Post-Quantum-Secure Electric Vehicle Charging

Atakan Arda Celik
University of Passau
Seminar: Hardware Security Solutions for the Internet of Things
Passau, Germany
celikatakanarda@gmail.com

***Abstract*—The new developments in quantum computing make it easier for sophisticated threats to exploit the cryptographic systems that support modern electric vehicle charging systems and as a result they compromise the security and privacy of such hardwares. As a counter to such sophisticated strategies, there has been a surge in interest to integrate quantum-resistant strategies into the algorithms used for EV charging. The paper investigates the state of the art implementations related to PQC in the context of EV charging networks and presents several new ideas, including QuantumCharge and DynamiQS. QuantumCharge aims to add PQC features to the existing crypto-suite defined by the ISO 15118 by adopting the concepts of crypto-agility, migration plan and strong security guarantees. Furthermore, DynamiQS has developed a post-quantum secure authentication schema for dynamic wireless charging systems that are capable of being resistant to quantum powered threats and protect user privacy. The study concludes with extensive formal analysis and prototype implementations this work shows how post quantum cryptography can be used to ensures security of the EV charging system in the age of quantum computing.**

***Index Terms*—Post-Quantum Cryptography, Cybersecurity Electric Vehicle Charging, Dynamic Wireless Charging, QuantumCharge, DynamiQS, ISO 15118, Authentication Protocols, Security Migration Strategies, Crypto-Agility.**

I. Introduction

Global Shift towards Electric Vehicles is on the rise due to environmental and Technological reasons. But as charging platforms get integrated and dependent on communication networks, it is vulnerable to cybercrimes. We are faced with quantum computing that is not easily addressed and can in effect threaten classical cipher techniques. This paper centers its work on incorporating PQC into the EV charging system to plan for security after a few years. [2]

Key contributions include:

- A survey and analysis of current literature on EV charging security protocols.
- Identification of the most appropriate PQC algorithms for implementation in EV charging application.
- The proposed architecture is an integrated architecture that relies on PQC.
- Problem Solving and details of impacts made on PQC adoption.

II. Background

A. Electric Vehicle Charging Infrastructure

Current charging infrastructure is based on standards like ISO 15118 for the full implementation of charging features within the PnC domain. These systems use cryptographic credentials for authentication and billing, which need long-life security.

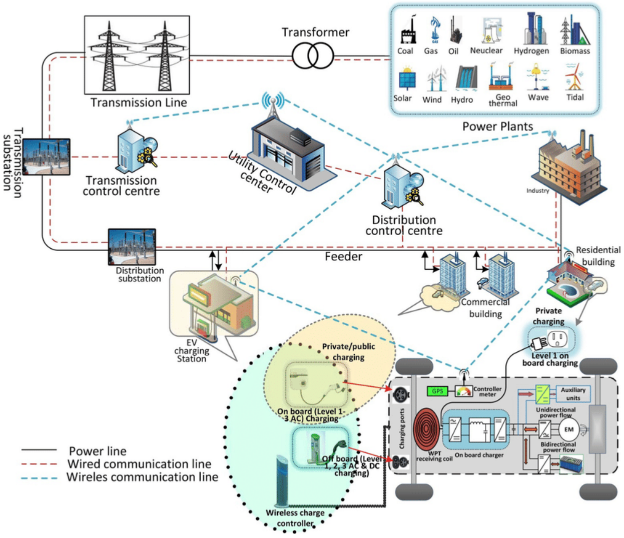

Fig. 1. Charging infrastructure and communication protocol for EV in general. [4]

ISO 15118 provides for data exchange integrity through the connection with TLS (Transport Layer Security). It supports such as: automatic payment and identification using digital certificates. Yet these conventional cryptographic techniques are prone to quantum dangers, and thus require post-quantum versions.

B. Quantum Computing and Cryptography

Quantum computers endanger RSA and ECC, traditional methods of encrypting data and information, with the help of that quantum algorithm called Shor's. Some of the post-quantum cryptographic algorithm includes lattice based cryptography, hash based cryptography and multivariate polynomial based cryptography which make them resist these threats. Table I shows how classical and PQC fit in terms of computational complexity and resource utilization.

