Computers, Materials & Continua
DOI: 10.32604/cmc.2023.036189
Article

Tech Science Press

Lattice-Based Authentication Scheme to Prevent Quantum Attack in Public Cloud Environment

Naveed Khan[1], Zhang Jianbiao[1], Intikhab Ullah[2], Muhammad Salman Pathan[3] and Huhnkuk Lim[4,*]

[1]Faculty of Information Technology, Beijing University of Technology, Beijing, 100124, China
[2]Lecture in Computer Science, Shaheed Benazir Bhutto University, Sheringal, 18050, Pakistan
[3]Department of Computer Science, Maynooth University, Maynooth, W23 A3HY, Ireland
[4]Department of Computer Engineering, Hoseo University, Asan-si, 31499, Korea
*Corresponding Author: Huhnkuk Lim. Email: slow63347@gmail.com
Received: 20 September 2022; Accepted: 04 November 2022

Abstract: Public cloud computing provides a variety of services to consumers via high-speed internet. The consumer can access these services anytime and anywhere on a balanced service cost. Many traditional authentication protocols are proposed to secure public cloud computing. However, the rapid development of high-speed internet and organizations' race to develop quantum computers is a nightmare for existing authentication schemes. These traditional authentication protocols are based on factorization or discrete logarithm problems. As a result, traditional authentication protocols are vulnerable in the quantum computing era. Therefore, in this article, we have proposed an authentication protocol based on the lattice technique for public cloud computing to resist quantum attacks and prevent all known traditional security attacks. The proposed lattice-based authentication protocol is provably secure under the Real-Or-Random (ROR) model. At the same time, the result obtained during the experiments proved that our protocol is lightweight compared to the existing lattice-based authentication protocols, as listed in the performance analysis section. The comparative analysis shows that the protocol is suitable for practical implementation in a quantum-based environment.

Keywords: Lattice; authentication; quantum attack; ProVerif

1 Introduction

Recently, cloud computing has become very popular among corporations, individuals, and government organizations for its ability to provide low-cost services via the internet. Due to the availability of high-speed internet connections, these services can be accessed easily for numerous purposes. Cloud computing offers various services, and storage is considered one of the most important services for various architectures and applications. Annually, billions of devices outsource massive amounts of data, which are stored in cloud computing globally. However, security is a significant concern for these outsourced stored data in cloud computing environments because of advanced computing devices and strong adversaries. Therefore, cryptographic techniques such as Elliptic-curve cryptography (ECC), Symmetric, Asymmetric, Identity-based, Hashing, and many more techniques are used to protect outsourced data in the cloud computing environment. The ECC authentication protocols are based on discrete logarithm problems, whereas RSA (Rivest–Shamir–Adleman) is based on large numbers of factorizations. RSA-based cryptography techniques are slower because of the exponentiation and heavy computation and communication costs.

Recently, the world has seen a race among countries and organizations to build superior quantum computers. These quantum computers are so strong that they can break the traditional cryptographic algorithms, add more attacks on authentication protocols, and open a way to easily access the stored data on the public cloud. On the other hand, lattice-based cryptography provides excellent efficiency and simplicity in the post-quantum cryptographic era. For this purpose, we have proposed a lattice-based authentication scheme for public cloud computing in this study. So far, the lattice-based cryptography protocols resist quantum attacks.

1.1 Motivation and Contributions

The Lattice-based cryptographic authentication technique gives hope for the post-quantum era. A lattice is a set of all the integer's linear combinations of base vectors, such as $\mathscr{b}_1, \mathscr{b}_2, \mathscr{b}_2, \ldots \mathscr{b}_n \in Z^n$, $\mathrm{A} = \left\{\sum a_i * \mathscr{b}_i : a_i \in Z^n\right\}$. The lattice is based on a base vector and can only be scaled by integers; no fractions are involved. Even quantum computers cannot solve the lattice-based problem in polynomial time. The lattice that only two basis vectors are defined $v_1 = (0, 1)$ and $v_2 = (1, 0)$. Here, the lattice is a set of all values that can be reached by any scale and combination of basis vectors. There is no point to reach $v_1 = (0, 1)$ and $v_2 = (1, 0)$ without fractional scalars, and the scale is only possible with whole integers. However, traditional cryptographic techniques, such as RSA, are based on mathematical problems that can be easily verified but are hard to compute. RSA is based on prime factorization and works excellently with traditional computers but failed in the quantum computing era. Therefore, the lattice shortest vector problem is a major cryptographic algorithm that can prevent quantum attacks excellently. According to our knowledge, in the quantum computing era, the $\mathcal{A}$ can use Shor's technique and easily break traditional authentication protocols. The following are our contributions.

- We have utilized the lattice-based Ring with errors (RLWE) technique for the design of our protocol.
- Our proposed protocol is secure under the RLWE problematic assumptions.
- We have utilized the Gaussian probability distribution, also known as the discrete gaussian, which plays a vital role in lattice-based cryptography algorithms.
- The formal security analysis of our proposed scheme shows that it can fulfill the security requirements in public cloud environments in the post-quantum era.
- Our scheme is secure against all known traditional attacks in the informal security analysis.
- The protocol performance analysis section demonstrates that the proposed protocol is efficient as compared to the existing lattice-based techniques.

1.2 Network Model

Our protocol consists of two entities, a user and a public cloud server. The user uses portable devices to access the public cloud server. In contrast, public cloud servers provide various services to the user using high-speed internet, such as storage space, access to shared data and private data space, and many more. The detailed diagram of the proposed model is shown in Fig. 1.

