

Received 14 August 2023, accepted 7 October 2023, date of publication 19 October 2023,
date of current version 11 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3325886

RESEARCH ARTICLE

A Construction of Three Party Post Quantum Secure Authenticated Key Exchange Using Ring Learning With Errors and ECC Cryptography

DHARMINDER CHAUDHARY¹, (Member, IEEE), UDDESHAYA KUMAR²,
AND KASHIF SALEEM³, (Member, IEEE)

¹Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Chennai 601103, India

²Department of Mathematics, Gautam Buddha University, Greater Noida 201312, India

³Department of Computer Science and Engineering, College of Applied Studies and Community Service, King Saud University, Riyadh 11362, Saudi Arabia

Corresponding authors: Kashif Saleem (ksaleem@KSU.EDU.SA) and Dharminder Chaudhary (manndharminder999@gmail.com)

This work was supported by the King Saud University, Riyadh, Saudi Arabia, under Researchers Supporting Project number RSPD2023R697.


ABSTRACT A three-party authenticated key exchange protocol enables two entities to agree on a session key with the help of a dedicated server over a public channel. Shor's algorithm is a big threat to existing authenticated key exchange protocols. Lattice based cryptography plays a very important role in designing authentication and key agreements secure against the threat of quantum attacks. However, it is not an easy job to design quantum resistant password based three party protocols due to the high demand for security requirements and the limited resources nature of mobile devices. In this article, we have proposed a new post quantum three party key exchange based on ring learning with errors assumption. This protocol is motivated by Islam et al.'s authenticated key exchange protocol. Their protocol is not secure against stolen smartcard attacks, or password guessing attacks, and can't provide user anonymity. Anonymous communication is a big requirement for practical applications like e-healthcare services/smart vehicular communication. This paper also contains the performance analysis of the proposed protocol along with other relevant protocols.

INDEX TERMS Key exchange, authentication, ring learning, cryptography.

I. INTRODUCTION

An adversary (\mathcal{A}) always tries to listen to the communication whenever two parties Alice and Bob exchange messages over a public channel. To overcome this problem, an authenticated key agreement protocol is used to send a message between Alice and Bob, and a secure connection is established with the help of a session key. The connection between mobile users is more secure and privacy between them is obtained because of the high entropy of the session keys, and if the adversary tries to monitor the connection, then he cannot interrupt their communication. The authenticated key agreement protocol is classified into two categories, two parties, and multiparty. There are many papers on two party, and three party authenticated key agreements based on number theoretic assumptions. Soon quantum computers

will be available, so researchers can categorize cryptography into two parts, the first one is before the existence of quantum computers, and the second one is with the existence of quantum computers. The Shor's factoring algorithm is an efficient algorithm for solving prime factorization of a given number in polynomial time on a quantum computer. But, lattices are a rich source of assumptions that are secure against quantum computers. Lattices have become a highly appealing basis for cryptography during the last decade. To achieve security against quantum attacks, this paper focuses on three party post quantum authenticated key agreements. Three party authentication services are platforms that provide authentication for web applications, such as user registration, login, password change, social web login, email verification, and more. We have studied a number of three party authenticated key agreement protocols. There are only a few protocols available that are secure against quantum computers. Islam et al.'s [17] is the first who

The associate editor coordinating the review of this manuscript and approving it for publication was Junggab Son .

recently proposed a three party authenticated key agreement protocol. He has claimed that the protocol is secure to (a) user impersonation attacks, (b) smartcard stolen attacks, (c) password guessing attacks, and (d) user anonymity and traceability, but we found they are not able to achieve these security attributes. Islam et al.'s [17] protocol is vulnerable to (a) user impersonation attack, (b) smartcard stolen attack, (c) password guessing attack, and (d) user anonymity and traceability. Therefore, This paper contains a method that inherits Islam et al.'s approach and effectively repels the potential known assaults in order to address the flaws of their original scheme. Moreover, it is demonstrated that the proposed technique is safe even under the hard "Ring Learning with Errors" assumption. A legitimate proof for the system is provided, and it maintains all of the security features. In the registration phase, this paper uses elliptic curve cryptography that provides security against password guessing. In the authentication phase, the protocol used assumption ring learning with errors secure against the threat of quantum attacks.

The rest of the paper is organized as Section II comprehensively reviews the related work. Section III elaborates the motivations to conduct this research work and the contributions of this paper. Section IV presents the preliminaries. Section V describes the Islam et. al.'s scheme. The security weaknesses of Islam et. al.'s scheme are explained in Section VI. Section VII describes the proposed Three Party Post Quantum Secure Authenticated Key Exchange Using Ring Learning with Errors and ECC Cryptography. Section VIII shows the informal security analysis and formal security analysis in Section IX. The security comparisons and performance evaluation are given in Section X. Section XI concludes the paper with the future work.

II. RELATED WORK

In 2014, Peikert et al. [24] proposed a post quantum key exchange protocol. He proposed a new unbiased reconciliation technique. Peikert [24] presents an efficient and provably secure set of lower level primitives for practical post-quantum cryptography. Zhang et al. [30] proposed an authenticated key exchange algorithm. But, this protocol uses long term server keys again and again during the communication. It leads to the well known signal leakage attack. Kirkwood et al. [19] are the researchers who observed that the reuse of secret keys is dangerous in ring learning with errors in key exchange. This result opens a new track for the researchers, but it lacks a complete description. In 2016, Fluhrer [14] proposed the new innovative idea of key mismatch for ring learning with errors based protocols revising public/private keys. This idea is used to recover the private key of the honest party. The match or mismatch properties play a very important role in recovering the established key between two parties. But, this attack becomes useless when the key is established using the least significant bits of equal length keys. Taking inspiration from Fluhrer [14], in 2017, Ding et al. [8] introduced the idea of signal leakage attack for ring learning with errors based key

exchange reusing public/private keys. Ding et al. [8] proposed a provably secure password authentication and key exchange under ring learning with errors assumption. In this idea, an adversary analyzes 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 the least significant bits of approximately equal bit lengths. The number of steps required " $2q$ " to retrieve the private key of the server. Next year 2018, Ding et al. [9] introduced that 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 " $0 < c < q$ " is some constant. In 2018, Feng et al. [13] introduced an authenticated key exchange for mobile communication, but it lacks authentication. In 2020, Dabra et al. [3] analyzed the security of Feng et al. [13], and they discussed signal leakage attack on the protocol [13]. But, Dabra et al. [3] protocol possesses a weak login and authentication phase that leads to a denial of service attack (DoS). In 2020, Dharminder et al. [5] proposed a three factor authenticated key exchange protocol. However, it suffers from the signal leakage attack. In the same year, Islam et al. [16], [18] proposed two quantum safe two-party authenticated key exchanges, but [16] was found vulnerable to signal leakage attack [4]. Currently, Wang et al. [27] proposed an efficient quantum attacks resistant two factor authentication protocol for mobile devices. It uses three messages of exchange that create communication overhead. This protocol also uses more operations and creates extra computation overhead. In 2022, Dharminder et al. [6] proposed a lattice based secure reconciliation enabling key exchange for the Internet of Things (IoTs) environment. In 2023, Kumar et al. [21] proposed a new post quantum key exchange based on a variant of lattice assumption, the ring learning errors. This protocol ensures both authentication and key agreement. This protocol needs just two messages in exchange for authentication and key agreement. To make the system efficient, Basu et al. [2] proposed a Module Learning With Rounding based authentication and key exchange for two-party communication. But, all the above protocols are two party authenticated key agreements.

III. MOTIVATIONS AND CONTRIBUTIONS

To fill this gap, Islam et al. [17] proposed a new three-party protocol based on ring learning errors, claiming that their protocol is not only secure against the above attacks but also provides security against quantum computer attacks. We have found that Islam et al.'s protocol fails to provide anonymity to the users. It is vulnerable to smartcard loss attacks, password guess attacks, and impersonation attacks. In the year 2023, Rewal et al. [25] proposed a quantum attack resistant authentication protocol for mobile users using ideal lattices. They claimed for the improvement of

TABLE 1. Basic notations required for the proposed scheme.