TABLE I
COMPARISON OF CLASSICAL AND POST-QUANTUM CRYPTOGRAPHIC ALGORITHMS

Algorithm	Type	Quantum Resistance
RSA	Classical	Vulnerable
ECC	Classical	Vulnerable
CRYSTALS-Dilithium	Lattice-based	Resistant
FALCON	Lattice-based	Resistant
SPHINCS+	Hash-based	Resistant

III. RELATED WORK

A. *QuantumCharge: Crypto-Agility in Action*

QuantumCharge has two features: Dynamic algorithm switching allows over-the-air (OTA) updates to PQC algorithms with using secure firmware, and Hardware Security Modules (HSMs) which some devices like Infineon's OPTIGA™ TPM store Kyber keys in the tamper-resistant environments.

B. *DynamiQS: Securing Dynamic Wireless Charging*

DynamiQS simply utilizes Ring Learning with Errors (RLWE) for authentication process in the dynamic wireless power transfer (DWPT) general systems. It is lightweight and well designed for real-time operations. Moreover, users can maintain anonymity through zero-knowledge proofs when they power up their smartphones.

PQC integration into EV charging has been discussed in several papers. DynamiQS employs identity-based encryption based on lattice, and has safe DWPT. Like for ISO 15118, QuantumCharge adds PQC and the concept of crypto-agility to guarantee secure charging sessions. A clear description of these solutions reveals their advantages and disadvantages as presented below.

Combining NTRU lattices, DynamiQS employs the RLWE framework so as to protect data from quantum threats, while achieving efficient authentication. QuantumCharge, on the other hand, targets the further improvement of the evaluated ISO 15118 with the incorporation of PQC-enabled HSMs and crypto-agility elements. [1]

IV. PROPOSED ARCHITECTURE

In the following, Figure 3 shows the proposed architecture to include PQC in EV charging infrastructures. Key components include:

- **PQC-enabled Hardware Security Modules (HSMs):** Monitor proper storage of keys and perform cryptographic tasks as well.
- **Hybrid Protocols:** During the transition period support both the classical and the quantum-resistant algorithm.
- **Enhanced Communication Security:** Settle PQC algorithms regarding TLS channels and digital signatures.

A. *PQC-Enabled Hardware Security Modules (HSMs)*

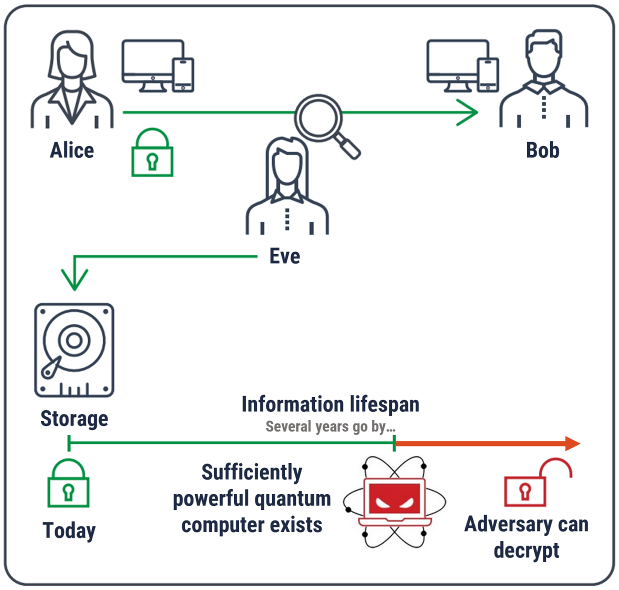

Fig. 2. Impact of quantum computing on classical cryptography. [5]

HSMs need enhancement to implement PQC algorithms because quantum threats are emerging while still requiring security guarantees and performance levels. Modern HSMs function as tamper-resistant devices for storing cryptographic keys and executing them along with performing cryptographic acceleration securely. EV charging facilities integrate PQC algorithms within HSMs to secure them against quantum defense threats.

