International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 15, No. 7, July, 2025, pp. 1409-1414
Journal homepage: http://iieta.org/journals/ijsse

Ring-LWE Authentication in Centralized Cognitive Radio Networks

Israa Nasir Abdulhussien

General Directorate of Education in Al-Qadisiya Governorate/Ministry of Education, Qadisiya 58002, Iraq

Corresponding Author Email: Israa.nasir84@qu.edu.iq

https://doi.org/10.18280/ijsse.150708

Received: 20 May 2025
Revised: 6 July 2025
Accepted: 23 July 2025
Available online: 31 July 2025

Keywords:
cognitive radio network, BAN logic, authentication, ring LWE, protocol, quantum resistance, lattice cryptography

ABSTRACT

Security is the primary component of wireless communication. We employ security algorithms to protect our data. Ring-LWE achieves the best possible balance between security, flexibility, compactness, and efficiency. surpasses ECC in terms of authentication accuracy and convergence while preserving post-quantum security guarantees that are absent from traditional ECC. In this paper, a quantum-resistant mutual authentication scheme based on the Ring-LWE problem is proposed for centralized cognitive radio networks (CRNs). With its use of lattice-based cryptography, the suggested approach offers robust defense against both classical and quantum attacks, providing a notable boost in security, efficiency, and ease of implementation compared to conventional LWE or ECC-based authentication. In contrast to earlier schemes, our method supports dynamic node access without rekeying, lowers computational complexity, and does away with the need for public key infrastructure (PKI). Utilizing automated tools to show resistance against multiple attack vectors, such as replay, brute-force, and attacks by a man in the middle, the protocol's security is formally confirmed using BAN logic. Because of this, our solution is a solid contender to secure CRNs in the future.

1. INTRODUCTION

Due to the rapid increase in wireless devices, there is a need for effective improvement in the demand for efficient spectrum usage to improve connectivity [1]. The intelligent wireless communication system known as cognitive radio CR is poised to bring about a revolution in wireless communication, affecting several aspects of technology. Specifically, it will enable secondary users SUs, to operate on the unoccupied spectrum segments designated for primary users Pus [2]. Many people believe that CR is a potential solution to address the issue of spectrum scarcity brought on by the existing rigid spectrum distribution policy. It can sense its radio environment and adjust transmission parameters based on the results of the sensing, which enhances the performance of cognitive radio systems and prevents interference with Pus [3, 4].

An exchange of messages with a particular format for principal authentication using cryptographic techniques is called an authentication protocol [5]. Authentication does not determine which entities should be given access in security, but only verifies that an entity is who they claim to be [6]. It might be regarded as one of the most important components of cryptographic security protocols [7]. As well as it is an essential issue in a Cognitive Radio Network (CRN) and aims to inhibit illegal use of spectrum bands by malicious users [8]. Given that a cognitive node can dynamically join or exit the spectrum, ensuring safe communication becomes more challenging and needs further research [9]. One of the main security features of wireless networks is authentication, which involves confirming a cognitive node's identity before granting it access to resources [10].

However, the security issues of cognitive radio were not the emphasis of the current study, as is the case with many emerging technologies. Usually, security is "pulled on" after the fact by incorporating encryption and connection authentication [11]. In this paper, we will employ Ring LWE encryption while on the other side the certification authority (CA) and digital certificate (DC) technologies are very crucial in providing security against any malicious users and heuristic approaches such as digital signatures (DS) which can further enhance the void to ensure safety including integrity and non-repudiation. Any design that does not ensure the security concerns of a protocol never sees the light of day, and its security requirements go largely unanalyzed. We will apply one of the methods of protocol security analysis/verification; it is BAN logic. It is used to instantiate the study stage of the protocol in addition to validate that the security aspects are strong enough as far as possible of the protocol.

The paper's remaining sections are organized as follows: Part 2. provides a summary of the pertinent literature along with an explanation of the reasoning behind the authentication mechanism selected for CRs. Section 3 provides an explanation of ring TWE. In Section 4, we outline our proposed authentication scheme and provide evidence of its accuracy. Section 5 looks at the recommended plan from both a security and performance perspective. The final conclusions are given in Section 6.

The following are this work's primary contributions:

•putting forward a brand-new Ring-LWE-based

authentication system made especially for centralized CRNs.
- utilizing BAN logic to provide a formal security verification.
- proving the protocol's resistance to various forms of attack.
- demonstrating its effectiveness and low overhead while contrasting the results with those of current schemes.