Notation	Description
\mathcal{U}_i	User-i with $i \in \{a, b\}$
S_j	Server-j
e	Server's public key
s	Server's secret key
R_q	Finite ring of polynomials
$Cha(\cdot)$	Characteristic function
$E(F_q)$	Elliptic curve over finite field
χ_δ	Discrete Gaussian
δ	Standard deviation
A_d	Adversary
ID_i	Identity of \mathcal{U}_i
ω_i	Biometric imprint of \mathcal{U}_i
PW_i	Password of \mathcal{U}_i
$h(\cdot)$	Cryptographic hashing
$G(\cdot)$	Fuzzy Extractor
\oplus	Bitwise XOR
\parallel	String concatenation

the efficiency of lattice-based authenticated key exchange protocol and the security against password-guessing attacks. However, their scheme does not provide anonymity, and they have used biometric hashing which is a costly operation. The secret value is directly XORed with a biometric value which means it can't provide three factor security. Moreover, smartphone fingerprint scanners often rely on partial matches. Researchers have found that it's possible to create "master prints" that match the partials of many people and can thus give access to a large number of user accounts.

IV. PRELIMINARIES

This section contains some basic notations (see Table (1)). Consider $n = 2^t$, where $t \in \mathbf{Z}$ is a security parameter. An irreducible polynomial is define as $(x^n + 1) \in \mathbf{Z}[x]$ over \mathbf{Z} . The rings of polynomial is indicated as $\mathbf{Z}_q[x]$ over \mathbf{Z}_q , where $q \bmod 2n \equiv 1$ ($q = 2^{\omega(\log_2 n)} + 1$) is a prime modulus. The rings of integer polynomials modulo is defined as $(x^n + 1)$ over \mathbf{Z} is $\mathbf{R} = \mathbf{Z}[x]/(x^n + 1)$. The rings of polynomials $\mathbf{R}_q = \mathbf{Z}_q[x]/(x^n + 1)$ with the same modulus and each coefficient is reduced modulo q over \mathbf{Z}_q . \mathbf{R} has q^n elements, each of which is a polynomial of degree less than n with $\mathbf{Z}_q = \{0, 1, \dots, q-1\}$ coefficients. A fixed real number β is given, where $\beta > 0$. The discrete Gaussian distribution is denoted as x_β over \mathbf{R}_q . The definition of the auxiliary modular function $\mathbf{Mod}_2: \mathbf{Z}_q \times \{0, 1\} \rightarrow \{0, 1\}$ can be written as $\mathbf{Mod}_2(v, d) = (v + d \cdot \frac{q-1}{2}) \bmod q \bmod 2$, where $v \in \mathbf{Z}_q$ and $d = \mathbf{Cha}(v)$ [30].

Lemma 1: The security parameter is given by n , consider $q = (2^{\omega(\log_2 n)} + 1) > 2$ be a odd prime. Consider that v is drawn at uniformly at random from the modular group \mathbf{Z}_q . For $c, d \in \{0, 1\}$ and $c, \omega \in \mathbf{Z}_q$ the output distribution of $\mathbf{Mod}_2(v + \omega, d)$ given $\mathbf{Cha}(v)$ is statistically close to uniform on $\{0, 1\}$ [30].

Lemma 2: Given q and $c, e \in \mathbf{R}_q$ such that $|e| < \frac{q}{8}$, we have $\mathbf{Mod}_2(c, \mathbf{Cha}(c)) = \mathbf{Mod}_2(\omega, \mathbf{Cha}(c))$, where $\omega = c + 2e$ [30].

On \mathbf{R}_q , \mathbf{Cha} and \mathbf{Mod}_2 are easily extendable functions as: Given $c = c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1} \in \mathbf{R}$, we considered it as a vector $c =$

$(c_0, c_1, \dots, c_{n-1})$. For $v = (v_0, v_1, \dots, v_{n-1}) \in \{0, 1\}^n$, we have $\mathbf{Cha}(c) = (\mathbf{Cha}(c_0), \mathbf{Cha}(c_1), \dots, \mathbf{Cha}(c_{n-1}))$, $\mathbf{Mod}_2(c, v) = (\mathbf{Mod}_2(c_0, v_0), \dots, \mathbf{Mod}_2(c_{n-1}, v_{n-1}))$.

Definition 1 Ring Learning With Errors (RLWE): Consider $s \in \mathbf{R}_q$ and $\text{mathbf{A}}_{\beta, x_\beta}$ are distributions over $(c, c.s + 2.e) \in \mathbf{R}_q \times \mathbf{R}_q$, $c \in \mathbf{R}_q$ is chosen uniformly at random, and $e \leftarrow x_\beta$. A polynomial time-limited algorithm \mathcal{B} cannot distinguish \mathbf{A}_{s, x_β} from the uniform distribution on $\mathbf{R}_q \times \mathbf{R}_q$ given a fixed sample size from x_β and polynomial many samples. \hat{A}

A. ELLIPTIC CURVE CRYPTOGRAPHY FUNDAMENTALS

An elliptic curve over \mathbf{Z}_q (where $q > 3$) is defined as a set of all pairs (x, y) that belong to \mathbf{Z}_q and meet the equation $y^2 \equiv x^3 + a.x + b \pmod{q}$ along with an imaginary point referred to as infinity (\mathcal{O}). The values a and b belong to \mathbf{Z}_q , and the condition $4.a^3 + 27.b^2 \not\equiv 0 \pmod{q}$ must be satisfied. The term "elliptic curve" implies that the curve has no singularities. In terms of geometry, this means that the plot does not cross over itself or have any vertices, which is guaranteed when the discriminant of the curve, $4a^3 + 27b^2$, is not equal to zero.

B. DISCRETE LOGARITHM PROBLEM WITH ELLIPTIC CURVES

The Elliptic Curve Discrete Logarithm Problem (ECDLP) involves a given elliptic curve E . The problem is to find an integer d , where $(1 \leq d \leq \#E)$ and $\#E$ is the number of points on the curve, such that the primitive P added to itself d times equals T . where T is another element on the curve.

$$T = dP = P + P + \dots + P \text{ (d times)} \tag{1}$$

In cryptography, d is viewed as a private integer key, and public key T is represented as a point on the curve with coordinates (x_T, y_T) . The ECDLP differs from the discrete logarithm problem for \mathbf{Z}_q^* , where both keys are integers. The expression $T = dP$, called point multiplication, is just a notation for repeatedly applying the group operation ($y^2 \equiv x^3 + a.x + b \pmod{q}$), not the actual multiplication of an integer d and a curve point P .

C. FUZZY EXTRACTOR

This paper contains the extraction mechanism from the biometric imprints. A fuzzy extractor is used to generate keys from biometric imprints and other noisy data. The generated key can be used to construct any cryptographic application because its information entropy is sufficient for security. The extraction method Fext [10] is opted, which enables to extraction of a random binary string that has been chosen uniformly. This extractor allowed to extraction of personal information from the physiological input like biometric imprints with a given error margin. In the regeneration, the Fext algorithm retrieves a similar biometric key string for noisy biometric imprints using a stored string. The fuzzy extractor contains two components $Gen(\cdot)$, and

$GRep(\cdot)$, respectively. The algorithm $Gen(\cdot)$ is a probabilistic algorithm that takes input biometric imprints ω , and generates $Gen(\omega) = (B_i, B_i^*)$, where B_i is a private key, and B_i^* is the corresponding helper string. However, B_i will be the same with the assistance of B_i^* even if the biometric threshold value satisfies $|\omega' - \omega| \leq \Delta\omega$. The algorithm $GRep(\cdot)$ uses a noisy biometric imprints ω' , and the binary string B_i^* to generate $GRep(\omega', B_i^*) = B_i$ if $|\omega' - \omega| \leq \Delta\omega$ holds.