1) *Various Implementations of PQC-Enabled HSMs:*

- **Infineon OPTIGA™ TPM:** Supports post-quantum algorithms like Kyber (for key encapsulation) and Dilithium (for digital signatures). The system stores keys through 256-bit secure security protocol to protect against traditional and quantum threats. This device defends automotive security through its operation in both EV charging stations and vehicle-to-grid (V2G) communication systems.
- **NXP EdgeLock SE050:** SPHINCS+ hash-based signature scheme joins the framework because it excels in resources-limited environments such as embedded systems and IoT. Long-term security becomes possible because the scheme avoids number-theoretic hardness assumptions. The mechanism enables dependable boot operations along with firmware validation within EV charging systems.

B. *Hybrid TLS 1.3 Handshake*

A hybrid TLS 1.3 handshake solves the need to transition easily to post-quantum security while preserving functionality with current EV charging networks. During the handshake process the hybrid cryptographic mechanism lets EVs and charging stations pick the maximum security option from traditional and post-quantum primitives.

1) *General Process Operation:*

- **Starting with Client Hello:** At the start of TLS handshake the EV transmits its key exchange algorithm list which contains RSA in addition to Kyber post-quantum key.

- **Choosing of Server Selection:** During evaluation the charging station selects one of the available cryptographic options. The server chooses Kyber as its key exchange protocol when it supports the cryptographic functionality. The system selects RSA if the server lacks support for Kyber.
- **Session Setting Up:** When using Kyber the system conducts key exchange functions to provide quantum resistance through forward secrecy. The session key derives from post-quantum algorithms that protect against quantum computer threats. An encrypted managerial link establishes between an EV and a charging station during handshake completion.

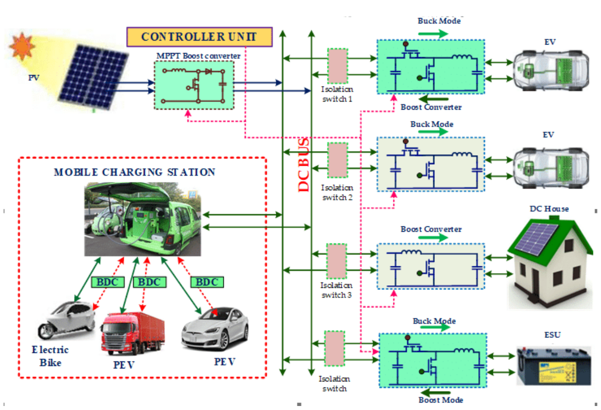

Fig. 3. Architecture of EV charging based on Proposed PQC. [7]

V. Migration Strategies for PQC

Although it is realized that there will always be some disruption in transitioning from classical cryptography to PQC, it is important that every effort is made to contain this disruption. The following strategies can facilitate a seamless migration:

- **Hybrid Cryptographic Protocols:** While both classical and quantum-safe algorithms are being used during the transition phase, the approach allows for the algorithms to be backward compatible.
- **Phased Deployment:** Sequential integration of PQC algorithms to the various parts of EV and charging systems lessens threats.
- **Post-Quantum Readiness Testing:** By implementing PQC solutions in such environments the deficiencies affecting performance can be easily determined.

A. Hybrid Protocols in Action

Hybrid protocols include combining of PQC algorithms with the traditional cryptographic techniques. For example, the migrations of Transport Layer Security (TLS) can use RSA together with CRYSTALS-Dilithium as mechanisms of interaction during handshakes. Figure 4 illustrates the operational flow of a hybrid TLS handshake.

B. EU's EVC-PQC Pilot

The European Union's pilot project deployed hybrid certificates (RSA + Dilithium) to serve 500 highway charging stations located in Germany. Results: [6]

- **80 Percent Reduction in Quantum Vulnerability:** Dilithium signatures took over from ECDSA as a security method for billing authentication.
- **Legacy Support:** The RSA implementation for older EV models will ensure uninterrupted service to customers.

