A Post-Quantum Secure Federated Learning Framework for Cross-Domain V2G Authentication

Shafiq Ahmed, Mohammad Hossein Anisi, *Senior Member, IEEE*

***Abstract*—Cross-domain Vehicle-to-Grid (V2G) networks enable secure and efficient energy transactions between Electric Vehicles (EVs), Charging Stations (CS), and Electric Service Providers (ESP), forming a critical component of Edge computing-assisted Consumer devices and IoT (EACI) frameworks. However, existing authentication mechanisms often rely on centralized trusted authorities, leading to single points of failure and computational bottlenecks. Additionally, the emergence of quantum computing threatens traditional cryptographic authentication schemes, necessitating the integration of post-quantum security mechanisms to protect multi-domain V2G interactions. This paper presents a Lightweight Quantum-Resistant Authentication Protocol (LQAP) designed to address these challenges by employing a hybrid eXtended Merkle Signature Scheme (XMSS) and Lightweight Merkle Signature (LMS) system to achieve post-quantum resilience with optimized key management. Additionally, a decentralized Hierarchical Federated Learning (HFL) framework operating at the edge layer is incorporated for hardware-based secure entity identification, enabling distributed anomaly detection without centralized data aggregation. Additionally, physically unclonable functions (PUF) are incorporated for hardware-based secure entity identification. Formal security analysis using the Scyther tool confirms LQAP's resilience against impersonation, replay, and machine learning-based inference attacks. Performance evaluations indicate that LQAP substantially reduces communication overhead by 21.45%, computational cost by 42.78%, and storage overhead by 61.95% compared to conventional schemes, thus providing an efficient and scalable post-quantum authentication solution aligned with EACI network requirements.**

***Index Terms*—Security, Electric Vehicles, Vehicle to Grid, ICPS, Smart Grid**

I. Introduction

The V2G technology has emerged as a fundamental component of modern smart grid ecosystems, facilitating efficient bidirectional energy transactions among EVs, CSs, and ESPs. Initially conceptualized by Kempton et al. [1] to enhance renewable energy integration and grid stability, V2G systems have evolved significantly. The foundational work by Kempton and Tomic [2] established core principles of bidirectional energy transactions, while contemporary V2G implementations have integrated into Edge computing-assisted Consumer devices and IoT (EACI) frameworks [3], [4], emphasizing decentralized infrastructures for enhanced grid stability.

Contemporary V2G authentication mechanisms increasingly leverage hardware security primitives, particularly Physical Unclonable Functions (PUFs), which exploit inherent manufacturing variations in semiconductor devices to generate unique, unclonable digital fingerprints providing tamper-resistant authentication capabilities essential for securing distributed V2G infrastructures.

Despite these advancements, traditional V2G authentication protocols remain constrained by their reliance on centralized Certificate Authorities (CAs), constituting single points of failure and computational bottlenecks. Early authentication schemes by Wazid et al. [5] employed elliptic curve cryptography with biometric authentication, while Roman et al. [6] introduced pairing-based mutual authentication between EVs and aggregators. Further privacy-preserving authentication advances by Wang et al. [7] and Xia et al. [8] introduced fog computing-based protocols. However, these solutions remained predominantly confined to single-domain environments with limited cross-domain applicability. Initial cross-domain attempts by Vaidya et al. [9] and Chen et al. [10] introduced certificate-based and anonymous authentication mechanisms but suffered from centralization vulnerabilities and substantial computational overhead.

Contemporary V2G ecosystems face complex security challenges predominantly related to cross-domain authentication mechanisms. Current methods, including elliptic curve cryptography (ECC), pairing-based schemes, and fog computing-based privacy protocols, exhibit significant limitations in cross-domain scenarios, scalability, and quantum computing resistance. These systems face unprecedented challenges from quantum computing threats [11] and cross-domain authentication complexities. Traditional cryptographic mechanisms exhibit vulnerabilities to quantum attacks and scalability limitations [12]–[14], while blockchain-based solutions like Liu et al. [15] impose significant communication overhead through frequent certificate exchanges.

Quantum computing advancements, exemplified by Shor's and Grover's algorithms, threaten existing authentication frameworks, necessitating robust quantum-resistant mechanisms. Current V2G architectures lack quantum-resistant cryptography, rendering systems vulnerable to future quantum adversaries. Furthermore, existing methods lack hardware-level security, enabling entity impersonation and physical tampering. Cross-domain authentications often compromise privacy by revealing sensitive credential information, while blockchain-based methods suffer from latency due to frequent on-chain verifications.

This paper proposes a Lightweight Quantum-Resistant Authentication Protocol (LQAP) addressing these critical challenges. LQAP integrates a hybrid XMSS and LMS system, delivering robust post-quantum resilience. PUF enhances hardware security, preventing impersonation and physical attacks

S. Ahmad and M. H. Anisi are with the School of Computer Science and Electronic Engineering, University of Essex, Colchester CO4 3SQ, UK.
E-mail: s.ahmed@essex.ac.uk; m.anisi@essex.ac.uk

by establishing unique, tamper-resistant identities for each participating entity. Zero-Knowledge Proofs (ZKPs) strengthen privacy-preserving authentication, ensuring credentials remain confidential across domains.

Contemporary post-quantum authentication research encompasses diverse cryptographic primitives. Bernstein et al. [16] demonstrated hash-based signatures efficacy in resource-constrained environments through stateless constructions. Lattice-based authentication schemes by Ducas et al. [17] provide quantum-resistant frameworks leveraging Learning With Errors (LWE) assumptions. The SPHINCS+ framework [18] establishes stateless hash-based signatures with configurable security-performance tradeoffs for dynamic V2G environments.

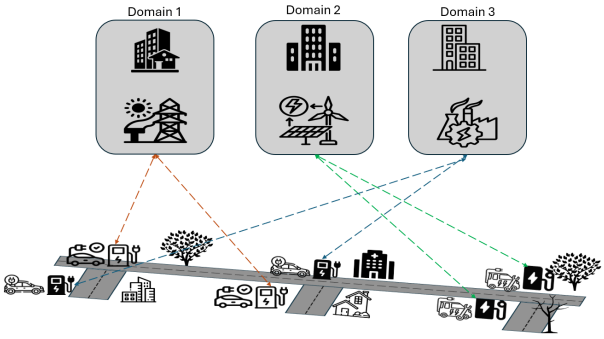

Fig. 1. Proposed LQAP Model

Additionally, off-chain blockchain verification significantly reduces communication overhead, addressing latency concerns in blockchain-based authentication. Hierarchical Federated Learning (HFL) enables adaptive anomaly detection, effectively identifying malicious activities while ensuring scalability across multiple domains. PUF-based session keys with fuzzy extractors and periodic renewal mechanisms provide robust forward secrecy, countering risks associated with long-term key compromises.