2. RELATED WORK

Tang and Wu [12] provided an overview of the security issues that the cognitive radio network has encountered and addressed some of its main concerns. The dynamic of artificial intelligence security and the access spectrumare then analyzed and discussed by the distinctions between the cognitive radio network and the wireless network current. Ultimately, it concludes that there are security issues with cross-layer design. Strong detection capabilities are provided by cross-layer operations, but synchronization and processing overhead become more complicated.

Zhang et al. [13] proposed cooperative spectrum access for CRNs, which aims to enhance the primary user's secure transmission by a collaborating secondary user that would be created by specific transmission options. Trust-based cooperative access and relaying aids in PU transmission security, but if SU trust is weakened, it introduces protocol overhead and attack points.

Thakre and Dixit [14] were determined to the risks associated with the wireless communication environment, use energy sensing to detect any empty spectrum, and focus on mitigating the effects of jamming and primary user emulation attacks, among other dangers. The wireless communication environment posed by cognitive radio networks is primarily threatened by these two. For initial sensing, energy detection is straightforward and helpful, but it is brittle in hostile environments.

Elkashlan et al. [15] proposed the enhancement of cognitive multiantenna listening channels' physical security layer. To evaluate the secrecy performance in a passive wiretap, we employ the secrecy cutout probability as a practical performance parameter. In order to secure broadcasting at the physical layer, where the signal from the secondary transmitter to the secondary receiver is heard by the eavesdropper, we also consider the cognitive wiretap channel and recommend the use of several antennas. In relay or MIMO configurations, multi-antenna physical-layer security maximizes secrecy, but only if channel estimation is accurate.

Our suggested strategy makes use of lattice-based primitives, which provide post-quantum security and improved efficiency, in contrast to earlier techniques like those based on PKI or ECC. Our approach drastically lowers the overhead and authentication time without sacrificing security, in contrast to many other approaches that have high computational costs and are susceptible to quantum attacks.

3. RING LWE BACKGROUND

Solving a series of univariate polynomial equations, usually in a cyclotomic field, when the right side was "slightly" perturbed, is known as the Ring Learning with Errors problem (LWE) [16]. It is an extension of the Learning with Errors (LWE) problem, which is a fundamental problem in lattice-based cryptography [17]. Ring-LWE provides improved efficiency and performance over LWE by taking advantage of algebraic structures, specifically polynomial rings [18]. Differentiating between uniformly random samples and noisy samples of the type (a,b=a·s+e) is the Ring-LWE issue [19], where:

- a is a uniformly random element in the ring Rq.
- s is a secret element in Rq.
- e is an error term, typically sampled from a discrete Gaussian distribution over the ring.
- The operation a·s denotes polynomial multiplication in the ring.

The error term e ensures that the problem remains hard, making it difficult to solve even for quantum computers.

4. MODEL OF THE SYSTEM

In this approach, the server is used to authenticate users, which works with users to generate public keys that are known to all parties. In exchange, each participant creates a private key that only that specific person knows. Figure below Figure 1 shows an illustration of the authentication scheme.

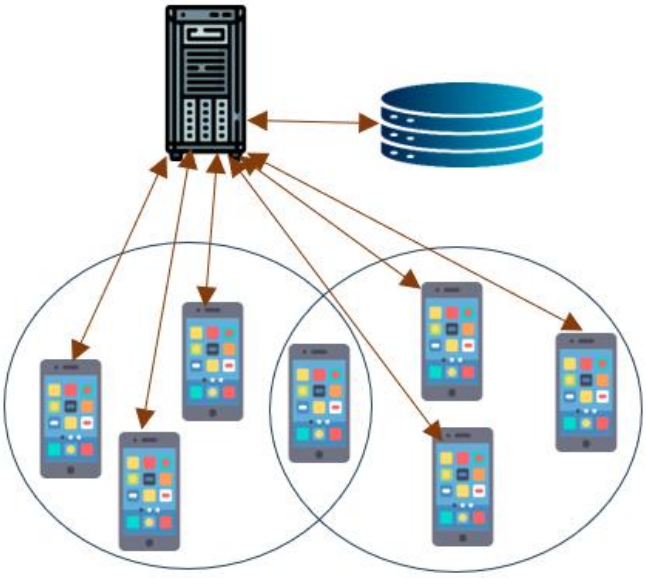

Figure 1. Connection in CRNs

4.1 The proposed user authentication scheme

In cognitive radio networks (CRNs), authentication plays a vital role in guaranteeing that only authorized users may access the network and preventing unauthorized organizations from abusing the available spectrum. In light of the requirement for post-quantum security, Ring-LWE authentication in CRNs can offer a reliable solution. Here is a suggested method for leveraging Ring-LWE to implement authentication in a CRN.

