IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Post-quantum secure anonymous authentication for smart cities

Ali Hamzah Obaid[1], Khansaa Azeez Obayes Al-Husseini[1], Mahmood A. Al-Shareeda[2*], Mohammed Amin Almaiah[3], Rami Shehab[4]

[1]Babylon Technical Institute, Al-Furat Al-Awsat Technical University, Babylon, Iraq.
[2]Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, Iraq.
[3]King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan.
[4]Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa, Saudi Arabia.

Corresponding author: Mahmood A. Al-Shareeda (*Email: mahmood.alshareedah@stu.edu.iq*)

Abstract

The explosive growth of smart city infrastructures demands secure and private message exchange between heterogeneous IoT devices deployed in the city. Standard authentication schemes, primarily based on elliptic curve cryptography (ECC) or symmetric primitives, are vulnerable to future quantum adversaries and, thus, are not suitable for extended deployment in public urban settings. In this work, we introduce a new post-quantum anonymous authentication scheme that is based on key encapsulation via CRYSTALS-Kyber and signatures via CRYSTALS-Dilithium. This scheme is able to provide mutual authentication, user anonymity, perfect forward secrecy, and lightweight communication, making it applicable to resource-constrained environments in typical scenarios of smart cities. We provide a formal security proof of our construction under the RealOr-Random model for quantum adversaries (ROR-Q) and an informal analysis showing security against a number of attacks, including impersonation, replay, man-in-the-middle, and key compromise. We provide experimental evaluation on constrained platforms to show the feasibility of the protocol in terms of computational cost and the efficiency of the proposed solution for bandwidth validation for modern smart city applications.

Keywords: Anonymity, Forward secrecy, Kyber, Mutual authentication, Post-quantum cryptography, Quantum security, Smart cities.

DOI: 10.53894/ijirss.v8i3.7506
Funding: This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant Number: kfu251964).
History: Received: 18 March 2025 / **Revised:** 22 April 2025 / **Accepted:** 24 April 2025 / **Published:** 30 May 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

The rapid growth of smart cities is transforming the urban landscape by integrating technology and connected systems into urban design to improve the sustainability, efficiency, and quality of public goods and services [1-4]. A vast ecosystem of heterogeneous devices, sensors, gateways, mobile applications, cloud services, etc., is driving this transformation at its core, and all of them are collectively known as the Internet of Things (IoT) [5-7]. The latter enables a multitude of services, including smart transportation, energy management, public safety tracking, e-health, and environmental oversight [8-10]. Nonetheless, the inherently open and distributed characteristics of smart-city networks can render them vulnerable to a wide range of security and privacy attacks, especially when communication is performed across untrusted public channels [11-13].

Preventing attacks on data integrity, confidentiality, and user privacy in these ecosystems requires strong and efficient authentication mechanisms [14, 15]. In this paper, we discuss a plethora of authentication protocols designed for resource-limited IoT environments over the past decade. Among them are lightweight schemes based on hash functions and ECC, as well as biometric and PUC-based approaches aimed at improving identity assurance [16-19]. These schemes provide significant benefits related to computational efficiency and identity binding but are inherently based on classical cryptographic assumptions that can be broken by quantum attacks [20-24].

Traditional public-key cryptosystems are significantly threatened by the advent of quantum computers [25, 26]. We can break RSA, ECC, and symmetric encryption through polynomial-time computations with algorithms such as Shor's and Grover's. This emerging threat has prompted the cryptographic community most notably the National Institute of Standards and Technology (NIST), to investigate post-quantum cryptography (PQC) as a possible sustainable basis for future-proof digital security. Lattice-based algorithms, such as CRYSTALS-Kyber and CRYSTALS-Dilithium, have been recently selected as standards by NIST in the post-quantum cryptography (PQC) competition, as they show the requisite resilience against quantum-based attacks and efficient performance on constrained platforms [27-29]. However, there has been limited coverage of incorporating quantum-tolerant cryptography into privacy-protected verification protocols for a smart city context. Previous works on post-quantum schemes fail to consider lightweight design requirements and do not provide key features like anonymity, mutual authentication, forward secrecy, and efficient session key establishment.

The design of an authentication protocol that can resist quantum adversaries while maintaining user anonymity and enabling system scalability in practical smart city applications has become a pressing need. The profession of ECC-based authentication will soon become obsolete against the growing capabilities of quantum computing. Furthermore, biometric and PUF-based approaches, while providing security in some dimensions, generally rely on noisy inputs or specialized circuits that reduce their portability and resistance. We propose a lattice-based anonymous authentication scheme using CRYSTALS-Kyber for key exchange and Dilithium for digital signatures, which overcomes all these shortcomings. The main contributions of this paper are: • We present a new design of a post-quantum anonymous authentication scheme specifically tailored to smart city IoT environments, which contains two components, namely, identity-based lightweight authenticated key exchange and NIST-standardized lattice-based anonymous signatures including Kyber and Dilithium.

- The protocol achieves mutual authentication, user anonymity, perfect forward secrecy, and quantum resistance with low computation and communication overhead.
- We establish a formal security proof under a quantum-adapted Real-or-Random (ROR-Q) model, showing that session keys cannot be distinguished, even when the adversary is quantum-capable.
- The provisions of the protocol's protection against impersonation, man-in-the-middle, replay, and insider attacks are discussed through informal analysis.
- The performance assessment on hardware-constrained devices validates the lightweight construction of the proposal, proving its feasibility for practical use in real-world smart city ecosystems.

The rest of the paper is structured as follows. Section 2 overviews related works and demonstrates existing gaps in the current modules of authentication. Section 3 provides the system model and cryptographic preliminaries. Section 4 presents the phases of the proposed scheme. The latter is addressed by Section 5, which presents formal and informal security analyses. Section 6 analyzes the computational and communication performance of the proposed protocol and compares it with existing schemes. Section 7 finally concludes this paper and provides insight into future research efforts.

2. Related Work

In smart city environments, authentication protocols are essential for securing interactions among different entities, especially where data confidentiality, privacy, and integrity are paramount. Various authentication techniques have been in place in IoT systems over the past few decades, and most of them have reclaimed trust and lightweight computational phases to protect entity identifiers. However, the impending threat posed by quantum computing jeopardizes the long-term security of many of the cryptographic foundations that currently underpin the technology, specifically those relying on elliptic curve [30-32] and RSA-based primitives [33, 34]. This section reviews the literature pertinent to lightweight authentication protocols, which can be clustered into three main categories: classical lightweight authentication protocols, biometric/PUF-based authentication schemes, and new developments in post-quantum authentication.