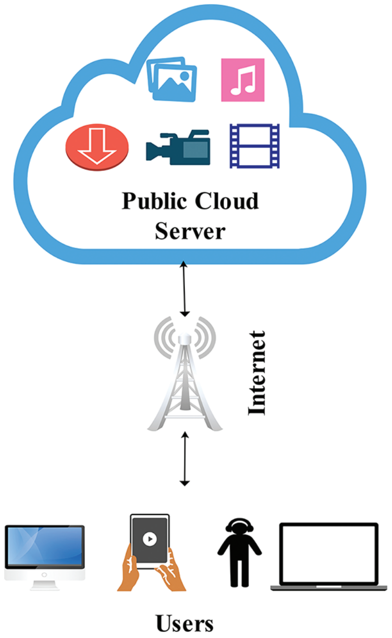


Figure 1: Proposed network model

2 Literature Review

In this portion of the paper, we will discuss and analyze the limitations of existing authentication techniques.

Different cryptographic techniques have been used to authenticate different peers in different environments, Hashing, Bilinear pairing, Identity-based, Elliptic curve (ECC), Chaotic maps, Code-based, and Lattice-based. However, some of these cryptographic techniques are not secure against quantum attacks. The authors of [1] proposed an authentication scheme for a public cloud server environment that achieved all known security goals but was not much feasible for the quantum computing era. Some existing proposed schemes are not efficient against quantum attacks and are vulnerable to known security attacks, for example, the schemes [2–13] suffer from offline password attacks, while the schemes [5,6,10,13–21] cannot provide anonymity. As a result, the protocols [4,9,21–24] are vulnerable to insider attacks. Furthermore, the schemes [5–9,13,16–19,24–27] are not secure enough against impersonation attacks, and the protocols [18,19,28] are vulnerable to replay attacks.

The increasing competition to build high-performance quantum computers among organizations will potentially threaten these cryptographic techniques. However, the lattice-based cryptography method is the most secure against quantum attacks. Therefore, the researchers are trying to utilize the lattice-based cryptography technique to propose an authentication scheme for various environments. For example, an ideal lattice-based authentication scheme for mobile devices is proposed in [29]. The authors of [30] proposed a lattice-based authentication protocol for Internet of Things (IoT) devices. In [29], the authors claimed that their scheme is the first ever lattice-based scheme for mobile devices. However, the communication and computation costs were much higher than our proposed scheme.

Furthermore, the authors utilized a Radio Frequency Identification (RFID) system for an IoT environment to secure communications and resist quantum attacks, and the author used the lattice-based cryptography technique. Another scheme is proposed in [31] for IoT-enabled smart devices under the ring LWE problem using a lattice-based cryptography technique. Although the scheme is proposed for IoT devices, but the communication and computation costs are very high as compared to our proposed scheme. Finally, the authors of [32] proposed an authentication scheme for the internet of vehicles, where the authors utilized the identity-based technique in lattice-based cryptography. In this scheme, the edge nodes first gets private keys from the private key generator (PKG) and later communicate with each other using these keys. Furthermore, the author uses identity-based cryptography (IBC) to reduce the overhead of certificate management.

The distribution of quantum keys using fuzzy logic is presented in [33]. The scheme is intended for nuclear command and control centers (NCCC) and has management, rigor, self-learning, inherent security, and authentication capabilities. The distribution of quantum keys based on fuzzy logic guarantees the user's identity. In [34], the authors utilize the edge and fog computing through deep learning in a quantum computing framework, where the edge node has the capacity for processing, communication, caching, and storage. The scheme used an intelligent quantum computing framework coupled with deep learning for updating edge caching contents in a fog-computing radio access network.

3 Proposed Scheme

In this section of our research study, we present an authentication strategy for public cloud environments based on lattice cryptography.

3.1 Setup Procedure

- The public cloud server selects random number $\mathrm{r_S} \in Z_q^{ixi}$ Where q is an odd prime number, and i is an integer that satisfies q mod 2i = 1.
- The public cloud server selects secure hash function h(.).
- The public cloud server selects the secret value S that belongs $e \leftarrow \chi_\beta \Rightarrow f\,(x) = \frac{1}{\sqrt[\sigma]{2\pi}} e^{-\frac{1}{2}(\frac{x-\mu}{\sigma})^2}$.
- The Public cloud server Select $\partial \Rightarrow \chi_\beta$, where χ_β is the Gaussian distribution
- The public cloud server calculates public key $\mathrm{PK_S} = \mathrm{r_S}.\ \mathrm{S} + 2.\mathrm{e}$
- The public cloud server published {q, i, $\mathrm{r_S}$, $\mathrm{PK_S}$, h(.)} and saved S as a secret key.

Table 1: Symbols and description

Symbols	Description
U	User
PCS	Cloud server
$\mathrm{ID_U}$	Identity of user
$\mathrm{PW_U}$	Password of user
$\mathrm{r_S}$, $\mathrm{r_{S1}}$	The random numbers of cloud server
$\mathrm{r_U}$	A random number of user
χ_β	Gaussian distribution
$\partial,\ \gamma, \rho$	Gaussian distribution samples
q	Odd prime number
i	Integer

(Continued)

Table 1: Continued

Symbols	Description
S	The secret key of the cloud server
PK_S	The public key of the cloud server
$\|\|$	Concatenation

3.2 Registration Procedure

- Select ID_U and send it to the public cloud server.
- The public cloud server then selects the random number $r_S \in Z_q^{ixi}$, choose $\gamma, \rho \leftarrow \chi_\beta$ and calculates the user secret key $S_U = h\ (ID_U || S)$, and $S_1 = h\ (ID_u || r_S) \oplus S_U$. After calculation, the public cloud server sends $\{r_{S1}, S_1\}$ to the user.
- The user then selects the password PW_U and calculates $S_2 = h\ (r_S || ID_U) \oplus h\ (PW_u || ID_U) \oplus S_1$, and $S_3 = h\ (ID_u || PW_u || S_2)$. The user store $\{S_2, S_3, \rho, \partial\ \}$.