4.1.1 System configuration

A. Key generation

○ **Private Key**: The prover generates a secret key s(x), which is a small polynomial sampled from a specific distribution (e.g., discrete Gaussian).

○ **Public Key**: The corresponding public key p(x) is generated as described in the verification key generation process:

$$\mathcal{P}(\mathcal{X}) = a(\mathcal{X}).\mathcal{S}(\mathcal{X}) + e(\mathcal{X})\, mod(q)$$

where, $a(\mathcal{X})$ is a random polynomial in R_q, and $e(\mathcal{X})$ is an error polynomial.

The public key p(x) is shared with the verifier, while the prover keeps the secret key s(x) private.

B. Authentication protocol

Step 1: Challenge generation

o The verifier generates a random challenge polynomial c(x) from R_q and sends it to the prover.

Step 2: Response by prover

o The prover computes the response r(x) using their secret key s(x) and the received challenge c(x). This might involve an operation such as: r(x)=c(x)·s(x)+error term (mod q)

o The error term could be a small random polynomial or the result of a controlled noise addition to ensure security properties.

o The prover sends r(x) back to the verifier.

Step 3: Verification by verifier

o The verifier checks the validity of the response using the public key p(χ). This typically involves verifying that the response r(χ) matches the expected form given the challenge c(χ) and the public key p(χ):

$$r(\chi)=c(\chi)\cdot p(\chi)+\text{small error term (mod q)}$$

o The verifier accepts the authentication if the above condition holds true, meaning the prover knows the secret key corresponding to the public key.

C. Authentication process

The BS verifies for each node a and b that they want to communicate with each other

First, BS is satisfied with node A.

Step 1: Authentication Request:

- o When an SU or PU wants to access the network, it sends an authentication request to the BS.
- o The request includes a challenge message m encrypted using the user's public key.

Step 2: Challenge-Response Protocol:

- o BS generates a challenge: The BS generates a random challenge polynomial r(χ) and computes:
  - ▪ c1(χ)= ai(χ) · r(χ) + e1(χ)
  - ▪ c2(χ)= bi(χ) · r(χ) + e2(χ) + m(χ)
- o The challenge (c1(χ), c2(χ)) is sent to the user.

Step 3: User Response:

- o The user decrypts the challenge using their secret key Si(χ) to recover m(χ).
- o The user sends a response m′(χ), a function of m(x), back to the BS.

Step 4: Verification:

- o The BS verifies the response:
  - ▪ If m′(χ) matches the expected response based on m(χ), the user is authenticated.
  - ▪ Otherwise, access is denied.

Steps 1-4 also verify from node B if the two nodes A and B are authenticated, then node A and B can communicate with each other; else if one node is not authenticated, access is denied.

The authentication protocol is as follows:

- $\mathcal{A}\rightarrow S: \mathcal{A}, \mathcal{B}, ja$
- $S \rightarrow \mathcal{A} : \{ja, \mathcal{B}, \mathcal{K}ab, \{\mathcal{K}ab, \mathcal{A}\}\mathcal{K}bs\}Kas$
- $\mathcal{A}\rightarrow S: \{\mathcal{K}ab, \mathcal{A}\}\mathcal{K}bs$
- $S \rightarrow \mathcal{B} : \{ja, B, \mathcal{K}ab \{\mathcal{K}ab, \mathcal{A}\}\mathcal{K}bs\}\mathcal{K}as$
- $B \rightarrow S: \{\mathcal{K}ab, A\}\mathcal{K}bs$
- $\mathcal{A} \rightarrow \mathcal{B} : \{\mathcal{K}ab, A\}\mathcal{K}bs$
- $\mathcal{B} \rightarrow \mathcal{A} : \{jb\}\mathcal{K}ab$

Ring-LWE-based operations are more efficient than standard LWE because their computational complexity is polynomial in the ring dimension and modulus size. Our scheme achieves practical performance appropriate for real-time CRN environments by utilizing fast Number Theoretic Transforms (NTT) and structured algebraic operations.