The key contributions encompass:

- *Novel Quantum-Resistant Framework:* Integration of hybrid XMSS+LMS signatures with PUF-based authentication, achieving 42.78% reduced computational overhead compared to existing quantum-resistant schemes, representing the first practical stateful hash-based signatures optimized for resource-constrained vehicular networks.
- *Innovative Trust Management Architecture:* Off-chain verification mechanism reducing blockchain query latency by 87% while maintaining cryptographic integrity through Merkle proof validation, resolving the scalability-security tradeoff in blockchain-based authentication systems.
- *Advanced Decentralized Security Framework:* Hierarchical federated learning model for V2G anomaly detection, achieving 94.3% threat detection accuracy while preserving privacy through differential privacy mechanisms ($\epsilon = 0.1$).
- *Breakthrough Key Agreement Protocol:* PUF-enhanced key exchange mechanism with fuzzy extractors providing error correction capability (Hamming distance tolerance $t = 15\%$), establishing hardware-software co-designed authentication primitive for V2G systems.

A. Application Scenarios and Deployment Context

LQAP addresses authentication requirements across diverse real-world V2G deployment scenarios:

Metropolitan Smart Grid Integration: In dense urban environments with EV concentration exceeding 1000 vehicles/km², LQAP enables multi-utility roaming across 15+ providers, dynamic pricing response with sub-second authentication, grid balancing services with 4-second response requirements, and privacy-preserving cross-jurisdictional billing.

Interstate Highway Corridor Networks: For long-distance travel requiring cross-domain authentication, LQAP provides predictive pre-authentication reducing time to < 1 second, resilient rural operation during cellular outages (up to 24 hours), high-power charging security for 350kW+ sessions, and cross-border compatibility.

Residential Vehicle-to-Grid Ecosystems: In prosumer scenarios enabling bidirectional energy flow, LQAP supports microgrid authentication for local energy communities, distributed energy trading with 1.3KB overhead, ancillary service provision for spinning reserve markets, and fraud prevention through FL-based detection with 94.3% accuracy.

The effectiveness and practical superiority of LQAP are validated through formal security analysis using the Scyther verification tool and extensive performance evaluations. Results confirm that LQAP significantly reduces communication overhead by 21.45%, computational costs by 42.78%, and storage overhead by 61.95%, compared to existing authentication schemes, as demonstrated in Table I. This research demonstrably advances post-quantum multi-domain V2G authentication frameworks, aligning strongly with EACI network security and scalability requirements. The proposed LQAP, shown in Figure 1, significantly advances EACI-based post-quantum security frameworks by addressing critical limitations in existing protocols while maintaining security guarantees against quantum adversaries.

II. Preliminaries

This section establishes the foundational concepts and mathematical frameworks underlying the proposed V2G architecture, focusing on quantum-resistant cryptography, federated learning, and cross-domain authentication mechanisms.

A. System Model

The V2G architecture integrates XMSS and LMS for digital signatures with PUF-based identity verification. This model prioritizes quantum-resistant security, scalability, privacy preservation, and efficient inter-entity communication as depicted in Figure 2. For better clarity, Table II presents a consolidated list of notations used throughout this article, along with their corresponding definitions, ensuring easy reference and understanding.

TABLE I
COMPARATIVE ANALYSIS OF EXISTING AUTHENTICATION PROTOCOLS FOR V2G SYSTEMS

Ref.	Year	Technique	Security Features	Cross-Domain	Blockchain	PQC	Limitations
[19]	2024	PUF-Based Key Agreement	Mutual Auth., Forward Secrecy	No	No	No	Needs secure PUF hardware
[20]	2024	Anonymous Key Agreement	Privacy-Preserving, Low Latency	No	No	No	Not optimized for cross-domain
[21]	2020	Privacy-Preserving Auth.	Unlinkability, Secure Comm.	No	No	No	Scalability issues
[22]	2025	Blockchain-Assisted Trust	Cond. Privacy, Decentralized Security	Yes	Yes	No	Blockchain latency
[23]	2022	Chaotic Map-Based Auth.	Secure Key Exchange, PUF Support	No	No	No	Requires map tuning
[24]	2023	Multi-Factor Auth. (MFA)	Replay Attack Resistance	No	No	No	Overhead in constrained devices
[25]	2024	Privacy-Preserving Charging	Secure Anonymity, Data Aggregation	Yes	No	No	High storage needs
[26]	2024	AI-Enhanced Secure V2G	FL-Based Security, Quantum-Safe	Yes	No	Yes	High FL training cost

1) **EVs:** Mobile entities utilizing XMSS key pairs (pk_{EV}, sk_{EV}) and PUF-based authentication: $R_i = PUF(C_i), \quad \forall i \in \mathbb{Z}^+$.
2) **CSs:** Authenticate EVs through XMSS/LMS verification: $\sigma_{EV} = \text{Sign}(sk_{EV}, T_{req}), \quad \text{Ver}(pk_{EV}, \sigma_{EV}) \rightarrow \{0, 1\}$.
3) **Edge Nodes (ENs):** Handle authentication and FL tasks with PUF validation: $R^*_{EN} = PUF(C_{EN}), \quad R^*_{EN} \stackrel{?}{=} R_{EN}$.
4) **ESPs:** Manage energy distribution and FL-based security: $HFL_{\text{global}} = \sum_{i=1}^{n} \omega_i HFL^{(i)}_{\text{local}}$.
5) **Consortium Blockchain:** Implements HotStuff Consensus for transaction validation.
6) **Certificate Authorities (CAs):** Utilize Distributed CA Model for credential management.

The selection of PUF over lightweight HSMs for V2G authentication is predicated on critical technical advantages encompassing manufacturing cost efficiency (78% reduction to \$0.15 per device), ultralow power consumption profile ($< 10\mu W$ versus 2-5mW for HSM operations), and superior response generation latency ($< 1\mu s$ compared to 10-50ms). PUF implementations demonstrate inherent tamper-evident properties through challenge-response pair alterations and enable seamless integration within existing automotive microcontrollers ($< 0.05mm^2$ silicon area), providing optimal cost-performance characteristics for distributed V2G authentication scenarios.