User		Public Cloud Server
Select ID_U		
	$\underset{\longrightarrow}{\{ID_U\}}$	
		$r_S \in Z_q^{ixi}$ $\gamma, \rho \leftarrow \chi_\beta,$ $S_U = h\ (ID_U \|\| S)$ $S_1 = h\ (ID_u \|\| r_{S1}) \oplus S_U$ Store $\{\ \gamma, \partial\}$
	$\underset{\longleftarrow}{\{r_S, S_1,\ \rho, \partial\}}$	
selects the password PW_U $S_2 = h\ (r_S \|\| ID_U) \oplus h\ (PW_u \|\| ID_U) \oplus S_1$ $S_3 = h\ (ID_u \|\| PW_u \|\| S_2)$ Store $\{S_2, S_3, \rho, \partial\ \}$		

Module 1: User registration procedure

3.3 Login and Registration Procedure

- The user input $ID_U{}^*$ and $PW_U{}^*$ and calculate the $S_3{}^* = h\ (ID_u{}^* || PW_u{}^* || S_2)$ and check $S_3{}^*? = S_3$ if true, then the system proceeds further; otherwise, connection is terminated. The user selects a random number $r_U \in Z_q^{ixi}$ and calculates further. $M = r_S.\ r_U + 2.\rho$ and forward $\{M\}$ towards the public cloud server.
- The public cloud server selects the random number $r_{S1} \in Z_q^{ixi}$ and calculates further $M_1 = r_{S.}$ $rS1 + 2.\ \gamma$, $M_2 = (M||S)$, $M_3 = \partial\ (M_2)$, $M_4 = (M_2||M_3)$, $M_5 = h\ (M|| M_1|| M_3|| M_4)$ and sends $\{M_1, M_3, M_5\}$ to user.
- The user calculates $M_2{}' = (r_U\ .\ PK_S)$, $M_4{}' = (M_2{}'|| M_3)$, $M_5{}'? = h(M|| M_1|| M_3|| M_4)$ if the value matches, then proceed further otherwise, terminate the connection. The user further calculates

$M_6 = h\ (ID_U||\ PW_U) \oplus S_2$, $M_7 = (M_1||\ r_U)$, $M_8 = \partial\ (M_7)$, $M_9 = (M_7||\ M_8)$, $M_{10} = h\ (M||\ M_8||\ M_9||\ M_1||\ M_3||\ M_4||\ M_2) \oplus ID_U$, $M_{11} = h\ (ID_U||\ M_6||\ M_{10}||\ M||\ M_8||\ M_9||\ M_1||\ M_3||\ M_2'||\ M_5)$, $S_{KU} = h\ (ID_U||\ M_{10}||\ M||\ M_8||\ M_9||\ M_{11}||\ M_1||\ M_3||\ M_2'||\ M_5)$ and sends $\{M_{10}, M_8, M_{11}\}$ towards public cloud server.

- The public cloud server calculates further $M_7' = (M||\ r_{S1})$, $M_9' = (M_7'||M_8)$, $ID_U = h\ (M||\ M_8||\ M_9'||\ M_1||\ M_3||\ M_4||\ M_2) \oplus M_{10}$, $M_6' = h\ (ID_U||S)$, $M_{11}' = h\ (ID_U\ ||M_6'||\ M_{10}||\ M||\ M_8||\ M_9'||\ M_1||\ M_3||\ M_2||\ M_5)$ and check $M_{11}'? = M_{11}$ if true, proceed further; otherwise, terminate the connection. The public cloud server calculates the session key $S_{KS} = h\ (ID_U||\ M_{10}||\ M||\ M_8||\ M_9'||\ M_{11}||\ M_1||\ M_3||\ M_2||\ M_5)$.

User		Public Cloud Server
ID_U^* and PW_U^*		
Calculate		
$S_3^* = h\ (ID_u^*||PW_u^*||S_2)$		
Check $S_3^*? = S_3$		
random number $r_U \in Z_q^{ixi}$		
$M = r_S.\ r_U + 2.\rho$		
	$\{M\}$ $\rightarrow$	
		random number $r_{S1} \in Z_q^{ixi}$
		Calculates
		$M_1 = r_{S.}\ r_{S1} + 2.\ \gamma$
		$M_2 = (M.S)$
		$M_3 = \partial\ (M_2)$
		$M_4 = (M_2.M_3)$
		$M_5 = h(M||M_1||M_3||M_4)$
	$\{M_1, M_3, M_5\}$ $\leftarrow$	
Calculates		
$M_2' = (r_U\ .\ PK_S)$		
$M_4' = (M_2'||M_3)$		
$M_5'? = h(M||M_1||M_3||M_4)$		
$M_6 = h(ID_U||PW_U) \oplus S_2$		
$M_7 = (M_1.\ r_U)$		
$M_8 = \partial\ (M_7)$		
$M_9 = (M_7||M_8)$		