5. PERFORMANCE ANALYSIS

This section examines the suggested user authentication scheme's performance in terms of security, computation overhead, storage overhead, and communication overhead.

5.1 Attack resistance and functionality

The suggested user authentication strategy's functionality and resilience to attacks are contrasted with those of the existing schemes, as in Table 1 below.

Brute force attack prevention: is a cryptanalytic assault that looks for the correct key to decrypt any encrypted data until it is found [20]. Since our suggested method makes use of a hash function, a brute force attack is resistant.

Replay attack prevention: Because our suggested method makes use of a hash function, brute force attack is resistant [21]. The current communication's message differs from the messages of previous conversations due to the timestamp. As a result, the protocol is safe from replay assaults.

Table 1. Performance comparison

Functionally	New Authentication [22]	Trust- Authentication [23]	Mechanism [24]	Keyless Security [25]	Proposed Method
Brute force attack resistance	No	Yes	No	Yes	Yes
Resistance to replay attacks	No	Yes	Yes	No	Yes
mutual trust	Yes	No	Yes	No	Yes
Man-in-the-middle attack resistance	Yes	No	Yes	No	Yes
Agreement on the session key	Yes	No	Yes	No	Yes

Attack by a man in -the - middle prevention: this kind of attack, the attacker tries to listen in on the conversations that two users are having across a network. Since our approach relies on mutual authentication and uses random integers that are updated with every protocol iteration, attack by a man in the middle is not feasible.

From Table 1, we note that the proposing method is better at resisting attacks when comparing four previous studies with the proposing method in terms of (Brute force attack resistance, Resistance to replay attacks, man in middle attack resistance). These results demonstrate the feasibility of the scheme for implementation on real-world CRN devices, with better performance than previous approaches.

5.2 Using Ban logic for analysis

Analysis of the protocol using BAN logic

Burrows-Abadi-Nedham (BAN) Logic uses different symbols in cryptographic scheme as follows [26, 27]:

① $\sigma\ |{\equiv}\rho$: σ believes ρ;
② $\sigma \rhd \rho$: σ sees ρ;
③ $\sigma|{\sim}\rho$: σ send ρ;
④ $\sigma \mid \Rightarrow \rho$: σ controls ρ;
⑤ $\#(\rho)$: ρ is fresh;
⑥ $\sigma \mid \overset{k}{\rightarrow} \rho$: K is the key shared by σ and ρ;
⑦ $\{\rho\}_K$: the cipher text of ρ encrypted by the key K.

Security analysis

The original messages are analyzed via BAN logic. The analysis is performed.

Analysis of Ring LWE algorithm via BAN logic

The ideal protocol is as follows:

MSGA 2: $S \rightarrow A$: $\{\rho_A, G, \overset{\mathcal{KS}}{-}\ S\}(\mathcal{KS})^{-1}$ commencing S
MSGB 3: $A \rightarrow S$: $\{\rho_B, PA, \overset{\mathcal{KS}}{-}\ S\}\ \mathcal{KA}$ commencing A
MSGC 4: $S \rightarrow B$: $\{\rho_B, \#(M), \overset{\mathcal{KS}}{-}\ S\}\ (\mathcal{KS})^{-1}$ commencing S
MSGD 5: $B \rightarrow S$: $\{\rho_A, PB, \overset{\mathcal{KS}}{-}\ \}\ \mathcal{KB}$commencing B
MSGE 6: $A \rightarrow B$: $\{\rho_A, P_A, \overset{\mathcal{KS}}{-}\ S\}\ \mathcal{KA}$commencingA
MSGF 7: $B \rightarrow A$: $\{K1\ , C1, C2, \overset{\mathcal{KA}}{\longrightarrow}A\}\ \mathcal{KB}$commencing B
State the assumption about the original message.