C. Tesla's SPHINCS+ Deployment

Home chargers can now enable optional SPHINCS+ support through Tesla's 2024 firmware update. These are the key insights:

- **Phased Rollout:** Most Tesla users activated PQC through their smartphone application which gained 60 percent acceptance during the first six months.
- **Performance Trade-Offs:** SPHINCS+ extended signature storage security while signature generation needed 310ms to complete the process.

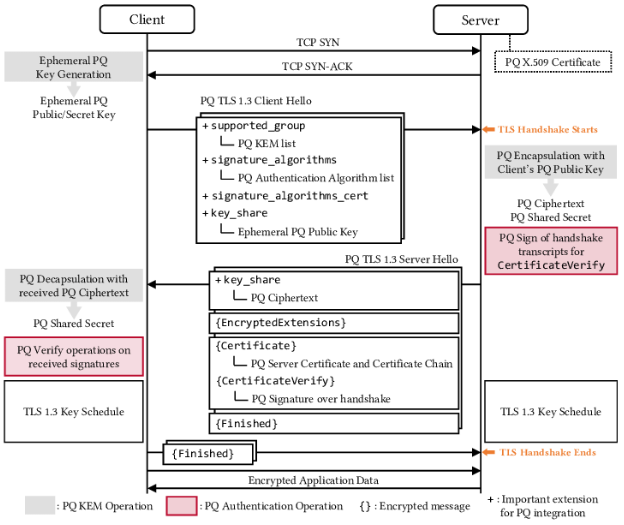
Client
Server
TCP SYN
TCP SYN-ACK
PQ X.509 Certificate
Ephemeral PQ Key Generation
Ephemeral PQ Public/Secret Key
PQ TLS 1.3 Client Hello
+ supported_group
PQ KEM list
+ signature_algorithms
PQ Authentication Algorithm list
+ signature_algorithms_cert
+ key_share
Ephemeral PQ Public Key
TLS Handshake Starts
PQ Encapsulation with Client's PQ Public Key
PQ Ciphertext
PQ Shared Secret
PQ Sign of handshake transcripts for CertificateVerify
PQ TLS 1.3 Server Hello
PQ Decapsulation with received PQ Ciphertext
+ key_share
PQ Ciphertext
{EncryptedExtensions}
PQ Shared Secret
PQ Verify operations on received signatures
{Certificate}
PQ Server Certificate and Certificate Chain
{CertificateVerify}
PQ Signature over handshake
TLS 1.3 Key Schedule
TLS 1.3 Key Schedule
{Finished}
{Finished}
TLS Handshake Ends
Encrypted Application Data
: PQ KEM Operation
: PQ Authentication Operation
{} : Encrypted message
+ : Important extension for PQ integration

Fig. 4. Hybrid TLS handshake combining classical and post-quantum cryptography.

VI. Use Cases

The integration of PQC benefits various EV charging scenarios:

- **Highway Charging Stations:** Guarantees safe billing with no possibility to impersonate a user.
- **Fleet Management:** Preserves the transmission of data through a fleet of mobile automobiles back to a central system.
- **Smart Grid Integration:** Secures data exchange in vehicle-to-grid (V2G) communications.
- **Home Charging Solutions:** Protects personal charging arrangements from being hatched by hackers.
- **Shared Mobility Networks:** Halts data breaches in the car-sharing or ride hailing networks.

The mentioned use cases prove how PQC fits the security utility across different types of EV charging: personal, public, and industrial.

A. Vehicle-to-Grid (V2G) Security

Vehicle-to-Grid (V2G) technology permits electric vehicles (EVs) to exchange power between themselves and the power grid in both directions making EVs capable of supplying electricity to the grid during peak usage periods. Security challenges at various levels are present in V2G systems stemming from their use of wireless data exchange with cloud-based platforms and smart grid management systems. Data security in V2G networks must guarantee complete integrity in addition to maintaining privacy and authenticating exchanged messages to protect users from disruptive attacks and data breaches. [17]

1) The Role of Post-Quantum Cryptography (PQC) in V2G Security: Post-Quantum Cryptography (PQC) enables the use of cryptographic algorithms that can withstand the challenges posed by quantum algorithms. Both RSA and ECC public-key cryptographic methods remain susceptible to Shor's algorithm alongside discrete logarithm problem solution capabilities which quantum algorithms can perform easily. Standards from NIST specify PQC algorithms that provide protection measures which defend V2G communications from contemporary attackers as well as quantum adversaries in the long term.

