QLAP: A Quantum-Resilient Security and Privacy Framework for Dynamic Spectrum Access

Saleh Darzi
University of South Florida
Tampa, Florida, USA
salehdarzi@usf.edu

Gökcan Cantali
Zurich University of Applied Sciences; University of Zurich
Winterthur; Zurich, Switzerland
canl@zhaw.ch

Dina Abdelhadi
Zurich University of Applied Sciences
Winterthur, Switzerland
abdh@zhaw.ch

Attila Altay Yavuz
University of South Florida
Tampa, Florida, USA
attilaayavuz@usf.edu

Gürkan Gür
Zurich University of Applied Sciences
Winterthur, Switzerland
gurkan.gur@zhaw.ch

Abstract

The widespread deployment of ultra-distributed computing infrastructure and the adoption of the edge-cloud continuum architecture create an ever-increasing need for spectrum access. Database-driven cognitive radio networks (DB-CRNs) are a promising avenue to addressing spectrum scarcity in the wireless access domain. Since DB-CRNs are a key component in emerging wireless access networks, they are expected to be future-proof, providing crucial quantum-resilient security and privacy. To this end, we propose `QLAP`, a post-quantum (PQ)-secure and privacy-preserving spectrum access framework for DB-CRNs that protects secondary user (SU) identity and location privacy while enabling verifiable proximity-backed location assurance and regulatory-compliant spectrum access under realistic adversarial settings, with demonstrated practical efficiency against both classical and quantum adversaries.

CCS Concepts

• **Security and privacy → Digital signatures**.

Keywords

Wireless and mobile security, post-quantum security, dynamic spectrum access, privacy

MobiArch '26, Austin, TX, USA

ACM ISBN 979-8-4007-2955-3/26/10
https://doi.org/10.1145/3842432.3843786

ACM Reference Format:
Saleh Darzi, Gökcan Cantali, Dina Abdelhadi, Attila Altay Yavuz, and Gürkan Gür. 2026. QLAP: A Quantum-Resilient Security and Privacy Framework for Dynamic Spectrum Access. In *Workshop on Mobility in the Evolving Internet Architecture (MobiArch '26), October 26–30, 2026, Austin, TX, USA.* ACM, Austin, Texas, USA, 7 pages. https://doi.org/10.1145/3842432.3843786

1 Introduction

The rapid growth of wireless services, driven by mobile computing, IoT deployments, and bandwidth-intensive applications, has increased pressure on traditional spectrum allocation models [1]. Database-driven cognitive radio networks (DB-CRNs) address this by allowing Secondary Users (SUs) to opportunistically access underutilized licensed spectrum through regulator-approved geolocation databases (DBs), with practical deployments such as CBRS in the 3.5 GHz band [1]. Despite their efficiency, DB-CRNs raise fundamental security and privacy concerns: regulatory policies require SUs to disclose precise location, device identifiers, and transmission parameters to centralized DBs, exposing them to location tracking, behavioral profiling, and long-term activity inference [10]. Since spectrum allocation depends directly on user-reported location, DB-CRNs are also inherently vulnerable to location-spoofing attacks [16]. These concerns become critical in the quantum era, where classical cryptographic mechanisms underlying existing solutions are broken by quantum adversaries [3, 7]. *No unified framework simultaneously provides PQ security, unlinkable anonymous SU access, location assurance, and regulatory DB-CRN compatibility.*

1.1 Prior Works and Open Problems

(i) Privacy-Preserving and Anonymous Spectrum Access: DB operators and logging systems can observe and correlate sensitive query metadata [1, 15] since SUs must repeatedly disclose location and device characteristics to DBs, even over secured

channels (e.g., TLS). Therefore, even coarse-grained reports can be correlated over time to infer identities and mobility patterns. Existing approaches address either anonymity or location privacy, but rarely both: anonymity alone cannot prevent tracking when location remains visible, whereas location obfuscation without unlinkability allows repeated queries to be correlated. Effective protection requires mechanisms jointly ensuring location privacy, anonymity, and unlinkability while remaining compatible with regulatory DB-CRN deployments.
(ii) Location Assurance and Spoofing Resistance: Since spectrum authorizations depend directly on user-reported location, malicious users may falsify location to obtain unauthorized access or disrupt operations [11]. Existing location-proof mechanisms rely on trusted infrastructure, specialized hardware, or dedicated verification servers [16], which may be unavailable in practical deployments. Fundamentally, privacy and verifiable location introduce an inherent tension: revealing precise location simplifies verification but compromises SU privacy, whereas concealing it may enable spoofing. Practical mechanisms must verify proximity without disclosing sensitive geographic data while resisting replay and spoofing attacks.
(iii) Spectrum Access in the Post-Quantum Era: Most privacy-preserving DB-CRN mechanisms rely on classical security assumptions (e.g., discrete logarithm, integer factorization), broken by quantum adversaries [3, 7]. Even schemes that partially address SU anonymity or location privacy, such as ring signatures [16] or PIR [9], lack end-to-end PQ security across authentication, location assurance, and spectrum access, a requirement that existing solutions leave unmet.

1.2 Our Contributions

We present `QLAP`*, a PQ-secure and privacy-preserving spectrum access framework for DB-CRNs that protects SU identity and location privacy while enabling verifiable proximity-backed location assurance and regulatory-compliant spectrum access under realistic adversarial settings, using a single database and unmodified access-network interfaces.*

• ***PQ-Secure Anonymous Spectrum Access:*** We develop a PQ-secure anonymous spectrum-access mechanism that protects SU identity and location privacy during spectrum queries. Unlike state-of-the-art schemes that rely on signature-based authentication and may expose identity or enable session linkability, our design leverages PQ Anonymous Credentials (PQ-AC) with selective disclosure to authenticate users without revealing identity, disclosing credential contents, or enabling cross-query linkage, providing stronger unlinkable access control compatible with regulatory DB-CRN architectures.

