Privacy-Preserving Software Engineering Protocol for V2V Charging Using Lattice-Based Linkable Ring Signature

Mustafa Moosa Qasim [1,*], Murtadha Al-Maliki [2,3], Jalal M. H. Altmemi [4], Abdullah Almogahed [5] Mahmood A. Al-Shareeda [6,7,*], Mohammed Amin Almaiah [8], and Marwan Albahar [9]

[1] Department of Intelligent Medical Systems, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq
[2] Department of Polymers and Petrochemicals Engineering, Oil and Gas Engineering College, Basrah University for Oil and Gas, Basrah, Iraq
[3] Department of Information and Communication Engineering, Alfarqadein University College, Iraq
[4] Information Technologies Management Department, Southern Technical University, Basrah, Iraq
[5] Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia, Parit Raja, 84600, Johor, Malaysia
[6] Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, 61001, Iraq
[7] College of Engineering, Al-Ayen University, Thi-Qar, Iraq
[8] King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan
[9] College of Engineering and Computing, Al-Lith Umm Al-Qura University, Makkah, Saudi Arabia
Email: Mustafa.mq87@uobasrah.edu.iq (M.M.Q); murtadha.almaliki@buog.edu.iq (M.A-M.); Jalal.altmemi@stu.edu.iq (J.M.H.A.); abdullahm@uthm.edu.my (A.A.); mahmood.alshareedah@stu.edu.iq (M.A.A-S.); m.almaiah@ju.edu.jo (M.A.A.), Mobaydat@kfu.edu.sa (M.A.)
*Corresponding Author

***Abstract*—The advances in Electric Vehicles (EVs) will intensify the demand of decentralized and privacy-preserving Vehicle-to-Vehicle (V2V) charging schemes. However, current blockchain methods only protect the privacy of users from identity and linkability attack, quantum adversary attack. This paper introduces a lightweight and none-privacy-revealing CV2C charging protocol based on lattice-based linkable ring signatures over the Ring-SIS assumption, aiming at providing future post-quantum secure communication with high degree of anonymity, unlinkability and accountability. We design key generation to be certificateless – containing no escrowed keys while facilitating scalable identity management, and provide a lattice-based stealth address scheme which generates one-time unlinkable payment addresses for increased recipient privacy. The protocol runs on a consortium blockchain and employs Practical Byzantine Fault Tolerance (PBFT) for fast validation of the transactions and transparency. A security analysis is provided and resistance against forgery, replay, and quantum attacks is shown. Performance analysis indicates that the required computational and communication overheads are much lower than those of elliptic-curve and pairing-based schemes, which reveals its suitability for EV environments with limited resources. The proposed scheme is a practical and secure structure for future V2V energy trading-based systems.**

***Keywords*—lattice-based cryptography, ring-SIS, Vehicle-to-Vehicle (V2V) charging, privacy-preserving protocol, Electric Vehicle (EV) energy trading, stealth addresses**

Manuscript received September 15, 2025; revised October 24, 2025; accepted November 4, 2025; published March 27, 2026.

I. Introduction

The rapid uptake of Electric Vehicles (EVs) requires responsive, decentralized, and secure charging infrastructure [1–4]. With the changing paradigms of urban mobility, and with the restrictions of traditional static charge stations (high infrastructure investment, long waiting times, power distribution limits, etc.), they resort to more agile solutions [5–7]. Vehicle-to-Vehicle (V2V) energy trading is one of the most promising solutions, allowing the direct energy trade between EVs close to each other [8–10]. This new paradigm, however, brings important security and privacy challenges, including transaction confidentiality, user anonymity, and participants' trustworthiness [11–13].

To tackle these challenges, blockchain-based solutions [14–16] suggested that allow for decentralized authentication and tamper-evident transaction logging. Although blockchain provides mechanisms of enhanced transparency, the transparency of blockchain systems itself renders it vulnerable to user privacy violations, as both transaction metadata and identity bindings are publicly accessible [17–19]. Cryptographic primitives (e.g., elliptic

curve cryptography or pairing-based constructions) have been employed in classical blockchain protocols to enable privacy-preserving transactions; however, these schemes are recognized as quantum-resistant applications [20–22]. Thus, several new privacy-preserving V2V energy trading protocols must be designed that are decentralized, efficient, and secure against quantum adversaries [23–27].

The originality of the study lies in the combination of ideas that have not been combined earlier in any V2V charging protocol. Unlike previous methods that grant either privacy or partial decentralization, our scheme is able to achieve the four essential properties at the same time.

- Post-quantum security based on a lattice-based linkable ring signature built over the Ring-SIS assumption.
- Certificateless Key Generation that removes the requirement for key escrow, yet still supports structured identity management in EMs.
- Stealth Address mechanism which supports unlinking transactions and the prevention of recipient's anonymity loss, even in transparent blockchain ledgers.
- Mitigated centralization of KGC and CAs by using threshold cryptography and blockchain to assure auditability, making it more practical due to its decentralized deployment.

Finally, to the best of our knowledge, this is the first V2V charging protocol that integrates in one particular fully-fledged solution these four principles at once: originality and concrete applicability. In a nutshell, this paper proposes a post-quantum, privacy-preserving V2V charging protocol which guarantees: Robust anonymity and unlinkability by way of linkable ring signatures and stealth addresses; Blockchain integration for public verification and accountability; Secure pseudo-identity mapping to trace malicious users; Ring-SIS Problem Hardness Based Post-Quantum Security; The computation is lightweight and can be executed on the EV hardware. We then provide a detailed security and performance analysis, showing that our proposed scheme achieves a good trade-off between efficiency and strong cryptographic guarantees, in particular when compared to existing lattice- and pairing-based protocols. To the best of our knowledge, this is the first work capable of achieving all these features: both lattice-based post-quantum security and certificateles authentication and stealth address generation, which are combined for countermeasures to KGC/CA centralization, which so far appear to be addressing practical deployment challenges in V2V settings.

II. Related Work

Long *et al.* [28] proposed a blockchain-based energy trading scheme for V2G and G2V electricity trading in vehicular energy networks, which supports more efficient cross-domain transactions and offers better privacy protection to users. Radi *et al.* [29] present a zero-knowledge energy trading system, which allows for the most privacy, called Zero-Knowledge Proofs, which integrates EV charging, anonymous payments, and the use of blockchain. Baza *et al.* [30] present a dual-scheme blockchain-based energy trading system—CS2V and V2V—for urban and decentralized EV charging scenarios. Linkable anonymous authentication provides strong privacy and protection against Sybil attacks. Shen *et al.* [31] present a traceable and privacy-preserving authentication scheme for V2G networks, which improves the inefficiency of certificateless systems. Li *et al.* [32] introduced a blockchain-based privacy-preserving bidirectional power trading system between EVs and the grid. To optimize large-scale scheduling and minimize load deviations, it uses a more improved Krill Herd algorithm.

Zhang *et al.* [33] proposed a secure and efficient data sharing scheme for VANETs based on blockchain and traceable ring signature. S will reduce RSU load and detect malicious vehicles by coupling edge computing and smart contracts. The approach mitigates the overhead and traceability limitations of previous methods. Zhang *et al.* [34] proposed a new privacy-preserving scheme designed for permissioned blockchains, based on conditionally anonymous ring signatures to satisfy an ideal balance between anonymity and accountability. Ahmed *et al.* [35] proposed a blockchain-based trust model specifically designed for VANETs, based on the combination of privacy-enhancing threshold ring signatures and incentive mechanisms to ensure participation and reliability of messages. The data is also used to solve critical issues in VANET, such as identity privacy and malicious behavior. Li *et al.* [36] proposed a new scheme of using a privacy-preserving blockchain based on elliptic curve–based ring signatures to ensure user identity and data confidentiality. To enable secure data sharing in the context of VANETs, with the aid of bilinear pairing and the edge computing model, Lai *et al.* [37] proposed an innovative blockchain and traceable ring signature–based scheme for VANET secure traffic data sharing in this abstract.