$M_{10} = h(M||M_8||M_9||M_1||M_3||M_4||M_2) \oplus ID_U$

$M_{11} = h(ID_U||M_6||M_{10}||M||M_8||M_9||M_1||M_3||M_2{}'||M_5)$

$S_{KU} = h(ID_U||M_{10}||M||M_8||M_9||M_{11}||M_1||M_3||M_2{}'||M_5)$

$$\underset{\longrightarrow}{\{M_{10}, M_8, M_{11}\}}$$

Calculates

$M_7{}' = (M \,.\, r_{S1})$

$M_9{}' = (M_7{}'.\, M_8)$

$ID_U = h(M||M_8||M_9{}'||M_1||M_3||$
$M_4||M_2) \oplus M_{10}$

$M_6{}' = h(ID_U.S)$

$M_{11}{}' = h(ID_U||M_6{}'||M_{10}||M||M_8||$
$M_9{}'||M_1||M_3||M_2||M_5)$

$M_{11}{}'? = M_{11}$

$S_{KS} = h(ID_U, M_{10}||M||M_8||M_9{}'||$
$M_{11}||M_1||M_3||M_2||M_5)$

$$\underset{\longleftrightarrow}{S_{KU} = S_K}$$

Module 2: Login and authentication procedure

4 Security Analysis

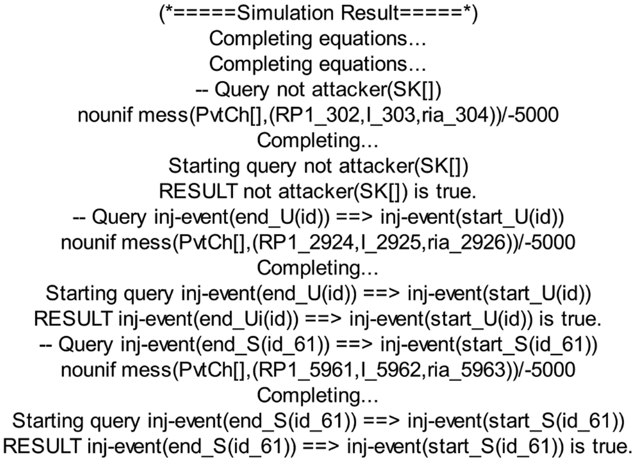
In this section, we will explain and validate our scheme against various attacks. We have proposed a lattice-based authentication scheme for the public cloud environment and used the Real-or-Random (ROR) model to check whether our proposed scheme is secure enough. With informal security analysis, we have further discussed the possible attacks on our proposed scheme.

4.1 Formal Security Analysis Using ProVerif

We have used ProVerif to check whether the session secret is secured, the session key exchanged between the communicating parties is confidential, and the attacker can access the session key at the start of the session. Fig. 2 is the ProVerif simulation results, showing that our protocol is secure.

4.2 Formal Security Analysis Using ROR Model

In this section, we have tested our proposed scheme in the ROR model against a strong adversary $\mathcal{A}$. In the ROR model, five queries have been defined that show the capabilities of $\mathcal{A}$. We let the $\mathcal{A}$ launch various attacks on our protocol. The five queries are defined in Table 2.



```
(*=====Simulation Result=====*)
Completing equations...
Completing equations...
-- Query not attacker(SK[])
nounif mess(PvtCh[],(RP1_302,I_303,ria_304))/-5000
Completing...
Starting query not attacker(SK[])
RESULT not attacker(SK[]) is true.
-- Query inj-event(end_U(id)) ==> inj-event(start_U(id))
nounif mess(PvtCh[],(RP1_2924,I_2925,ria_2926))/-5000
Completing...
Starting query inj-event(end_U(id)) ==> inj-event(start_U(id))
RESULT inj-event(end_Ui(id)) ==> inj-event(start_U(id)) is true.
-- Query inj-event(end_S(id_61)) ==> inj-event(start_S(id_61))
nounif mess(PvtCh[],(RP1_5961,I_5962,ria_5963))/-5000
Completing...
Starting query inj-event(end_S(id_61)) ==> inj-event(start_S(id_61))
RESULT inj-event(end_S(id_61)) ==> inj-event(start_S(id_61)) is true.
```

Figure 2: ProVerif code result

Table 2: Queries and description

Queries	Description
Execute ($\P_e$)	This is in the form of a passive attack, where the exchanged messages are delivered to $\mathcal{A}$.
Send ($\P_s$)	This is in the form of an active attack, where the $\mathcal{A}$ transmits a false message towards legal peers, and the legal peer calculates the values and sends it back to the $\mathcal{A}$.
Corrupt ($\P_c$)	The $\mathcal{A}$ can use this query and obtain the user password or secret information from his/her store data.
Reveal ($\P_r$)	In this query, the $\mathcal{A}$ can access the session key S_{ku}/S_{ks}.
Test ($\P_t$)	In this query, the $\mathcal{A}$ can access the session key partially. Now it is up to the legal peers that can accept the session key from $\mathcal{A}$.

Two participants are involved in our scenario, i.e., the user $\mathcal{P}_{\mathcal{U}}^{\mathcal{T}}$ and public cloud server $\mathcal{P}_{\mathcal{PS}}^{\mathcal{T}}$.

