G_u$, where x is a master secret key of S_j. S_j stores G_1 in its database and sends $< G_2 >$ to U_i.

Step 3: Upon receiving $< G_2 >$, U_i first determines $G_1 = G_2 \oplus G_u$. Then, U_i computes $G_v = h(ID_{U_i}||PW_i||G_1)$ and stores $< G_2, G_v >$.

3.3 *Authentication phase*

In this phase, U_i and S_j mutually authenticate.

Step 1: U_i inputs ID_{U_i} and PW_i. Then, the smart device computes $G_u = h(PW_i||ID_{U_i})$, $G_1' = G_2 \oplus G_u$, and $G_v' = h(ID_{U_i}||PW_i||G_1')$ and verifies $G_v' = ?G_v$.

Step 2: After successful login, the smart device randomly generates r_i,f_i sample from discrete Gaussian distribution (χ_β). Then, it computes distribution $X_u = c \cdot r_i + 2 \cdot f_i$ and $K_u = r_i \cdot P_i$. The characteristic function play a role as $C_u = Cha(K_u)$, and auxiliary modular function computes $M_u = Mod_2(K_u, C_u)$. Then, it computes $G_3 = ID_{U_i} \oplus h(K_u \oplus M_u \oplus X_u)$ and $G_w = h(G_3||X_u||K_u||M_u||ID_{U_i})$. Finally, U_i sends (X_u, G_w, G_3, C_u) to S_j.

Step 3: After receiving (X_u, G_w, G_3, C_u) from U_i, S_j computes $K_u' = X_u \cdot x$,$M_u' = Mod_2(K_u, C_u)$. Then, it retrieves $ID_{U_i} = G_3 \oplus h(K_u' \oplus M_u' \oplus X_u)$ and $G_w* = h(G_3||X_u||K_u'||M_u'||ID_{U_i}')$. Moreover, it verifies $G_w* = ?G_w$. If verification holds, S_j generates random sample r_s,$f_s \leftarrow \chi_\beta$, and computes $X_s = c \cdot r_s + 2.f_s$, $K_s = r_s \cdot X_u$, $C_s = Chaa(K_s)$, $M_s = Mod_2(K_s, C_s)$. Then, it selects stored G_1 value and generates session key $SK = (G_1||X_u||X_s||K_u||K_s||M_u||M_s)$, $G_z = h(SK||G_1||X_s||K_s|M_u)$. S_j sends (G_z, C_s, X_s) to U_i.

Step 4: After receiving (G_z, C_s, X_s), U_i computes $K_s' = r_i.X_s$, $M_s' = Mod_2(K_s', C_s)$. Then, U_i determines $G_1 = G_u \oplus G_v$ and computes $SK' = h(G_1||X_u||X_s||K_u||K_s||M_u||M_s)$, $G_z' = ?h(SK||G_1||X_s||K_s||M_u)$ if $G_z = ?G_z'$.

3.4 *Verification of mutual authentication correctness*

The authentication between U_i and S_j depends upon verification of K_u and K_s where

$$K_u = r_i \cdot P_i \cdot K_u = r_i \cdot (c \cdot x + 2 \cdot e) = c \cdot r_i \cdot x + 2 \cdot e \cdot r_i \quad (1)$$

$$K_u{}' = X_u \cdot x = (c \cdot r_i + 2 \cdot f_i) \cdot x = c \cdot r_i \cdot x + 2 \cdot f_i \cdot x \quad (2)$$

We can express as follows:

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

By lemmas 1 and 2

$$\begin{aligned} |r_i \cdot e - f_i \cdot x| &\leq |r_i \cdot e| + |f_i \cdot x| \\ &\leq \sqrt{n} \cdot ||r_i|| \cdot ||e|| + \sqrt{n} \cdot ||f_i|| \cdot ||x|| \\ &< \sqrt{n} \cdot \beta\sqrt{n} \cdot \beta\sqrt{n} + \sqrt{n} \cdot \beta\sqrt{n} \cdot \beta\sqrt{n} \\ &= 2 \cdot \beta^2 \cdot n^{\frac{3}{2}} \end{aligned} \quad (4)$$

By lemma 2, $\beta = \omega\sqrt{logn}$ and $n << q$.

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

By lemma 3, the following equation will also hold:

$$M_u = Mod_2(K_u, C_u) = Mod_2(K_u{}', C_u) = M_u{}' \quad (6)$$

Hence equations (6) and (7) show that transmitted messages are authenticated on both sides successfully under RLWE assumption.