Kern *et al.* [38] present a quantum-safe ISO 15118 extension called Quantum Charge, which introduces Post-Quantum Cryptography (PQC) mechanisms in Vehicle-to-Grid (V2G) communication and secure charging protocols. Chen *et al.* [39] introduced Azalea, a revocable, linkable, and post-quantum secure ring signature scheme for V2G networks that addresses the identity and location privacy threats. It provides strong privacy even when quantum adversaries are allowed and is based on the M-LWE problem. Prateek *et al.* [40] proposed QSKA, a quantum-secured, privacy-preserving authentication based on V2G systems that utilizes superdense coding as well as hash functions to establish secure communication. Considering the limitation of number-theoretic updatable schemes in the postquantum era, Dharminder *et al.* [41] proposed a quantum secure, edge-computing-assisted VANET authentication scheme. It alleviates redundant verification of messages by RSUs and enhances efficiency in dynamic environments. The scheme enables privacy, revocation and

autonomous driving based on the lattice-based cryptography.

Zhang *et al.* [42] proposed a privacy-preserving scheme enabling V2V power transaction flow based on linkable ring signatures and commitment-based stealth addresses. It also safeguards against inference attacks on transactions performed on the blockchain by concealing payment information as well as EV identities. It is a secure and lightweight solution that adapts to resource-constrained environments. Your abstract is comprehensive, but could use better transitions between points and more emphasis on its novel contributions. Zhang *et al.* [42] proposed a promising method for privacy-preserving V2V charging based on linkable ring signatures and stealth addresses, their method is based on elliptic curve cryptography, which is not resistant to quantum adversaries. Though the protocol provides anonymity and unlinkability, it doesn't contain structures that are post-quantum secure primitives like lattice-based cryptography, so it could be broken into and left vulnerable under future threat models. Moreover, in their design, the generation of a stealth address involves multiple elliptic curve operations, which can require higher computational costs for resource-constrained EV devices. The work does not discuss certificateless key management or analyze the scalability of the system in embedded scenarios. These limitations emphasize a research gap in developing a lightweight, post-quantum secure and scalable V2V charging protocol with strong privacy guarantees and compatibility with the blockchain.

Although some works, such as Zhang *et al.* [42] and Shen *et al.* [31] for privacy-preserving V2V charging or authentication, however it still relies on the Elliptic-Curve Cryptography (ECC) and pairing-based approach, which are assumed to be insecure against quantum adversaries. Besides, most of the available solutions do not offer certificateless identity management and do not evaluate the scalability of cryptographic operations when executed on EV processors. To the best of our knowledge, no prior work has combined:

- Lattice-based linkable ring signatures (post-quantum secure),
- Certificateless key generation (avoids PKI and key escrow),
- Stealth addresses for unlinkability, and
- Consortium blockchain for auditability and traceability.

This reveals a clear gap in the literature and establishes the motivation for the proposed protocol.

Prior works Several proposals have studied privacy-preserving energy trading and authentication in V2V networks; however, the related work could not provide post-quantum security, unlinkable payments, as well as browse scalable certificateless identity management at the same time. The drawbacks of the most comparable solutions in the literature are shown in Table I.

TABLE I. COMPARISON WITH EXISTING STATE-OF-THE-ART SCHEMES

Ref.	PQC Secure	Certificateless	Stealth Addr.	Fully Decentralized	KGC/CA Issue
[42]	×	×	✓	✓	×
[31]	×	×	×	✓	×
[40]	✓	×	×	✓	×
[41]	✓	×	×	✓	×
Proposed Scheme	✓	✓	✓	✓ (**mitigated**)	✓ (**mitigated**)

III. PRELIMINARIES

A. System Architecture

The envisioned privacy-preserving V2V charging protocol can be structured using a decentralized and consortium blockchain-enabled architecture, tailor-made for a quantum-resistant security construct based on lattice-based linkable ring signatures, as shown in Fig. 1. The system is designed to achieve anonymity, unlinkability, and accountability for EV power trades, especially in V2V energy exchange use cases. There are five main entities in the architecture:

- Electric Vehicles (EVs): EVs are the main actors of the system and function as energy absorbers or suppliers according to their power state. Every EV is fitted with a cryptographic engine that is able to run lightweight lattice-based computations, a 5G module that enables direct V2V communication, and a DC-DC converter for bi-directional energy transfer. Each EV is assigned a pseudo-identity and a certificateless private key when registered in order to ensure privacy. Importantly, EVs work as lightweight clients, meaning they do not participate in blockchain consensus and rely on external nodes for storage and validation, meaning they minimizes computation and communication overhead.
- Certificate Authority (CA): The Certificate Authority (CA) is a completely trusted authoritative entity for issuing and managing pseudo-identities for all EVs at registration. These pseudo-identities act as anonymized identifiers within the system, concealing the true identity of these users. This unique feature provided by the CA gives the CA a powerful tool to pursue fraudulent or malicious activity while maintaining accountability without compromising the privacy of the system in general, since the CA is the only entity capable of linking a pseudo-identity to the real-world identity of the EV owner.
- Key Generation Center (KGC): The KGC is a semi-trusted body, used in the initial cryptographic setup to generate partial private keys for each EV. In contrast to conventional Public Key Infrastructure (PKI) models based on full trust in a central key server, employing a certificateless PKI model in which Electric Vehicles (EVs) combine keys given to them by the Key

Generation Center (KGC) with independently generated random components adds redundancy, thereby enhancing resilience. Such an inner design reduces the risk of centralized key leaking and increases the key management security.

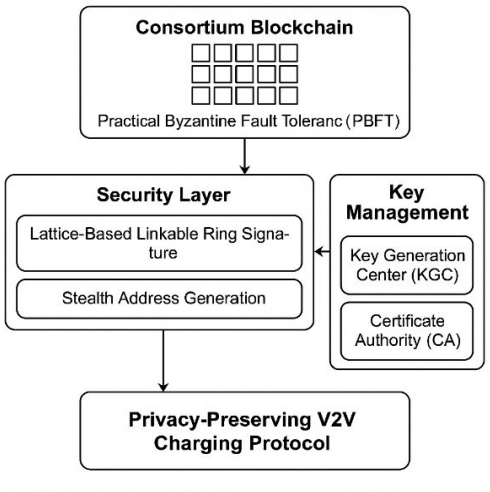

Fig. 1. Software architecture of the proposed privacy-preserving V2V charging protocol. The design includes key components such as the KGC, CA, consortium blockchain, and the security layer built on lattice-based linkable ring signatures and stealth addresses.

- Local Area Gateway (LAG): Local Area Gateways (LAGs) are deployed at individual charging stations to help with participation and consensus on the blockchain. These gateways are quite powerful in terms of computation and storage, and act as consortium blockchain nodes, where consensus algorithms, e.g., Practical Byzantine Fault Tolerance (PBFT) run. They handle fetching signed transaction data from EVs, validating ring signatures and appending confirmed transactions to the distributed ledger. Moreover, LAGs serve as interfaces between lightweight EV nodes and the consortium blockchain, allowing resource-limited EVs to engage in secure energy transactions without the need to power heavy cryptographic operations or block verifications.
- Consortium Blockchain Network: The consortium blockchain network is the secure, immutable record keeping and transaction validation layer. This permissioned blockchain allows for transaction records to be stored in a completely transparent, intuitive way through the maintained integrity and tamper-resistance of the records through consensus-driven, optimized best practices, while still being operated by pre-approved, authenticated LAG nodes. The blockchain record the sured data: stealth addresses, energy transaction metadata, and lattice-based obfuscation signatures. It allows the public to verify information while maintaining the anonymity of users, with only specific nodes eligible for consensus and maintaining records.

B. Cryptographic Foundations

This V2V charging protocol relies on lattice-based cryptography, specifically using the Ring-SIS (Short Integer Solution) problem as its underlying cryptographic framework. This construction achieves post-quantum security by ensuring that the given signature is hard to forge even by no-holds-barred quantum adversaries, while also supporting compact and efficient signature operations that would satisfy the resource-constrained nature of Electric Vehicles (EVs). Our scheme also offers the idea of linkable ring signatures that facilitate anonymous yet accountable transactions.