$S\|\ \#\ \rho_B$	$S\|\equiv G$	$A\ \|\equiv\ \mathbb{S} \overset{\mathcal{KS}}{\Rightarrow -}\ \mathbb{S}$
$S\|\equiv \#M$	$A\|\equiv \#\rho_A$	$B\|\equiv\ A \overset{\mathcal{KA}}{\Rightarrow -}\ A$
$S\|\equiv \overset{\mathcal{KB}}{-}\ B$	$A\|\equiv \overset{\mathcal{KS}}{-}\ S$	$B\ \|\equiv A \overset{\mathcal{KS}}{\Rightarrow -}\ \mathbb{S}$
$B\|\equiv \overset{\mathcal{KA}}{-}\ A$	$B\|\equiv \overset{\mathcal{KB}}{-}\ B$	$B\ \|\equiv \overset{\mathcal{KS}}{\Rightarrow -}\ \mathbb{S}$
$A\|\equiv \overset{\mathcal{KA}}{-}\ A$	$B\|\equiv \#\ \rho_A$	$A\ \|\equiv\ B \overset{\mathcal{KA}}{\Rightarrow -}\ A$
$S\|\equiv \#\ \rho_A$	$B\|\equiv \overset{\mathcal{KS}}{-}\ \mathbb{S}$	$S\ \|\equiv\ B \overset{\mathcal{KB}}{\Rightarrow -}\ B$
$A\|\equiv \overset{\mathcal{KB}}{-}\ B$	$S\|\equiv \overset{\mathcal{KS}}{-}\ S$	

Apply the following rules:

MSG 2: $A \rhd \{\rho_A, \#\ G, \overset{\mathcal{KS}}{-}\ S\}\mathcal{KS}^{-1}$ commencing S

$$R1 = \frac{A|\equiv \overset{\mathcal{KS}}{-}\ S, A \rhd \{\rho A, G, \overset{\mathcal{KS}}{-}\ S\} - \mathcal{KS}^{-1}}{A\ |\equiv S|\sim\overset{\mathcal{KS}}{\longrightarrow}S}$$

$$R2 = \frac{A\ |\equiv\#(\rho B), A|\equiv S|\sim\overset{\mathcal{KS}}{-}\ S}{A\ |\equiv S|\equiv\overset{\mathcal{KS}}{\longrightarrow}S}$$

$$R3 = \frac{A\ |\equiv S \overset{KS}{\Rightarrow -}\ S\ , A\ |\equiv S|\equiv \overset{\mathcal{KS}}{-}\ S}{A|\equiv \overset{\mathcal{KS}}{-}\ S}$$

The results are $A\ |\equiv S|\ \equiv \overset{\mathcal{KS}}{-}\ S\ A|\ \equiv \overset{\mathcal{KS}}{-}\ S$.

MSG 3: $S \rhd \{\rho_B, P_A, \overset{\mathcal{KS}}{-}\ S\}_{\ KB}$ commen B

$$R1 = \frac{S|\equiv \overset{KA}{-}\ A, S \rhd \{\rho B, PA, \overset{\mathcal{KS}}{-}\ S\}\ KA}{S\ |\equiv A|\sim\overset{\mathcal{KS}}{\longrightarrow}S}$$

$$R2 = \frac{S\ |\equiv\#(\rho A), S\ |\equiv A|\sim\overset{KS}{-}\ S}{S\ |\equiv A|\equiv\overset{KS}{\longrightarrow}S}$$

$$R3 = \frac{S\ |\equiv A \overset{KA}{\Rightarrow -}\ A, S\ |\equiv A|\equiv \overset{\mathcal{KS}}{-}\ S}{S|\equiv \overset{\mathcal{KS}}{-}\ S}$$

The results are $S\ |\equiv A|\ \equiv \overset{\mathcal{KS}}{-}\ S\ S|\ \equiv \overset{\mathcal{KS}}{-}\ S$.

MSG 4: $B \rhd \{\rho_B, \#(M), \overset{\mathcal{KS}}{-}\ S\}\ (\mathcal{KS})^{-1}$ commencing S

$$R1 = \frac{B|\equiv \overset{K_S}{-}S, B \rhd \{\rho B, G, \overset{KS}{-}\ S\}\mathcal{KS}^{-1}}{B\ |\equiv S|\sim\overset{\mathcal{KS}}{\longrightarrow}S}$$

$$R2 = \frac{B\ |\equiv\#(\rho A), B\ |\equiv S|\sim\overset{\mathcal{KS}}{-}\ S}{B\ |\equiv S|\equiv\overset{\mathcal{KS}}{\longrightarrow}S}$$

$$R3 = \frac{B\ |\equiv S \overset{\mathcal{KS}}{\Rightarrow -}\ S\ , B\ |\equiv S|\equiv \overset{\mathcal{KS}}{-}\ S}{B|\equiv \overset{\mathcal{KS}}{-}\ S}$$

The results are $B\ |\equiv S|\ \equiv \overset{\mathcal{KS}}{-}\ S\ B|\ \equiv \overset{\mathcal{KS}}{-}\ S$.