• ***PQ-Secure Privacy-Preserving Location Assurance and Spoofing Resistance:*** We develop a PQ-secure location assurance framework combining event-oriented PQ Linkable Ring Signatures (LRSs) with Access Point (AP)-backed proximity verification to provide anonymous yet verifiable proximity-backed location assurance. Access decisions are bound to fresh, context-specific proximity evidence, while LRS-based rate limiting enforces bounded reuse of proof-of-location (PoL) artifacts per epoch, providing event-scoped resistance against replay and spoofing without revealing SU identity. Architecturally, this separates attestation from policy: the AP verifies physical presence at the access edge while the PSD enforces regulatory constraints without ever observing an identity-bound location, a trust decomposition that prior DB-CRN designs collapse into the database.

• ***Performance Analysis and Benchmarking:*** We provide analytical and empirical evaluation through primitive-level micro-benchmarks, computational and communication complexity analysis, and end-to-end overhead assessment. We compare `QLAP` against state-of-the-art DB-CRN schemes and demonstrate stronger security guarantees under a single-DB architecture, with over 30% lower E2E delay and 2.8-4.1× less communication overhead than the prior PQ-capable schemes.

2 Preliminaries, Building Blocks, and Models

This section introduces the notation, system architecture, and primitives that underpin the proposed framework.

Notations: The operators $||$, $|x|$, and $\{0,1\}^k$ denote concatenation, the bit-length of x, and the set of k-bit strings, respectively. Let λ denote the security parameter and $H(\cdot)$ denote a cryptographic hash function. For a sequence $\{x_i\}_{i=1}^{\ell}$ we write $(x_1, \ldots, x_\ell)$. Secret keys, public keys, and identities are denoted by sk, PK, and `ID`, respectively, and protocol messages by $m \in \mathcal{M}$. The symbol $\leftrightarrow$ denotes an interactive protocol execution. $\mathsf{negl}(\lambda)$ denotes a negligible function in λ and $\Pr[\cdot]$ denotes probability over the randomness of the experiment.

2.1 System Architecture: DB-CRN

A DB-CRN is a regulated spectrum-sharing framework in which unlicensed devices obtain transmission authorization by querying certified geolocation DBs [13], deployed in systems such as TVWS and CBRS under regulatory oversight [4]. The *spectrum regulator* (e.g., FCC) defines DB-CRN rules, certifies DB operators, and provides authoritative incumbent data [1]. *Private Spectrum DBs (PSDs)* maintain incumbent records and access policies [5], processing SU queries against regulatory constraints to return channel assignments, power limits, and validity intervals [1]. *User Equipments (UEs)* are unlicensed SU devices, such as mobile phones, IoT devices, or fixed terminals, that determine their location, query a PSD, and operate on authorized channels [8]. *Access Points (APs)* (e.g., WiFi router, LTE eNodeB, 5G gNodeB) provide last-hop connectivity and, in enhanced settings, support privacy-preserving proximity verification and proof-of-location generation while remaining separate from spectrum control. *Servers* are application-layer entities accessed by UEs post-authorization that operate at the service layer only [10].

Communication Flow: DB-CRN operation follows a standard IP-based client-server model [1]: a UE attaches to a nearby AP (IEEE 802.11 or 3GPP LTE/5G) [12], submits spectrum queries to a PSD via HTTPS/TLS (IETF PAWS, RFC-7545), and receives authorized channels, power limits, and validity intervals [1]; it then communicates with servers over approved spectrum using standard IP protocols, with no modification to existing infrastructure.

2.2 Building Blocks

Anonymous Credentials (AC): We use a PQ AC scheme [2] supporting multi-level attribute issuance and anonymity.

DEFINITION 1. A PQ-AC scheme is defined by the following polynomial-time algorithms and interactive protocols:

- $\texttt{Setup}(1^\lambda, 1^t) \to (pp, sk_I, PK_I)$; $\texttt{KeyGen}(pp) \to (PK_U, sk_U)$; $\texttt{NymGen}(PK_U) \to (nym_U, aux_U)$: Parameter generation, issuer/user key pairs, and fresh unlinkable pseudonym with auxiliary randomness.
- $\texttt{IssueCred}(PK_I, sk_I, sk_U, A) \leftrightarrow \texttt{ReceiveCred}(PK_I, PK_U) \to cred_U$: Interactive issuance; the user obtains credential $\texttt{cred}_U$ bound to attribute set A.
- $\texttt{CredProve}(PK_I, sk_U, nym_U, aux_U, cred_U, A_D, m) \leftrightarrow \texttt{CredVerify}(PK_I, nym_U, A_D, m) \to \{0,1\}$: Zero-knowledge presentation; the user anonymously proves possession of $\texttt{cred}_U$ while selectively disclosing $A_D \subseteq A$, with the proof bound to message m. The verifier extracts $\texttt{nym}_U$ from the proof transcript.

Linkable Ring Signature (LRS): Ring signatures allow anonymous signing on behalf of a group; LRSs additionally detect multiple signatures by the same signer. We adopt the PQ-secure event-oriented LRS of [17], built from a hash function and STARK-based Signature of Knowledge (SoK). An event identifier $e_{\texttt{ID}}$ is embedded per signature, enabling linkability across signatures sharing the same key and $e_{\texttt{ID}}$ via tag matching, without revealing signer identity.