Theorem. The $a\ adv$ can violate the session key of our proposed scheme

$$adv_a = \left| \mathcal{P}r\ (Succ) - \frac{1}{2} \right|$$

$\mathcal{P}r\ (Succ)$ means the probability of success. Our proposed scheme is secure if

$$adv_a \leq \frac{q_{\hbar}^2}{2} + \left(\frac{\P_e + \P_s}{\P} \right)^2 + \left(\P_e + \P_s \right) adv_a^{RE}$$

where Execute query is denoted with $\P_e$. The Send query is denoted by $\P_s$ and Ring learning with errors denoted by adv_a^{RE}.

Proof. In this section, we will play Games with $\mathcal{A}$ to check whether our scheme is secure.

$\mathcal{GAME}_0$. The $\mathcal{A}$ launch an actual attack on the proposed scheme in this game and tries to win the game.

$$\mathcal{adv}_a = \left| \mathcal{Pr}\left(Succ_0\right) - \frac{1}{2} \right|$$

$$= \left| \mathcal{Pr}\left(Succ_0\right) - \mathcal{Pr}\left(Succ_4\right) + \mathcal{Pr}\left(Succ_4\right) - \frac{1}{2} \right|$$

$$= \left| \sum_{a=1}^{4} \mathcal{adv}_a + \mathcal{Pr}\left(Succ_4\right) - \frac{1}{2} \right|$$

$\mathcal{GAME}_1$. The $\mathcal{A}$ intercept transmitted message in the login & authentication phase and try to launch an eavesdropping attack by using Execute query. But ρ and γ are a sample from the Gaussian distribution χ_β. Therefore, we obtain

$$\mathcal{adv}_a = \left| \mathcal{Pr}\left(Succ_0\right) - \mathcal{Pr}\left(Succ_1\right) \right| = 0$$

$\mathcal{GAME}_2$. If collision occurs among transmitted messages {M}, {M_1, M_3, M_4} and {M_{10}, M_8, M_{11}}. However, the random number is generated using $\in Z_q^{ixi}$. Therefore, we obtained the following:

$$\mathcal{adv}_a = \left| \mathcal{Pr}\left(Succ_1\right) - \mathcal{Pr}\left(Succ_2\right) \right| \le \frac{\mathbb{d}_{\hbar}^2}{2} + \left(\frac{\mathbb{q}_e + \mathbb{q}_s}{\mathbb{q}}\right)^2$$

$\mathcal{GAME}_3$. The $\mathcal{A}$ guesses the session key S_K in this game. According to our proposed scheme, the session key is calculated $S_K = h$ (ID_U, M_{10}, M, M_8, M_9, M_{11}, M_1, M_3, M_2, M_5), and the values of each instance belong to $\in Z_q^{ixi}$ and χ_β. Hence,

$$\mathcal{adv}_a = \left| \mathcal{Pr}\left(Succ_2\right) - \mathcal{Pr}\left(Succ_3\right) \right| \le \left(\mathbb{q}_e + \mathbb{q}_s\right) \mathcal{adv}_a^{RE}$$

$\mathcal{GAME}_4$. In this game, the $\mathcal{A}$ used a Test query in order to get the secret values. Thus, we obtain

$$\mathcal{adv}_a = \left| \mathcal{Pr}\left(Succ_3\right) - \mathcal{Pr}\left(Succ_4\right) \right| \le \frac{\mathbb{d}_{\hbar}^2}{2}$$

Therefore, the $\mathcal{A}$ cannot construct the session key S_K.

$$\left|\mathcal{Pr}\left(Succ_4\right)\right| = \frac{1}{2}$$

Hence, our proposed scheme is secure under the assumption of lattice-based Ring learning with errors method.

4.3 Informal Security Analysis

The proposed scheme is based on Lattice-based cryptography, where the users and public cloud servers register themselves using a secure channel. However, if the $\mathcal{A}$ by any chance captures transmitted messages in the login & authentication phase, it still cannot extract secret values. Furthermore, our scheme resists all known attacks, and more details are given below.

1. Provide anonymity. Our scheme provides anonymity to users and public cloud servers. The user's identity is secured using a one-way hash function and public cloud server secret key. The messages that include identity are M6 = h (IDU|| PWU) $\oplus$ S2, and M11 = h (IDU|| M6|| M10|| M|| M8|| M9|| M1|| M3|| M2/|| M5). Therefore, it is challenging for a to break or guess

the secret key and random numbers of a public cloud server. Hence, our proposed scheme provides anonymity.