4. Security analysis

To achieve all security requirements of the proposed scheme, we demonstrate a brief security analysis in this section.

4.1 *Formal security analysis*

Security model

1 The User U_i can select his password PW_i independently from the dictionary. The cloud server is denoted by S_j with secret key x. During registration phase, U_i stores (G_2, G_v) in the smart device

2 There are many instances for each communicating party. Instance η of user i is represented as Π_i^η and instance μ for server S_j. Then the jth instance is represented as Π_j^μ. Each instance is called an oracle in this security model and Consumer C belongs to either U_i or S_j, $C \in (U_i, LS_j)$. We assume that an adversary $\Im_{Ad}$ can handle all communication between U_i and S_j.

3 If adversary wishes to make communication with Π_i^C, then $\Im_{Ad}$ invokes the oracle queries. We assume that $\Im_{Ad}$ either steals the smart device (σ) or gets the password from any alternative way (ω). In the proposed protocol q_h, q_e, and q_s denote hash query, execute query, and send query, respectively.

These queries determine the potential of $\Im_{Ad}$, where $\Im_{Ad}$ simulates several kinds of attacks in the security model. It must be remembered that only $\Im_{Ad}$ is allowed to send test query to its partner.

i The instances Π_σ^η and Π_ω^μ are called partners iff both have a common session identifier and finish up with accept states and vice-versa.

ii We represent $succ(\Im_{Ad})$ as the event where $\Im_{Ad}$ successfully guesses bit c. The $succ(\Im_{Ad})$ is denoted as $Pr(S_j)$. In our protocol for smart devices, the advantage for $\Im_{Ad}$ is the difference between probability of success and random guess:

$$ADV_{\Im_{Ad}}(t) = |Pr(succ(\Im_{Ad})) - \frac{1}{2}|.$$

Our scheme is semantically secure if Π_i^C and Π_j^C end on accept state for PPT adversary and generate the same session key. Advantage of PPT adversary, $ADV_{\Im_{Ad}}(t)$, is negligible.

Theorem 1 *The proposed scheme is secure under RLWE assumption if an advantage $ADV_{\Im_{Ad}}^{RLWE}(t)$ of PPT time adversary $\Im_{Ad}$ to solve RLWE problem in bounded time t will be*

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

Proof 1 We play a few games to stimulate the threats from $\Im_{Ad}$. Here, we denote every game $(0 \leq i \leq 4)$. When $\Im_{Ad}$ correctly guesses c bits in test query then it is an adversary in the game. The event S_j will appear in this process. It is expressed as $Pr(succ(\Im_{Ad}))$.

G_0 The real attack of proposed scheme is simulated under random oracle model. Then we have

$$ADV_{\Im_{Ad}}(t) = |Pr(succ(\Im_{Ad_0}) - \frac{1}{2}|.$$

Transform the equation as

$$\begin{aligned}
&= |Pr(succ(\Im_{Ad_0}) - Pr(succ(\Im_{Ad_4}) + \\
&Pr(succ(\Im_{Ad_4}) - \frac{1}{2}| \\
&= |Pr(succ(\Im_{Ad_0})) - Pr(succ(\Im_{Ad_4})) + \\
&Pr(succ(\Im_{Ad_3})) - Pr(succ(\Im_{Ad_3})) + Pr(succ(\Im_{Ad_4})) - \frac{1}{2}| \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&= \\
&|\sum_{i=1}^{4} P_i + Pr(succ(\Im_{Ad_4}) - \frac{1}{2}|.
\end{aligned}$$

Here P_i represents the difference success probability of $\Im_{Ad_{i-1}}$ and $\Im_{Ad_i}$ such that

$$P_i = |Pr(\Im_{Ad_{i-1}}) - Pr(\Im_{Ad_i})|.$$

G_1 The $\Im_{Ad}$ rises hash query, which is simulated by maintaining the hash list H_l. The H_l is initially empty and it consists of (x, y) type of element, where x is a given input and y = h(x) is the output of hash. After receiving the q_h, oracle first searches in H_l s.t. $q_s \in H_l$. If it exists then return the corresponding value, otherwise store $(x, y) \in H_l$ where $y \in \{0,1\}^l$. All the respective instances played with execute, send, reveal, corrupt, and test queries are real entities. This game simulation is absolutely indistinguishable from G_0.