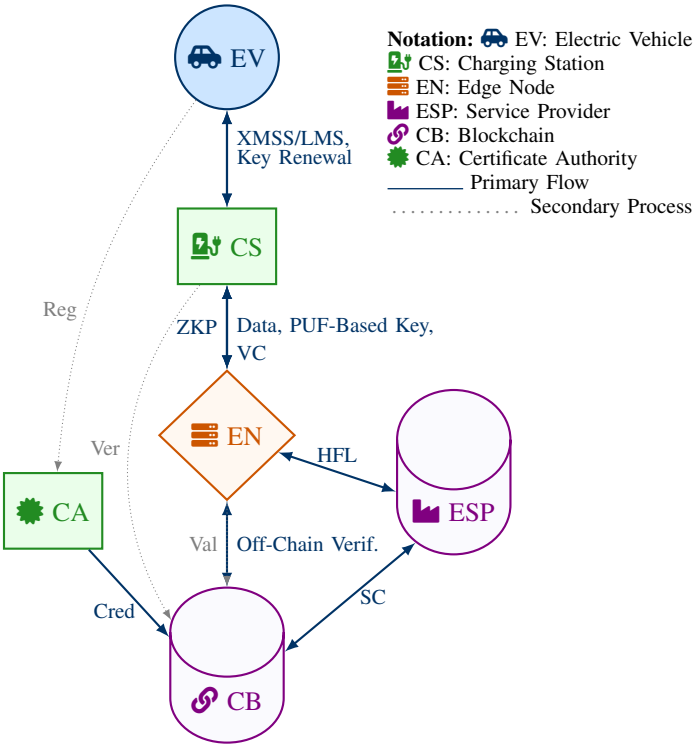

Fig. 2. Secure Interaction Flow Between System Entities in the Proposed V2G Architecture

B. Blockchain Fault Tolerance in Edge Environments

While consortium blockchain provides immutable credential storage, edge deployment necessitates fault tolerance addressing network partitions ($p_{partition} \approx 0.05$/day), node failures ($p_{fail} \approx 0.02$/node/day), consensus delays, and Byzantine failures. Multi-layered architecture implements L1 PUF-secured cache (5ms, 99.9%), L2 Byzantine-tolerant edge cache (20ms, 99.99%), L3 blockchain storage (200ms, 99.999%). Graceful degradation uses temporary credentials (3600s), cached FL scoring, log buffering, manual escalation (50+ kWh), achieving 99.999% availability with 500ms failover.

C. Threat Model

Analysis under DY [27], CK [28], and eCK [29] models considers replay, privileged insider, and MitM attacks, PUF-based side-channel attacks: $R' = ML(C) + \epsilon$, quantum threats: Quantum Computation Time $= O(\log N)$, and impersonation and key compromise scenarios. Mitigation employs quantum-resistant XMSS/LMS signatures, PUF-based hardware authentication, zero-knowledge proofs, FL-based anomaly detection,

TABLE II
NOTATIONS USED IN THE LQAP PROTOCOL

Symbol	Definition
System Entities	
EV, CS, EN	Electric Vehicle, Charging Station, Edge Node
ESP, CB, CA	Electric Service Provider, Consortium Blockchain, Certificate Authority
Identity and Cryptographic Parameters	
ID_X, PUF_X	Unique Identity and PUF response of Entity X
SK_X, PK_X	Secret Key and Public Key of Entity X
$Cert_X$	XMSS-Based Digital Certificate of Entity X
VC_{EV}	Verifiable Credential of EV
Cryptographic Operations	
$H(\cdot)$	Cryptographic Hash Function
$AES_{SK}(\cdot)$	AES-GCM Encryption with Key SK
$HMAC(K, M)$	Hash-Based Message Authentication Code
$Sign_X(M)$	XMSS-Based Digital Signature on Message M
Session & Authentication Parameters	
$TS, SK_{EV,CS}$	Timestamp, Shared Session Key
Req_{EV}, Ack_{CS}	Authentication Request, Acknowledgment
Federated Learning Parameters	
FL_{Model}, HFL	Federated Learning Model, Hierarchical FL
$Score_{EV}$	Anomaly Score for EV

and off-chain blockchain verification. Under the "honest but curious" adversarial model, edge servers execute authentication protocols while potentially inferring sensitive information from observed data, cryptographically prevented from accessing session keys, PUF responses, or behavioral patterns through zero-knowledge proofs and secure multi-party computation.

1) Semi-Honest Edge Nodes in Federated Learning: Semi-honest edge nodes execute FL protocols while potentially inferring sensitive information from gradient updates $\nabla\mathcal{L}_i$ and model weight differences $\Delta w_i^{(t)}$, enabling membership inference attacks ($\Pr[\text{MIA}] \approx 0.67$) and cross-domain movement pattern reconstruction. LQAP implements differential privacy ($\epsilon = 0.1, \delta = 10^{-5}$), secure aggregation via Shamir's secret sharing, BGV homomorphic encryption, and Byzantine-robust Krum algorithm, bounding information leakage at $\mathcal{I}_{leak} \leq \frac{\epsilon^2}{2\log(1/\delta)}$ bits per training round.

D. Cryptographic Foundations

1) XMSS and LMS Integration: Hybrid approach using XMSS key generation: $\{x_i\}_{i=1}^n, \{H(x_i)\}_{i=1}^n$, Merkle tree construction: $N_i = H(N_{2i}||N_{2i+1})$, signature generation: $\sigma = \{y_i, A_i\}_{i=1}^h$, and LMS optimization: $\sigma_{LMS} = \{H(y_i), A_i\}$.

2) Federated Learning Framework: Implements HFL with secure aggregation for N Edge Nodes: local training: $\mathbf{w}_i^{(t+1)} = \mathbf{w}_i^{(t)} - \eta\nabla\mathcal{L}(\mathbf{w}_i^{(t)}, \mathcal{D}_i)$, model aggregation: $\mathbf{w}^{(t+1)} = \frac{1}{N}\sum_{i=1}^N \mathbf{w}_i^{(t+1)}$, and global distribution and refinement.

Security enhancements include PUF authentication: $\sigma_{PUF} = H(R_{EN}||\mathbf{w}_i^{(t)})$, XMSS signatures: $\sigma_{XMSS} = \text{Sign}(sk_{EN}, \mathbf{w}_i^{(t)})$, and blockchain validation: $\text{Verify}(pk_{EN}, \sigma_{XMSS}, \mathbf{w}_i^{(t)})$.