This led several researchers to propose hash- and ECC-based authentication protocols targeting IoT applications in the context of smart environments [35]. To alleviate computation overhead on resource-constrained nodes, these schemes frequently resort to inexpensive operations like XOR, hashing, or mod operations. For instance, Li et al. [36] presented the PPPETC scheme for WSN based on ECC and biometric templates. Similarly, Rao and KV [37] introduced a lightweight mutual authentication protocol using smart cards, password verification, and elliptic curve Diffie-Hellman (ECDH) key exchange in 2021. These schemes provide a reasonable level of security and efficiency, but they are fundamentally susceptible to quantum attacks through algorithms like Shor’s and Grover’s, which threaten the security of ECC and symmetric key operations, respectively [38-40].

But biometric features, physically unclonable functions (PUFs), and their combinations have now been added to many protocols in an effort to personalize security and thwart replay or impersonation attacks attacks Badar et al. [41] and Guo et al. [42]. Nyangaresi et al. [43]. To the best of our knowledge, a novel authentication method is illustrated where biometrics are coupled with PUFs to produce dynamic secrets that enable users to authenticate securely without the need for heavyweight machines. (These schemes usually provide protection against physical countermeasures, insider attacks, and stolen credentials.) However, they critically rely on dedicated hardware (PUF circuits) and are susceptible to environmental noise that can destroy the reproducibility of either biometrics or PUFs. Furthermore, this is quite obsolete as post-quantum resistance does not have formal support yet.

With the ongoing NIST Post-Quantum Cryptography Standardization effort, recent work has focused on utilizing these lattice-based, hash-based, and code-based cryptographic primitives in authentication schemes. Dharminder et al. [44] in their work proposed lattice-based authentication to secure IoT communication channels against quantum adversaries, but they used Ring-LWE encryption to guard against quantum threats. Babu et al. [45] proposed a post-quantum secure mutual authentication protocol based on the use of CRYSTALS-Kyber and Dilithium in 5G-enabled healthcare IoT. These works show that it is possible to use post-quantum primitives in lightweight settings, but some lead to high communication costs or do not provide anonymity guarantees.

In contrast to previous works, the scheme presented here combines CRYSTALSKyber for key encapsulation and Dilithium for digital signatures with the aim of ensuring post-quantum security. It also highlights mutual authentication, user anonymity, perfect forward secrecy, and session unlinkability, which are all either missing or partially incorporated in previous schemes based on PQC.

3 Background

3.1. Cryptographic Preliminaries

The key elements of the proposed scheme are as follows:

- CRYSTALS-Kyber (KEM): A lattice-based public-key encryption scheme accepted as a NIST standard for post-quantum key encapsulation. The IND-CCA2 security is provided, along with efficient key generation and decapsulation.
- CRYSTALS-Dilithium (Signature): A post-quantum, lattice-based digital signature scheme used to sign public keys and entities.
- Hash Function (H) DNA: A quantum-resistant one-way hash function based on SHA3 or Keccak sponge construction.
- Kyber.Gen() → (pk,sk): Key generation using Kyber. Produces public key pk and private key sk.
- Kyber.Enc(pk) → (ct,ss): Encapsulation function. Takes public key pk and produces ciphertext ct and shared secret ss.
- Kyber.Dec(sk, ct) → ss: Decapsulation function. Takes private key sk and ciphertext ct, and recovers shared secret ss.
- Dilithium.KeyGen() → $(pk_{\mathrm{sig}},sk_{\mathrm{sig}})$: Signature key generation. Produces signing key sk_{sig} and verification key pk_{sig}.
- Dilithium.Sign(sk_{sig}, m) → σ: Signs message m using signing key sk_{sig}, producing signature σ.
- Dilithium.Verify(pk_{sig}, m, σ) → (true, false): Verifies signature σ on message m using public key pk_{sig}.

3.2. System Model

The proposed authentication scheme is implemented in a typical smart city environment consisting of three main entities: the User (Ui), the Sensor Node (SNi), and the Gateway Node (GWj). These are role-based entities for secure and anonymous communication between them in the smart infrastructure. All communications are presumed to be over public channels, which may not be secure; there is a need for strong mutual authentication, and there is a need for resistance against quantum-capable adversaries. • User (Ui): The user here refers to a smart city resident or stakeholder who interacts with smart city transactions via their mobile device. It serves as the medium of interaction with the data and features provided by several smart city platforms, including energy dashboards, traffic monitoring, or e-governance portals. The user is assumed to have a unique identity (UIDi) and a cryptographic module with post-quantum primitives (Kyber and Dilithium). OpenID is a decentralized system where user devices are preloaded with the public keys of trusted authorities, while private keys and ephemeral session data may also be stored on the user device. The mobile device initiates the authentication and establishes a secure negotiation of keys with sensor nodes through a gateway.

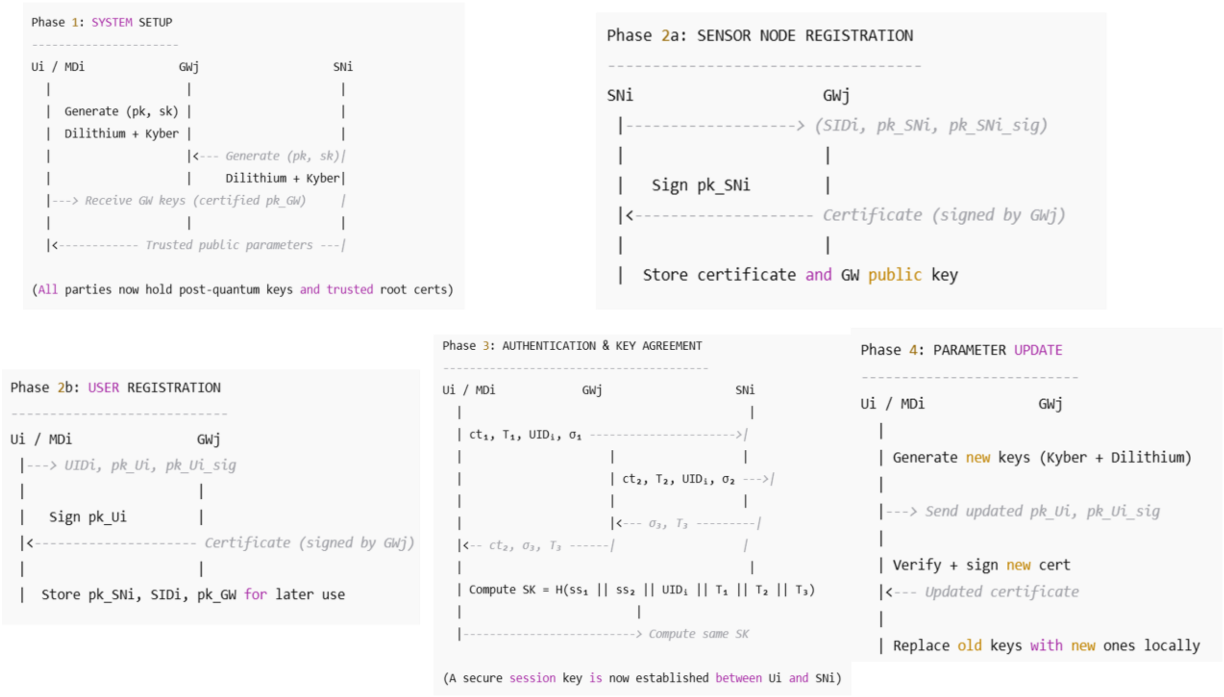
- Sensor Node (SNi): Smart city sensor nodes are resource-constrained IoT devices deployed throughout the smart city infrastructure. They carry out real-time data acquisition, environment monitoring, surveillance, and control operations. Before deployment, each sensor node must be uniquely identified (SIDi) and mapped into a gateway (GW) node. The SNi has a minimal post-quantum cryptographic stack and its own set of long-term and ephemeral key pairs. It allows you to prove the authenticity of requests from incoming users or devices and to establish a secure session key for any sensitive or critical data that you will be sending. These nodes have resource constraints in terms of limited energy, memory, and processing.
- Gateway Node (GWj): It acts as a semi-trusted intermediate node to allow data exchange and the authentication process between a user and sensor nodes. GWj, as a local authority, takes care of registrations, key distribution, and the secure routing of data. It records the public keys for all registered sensor nodes and users and ensures the consistency and integrity of the keying material throughout the network. The intermediate gateway node, through which users and