DEFINITION 2. An LRS consists of four algorithms:

- $\texttt{LRS.Gen}(1^\lambda) \to pp$; $\texttt{LRS.KeyGen}(pp) \to (sk, PK)$: Parameter and key generation.
- $\texttt{LRS.Sign}(e_{ID}, sk_{l_r}, m, \mathrm{R}) \to \sigma$: igns m anonymously on behalf of ring R under event $e_{\texttt{ID}}$.
- $\texttt{LRS.Verify}(e_{ID}, \sigma, m, \mathrm{R}) \to \{0,1\}$: Verifies signature σ on m w.r.t. ring R and event $e_{\texttt{ID}}$.
- $\texttt{LRS.Link}(e_{ID}, m, \sigma, m', \sigma', \mathrm{R}, \mathrm{R}') \to \{0,1\}$: Returns 1 if the same signer generated (σ, σ') under $e_{\texttt{ID}}$, 0 otherwise.

2.3 Threat Model and Scope

Threat Model: We consider a quantum-capable probabilistic polynomial-time (QPT) adversary with full control over the wireless channel between UEs and infrastructure (PSDs, APs, servers). The adversary may eavesdrop, inject, modify, replay, delay, or block messages. Malicious UEs may issue adaptive queries and submit manipulated location information to gain unauthorized access or amplify leakage. The FCC is trusted as the root authority for key provisioning and credential issuance; APs are certified entities with valid long-term keys for PoL generation. APs, PSDs, and servers are honest-but-curious: they follow the protocol but may attempt to infer user identity, session linkability, or precise location from transcripts, metadata, or repeated queries. The adversary mounts two representative attacks: *(i) SU Privacy and Anonymity*: PSDs, servers, or external observers may infer UE identity, location, or device attributes, or link sessions via message or metadata analysis; and *(ii) Location Spoofing*: malicious UEs submit falsified or replayed location/proximity information, reuse PoL artifacts, or exploit relay-assisted proximity manipulation [11].

Scope: QLAP protects SU identity and location privacy during spectrum queries and service access, and enforces bounded PoL reuse against replay and spoofing under PQ security guarantees. While location is disclosed in plaintext to certified entities for authorization, it remains unlinkable to any persistent SU identity via PQ-AC QLAP covers exclusively the spectrum query and access phases, and does not address privacy risks during user registration, credential provisioning, or post-authorization spectrum utilization, including location leakage during mobility or handover [13]. Although QLAP is extensible to PU interactions with PSDs, PU-related protections are out of scope. Timing attacks, side-channel leakage, and physical-layer localization (e.g., triangulation or signal analysis) are also excluded [10].

3 The Proposed Scheme: QLAP

This section outlines the QLAP framework, detailing its initial setup, core operations, and security analysis.

3.1 QLAP Framework Initial Setup

Access Point Configuration: APs within a region form a logical ring; each holds a key pair $(sk_{\texttt{AP}}, PK_{\texttt{AP}})$ generated by the FCC via $\texttt{LRS.KeyGen}(pp, \texttt{ID}_{\texttt{AP}})$ (Def. 2). APs are organized into region-specific rings whose membership digests are distributed by the regulator for a bounded validity window; compromised or retired APs are excluded in subsequent updates. APs periodically broadcast time-synchronized beacons $\beta_{\texttt{TW}}$ during epochs TW. Proximity is evaluated as $\Delta \leftarrow \texttt{ProxVerify}(RSS, RTT, env_{params})$ using received signal strength (RSS) and round-trip time (RTT), where environment parameters such as path-loss or multipath refine distance estimation [14]. Finally, the result is compared against a threshold Δ_{th} to determine whether the UE lies within the AP's trusted proximity region.

System Initialization: The FCC generates public parameters pp, publishes $PK_{\texttt{FCC}}$, and issues each UE a credential $\texttt{cred}_{\texttt{UE}} \leftarrow \texttt{IssueCred}(PK_{\texttt{FCC}}, sk_{\texttt{FCC}}, PK_{\texttt{UE}}, A)$ binding attributes A (e.g., registration status, device class, maximum transmission power, expiration) without revealing identity. Spectrum DBs maintain FCC-compliant records indexed by

Algorithm 1 QLAP Scheme

1 $(m, A_D) \leftarrow \texttt{UE.PoL.Request}(\beta_{\texttt{TW}})$:

1: Given the latest beacon $\beta_{\texttt{TW}}$:
2: $A_D \leftarrow (reg_{\texttt{UE}}, \texttt{UE}_{class}, \texttt{MTP}, t_{Exp})$ and Set $m \leftarrow ((l_x, l_y), \texttt{TW}, \beta_{\texttt{TW}})$
3: $\texttt{CredProve}(PK_{\texttt{FCC}}, sk_{\texttt{UE}}, \texttt{nym}_{\texttt{UE}}, \texttt{aux}_{\texttt{UE}}, \texttt{cred}_{\texttt{UE}}, A_D, m)$
4: Send (m, A_D) to AP

2 $(\sigma_{\texttt{AP}}, e_{\texttt{ID}}) \leftarrow \texttt{AP.PoL.Response}(m, A_D)$:

5: **If** $1 = \texttt{CredVerify}(PK_{\texttt{FCC}}, \texttt{nym}_{\texttt{UE}}, A_D, m)$
6: **If** $\beta_{\texttt{TW}}$ is not the latest beacon, **Return** $\perp$
7: **Else** $\Delta_{\texttt{UE}} \leftarrow \texttt{ProxVerify}(RSS, RTT, env_{params})$
8: **If** $(l_x, l_y) \in \Delta_{\texttt{UE}}$ and $\Delta_{\texttt{UE}} \leq \Delta_{th}$:
9: $h_{\texttt{AP}} \leftarrow H((l_x, l_y)||\texttt{TW})$ and $e_{\texttt{ID}} \leftarrow H'(R_{\texttt{AP}}, h_{\texttt{AP}}, \texttt{nym}_{\texttt{UE}})$
10: $\sigma_{\texttt{AP}} \leftarrow \texttt{LRS.Sign}(e_{\texttt{ID}}, h_{\texttt{AP}}, sk_{\texttt{AP}})$; Send $(\sigma_{\texttt{AP}}, e_{\texttt{ID}})$ to UE

3 $\{\Phi_{\texttt{UE}}, \perp\} \leftarrow \texttt{UE.PoL.Verify}(\sigma_{\texttt{AP}}, e_{\texttt{ID}})$:

11: **If** $1 = \texttt{LRS.Verify}(e_{\texttt{ID}}, \sigma_{\texttt{AP}}, h_{\texttt{AP}}, R_{\texttt{AP}})$,
12: **Return** $\Phi_{\texttt{UE}} \leftarrow (h_{\texttt{AP}}, \sigma_{\texttt{AP}}, e_{\texttt{ID}})$

4 $q_{\texttt{UE}} \leftarrow \texttt{UE.Query}((l_x, l_y), \texttt{cred}_{\texttt{UE}}, \Phi_{\texttt{UE}})$:

13: Given $((l_x, l_y), \texttt{TW}, (\texttt{Ch}, \texttt{EIRP}, \texttt{TV}))$, UE **do**:
14: $A_D \leftarrow (reg_{\texttt{UE}}, \texttt{UE}_{class}, \texttt{MTP}, t_{Exp})$
15: Set $m_q \leftarrow ((l_x, l_y), \texttt{TW}, \Phi_{\texttt{UE}}, (\texttt{Ch}, \texttt{EIRP}, \texttt{TV}))$
16: $\texttt{CredProve}(PK_{\texttt{FCC}}, sk_{\texttt{UE}}, \texttt{nym}_{\texttt{UE}}, \texttt{aux}_{\texttt{UE}}, \texttt{cred}_{\texttt{UE}}, A_D, m_q)$
17: Query a PSD for $q_{\texttt{UE}} \leftarrow (m_q, A_D)$

5 $\rho_{\texttt{PSD}} \leftarrow \texttt{PSD.Respond}(q_{\texttt{UE}})$:

18: **If** $1 = \texttt{CredVerify}(PK_{\texttt{FCC}}, \texttt{nym}_{\texttt{UE}}, A_D, m_q)$
19: **If** $h_{\texttt{AP}} \neq H((l_x, l_y)||\texttt{TW})$, **Return** $\perp$
20: **If** $1 = \texttt{LRS.Verify}(e_{\texttt{ID}}, \sigma_{\texttt{AP}}, h_{\texttt{AP}}, R_{\texttt{AP}})$, Record $(\sigma_{\texttt{AP}}, e_{\texttt{ID}})$
21: **If** $e_{\texttt{ID}} = H'(R_{\texttt{AP}}, h_{\texttt{AP}}, \texttt{nym}_{\texttt{UE}})$, **For all** $i \in \texttt{TW}$:
22: **If** $1 = \texttt{LRS.Link}(e_{\texttt{ID}}, h_{\texttt{AP}}, \sigma_{\texttt{AP}}, h_i, \sigma_i, R_{\texttt{AP}}, R_i)$, **Return** $\perp$
23: Send $\rho_{\texttt{PSD}}$ for (l_x, l_y), TW to UE

6–7 Service Request & Server Respond: Mirror blocks **4–5** with $req \leftarrow \rho_{\texttt{PSD}}$ and $m_r \leftarrow ((l_x, l_y), \texttt{TW}, \Phi_{\texttt{UE}}, req)$; server verifies CredVerify, checks $h_{\texttt{AP}}$, and performs LRS.Verify identically.

geographic coordinates (e.g., 50 m granularity), storing availability, validity intervals (TV), and EIRP limits. The UE later proves credential possession via CredProve, selectively disclosing $A_D \subseteq A$ while preserving unlinkability; $\texttt{nym}_{\texttt{UE}}$ is refreshed across independent sessions and fixed only within a narrowly scoped PoL event when accountability is required.

3.2 QLAP Framework Main Operations

The overall workflow of QLAP is illustrated in Figure 1 and detailed in Algorithm 1.