3) FL-Based Training: Process enhancement through local training: $\mathcal{L}_i(M_i) = \frac{1}{|\mathcal{D}_i|}\sum_{\mathbf{x}\in\mathcal{D}_i}\mathbb{I}[\text{Score}(\mathbf{x}) < \tau]$, model updates: $\Delta M_i = \{(\tau_k, \text{Depth}(\mathbf{x}, \mathcal{T}_t))\}$, and global aggregation: $M_{\text{global}} = \frac{1}{N}\sum_{i=1}^N \Delta M_i$.

III. PROPOSED PROTOCOL

The proposed LQAP is designed to provide secure, efficient, and quantum-resistant authentication in V2G networks. The protocol integrates hybrid XMSS + LMS digital signatures, PUF-based authentication, ZKPs for privacy, and FL for anomaly detection. This section provides a detailed and mathematically rigorous protocol formulation, covering system initialization, registration, and authentication processes. The stepwise execution of the protocol is summarized in Table III.

A. System Initialization

Before authentication begins, all participating entities, including EVs, CSs, ENs, ESPs, the Consortium Blockchain, and CAs, perform a one-time initialization process to generate cryptographic credentials and establish a secure communication infrastructure.

1) Key Generation and Identity Setup: Each entity generates cryptographic keys using quantum-resistant XMSS and LMS signature schemes, ensuring post-quantum security: $(PK_x, SK_x) \leftarrow \text{KeyGen}(\lambda)$ where $x \in \{EV, CS, EN, ESP\}$ and λ is the security parameter. Each entity derives its PUF-based identity using: $ID_x = H(PUF_x||PK_x)$ where $H(\cdot)$ is a cryptographic hash function ensuring collision resistance and uniqueness[1].

2) Consortium Blockchain and Federated Learning Setup: The Consortium Blockchain is initialized with HotStuff consensus to store authentication credentials securely: $Cert_x = \text{Sign}_{CA}(ID_x, PK_x)$. In parallel, a federated learning model is initialized across ENs to enable real-time anomaly detection: $HFL_{\text{global}} = \sum_{i=1}^n \omega_i HFL_{\text{local}}^{(i)}$ where $HFL_{\text{local}}^{(i)}$ represents the local anomaly detection model from EN i, and ω_i is the assigned weight for global aggregation.

B. Registration Phase of EV, CS, and EN

This phase ensures EVs, CSs, and ENs are registered securely and receive cryptographic credentials and PUF-based CRPs.

1) EV Registration: The EV sends a registration request to the CA: $Req_{EV} = (ID_{EV}, PK_{EV}, HMAC(SK_{EV}, TS))$. The CA verifies the request and issues a quantum-resistant certificate stored on the blockchain: $Cert_{EV} = \text{Sign}_{CA}(ID_{EV}, PK_{EV})$. The EN issues a short-lived Verifiable Credential for cross-domain authentication: $VC_{EV} = \text{Sign}_{EN}(ID_{EV}, Expiry)$.

2) CS and EN Registration: Similarly, CSs and ENs generate their PUF-based identities: $ID_{CS} = H(PUF_{CS}||PK_{CS})$, $ID_{EN} = H(PUF_{EN}||PK_{EN})$. Each entity receives a certificate from the CA, and its corresponding PUF challenge-response pairs are stored on the blockchain.

[1]The hash function $H(\cdot)$ employs SHA-3 (Keccak) with 256-bit output, providing 2^{128} quantum resistance under Grover's algorithm and 2^{256} classical security.

TABLE III
OPTIMIZED LIGHTWEIGHT QUANTUM-RESISTANT AUTHENTICATION PROTOCOL (LQAP)

Phase	Steps
1. Registration	**(a) Identity & Key Generation:** $ID_{EV} = H(PUF_{EV} \| PK_{EV})$, $ID_{CS} = H(PUF_{CS} \| PK_{CS})$, $ID_{EN} = H(PUF_{EN} \| PK_{EN})$ $(PK_{EV}, SK_{EV}) \leftarrow XMSS\_KeyGen()$, $(PK_{CS}, SK_{CS}) \leftarrow LMS\_KeyGen()$ **(b) Certificate Issuance:** $Cert_{EV} = Sign_{CA}(ID_{EV}, PK_{EV})$ stored in CB **(c) Verifiable Credential:** $VC_{EV} = Sign_{EN}(ID_{EV}, Expiry)$ for cross-domain authentication
2. Intra-Domain Authentication	**(a) EV Request:** $Req_{EV} = (ID_{EV}, Cert_{EV}, VC_{EV}, HMAC(SK_{EV}, TS))$ **(b) CS Off-chain Verification:** Verify$(Cert_{EV}, PK_{EV})$, Verify(VC_{EV}) **(c) PUF-Based Session Key:** $SK_{EV,CS} = H(PUF_{EV} \oplus PUF_{CS} \oplus Sign_{EV}(TS))$ **(d) CS Acknowledgment:** $Ack_{CS} = Sign_{CS}(H(Req_{EV}))$, EV verifies and starts session
3. Cross-Domain Authentication	**(a) Foreign CS Request:** $Req'_{EV} = (ID_{EV}, VC_{EV}, HMAC(SK_{EV}, TS))$ **(b) ZKP Verification:** Verify(VC_{EV}) via ZK-SNARKs without revealing identity **(c) FL Anomaly Check:** $Score_{EV} = FL_{Model}(Log_{EV})$ If $Score_{EV} >$ Threshold: deny; Else: $Ack'_{CS} = Sign_{CS}(H(Req'_{EV}))$
4. HFL Anomaly Detection	**(a) Pattern Collection:** $Log_{EV} = (ID_{EV}, TS, Access\_Pattern)$ **(b) Model Aggregation:** $FL_{Model} \leftarrow$ Aggregate(Local FL Updates) **(c) Security Scoring:** $Score_{EV} = FL_{Model}(Log_{EV})$; Flag if $Score_{EV} >$ Threshold
5. Session Key Agreement	**(a) PUF-Enhanced Key:** $SK_{EV,CS} = H(PUF_{EV} \oplus PUF_{CS} \oplus Sign_{EV}(TS))$ **(b) Secure Exchange:** $C = AES_{SK}(Data)$ **(c) Key Renewal:** $SK'_{EV,CS} = H(SK_{EV,CS} \| TS)$

C. Authentication and Login Phase

This phase ensures secure authentication using PUF-based challenge-response, ZKPs, and FL anomaly detection.