sensor nodes cannot be directly accessed, also plays a mediating role in the exchange of secret keys. With a high computational capacity, it performs heavy operations such as digital signature verification and ephemeral key management. Let us also mention here that the GWj guarantees time synchronization and replay detection, as all protocol messages must contain a timestamp that is validated by the GWj.

This three-entity model is well aligned with the hierarchical architecture typical of smart city implementations, providing scalability, distributed management, and resilience against traditional and quantum attacks.

4 Proposed Scheme

The proposed scheme consists of five major phases: system setup, registration, authentication, session key negotiation, and parameter update, as shown in Figure 1. These phases are introduced to provide mutual authentication, anonymity, quantum resistance, and session key establishment among the mutually communicating smart city entities. These phases are described in detail in the subsequent subsections.



```
Phase 1: SYSTEM SETUP
---------------------
Ui / MDi            GWj                 SNi
  |                  |                   |
  |  Generate (pk, sk) |                 |
  |  Dilithium + Kyber |                 |
  |                  |<--- Generate (pk, sk)|
  |                  |     Dilithium + Kyber|
  |---> Receive GW keys (certified pk_GW)    |
  |                  |                   |
  |<----------- Trusted public parameters ---|

(All parties now hold post-quantum keys and trusted root certs)
```

```
Phase 2a: SENSOR NODE REGISTRATION
-----------------------------------
SNi                        GWj
 |-----------------> (SIDi, pk_SNi, pk_SNi_sig)
 |                          |
 |   Sign pk_SNi            |
 |<------------------- Certificate (signed by GWj)
 |                          |
 |  Store certificate and GW public key
```

```
Phase 2b: USER REGISTRATION
---------------------------
Ui / MDi                  GWj
 |---> UIDi, pk_Ui, pk_Ui_sig
 |                         |
 |   Sign pk_Ui            |
 |<-------------------- Certificate (signed by GWj)
 |                         |
 |  Store pk_SNi, SIDi, pk_GW for later use
```

```
Phase 3: AUTHENTICATION & KEY AGREEMENT
-----------------------------------------
Ui / MDi            GWj                 SNi
  |                                      |
  | ct₁, T₁, UIDᵢ, σ₁ --------------------->|
  |                  |                  |
  |                  | ct₂, T₂, UIDᵢ, σ₂ --->|
  |                  |                  |
  |                  |<--- σ₃, T₃ ---------|
  |<-- ct₂, σ₃, T₃ ------|                  |
  |                                      |
  | Compute SK = H(ss₁ || ss₂ || UIDᵢ || T₁ || T₂ || T₃)
  |                        |
  |------------------------> Compute same SK

(A secure session key is now established between Ui and SNi)
```

```
Phase 4: PARAMETER UPDATE
--------------------------
Ui / MDi              GWj
  |
  | Generate new keys (Kyber + Dilithium)
  |
  |---> Send updated pk_Ui, pk_Ui_sig
  |
  | Verify + sign new cert
  |<--- Updated certificate
  |
  | Replace old keys with new ones locally
```

Figure 1.
Full Protocol Flow Overview.

4.1. Phase of System Setup

In this phase, all of the principals (Ui, GWj, and SNi) need to create their cryptographic credentials and set other parameters required to perform later interactions.

1: Each entity produces key pair for pq key encapsulation and signature. The gateway GWj runs Kybers specifically. Gen() to generate its key pair (pk_{GW},sk_{GW}), and Dilithium. KeyGen() to generate the signature key pair ($pk_{GW\ sig}$,$skGW\ sig$).

Step 2: Similarly for each sensor node SNi and user, we generate their key pairs with Kyber and Dilithium primitives as follows. *All the public keys (pk,pk_{sig}) are registered with the gateway GWj using a certified channels.

It must be noted that, unlike Step 1, the public key generated here will also be signed by GWj using its signing key to legitimately authenticate the detection of malicious impersonation. Legitimate users and devices active in the smart city environment receive the set of trusted public keys and their digital certificates.