MSG 5: $S \rhd \{\rho_A, P_B, \overset{\mathcal{KS}}{-}\ S\}_{\ KB}$ commencing B

$$R1 = \frac{S|\equiv \overset{KB}{-}\ B, S \rhd \{\rho A, PB, \overset{\mathcal{KS}}{-}\ S\}\ KB}{S\ |\equiv B|\sim\overset{\mathcal{KS}}{\longrightarrow}S}$$

$$R2 = \frac{S\ |\equiv\#(\rho B), S\ |\equiv BB|\sim\overset{\mathcal{KS}}{-}\ S}{S\ |\equiv BB|\equiv\overset{\mathcal{KS}}{\longrightarrow}S}$$

$$R3 = \frac{S\ |\equiv B \overset{KB}{\Rightarrow -}\ B, S\ |\equiv BB|\equiv \overset{\mathcal{KS}}{-}\ S}{S|\equiv \overset{\mathcal{KS}}{-}\ S}$$

The results are $S\ |\equiv B|\ \equiv \overset{\mathcal{KS}}{-}\ S\ S|\ \equiv \overset{\mathcal{KS}}{-}\ S$.

MSG 6: A: $\{\rho_A, \#(M), \overset{KS}{\rightarrow}S\}\ \mathcal{KS}^{-1}$ commencing S

$$R1 = \frac{A|\equiv \overset{kS}{-}\ S, A \rhd: \{\rho A, \#(M), \overset{KS}{-}\ \}\mathcal{KS}^{-1}}{A\ |\equiv S|\sim\overset{\mathcal{KS}}{\longrightarrow}S}$$

$$R2 = \frac{A\ |\equiv\#(\rho A), A\ |\equiv S|\ \sim\overset{\mathcal{KS}}{-}\ S}{A\ |\equiv S|\equiv\ \overset{\mathcal{KS}}{\longrightarrow}S}$$

$$R3 = \frac{A\ |\equiv S \overset{\mathcal{KS}}{\Rightarrow -}\ S\ , A\ |\equiv S|\equiv\ \overset{\mathcal{KS}}{-}\ S}{A|\equiv \overset{\mathcal{KS}}{-}\ S}$$

The results are $A\ |\equiv S|\ \equiv\ \overset{\mathcal{KS}}{-}\ S\ A|\ \equiv \overset{\mathcal{KS}}{-}\ S$.

MSG 7: $B \rhd \{\rho_A, P_A, \overset{\mathcal{KS}}{-}\ S\}_{\ KA}$ commencing A

$$R1 = \frac{B|\equiv \overset{kA}{-}\ A, B \rhd \{\rho A, PA, \overset{\mathcal{KS}}{-}\ S\}\ KA}{B\ |\equiv A|\sim\ \overset{\mathcal{KS}}{\longrightarrow}S}$$

$$R2 = \frac{B\ |\equiv\#(\rho A), B\ |\equiv A|\sim\ \overset{\mathcal{KS}}{-}\ S}{B\ |\equiv A|\equiv\ \overset{\mathcal{KS}}{\longrightarrow}S}$$

$$R3 = \frac{B\ |\equiv A \overset{\mathcal{KS}}{\Rightarrow -}\ S, B\ |\equiv A|\equiv\ \overset{\mathcal{KS}}{-}\ S}{B|\equiv \overset{\mathcal{KS}}{-}\ S}$$

The results are $B\ |\equiv A|\ \equiv\overset{\mathcal{KS}}{\longrightarrow} S\ B|\ \equiv\overset{\mathcal{KS}}{\longrightarrow} S$.

In all messages, we achieve the goal and subgoal; therefore, the protocols are secure.

The results of the performance investigation demonstrate that our suggested technique outperforms other user authentication systems currently in use.