- **Dilithium Signatures for Authentication in V2G Systems** The main security risk in V2G networks originates from fake control commands which distort energy management flows. An attacker can transmit artificial demand-response commands which lead to grid instability as well as unauthorized energy consumption. The authentication risk can be reduced through implementation of Dilithium which serves as a lattice-based digital signature algorithm. As a use case, the grid operator uses Dilithium signatures to digitally authenticate commands that will be sent to EVs. EVs need to check digital signatures before performing any actions on grid commands to verify authorized control signals for charging and discharging operations.
- **Kyber Key Exchange for Secure V2G Communications** For V2G systems to function securely it is essential to create a protected link between EVs and charging stations together with grid operators. Attackers acquire control over encryption keys which allows them to overhear sensitive information as well as send unlawful commands. The key encapsulation method Kyber represents a quantum-resistant option for key exchange because it works based on lattices instead of Diffie-Hellman or RSA protocols. For general use case, the EV establishes an encrypted connection with the charging station through Kyber for exchanging keys before data transmission begins.

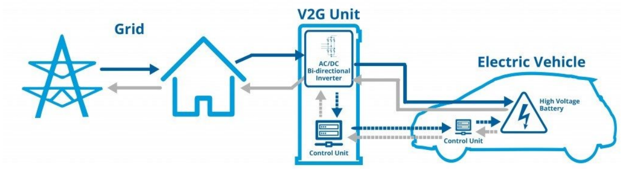

Fig. 5. General Representation of V2G [10]

B. Drone-Based Mobile Charging

The growing number of electric vehicle adopters requires the development of immediate charging systems because EV owners need flexible charging solutions now. Using drone-delivered mobile charging enables autonomous drone platforms to utilize wireless energy transfer technology for continuously charging electric vehicles out in the open. The system guarantees EVs will not face battery emergencies since it operates effectively in locations with restricted charging infrastructure.

1) Autonomous Charging Drones and NTRU-Based Authentication: The fundamental requirement for drone-based mobile charging systems consists of protecting both drone-EV data exchanges and verification procedures. The secure nature of RSA or ECC traditional cryptography stands at risk in quantum attacks so the NTRU post-quantum cryptographic algorithm acts as a reliable substitute.

Here is an example of how NTRU-based authentication plays a key role in enabling safe drone-based EV charging:

- **Real-Time Verification:** The system needs an efficient authentication procedure for preventing delays during charging operations. The authentication process performed with NTRU requires under 50 milliseconds which results in instant charging initiation.
- **Lightweight Design:** Drones must use lightweight cryptographic algorithms because they have strict weight limitations regarding their payloads. NTRU possesses optimal key storage capabilities which measure only around 1 KB thus being suitable for resource-restricted platforms such as autonomous charging drones.

VII. Discussion and Evaluation

Many PQCs algorithms like CRYSTALS-Dilithium-FALCON is found to be computationally viable for EV charging systems from the simulation point of view. Despite the usage of these keys in the generating SPHINCS+ being time-consuming, offers compelling security to warrant the performance in critical functions. [3]

A. Performance Analysis

The results also show that the performance of PQC algorithms is satisfactory in terms of meeting the latency requirements of EV charging. In Figure 7 it is represented the difference in the implementation of classical and post quantum types of algorithms.