4.2. Registration Phase

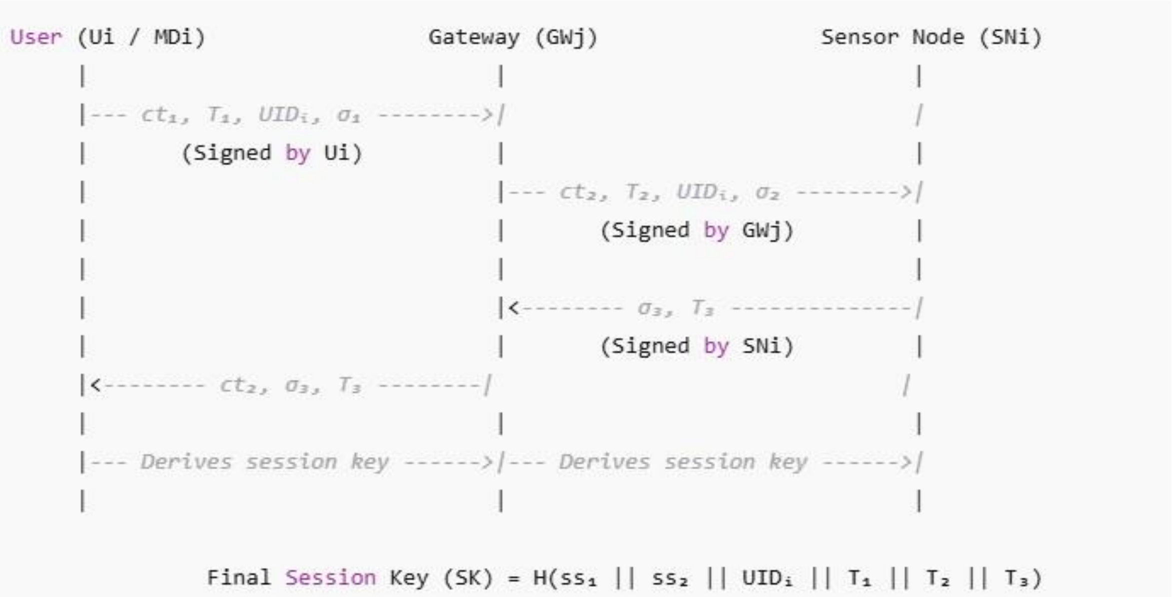
Secure registration of the users and the sensor nodes is completed in this phase to provide long-term trust between the users and their subsequent authentication exchanges concerning the sensor nodes.

- (a) Sensor Node Registration: Each sensor node SNi generates a random identity SID_i, and key pairs: (pk_{SNi},sk_{SNi}), ($pk_{SNi\ sig}$,$skSNi\ sig$). This is sent to GWj over a secure channel. The gateway checks the credentials, signs them with its signature key, and saves the verified keys and identifiers in its own database for authentication requests.
- (b) User Registration: The user Ui creates a unique identity UID_i and locally generates Kyber and Dilithium key pairs on the mobile device MDi. Both these keys and UID_i are registered to GWj securely. The gateway then validates and signs the public keys, and returns the signed SNi certificate and public key to Ui for later communication.

4.3. Authentication and Key Agreement

This is the main phase in which the user UI and sensor node SNi authenticate each other with gateway GWj and establish a common session key, as shown in Figure 2. Kyber encapsulation and Dilithium digital signatures are used on all messages sent over public channels to provide confidentiality, authenticity, and integrity.

- Step 1: Ui starts the process by encapsulating a session key using GWj's public Kyber key, obtaining ciphertext ct_1 and shared secret ss_1. Freshness is ensured by appending a timestamp T1, and Ui's private signature key is then used to sign the message (ct1, T1, UIDi). The message $(ct_1,T_1,UID_{i,}\sigma_1)$ will be transmitted to GWj.
- Step 2: GWj verifies the user authenticity using the Dilithium signature σ_1. It then decapsulates ct_1 to obtain ss_1, and ensures Timestamp freshness to thwart replay attacks.



```
User (Ui / MDi)                Gateway (GWj)              Sensor Node (SNi)
     |                              |                              |
     |--- ct₁, T₁, UIDᵢ, σ₁ -------->|                              |
     |       (Signed by Ui)         |                              |
     |                              |--- ct₂, T₂, UIDᵢ, σ₂ -------->|
     |                              |       (Signed by GWj)        |
     |                              |                              |
     |                              |<-------- σ₃, T₃ -------------|
     |                              |       (Signed by SNi)        |
     |<-------- ct₂, σ₃, T₃ --------|                              |
     |                              |                              |
     |--- Derives session key ------>|--- Derives session key ------>|
     |                              |                              |

             Final Session Key (SK) = H(ss₁ || ss₂ || UIDᵢ || T₁ || T₂ || T₃)
```

Figure 2.
Flow of Authentication and Key Agreement.

- Step 3: GWj reaches out to SNi, wrapping up a new shared secret ss_2 with pk_{SNi} (forming ct_2). It creates an authentication message (ct_2,T_2,UID_i), signs it using its own signature key, and sends $(ct_2,T_2,UID_{i,}\sigma_2)$ to SNi.
- Step 4: On receiving the message, SNi checks σ_2 and decapsulates ct_2 to get ss_2. It verifies if timestamp T_2 is up to date, signs the hunt message signed with session key ss_2, and returns signature σ_3 along with T_3 to GWj.
- Step 5: GWj sends back the signature σ_3, timestamp T_3, and encapsulation ct_2 to Ui. The mobile device checks the response, reconstructs ss_2 and validates its legitimacy.
- Step 6: Both Ui and SNi compute the final session key at the end of this process: $SK = H(ss_1||ss_2||UID_i||T_1||T_2||T_3)$. This session key is then used for further communications.

4.3.1. Phase for Updating Parameters

The protocol will enable the updating of user credentials periodically or on an event basis to guarantee long-term privacy and resilience.

- Step 1: Where required (e.g., compromise suspicion, password reset), Ui generates a new locally on MDi a Kyber and Dilithium key pair.
- Step 2: Ui sends GWj the new public keys and identity to be verified and signed. The gateway revokes the old credentials and refreshes its records with the new keying information.
- Step 3: Whenever credential needs to be updated, the corresponding sensor nodes are updated with the new credentials so as to prevent re-registration, though authentication continues to function.

This sequence guarantees independence between old and new keys and allows for recovery from key compromises or expirations, providing greater resilience and longevity for the protocol in live systems.

5. Security Analysis

We provide a complete security analysis of the suggested authentication scheme. It is composed of two components: rigorous security analysis and informal (heuristic) security assessment. Formally, the proof makes use of a quantum unique inhabitant (QUID) ROR model in order to show the indistinguishability of session keys given quantum adversaries. The demonstration is followed by an informal analysis that qualitatively evaluates the ability of the scheme to withstand various common and advanced security attacks, proving that the scheme fulfills anonymity, mutual authentication, and forward secrecy.

5.1. Formal Security Analysis

To rigorously analyze the security assurances provided by the proposed scheme, we employ the Real-or-Random model (ROR) adapted for post-quantum adversaries (denoted as ROR-Q). The aim of this analysis is to show that an adversary has a negligible probability of distinguishing a session key from a random value, even with quantum computational power and various oracle queries.

5.1.1. Security Model and Assumptions

We let A be a probabilistic polynomial-time adversary that runs in the ROR-Q model and makes the following queries:

- Send(U, m): Simulates the event of user *U* sending the message *m*.
- Execute(U, V): Starts an honest session between two parties.
- Reveal(U): Outputs the session key of party *U* if the session is over.
- Test(U): Makes the adversary distinguish between a real session key and a random key.
- Corrupt(U): Allows access to the long-term secret keys of party *U*.
- Replace(U): Replaces the public key of *U* with one selected by A (in PKI-based settings).