V. REVIEW OF ISLAM et. al.'s SCHEME

A. INITIALIZATION PHASE

- An odd prime number $q > 16\beta^2 n^{\frac{3}{2}}$ is chosen by server S , where $q \bmod 2n \equiv 1$ and $n = 2^t \in Z_q$, where $t \in Z$ is a positive non zero.
- Server S chooses $s \in Z_q$ as a long term secret, SHA-512 hash functions H_1, H_2, H_3 and a fix element $x \in \chi_\beta$ randomly.
- Finally, server S declares the public parameters $\langle q, n, a, \chi_\beta, H_1, H_2, H_3 \rangle$ after choosing a fixed random element a from R_q .

B. REGISTRATION PHASE

In order to get the services, user $U_i : i \in \{a, b\}$ have to register themselves to the server S . For that U_i communicate to the server through a secure channel:

- U_i chooses ID_i, PW_i and compute $L_i = H_1(PW_i, b_i)$ after choosing $b_i \in Z_q$ randomly. Then send ID_i, L_i to S .
- S computes $D_i = H_1(ID_i, s), X_i = H_1(ID_i, L_i), N_i = X_i \oplus D_i, V_i = H_1(X_i, D_i)$ and send $\langle N_i, V_i \rangle$ to i .
- U_i stores $\langle b_i, V_i, N_i, q, a, n, \chi_\beta, H_1, H_2, H_3 \rangle$ in their mobile application.

C. AUTHENTICATED KEY AGREEMENT PHASE

To opt services $U_i : i \in \{a, b\}$ have to agree on a shared session key. For that, they have to follow the following steps:

- User U_a initiate the session with login into mobile application. For that U_a has to input ID_a, PW_a in her/his mobile application. Then mob. app. computes $L_A^* = H_1(PW_a, b_A), X_A^* = H_1(ID_a, L_A), D_A^* = N_A \oplus X_A^*$ and then verify $V_A \stackrel{?}{=} V_A^* = H_1(X_A^*, D_A^*)$. If verification fails the session otherwise generates r_A, f_A from χ_β randomly and computes $x_A = a.r_A + 2.f_A, \Sigma_A = H_2(ID_a, T_A, x_A, D_A)$ where T_A is the time stamp. Now finally sends $\langle ID_A, request \rangle$ to user U_b and $\langle ID_a, T_A, x_A, \Sigma_A \rangle$ to S .
- After getting the request message from U_a, U_b has to login into their mobile application by input their ID_b, PW_b . Mobile application then verify $V_B \stackrel{?}{=} V_B^* = H_1(X_B^*, D_B^*)$ by computing $L_B^* = H_1(PW_b, b_B), X_B^* = H_1(ID_b, L_B), D_B^* = N_B \oplus X_B^*$. If verification gets success, it generates r_B, f_B from χ_β randomly and sends $\langle ID_b, T_B, x_B, \Sigma_B \rangle$ to S after computing $x_B = a.r_B + 2.f_B, \Sigma_B = H_2(ID_b, T_B, x_B, D_B)$ where T_B is the time stamp otherwise stops the session.

- After getting the message from users U_a and U_b, S firstly verify the authenticity of users by $\Sigma_A = ?\Sigma_A^* = H_2(ID_a, T_A, x_A, H_1(ID_a, s)), \Sigma_B \stackrel{?}{=} \Sigma_B^* = H_2(ID_b, T_B, x_B, H_1(ID_b, s))$.

If either $\Sigma_A \neq \Sigma_A^*$ or $|T_A - T_A'| > \Delta T$, S ends U_a 's session. Otherwise computes $\Sigma_{S_A} = H_2(ID_S, T_{S_A}, x_B, H_1(ID_a, s))$, where T_{S_A} is the timestamp. Now sends $\langle ID_S, T_{S_A}, x_B, \Sigma_{S_A} \rangle$ to U_a .

In a similar way if either $\Sigma_B \neq \Sigma_B^*$ or $|T_B - T_B'| > \Delta T$, S ends U_b 's session. Otherwise computes $\Sigma_{S_B} = H_2(ID_S, T_{S_B}, x_A, H_1(ID_b, s))$, where T_{S_B} is the timestamp. Now sends $\langle ID_S, T_{S_B}, x_A, \Sigma_{S_B} \rangle$ to U_b .

- U_a checks $\Sigma_{S_A}^* = H_2(ID_S, T_{S_A}, x_B, D_A)$ and $|T_{S_A} - T_{S_A}'| < \Delta T$, if either of these fails then abort the session otherwise compute $t_A = r_A.x_B, w_A = Cha(t_A), \sigma_A = Mod_2(t_A, w_A), \alpha_A = H_2(x_A, x_B, w_A, \sigma_A)$ and sends $\langle ID_a, w_A, \alpha_A \rangle$ to U_b .
- After getting the message from S , firstly U_b has to verify $\Sigma_{S_B}^* = H_2(ID_S, T_{S_B}, x_A, D_B)$ and $|T_{S_B} - T_{S_B}'| < \Delta T$, if either of these fails then U_b ends the session else compute $t_B = r_B.x_A, w_B = Cha(t_B), \sigma_B = Mod_2(t_B, w_B), \alpha_B = H_2(x_B, x_A, w_B, \sigma_B)$ and sends $\langle ID_b, w_B, \alpha_B \rangle$ to U_a .
- In this step U_a gets $\langle ID_b, w_B, \alpha_B \rangle$ from U_b and computes $\sigma_B^* = Mod_2(t_A, w_B), \alpha_B^* = H_2(x_B, x_A, w_B, \sigma_B^*)$. Now verify $\alpha_B^* \stackrel{?}{=} \alpha_B$. If these are not equal abort the session else computes $sid = (ID_a, ID_b, x_A, x_B, w_A, w_B, \alpha_A, \alpha_B)$ and $SK_{AB} = H_3(sid, \sigma_A^*, \sigma_B)$.
- After getting the message $\langle ID_a, w_A, \alpha_A \rangle$ from $U_a, \sigma_A^* = Mod_2(t_B, w_A), \alpha_A^* = H_2(x_A, x_B, w_A, \sigma_A^*)$. Now verify $\alpha_A^* \stackrel{?}{=} \alpha_A$. If these are not equal abort the session otherwise computes $sid = (ID_a, ID_b, x_A, x_B, w_A, w_B, \alpha_A, \alpha_B)$ and $SK_{BA} = H_3(sid, \sigma_A, \sigma_B^*)$.

VI. SECURITY PITFALLS OF ISLAM et al.'s SCHEME

In the paper [16], Islam et al. use the Dolev-Yao model [11] with Kocher et al. model [20](side channel attack). He assumes that an adversary has the following capabilities:

- A_d has access to an open public network, he can monitor and store every communication sent between U_a, U_b , and S via an open public network.
- A_d has the ability to alter, edit, and replay the communications that are sent between U_a, U_b , and S via an open, public network.
- The mobile device of the user can be stolen or accessed by the A_d . From which A_d may extract the user's credentials by using various techniques.
- A_d can use the dictionary attack in order to guess the passwords of the users.

A. STOLEN SMART-CARD ATTACK

According to the threat model described in paper [17], user U_a 's mobile device may be accessed by A_d , who may then extract the user's credentials. The password guessing attack can be tried using these credentials and the messages

exchanged across the public channel. To implement it, A_d extract $\{N_i, V_i, b_i, H_1(\cdot)\}$ from mobile application of the user. The following steps have been followed by A_d : (a) It guesses the password says PW'_i . (b) calculates $L'_i = H_1(PW'_i, b_i)$, $X'_i = H_1(ID_i, L'_i)$, $D'_i = N_i \oplus X'_i$ and $V'_i = (H_1(X'_i, D'_i))$. (c) at last verifies $V_i = ?V'_i$. The guessed password for A_d is the real password if verification is successful. If not, they must repeat these actions until they are successful.

B. USER ANONYMITY AND TRACEABILITY

In the Authenticated key agreement phase, users \mathcal{U}_a and \mathcal{U}_b uses their original identity ID_a and ID_b , when messages are exchanged through public channel. So user's anonymity does not exist in [17]. Also, it allows A_d to separate the targeted user in each login session.