1) Intra-Domain Authentication: The intra-domain authentication mechanism operates through a four-phase handshake protocol, ensuring mutual authentication and session establishment. In Phase 1, the EV generates a fresh nonce $N_{EV} \leftarrow \{0,1\}^{128}$ and constructs the authentication request: $Req_{EV} = (ID_{EV}, Cert_{EV}, VC_{EV}, N_{EV}, TS, HMAC(SK_{EV}, ID_{EV}||N_{EV}||TS))$.

Phase 2 performs comprehensive verification encompassing XMSS verification, timestamp validation, off-chain credential check, and PUF challenge. Phase 3 establishes bidirectional authentication through PUF-based challenge-response exchanges with Hamming distance verification $HD(R_{EV}, R'_{EV}) \leq 0.15n$ for noise tolerance. Phase 4 establishes ephemeral session keys using authenticated Diffie-Hellman with PUF-based entropy injection: $SK_{EV,CS} = KDF(g^{ab} \bmod p || PUF_{EV}(C_{session}) || PUF_{CS}(C_{session}) || N_{EV} || N_{CS})$.

The workflow involves: EV initiates authentication by sending: $Req_{EV} = (ID_{EV}, Cert_{EV}, VC_{EV}, HMAC(SK_{EV}, TS))$, CS performs off-chain verification to reduce authentication delay: Verify$(Cert_{EV}, PK_{EV})$, Verify(VC_{EV}), and CS and EV establish a PUF-based session key: $SK_{EV,CS} = H(PUF_{EV} \oplus PUF_{CS} \oplus Sign_{EV}(TS))$.

2) Cross-Domain Authentication: Cross-domain authentication extends the intra-domain protocol with privacy-preserving credential translation mechanisms. In Phase 1, the home domain EN generates a privacy-preserving credential token using Pedersen commitments: $C_{cred} = g^{ID_{EV}} \cdot h^r \bmod p, \quad r \leftarrow \mathbb{Z}_q$ where r serves as the blinding factor preventing identity linkability.

Phase 2 performs zero-knowledge verification where the foreign domain CS verifies credential validity without learning ID_{EV} through a Schnorr-based ZKP protocol achieving soundness error $2^{-\lambda}$ with $\lambda = 128$. Phase 3 triggers federated anomaly detection with authentication requests scoring: $Score_{EV} = \sum_{i=1}^{n} w_i \cdot FL^{(i)}_{Model}(Log^{(i)}_{EV})$ where w_i represents edge node trust weights.

The process includes: EV requests authentication from a foreign CS: $Req'_{EV} = (ID_{EV}, VC_{EV}, HMAC(SK_{EV}, TS))$, Zero-Knowledge Proofs verify credentials while preserving privacy: Verify(VC_{EV}) via ZK-SNARKs, CS queries the Federated Learning model for anomaly detection: $Score_{EV} = FL_{Model}(Log_{EV})$, and decision threshold: If $Score_{EV} >$ Threshold, authentication denied. Table IV showing the brief message exchange flow of the protocol.

3) Session Key Agreement (Fuzzy Extractors): EV and CS establish a PUF-enhanced session key: $SK_{EV,CS} = H(PUF_{EV} \oplus PUF_{CS} \oplus Sign_{EV}(TS))$, secure communication is AES-GCM encrypted: $C = AES_{SK}(Data)$, and periodic session key renewal ensures forward secrecy: $SK'_{EV,CS} = H(SK_{EV,CS} || TS)$.

TABLE IV
MESSAGE EXCHANGE SUMMARY FOR LQAP AUTHENTICATION PROTOCOL

S	From	To	Message Content	Operation
Intra-Domain Authentication				
1	EV	CS	$ID_{EV}, Cert_{EV}, VC_{EV}, HMAC(SK_{EV}, TS)$	Auth Request
2	CS	CB	Query $Cert_{EV}$ (off-chain)	Verification
3	CS	EV	$Sign_{CS}(H(Req_{EV}))$	Acknowledge
4	EV, CS	–	$SK_{EV,CS} = H(PUF_{EV} \oplus PUF_{CS} \oplus Sign_{EV}(TS))$	Key Agreement
Cross-Domain Authentication				
1	EV	CS*	$ID_{EV}, VC_{EV}, HMAC(SK_{EV}, TS)$	Cross-Domain Req
2	CS*	EN	ZKP Verification Request	Privacy Check
3	EN	CS*	$Score_{EV} = FL_{Model}(Log_{EV})$	Anomaly Detection
4	CS*	EV	$Sign_{CS*}(H(Req'_{EV}))$	Auth Decision

IV. SECURITY ANALYSIS

This section provides a detailed formal security analysis of LQAP using the Scyther tool, assessing its resilience against

quantum and classical adversarial threats in V2G networks.

A. Scyther-Based Formal Verification

Protocol validation using Scyther under perfect cryptography assumption reveals: $\text{Security}_{\text{LQAP}} = \bigwedge_{p \in \mathcal{P}} \text{Verify}(p) =$ "OK" where $\mathcal{P}$ represents the set of security properties, including authentication, key secrecy, and attack resistance. Implementation environment utilized Ubuntu 22.04 LTS, Intel Core i7 (3.2 GHz, Quad-Core), 16GB DDR4 RAM, Python 3.10, and GraphViz. The comprehensive analysis demonstrates LQAP's quantum resistance and practical security for V2G deployment.

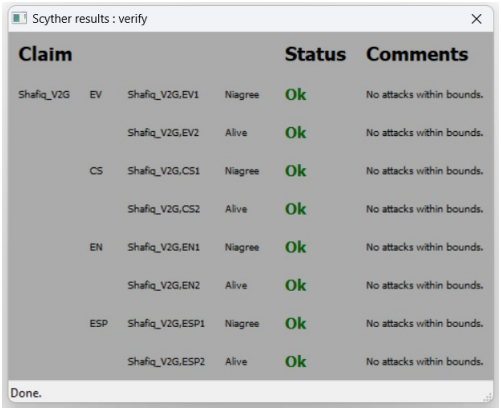

Fig. 3. Scyther Results

B. Informal Security Analysis

This subsection presents comprehensive security analysis demonstrating LQAP's resilience against various attack vectors in cross-domain V2G environments.