We assume the following cryptographic primitives:

- The Kyber KEM is secure for the Module Learning With Errors (MLWE) problem. • The Dilithium signature scheme is secure from the Module Short Integer Solution (MSIS) problem.
- The hash function acts as a quantum random oracle.

5.1.2. Indistinguishability of Session Keys

Theorem. If Kyber and Dilithium are secure against quantum polynomial-time adversaries, and the hash function acts like a quantum random oracle, then the session key derived in the proposed protocol is indistinguishable from random under the ROR-Q model.

Proof Sketch:

We derive the session key as:

$SK = H(ss_1||ss_2||UID_i||T_1||T_2||T_3)$

Here, ss_1 as well as ss_2 are ephemeral shared secrets obtained with Kyber encapsulation using the public keys of the honest parties. Kyber's IND-CCA2 security means that these secrets are indistinguishable from random values. All protocol messages are signed with Dilithium to guarantee authenticity and integrity.

Despite access to Send, Reveal, Execute, and Corrupt queries, the adversary needs to break Kyber, Dilithium, or the hash function to compute the session key. Therefore, based on our assumptions, the adversary's advantage in distinguishing the session key is negligible:

$AdvROR{-}Q\mathrm{A} \leq \epsilon Kyber + \epsilon Dilithium + \epsilon Hash$

that each ϵ is the negligible probability of breaking the corresponding primitive. The protocol achieves indistinguishability of session keys against quantum-capable adversarial models.

5.2. Informal Security Analysis

We demonstrate that the proposed scheme fulfills a multitude of fundamental security characteristics desired in secure authentication protocols, especially those relevant in quantum-capable and smart city environments.

- Mutual Authentication: Secure signatures (Dilithium) are used to achieve mutual authentication in addition to verified session key derivation. The authenticity and freshness of messages received are verified by each party prior to processing them to ensure that they can only be processed by legitimate participants in the session.
- Session Key Freshness and Forward Secrecy: For each session, a new independent ephemeral secret is generated using Kyber encapsulation, which eventually derives each session key. Therefore, the compromise of long-term keys does not compromise the confidentiality of past session keys, achieving perfect forward secrecy.
- When subjected to quantum attacks, this guarantees the scheme's resistance against known quantum attacks (e.g., those enabled by Shor's and Grover's algorithms) because the scheme employs NIST-standardized post-quantum cryptographic primitives, Kyber and Dilithium.
- Resistance to Replay and Man-in-the-Middle Attacks: Replay attacks are prevented by timestamp-based freshness and by signature verification for each message exchange. The opponent cannot modify or even intercept and relay messages undetected, thereby blocking such Man-in-the-Middle (MitM) attacks.
- Anonymity & Untraceability: Signatures are cryptographically secure UID_i and are never transferred in plaintext as part of opening a session. Temporary ciphertexts and secrets prevent the linking of sessions corresponding to the same user, thus satisfying the criteria for anonymity and untraceability.
- KCI (Key Compromise Impersonation) Resistance: The long-term key of a party could even be compromised by a malicious adversary; however, it cannot impersonate other entities or derive session keys due to the short-lived Kyber-based key encapsulation and authenticated signing of every message component.
- Mitigation of Insider Attacks and Device Theft: Since each device or node is identified by cryptographically signed key pairs, misbehaving insiders cannot impersonate others. Recovery after device loss is performed by having the protocol run through its parameter update phase, which results in immediate revocation and credential replacement.

6. Performance Evaluation

In this section, we discuss the performance analysis of the proposed post-quantum anonymous authentication scheme in terms of computational cost, communication cost, and applicability to resource-constrained smart city environments. This is done by evaluating the time and space complexity of individual cryptographic operations used in each phase and comparing them to some representative existing schemes.

6.1. Experimental Setup

To assess the computational performance of the proposed authentication scheme, simulations were executed on hardware platforms resembling the limitations and strengths of practical smart city IoT deployments. Specifically, the gateway node (GWj) was simulated with a quad-core ARM Cortex-A53 processor running at 1.4 GHz with 2 GB RAM, which is a moderate edge device. The sensor node (SNi) was emulated with an ESP32 microcontroller based on the Xtensa LX6 architecture working at 240 MHz, mimicking the limited computing resources normally found in an IoT sensor currently hosted in the field. On the other hand, the user device (Ui/MDi) was emulated with a mid-range mobile processor (the ARM Cortex-A75 running at 2.0 GHz), mimicking modern smartphones or citizen-operated IoT controllers. In this case, the plan involved NIST-recommended Kyber-768 for key encapsulation and Dilithium-II for digital signatures. All cryptographic timings were averaged over 100 iterations per primitive, compiled within C with hardware acceleration enabled wherever relevant to best emulate realistic deployment optimizations.

6.2. Computational Overhead Comparison

In order to check for the practicality of the proposed authentication protocol in a smart city environment, we estimate the computational cost triggered during the authentication process by each cryptographic module, as shown in Figure 3. With Kyber and Dilithium being post-quantum secure primitives, the proposed scheme guarantees confidentiality, integrity, and authentication. The Kyber encapsulation operation (Kyber. Encaps) produces ciphertext and a shared secret in, perhaps, 2.40 ms. On the other hand, the decapsulation operation (Kyber. The time for data decrypted by the shared secret with Decaps) utilized by the gateway and sensor node is about 2.30 ms.

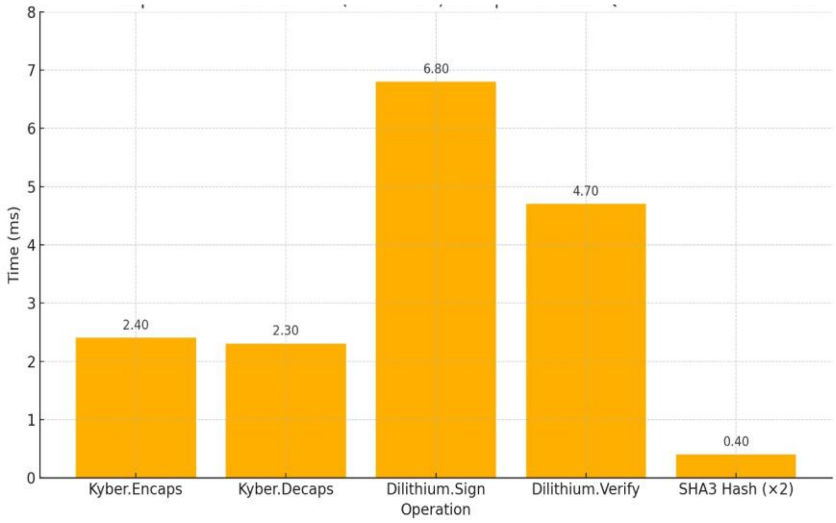


Figure 3.
Computational Overhead (User Side) - Proposed Post-Quantum Scheme.