VII. PROPOSED THREE PARTY POST QUANTUM SECURE AUTHENTICATED KEY EXCHANGE USING RING LEARNING WITH ERRORS AND ECC CRYPTOGRAPHY

This section describes the proposed protocol based on "ring learning with error" for mobile devices. The protocol comprises four phases including the set-up phase, registration phase, login, and authentication are discussed in Figure (1).

A. SETUP PHASE

Server S runs the setup algorithm to produce system settings during setup and chooses its master secret key in the manner described below:

- 1) S chooses a sizeable prime number q with an integer "n", where "n" is of the form of a power of two.
- 2) Then S chooses χ_δ the Gaussian distribution with $\delta > 0$ as standard deviation.
- 3) S chooses $\alpha \in \mathcal{Q}_q$ and computes public key $\varrho = \alpha s + 2e$ after sampling $s, e \leftarrow \chi_\delta$ randomly.
- 4) S selects $h : \{0, 1\}^* \rightarrow \{0, 1\}^\gamma$ as hash function with output of γ length, and an elliptic curve $E(F_p)$ with point P as a generator for the elliptic curve group.
- 5) At last S announce $\{n, q, \alpha, \chi_\delta, \varrho, h(\cdot), P\}$ as public parameters keeping s as a secret key.

B. REGISTRATION PHASE

User \mathcal{U}_i , where $i \in \{a, b\}$, must register before using any services. All messages sent during the registration phase are sent through a secure channel. The following actions are required to ensure registration.

- 1) User \mathcal{U}_i selects ID_i as identity, PW_i password, and imprints biometric ω and generates $Gen(\omega) = (B_i, B_i^*)$, and computes $A_i = h(ID_i || PW_i || B_i) \cdot P$, where P is the point on the elliptic curve, and sends ID_i, A_i to the server.
- 2) When the server receives ID_i, A_i it computes SID_i , where $SID_i = h(ID_i || s)$, $C_i = SID_i \oplus h(A_i)$, stores $h(ID_i)$ and sends $C_i, h(\cdot)$ to the user \mathcal{U}_i .
- 3) User \mathcal{U}_i receives $C_i, h(\cdot)$, where $i \in \{a, b\}$ and computes $A_i = h(ID_i || PW_i || B_i) \cdot P$, $SID_i = C_i \oplus h(A_i)$, $V_i =$

$h(ID_i || PW_i || B_i || SID_i)$, and stores $\{C_i, V_i, D_i, B_i^*, h(\cdot)\}$ into the smart phone app.

Correctness Server authenticate \mathcal{U}_a by verifying $v_a = ?v'_a$ where $v_a = h(Aid_a || z_a || m_a || ID_a)$ and $v'_a = h(Aid_a || z_a || m'_a || ID'_a)$. Since \mathcal{U}_a sends $\{z_a, v_a, Aid_a, c_a\}$ to the server. So server needs to calculate m_a, ID_a , for that, server uses Z_a, c_a and Aid_a . Since $m_a = Mod_2(k_a, c_a)$, so to get correct m_a, k_a and k'_a should follow the inequality $|k_a - k'_a| < \frac{q}{8}$.

$$k_a = r_a \cdot \varrho = r_a \cdot \alpha \cdot s + 2e \cdot r_a \quad (2)$$

$$k'_a = z_a \cdot s = \alpha \cdot r_a \cdot s + 2v_a \cdot s \quad (3)$$

From equation (2) and (1), we obtained

$$|k_a - k'_a| = 2|e \cdot r_a - v_a \cdot s| \quad (4)$$

By applying Lemma 1 and Lemma 2, we have

$$\begin{aligned} |e \cdot r_a - v_a \cdot s| &\leq |e \cdot r_a| + |v_a \cdot s| \leq \sqrt{n} \cdot \|e\| \cdot \|r_a\| \\ &\quad + \sqrt{n} \cdot \|v_a\| \cdot \|s\| \\ &< \sqrt{n} \cdot \sqrt{n} \cdot \delta \cdot \sqrt{n} \cdot \delta + \sqrt{n} \cdot \sqrt{n} \cdot \delta \cdot \sqrt{n} \cdot \delta \\ &= 2 \cdot \sqrt[3]{n} \cdot \delta^2, \end{aligned}$$

where $n \ll q$ and $\delta = \omega(\sqrt{\log n})$. So

$$|e \cdot r_a - v_a \cdot s| \leq 2\sqrt[3]{n} \cdot \delta^2 < \frac{q}{8}. \quad (5)$$

Now by Lemma 3, we have

$$\phi_2(k_a, c_a) = \phi_2(k'_a, c_a) \quad (6)$$

From equation (5), we have

$$\begin{aligned} v_a &= h(Aid_a || z_a || k_a || m_a || ID_a) \\ &= h(Aid_a || z_a || k'_a || m'_a || ID'_a) = v'_a. \end{aligned} \quad (7)$$

Similarly server authenticate \mathcal{U}_b by verifying v_b .

Server sends $\{z_b, N_a, v_s\}$ to \mathcal{U}_a , then \mathcal{U}_a verifies server and \mathcal{U}_b by verifying v_s , where $v_s = h(ID_a || ID_b || s_i)$. For this \mathcal{U}_a needs to compute correct s_i and since he has SID_a and m_a , he can compute s_i correctly.

VIII. INFORMAL SECURITY ANALYSIS

A. MAN IN THE MIDDLE ATTACK

Man-in-the-middle (MITM) attacks are a type of cyber-attack in which an attacker manipulates and intercepts two parties' communication to make them believe they are communicating directly to one another. Since the attacker is effectively "in the middle" of the discourse, the moniker was born. Since an adversary A_d has the capability to intercept and manipulate all communications through a public channel. So A_d can get the \mathcal{U}_a messages $\langle z_a, v_a, Aid_a, c_a \rangle$. Here $z_a = \alpha r_a + 2v_a$ in order to attack, he manipulates the message by $\langle z'_a, v'_a, Aid'_a, c'_a \rangle$ by generating new r'_a, v'_a and send it the server. But the server can detect the malicious message by verifying v'_a . Since $v_a = h(Aid_a || z_a || m_a || ID_a || SID_a)$ and $SID_i = h(ID_i || s)$, so to create a valid v'_a , A_d needs the secret key of server. With this A_d can also intercept and manipulates the message from the server to \mathcal{U}_a , that is z_b, N_a, v_s . But since



FIGURE 1. Illustration of login and authentication phase.

it is protected by v_s and to create a legit v_s , A_d needs to create N_a that again requires SID_a . So MITM attack is not possible between $(U)_a$ and the server. In the similar, we can say that it is also not possible between $(U)_b$ and the server.

A_d also can try between U_a and U_b by intercepting c_{ab}, v_f and sending new modified message but since v_f is protected by session specific keys like r_a and r_b , so it is not possible for an adversary to create a valid v_f .

B. PERFECT FORWARD SECURITY

Perfect forward security ensures the confidentiality of past communications even if long term private keys of the

involved parties are compromised. In our proposed protocol to eliminate this type of threat we use session specific secret keys such as r_a, r_b, s_i etc. The session key sk is not dependent only on long term secret keys. So even if long term secret keys of any of the involved parties are exposed, it is not possible for any adversary to create a legit sk . Since $sk = h(ID_a || ID_b || s_i || z_a || z_b || m_{ab})$, so if s is exposed somehow, A_d can get ID_a and ID_b by capturing $\langle z_a, v_a, Aid_a, c_a \rangle$ and $\langle z_b, v_b, Aid_b, c_b \rangle$ and computing m_a and m_b respectively. Now in order to compute correct sk , A_d needs r_a and r_b , to compute m_{ab} , which is not possible.