$$P_1 = |Pr(\Im_{Ad_0}) - Pr(\Im_{Ad_1})|$$

G_2 In this game, the simulation process is the same as G_1 but it is terminated when some collisions occur in authentication message (G_z, G_w) and (G_1, G_v). The collision probability in the oracle will be $\frac{{q_h}^2}{2^{l+1}}$ and $\frac{(q_e+q_s)^2}{q}$ at most. The (X_u, X_s) are chosen from gaussian distribution χ_β.

$$P_2 = |Pr(\Im_{Ad_1}) - Pr(\Im_{Ad_2})| \leq \frac{{q_h}^2}{2^{l+1}} + \frac{(q_e+q_s)^2}{q}.$$

G_3 In this game, we assume that the session key SK is revealed without simulating the hash oracles. The proposed scheme SK is $SK = h(G_1||X_u||X_s||K_u||K_s||M_u||M_s)$, where $M_u = Mod_2(r_i.P_i, Cha(K_u))$ and $M_s = Mod_2(r_sX_u, Cha(K_s))$. In this game, it is hard to solve the *RLWE* problem. However, if $\Im_{Ad}$ successfully guesses SK then the challenger can solve the RLWE problem.

$$P_3 = |Pr(\Im_{Ad_2}) - Pr(\Im_{Ad_3})| \leq (q_e + q_s)ADV^{RLWE}_{\Im_{Ad}}(t).$$

G_4 In this game, $\Im_{Ad}$ queries to the hash oracle with given input $G_1, X_u, X_s, K_u, K_s, M_u, M_s$. Hence, the probability of guessing the bit c in test query in hash oracle is at most $\frac{{q_h}^2}{2^l+1}$.

$$P_4 = |Pr(\Im_{Ad_3}) - Pr(\Im_{Ad_4})| \leq \frac{{q_h}^2}{2^l+1}.$$

Otherwise, there is no advantage to $\Im_{Ad}$. The SK from any random string gives

$$Pr|Pr(\Im_{Ad_4})| = \frac{1}{2}.$$

Games G_0, G_1, G_2, G_3, G_4 show that our proposed scheme is secure under RLWE.

□

Theorem 2 *The proposed RLWE-based protocol ensures user anonymity and unlinkability against any polynomial time adversary.*

Proof 2 Anonymity and unlinkability. For achieving the anonymity and unlinkability in the proposed scheme, the message $< G_w, G_3, X_u, C_u >$ includes user's dynamic identity G_3 instead of user's identity. G_3 does not reveal user's identity and does not link any two messages, which is justified with the following points:

- To achieve user's identity ID_{U_i} from G_3, $h(K_u \oplus M_u \oplus X_u)$ is needed as $G_3 = \mathrm{ID}_{U_i} \oplus h(K_u \oplus M_u \oplus X_u)$.
- To achieve $h(K_u \oplus M_u \oplus X_u)$, $X_u = c.r_i + 2.f_i$, $K_u = r_i.P_i$ and $C_u = Cha(K_u)$ is needed as $h(K_u \oplus M_u \oplus X_u) \oplus G_3$.
- To retrieve the identity ID_{U_i}, any $\Im_{Ad}$ needs to generate X_u, K_u, which is infeasible under the RLWE problem.

- For each session, different random samplings are processed for different sessions and used as $X_u = c.r_i + 2.f_i$, where r_i, f_i are randomly sampled parameters for each session.
- To retrieve next session values r_i', f_i' from the message $< X_u', G_w', G_3', C_u' >$, $h(K_u' \oplus M_u' \oplus X_u')$ is needed as $G_3' = ID_{U_i} \oplus h(K_u' \oplus M_u' \oplus X_u')$. Again, it is infeasible to compute user identity at any cost.
- To compute $h(K_u' \oplus M_u' \oplus X_u')$, the parameter K_u is needed along with r_i, f_i.

It is very trivial that U_i's identity along with password is needed to retrieve identity of user from the login message. Moreover, any two session messages are not linked as the server generates different values r_i, f_i for each session. □

Theorem 3 *The man in the middle attack does not exist for any polynomial time executed adversary.*

Proof 3 An $\mathfrak{I}_{Ad}$ may attempt to set up independent connections with S_j and U_i.