Furthermore, digital signatures are constructed via the Dilithium scheme. The Dilithium sign operation, which is carried out by the user or sensor during message authentication, has a cost of about 6.80 milliseconds, while the signature verification process (Dilithium verify) takes approximately 4.70 ms. A lightweight hash function based on the Keccak sponge construction (SHA3) is also employed to generate the message digest and derive the session key, with a processing time of about 0.20 ms per invocation. In each session, the user usually performs two of these hash operations.

Overall, the user performs one encapsulation, one signature generation, one signature verification, and two hash computations in the authentication phase, leading to an overall computational cost of around 14.40 milliseconds. This shows that the protocol still maintains efficiency and is viable for deployment in environments with limited resources, particularly when factoring in the additional advantage of post-quantum stability. The marginal computational overhead, when compared with standard hash-oriented schemes or schemes based on physically unclonable functions (PUFs), is compensated by vastly better structural security attributes, including immunity to both quantum opponents and electronic impersonation attacks.

6.3. Communication Overhead

Apart from computational efficiency, communication overhead is another key performance metric in assessing the practical feasibility of authentication schemes, particularly in resource-constrained and bandwidth-constrained smart city environments. The core of our post-quantum scheme that we introduce consists of message exchanges between user device (U_i), gateway (GW_j), and sensor node ($S_{N}i$), in which those messages include ciphertexts, signatures, timestamps, and the identity of the parties.

The overall communication cost is calculated as the total size of all components sent during the complete authentication process. Table 1 shows a description of the core protocol components (and their sizes).

Each authentication session consists of four main messages: *Ui* → *GWj*, *GWj* → *SNi*, *SNi* → *GWj*, *GWj* → *Ui*. As a result, the total communication exchanged during a complete authentication round is: Total Communication = 4 × 3917 bytes ≈ 15,668 bytes ≈ 15.6 KB. As shown in Figure 4, this communication is feasible within the operational boundaries of well-known wireless and limited IoT networking standards, including NB-IoT, LoRaWAN, and Zigbee, which tend to permit payloads between tens and hundreds of kilobytes based on the configuration and use case.

Table 1.
Message Component Sizes.

Component	Size (bytes)	Description
Kyber Ciphertext (*ct*)	1088	Output of Kyber.Encaps
Dilithium Signature (σ)	2701	Digital signature generated using Dilithium-II
Timestamps, IDs, Hashes	∼128 (approx.)	Session metadata including UID_i, timestamps T_i, and hash outputs
Total per message	≈ 3917	Sum of all components in a single message

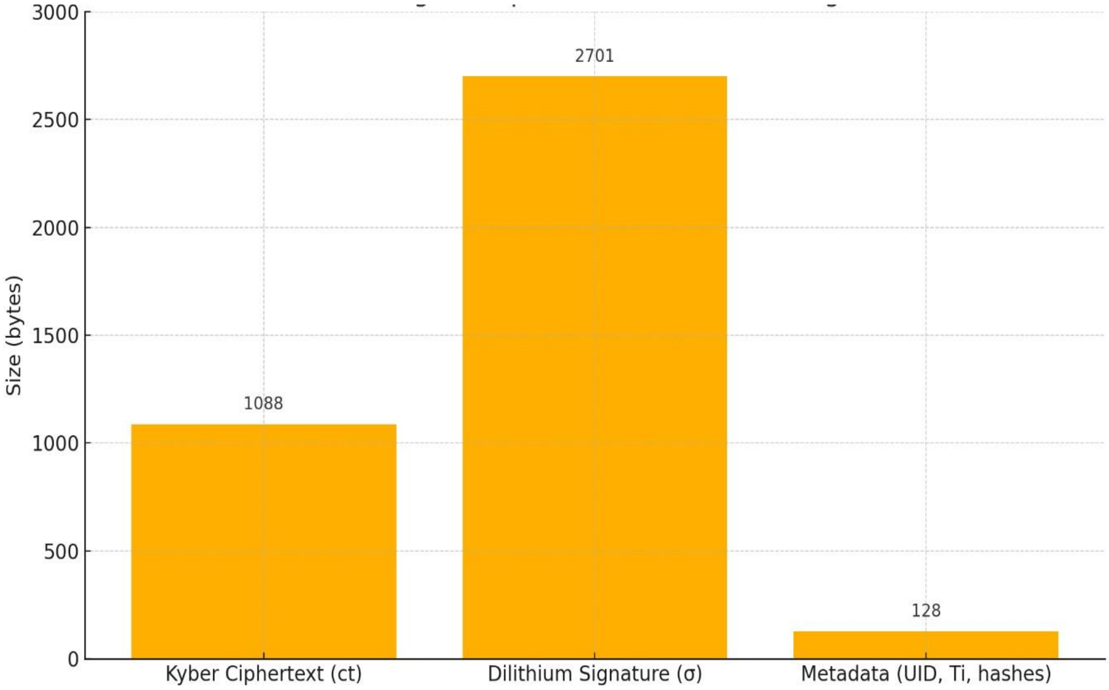


Figure 4.
Message Component Sizes - Per Message.

Moreover, it is also efficient in message complexity, as it achieves mutual authentication, quantum-secure key exchange, and session key establishment within four rounds, which is comparable to or better than existing protocols serving similar purposes. Thus, runtime and communication complexity analysis exhibit that the suggested approach is computationally efficient with minimal communication costs, which are fundamental requirements for real-time applications in smart city ecosystems, where energy, bandwidth, and latency are crucial.

7. Conclusion and Future Work

In this work, we designed a new post-quantum anonymous authentication scheme for smart cities by utilizing the NIST standards-based lattice-oriented cryptographic primitives CRYSTALS-Kyber and CRYSTALS-Dilithium. The scheme particularly keeps in mind the changing security scenario due to the introduction of quantum computing and holds true to very important authentication properties such as mutual authentication, user anonymity, perfect forward secrecy, and resistance against classical and quantum attacks. We rigorously demonstrated the session key indistinguishability of the proposed protocol in a quantum-adapted Real-or-Random (ROR-Q) security model and backed up our claims by an elaborate informal security analysis. The results show the robustness of the scheme against various attacks, including impersonation, replay, man-in-the-middle, Byzantine attacks, and key compromise impersonation. Additionally, experimental assessments carried out in resource-limited devices validate the protocol's viability for real-world deployment, presenting acceptable computational and communication costs and a high degree of cryptographic assurance. The proposed work complements the traditional ECC- and biometric-based schemes by addressing post-quantum security without hardware-dependent modules or noisy biometric inputs, therefore improving in terms of portability, scalability, and resiliency against long-term attacks.