C. IMPERSONATION ATTACK

In our proposed protocol three parties \mathcal{U}_a , \mathcal{U}_b , and server are involved so A_d could impersonate as any of them. To impersonate as user \mathcal{U}_a , adversary uses the message $\langle z_a, v_a, Aid_a, c_a \rangle$ that is from \mathcal{U}_a to server. It is protected by v_a , since $v_a = h(Aid_a || z_a || m_a || ID_a || SID_a)$, so to create a valid v_a , A_d needs SID_a , which is $h(ID_a || s)$. So A_d needs secret key s in order to create v_a . That's why impersonation attack using \mathcal{U}_a is not possible in our proposed protocol. Similarly, we can say that an impersonation attack through \mathcal{U}_b 's identity is not possible. Also, A_d can try through the server side by capturing and modifying the messages from a server to \mathcal{U}_a and \mathcal{U}_b . Since both the messages are protected by v_s , and v_s is protected by s_i , which is session specific secret key of the server. So in our proposed scheme, every message by any involved party is authenticated by the respective receiver. So impersonation attack is not possible in our proposed scheme.

D. REPLAY ATTACK

A replay attack is when an attacker intercepts a valid message or communication and retransmits it at a later time to gain access to a system or seem to be a legitimate user. This can be done by listening to the signal, intercepting it, and then replaying it either directly to the system or across a network. In our proposed protocol we use session specific secret values to ensure the uniqueness of every transaction. Messages $\langle z_a, v_a, Aid_a, c_a \rangle$ and $\langle z_b, v_b, Aid_b, c_b \rangle$ are uses r_a and r_b respectively. Whereas messages z_a, N_b, v_s and z_b, N_a, v_s uses s_i . Also, each recipient of messages could authenticate the received message using a hash function.

E. PASSWORD GUESSING ATTACK

Suppose A_d intercepts all the messages communicated through the public channel and somehow gets all the information stored in the user's mobile application. In our proposed scheme we do not use public channels for sharing any information related to passwords. Also mobile application stores $\{C_i, V_i, h(\cdot), Gen(\cdot)\}$, where $C_i = SID_i \oplus h(A_i)$ and $V_i = h(ID_i || PW_i || B_i || SID_i)$. To implement password guessing attack A_d needs to verify the guessed password by V_i , for that A_d needs to calculate correct A_i which is $h(ID_i || PW_i || B_i)$. P , therefore A_d needs PW_i , ID_i and B_i simultaneously. So it is not possible for an A_d to implement password guessing attack.

F. USER ANONYMITY AND UNTRACEABLE

Users $\mathcal{U}_a, \mathcal{U}_b$ chooses r_a, v_a , and r_b, v_b respectively from χ_δ and computes $z_a = \alpha r_a + 2v_a, z_b = \alpha r_b + 2v_b, k_a = r_a Q, k_b = r_b Q, c_a = CH(k_a), c_b = CH(k_b), m_a = Mod_2(k_a, c_a), m_b = Mod_2(k_b, c_b)$, and masked the ID_a and ID_b by $Aid_a = ID_a \oplus h(m_a || z_a)$ and $Aid_b = ID_b \oplus h(m_b || z_b)$. Finally after computing verification factors $v_a = h(Aid_a || z_a || m_a || ID_a)$ and $v_b = h(Aid_b || z_b || m_b || ID_b)$, \mathcal{U}_a and \mathcal{U}_b sends $\langle z_a, v_a, Aid_a, c_a \rangle$ and $\langle z_b, v_b, Aid_b, c_b \rangle$ respectively to the server. So instead of ID_a and ID_b we use Aid_a and Aid_b

as identity over public channel. So proposed protocol follows the user's anonymity. Since these Aid_i 's uses session specific secret keys r_a, r_b they keep changing in every session. As a result, the proposed protocol is untraceable.

G. CONFIDENTIALITY

Confidentiality is a crucial characteristic of a cryptographic protocol since it makes sure that only authorized parties may access the data. The proposed protocol uses the hash function's property and RLWE problem to ensure confidentiality. In proposed protocol \mathcal{U}_a and \mathcal{U}_b sends $\langle z_a, v_a, Aid_a, c_a \rangle$ and $\langle z_b, v_b, Aid_b, c_b \rangle$ to server through public channel. In these messages, Z_a and Z_b are protected by RLWE' problem, as a result, A_d can not get session specific secret keys r_a and r_b until he solves RLWE problem. Also, v_a, Aid_a, v_b , and Aid_b are protected by a hash function. Further server verifies these messages by v_a and v_b which are protected by $h(\cdot)$. So proposed protocol includes confidentiality.

H. MUTUAL AUTHENTICATION AND KEY AGREEMENT

A secure secret key is established between the parties by mutual authentication and key agreement, which allows for the encryption and decryption of messages transferred between them. In our proposed protocol server verifies \mathcal{U}_a and \mathcal{U}_b by v_a and v_b respectively. Whereas \mathcal{U}_a and \mathcal{U}_b verifies server by v_s . Also at the end of the protocol both \mathcal{U}_a and \mathcal{U}_b agree on a common secret key.

IX. FORMAL SECURITY ANALYSIS

In this section we will present the formal security analysis of the proposed protocol by provable security method [7], [22] with the security model and assumptions.

A. SECURITY MODEL

The provable security is used to analyze the resistance of the proposed scheme against well known attacks. To put the proof concisely, we assume that our protocol E has three participants: $\mathcal{U}_a, \mathcal{U}_b$ and Server S and i^{th} instance for participants denoted as P^i .

1) ADVERSARY CAPABILITIES

In this paper, we employ the random oracle security model, which includes widely accepted security presumptions about adversary capability. In this, only oracle queries, which simulate an adversary's capabilities in an actual attack, allow the interaction between A_d and the participant. The dictionary $|D|$ size is a fixed constant that is unaffected by the security parameter that PPT attempts to break. The session key bit-length is the security parameter. Using the oracles, the list of query types that are accessible to A_d are as follows:

- Execute $(\Pi_{\mathcal{U}_a}^i, \Pi_{\mathcal{U}_b}^k, S^j)$: Passive attacks are modelled using execute query. The simulation of this query allows an adversary to get all the information exchanged

between participants. For example, when the challenger (after being asked by an adversary) simulates executing a query it returns with the messages that are exchanged between participants.

- $\text{Send}(\Pi_E^i, m)$: Send query used to model active attack on the given protocol. The simulation of this query not only allows an adversary to get messages, that are exchanged between participants but the adversary can either modify, create new messages, or forward them to the intended participant. In response to the send query, the participant instance generates the message as the output of the send query.
- $\text{Test}(\Pi_E^i)$: It is used to define the semantic security of the protocol. In this if the session key is not defined or the reveal query was not asked earlier then it returns with \perp otherwise a random number b is chosen, if $b = 0$ then it returns a random number of the same size as sk otherwise returns with sk .
- $\text{Reveal}(\Pi_E^i)$: It is modeled the misuse of the session key by the user. The $\text{Reveal}(\Pi_E^i)$ query is typically used to evaluate the security of a protocol against attacks that aim to extract session keys from compromised participants. It helps an adversary to get the session key that is computed by $\Pi_{U_a}^i, \Pi_{U_b}^k, S^j$ of instance I. That means when the reveal query is simulated, if the session key is not defined or the test query was asked earlier it returns with \perp otherwise returns with sk .
- $\text{Corrupt}(\Pi_E^i)$: This query is used to measure the corruption capability of an adversary. In this when A_d asks the challenger to simulate the Corrupt query it provides one of the authentication factors to A_d . That may be either long term secret key of the server or the password of user U_i .

2) DEFINITION OF SECURITY

This section outlines what exactly violates our protocol. Let's first establish the formal concepts of security as follows.