- $\mathfrak{I}_{Ad}$ intercepts user's message $< X_u, G_w, G_3, C_u >$ and tries to modify and replace it as follows:
- $\mathfrak{I}_{Ad}$ may try to modify $< X_u, G_w, G_3, C_u >$ by replacing C_u by C_u^*, where $C_u^* = r_i.P_i$ for random value r_i. In this case $\mathfrak{I}_{Ad}$ has to compute $K_u^* = r_i^* P$, which requires the knowledge of randomly selected samples r_i, f_i. User's randomly selected samples are protected with $X_u = c.r_i + 2.f_i$, where c is master secrete key of S_j. $\mathfrak{I}_{Ad}$ cannot successfully modify user's login message.
- $\mathfrak{I}_{Ad}$ may intercept the message $< X_u, G_w, G_3, C_u >$ and replace it with previously transmitted message. However this attempt will not work due to randomly generated r_i, f_i, which is demonstrated earlier.

$\mathfrak{I}_{Ad}$ may intercept responder message $< G_z, C_s, X_s >$ and try to modify and replace it.

- $\mathfrak{I}_{Ad}$ may try to modify $< G_z, C_s, X_s >$ by replacing C_s with $C_s^* = Cha(K_s)$, where K_s generates $r_s.X_u$. In this case, $\mathfrak{I}_{Ad}$ also needs to replace $G_z = h(SK||G_1||X_s||K_s||M_u)$ with $M_u^* = Mod_2(K_s, C_s)$, where $SK^* = h(G_1||X_u||X_s||K_u||K_s||M_u||M_s)$. The computation of SK^* requires G_1, which is protected with the ID_{U_i}, $\mathfrak{I}_{Ad}$ secrete key so it cannot successfully compute SK^*.
- $\mathfrak{I}_{Ad}$ may replace $< G_z, C_s, X_s >$ with a previously transmitted message. It will not work as user can easily identify when user verifies the condition $G_z \stackrel{?}{=} h(SK||G_1||X_s||K_s||M_u)$, where $SK = h(G_1||X_u||X_s||K_u||K_s||M_u||M_s))$ as $G_z' = h(SK'||G_1'||X_s'||K_s'||M_u'))$ and for each session fresh random sampling and distribution are used. $\mathfrak{I}_{Ad}$ is not able to impersonate transmission in the middle.

□

Theorem 4 *There is no polynomial time adversary proposed that successfully achieves forward secrecy.*

Proof 4 If server's (S_j) secret key x is compromised, an $\mathfrak{I}_{Ad}$ may try to construct the established session key $SK = h(G_1||X_u||X_s||K_u||K_s||M_u||M_s)$ using the compromised key x.

- $\mathfrak{I}_{Ad}$ can achieve the values G_2, G_v from the stolen device attack and previously transmitted messages.
- To compute the session key $SK = h(G_1||X_u||X_s||K_u||K_s||M_u||M_s)$, different random sampling distributions occurring for each session K_s, X_s, and C_s need r_i, f_i to compute SK. G_1 requires a user identity ID_{U_i} along with x to generate a fresh G_1' parameter.
- To achieve ID_{U_i} from G_3, $\mathfrak{I}_{Ad}$ needs $h(K_u \oplus M_u \oplus X_u)$ as $G_3 = ID_{U_i} \oplus h(K_u \oplus M_u \oplus X_u)$.
- To compute $h(K_u \oplus M_u \oplus X_u)$, $\mathfrak{I}_{Ad}$ needs to compute $K_u' = r_i.P$ and $C_u' = Cha(K_u)$, as $ID_{U_i} = h(K_u \oplus M_u \oplus X_u) \oplus G_3$.
- $\mathfrak{I}_{Ad}$ can compute $h(K_u \oplus M_u \oplus X_u)$ and $SK = h(G_1||X_u||X_s||K_u||K_s||M_u||M_s)$ using comprised key x. As $G_1 = h(ID_{U_i}||x)$, to compute G_1, user's identity ID_{U_i} is also needed. Thus $\mathfrak{I}_{Ad}$ has not achieved the session key. To retrieve ID_{U_i} from G_3 also needs $h(K_u \oplus M_u \oplus X_u)$.

User (U_i)	Secure channel	Server (S_j)
Select ID_{U_i}, PW_i $G_u = h(ID_i\|\|PW_i)$		
	$< ID_{U_i}, G_u >$ ⟶	Check ID_{U_i}
		Compute $G_1 = h(ID_{U_i}\|\|x)$ Compute $G_2 = G_1 \oplus G_u$ Store (G_1)
	⟵ $< G_2, h(\cdot) >$	
$G_1 = G_2 \oplus G_u$ $G_v = h(ID_i\|\|PW_i\|\|G_1)$ Store (G_2, G_V)		

Figure 2. Illustration of registration phase.