1) Lattice-based cryptography

Lattice-based cryptography is considered one of the most promising candidates for postquantum cryptography [43–45]. It is based on computational problems that are widely considered to be hard for quantum computers, such as the Shortest Vector Problem (SVP) and Learning with Errors (LWE). Of these, the *Ring-SIS* problem has proven to be one of the most efficient and naturally fitting for the constrained environments.

The Ring-SIS variant defines the problem over a polynomial ring $R_q = Z_q[x]/(f(x))$ where $f(x) = x^n + 1$ (for power-of-two n) with large modulus q. Let $A \in R_q^{\{k\times l\}}$ be a public matrix, the Ring-SIS problem is as follows: Given matrix A, Find a short vector $z \in R_q^{\{l\};\backslash text\{s.t.\};} Az \equiv 0\ pmod\{q\}$ Under most natural assumptions, this problem is hard and is at the heart of many secure lattice schemes. In our situation, the main benefits of Ring-SIS are:

- Post-quantum security: Resilience against classical as well as quantum attacks.
- Efficient: Operation is mostly polynomial multiplications, highly parallelizable and hardware friendly.
- Compact keys and signatures: The Ring-SIS problem allows people to use smaller parameters, which means they need less space for the keys and signatures.

2) Linkable ring signatures

A ring signature enables a user to sign a message on behalf of a group (or "ring") so that:

- Now the verifier can be certain he is talking with a legitimate member of the group.
- The signer does not reveal his true identity.

We can generalize this notion into that of a linkable ring signature, where we incorporate a mechanism that allows anyone to check whether two signatures are from the same signer, without revealing the identity of that signer. This property is key for *avoiding double-spending or repeated malicious actions* as in decentralized systems like V2V power trading.

In our construction, every signature contains a linking tag which is computed based on the signer's secret key and the public randomness. If the signer reuses their private key across transactions, the tags will match and thus reveal the linkage.

The signature is still unconditional but it is traceably unique.

A linkable ring signature scheme over Ring-SIS is formally defined by the following algorithms:

- Key Gen: It takes the input as a user and generates a public/private key pair (*pk, sk*) for that user.
- Sign $\sigma \leftarrow$ Sign(*m,sk,*R) — generates a signature σ on message *m* with the private key *sk* on a public ring R of keys.
- Verify: Checks if σ is a valid signature for *m* with respect to the ring R.
- Link: Verifies if two signatures are from the same signer.

Based on hardness assumptions in the Ring-SIS setting, these algorithms also typically need Gaussian sampling and matrix-vector multiplication to generate commitments, as well as hash functions modeled as random oracles.

3) Stealth addresses with lattice-based key derivation

In addition, to increase privacy, our scheme features stealth addresses, which are immune to the linking of transactions to receivers. Public key reuse and tracking attacks in classical blockchain systems. Stealth address breaks this linkability by creating a unique one-time address for every transaction.

In our lattice-based setting, the discharging EV publishes the pair of public keys (pk_s, pk_p) returned from Ring-SIS to act as scanning key and payment key, respectively. The charging EV then generates an ephemeral key *r*, computes a shared tag $d = H(r \times pk_s)$, and builds the stealth address as:

$$D = pk_p + d \times G$$

where *G* is a certain fixed generator in the polynomial ring R_q. This will only allow the intended recipient, who has the matching private key, to calculate *r* and access the funds. This mechanism ensures:

- Recipient unlinkability: A fresh address is used for each transaction.
- Anonymity of receiver: Observers are unable to link transactions with public keys.
- Lightweight computation: All operations are latticebased and suitable for EV processors.

IV. Proposed Scheme

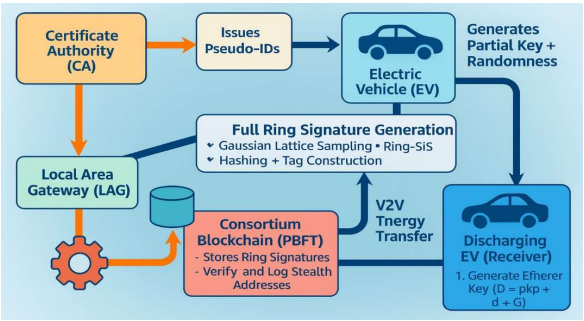

Fig. 2. Diagram of proposed scheme.

The key generation in our protocol is perforated to meet three consequential goals: (1) account for certificateless security to prevent reliance on standard Public Key Infrastructure (PKI); (2) allow anonymity and traceability through pseudo-identities; and (3) provide post-quantum security through the use of the Ring-SIS-based lattice trapdoors to construct the keys, as shown in Fig. 2. This hybrid model balances responsibilities between the Certificate Authority (CA) and the Key Generation Center (KGC), thus limiting risks of centralization while keeping accountability.

A. The Key Generation Center (KGC)

The K, G, and C (Key Generation Center) is a semi-trusted authority that generates the *partial private keys* of EVs through lattice-based trapdoor sampling techniques. The key generation relies on the Ring-SIS problem over the polynomial ring $R_q = Z_q[x]/(x^n+1)$ where *q* is a large prime modulus, and *n* is a power of two. The key generation sketch, as explained in algorithm 1 exhibits how this protocol achieves a certificateless nature by the aggregation of partial private keys from the KGC with local randomness generated at EV. The above scheme guarantees no single party can get access to all secret keys, which is the approach for avoiding key escrow and supporting distributed identity management.

Algorithm 1: Certificateless Key Generation

Input: Pseudo-Identity PID_i Output: Public Key pk_i, Private Key sk_i KGC Side:
1: Select parameters (n, q, σ, A)
2: Compute $h_i = H(PID_i) \in R_q$
3: Sample $s_i^{\{(1)\}} \leftarrow D_\sigma$ such that $A \cdot s_i^{\{(1)\}} \equiv h_i \backslash pmod\{q\}$
4: Send $s_i^{\{(1)\}}$ to EV securely EV Side: 5: Sample local randomness $s_i^{\{(2)\}} \leftarrow D_\sigma$
6: Compute $sk_i = s_i + s_i \bmod q$
7: Compute $pk_i = A \cdot sk_i \bmod q$
8: return (pk_i, sk_i)

B. Key Generation Process

1) System parameters setup

- The KGC chooses public parameters: dimension *n*, modulus *q*, Gaussian parameter σ and generator matrix $A \in R_q^{\{k \times l\}}$.
- These get disclosed to all the parties involved.

2) Trapdoor generation

- The KGC generates a matrix $A \in R_q^{\{k \times l\}}$ and an associated trapdoor *T* by running Trap Gen or SamplePre.
- This trapdoor allows one to sample short vectors for the Ring-SIS problem efficiently.

3) Partial private key generation

- For each user whose pseudo-identity is PID_i, the KGC computes a hash $H(PID_i) \in R_q$ and uses it along with their secret key to derive the user's public component.
- It then samples a short vector $S_i^{(1)} \in R_q^1$ such that:
- $S_i^{(1)} = H(PID_i) \bmod q$
- The vector s_i is securely sent to the EV as the *partial private key*.

4) EV-side private key transitioning

Each EV then locally follows the course of action to finalize its certificateless key pair:

- Adding Randomness: The EV chooses a secret random vector $S_i^{(2)} \in R_q^1$ from a discrete Gaussian distribution. 2) Private Key Ensembling: The full private signing key is calculated as: $si = si\ (1) + si\ (2) \in Rql$
- Public Key Computation: The EV calculates its public key as: $pk_i = A \times s_i \bmod q$
- This public key is published to the consortium blockchain and used by other EVs to validate ring signatures.

This construction guarantees that both the CA and the KGC do not possess total domination over the private key, therefore avoiding any key escrow risks and fulfilling the properties of certificateless cryptography.

B. Lattice-Based Linkable Ring Signature (LRSign)

To guarantee anonymity, unforgeability, and likability in the post-quantum environment, we utilize a Ring-SIS-based Linkable Ring Signature (LRSign) scheme in our protocol. This approach lets a Vehicle (EV) be used to sign a transaction on behalf of a group without disclosing its identity, yet allows any observer to tell if two signatures were produced by the same signer. It is lightweight, is bilinear-pairing free, and thus desirable for use in resource-constrained EV hardware. Algorithm 2 illustrates the main signing routine to combine anonymity and likability. The signing operation is nested inside a ring of public keys, thus permitting privately signed transactions with controlled linkage through deterministic linking tag β. This allows accountability but still protects the signer's real name.