- **Accepted State**: If an instance Π_E^i reaches an accepted state after receiving the final expected message, it is said to be accepted. The concatenation of all messages sent and received by Π_E^i makes up its session identity.
- **Fresh**: An oracle is considered fresh (or possesses a fresh SK) if all three of the following criteria are met:
 - (1) Neither Π_A^i nor its partner has been requested for a Reveal query.
 - (2) Π_A^i has been accepted.
 - (3) No oracle has been asked for a Corrupt query prior to Π_A^i being accepted.
- **Partnering**: Two Instances Π_A^i and Π_B^j are said to be partner if the following condition satisfied
 - (1) Both are in accepted state.
 - (2) Shares a common session secret key sk .
 - (3) No instance other than Π_A^i and Π_B^j shares sk .

B. FORMAL SECURITY-PROOF IN RANDOM ORACLE MODEL

Theorem 1: Let the advantage that an adversary A_d could interrupt the proposed protocol with at most S_q send queries, E_q execute queries and H_q hashes be $\text{Adv}(t)$. Again let $\text{Adv}_{A_d}^{\text{RLWE}}(t)$ denote the probability of solving RLWE problem with polynomial time 't'. Then for the proposed scheme, we have

$$\text{Adv}_{A_d}(t) \leq \frac{2H_q^2}{q} + \frac{2S_q}{q} + \frac{(E_q + S_q)^2}{q} + (2H_q)\text{Adv}_{A_d}^{\text{RLWE}}(t) + \frac{2H_q}{q} + 2(C_z \cdot S_q^{S_z}). \quad (8)$$

That is, the proposed authentication scheme's security depends upon the RLWE problem hardness. Here C_z and S_z are Zipf's parameters [26].

Proof: To demonstrate the attack the challenger C and adversary A_d play a challenge-response game, in which attacks carried out by adversary A_d by asking C to execute various queries. Then based on the query asked by A_d , C computes the response as per the protocol and returns it to A_d . Now A_d analyzes the response message and tries to breach the proposed protocol the session's key semantic security. We would prove this by a series of games from Gm_0 to Gm_5 . For that let E_i be the event for each G_i and the probability of the event E_i to be defined as $P_r(E_i)$. It should be emphasized that an event E_i is defined for each Gm_i based on whether or not A_d succeeds in compromising the semantic security of the proposed scheme in Gm_i . Let's say that while A_d is being executed, an event E , which is independent of E_i might happen, E may be observable by C . Observed that until E happens, Gm_i and Gm_i are identical. Therefore we have

$$|P_r[E_{i+1}] - P_r[E_i]| \leq P_r[E]$$

Defining the Games: Gm_0 : Under the random oracle modal Gm_0 is equivalent to the simulation of a real attack on the proposed scheme. Therefore we have

$$\text{Adv}_{A_d}(t) = |Pr(E_0) - \frac{1}{2}| \quad (9)$$

Now let $D_i = |Pr(E_{i-1}) - P_r(E_i)|$. So we can transform equation (2) as

$$\begin{aligned} \text{Adv}_{A_d}(t) &= |Pr(E_0) - \frac{1}{2}| = |P_r(E_0) - P_r(E_4) + P_r(E_4) - \frac{1}{2}| \\ &= | \sum_{i=1}^5 D_i + P_r(E_4) - \frac{1}{2} |, \end{aligned}$$

Gm_1 : In Gm_1 , A_d execute hash queries in different way then Gm_0 . Apart from that it is indistinguishable from Gm_0 . In Gm_1 , a list L_h , is maintained that includes ordered pairs of the form (a, b) , where $b = h(a)$. Now when A_d ask hash query $h(\cdot)$ for a , C searches the L_h for the ordered pair (a, b) , if it exist, then C return with b otherwise generates a value b' , uniformly at random and include (a, b') into L_h . Then return with b' to A_d . Thus we have

$$P_r[E_1] = P_r[E_0] \quad (10)$$

TABLE 2. Computation cost comparison.

Schemes	User-side Computation cost	Server-side Computation cost	Total Computation cost
Proposed scheme	$2(7t_{ha} + 2t_{\delta} + 2t_{om} + t_{am} + t_{sm} + 2t_{ch}) \approx 4.9990188$	$10t_{ha} + t_{\delta} + 2t_{om} \approx 0.215017$	5.2140358
Islam et al.2021[17]	$2(8t_{ha} + 2t_{\delta} + t_{om} + t_{am} + t_{sm} + t_{ch}) \approx 5.2873224$	$8t_{ha} \approx 0.11272$	5.4000424
Zhang et al.2020 [31]	$12t_{ha} + 4t_c \approx 12962.171568$	$7t_{ha} \approx 0.09863$	12962.270198
Xie et al.2018[28]	$12t_{ha} + 4t_c + 5t_{sym} \approx 21592.171568$	$7t_{ha} + 2t_c + 5t_{sym} \approx 12524.08863$	34166.260198
Islam et al.2015[15]	$4t_{ha} + 4t_c + 10t_{sym} \approx 30229.953856$	$3t_{ha} + 4t_{sym} \approx 1086.43427$	31316.388126
Li et al. [23]	$8t_{ha} + 4t_c + 4t_{sym} \approx 19865.447712$	$3t_{ha} + 4t_{sym} \approx 1086.43427$	20951.881982
Farash et al.[12]	$6t_c + 8t_{ha} \approx 19441.447712$	$4t_c + 4t_{ha} \approx 22332.05636$	41773.504072

Gm_2 : This game is indistinguishable to game Gm_1 except it will be aborted in case of collision in authentication messages $z_a, v_a, Aid_a, c_a, z_b, v_b, Aid_b, c_b, z_a, N_b, v_s, z_b, N_a, v_s$. Now based on the birthday paradox, the maximum probability that hash oracle may have the same output is at most $\frac{H_q^2}{2q}$ also the maximum probability that two random samples are the same is at most $\frac{(E_q + S_q)^2}{2q}$. So we have

$$D_2 = |Pr(E_1) - Pr(E_2)| \leq \left(\frac{H_a^2}{2q} + \frac{(E_q + S_q)^2}{2q} \right). \quad (11)$$

Gm_3 : This game's scenario is similar to that of the previous one Gm_2 , except user instance $\prod_s^{U_i}$ or server instance $\prod_s^{S_j}$ disregards a legit authentication value. Gm_2 will be terminated if A_d accurately predicts the bit b without simulating the hash oracle $h(\cdot)$ in the Test query. so we have

$$D_3 = |Pr[E_2] - Pr[E_3]| = \frac{H_q}{2q} \quad (12)$$

Gm_4 : The simulation of this game follows Gm_3 , with the exception of the session key sk is predicted fully independently of $h(\cdot)$ and without simulating the random oracle $h(\cdot)$. In proposed protocol the session key $sk = h(ID_a || ID_b || s_i || z_a || z_b || m_{ab})$, where $q_i R_s = q_i r_s P$ and $X_i = h(ID_i || k_s)$.

It is simulating using a self-reducible instance of RLWE problem, which means if A_d predicts sk correctly, then A_d can solve RLWE problem within polynomial time. Therefore we have

$$D_4 = |Pr(E_3) - Pr(E_4)| \leq H_q \cdot Adv_{A_d}^{RLWE}(t) + \frac{H_q}{q}. \quad (13)$$

Gm_5 The simulation of G_4 and G_5 is indistinguishable except the hash oracle query with input (sk, \cdot) . The probability of guessing correct bit b in test query is $\frac{H_q^2}{2p}$ at most. Also, A_d can not distinguish the actual session key from the random one if he/she does not simulate hash oracle with correct input. So $Pr(E_5) = \frac{1}{2}$.

With this to guess a password with low-entropy the Zipf's law on passwords [26] can be used. According to this if we take $S_q = 10^7$ or 10^8 , the A_d 's advantage will be greater than $\frac{1}{2}$ (considering guessing attack). On the other hand if $S_q \leq 10^6$, the A_d 's advantage will be over $\frac{1}{2}$, (considering targeted guessing attack). So off-line password guessing attack's probability will be $\leq C_z \cdot S_q^{S_z}$ [26]. So we

TABLE 3. Average run time in microseconds.