1) Proof of Location: Before spectrum querying, the UE must obtain a PoL bound to its region and epoch TW. Beacons $\beta_{\texttt{TW}}$ are region-scoped, time-dependent tokens without AP-specific identifiers; upon receiving one from a nearby AP, the UE prepares disclosure set A_D, constructs m, and proves credential possession via CredProve over (A_D, m), sending (m, A_D) to the strongest AP (Steps 1-4). The AP verifies the credential, checks $\beta_{\texttt{TW}}$ freshness to prevent replay, and evaluates proximity via ProxVerify; if the UE lies within Δ_{th}, it computes the location-time binding $h_{\texttt{AP}}$, derives $e_{\texttt{ID}}$

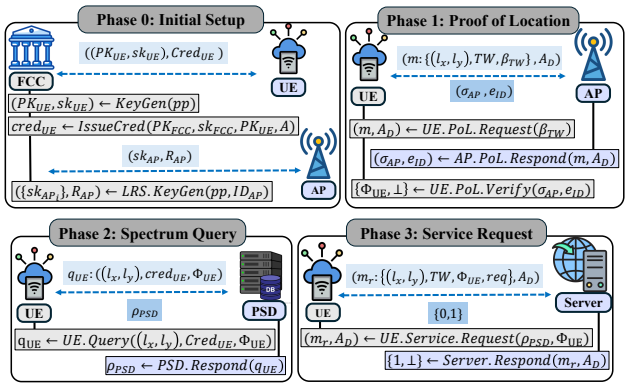

Figure 1: An overview of the QLAP main operations.

linking the AP ring, context, and UE pseudonym, and returns LRS $\sigma_{\texttt{AP}}$ over the ring $R_{\texttt{AP}}$ (Steps 5-11). The UE accepts $\Phi_{\texttt{UE}}$ as a valid PoL upon successful LRS.Verify.

2) Spectrum Query: The UE constructs m_q binding $\Phi_{\texttt{UE}}$ and query parameters (Ch, EIRP, TV), proves CredProve over (A_D, m_q), and submits $q_{\texttt{UE}} = (m_q, A_D)$ to the PSD (Steps 14-18). The PSD verifies the credential, checks the consistency of $h_{\texttt{AP}}$, and verifies the LRS $\sigma_{\texttt{AP}}$ to confirm AP legitimacy. It then applies LRS.Link over all epoch-TW signatures to detect multiple queries sharing the same event identifier and enforce bounded PoL reuse, rejecting linked requests while preserving SU anonymity (Steps 19-23). Upon passing all checks, the PSD evaluates spectrum availability against incumbent constraints and returns the grant $\rho_{\texttt{PSD}}$ (Step 24).

3) Service Access: After receiving $\rho_{\texttt{PSD}}$, the UE may report spectrum usage to the PSD or request services from an authorized server. The UE constructs m_r bound to $\Phi_{\texttt{UE}}$ and executes CredProve over (A_D, m_r), sending (m_r, A_D) to the PSD/server. The server mirrors the query-phase verification: CredVerify, $h_{\texttt{AP}}$ consistency, and LRS.Verify with LRS.Link for event-scoped replay detection, granting services upon success.

3.3 Security Analysis

Based on the threat model in Section 2.3, we prove that QLAP is secure in Theorem 1 below. Here, $\text{Adv}^{X}_{\mathcal{A}}(\lambda)$ denotes the advantage of a QPT adversary $\mathcal{A}$ in winning security experiment X, and $\text{Adv}^{X}_{\mathcal{B}}(\lambda)$ that of a reduction algorithm $\mathcal{B}$.

Theorem 1. *For any QPT adversary interacting with QLAP, the framework achieves, except with probability* $\text{negl}(\lambda)$*: (i) anonymous and unforgeable UE authentication, reducible to M-LWE/M-SIS hardness and zero-knowledge simulation-indistinguishability [2]; (ii) UE session unlinkability and privacy-preserving access, reducible to randomized-presentation privacy, selective-disclosure hiding, and witness-indistinguishable knowledge proofs over event-bound authentication transcripts [17]; (iii) verifiable and non-forgeable proximity-backed location assurance, reducible to correctness and extractability of the underlying knowledge-signature system,*

collision-/second-preimage resistance of the hash functions, and the soundness of AP-assisted proximity verification [14].

PROOF. *(i) Authentication and Anonymity:* Authentication relies on `CredProve` and `CredVerify` across all protocol phases. A forged PQ-AC presentation for undisclosed attributes implies breaking M-LWE/M-SIS hardness or zero-knowledge soundness. Since $\mathtt{nym}_{\mathtt{UE}} \leftarrow \mathtt{NymGen}(PK_{\mathtt{UE}})$ is freshly randomized per session and `CredProve` produces transcripts computationally indistinguishable from simulated ones, the anonymity holds; a non-negligible distinguishing advantage would imply breaking LWE pseudorandomness or zero-knowledge simulation-indistinguishability [2]. *(ii) Session Unlinkability and Location Privacy:* Unlinkability follows jointly from PQ-AC unlinkability and LRS anonymity. Pseudonyms are refreshed across independent sessions, and credential presentations are randomized, so transcripts remain computationally indistinguishable across sessions. The PoL artifact $\Phi_{\mathtt{UE}} = (h_{\mathtt{AP}}, \sigma_{\mathtt{AP}}, e_{\mathtt{ID}})$ reveals no UE identity beyond the spatio-temporal binding $h_{\mathtt{AP}} = H((l_x, l_y) \| \mathtt{TW})$; by LRS anonymity, the AP signer remains hidden within the ring. Hence $\mathsf{Adv}^{\mathsf{link}}_{\mathcal{A}}(\lambda) \le \mathsf{Adv}^{\mathsf{PQAC-unlink}}_{\mathcal{B}}(\lambda) + \mathsf{Adv}^{\mathsf{LRS-anon}}_{C}(\lambda) \le \mathsf{negl}(\lambda)$. *(iii) Location Assurance and Spoofing Resistance:* $h_{\mathtt{AP}} = H((l_x, l_y) \| \mathtt{TW})$ and $e_{\mathtt{ID}} = H'(R_{\mathtt{AP}}, h_{\mathtt{AP}}, \mathtt{nym}_{\mathtt{UE}})$ are computed by the AP, and $\sigma_{\mathtt{AP}} \leftarrow \mathtt{LRS.Sign}(e_{\mathtt{ID}}, h_{\mathtt{AP}}, sk_{\mathtt{AP}})$ is outputted. Forging a valid PoL without physical proximity requires one of: (1) forging an LRS signature without a ring secret key, violating LRS unforgeability; (2) finding a collision or preimage in H or H'; or (3) violating soundness of `ProxVerify`, each negligible by assumption. Bounded PoL reuse is enforced by LRS linkability: reusing the same event-bound artifact requires $\mathtt{LRS.Link}(e_{\mathtt{ID}}, \sigma_1, \sigma_2) = 0$ under the same key and event, contradicting linkability. Fully robust anti-relay or distance-bounding guarantees are outside the current instantiation. □