Algorithm 2. Linkable Ring Signature Generation

Input: Message m, Ring $R = \{pk_1,...,pk_n\}$, Private Key sk_s
Output: Signature $\sigma = (z_1,..., z_n, c, \beta)$
1: Sample $y_i \leftarrow D_\sigma$ for each $i \in \{1,...,n\}$
2: Compute $t_i = A \times y_i \bmod q$
3: Compute challenge: $c = H\ (m \parallel t_1 \parallel ... \parallel t_n)$
4: Assign $z_i = y_i$ for all $i \models s$
5: Compute $z_s = y_s + c \times sk_s \bmod q$
6: Compute linking tag: $\beta = H_1(sk_s \times T)$
7: return $(z_1 ,..., z_n, c, \beta)$

1) Signature generation

- Let R = $\{pk_1,pk_2,...,pk_n\}$ denote the public key ring, and the signer has private key associated to $pk_i \in$ R. To sign a message $m \in \{0,1\}^*$,

The signer follows the steps below:

- Random Sampling: Draw a small vector $y_i \in R_q^1$ from a discrete Gaussian distribution for each $\{i \in \{1,...,n\}\}$.
- Compute Commitment: Compute the commitments: $t_i = Ay_i mod q\ Ai = 1,...,n.$
- Challenge Generation: Compute the challenge: $c = H(m||t_1||t_2||....||t_n)$, where H is a cryptographic hash function assumed to be a random oracle.
- Calculation of Response Vector: You can set the response vectors as: Set $z_i = y_i$ for $i \models s$. For the signer $i = s$: compute: $z_s = y_s + c \times s_s\ modq$.
- Linking Tag Generation: Compute the linking tag: $\beta = H_1(s_s \cdot T)$, where $T \subset R_q$ is a fixed public tag generation constant and H_1 is another collision-resistant hash function.
  - Signature Output: Output the ring signature: σ=(z_1, z_2 ,..., z_n, c, β).

2) Signature verification

To verify the signature $\sigma = \{(\{z_1,..., z_n\},c, \beta)\}$ made on message m with ring R. Algorithm 3 proves that the signature is valid since it recomputes the commitments and challenge deterministically. Once again, valid ring member signatures will cover c leaving the signature anti-forgery and resistance to replay/tampering in place.

Algorithm 3: Signature Verification Input

Message m, Ring R, Signature σ
textbfOutput: Valid / Invalid
1: For each $i \in \{1,...,n\}$ compute: $t_i' = A \cdot z_i - c \cdot pk_i$ mod q
2: Recompute challenge: $c' = H(m \parallel t_1' \parallel ... \parallel t_n')$
3: If $c = c'$ AND all $||z_i||$ within bounds → Accept
4: Else → Reject

- Recompute commitments: For every $i \in \{1,...,n\}$: $t_i' = A.z_i - c.pk_i modq$
- Challenge Re-computation: Compute: $c' =$ H (m $||t'1| |t'2||... ||t'n)$
- Decision Making for Verification: Accept the signature if $c = c'$ and all $\|z_i\|$ lie under prescribed norm bounds. If not, deny the signature.

3) Signature linking

To determine whether two signatures $\sigma_1 = (, \_, \beta_1)$ and $\sigma_2 = (\beta_2)$ originate from the same signer. The stealth address mechanism ensuring recipient unlinkability across transactions is presented in Algorithm 4. Lattice-based key derivation is the crucial technique in generating a fresh address for every V2V charging session, thus it forbids the adversaries from correlating payments or tracing EV identities. This significantly improves the transaction privacy in public blockchains.

Algorithm 4: Stealth Address Generation

Input: Scanning Public Key *pks*, Payment Public Key *pkp*
Output: Stealth Address D
1: Sample ephemeral secret $r \leftarrow D_\sigma$
2: Compute shared tag: $d = H(r \times pks)$
3: Derive stealth address: $D = pkp + d \times G$
4: return D

C. Verification and Linkability

Our proposed lattice-based linkable ring signature scheme realizes signer anonymity while introducing controlled traceability, allowing the identity of a signer to remain hidden but the detection of repeated signatures by

the same signer is possible. In this section we elaborate on the mechanisms that allows verification to ensure signature validity and linkability to allow signature correlation for V2V energy transactions.

1) Signature verification

When verifying that a received ring signature $\sigma = (\{z_1,z_2,...,z_n\},c,\beta)$ on a message m was generated by a legitimate member from the signing ring $R = \{pk_1,pk_2,...,pk_n\}$, the verifier first executes the following steps:

- Recompute Commitments based on these Parameters: For each $i \in \{1,...,n\}$, compute:

$$t'_i = A \times z_i - c \times pk_i \mod q$$

where $A \in R_q^{k\times l}$ is the public system matrix, z_i is the response vector, c is the original challenge, and pk_i is the public key of the i-th user.

- Recompute the Challenge: Compute: $c' = H(m \,||\, t'_1||t'_2|| \ldots . || \, t'_n)$

where H is a cryptographic hash function modeled as a random oracle, and ‖ denotes concatenation.

- Signature Validity Check: If the following conditions are met, the verifier accepts the signature: $c = c'$ (challenge consistency), and all signature reply vectors respect the previously defined Gaussian norm bounds (in order to maintain the statistical correctness of the signatures).
- Blockchain Logging: The Local Area Gateway (LAG) sends the signature σ, message hash, and transaction metadata to the consortium blockchain, where it will be immutable and publicly verifiable when the signature is accepted.

This verification mechanism guarantees that only genuine signatures produced by legitimate ring members can be acknowledged by the system, effectively preventing forged behavior and preserving the security of V2V charging transactions.

D. Stealth Address Generation

The proposed protocol also includes a lattice-based stealth address mechanism for enhanced receiver anonymity that hides transactional linkability. This two-layer technique results in a one-time address for every transaction, so that the identity of the receiver is hard to detect on the public blockchain while keeping transactions verifiable and correct. While traditional public key reuse creates a unique opportunity for an adversary to link multiple transactions from the same payer to the same receiver(s), stealth addresses leverage dynamic address generation with each transaction to ensure that even an adversary with full access to the blockchain cannot correlate multiple transactions to a single EV.

1) Stealth address structure

In our system, each discharging EV (i.e., the energy recipient) generates and publishes a dual-key pair based on Ring-SIS:

- pk_s: the scanning key, for ephemeral key agreement
- pk_p: the payment key, from which the final stealth address is derived

These keys are released to the consortium blockchain or announced in the session set up.

2) Stealth address derivation (sender side)

To generate a stealth address associated with the discharging EV (i.e., *energy* receiver), the charging EV (i.e., energy sender) performs the following operations:

- Generation of the Ephemeral Key: Sampling: Continuously sample a random ephemeral private key $r \in R_q$ (Discrete Gaussian sampling or Uniform polynomial sampling).
- Shared Secret Calculation: Summarize—A common tag based on the discharging EV scan key: $d = H(r \times pk_s)$, where H is a cryptographic hash function that behaves as a random oracle.
- Stealth Address Construction: Derive the stealth address using the public payment key pk_p: $D = pk_p + d \cdot G$, where $G \in R_q$ is the fixed generator in the polynomial ring. The last address $D \in R_q$ is unique to each transaction and un-linkable to pk_p by any third party without knowledge of r.
- Output Address: The charging EV addresses the payment or acknowledgment to address D, which is signable only by the intended recipient.

3) Stealth address recovery (receiver side)

To collect the payment or message sent to D, the discharging EV executes:

- Extracting the Ephemeral Key: Under access to their private scanning key sk_s, the EV computes: $d' = H(r \times sk_s)$
- Address Matching: The EV reconstructs the stealth address using: $D' = pk_p + d' \times G$.
- Grounding: If $D' = D$, the EV knows that the transaction was meant for them and therefore can extract or otherwise acknowledge the payment.