- To retrieve r_i, f_i from X_n is infeasible as gaussian distribution RLWE is a hard problem.

We conclude from the brief discussion that U's identity ID_{U_i} is required to achieve random nonce G_1. As adversary cannot retrieve user's identity ID_{U_i} from the message, an adversary cannot construct the session key using compromised long-term secret key. □

4.2 *Informal security analysis*

In this phase, we discuss the security features of proposed authenticated content key distribution protocol for RLWE problem.

Key freshness property Every time, SK is comprised if distribution is used only once in a communication. The uniqueness property of random sampling guarantees different keys for every session. This construction ensures the key freshness property.

Mutual authentication License server and user verify the authenticity of each other using the conditions $G_w = h(G_3||X_u||K_u||M_u||ID_{U_i})$ and $G_z = h(SK||G_1||X_s||K_s||M_u))$, respectively, where $SK = h(G_1||X_u||X_s||K_u||K_s||M_u||M_s)$. To compute G_w and G_z, user's long-term secret keys r_i, f_i are needed. To retrieve ID_{U_i} from $G_3 = ID_{U_i} \oplus h(K_u||M_u||X_u)$, a randomly distributed number is needed. The principals who can compute the session key are the user and license server. Thus, both S_j and U_j verify each other.

Replay attack The replay attack arises when the adversary gets the authentication message from the previous session and uses this message in the present as a legal user. In the proposed protocol, every time fresh r_i, r_s and f_i, f_s are used by U_i and S_j, respectively. Thus, each authority catches the reply attack after verification.

Impersonation attack The adversary is not able to generate authentic messages G_w and G_z because we also show that the protocol holds anonymity and K_u, which is protected by random number r_i. If the adversary impersonates open transmitted message, then he will be detected at verification time. No impersonation attack is possible.

Offline dictionary attack Suppose the adversary gets all stored information (G_2, G_v) in the smart device. Then the adversary needs to construct a G_u; for constructing this the adversary guesses PW_i even if he/she does not know the ID_{U_i}. It is impossible to verify the correctness without the U_i identity. Thus, offline dictionary attacks are not practically possible.

5. Performance analysis

In this phase, we evaluate the proposed lattice-based key agreement protocol efficiency in term of communication cost and demonstrate by comparison to some existing scheme.

We consider Gaussian sampling distribution χ_β and fix the value of $\log_\beta = 17.1$ for the proposed protocol. We considered the following symbols: total time consumption for sampling from χ_β gaussion distribution function T_{gd}; componentwise scalar multiplication T_{mu}; componentwise multiplication and addition operations T_{mua}; characteristic function T_{Cha}; encryption/decryption T_{sym}, hash function T_h, T_b bilinear pairing, T_{ch} chaotic map, T_{ecm} elliptic curve multiplication, T_{fe} fuzzy extractor, and T_me modular exponent. We demonstrate the communication cost efficiency of proposed protocol in Figures 2 and 3. We have done our performance comparison in SPSS tool in which scatter piloting shows the significance of proposed protocol.

We know that T_h is very efficient for classical computation. The possible increasing order of these operations is $T_{mu} < T_{mua} < T_{Cha} < T_h < T_{gd} < T_{sym,dec} < T_{fe} < T_{ecm} < T_{me} < T_b$. The approximate computing time of the AES encryption algorithm and chaotic map are collected as $T_{Ch} \approx 0.02102$ s, $T_{sym} \approx 0.0056$ s, $T_h \approx 0.00032$ s, $T_b \approx 0.380$s, $T_{fe} \approx 0.0171$, $T_{me} \approx 0.0592$s [19, 21]. The quantum operations are performed in Lattice Crypto and Miracle Library on $C/C++$ language [22]. The performed operator configuration details are a Dell PC with 3.4-GH intelcore processor, 8 GB RAM, i-7 6700 CPU. They perform with several IoT devices. All the respective operations are performed in a second but we adopt [13] the result to convert into nanoseconds, evaluate the communication cost of existing scheme and compare to others.