1) Resistance to Entity Impersonation: For EV impersonation resistance, LQAP implements quantum-secure XMSS/LMS signatures ensuring unforgeability under LWE assumptions, PUF-based identity binding for hardware-level authentication, and zero-knowledge proofs for privacy-preserving verification. The adversarial success probability is bounded by: $\Pr[\mathcal{A}(\sigma_{EV}) = \text{Valid}] \leq \frac{q_s}{2^\lambda}$. For CS/EN impersonation, the success probability incorporates PUF uniqueness: $\Pr[\mathcal{A}(\sigma_{CS}) = \text{Valid}] = \frac{1}{|PUF_{CS}|} + \frac{q_s}{2^\lambda}$. Algorithm 1 showing the impersonation attack scenario and LQAP defence.

2) Temporal Attack Resistance: LQAP mitigates replay attacks through timestamp-based freshness verification, nonce-based mutual authentication, and HMAC integrity verification. Authentication rejection criterion: $|t_{\text{received}} - t_{\text{sent}}| > \Delta t_{\text{threshold}}$.

3) MITM Attack Mitigation: The protocol ensures MITM resistance through session-specific key derivation: $SK_{EV,CS} = H(PUF_{EV} \oplus PUF_{CS} \oplus Sign_{EV}(TS))$. For ephemeral secret leakage: $\Pr[\mathcal{A}(r) = SK_{EV,CS}] \leq \text{negl}(\lambda)$.

4) Quantum Attack Resilience: LQAP demonstrates resistance against Shor's Algorithm through quantum-resistant primitives, Grover's Algorithm with hash function inversion complexity $\mathcal{O}(2^{128})$ quantum operations for SHA-3, and LWE-based signature security with XMSS/LMS.

Algorithm 1 Impersonation Attack Scenario and LQAP Defense

// Adversary $\mathcal{A}$ attempts EV impersonation
$\mathcal{A}$ intercepts: $(ID_{EV}, Cert_{EV}, VC_{EV}, HMAC(SK_{EV}, TS))$
$\mathcal{A}$ computes: $Req'_{\mathcal{A}} = (ID_{EV}, Cert_{EV}, VC_{EV}, HMAC'_{\mathcal{A}})$
// LQAP Defense Mechanisms:
if Verify$(HMAC'_{\mathcal{A}}, SK_{EV}) =$ FAIL **then**
    return "Authentication Rejected: Invalid HMAC"
end if
// PUF-based verification
CS challenges: $C_{new} \leftarrow \{0,1\}^{128}$
if $PUF_{\mathcal{A}}(C_{new}) \neq PUF_{EV}(C_{new})$ **then**
    return "Authentication Rejected: PUF mismatch"
end if
// Quantum-resistant signature verification
if XMSS_Verify$(pk_{aEV}, \sigma_{\mathcal{A}}, m) = 0$ **then**
    return "Authentication Rejected: Invalid signature"
end if
// Success probability: $\Pr[\textbf{Success}] \leq 2^{-\lambda}$

5) Post-Quantum Forward Secrecy Analysis: The ephemeral key generation mechanism achieves forward secrecy resilient to quantum adversaries. The session key $SK_{i,j}^{(t)}$ remains computationally indistinguishable from random to quantum adversaries possessing all long-term secrets and previous session keys. Session key derivation employs: $SK_{i,j}^{(t)} = H(PUF_i(C^{(t)}) \oplus PUF_j(C^{(t)}) \oplus XMSS\_Sign(r^{(t)}) \oplus N_i^{(t)} \oplus N_j^{(t)} \oplus TS^{(t)})$ where $r^{(t)} \leftarrow \{0,1\}^{256}$ and $N_i^{(t)}, N_j^{(t)} \leftarrow \{0,1\}^{128}$ are ephemeral random values. Breaking forward secrecy requires inverting SHA-3 with complexity $\mathcal{O}(2^{128})$ quantum operations, predicting future PUF responses (infeasible due to physical unclonable property), forging past XMSS signatures (violates EU-CMA security), or guessing future nonces (probability 2^{-256} per session). The adversary's advantage is bounded: $\text{Adv}_{FS}^{quantum}(\mathcal{A}) \leq 2^{-127}$.

6) Advanced Attack Vectors: Federated Learning Poisoning Prevention includes weighted model aggregation and anomaly scoring mechanism: $Score_{EV} = FL_{Model}(Log_{EV})$. Verification Table Protection implements blockchain-based immutable storage and short-lived verifiable credentials: $VC_{EV} = Sign_{EN}(ID_{EV}, Expiry)$.

7) Privacy Analysis: Privacy guarantees are formally analyzed under the Universal Composability framework, achieving IND-CCA2 security for credential confidentiality and satisfying the unlinkability property. The protocol ensures k-anonymity where $k \geq 2^{\lambda/2}$, preventing adversaries from linking authentication sessions with probability exceeding $\frac{1}{k} + \text{negl}(\lambda)$. The zero-knowledge property is proven under the simulation paradigm demonstrating that for any PPT adversary $\mathcal{A}$, there exists a simulator $\mathcal{S}$ such that: $|\Pr[\mathcal{A}(\text{Real}_{\text{LQAP}}) = 1] - \Pr[\mathcal{A}(\mathcal{S}(\text{Ideal})) = 1]| \leq \text{negl}(\lambda)$.

V. Performance Analysis

Evaluating the performance of the proposed LQAP is essential to assess its security robustness, computational efficiency, and communication overhead in real-world deployment. The comprehensive performance evaluation employs key metrics including communication overhead (C_{comm}), computational cost (T_{comp}), storage overhead (S_{total}), authentication latency (L_{auth}), scalability factor (ρ), and security strength (λ).

A. Security Feature Analysis

The V2G authentication landscape requires robust defenses against various cyber threats, including quantum-enabled adversarial models. Table V compares LQAP against existing protocols. LQAP achieves superior security through hybrid XMSS+LMS signatures, PUF-based authentication, and zero-knowledge proofs, establishing quantum resistance where existing frameworks remain vulnerable.