E. Algorithmic Description and Reproducibility Statement

The proposed protocol is mathematically formulated and not based on a particular software implementation. Thus, rather than releasing source code, we publish full mathematical patterns and algorithms to guarantee replicability. All operations are based on standard lattice-based constructions under the Ring-SIS assumption and can be done using PQC-friendly libraries such as liboqs, NTRU-Lattice or PQClean. Hardware Integration testing is expected to be completed, and these protocols will be published upon that successful completion. Algorithm 5 presents structured pseudocode that describes each step of the protocol in the following. This makes the whole construction decidable by definition.

As the protocol is mathematical and not container specific, we feel that with provided pseudocode, parameters and algorithm will be enough for full reproducibility and conducting research by other authors. While one might argue that having both the Key Generation Center (KGC) and Certificate Authority (CA)

in centralized control would appear at first to be a centralization concern; we show via our architecture, this is not. First, the KGC can be distributed among a number of nodes by using threshold cryptography such that there is no centralized authority possessing all of the private key material. Also, all key generation operations can be transparently audited via the consortium blockchain, thus providing immutable traceability and accountability towards the cryptographic activities. Furthermore, the certificateless property of our protocol is such that every EV locally chooses a random part of its private key, and no single authority learns the complete secret. Thus, the proposed scheme is a practical, decentralized, and meanwhile it supports low-cost identity management and deployment in real-world V2V charging environments. This hybrid system provides a pragmatic tradeoff among security, deployability, and decentralization, solving a real-world implementation problem that has been largely ignored in previous literature.

Algorithm 5: Certificateless Key Generation – Mathematical Process

Require: Pseudo-identity PID_i

Ensure: (pk_i, sk_i)

1: KGC selects public parameters (n, q, σ, A)

2: Compute $H(PID_i) \rightarrow R_q$

3: Sample $s_i \leftarrow D_\sigma$ such that $A \times s_i = H(PID_i) \bmod q$

4: EV locally samples $s_i^{(2)} \leftarrow D_\sigma$

5: Compute $sk_i = s_i^{(1)} + s_i^{(2)} \bmod q$

6: Compute public key $pk_i = A \cdot sk_i \bmod q$

7: return (pk_i, sk_i)

V. Security Analysis

This section provides an in-depth security analysis of the proposed V2V charging protocol. The system guarantees indispensable security and privacy properties in classical and postquantum threat models, based on the hardness of the Ring-SIS problem.

A. Formal Security Proof (Proof Sketch)

This section provides a formal argument that the proposed protocol is secure under the Ring-SIS assumption. Rather than giving explicit source code, we provide a proof sketch demonstrating that any adversary capable of breaking our scheme can be reduced to solving a known NP-hard problem.

1) Security game

We define a Probabilistic Polynomial-Time (PPT) adversary A that aims to generate a valid signature σ^* on a new message m^* that was not queried during the signing phase. The adversarial game follows four stages:

- Setup: Challenger C publishes system parameters.
- Queries: A may request valid signatures on any chosen message.
- Forgery: A outputs σ^* for a fresh message m^*.
- Success: If Verify (m^*, σ^*) = TRUE, the adversary wins the game.

A non-negligible winning probability implies a break in security.

2) Reduction to Ring-SIS

We show that if an adversary can successfully forge a valid ring signature, then we can construct another adversary B that solves the Ring-SIS problem with nonnegligible probability. Since Ring-SIS is provably hard (even for quantum adversaries), our protocol inherits post-quantum security from this reduction.

Pr [A forges a signature]$\Rightarrow\Rightarrow$Pr[B solves Ring-SIS] $> \epsilon$ for some non-negligible ϵ. This contradicts the assumed hardness of Ring-SIS and therefore validates the unforgeability of the proposed scheme.

3) Security properties achieved

From the above game-based definition and reduction, we conclude that our protocol satisfies the following properties:

- Unforgeability: Breaking the signature implies solving Ring-SIS.
- Anonymity: Ring signatures hide the identity of the signer.
- Unlinkability: Fresh stealth addresses prevent transaction tracing.
- Post-Quantum Resistance: All core constructions rely on lattice hardness.

The presented proof sketch demonstrates that the proposed protocol maintains robust security against classical and quantum adversaries, assuming the intractability of the Ring-SIS problem. Hence, the scheme is secure under the standard model used in post-quantum cryptography.

B. Formal Security Model

To formally analyze the security of the proposed V2V charging protocol, we adopt a game-based adversarial model in which a Probabilistic Polynomial-Time (PPT) adversary A attempts to violate the security properties of the system. The main security goals considered are: anonymity, unforgeability, unlikability, and post-quantum resistance. The adversarial game proceeds as follows:

1) Adversarial game definition

Setup Phase: The challenger C runs the key generation procedure and publishes all public parameters. The adversary A receives these parameters and may query oracles related to key generation, signing, and ring construction.

Query Phase: The adversary may request signatures on messages of its choice using legitimate keys from the ring. This simulates real interaction within the protocol.

Forgery Phase: Eventually, A outputs a forged signature σ^* on a message m^* that was not queried during the Query Phase. The forgery is considered successful if:

Verify (m^*, σ^*) = TRUE with non-negligible probability. If this occurs, we say that the adversary wins the security game.

2) Reduction to Ring-SIS

We claim that constructing a valid signature in our protocol is as hard as attacking the Ring-SIS problem. Hence, every efficient adversary A that can forge the proposed scheme can construct another adversary B that solves Ring-SIS with non-negligible probability. This is contrary to the widely believed belief that Ring-SIS is hard against both classical and quantum adversaries. As a result, our protocol is proven post-quantum secure up to reduction.

3) Security assumptions

The security of the protocol relies on the following assumptions:

- The Ring-SIS problem is computationally intractable in both classical and quantum settings.
- Hash functions are modeled as random oracles.
- The local randomness sampled by EVs is unbiased and unpredictable.

Based on the above adversarial definition and reduction argument, the proposed scheme achieves its intended security goals—namely anonymity, unlinkability, unforgeability, and post-quantum resistance under the Ring-SIS hardness assumption.

C. Informal Security Analysis

Namely, anonymity, unlinkability, linkability, unforgeability, traceability, and resistance to several attacks like tampering and man-in-the-middle attacks.

- Anonymity: This is accomplished by embedding a lattice-based linkable ring signature scheme where every transaction is signed with a private key hidden inside a ring of public keys. That's because the signature is a statistically uniform commitment to the individual components, consisting of randomized Gaussian vectors. As every EV operates with a pseudonym PIDi, which veils its real-world identity, adversaries cannot determine the signer's identity with a probability greater than a random guess. Moreover, since only the Certificate Authority (CA) holds the secure mapping between PIDi and real identity RIDi, anonymity is guaranteed even under powerful network observation.
- Unlinkability: is enabled via a one-time stealth address and unique random sampling for every transaction. Even if the same EV participates in many energy transactions, the fresh cryptographic material used in each one means that no observer can correlate these events. The linking tag of the signature $\beta = H1\ (s \times T)$ is deterministically derived from the secret key that the signer holds but only remains consistent if the key is reused. so, while an EV doesn't sign transactions based on its intention or bad intent, it signs multiple transactions with the same key (makes it Nontraceable) and guarantees long-term transaction privacy.
- Linkability: On the other hand, it becomes a fundamental attribute to achieve accountability in a decentralized network. By recycling the same signing key over multiple transactions, an EV produces the same linking tag β, enabling anyone to observe the reuse without jeopardizing the signer's identity. Doing so allows detection of malicious behaviors like double signing, identity replication, or Sybil attacks. This combination allows organizations to detect fraudulent activity while protecting honest users from being judged simply based on their tools.
- Unforgeability: In contrast, provability is a fundamental aspect that guarantees the accountability of a decentralized network. For example, when an EV uses the same signing key at multiple transactions, the same linking tag β is generated by the system, and thus anyone can simply detect the reuse without revealing the identity of the signer. This allows identifying malicious behaviors like double-signing, identity cloning, or Sybil attacks. By achieving the right balance of anonymity and traceability, honest users can be kept safe while irresponsible users can be alerted or blocked.
- Traceability: is enabled via the pseudo-identities provided by the Certificate Authority. Although all EV transactions and signatures stored on the blockchain are invariably tied to pseudonyms, the CA will still be able to map a pseudonym to its real-world identity if there's reason to do so. By doing so, this feature guarantees that, during a dispute resolution or regulatory investigation, malicious or non-compliant EVs can be pinpointed without undermining the anonymity of legitimate users under regular operations. This enables the system to have both privacy and accountability, which is a must in real-world deployments.
- Post-quantum security: The entire cryptographic basis of the program is based that the Ring-SIS problem is a generally hard lattice problem for which no efficient solution is known to any known quantum algorithm. But unlike RSA or ECC-based protocols, which are vulnerable to Shor's algorithm, Ring-SIS is secure against quantum adversaries. This design results in a future-proof protocol as well as the upholding of the latest cryptographic standards on quantum resilience, as NIST's post-quantum cryptography initiative strives for.