Regarding total computation cost consumption of all existing schemes, we evaluate this consumption using Table 1. Then we take cost as $T_{ch} = 6 \times 0.0171$, $T_h = 13 \times 0.00032$ from [18], using which we evaluate the final computation cost of the respective schemes. Similarly, the

User (U_i)	Secure channel	Server (S_j)
Input ID_{U_i} and PW_{U_i}		
Compute $G_u = h(PW_{U_i} \oplus ID_{U_i})$		
$G_1' = G_2 \oplus G_u$		
$G_v' = h(ID_{U_i} \| PW_i \| G_1')$		
verifyG_v =?G_v^*		
Generate random sample		
$r_i, f_i \leftarrow \chi_\beta$		
$X_u = c.r_i + 2.f_i$		
$K_u = r_i.P_i$		
$C_u = Cha(K_u)$		
$M_u = Mod_2(K_u, C_u)$		
$G_3 = ID_{U_i} \oplus h(K_u \oplus M_u \oplus X_u)$		
$G_w = h(G_3 \| X_u \| K_u \| M_u \| ID_{U_i})$		
	$< X_u, G_w, G_3, C_u >$ $\longrightarrow$	Compute $K_u' = X_u.x$
		$M_u' = Mod_2(K_u', C_u)$
		$ID_{U_i} = G_3 \oplus h(K_u' \oplus M_u' \oplus X_u)$
		Verify, G_w =?G_w^*
		If verification holds
		Generate random sample
		$r_s, f_s \leftarrow \chi_\beta$
		$X_s = c.r_s + 2.f_s$
		$K_s = r_s X_u$
		$C_s = Cha(K_s)$
		$M_s = Mod_2(K_s, C_s)$
		Select $G_1 = h(ID_{U_i} \| x)$
		$SK = h(G_1 \| X_u \| X_s \| K_u \| K_s \| M_u \| M_s)$
		$G_z = h(SK \| G_1 \| X_s \| K_s \| M_u)$
	$< G_z, C_s, X_s >$ $\longleftarrow$	
$K_s' = r_i.X_s$		
$M_s' = Mod_2(K_s', C_s)$		
$G_1 = G_u \oplus G_v$		
$SK' = h(G_1 \| X_u \| X_s \| K_u \| K_s \| M_u \| M_s)$		
G_z =?$h(SK \| G_1 \| X_s \| K_s \| M_u)$		
If its holds then		
Store SK		

Figure 3. Illustration of authentication phase.

Table 1. Notations used in the scheme.

Notation	Description
U_i	User i
S_j	Server
Cha	Characteristic function
$\Im_{Ad}$	Adversary
Mod_2	Auxiliary modular function
ID_{U_i}	Identity of U_i
SK	Session key
PW_i	Password of user
x	Secret value of the server
$h(\cdot)$	Collision resistance function $h : Z_q^* \rightarrow Z_q^*$
$\oplus$	Bitwise XOR
$\|$	String concatenation

total computation cost of the rest of the schemes is evaluated and presented in Tables 2 and 3. We demonstrate the comparison in Figure 4.

We know that the Mod_2 operation is completed only with the AND operation; therefore, we neglect the cost of Mod_2 in analysis cost computation of proposed protocol.

In our proposed scheme for smart device, when U_i logs into the device, the user must give the input as its ID_{U_i} and PW_i; then the device verifies this by only a single hash operation. After successful login, the device is required to choose two random samples from χ_β and operate with one componentwise multiplication and addition operation over R_q [13]. Similarly, we compute K_u by componentwise multiplication and then operate K_u on the characteristic function. After this, for hiding the ID_{U_i}, we use one hash function and one extra hash function to authenticate all computations by G_w. Hence, the total time consumption from user side is $5T_h + T_{gd} + 3T_{mul} + T_{mua} + T_{ch} \approx 1546.117$ ns .

After receiving the request from U_i, S_j first verifies the user and then checks whether G_w is validated or not by componentwise multiplication operation. If verification is done successfully, it generates two random numbers and

Table 2. Total computation time consumption in respective operations, where time is presented in nanoseconds.

Operations	U_i side	S_j side
T_{gd}	561.483	73.503
T_{mu}	6.655	0.298
T_{mua}	29.505	2.549
T_{Cha}	35.515	0.689
T_h	180.964	14.06

calculates X_s by componentwise addition. In this manner, we compute K_s, C_s and generate a session key SK. Hence, total computation cost from S_j side will be $T_{gd} + 3T_h + T_{Cha} + 2T_{mu} + T_{mua} \approx 119.978$ ns .