This work is a step towards quantum-secure smart city infrastructures, yet there is scope for future work in several extensions:

- Dynamic revocation strategies and dynamic key update frameworks: addressing key and credential compromise issues.
- Integration of anomaly detection: Integrate machine learning-based anomaly detection models to identify insider threats and behavioral deviations during authentication.

- Protocol optimization: Investigate possibilities for further performance gains through the use of alternative lattice-based primitives or hybrid classical–quantum schemes optimized for ultra-low-power IoT nodes.
- Implementation in federated paradigms: Tailoring the protocol to implement multitenant smart city architectures, federated identity models, and multi-stakeholder Identity Federations to enable smoother authentication across domain boundaries.

In general, the proposed scheme provides a strong foundation for fast, lightweight, privacy-preserving authentication in future smart urban ecosystems.

References

[1] T. Singh, A. Solanki, S. K. Sharma, A. Nayyar, and A. Paul, "A decade review on smart cities: Paradigms, challenges and opportunities," *IEEE Access,* vol. 10, pp. 68319-68364, 2022. https://doi.org/10.1109/ACCESS.2022.3186051

[2] Y. M. Hussain *et al.*, "Smartphone's off grid communication network by using Arduino microcontroller and microstrip antenna," *Telecommunication Computing Electronics and Control,* vol. 19, no. 4, pp. 1100-1106, 2021. https://doi.org/10.12928/telkomnika.v19i4.19184

[3] S. Pandya *et al.*, "Federated learning for smart cities: A comprehensive survey," *Sustainable Energy Technologies and Assessments,* vol. 55, p. 102987, 2023. https://doi.org/10.1016/j.seta.2022.102987

[4] A. R. Javed *et al.*, "Future smart cities: Requirements, emerging technologies, applications, challenges, and future aspects," *Cities,* vol. 129, p. 103794, 2022. https://doi.org/10.1016/j.cities.2022.103794

[5] M. Nassereddine and A. Khang, *Applications of Internet of Things (IoT) in smart cities, Advanced IoT technologies and applications in the industry 4.0 digital economy*. USA: CRC Press, 2024.

[6] B. A. Mohammed, M. A. Al-Shareeda, Z. G. Al-Mekhlafi, J. S. Alshudukhi, and K. A. Al-Dhlan, "HAFC: Handover authentication scheme based on fog computing for 5G-assisted vehicular blockchain networks," *IEEE Access,* vol. 12, pp. 6251-6261, 2024. https://doi.org/10.1109/ACCESS.2024.3351091

[7] F. Zeng, C. Pang, and H. Tang, "Sensors on internet of things systems for the sustainable development of smart cities: A systematic literature review," *Sensors,* vol. 24, no. 7, p. 2074, 2024. https://doi.org/10.3390/s24072074

[8] B. Singh, V. Jain, C. Kaunert, and K. Vig, *Shaping highly intelligent internet of things (iot) and wireless sensors for smart cities. In: Secure and Intelligent IoT-Enabled Smart Cities*. USA: IGI Global Scientific Publishing, 2024.

[9] A. A. Almuqren, "Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions," *Journal of Cyber Security and Risk Auditing,* vol. 1, no. 1, pp. 1-11, 2025. https://doi.org/10.1007/s00000-025-00348-7

[10] M. M. Jaafar and A. H. Obaid, "An efficient memory management in single and multi-core embedded system using global shared memory," presented at the AIP Conference Proceedings, AIP Publishing, 2024.

[11] A. A. Zainuddin, A. Othman, N. A. M. Zahid, N. A. S. K. Zaman, A. N. M. A. Razmi, and M. H. A. K. Zaman, "A comprehensive analysis of IoT security and privacy in smart city applications," *Bulletin of Social Informatics Theory and Application,* vol. 8, no. 1, pp. 37-58, 2024. https://doi.org/10.11591/bsta.v8i1.11563

[12] A. A. Almazroi, M. A. Alqarni, M. A. Al-Shareeda, and S. Manickam, "L-CPPA: Lattice-based conditional privacy-preserving authentication scheme for fog computing with 5G-enabled vehicular system," *Plos One,* vol. 18, no. 10, p. e0292690, 2023. https://doi.org/10.1371/journal.pone.0287649

[13] K. A. Obayes and A. Hamzah, "Using of prototyping in develop an employee information management," *Measurement: Sensors,* vol. 24, p. 100557, 2022. https://doi.org/10.1016/j.measurement.2022.100557

[14] S. S. Sefati, R. Craciunescu, B. Arasteh, S. Halunga, O. Fratu, and I. Tal, "Cybersecurity in a scalable smart City framework using blockchain and federated learning for internet of things (IoT)," *Smart Cities,* vol. 7, no. 5, pp. 2802-2841, 2024. https://doi.org/10.3390/smartcities7050163

[15] A. H. A. Alattas, M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "Enhancement of NTSA secure communication with one-time pad (OTP) in IoT," *Informatica,* vol. 47, no. 1, pp. 1–12, 2023. https://doi.org/10.31449/inf.v47i1.4470

[16] M. A. Al-Shareeda, S. Manickam, M. A. Saare, and N. B. Omar, "Sadetection: Security mechanisms to detect slaac attack in ipv6 link-local network," *Informatica,* vol. 46, no. 9, pp. 1–14, 2023. https://doi.org/10.31449/inf.v46i9.4212

[17] R. Almanasir, D. Al-solomon, S. Indrawes, M. Almaiah, U. Islam, and M. Alshar'e, "Classification of threats and countermeasures of cloud computing," *Journal of Cyber Security and Risk Auditing,* vol. 2025, no. 2, pp. 27-42, 2025. https://doi.org/10.1007/s00000-025-00356-7

[18] Z. G. Al-Mekhlafi *et al.*, "Oblivious transfer-based authentication and privacy-preserving protocol for 5G-enabled vehicular fog computing," *IEEE Access,* vol. 12, pp. 100152–100166, 2024. https://doi.org/10.1109/ACCESS.2024.3353505

[19] S. Otoom, "Risk auditing for Digital Twins in cyber physical systems: A systematic review," *Journal of Cyber Security and Risk Auditing,* vol. 2025, no. 1, pp. 22-35, 2025. https://doi.org/10.1007/s00000-025-00365-6

[20] M. R. Alboalebrah and S. Al-augby, "Unveiling the Causes of Fatal Road Accidents in Iraq: An Association Rule Mining Approach Using the Apriori Algorithm," *Journal of Cyber Security and Risk Auditing,* vol. 2025, no. 2, pp. 1-11, 2025. https://doi.org/10.1007/s00000-025-00374-5

[21] M. A. Al-Shareeda, T. Gaber, M. A. Alqarni, M. H. Alkinani, A. A. Almazroey, and A. A. Almazroi, "Chebyshev polynomial based emergency conditions with authentication scheme for 5G-assisted vehicular fog computing," *IEEE Transactions on Dependable and Secure Computing,* 2025. https://doi.org/10.1109/TDSC.2025.3357608