4 Performance Evaluation

We evaluate the performance of `QLAP` through implementation-based benchmarking, analytical overhead modeling, and comparison with representative state-of-the-art schemes.

4.1 Configuration and Experimental Setup

Hardware and Libraries: We evaluate `QLAP` on an Intel Core *i9-11900K* @3.50*GHz*, 64GiB RAM, 1TB, Ubuntu 22.04 .4 LTS. The implementation spans C, Python, and Rust, using the PQ-AC library[1], *liboqs*[2] for PQ primitives, OpenSSL for hashing and modular arithmetic, and a PQ-LRS repository[3].

Configuration and Parameters: Physical-layer and network delays are excluded as deployment-dependent; all measurements use single-core execution. `QLAP` is instantiated at NIST Level I PQ security (≈128-bit [3]) with all components aligned to M-LWE/M-SIS assumptions. SHA-256 serves as the hash function; LRS relies on STARK-based proofs of knowledge with Rescue-Prime hash and Merkle commitments. Parameters are selected conservatively to satisfy the target security level across all protocol phases.

Evaluation Metrics: We benchmark computational and communication costs across all entities and protocol phases, quantifying PQ-AC proof generation/verification and LRS signing/verification, with qualitative and analytical comparison against representative DB-CRN schemes. The E2E delay captures the spectrum-query phase, including PoL acquisition and spectrum-availability retrieval from the DBs.

4.2 Experimental Results

The overhead evaluation of `QLAP` is summarized in Table 1.

• **Computational Costs:** Credential issuance is excluded (one-time at registration); the dominant runtime cost is PQ-AC proof generation/verification, with LRS contributing smaller overhead. *(i) PoL:* Signing complexity grows quasi-linearly with ring size $n_{\mathtt{AP}}$, while UE-side LRS verification scales polylogarithmically in $n_{\mathtt{AP}}$ (e.g., 2^3-2^{13}) and remains lightweight (∼1.4-8 ms). The UE generates a PQ-AC proof (module lattice operations, Gaussian/rejection sampling, and hashing: 268.6-398.47 ms); the AP verifies the credential and generates an LRS signature (220.53-226.32 ms); `ProxVerify` adds 1-10 ms. *(ii) Spectrum Query:* Dominated by PQ-AC: 262-392 ms at the UE and 206-212 ms at the PSD, plus LRS verification and event-scoped linkability checks over epoch-`TW` signatures. *(iii) Service Request:* Mirrors the query phase without DB evaluation; UE: 262-392 ms, server: 161-167 ms via PQ-LRS verification and hash checks.

• **Communication Overhead:** *(i) PoL:* The UE transmits minimal metadata-coordinates (16 B), beacon (32 B), timestamp (8 B)-plus a PQ-AC proof; the `PoL` artifact ranges 18-22 KB depending on STARK parameters and ring size $n_{\mathtt{AP}}$ (2^6–2^{13}, 99-128-bit security), for a total of 83.53-121.2 KB; verification is non-interactive with no additional communication. *(ii) Spectrum Query:* Overhead is dominated by the PQ-AC proof $\pi(\lambda, m, t)$ at 64-99 KB; the PSD returns a single grant $\rho_{\mathtt{PSD}}$ of ∼560 bytes, so the response is $O(1)$. *(iii) Service Request:* Mirrors the query phase (64-99 KB); the server returns a constant-size authorization token, so overhead is independent of $|\mathtt{DB}|$ and dominated by PQ-AC proof transmission.

• **Comparison with SOTA:** Most DB-CRN schemes rely on classical assumptions (e.g., DL, CDH, RSA, pairings) broken by quantum adversaries, and address SU location privacy or anonymity in isolation, via homomorphic encryption [18], PIR, pseudonyms [19], or group/ring signatures, without jointly providing both alongside cryptographically authenticated location assurance. PIR-based schemes [6, 9]

[1] https://github.com/Chair-for-Security-Engineering/lattice-anonymous-credentials

[2] https://openquantumsafe.org/

[3] https://github.com/yuxi16/Post-Quantum-Linkable-Ring-Signature

Table 1: Computational and communication overhead of QLAP.