2. Secure against replay attack. If $\mathcal{A}$ tries to impersonate any communicating peers and try to send a previous session key SK capture message. However, in our scheme, random numbers are generated randomly and fresh for each session. Therefore, the a cannot launch a replay attack on our scheme. Hence, the proposed scheme is secure against replay attacks.
3. Provide mutual authentication. In our proposed scheme, the communicating parties mutually authenticate each other using $S3^{*}? = S3$, $M5/? = M5$, and $M11/? = M11$. If these values are tempered or modified, the connection gets terminated. Thus, our scheme provides mutual authentication.
4. Provide session key. The user and public cloud server calculate the session key $SKU = SKS$. The connection will be terminated if any value is tempered or modified in the session key contraction phase. Therefore, our scheme provides a session key for secure communications.
5. Provide message integrity. The user and public cloud server check the message integrity in the login and authentication phase. The user side checks the messages $S3^{*}? = S3$, $M2/ = (rU \,||PKS)$, $M4/ = (M2/|| \, M3)$, $M5/? = h \, (M|| \, M1|| \, M3|| \, M4)$, and confirms whether these messages are from a public cloud server, while the public cloud server also checks the messages received from a user, such as $M7/ = (M \,|| \, rS1)$, $M9/ = (M7/ \,|| \, M8)$, $M6/ = h(IDU||S)$, and $M11/ = h(IDU|| \, M6/|| \, M10|| \, M|| \, M8|| \, M9/|| \, M1|| \, M3|| \, M2|| \, M5)$. The connection is terminated if any of these messages are modified or tempered. Hence, our scheme provides message integrity.
6. Secure against impersonation attack. In our proposed scheme, the random numbers are generated randomly, and the identity is secured using a one-way hash function and public cloud secret key. Therefore, the $\mathcal{A}$ cannot get any information from the transmitted messages. Hence, our proposed scheme is secure against impersonation attacks.
7. Secure against stolen verifier attack. In the registration phase, the public cloud server did not store any values. Therefore, our scheme is secure against stolen verifier attacks.
8. Secure against offline password attack. Let's suppose that $\mathcal{A}$ extracts all the secret values from the stored data on the user side. However, $\mathcal{A}$ will need a user identity, a public cloud server secret key, and a random number to get the password. Therefore, our scheme is secure against offline password-guessing attacks.
9. Secure against modification attack. In our proposed scheme login and authentication phase, the transmitted messages are verified by both communicating peers. For example, the user side verifies $S3^{*}? = S3$, $M5/? = h(M|| \, M1|| \, M3|| \, M4)$, while the public cloud server-side verifies $M11/? = M11$. If any of these values are modified, the connection will be terminated. Hence, our scheme is secure against modification attacks.
10. Secure against MITM attack. As we prove that our scheme is secure against impersonation and provide message integrity. Hence, our scheme is secure against a man-in-the-middle attack.

5 Performance Analysis

In this part of our research article, we have calculated our protocol's computation and communication costs. After calculating the communication and computation costs, we compare our scheme with the existing protocols.

5.1 Computation Cost

We have considered the work done in [29]**.** The T_{SM} represents the time taken for multiplication with the scalar operation, and T_{GD} means the time taken for Gaussian distribution samples. In contrast, T_M represents the time consumed during multiplication, and T_{MA} is the time taken during multiplication with addition, while T_∂ the time taken during characteristic function and the execution time taken by different operations are listed in Table 3. Considering the execution times shown in Table 3, our proposed scheme's total computation cost is ≅0.003888463 ms. We further calculated the user-side and server-side costs separately in Table 3 and combined them at the end. Fig. 3 shows the comparison of our proposed scheme with the recent existing scheme in terms of computation cost. The results show that our scheme computation cost is lower than the existing schemes.

Table 3: Computation cost of our scheme

User side costs	Server-side costs
$4T_{SM} + T_{GD} + T_{MA} + T_M + T_\partial + 6T_h$	$6T_{SM} + 3T_{GD} + T_{MA} + T_M + T_\partial + 5T_h$
$4(6.655e-6) + 1(0.000615483) + 1(2.9505e-5) + 1.3052e-5 + 3.5515e-5 + 6(0.000180964) = 0.001805959$	$6(0.000298) + 3(7.3503e-5) + 2.549e-6 + 3.07e{-}7 + 6.89e-7 + 5(1.409e-5) = 0.002082504$
Total cost = 0.003888463	

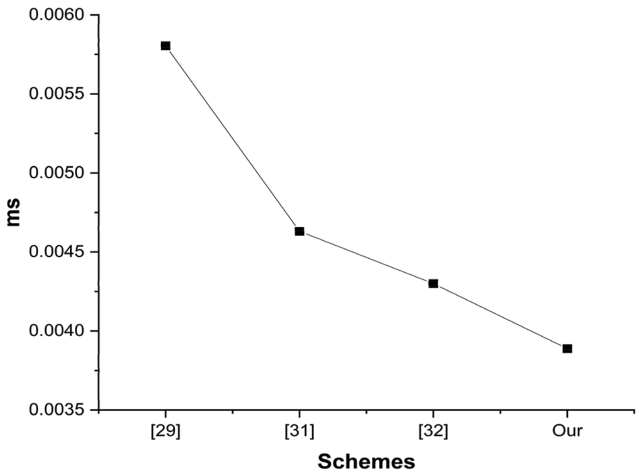


Figure 3: Computation cost

5.2 *Communication Cost*

We have computed the communication cost in this part of our lattice-based authentication protocol. We have considered the work [29] and calculated our communication cost. In our proposed scheme, the user and public cloud server exchange messages in the login and authentication phase. From these transmitted messages, we calculate our total communications cost. The one-way hash function fixed output is 512 bits, the identity is 32 bits, the timestamp is 64 bits, the random number is 256 bits, and the secret value is 256 bits. Therefore, the user-side transmitted messages are $[\{M\} + \{M_{10}, M_8, M_{11}\}]$ and the user-side communication cost equals to $\{1024\} + \{544\} + \{1536\} \cong 3104$ bits. Whereas the public cloud server-side transmitted messages are $[\{M_1, M_3, M_4\}]$ and the communication cost is equal to $[\{1024\} + \{1536\} + \{3072\} \cong 5632]$ bits. Hence, the total communication cost is equal to 8736 bits. Fig. 4 shows the comparison of our proposed scheme with other existing schemes. The results in Fig. 4 show that our scheme is much more lightweight than the existing protocols.