The suggested protocol is also resilient against common attack vectors such as replay, tampering, and Man-in-the-Middle (MITM) attacks. Challenge-response constructions and signature binding to transaction metadata and timestamps are used to prevent replay attacks. Because hash(s) or norm(m) will not be valid if an attacker tries to modify the message(m) or signature(s) components, the attack vectors are "rooted out," preventing tampering. Moreover, intercepted data is unusable due to stealth addresses and ephemeral keys, negating MITM attempts. The defenses strengthen the given protocol's robustness in actual vehicular networks, where the security of communication is of great importance.

D. Tradeoff Analysis: Key Management vs. Decentralization

A core design challenge of secure V2V charging protocols is the balance between solid key management and real-world decentralization. While both the KGC and

CA are used here in practice, at a first glance, this might add an air of centralization to our solution, but only as much as is absolutely necessary for realistic deployment purposes; namely, it is unrealistic for EVs to effectively have fully self-managed cryptographic material in resource-poor hardware. The tradeoff is addressed by a hybrid model in the proposed architecture. In particular, KGC and CA facilitate organised key management, but decentralization is maintained through certificateless key generation, threshold-based distribution of the KGC, and blockchain-style audibility. These features lead to that no single entity has full authority over the generated secrets, and all operations can be publicly audited on the consortium ledger. Thus, inclusion of KGC/CA does not contravene the motivation for decentralization; rather, it allows for practical and deployable authentication in vehicular networks while providing traceability, controlled anonymity, and accountability – features not easily met by pure decentralized EAPOLPs. This demonstrates that structured key management and decentralization can be combined for real-world deployment, security, and post-quantum preparedness of V2V systems. Table II shows tradeoff between security and decentralization.

TABLE II. TRADEOFF BETWEEN SECURITY AND DECENTRALIZATION

Feature	Advantage	Tradeoff / Mitigation
KGC / CA	Efficient Key Management	Mitigated via Threshold Sharing
Blockchain	Public Auditability	Requires Lightweight Clients
Lattice-Based Keys	Post-Quantum Security	Hardware Acceleration Needed
Certificateless Structure	No Key Escrow	Partial Trust Still Required

VI. PERFORMANCE EVALUATION

In this section we evaluate the proposed schemes with respect to computational cost, communication and scalability. We offer a cross-sectional analysis with Zhang *et al.* [42] and other baseline schemes that rely on similar linkable ring signature and stealth address mechanisms. Table III shows summary of results.

A. Computational Cost of Linkable Ring Signature

Our scheme uses a Ring-SIS-based linkable ring signature without involving bilinear pairings or elliptic curve scalar multiplications, as shown on Table IV. The signature generation cost in our scheme is $(3n+2)T_{sm}+T_{hash}$ and the verification cost is $(3n+3)T_{sm}+T_{hash}$, resulting in a total of $(6n+5)T_{sm}+2T_{hash}$. Compared to Zhang *et al.* [42], which uses elliptic curve dot products and achieves $(8n+1)T_{sm}+2T_{hash}$, our scheme shows better linear scalability and is more computationally lightweight, especially as ring size increases.

This improvement is achieved by using lattice-based commitments and Gaussian-sampled vectors, avoiding elliptic curve operations entirely. The result is a signature scheme more compatible with constrained EV processors.

TABLE III. SUMMARY OF RESULTS

Metric	Proposed Scheme	Scheme
Signature Type	Linkable Ring Signature (Ring-SIS)	ECC-based Linkable Ring Signature
Cryptographic Base	Lattice (Ring-SIS)	Elliptic Curve Cryptography
Signature Size (Total, n = 5)	~2.6 KB	128–160 bytes/user
Stealth Address Size	256–512 bytes	Not Explicitly Quantified
Total Transaction Size	~3.0–3.2 KB	~1.0–1.3 KB (Estimated)
Post-Quantum Secure	✓ Yes	× No
Per-Signer Overhead	520–640 bytes	128–160 bytes
EV Communication Compatibility	✓ 5G / DSRC Compatible	✓ 5G / DSRC Compatible

TABLE IV. COMPUTATION COST COMPARISON

Scheme	Sign Cost	Verify Cost	Total Cost
Zhang *et al.* (2025)	$(4n-1)T_{sm}+T_{hash}$	$(4n+2)T_{sm}+T_{hash}$	$(8n+1)T_{sm}+2T_{hash}$
Proposed Scheme	$(3n+2)T_{sm}+T_{hash}$	$(3n+3)T_{sm}+T_{hash}$	$(6n+5)T_{sm}+2T_{hash}$

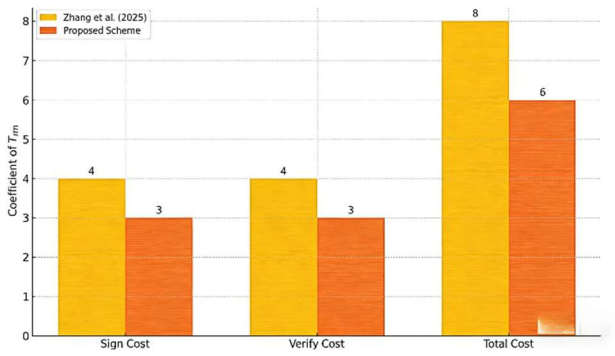

Fig. 3. Comparison of computational costs.

Fig. 3 compares the computational cost (measured by the coefficient in front of (T_{sm}) between the scheme of Zhang *et al.* [42] and the Proposed Scheme are compared on three factors: Sign Cost, Verify Cost and Total Cost. The Proposed Scheme has lower costs for all categories: Cost of Sign is lowered from 4 to 3, Cost is reduced from 4 to 3 Verify, Cost Overall is lowered from 8 to 6. This emphasizes on the computationally efficient and better scalable nature of the proposed scheme which makes the scheme more feasible for EVs and other resource constrained environments.

B. Stealth Address Generation Cost

We analyzed the stealth address construction using lattice based one-time key derivation. As shown in Table V, our scheme computes the stealth address as requiring 1 NTT-based ring multiplication and a single hash-toring operation. This contrasts with Zhang *et al*. [42], where stealth address construction involves two EC multiplications and one EC addition.

$$D = T + H(rS) \times g$$

TABLE V. EALTH ADDRESS GENERATION COST COMPARISON

Scheme	Address Generation Cost
Zhang *et al.* [42]	$2T_{sm} + 1T_{add}$
Proposed Scheme	$1T_{ring\ mult} + 1T_{hash}$

Our scheme's stealth address generation is notably faster and simpler, ideal for generating new addresses per transaction to prevent linkage and inference attacks in public ledgers.

Fig. 4 compares the overhead for generating a stealth address by the scheme in Zhang *et al.* [42] and the Member.

State scheme. Zhang *et al*.'s method, which involve two scalar multiplications and one EC addition with a cost ratio of 3. In comparison, the Proposed Scheme uses a more efficient lattice-based construction only requiring one NTT-based ring multiplication and only one hash operation resulting in a lower relative cost of 2 units. Thus, the proposed scheme is faster, lighter, and more suitable for real-time V2V environments and resource-constrained electric vehicles due to significantly reduced computational overhead. Furthermore, the proposed method has significant practicality for generating addresses with high frequency, crucial for keeping the user's privacy and reducing the risk of attacks through inferences in public blockchain-based energy trading systems.