According to [13], the ring of polynomial R_q fixes 4096 bits and the hash function SHA-3 gives the 512 bits output. The classical crypto-system applies 256-bit AES with private key encryption and 1024-bit modulus. The timestamp will be 32-bit with 160-bit elliptic curve output [23].

In [13], the U_i sends $< x_{i,i}, \alpha_i, aid_i >$ to S_j messages and computes the communication cost in this transmission as $4096 + 512 + 1 + 512 = 5121$ bit. After this, S_j sends back $< \alpha_S, S, \alpha_S >$ to the U_i where α_i, α_s are hash output, $x_i, x_S \in R_q$ and other w_i,$_S$ are random binary bits. Then finally calculate the overhead as $4096 + 1 + 512 = 4609$ bit. Hence, total overhead of communication will be 9730 bit.

Similarly, the proposed protocol performs as follows: the U_i sends $< X_u, G_w, G_3, C_u >$ to S_j and computes the communication cost in this transmission as $4096 + 512 + 1 + 512 = 5121$ bit. After this, S_j sends back $< G_z, X_s, C_s >$ to U_i where α_i, α_s are hash output, $x_i, x_S \in R_q$ and other w_i,$_S$ are random binary bits. Then finally calculate the overhead as $4096 + 1 + 512 = 5121$ bits. Hence, total overhead of communication will be 9730 bit.

Table 3. Number of operations required in a protocol during authentication session execution.

Schemes	U_i side	S_j side	Total computation cost (ns)
[18]	$7T_h + 3T_{ch}$	$6T_h + 3T_{ch}$	13016950
[19]	$6T_h + T_{me} + 3T_{ecm}$	$6T_h + T_{me} + 2T_b + 2T_{ecm}$	27633000
[20]	$2T_h + 1T_{me} + T_{fe}$	$2T_h + 2T_{me}$	19523200
[14]	$5T_h + 2.T_{gd} + 4T_{mu} + 1.T_{mua} + 3T_{Cha}$	$2T_{gd} + 3T_h + 1T_{mu} + 3T_{mua} + 4T_{Cha}$	3233.987
[15]	$6T_h + 1.T_{gd} + 5T_{mu} + 2T_{mua} + T_{Cha}$	$3T_{gd} + 4T_h + 2T_{mu} + 2T_{mua} + T_{Cha}$	2933.536
[13]	$6T_h + T_{gd} + 3T_{mu} + T_{mua} + T_{Cha}$	$T_{gd} + 4T_h + 3T_{mu} + T_{mua} + T_{Cha}$	1892.435
Proposed	$5T_h + T_{gd} + 3.T_{mu} + T_{mua} + T_{Cha}$	$T_{gd} + 3T_h + T_{Cha} + 2T_{mu} + T_{mua}$	1665.335

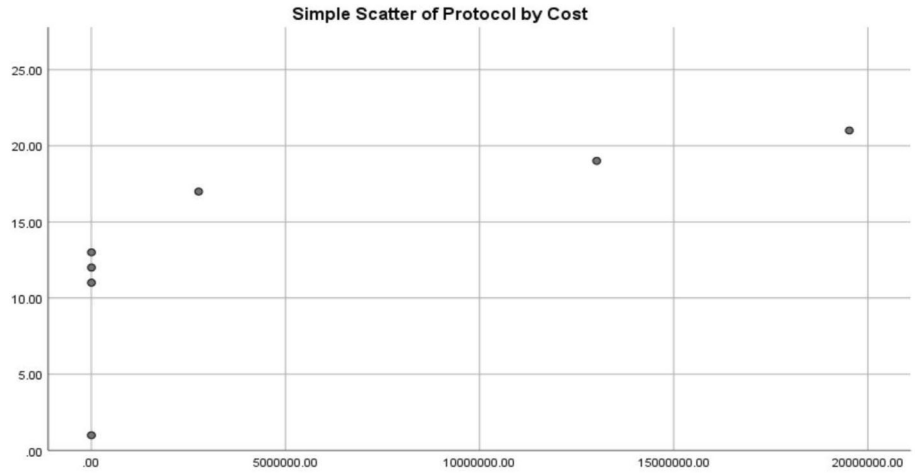

Figure 4. Computation cost in nanoseconds.