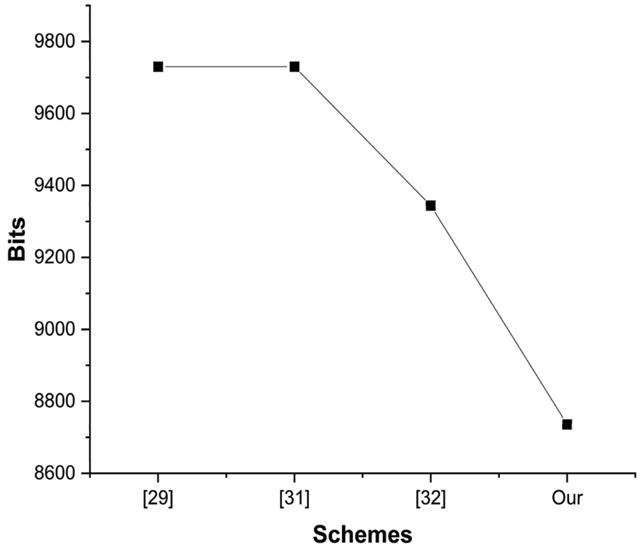


Figure 4: Communication cost

5.3 Security Comparison Analysis

Here, we have examined some contemporary and established authentication systems, both lattice-based and more conventional, and compared them with our approach. Existing lattice-based techniques offer the same level of security as our proposed scheme, but at substantially higher costs in terms of computation and communication. Furthermore, quantum attacks can compromise conventional authentication methods. Table 4 displays the comparative analysis in terms of the security of our system with existing schemes.

Table 4: Security comparison analysis

Features	Schemes								
	[29]	[31]	[32]	[1]	[15]	[35]	[36]	[37]	Our
Resist quantum attacks	✓	✓	✓	x	x	x	✓	x	✓
Provide anonymity	✓	✓	✓	✓	✓	✓	✓	x	✓
Provide mutual authentication	✓	✓	✓	✓	✓	✓	x	✓	✓
Resist insider attacks	✓	✓	✓	✓	✓	✓	x	✓	✓
Resist offline password-guessing attacks	✓	✓	✓	✓	✓	✓	✓	✓	✓
Resist replay attacks	✓	✓	✓	✓	✓	✓	✓	✓	✓
Resist impersonation attacks	✓	✓	✓	✓	✓	x	x	x	✓
Resist DoS attacks	✓	✓	✓	✓	✓	✓	x	✓	✓
Provide untraceability	✓	✓	✓	✓	x	✓	x	x	✓

6 Conclusion

The traditional cryptographic algorithms work great with classical computers. However, things will change once quantum computers come to reality. Shor's technique can easily break traditional cryptographic techniques using quantum computing. Keeping this in mind, we have proposed a lattice-based cryptography technique to authenticate peers in public cloud computing. The security of the proposed scenario has been conducted using the ROR model, while the performance analysis section considers two aspects, communication and computation costs. Both analysis showed that the proposed mechanism is robust, lightweight, efficient, and can easily be implemented for practical use.

In future work, we intend to modify and reduce the proposed scheme's computation and communication costs. Furthermore, we will also try to use the proposed scheme for IoT-enabled devices in a public cloud environment.

Funding Statement: The authors wish to thank the Korean Government (Ministry of Science and ICT) through the National Research Foundation of Korea (NRF) Grant 2021R1A2C1010481.

Conflicts of Interest: The authors declare they have no conflicts of interest to report regarding the present study.

References

[1] N. Khan, J. Zhang and S. U. Jan, "A robust and privacy-preserving anonymous user authentication scheme for public cloud server," *Security and Communication Networks*, vol. 2022, pp. 1–14, 2022.

[2] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari *et al.,* "Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2884–2895, 2017.

[3] S. Qiu, D. Wang, G. Xu and S. Kumari, "Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1338–1351, 2020.

[4] M. Fakroon, M. Alshahrani, F. Gebali and I. Traore, "Secure remote anonymous user authentication scheme for smart home environment," *Internet of Things*, vol. 9, pp. 100158, 2020.

[5] B. Ying and A. Nayak, "Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography," *Journal of Network and Computer Applications*, vol. 131, pp. 66–74, 2019.

[6] M. Nikooghadam, R. Jahantigh and H. Arshad, "A lightweight authentication and key agreement protocol preserving user anonymity," *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13401–13423, 2017.

[7] R. Amin, T. Maitra, D. Giri and P. Srivastava, "Cryptanalysis and improvement of an RSA based remote user authentication scheme using smart card," *Wireless Personal Communications*, vol. 96, no. 3, pp. 4629–4659, 2017.

[8] M. Luo, Y. Zhang, M. K. Khan and D. He, "A secure and efficient identity-based mutual authentication scheme with smart card using elliptic curve cryptography," *International Journal of Communication Systems*, vol. 30, no. 16, pp. e3333, 2017.

[9] T. Maitra, M. S. Obaidat, R. Amin, S. H. Islam, S. A. Chaudhry *et al.,* "A robust ElGamal-based password-authentication protocol using smart card for client-server communication," *International Journal of Communication Systems*, vol. 30, no. 11, pp. e3242, 2017.

[10] S. H. Islam, "Design and analysis of an improved smartcard-based remote user password authentication scheme," *International Journal of Communication Systems*, vol. 29, no. 11, pp. 1708–1719, 2016.

[11] T. Maitra, M. S. Obaidat, S. H. Islam, D. Giri and R. Amin, "Security analysis and design of an efficient ECC-based two-factor password authentication scheme," *Security and Communication Networks*, vol. 9, no. 17, pp. 4166–4181, 2016.