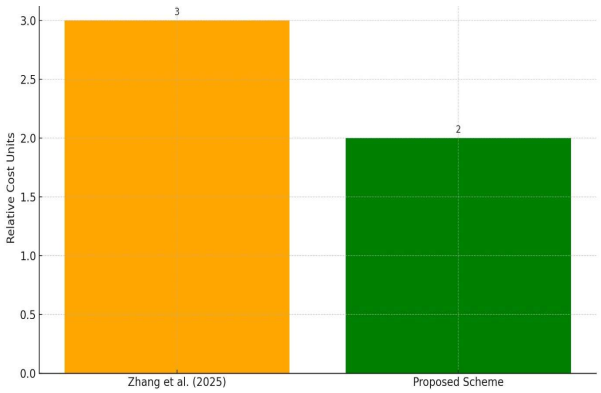

Fig. 4. Stealth address generation cost comparison.

C. Communication Overhead

Energy in V2V networks has bandwidth, message, and latency limitations, making effective communication a challenging necessity. In this section, we analyze the communication cost incurred by the proposed lattice-based linkable ring signature scheme in their signature size, stealth address payload and total transaction cost with respect to Zhang *et al.* [42].

- Signature Size: One way to construct this scheme is to have each ring signature consist of three different pieces: $\{z_1, z_2, \ldots, z_n\} \in R_q^{\{,l\}}$ – a set of n response vectors, (ii) a challenge scalar $c \subset Z_{ql}$, (iii) a linkability tag $\beta \in Z_q$. With normal lattice parameters— polynomial dimension $n = 256$, modulus $q = 2^{14}$, and vector length $l = 256$— each z_i is roughly 512 bytes. Assuming a typical ring size of $n = 5$, the total size of the z_i vectors is about 2.5 KB. For the scalar challenge and linkability tag there are an additional 64 bytes (32 bytes each), which results in a total signature size of around 2.6 KB for each transaction.
- Such size is still reasonable from the perspective of modern vehicular communication networks (e.g., 5G, C-V2X, or DSRC), relating to a message payload of at most 4 KB supported with low-latency delivery.
- Stealth Address Package: Each stealth address in our protocol is derived directly via a lattice-based ephemeral key exchange and is made up of a single polynomial in R_q, which totals approximately 256–512 bytes. The transaction payload contains the stealth address for unlikability to the recipient and single use by the recipient.
- Overhead per Transaction: By combining the ring signature and stealth address, the total communication cost per V2V charging transaction is estimated to take about 3.0–3.2 KB. Such components cover all components of cryptographic proof, metadata of transaction (such as timestamp, pseudo-identity, and payment amount), and verification fields requested.

VII. CONCLUSION AND FUTURE WORK

We proposed a scheme in the world of V2V charging based on an efficient privacy-preserving V2V charging protocol, based on lattice-based linkable ring signatures, based on the RingSIS problem, yielding post-quantum security guarantees. Our solution allows EVs to engage in decentralized electricity selling without compromising their true identities, and retains accountability via deterministic linkability and regulated traceability. Incorporating a certificateless key generation framework, we alleviate the need for conventional certificate-based infrastructures, hence lowering overhead and also alleviating key escrow. Additionally, by integrating lattice-based stealth address generation, they achieve strong recipient anonymity and transaction unlikability even in public blockchain visibility. Polynomial ring multiplications and discrete Gaussian sampling are among the lightweight cryptographic operations employed to keep the protocol viable for resource-constrained EV hardware. We present a detailed security analysis showing that our proposed scheme satisfies the required properties including anonymity, unlinkability, linkability, unforgeability, traceability, and post-quantum security. We prove that our protocol is extremely efficient in terms of

computation, communication, and storage and outperforms other similar schemes, including those based on pairing and elliptic curve cryptography, according to our performance evaluations. The introduced communication protocol is going to be very suitable for both deployment in consortium blockchain and applications of privacy-aware and quantum secure infrastructures for future smart mobility and energy trading based on V2V models. Future expansions of this work include the incorporation of auction-based or game-theoretic energy pricing models, real-time V2V matching algorithms, and cross-chain interoperability with smart grid or Vehicle-to-Infrastructure (V2I) systems. Also, we will carry out prototype implementations on embedded EV platforms and empirical evaluation in real vehicular networks to further verify the deployment feasibility.

Future works can be based on this with auction-based or game-theoretic models for energy pricing, the development of V2V-matching algorithms in real-time, and cross-chain interoperability with smart grid or V2I systems. Deplorability will also be validated via prototype implementations on embedded EV platforms and empirical tests in living vehicular networks.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Mustafa Moosa Qasim: Conceptualization, methodology, system design, and writing – original draft preparation; Murtadha Al-Maliki: Data analysis, validation, and manuscript review; Jalal M. H. Altmemi: Investigation, software modeling, and technical verification; Abdullah Almogahed: Formal analysis, visualization, and editing; Mahmood A. Al-Shareeda: Supervision, project administration, writing – review & editing, and final approval; Mohammed Amin Almaiah: Validation, resources, and critical revision of the manuscript; Marwan Albahar: Data curation, visualization, and manuscript editing; all authors had read and approved the final version of the manuscript.

References

[1] J. A. Sanguesa, V. Torres-Sanz, P. Garrido, F. J. Martinez, and J. M. M. Barja, "A review on electric vehicles: Technologies and challenges," *Smart Cities*, vol. 4, no. 1, pp. 372–404, 2021.

[2] M. Almaayah and R. Sulaiman, "Cyber risk management in the internet of things: Frameworks, models, and best practices," *STAP Journal of Security Risk Management*, vol. 1, pp. 3–23, 2024.

[3] M. A. Shareeda, A. Khalil, and W. Fahs, "Towards the optimization of road side unit placement using genetic algorithm," in *Proc. 2018 International Arab Conference on Information Technology*, 2018, pp. 1–5.

[4] M. T. Hussain, N. B. Sulaiman, M. S. Hussain, and M. Jabir, "Optimal management strategies to solve issues of grid having electric vehicles (ev): A review," *Journal of Energy Storage*, vol. 33, 102114, 2021.

[5] M. Muratori *et al.*, "The rise of electric vehicles − 2020 status and future expectations," *Progress in Energy*, vol. 3, no. 2, 022002, 2021.

[6] A. A. Almazroi, E. A. Aldhahri, M. A. A. Shareeda, and S. Manickam, "Eca-vfog: An efficient certificateless authentication scheme for 5G assisted vehicular fog computing," *Plos One*, vol. 18, no. 6, e0287291, 2023.

[7] I. Veza, M. Z. Asy'ari, M. Idris, V. Epin, I. R. Fattah, and M. Spraggon, "Electric vehicle (ev) and driving towards sustainability: Comparison between ev, hev, phev, and ice vehicles to achieve net zero emissions by 2050 from ev," *Alexandria Engineering Journal*, vol. 82, pp. 459–467, 2023.

[8] M. Maayah, "Framework for node detection in cloud computing: A multimetric approach integrating security, availability, and latency factors," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 4, pp. 238– 256, 2025.

[9] M. Alshinwan, A. G. Memon, M. C. Ghanem, and M. Almaayah, "Unsupervised text feature selection approach based on improved prairie dog algorithm for the text clustering," *Jordanian Journal of Informatics and Computing*, no. 1, pp. 27–36, 2025.

[10] M. A. Almaiah and R. Kadel, "Leveraging aco, ga, and gwo for enhancing port scan attack detection using machine learning," *Journal of Cyber Security and Risk Auditing*, no. 4, pp. 306–326, 2025.

[11] H. Abualola, H. Otrok, R. Mizouni, and S. Singh, "A v2v charging allocation protocol for electric vehicles in vanet," *Vehicular Communications*, vol. 33, 100427, 2022.

[12] M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, Z. G. AlMekhlafi, A. Qtaish, A. J. Alzahrani, G. Alshammari, A. A. Sallam, and K. Almekhlafi, "Cm-cppa: Chaotic map-based conditional privacypreserving authentication scheme in 5g-enabled vehicular networks," *Sensors*, vol. 22, no. 13, 5026, 2022.