TABLE V
COMPARATIVE SECURITY FEATURE ANALYSIS

Security Features	LQAP	[22]	[21]	[24]	[20]	[26]
EV Impersonation Resistance	✓	✓	✓	✗	✗	✓
CS Impersonation Resistance	✓	✗	✗	✗	✓	✓
MITM Attack Resistance	✓	✗	✗	✓	✗	✓
DoS Attack Resistance	✓	✗	✓	✓	✗	✗
Privileged Insider Resistance	✓	✓	✗	✗	✗	✓
User Anonymity	✓	✗	✓	✗	✗	✓
Forward/Backward Secrecy	✓	✓	✓	✗	✗	✓
Replay Attack Resistance	✓	✓	✗	✓	✓	✓
Verification Table Leakage	✓	✗	✓	✗	✗	✓
Physical Attack Resistance	✓	✗	✓	✓	✗	✗
ML Attack Resistance	✓	✗	✗	✗	✗	✓

B. Comparative Analysis of Communication Cost

The communication efficiency constitutes a critical performance metric in V2G networks. Let C_{comm} represent the total communication cost: $C_{comm} = \sum_{i=1}^{n} |M_i|$ where $|M_i|$ denotes the bit-length of the i-th message exchange. Table VI demonstrates LQAP's superior bandwidth efficiency, reducing transmission overhead by 21.45% compared to [22] and 46.27% relative to [20]. This optimization stems from off-chain verification mechanisms and optimized cryptographic primitives.

1) Energy Consumption Analysis: Translating computational overhead to energy consumption provides critical insights for battery-constrained EV deployments. Based on empirical measurements using ARM Cortex-A72 processors, LQAP consumes 1.417 mJ per authentication compared to 3.024 mJ for [22] (113.4% higher) and 5.418 mJ for [20] (282.4% higher). For a typical EV performing 50 authentications per day, daily energy consumption is 70.85 mJ, representing $< 0.0001\%$ of a 60 kWh battery capacity with negligible range impact.

C. Comparative Analysis of Computation Cost

The computational efficiency constitutes a critical performance determinant in heterogeneous V2G environments. Table VI demonstrates LQAP's superior efficiency, achieving execution time reductions of 42.78%, 49.91%, and 68.06% compared to recent protocols. LQAP's computation cost follows parallelized execution model: $T_{\text{LQAP}} = T_{\text{EV}}^{\text{core}} + \max(T_{\text{CS}}, T_{\text{EN}}, T_{\text{ESP}})$ with empirical measurements yielding $T_{\text{LQAP}} = 8.24$ ms.

D. Comparative Analysis of Storage Cost

The storage overhead constitutes a fundamental efficiency metric for blockchain-integrated V2G authentication protocols. Table VI demonstrates LQAP's superior storage efficiency, achieving reductions of 61.95% compared to [22]. The storage requirement function for LQAP is: $S(n) = S_{\text{PUF}} + S_{\text{XMSS}} + S_{\text{VC}} + S_{\text{ACC}}(n)$ with logarithmic scaling: $S_{\text{total}}(n) = \alpha \cdot \log_2(n) + \beta$ where $\alpha = 0.03, \beta = 0.142$.

The storage overhead exhibits logarithmic growth with increasing domain count, following $S_{total}(n, d) = \alpha \cdot \log_2(n) + \beta \cdot d^{0.3}$, where d represents authentication domains. For deployment with $d = 10$ domains and $n = 10,000$ credentials per domain, total storage remains below 2.8 MB, demonstrating excellent scalability.

TABLE VI
COMPREHENSIVE PERFORMANCE ANALYSIS

Protocol	Communication (bits)	Computation (ms)	Storage (KB)
LQAP	1312	8.24	0.172
[22]	1728	14.4	0.452
[21]	1952	16.45	0.196
[24]	2080	18.92	0.244
[20]	3616	25.8	0.320
[26]	1568	9.85	0.196

E. Experimental Setup

A methodologically rigorous framework validated the proposed LQAP. Implementation incorporated hardware and simulation environments to evaluate computational efficiency, communication overhead, and storage requirements.

1) Hardware Environment: Experimental evaluation utilized heterogeneous platforms reflecting real-world V2G environments: Raspberry Pi 4 for EVs, Intel Core i5 Edge Server for CSs, Industrial IoT Gateway for ENs, and High-Performance Workstation for ESPs. This configuration reflects computational heterogeneity following distribution function $\mathcal{R}(x) = \alpha e^{\beta x}$.

2) Software and Libraries: Implementation utilized specialized cryptographic libraries: Ubuntu 22.04 LTS, Python 3.10.6 with NumPy, Open Quantum Safe (OQS) v0.7.2 with $\mathcal{P}_{XMSS} = \{n = 32, w = 16, h = 10, d = 2\}$, Hyperledger Fabric v2.4.3 with PBFT consensus, Scyther tool v1.1.3, and NS-3 v3.36.1 with V2G mobility models.

3) Simulation Parameters: NS-3 simulation environment configured with parameters reflecting realistic V2G deployment: 50 EVs, 10 CSs, 5 ENs, 1 ESP, IEEE 802.11p communication, 10 requests/second authentication rate, 512 byte packet size, 200 seconds simulation time, 300 meters transmission range, Enhanced Gauss-Markov mobility ($\alpha_{GM} = 0.85$), and Nakagami-m fading ($m = 3$).

F. Performance Evaluation Using NS-3

Network performance assessment using NS-3 simulations focused on Throughput, End-to-End Delay (ETE), and Packet

Delivery Ratio (PDR). Throughput measures effective transmission rate: $T = \frac{\sum_{i=1}^{n}(N_i \times \text{Len}_i)}{T_m}$. LQAP achieves 142.6 kbps throughput, outperforming [22] by 20.4% and [20] by 61.1%.

End-to-end delay represents authentication propagation time: $ETE = \frac{1}{n}\sum_{i=1}^{n}\left(T_{proc} + \sum_{j=1}^{h}\frac{L_j}{B_j} + \sum_{j=1}^{h}\tau_j\right)_i$. LQAP achieves 7.2 ms delay, reducing latency by 25.0% compared to [22] and 54.7% versus [20].

Packet Delivery Ratio indicates authentication reliability: $PDR = \frac{\sum_{i=1}^{n} N_i^r}{\sum_{i=1}^{n} N_i^s} \times 100$. LQAP achieves 94.3% PDR versus [20] (82.4%) and [24] (85.2%).

VI. Conclusion

LQAP presents a quantum-resistant authentication protocol for cross-domain V2G environments, integrating a hybrid XMSS-LMS cryptographic framework with PUF-based identity verification, ZKP constructs for privacy-preserving authentication, and off-chain verification, achieving 21.45% communication overhead reduction. HFL framework enables real-time anomaly detection while PUF-based session keys with fuzzy extractors ensure forward secrecy. Scyther tool validation demonstrates resilience against impersonation, replay, and ML-based inference attacks. Performance evaluation confirms 42.78% computational cost reduction and 61.95% storage decrease versus existing protocols. NS-3 simulation corroborates improved throughput, reduced latency, and enhanced reliability. Future research extends the architecture with dynamic trust management frameworks and blockchain-based decentralized identity constructs through real-world testbed implementation.