Operations	User side	Server side
t_{δ}	0.561483	0.073503
t_{sm}	0.006655	0.000298
t_{am}	0.029505	0.002549
t_{om}	0.0013052	0.000307
t_{ch}	0.035515	0.000689
t_{ha}	0.180964	0.01409
t_c	3240	5583
t_{sym}	1726.923	271.598

have

$$D_5 = |Pr(E_4) - Pr(E_5)| \leq \frac{H_q^2}{2q} + C_z \cdot S_q^{S_z}. \quad (14)$$

We get the equation (1), after combining all the equations and inequalities. So, the proposed scheme is secure under RLWE assumption. \square

X. SECURITY COMPARISON AND PERFORMANCE ANALYSIS

In this section, the evaluation of the proposed framework is analyzed in terms of communication costs, computation time, and security attributes (see Table (2) and Table (4)). This paper contains the parameters of the scheme [30]. The parameters are $n = 1024$ bits, $\log \delta = 17.01$ for discrete Gaussian, where δ represents the standard deviation, and $q > 2$ is a big prime. The proposed one follows same parameters as Zhang et al [30], Feng et al. [13] follows: (1) Lattice-crypto library [1], and (2) Miracle libraries [github.com/miracl/MIRACL]. The article follows implementation on Dell PC's, 8 GB RAM, Windows-10, Intel's i7, [C and C++] language, 3.4GHz operating-system for server side, whereas 1.4GHz Samsung mobile with 1GB RAM, 4.3 operating-systems, processors Exynos-4412 are used on user end. The notations used to describe the cost of cryptographic operations are Gaussian χ_{δ} by t_{δ} , average cost for single multiplication by t_{sm} , whereas t_{om} used to denote average cost of single multiplication in Q_q , for one multiplication and addition in Q_q , t_{am} is used for cost of characteristics function t_{ch} is used, for symmetric encryption/decryption t_{sym} , for hashing t_{ha} , for exponentiation t_{exp} , for chaotic map operation t_c are used to denote. The cost of each operation is given in Table (3).

We have made a comparison with respect to communication cost and computation cost. The proposed protocol is

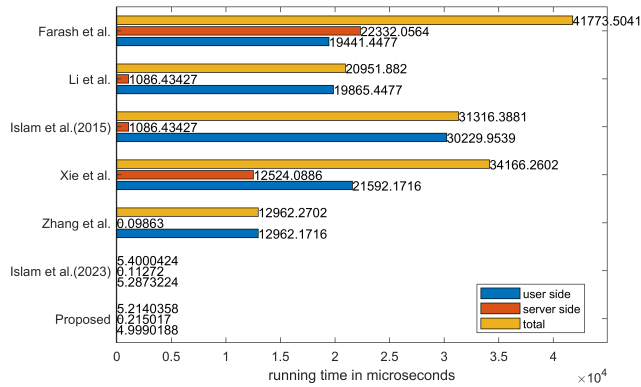


FIGURE 2. Description of computation cost.

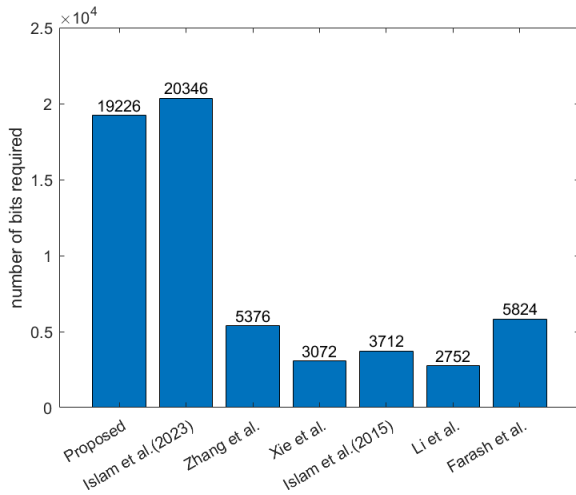


FIGURE 3. Description of communication cost.

TABLE 4. Communication cost comparison.

Schemes	Message structure	Communication cost
Proposed scheme	$4R_e + 7H + 2$	19226
Islam et al.2021[17]	$14I + 6H + 4R_e + 2$	20346
Zhang et al.2020 [31]	$9H + 4I + 2C_m$	5376
Xie et al.2018[28]	$6E + 2H + 2C_m$	3072
Islam et al.2015[15]	$6H + 10I$	3712
Li et al. [23]	$2H + 3I + 6E$	2752
Farash et al.[12]	$8H + 3I + 6C_m$	5824

compared [12], [15], [17], [23], [28], [29], [31]. The cost of computation and its comparison has been shown in the Table (2), and the Figure (2).

To illustrate communication costs associated with several pertinent protocols we use 64-bit for each binary string including a password, nonce, identity, and time stamp, and let I denote the communication cost associated with them, that is used in protocols. For hashing, we use 512 bits output SHA1; for symmetric encryption/decryption, we use a 256-bit key; for a chaotic map, we use a 256-bit size; and for each element from Qq , we use a 4094-bit size and let H, E, C_m, R_e represent their relative communication costs. Table (4), and Figure (3) show the communication costs associated with each protocol’s authentication key negotia-

TABLE 5. Comparison of schemes.

schemes→ features↓	[12]	[23]	[15]	[28]	[31]	[17]	Ours
Smart card stolen attack	✓	✓	✓	✓	✓	×	✓
User anonymity	×	×	✓	×	✓	×	✓
Man in the middle attack	✓	✓	✓	✓	✓	✓	✓
Mutual authentication	✓	✓	✓	✓	✓	✓	✓
Impersonation attack	✓	✓	✓	✓	×	✓	✓
Perfect forward secrecy	✓	✓	✓	✓	✓	✓	✓
Replay attack	×	×	×	✓	✓	✓	✓
Password guessing attack	×	×	✓	✓	✓	×	✓
Insider attack	×	×	✓	✓	✓	✓	✓
Quantum computer attack	×	×	×	×	×	✓	✓

tion procedure. For security characteristics comparison the security against password guessing attacks, replay assaults, impersonation attacks, man-in-the-middle attacks, known-key security, mutual authentication, and the perfect forward secrecy of the session key are our core concerns. In Table 5, security comparisons of pertinent protocols are displayed. “✓” indicates that a condition is satisfied in the Table 5 while “×” indicates that a property is not satisfied.

XI. CONCLUSION

In this paper, we have analyzed Islam and Basu’s protocol and discuss various security flaws, including impersonation attacks, stolen smartcard attacks, password guessing attacks, and user anonymity. We have presented an authentication protocol by fixing the Islam and Basu security pitfalls. Formal security using the ROM method shows that the proposed protocol is secure under the Ring Learning with Errors assumption. The proposed protocol is found more efficient than Islam and Basu’s protocol regarding computation and communication costs. In the future, the proposed security algorithm will be programmed and flashed in IoT operating system for realtime testbed experimentations.

ACKNOWLEDGMENT

The authors would like to thank the “Researchers Supporting Project number (RSPD2023R697), King Saud University, Riyadh, Saudi Arabia” for supporting the work.

REFERENCES

- [1] C. Aguilar-Melchor, J. Barrier, S. Guelton, A. Guinet, M.-O. Killijian, and T. Lepoint, “NFLLIB: Ntt-based fast lattice library,” in *Proc. Cryptographers’ Track RSA Conf.*, San Francisco, CA, USA, Feb. 2016, pp. 341–356.
- [2] S. Basu, K. Seyhan, S. H. Islam, and S. Akleylek, “MLWR-2PAKA: A hybrid module learning with rounding-based authenticated key agreement protocol for two-party communication,” *IEEE Syst. J.*, early access, Jul. 18, 2023, doi: 10.1109/JSYST.2023.3288629.
- [3] 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.
- [4] V. Dabra, A. Bala, and S. Kumari, “Flaw and amendment of a two-party authenticated key agreement protocol for post-quantum environments,” *J. Inf. Secur. Appl.*, vol. 61, Sep. 2021, Art. no. 102889.
- [5] 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, Oct. 2020.
- [6] D. Dharminder, C. B. Reddy, A. K. Das, Y. Park, and S. S. Jamal, “Post-quantum lattice-based secure reconciliation enabled key agreement protocol for IoT,” *IEEE Internet Things J.*, vol. 10, no. 3, pp. 2680–2692, Feb. 2023.