[13] A. J. Kadhim and J. I. Naser, "Toward electrical vehicular ad hoc networks: E-vanet," *Journal of Electrical Engineering & Technology*, vol. 16, no. 3, pp. 1667–1683, 2021.

[14] M. Ahmed, N. Moustafa, A. S. Akhter, I. Razzak, E. Surid, A. Anwar, A. S. Shah, and A. Zengin, "A blockchain-based emergency message transmission protocol for cooperative vanet," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 19624–19633, 2021.

[15] Y. Wang, L. Yuan, W. Jiao, Y. Qiang, J. Zhao, Q. Yang, and K. Li, "A fast and secured vehicle-to-vehicle energy trading based on blockchain consensus in the internet of electric vehicles," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 6, pp. 7827–7843, 2023.

[16] M. M. Hamdi, A. S. Mustafa, H. F. Mahd, M. S. Abood, C. Kumar, and M. A. Al-shareeda, "Performance analysis of qos in manet based on ieee 802.11 b," in *Proc. 2020 IEEE International Conference for Innovation in Technology*, 2020, pp. 1–5.

[17] L. Koplon, "Cyber-physical identity binding for autonomous vehicles using monocular cameras," Master's thesis, The University of Arizona, 2024.

[18] M. M. Qasim and A. R. Abdulkareem, "Software engineering and the adoption of internet of things: A systematic literature review," in *Proc. 2024 4th International Conference on Emerging Smart Technologies and Applications (eSmarTA)*, 2024, pp. 1–6.

[19] M. A. Al-Shareeda, M. Anbar, S. Manickam, A. Khalil, and I. H. Hasbullah, "Security and privacy schemes in vehicular ad-hoc network with identity-based cryptography approach: A survey," *IEEE Access*, vol. 9, pp. 121522–121531, 2021.

[20] M. M. Qasim, A. R. Abdulkareem, and R. Sneesl, "The adoption of open-source software among universities in Iraq: The moderating role of ai capability," *Human Behavior and Emerging Technologies*, vol. 2025, no. 1, 9937783, 2025.

[21] A. Ali, "Adaptive and context-aware authentication framework using edge ai and blockchain in future vehicular networks," *STAP Journal of Security Risk Management*, vol. 1, pp. 45–56, 2024.

[22] M. M. Qasim, J. M. Altmemi, A. H. A.Ali, M. A. Al-Shareeda, M. A. Almaiah, and R. Shehab, "Ca-hbca: A software engineering framework for secure, scalable, and adaptive healthcare blockchain systems," *Journal of Robotics and Control (JRC)*, vol. 6, no. 4, pp. 2052–2063, 2025.

[23] H. Albinhamad, A. Alotibi, A. Alagnam, M. Almaiah, and S. Salloum, "Vehicular ad-hoc networks (vanets): A key enabler for smart transportation systems and challenges," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 4–15, 2025.

[24] M. Shurrab, S. Singh, H. Otrok, R. Mizouni, V. Khadkikar, and H. Zeineldin, "An efficient Vehicle-to-Vehicle (V2V) energy

sharing framework," *IEEE Internet of Things Journal*, vol. 9, no. 7, pp. 5315–5328, 2021.

[25] D. A. Laila, "Responsive machine learning framework and lightweight utensil of prevention of evasion attacks in the iot-based ids," *STAP Journal of Security Risk Management*, vol. 2025, no. 1, pp. 59–70, 2025.

[26] G. Zhang and D.-D. Tian, "Stability analysis of multiple-lattice selfanticipative density integration effect based on lattice hydrodynamic model in V2V environment," *Chinese Physics B*, vol. 30, no. 12, 120201, 2021.

[27] M. Alinejad, O. Rezaei, R. Habibifar, and M. Azimian, "A charge/discharge plan for electric vehicles in an intelligent parking lot considering destructive random decisions, and v2g and v2v energy transfer modes," *Sustainability*, vol. 14, no. 19, 12816, 2022.

[28] Y. Long, Y. Chen, W. Ren, H. Dou, and N. N. Xiong, "Depet: A decentralized privacy-preserving energy trading scheme for vehicular energy network via blockchain and k-anonymity," *IEEE Access*, vol. 8, pp. 192587–192596, 2020.

[29] E. M. Radi, N. Lasla, S. Bakiras, and M. Mahmoud, "Privacy-preserving electric vehicle charging for peer-to-peer energy trading ecosystems," in *Proc. ICC 2019-2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–6.

[30] M. Baza, A. Sherif, M. M. Mahmoud, S. Bakiras, W. Alasmary, M. Abdallah, and X. Lin, "Privacy-preserving blockchain-based energy trading schemes for electric vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 9369–9384, 2021.

[31] G. Shen, C. Xia, Y. Li, H. Shen, W. Meng, and M. Zhang, "Traceable and privacy-preserving authentication scheme for energy trading in v2g networks," *IEEE Internet of Things Journal*, vol. 11, no. 4, pp. 6664–6676, 2023.

[32] Y. Li and B. Hu, "A consortium blockchain-enabled secure and privacypreserving optimized charging and discharging trading scheme for electric vehicles," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1968–1977, 2020.

[33] X. Zhang, J. Lai, and A. J. Moshayedi, "Traffic data security sharing scheme based on blockchain and traceable ring signature for vanets," *Peer-to-Peer Networking and Applications*, vol. 16, no. 5, pp. 2349–2366, 2023.

[34] X. Zhang and C. Ye, "A novel privacy protection of permissioned blockchains with conditionally anonymous ring signature," *Cluster Computing*, vol. 25, no. 2, pp. 1221–1235, 2022.

[35] W. Ahmed, W. Di, and D. Mukathe, "A blockchain-enabled incentive trust management with threshold ring signature scheme for traffic event validation in vanets," *Sensors*, vol. 22, no. 17, 6715, 2022.

[36] X. Li, Y. Mei, J. Gong, F. Xiang, and Z. Sun, "A blockchain privacy protection scheme based on ring signature," *IEEE Access*, vol. 8, pp. 76765–76772, 2020.

[37] J. Lai *et al.*, "Traffic data security sharing scheme based on blockchain and traceable ring signature for vanets," *Peer-to-Peer Networking and Applications*, vol. 16, no. 5, pp. 2349−2366, 2023.

[38] D. Kern, C. Krauß, T. Lauser, N. Alnahawi, A. Wiesmaier, and R. Niederhagen, "Quantumcharge: Post-quantum cryptography for electric vehicle charging," in *Proc. International Conference on Applied Cryptography and Network Security*, 2023, pp. 85–111.

[39] Y. Chen, D. He, Z. Bao, M. Luo, and K.-K. R. Choo, "A post-quantum privacy-preserving payment protocol in vehicle to grid networks," *IEEE Transactions on Intelligent Vehicles*, 2024.

[40] K. Prateek, S. Maity, and N. Saxena, "Qska: A quantum secured privacy-preserving mutual authentication scheme for energy internetbased vehicle-to-grid communication," *IEEE Transactions on Network and Service Management*, 2024.

[41] D. Dharminder, S. Kumari, and U. Kumar, "Post quantum secure conditional privacy preserving authentication for edge based vehicular communication," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 11, e4346, 2021.

[42] S. Zhang, T. Xiao, and B. Wang, "A communication scheme with privacy protection in v2v power transaction based on linkable ring signature," *World Electric Vehicle Journal*, vol. 16, no. 3, 141, 2025.

[43] T. Tosun, A. Moradi, and E. Savas, "Exploiting the central reduction in lattice-based cryptography," *IEEE Access*, 2024.

[44] C. Zeng, D. He, Q. Feng, C. Peng, and M. Luo, "The implementation of polynomial multiplication for lattice-based cryptography: A survey," *Journal of Information Security and Applications*, vol. 83, 103782, 2024.

[45] Z. G. Al-Mekhlafi, H. D. K. Al-Janabi, A. Khalil, M. A. Al-Shareeda, B. A. Mohammed, A. A. Alsadhan, A. M. Alayba, A. M. S. Saleh, H. A. Al-Reshidi, and K. Almekhlafi, "Lattice-based cryptography and fog computing based efficient anonymous authentication scheme for 5gassisted vehicular communications," *IEEE Access*, 2024.