[12] S. D. Kaul and A. K. Awasthi, "Security enhancement of an improved remote user authentication scheme with key agreement," *Wireless Personal Communications*, vol. 89, no. 2, pp. 621–637, 2016.

[13] M. Qi and J. Chen, "New robust biometrics-based mutual authentication scheme with key agreement using elliptic curve cryptography," *Multimedia Tools and Applications*, vol. 77, no. 18, pp. 23335–23351, 2018.

[14] A. Hassan, N. Eltayieb, R. Elhabob and F. Li, "An efficient certificateless user authentication and key exchange protocol for client-server environment," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 6, pp. 1713–1727, 2018.

[15] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma *et al.,* "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9390–9401, 2020.

[16] W. -i. Bae and J. Kwak, "Smart card-based secure authentication protocol in multi-server IoT environment," *Multimedia Tools and Applications*, vol. 79, no. 23, pp. 15793–15811, 2020.

[17] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay and Y. Park, "An efficient, anonymous and robust authentication scheme for smart home environments," *Sensors*, vol. 20, no. 4, pp. 1215, 2020.

[18] L. Zhou, X. Li, K. -H. Yeh, C. Su and W. Chiu, "Lightweight IoT-based authentication scheme in cloud computing circumstance," *Future Generation Computer Systems*, vol. 91, pp. 244–251, 2019.

[19] R. Martínez-Peláez, H. Toral-Cruz, J. R. Parra-Michel, V. García, L. J. Mena *et al.,* "An enhanced lightweight IoT-based authentication scheme in cloud computing circumstances," *Sensors*, vol. 19, no. 9, pp. 2098, 2019.

[20] S. Kumari, X. Li, F. Wu, A. K. Das, K. -K. R. Choo *et al.,* "Design of a provably secure biometrics-based multi-cloud-server authentication scheme," *Future Generation Computer Systems*, vol. 68, pp. 320–330, 2017.

[21] S. S. Sahoo, S. Mohanty and B. Majhi, "A secure three factor based authentication scheme for health care systems using IoT enabled devices," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 1419–1434, 2021.

[22] A. G. Reddy, E. -J. Yoon, A. K. Das, V. Odelu and K. -Y. Yoo, "Design of mutually authenticated key agreement protocol resistant to impersonation attacks for multi-server environment," *IEEE Access*, vol. 5, pp. 3622–3639, 2017.

[23] R. Amin and G. Biswas, "Design and analysis of bilinear pairing based mutual authentication and key agreement protocol usable in multi-server environment," *Wireless Personal Communications*, vol. 84, no. 1, pp. 439–462, 2015.

[24] R. Ali and A. K. Pal, "An efficient three factor–based authentication scheme in multiserver environment using ECC," *International Journal of Communication Systems*, vol. 31, no. 4, pp. e3484, 2018.

[25] F. Wang, G. Xu, C. Wang and J. Peng, "A provably secure biometrics-based authentication scheme for multiserver environment," *Security and Communication Networks*, vol. 2019, pp. 1–15, 2019.

[26] R. Amin, S. H. Islam, N. Kumar and K. -K. R. Choo, "An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks," *Journal of Network and Computer Applications*, vol. 104, pp. 133–144, 2018.

[27] A. H. Moon, U. Iqbal and G. M. Bhat, "Mutual entity authentication protocol based on ECDSA for WSN," *Procedia Computer Science*, vol. 89, pp. 187–192, 2016.

[28] P. Chandrakar and H. Om, "An extended ECC-based anonymity-preserving 3-factor remote authentication scheme usable in TMIS," *International Journal of Communication Systems*, vol. 31, no. 8, pp. e3540, 2018.

[29] Q. Feng, D. He, S. Zeadally, N. Kumar and K. Liang, "Ideal lattice-based anonymous authentication protocol for mobile devices," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2775–2785, 2018.

[30] S. Akleylek and M. Soysaldı, "A new lattice-based authentication scheme for IoT," *Journal of Information Security and Applications*, vol. 64, pp. 103053, 2022.

[31] 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.

[32] D. S. Gupta, S. Ray, T. Singh and M. Kumari, “Post-quantum lightweight identity-based two-party authenticated key exchange protocol for internet of vehicles with probable security,” *Computer Communications*, vol. 181, pp. 69–79, 2022.

[33] M. Shabbir, F. Ahmad, A. Shabbir and S. A. Alanazi, “Cognitively managed multi-level authentication for security using fuzzy logic based quantum key distribution,” *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 4, pp. 1468–1485, 2022.

[34] T. Hasan, F. Ahmad, M. Rizwan, N. Alshammari, S. A. Alanazi *et al.,* “Edge caching in fog-based sensor networks through deep learning-associated quantum computing framework,” *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1–17, 2022.

[35] B. Bera, D. Chattaraj and A. K. Das, “Designing secure blockchain-based access control scheme in IoT-enabled internet of drones deployment,” *Computer Communications*, vol. 153, pp. 229–249, 2020.

[36] J. Srinivas, A. K. Das, N. Kumar and J. J. Rodrigues, “TCALAS: Temporal credential-based anonymous lightweight authentication scheme for internet of drones environment,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 6903–6916, 2019.

[37] Z. Ali, S. Hussain, R. H. U. Rehman, A. Munshi, M. Liaqat *et al.,* “ITSSAKA-MS: An improved three-factor symmetric-key based secure AKA scheme for multi-server environments,” *IEEE Access*, vol. 8, pp. 107993–108003, 2020.