- [7] J. Ding, S. Alsayigh, J. Lancrenon, S. Rv, and M. Snook, "Provably secure password authenticated key exchange based on RLWE for the post-quantum world," in *Proc. Cryptographers' Track RSA Conf.*, San Francisco, CA, USA, Feb. 2017, pp. 183–204.
- [8] J. Ding, S. Alsayigh, R. V. Saraswathy, S. Fluhrer, and X. Lin, "Leakage of signal function with reused keys in RLWE key exchange," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.
- [9] J. Ding, S. Fluhrer, and S. Rv, "Complete attack on RLWE key exchange with reused keys, without signal leakage," in *Proc. Australas. Conf. Inf. Secur. Privacy*. Cham, Switzerland: Springer, 2018, pp. 467–486.
- [10] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, Interlaken, Switzerland, May 2004, pp. 523–540.
- [11] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
- [12] M. S. Farash and M. A. Attari, "An efficient and provably secure three-party password-based authenticated key exchange protocol based on Chebyshev chaotic maps," *Nonlinear Dyn.*, vol. 77, nos. 1–2, pp. 399–411, Jul. 2014.
- [13] Q. Feng, D. He, S. Zeadally, N. Kumar, and K. Liang, "Ideal lattice-based anonymous authentication protocol for mobile devices," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2775–2785, Sep. 2019.
- [14] S. Fluhrer, "Cryptanalysis of ring-LWE based key exchange with key share reuse," *Cryptol. ePrint Arch.*, Tech. Paper 2016/085, 2016. [Online]. Available: <https://eprint.iacr.org/2016/085>
- [15] S. H. Islam, "Design and analysis of a three party password-based authenticated key exchange protocol using extended chaotic maps," *Inf. Sci.*, vol. 312, pp. 104–130, Aug. 2015.
- [16] S. H. Islam, "Provably secure two-party authenticated key agreement protocol for post-quantum environments," *J. Inf. Secur. Appl.*, vol. 52, Jun. 2020, Art. no. 102468.
- [17] S. H. Islam and S. Basu, "PB-3PAKA: Password-based three-party authenticated key agreement protocol for mobile devices in post-quantum environments," *J. Inf. Secur. Appl.*, vol. 63, Dec. 2021, Art. no. 103026.
- [18] S. H. Islam and S. Zeadally, "Provably secure identity-based two-party authenticated key agreement protocol based on CBI-ISIS and bi-ISIS problems on lattices," *J. Inf. Secur. Appl.*, vol. 54, Oct. 2020, Art. no. 102540.
- [19] D. Kirkwood, B. C. Lackey, J. McVey, M. Motley, J. A. Solinas, and D. Tuller, "Failure is not an option: Standardization issues for post-quantum key agreement," in *Proc. Workshop Cybersecurity Post-Quantum World*, 2015, p. 21.
- [20] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to differential power analysis," *J. Cryptograph. Eng.*, vol. 1, no. 1, pp. 5–27, Apr. 2011.
- [21] U. Kumar, M. Garg, S. Kumari, and D. Dharminder, "A construction of post quantum secure and signal leakage resistant authenticated key agreement protocol for mobile communication," *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 1, Jan. 2023, Art. no. e4660.
- [22] H. Lai, M. A. Orgun, J. Xiao, J. Pieprzyk, L. Xue, and Y. Yang, "Provably secure three-party key agreement protocol using Chebyshev chaotic maps in the standard model," *Nonlinear Dyn.*, vol. 77, no. 4, pp. 1427–1439, Sep. 2014.
- [23] X. Li, J. Niu, S. Kumari, M. K. Khan, J. Liao, and W. Liang, "Design and analysis of a chaotic maps-based three-party authenticated key agreement protocol," *Nonlinear Dyn.*, vol. 80, no. 3, pp. 1209–1220, May 2015.
- [24] C. Peikert, "Lattice cryptography for the internet," in *Proc. Int. Workshop Post-Quantum Cryptogr.*, Waterloo, ON, Canada, Oct. 2014, pp. 197–219.
- [25] P. Rewal, M. Singh, D. Mishra, K. Pursharthi, and A. Mishra, "Quantum-safe three-party lattice based authenticated key agreement protocol for mobile devices," *J. Inf. Secur. Appl.*, vol. 75, Jun. 2023, Art. no. 103505.
- [26] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2776–2791, Nov. 2017.
- [27] Q. Wang, D. Wang, C. Cheng, and D. He, "Quantum2FA: Efficient quantum-resistant two-factor authentication scheme for mobile devices," *IEEE Trans. Depend. Secure Comput.*, vol. 20, no. 1, pp. 193–208, Jan. 2023.
- [28] Q. Xie, Y. Lu, X. Tan, Z. Tang, and B. Hu, "Security and efficiency enhancement of an anonymous three-party password-authenticated key agreement using extended chaotic maps," *PLoS ONE*, vol. 13, no. 10, Oct. 2018, Art. no. e0203984.
- [29] H. Yang, Y. Zhang, Y. Zhou, X. Fu, H. Liu, and A. V. Vasilakos, "Provably secure three-party authenticated key agreement protocol using smart cards," *Comput. Netw.*, vol. 58, pp. 29–38, Jan. 2014.
- [30] 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.*, Sofia, Bulgaria, Apr. 2015, pp. 719–751.
- [31] Y. Zheng, S. Hu, L. Wei, Y. Chen, H. Wang, Y. Yang, Y. Li, B. Xu, W. Huang, and L. Chen, "Design and analysis of a security-enhanced three-party authenticated key agreement protocol based on chaotic maps," *IEEE Access*, vol. 8, pp. 66150–66162, 2020.



DHARMINDER CHAUDHARY (Member, IEEE) received the Ph.D. degree in cryptography and network security. He is currently an Assistant Professor (Senior Grade) with the Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Chennai, India. He has published 30 SCI/Scopus indexed articles in the areas of cryptography, network security, and the Internet of Drones/vehicles security.



UDESHAYA KUMAR received the B.Sc. and M.Sc. degrees in mathematics from CCS University. He is currently an Assistant Professor with Gautam Buddha University, Noida, India. His research interests include cryptography, vehicular communication, security and privacy in the IoT, and the IoT.



KASHIF SALEEM (Member, IEEE) received the B.Sc. degree in computer science from Allama Iqbal Open University, Islamabad, Pakistan, in 2002, the P.G.D. degree in computer technology and communication from the Government College University, Lahore, Pakistan, in 2004, and the M.E. degree in electrical engineering electronics and telecommunication and the Ph.D. degree in electrical engineering from the University of Technology Malaysia, in 2007 and 2011, respectively. Since 2012, he has been with the Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia, where he is currently an Associate Professor. He is also an Adjunct Professor with the Department of Computer Sciences and Engineering, College of Applied Studies and Community Service, King Saud University. He is professionally certified by the Massachusetts Institute of Technology (MIT) in cybersecurity, the University of the Aegean in information and communication security, Institut Mines-Tcom in queuing theory, IBM in security intelligence analyst, and Microsoft and Cisco in computer networks. He acquired several research grants in Saudi Arabia, EU, and other parts of the world. He has authored or coauthored over 140 papers in refereed journals and international conferences. His research interests include ubiquitous computing, mobile computing, the Internet of Things (IoT), machine-to-machine (M2M) communication, wireless mesh networks (WMNs), wireless sensor networks (WSNs), and mobile ad-hoc networks (MANETs), intelligent autonomous systems, information security, and bioinformatics. He served as a technical program committee member and organized numerous international workshops and conferences. He is serving as an Associate Editor for *Alexandria Engineering Journal*, *Journal of Multimedia Information System (JMIS)*, *International Journal of E-Health and Medical Communications (IJEHMC)*, *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, and IEEE ACCESS.