5.3 Complexity of the Ring-LWE

The challenges presented by quantum computing threats can be effectively addressed by integrating Ring-LWE-based authentication mechanisms in centralized cognitive radio networks. These schemes offer safe and effective authentication, guaranteeing the integrity and dependability of CRNs in the dynamic world of wireless communications by taking advantage of the mathematical difficulty of lattice problems and streamlining computational procedures. Table 2 shows the effectiveness that performed on:

Operating System: Windows 11 Professional

Processor: 2.50 GHz Intel Core i5 13400F (13th Gen)

32 GB of random-access memory

Tested algorithm variations include Ring-LWE, standard LWE, and ECC.

Ring parameters: polynomial ring modulus x^{1024}+1, modulus q-122998 , qaussian error 3.19

Ring-LWE, combines provable post-quantum security with significantly smaller key sizes and faster computation. In a setting involving centralized cognitive radio authentication, this makes it evidently better than standard LWE and generally more effective than ECC.

Table 2. Criteria of performance

Algorithm	Key Size	Complexity	Iteration Coverage	Max Accuracy	Security	Efficiency
Standard LWE	Very large O(n2)	$O(n^2)$	390	88.5% (55 sample)	Worst-case lattice	Low
ECC	Small (256 bit)	Fast	477	77.4% (46 sample	Classical	Efficient but quantum
Ring -LWE	compact	O(nlogn)	253	94.7% (66 sample)	Ideal lattice SVP reduction	High

6. CONCLUSIONS

This work proposed a quantum-resistant mutual authentication based on the ring LWE for centralized CRNs. The proposed strategy is free from the shortcomings of public key infrastructure designs, such as their high prices and poor efficiency, because it does not rely on digital certificates.

The author used BAN reasoning to show how to formally verify it. We used the difficulty of solving the lattice's shortest vector issue to illustrate the security of our system.

In summary, the suggested Ring-LWE-based authentication scheme offers centralized CRNs a lightweight, secure, and quantum-resistant solution. It offers scalable, low-latency authentication and overcomes the drawbacks of current public-key-based protocols.Our study focuses on the Ring LWE algorithm, which is used in CRN systems to generate an encryption key and to ensure that the resulting key is implemented securely and quickly. The results demonstrated that the enhanced approach is more effective and superior on security and other dimensions when compared to using other algorithms by using some metrics.

ACKNOWLEDGMENT

The author is grateful to the University of Kufa's computer department/college of computer sciences and mathematics for their invaluable counsel, direction, and support in helping me finish my paper.

REFERENCES

[1] Qamar, F., Siddiqui, M.U.A., Hindia, M.N., Hassan, R., Nguyen, Q.N. (2020). Issues, challenges, and research trends in spectrum management: A comprehensive overview and new vision for designing 6G networks. Electronics, 9(9): 1416. https://doi.org/10.3390/electronics9091416

[2] Gashema, G., Lee, J.M., Kim, D.S. (2020). Efficient-spectrum management based on localisation of primary user position towards 5G. IET Communications, 14(20): 3567-3577. https://doi.org/10.1049/iet-com.2020.0284

[3] Tlouyamma, J., Velempini, M. (2021). Channel selection algorithm optimized for improved performance in cognitive radio networks. Wireless Personal Communications, 119(4): 3161-3178. https://doi.org/10.1007/s11277-021-08392-5

[4] Yu, F.R., Tang, H. (2011). Cognitive Radio Mobile Ad Hoc Networks. New York: Springer.

[5] Mayouf, M.A., Shukur, Z. (2008). Animation of natural language specifications of authentication protocols. Journal of Computer Science, 4(7): 503-508.

[6] Hardjono, T., Dondeti, L.R. (2005). Security in Wireless LANS and MANS (Artech House Computer Security). Artech House, Inc.

[7] Park, D., Boyd, C., TDawson, E. (2000). Classification of authentication protocols: A practical approach. In: Goos, G., Hartmanis, J., van Leeuwen, J., Pieprzyk, J., Seberry, J., Okamoto, E. (eds) Information Security. ISW 2000. Lecture Notes in Computer Science, vol 1975. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44456-4_15

[8] Bakhtiari Chehelcheshmeh, S., Hosseinzadeh, M. (2016). Quantum-resistance authentication in centralized cognitive radio networks. Security and Communication Networks, 9(10): 1158-1172. https://doi.org/10.1002/sec.1408

[9] Hilal, W., Gadsden, S.A., Yawney, J. (2023). Cognitive dynamic systems: A review of theory, applications, and recent advances. Proceedings of the IEEE, 111(6): 575-622. https://doi.org/10.1109/JPROC.2023.3272577

[10] Alhoraibi, L., Alghazzawi, D., Alhebshi, R., Rabie, O.B.J. (2023). Physical layer authentication in wireless networks-based machine learning approaches. Sensors, 23(4): 1814. https://doi.org/10.3390/s23041814

[11] Burnett, M. (2006). Perfect Password: Selection, Protection, Authentication. Elsevier.