Phase	Entity	Computational Complexity	Communication Complexity	Computational (*ms*)	Communication (*KB*)
PoL Phase	UE	$\Theta(n_{\mathrm{AP}}) \cdot \mathsf{H}' + O(\mathrm{polylog}(\log(n_{\mathrm{AP}}))) + O(d_b) \cdot \mathsf{M} + O(1) \cdot \mathsf{Q} + O(1) \cdot \mathsf{S} + O(\rho_S) \cdot \mathsf{R} + 4\mathsf{H}$	$O(\mathrm{polylog}(\log(n_{\mathrm{AP}})))$	268.6 – 398.47	83.53 – 121.2
	AP	$(\lvert\mathtt{TW}\rvert + \Theta(n_{\mathrm{AP}})) \cdot \mathsf{H}' + O(\log(n_{\mathrm{AP}}) \cdot \log\log(n_{\mathrm{AP}})) + \mathsf{H} + + O(d_b) \cdot \mathsf{M} + O(1) \cdot \mathsf{Q} + O(1) \cdot \mathrm{Norm}$	$+O(\lvert\pi(\lambda, m, t)\rvert)$	220.53 – 226.32	
Spectrum Query	UE	$O(d_b) \cdot \mathsf{M} + O(1) \cdot \mathsf{Q} + O(1) \cdot \mathsf{S} + O(\rho_S) \cdot \mathsf{R} + 4\mathsf{H}$	$O(\lvert\pi(\lambda, m, t)\rvert) +$	262 – 392.12	64.63 – 99.26
	PSD	$O(d_b) \cdot \mathsf{M} + O(1) \cdot \mathsf{Q} + O(1) \cdot \mathrm{Norm} + 4\mathsf{H} + \lvert\mathtt{TW}\rvert \cdot \mathsf{H}' + \Theta(n_{\mathrm{AP}}) \cdot \mathsf{H}' + O(\log(n_{\mathrm{AP}}) \cdot \log\log(n_{\mathrm{AP}}))$	$O(\mathrm{polylog}(\log(n_{\mathrm{AP}})))$	206.18 – 211.97	
Service Request	UE	$O(d_b) \cdot \mathsf{M} + O(1) \cdot \mathsf{Q} + O(1) \cdot \mathsf{S} + O(\rho_S) \cdot \mathsf{R} + 4\mathsf{H}$	$O(\lvert\pi(\lambda, m, t)\rvert) +$	262 – 392.12	64.07 – 98.7
	Server	$O(d_b) \cdot \mathsf{M} + O(1) \cdot \mathsf{Q} + O(1) \cdot \mathrm{Norm} + \mathsf{H} + (\lvert\mathtt{TW}\rvert + \Theta(n_{\mathrm{AP}})) \cdot \mathsf{H}' + O(\log(n_{\mathrm{AP}}) \cdot \log\log(n_{\mathrm{AP}})) + \mathsf{H}$	$O(\mathrm{polylog}(\log(n_{\mathrm{AP}})))$	161.18 – 166.97	

Notes: n_{AP} denotes the number of APs in the region forming a group. $|\mathtt{TW}|$ is the number of prior event-bound signatures checked for replay or repeated-reuse detection within the current time window. H' denotes the Rescue-Prime hash cost (PQ-LRS), H is the hash cost (e.g., SHA-256), M is a module matrix-vector multiplication where, for module dimension d_b and ring degree n_b, $\mathsf{M} = O(d_b n_b \log n_b)$. Q denotes a quadratic-form evaluation, S Gaussian sampling, R rejection sampling with expected repetition factor ρ_S, and Norm Euclidean bound checks. $|\pi(\lambda, m, t)|$ denotes the PQ-AC proof size for the security parameter λ with m hidden attributes and maximum attribute capacity t.

require ℓ synchronized PSDs, provide no location verification, and incur 125-6000 KB/query (LP-Chor: 753 KB, LP-Goldberg: 6000 KB, RAID-LP-Chor: 125 KB, TrustSAS: 1250 KB); they achieve only partial PQ security through IT-secure PIR while lacking PQ authentication and location assurance. Schemes providing location verification, such as Li *et al.* [11], Xin *et al.* [16], SLAP [8], rely on classical AP-backed mechanisms (PPT, Ring.Sig, Group.Sig) within 1-DB architectures, offering no quantum resilience. PACDoSQ [7]-the only fully PQ-capable prior scheme-provides SU privacy via PIR and anonymity via PQ-Tor, but offers no location assurance and suffers 1373.6 ms E2E delay and 605.92 KB overhead due to multi-hop PQ-Tor and PIR. In contrast, QLAP uniquely combines SU location privacy and unlinkable anonymous access via PQ-AC, proximity-backed location assurance via PQ-LRS with AP-backed proximity verification, and full end-to-end PQ security (M-LWE, M-SIS)-all within a *single*-DB architecture requiring no replicated PSDs or dedicated verification servers. QLAP achieves 957.31 ms E2E delay (>30% lower than PACDoSQ) and 148-220 KB overhead; for PoL, QLAP (489.13 ms UE+AP) is the only PQ-secure option vs. classical counterparts: SLAP [8] (107.17 ms), Li *et al.* [11] (210 ms), Xin *et al.* [16] (430 ms), which require auxiliary infrastructure and offer no quantum resilience.

• **Scalability, Mobility, and Network Effects:** Reported delays are compute-bound; transferring the 148-220 KB payload over a 10-50 Mbps uplink adds 24-176 ms (2-18%), keeping QLAP ahead of PACDoSQ. Scalability rests on two tunable parameters: the ring size n_{AP}, whose 2^3-2^{13} sweep spans rural to dense urban densities with polylogarithmic UE-side growth, and the epoch $|\mathtt{TW}|$, which linearly bounds the PSD's linkability check. A PoL stays valid region-wide for a full epoch, so intra-region mobility is free; entering a new region re-runs only the PoL phase (489.13 ms).