6. Conclusion

In this paper, we have presented a lattice-based authentication protocol based on the RLWE. The proposed protocol is very user-friendly and easily adaptable for IoT devices. We have performed the analysis of security for the proposed protocol in a widely accepted random oracle model. Using the informal and formal analysis of security, we have demonstrated that the proposed scheme successfully prevents existing active and passive attacks along with the security threat due to Shor's algorithm. After comparing with the existing schemes, we have identified that the proposed protocol is also efficient in term of computation overhead. Finally, we conclude that the proposed protocol has the capability to ensure efficient and secure communication in the quantum computing era.

References

[1] Gope P 2019 Anonymous mutual authentication with location privacy support for secure communication in m2m home network services. *J. Ambient Intell. Humaniz. Comput.* 10(1): 153–161

[2] Gupta M and Chaudhari N S 2019 Anonymous roaming authentication protocol for wireless network with backward unlinkability, exculpability and efficient revocation check. *J. Ambient Intell. Humaniz. Comput.* 10(11): 4491–4501

[3] Mishra D and Rana S 2020 Authenticated content distribution framework for digital rights management systems with smart card revocation. *Int. J. Commun. Syst.* 33(9): 1–19

[4] Rana S and Mishra D 2020 Secure and ubiquitous authenticated content distribution framework for IoT enabled DRM system. *Multimed. Tools Appl.* 79: 20319–20341

[5] Ajtai M 1996 Generating hard instances of lattice problems. In: *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, pp. 99–108

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

[7] Shor P W 1999 Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* 41(2): 303–332

[8] Lyubashevsky V, Peikert C, and Regev O 2010 On ideal lattices and learning with errors over rings. In: *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 1–23

[9] Zhang J, Zhang Z, Ding J, Snook M, and Dagdelen O 2015 Authenticated key exchange from ideal lattices. In: *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 719–751

[10] Alkim E, Ducas L, Pöppelmann T, and Schwabe P 2016 Post-quantum key exchange—a new hope. In: *Proceedings of the 25th USENIX Security Symposium (USENIX Security 16)*, pp. 327–343

[11] Ding J, Branco P, and Schmitt K 2019 Key exchange and authenticated key exchange with reusable keys based on RLWE assumption. Technical Report, Cryptology ePrint Archive, Report 2019/665, pp. 1–35

[12] Ding J, Alsayigh S, Lancrenon J, Saraswathy R V, and Snook M 2017 Provably secure password authenticated key exchange based on RLWE for the post-quantum world. In: *Proceedings of the Cryptographers Track at the RSA Conference*. Springer, pp. 183–204

[13] Feng Q, He D, Zeadally S, Kumar N, and Liang K 2018 Ideal lattice-based anonymous authentication protocol for mobile devices. *IEEE Systems Journal* (99) 1–11

[14] Islam S K 2020 Provably secure two-party authenticated key agreement protocol for post-quantum environments. *J. Inform. Secur. Appl.* 52: 102468

[15] Dharminder D and Chandran K P 2020 LWESM: learning with error based secure communication in mobile devices using fuzzy extractor. *J. Ambient Intell. Humaniz. Comput.* 11: 4089–4100

[16] Micciancio D and Mol P 2011 Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions. In: *Proceedings of the Annual Cryptology Conference*, pp. 465–484

[17] Micciancio D 2007 Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Comput. Complex.* 16(4): 365–411

[18] Madhusudhan R and Nayak C S 2019 A robust authentication scheme for telecare medical information systems. *Multimed. Tools Appl.* 78(11): 15255–15273

[19] Odelu V, Das A K, Wazid M, and Conti M 2018 Provably secure authenticated key agreement scheme for smart grid. *IEEE Trans. Smart Grid* 9(3): 1900–1910

[20] Chen H B, Lee W B, and Chen T H 2018 A novel DRM scheme for accommodating expectations of personal use. *Multimed. Tools Appl.* 77(18): 1–16

[21] Chatterjee S, Roy S, Das A K, Chattopadhyay S, Kumar N, and Vasilakos A V 2018 Secure biometric-based authentication scheme using Chebyshev chaotic map for multi-server environment. *IEEE Trans. Dependable Secure Comput.* 15(5): 824–839

[22] Melchor C A, Barrier J, Guelton S, Guinet A, Killijian M O, and Lepoint T 2016 NFLlib: NTT-based fast lattice library. In: *Proceedings of the Cryptographers' Track at the RSA Conference*, pp. 341–356

[23] Odelu V, Das A K, and Goswami A 2015 An efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card. *J. Inform. Secur. Appl.* 21: 1–19