[12] Tang, L., Wu, J. (2012). Research and analysis on cognitive radio network security. Wireless Sensor

Network, 4(4): 120-126. http://doi.org/10.4236/wsn.2012.44017

[13] Zhang, N., Lu, N., Cheng, N., Mark, J.W., Shen, X.S. (2013). Cooperative spectrum access towards secure information transfer for CRNs. IEEE Journal on Selected Areas in Communications, 31(11): 2453-2464. https://doi.org/10.1109/JSAC.2013.131130

[14] Thakre, S., Dixit, S. (2014). Security threats and detection technique in cognitive radio network with sensing strategies. International Journal of Research in Engineering and Technology, 3(1): 591-593. https://doi.org/10.15623/IJRET.2014.0301100

[15] Elkashlan, M., Wang, L., Duong, T.Q., Karagiannidis, G.K., Nallanathan, A. (2014). On the security of cognitive radio networks. IEEE Transactions on Vehicular Technology, 64(8): 3790-3795. https://doi.org/10.1109/TVT.2014.2358624

[16] Bootland, C., Castryck, W., Vercauteren, F. (2020). On the security of the multivariate ring learning with errors problem. Open Book Series, 4(1): 57-71. https://doi.org/10.2140/obs.2020.4.57

[17] Pedrouzo-Ulloa, A., Troncoso-Pastoriza, J.R., Gama, N., Georgieva, M., Pérez-González, F. (2021). Revisiting multivariate ring learning with errors and its applications on lattice-based cryptography. Mathematics, 9(8): 858. https://doi.org/10.3390/math9080858

[18] Jain, A., Lin, H., Saha, S. (2024). A Systematic Study of Sparse LWE. In: Reyzin, L., Stebila, D. (eds) Advances in Cryptology – CRYPTO 2024. CRYPTO 2024. Lecture Notes in Computer Science, 14922. Springer, Cham. https://doi.org/10.1007/978-3-031-68382-4_7

[19] Villena, R.C., Terada, R. (2024). Recovery of the secret on Binary Ring-LWE problem using random known bits-extended version. Journal of Internet Services and Applications, 15(1): 39-45. https://doi.org/10.5753/jisa.2024.3871

[20] Williams, L.C. (2001). A discussion of the importance of key length in symmetric and asymmetric cryptography. SAN Inst. 2000.

[21] Butt, M.A. (2013). Cognitive radio network: Security enhancements. Journal of Global Research in Computer Science, 4(2): 36-41

[22] Zhu, X.L., Xu, S.L. (2012). A new authentication scheme for wireless ad hoc network. In 2012 International Conference on Information Management, Innovation Management and Industrial Engineering, Sanya, China, pp. 312-315. https://doi.org/10.1109/ICIII.2012.6339841

[23] Parvin, S., Han, S., Tian, B., Hussain, F.K. (2010). Trust-based authentication for secure communication in cognitive radio networks. In 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Hong Kong, China, pp. 589-596. https://doi.org/10.1109/EUC.2010.95

[24] Khasawneh, M., Agarwal, A. (2017). A secure and efficient authentication mechanism applied to cognitive radio networks. IEEE Access, 5: 15597-15608. https://doi.org/10.1109/ACCESS.2017.2723322

[25] Albermany, S.A., Safdar, G.A. (2014). Keyless security in wireless networks. Wireless Personal Communications, 79(3): 1713-1731. https://doi.org/10.1007/s11277-014-1954-1

[26] Nabih, A., Hossain, A., Shepherd, S., Khaled, M. (2008). "Where you are" based authentication: An improved security protocol using BAN logic. In ECIW2008-Proceedings of the 7th European Conference on Information Warfare and Security: ECIW, p. 153. Academic Conferences Limited.

[27] Wang, M., Pan, J. (2014). RFID authentication protocol design via BAN logic. Journal of Chemical and Pharmaceutical Research, 6(7): 708-717.