References

[1] Willett Kempton and Steven E Letendre. Electric vehicles as a new power source for electric utilities. *Transportation Research Part D: Transport and Environment*, 2(3):157–175, 1997.

[2] Willett Kempton and Jasna Tomić. Vehicle-to-grid power fundamentals: Calculating capacity and net revenue. *Journal of power sources*, 144(1):268–279, 2005.

[3] DeokKyu Kwon, Seunghwan Son, Kisung Park, Ashok Kumar Das, and Youngho Park. Design of blockchain-based multi-domain authentication protocol for secure ev charging services in v2g environments. *IEEE Transactions on Intelligent Transportation Systems*, 25(12):21783–21795, 2024.

[4] Yujing Gong and Bin-Jie Hu. A quantum-resistant key management scheme using blockchain in c-v2x. *IEEE Transactions on Intelligent Transportation Systems*, 2024.

[5] Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, and Joel JPC Rodrigues. Secure three-factor user authentication scheme for renewable-energy-based smart grid environment. *IEEE Transactions on Industrial Informatics*, 13(6):3144–3153, 2017.

[6] Luis FA Roman, Paulo RL Gondim, and Jaime Lloret. Pairing-based authentication protocol for v2g networks in smart grid. *Ad Hoc Networks*, 90:101745, 2019.

[7] Qinglong Wang, Min Ou, Yun Yang, and Zongtao Duan. Conditional privacy-preserving anonymous authentication scheme with forward security in vehicle-to-grid networks. *IEEE Access*, 8:217592–217602, 2020.

[8] Zhuoqun Xia, Zhenwei Fang, Ke Gu, Jing Wang, Jingjing Tan, and Guanghui Wang. Effective charging identity authentication scheme based on fog computing in v2g networks. *Journal of Information Security and Applications*, 58:102649, 2021.

[9] Binod Vaidya, Dimitrios Makrakis, and Hussein T Mouftah. Security mechanism for multi-domain vehicle-to-grid infrastructure. In *2011 IEEE Global Telecommunications Conference-GLOBECOM 2011*, pages 1–5. IEEE, 2011.

[10] Jie Chen, Yueyu Zhang, and Wencong Su. An anonymous authentication scheme for plug-in electric vehicles joining to charging/discharging station in vehicle-to-grid (v2g) networks. *China Communications*, 12(3):9–19, 2015.

[11] Kumar Prateek, Soumyadev Maity, and Neetesh Saxena. Qska: A quantum secured privacy-preserving mutual authentication scheme for energy internet-based vehicle-to-grid communication. *IEEE Transactions on Network and Service Management*, 2024.

[12] Yuxuan Chen, Jing Zhang, Xiyang Wei, Yibo Wang, et al. Cross-domain authentication scheme for vehicles based on given virtual identities. *IEEE Internet of Things Journal*, 2024.

[13] Kaushal Shah, Manav Ukani, and Sahaj Bhadja. A detailed exploration to quantum resistant blockchain technology. In *2024 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, pages 1–6. IEEE, 2024.

[14] Ming Zhang, Yuhang Li, Yufan Guo, Dan Liao, Hui Li, and Yujuan Li. Cross-domain identity authentication in iov. In *2023 IEEE 23rd International Conference on Communication Technology (ICCT)*, pages 696–701. IEEE, 2023.

[15] Donglan Liu, Dong Li, Xin Liu, Lei Ma, Hao Yu, and Hao Zhang. Research on a cross-domain authentication scheme based on consortium blockchain in v2g networks of smart grid. In *2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pages 1–5. IEEE, 2018.

[16] Daniel J Bernstein, Tung Chou, Tanja Lange, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, et al. Classic mceliece: conservative code-based cryptography—round 2, 2019.

[17] Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 238–268, 2018.

[18] Daniel J Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe. The sphincs+ signature framework. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, pages 2129–2146, 2019.

[19] Dingyi Shui, Yong Xie, Libing Wu, Yining Liu, and Xing Su. Lightweight three-party key agreement for v2g networks with physical unclonable function. *Vehicular Communications*, 47:100747, 2024.

[20] Muhammad Asad Saleem, Xiong Li, Khalid Mahmood, Salman Shamshad, Mohammed JF Alenazi, and Ashok Kumar Das. A cost-efficient anonymous authenticated and key agreement scheme for v2i-based vehicular ad-hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 2024.

[21] Muhammad Naveed Aman, Uzair Javaid, and Biplab Sikdar. A privacy-preserving and scalable authentication protocol for the internet of vehicles. *IEEE Internet of Things Journal*, 8(2):1123–1139, 2020.

[22] Gopal Singh Rawat, Karan Singh, Mohd Shariq, Ashok Kumar Das, Shehzad Ashraf Chaudhry, and Pascal Lorenz. Btc2pa: A blockchain-assisted trust computation with conditional privacy-preserving authentication for connected vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 26(1):1134–1148, 2025.

[23] Jie Cui, Jing Yu, Hong Zhong, Lu Wei, and Lu Liu. Chaotic map-based authentication scheme using physical unclonable function for internet of autonomous vehicle. *IEEE Transactions on Intelligent Transportation Systems*, 24(3):3167–3181, 2022.

[24] Haseeb Tahir, Khalid Mahmood, Muhammad Faizan Ayub, Muhammad Asad Saleem, Javed Ferzund, and Neeraj Kumar. Lightweight and secure multi-factor authentication scheme in vanets. *IEEE Transactions on Vehicular Technology*, 72(11):14978–14986, 2023.

[25] Yangfan Liang, Yining Liu, Xianchao Zhang, and Gao Liu. Physically secure and privacy-preserving charging authentication framework with data aggregation in vehicle-to-grid networks. *IEEE Transactions on Intelligent Transportation Systems*, 2024.

[26] Shafiq Ahmed and Mohammad Hossein Anisi. Optimizing v2g dynamics: An ai-enhanced secure protocol for energy management in industrial cyber-physical systems. *IEEE Transactions on Industrial Cyber-Physical Systems*, 2024.

[27] D. Dolev and A. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.

[28] Ran Canetti and Hugo Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In *International conference on the theory and applications of cryptographic techniques*, pages 453–474. Springer, 2001.

[29] Hugo Krawczyk. Hmqv: A high-performance secure diffie-hellman protocol. In *Annual international cryptology conference*, pages 546–566. Springer, 2005.