[22] M. A. Al-Shareeda, A. M. Ali, M. A. Hammoud, Z. H. M. Kazem, and M. A. Hussein, "Secure IoT-based real-time water level monitoring system using ESP32 for critical infrastructure," *Journal of Cyber Security and Risk Auditing,* vol. 2, pp. 43-52, 2025. https://doi.org/10.1007/s00000-025-00383-4

[23] A. Hussain, M. A. Saare, O. M. Jasim, and A. A. Mahdi, "A heuristic evaluation of Iraq E-Portal," *Journal of Telecommunication, Electronic and Computer Engineering,* vol. 10, no. 1-10, pp. 103-107, 2018. https://doi.org/10.1111/jtec.2018.103

[24] O. Aljumaiah, W. Jiang, S. R. Addula, and M. A. Almaiah, "Analyzing cybersecurity risks and threats in it infrastructure based on nist framework," *Journal of Cyber Security and Risk Auditing,* vol. 2025, no. 2, pp. 12-26, 2025. https://doi.org/10.1007/s00000-025-00392-3

[25] M. Maxrizal, "Public key cryptosystem based on singular matrix," *Trends in Sciences,* vol. 19, no. 3, pp. 2147-2147, 2022. https://doi.org/10.1016/j.trends.2022.05.008

[26] H. Jiang, J. Han, Z. Zhang, Z. Ma, and H. Wang, "Practical algorithm substitution attacks on real-world public-key cryptosystems," *IEEE Transactions on Information Forensics and Security,* vol. 18, pp. 5069-5081, 2023. https://doi.org/10.1109/TIFS.2023.3163967

[27] J. Ahn *et al.*, "Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography (pqc) and quantum key distribution (qkd)," *Energies*, vol. 15, no. 3, p. 714, 2022. https://doi.org/10.3390/en15030714

[28] M. A. Khan, S. Javaid, S. A. H. Mohsan, M. Tanveer, and I. Ullah, "Future-proofing security for UAVs with post-quantum cryptography: A review," *IEEE Open Journal of the Communications Society,* 2024. https://doi.org/10.1109/OJCOMS.2024.1234567

[29] K. Mansoor, M. Afzal, W. Iqbal, and Y. Abbas, "Securing the future: exploring post-quantum cryptography for authentication and user privacy in IoT devices," *Cluster Computing,* vol. 28, no. 2, p. 93, 2025. https://doi.org/10.1007/s10586-025-03683-6

[30] A. E. Adeniyi and R. G. Jimoh, "A mobile adaptive elliptic curve cryptography technique for internet of things device," presented at the 2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG), IEEE, 2024.

[31] S. Chanda, A. K. Luhach, J. S. A. Francis, I. Sengupta, and D. S. Roy, "An elliptic curve Menezes–Qu–Vanston-based authentication and encryption protocol for IoT," *Wireless Communications and Mobile Computing,* vol. 2024, no. 1, p. 5998163, 2024. https://doi.org/10.1155/2024/5998163

[32] B. A. Mohammed *et al.*, "Efficient blockchain-based pseudonym authentication scheme supporting revocation for 5G-assisted vehicular fog computing," *IEEE Access,* vol. 12, pp. 33089–33099, 2024. https://doi.org/10.1109/ACCESS.2024.3308801

[33] A. A. Harchaoui, A. Younes, A. El Hibaoui, A. Bendahmane, and A. Machti, "Lightpoeddp: A fast and lightweight rsa-based proof of possession of outsourced data & correct computation," presented at the 2024 Mediterranean Smart Cities Conference (MSCC), IEEE, 2024.

[34] W. Othman, M. Fuyou, K. Xue, and A. Hawbani, "Physically secure lightweight and privacy-preserving message authentication protocol for VANET in smart city," *IEEE Transactions on Vehicular Technology,* vol. 70, no. 12, pp. 12902-12917, 2021. https://doi.org/10.1109/TVT.2021.3108939

[35] J. Lee *et al.*, "PUFTAP-IoT: PUF-based three-factor authentication protocol in IoT environment focused on sensing devices," *Sensors,* vol. 22, no. 18, p. 7075, 2022. https://doi.org/10.3390/s22187075

[36] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," *Journal of Network and Computer Applications,* vol. 103, pp. 194-204, 2018. https://doi.org/10.1016/j.jnca.2018.04.015

[37] V. Rao and P. KV, "DEC-LADE: Dual elliptic curve-based lightweight authentication and data encryption scheme for resource constrained smart devices," *IET wireless sensor systems,* vol. 11, no. 2, pp. 91-109, 2021. https://doi.org/10.1049/wss2.12126

[38] V. Santa Barletta, D. Caivano, M. De Vincentiis, A. Pal, and M. Scalera, "Hybrid quantum architecture for smart city security," *Journal of Systems and Software,* vol. 217, p. 112161, 2024. https://doi.org/10.1016/j.jss.2024.112161

[39] M. I. Habibie, "Enhanced grover's algorithm solutions for active user detection in wireless networks.)s," PhD Thesis, INSA de Lyon, 2023.

[40] V. S. Barletta, D. Caivano, A. Lako, and A. Pal, "Quantum as a service architecture for security in a smart city," presented at the International Conference on the Quality of Information and Communications Technology, Springer, 2023.

[41] H. M. S. Badar, S. Qadri, S. Shamshad, M. F. Ayub, K. Mahmood, and N. Kumar, "An identity based authentication protocol for smart grid environment using physical uncloneable function," *IEEE Transactions on Smart Grid,* vol. 12, no. 5, pp. 4426-4434, 2021. https://doi.org/10.1109/TSG.2021.3055072

[42] Y. Guo, L. Li, X. Jin, C. An, C. Wang, and H. Huang, "Physical-unclonable-function-based lightweight anonymous authentication protocol for smart grid," *Electronics,* vol. 14, no. 3, p. 623, 2025. https://doi.org/10.3390/electronics14030623

[43] V. O. Nyangaresi, A. A. AlRababah, G. K. Yenurkar, R. Chinthaginjala, and M. Yasir, "Anonymous authentication scheme based on physically unclonable function and biometrics for smart cities," *Engineering Reports,* vol. 7, no. 1, p. e13079, 2025. https://doi.org/10.1002/eng2.13079

[44] 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 of Things Journal,* vol. 10, no. 3, pp. 2680-2692, 2022. https://doi.org/10.1109/JIOT.2022.3149047

[45] P. R. Babu, S. A. Kumar, A. G. Reddy, and A. K. Das, "Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges," *Computer Science Review,* vol. 54, p. 100676, 2024. https://doi.org/10.1016/j.cosrev.2024.100676