• **Deployment and Standards Compatibility:** QLAP leaves the DB-CRN control plane unchanged. The beacon $\beta_{\mathtt{TW}}$ carries no AP identifier and fits an existing broadcast field (802.11 vendor IE or 3GPP SIB), while $\Phi_{\mathtt{UE}}$ and the credential presentation ride as opaque parameters in the PAWS available-spectrum request; the PHY, query schema, FCC DB records, and UE radio are untouched. Deployment thus reduces to a software update at APs and a verification module at PSDs. The trade-offs are that APs must hold FCC-issued keys and be trusted for proximity evaluation, and that TW balances linkability resolution against unlinkability. Architecturally, location assurance moves from the database to the access edge: the AP attests presence, the PSD stays a pure policy engine, and regulatory enforcement no longer requires the database to observe identity-bound location.

5 Conclusion

We presented QLAP, a PQ-secure and privacy-preserving spectrum access framework for DB-CRNs. By combining PQ-AC and PQ-LRSs, QLAP protects SU identity and location privacy, provides verifiable proximity-backed location assurance, and enforces epoch-scoped spoofing resistance-all within a single-DB architecture compatible with regulatory DB-CRN deployments. Formal security analysis and empirical evaluation confirm strong guarantees against both classical and quantum adversaries, achieving more than 30% decrease in E2E latency and a significant reduction in communication overhead compared to the SOTA schemes.

Acknowledgement

This work has received co-funding from the NSF and SNSF, in the framework of the SATUQ project under SNSF (Grant No 10000409) and NSF (ECCS 2444615).

References

[1] Pranay Agarwal, Mohammedhusen Manekiya, Tahir Ahmad, Ashish Yadav, Abhinav Kumar, and Donelli. 2022. A survey on citizens broadband radio service (cbrs). *Electronics* 11, 23 (2022), 3985.

[2] Sven Argo, Tim Güneysu, Corentin Jeudy, Georg Land, Adeline Roux-Langlois, and Olivier Sanders. 2024. Practical post-quantum signatures for privacy. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*. 1523–1537.

[3] Ritik Bavdekar, Eashan Jayant Chopde, Ankit Agrawal, Ashutosh Bhatia, and Kamlesh Tiwari. 2023. Post quantum cryptography: a review of techniques, challenges and standardizations. In *2023 International Conference on Information Networking (ICOIN)*. IEEE, 146–151.

[4] Marcello Caleffi and Angela Sara Cacciapuoti. 2014. Database access strategy for TV white space cognitive radio networks. In *2014 Eleventh Annual IEEE International Conference on SECON Workshops*. 34–38.

[5] V Chen, S Das, L Zhu, J Malyar, and P McCann. 2015. *Protocol to access white-space (paws) databases*. Technical Report.

[6] Saleh Darzi and Attila A Yavuz. 2024. Counter denial of service for next-generation networks within the artificial intelligence and post-quantum era. In *2024 IEEE 6th International Conf. on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*. IEEE.

[7] Saleh Darzi and Attila Altay Yavuz. 2024. Privacy-Preserving and Post-Quantum Counter Denial of Service Framework for Wireless Networks. In *MILCOM 2024- IEEE Military Communications Conference*. IEEE.

[8] Saleh Darzi and Attila A Yavuz. 2025. SLAP: Secure Location-proof and Anonymous Privacy-preserving Spectrum Access. (2025), 1–8.

[9] Mohamed Grissa and Attila Altay Yavuz. 2019. Location privacy in cognitive radios with multi-server private information retrieval. *IEEE Trans. on Cognitive Comm. and Networking* (2019).

[10] Doaa K Jasim and Sattar B Sadkhan. 2021. Cognitive radio network: Security and reliability trade-off-status, challenges, and future trend. In *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*. IEEE, 149–153.

[11] Yi Li, Lu Zhou, Haojin Zhu, and Limin Sun. 2015. Privacy-preserving location proof for securing large-scale database-driven cognitive radio networks. *IEEE IoT Journal* 3, 4 (2015).

[12] Ying-Chang Liang, Kwang-Cheng Chen, and Geoffrey Ye Li. 2011. Cognitive radio networking and communications: An overview. *IEEE transactions on vehicular technology* 60, 7 (2011).

[13] Anita Patil, Sridhar Iyer, Onel L.A. López, Rahul J. Pandya, and Krishna Pai. 2024. A comprehensive survey on spectrum sharing techniques for 5G/B5G intelligent wireless networks: Opportunities, challenges and future research directions. *Computer Networks* 253 (2024).

[14] Sascha Rösler, Nils Eising, and Anatolij Zubow. 2025. Improving WiFi Ranging Through Frequency Diversity and Mobility. In *2025 IEEE 50th Conf. on Local Computer Networks (LCN)*.

[15] Shanghao Shi, Yang Xiao, Wenjing Lou, and Chonggang Wang. 2021. Challenges and new directions in securing spectrum access systems. *IEEE Internet of Things Journal* 8, 8 (2021).

[16] Jiajun Xin, Ming Li, and Changqing Luo. 2016. Privacy-preserving spectrum query with location proofs in database-driven CRNs. In *2016 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 1–6.

[17] Yuxi Xue, Xingye Lu, and Man Ho Au. 2024. Efficient linkable ring signatures: new framework and post-quantum instantiations. In *European Symposium on Research in Computer Security*. Springer.

[18] He Yu, Shanghao Shi, Yi Shi, and Eric Burger. 2024. Pri-Share: Enabling Inter-SAS Privacy Protection via Secure Multi-Party Spectrum Allocation. In *2024 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. IEEE, 347–356.

[19] Yali Zeng, Li Xu, Xu Yang, and Xun Yi. 2019. An efficient privacy-preserving protocol for database-driven cognitive radio networks. *Ad hoc networks* 90 (2019), 101739.