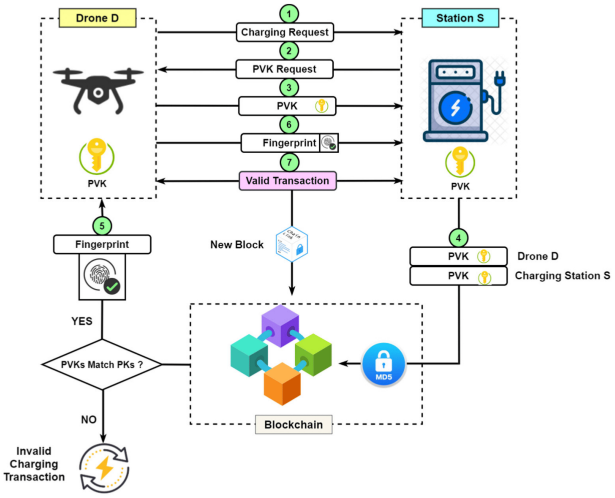

Fig. 6. Main Architecture of the Drone Charging System [11]

B. Challenges

- **Resource Constraints:** PQC on EVs has to be optimised for embedded systems.
- **Interoperability:** How those with legacy systems that are PQC-enabled can ensure that newer PQC capability is compatible with their current systems?
- **Migration Complexity:** It requires numerous changes to switch to PQC.

VIII. Conclusion and Future Work

In doing so, this paper highlights the need to adopt post-quantum cryptography for protecting the charging structures of EVs. With regards to novel quantum risk factors, it is possible to counter them with the help of PQC algorithms and the application of hybrid protocols. Future work includes real-world implementation and comprehensive performance evaluations, focusing on:

- PQC algorithms that have low hardware footprint for integration to resource-constraint embedded systems.
- Improving the compatibility of the classical and quantum-safe systems
- Carrying out generic trials for the proposed architectures in large scale field tests.

A. Roadmap For Future Technologies

A systematic guide must be implemented to build a secure and globally interoperable EV charging infrastructure. The following benchmarks present the essential development process for securing EV charging networks with post-quantum measures:

1) Hybrid Certificate Mandate for Public Charging Stations(2025): Public EV charging stations operated in EU territory and California must employ hybrid classical plus PQC certificates for authentication purposes. Initial pilot deployments of post-quantum secure communication protocols (e.g., TLS 1.3 with PQC support). [12]

Factors	**DES**	**3DES**	**AES**	**Blowfish**	**RSA**	**ECC**
Developed	IBM in 1975	IBM in 1978	Vicent rijman, Joan Daemon 2001	Bruce Schneier 1993	Ron Rivest 1978	Neal Koblitz, Victor Miller 1985
Key length	56bits	168bits (k1, k2, k3) 112bits (k1 and k2)	128, 192, 256 bits	32 to 448bits	1024bits	160bits
Block size	64bits	64bits	128bits	64 bits	Min 512 bits	64bits
Security	Not secure enough	Not secure enough	Adequately secured	Least secure	Least secure	Adequately secured
Cipher type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Asymmetric block cipher	Asymmetric discrete logarithm
Speed	Moderate	Slower	Faster	Faster	Slower	Faster
Rounds	16	48	10-128 bits key 12- 192 bits key 14- 256 bits key	16	1	16
Power Consumption	Low	Low	Low	Low	High	Low

Fig. 7. Comparison of classical and post-quantum algorithm. [9]

2) NIST Phase IV Finalization(2026): NIST completes the Phase IV standards development for post-quantum cryptography. Standard PQC algorithms start integrating into firmware and security modules of EV manufacturers as well as charging network providers. [13]

3) ISO 15118-PQC Integration(2027): The ISO 15118 gateway plug-and-charge authentication system receives its support for post-quantum cryptographic algorithms through updates to its standards. The adoption of post-quantum certificates needs to be standard at all facilities delivering charging services. [14]

4) Quantum Key Distribution (QKD) Pilot Deployment(2028): QKD pilots start by deploying the technology in charging systems maintaining high security standards (particularly those serving military forces and governments and corporate fleets). The research explores how combining QKD and PQC elements creates better secure network architectures for charging networks. [15]

5) Global Interoperability Standards for Cross-Border Charging(2030): The development of international standards for quantum-secure authentication processes within multinational EV charging systems. Full-scale deployment of AIenhanced post-quantum threat detection in smart charging grids. [16]

References

[1] T. Bianchi, A. Brighente, and M. Conti, ”DynamiQS: Quantum Secure Authentication for Dynamic Charging of Electric Vehicles,” in *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2024, pp. 174–185.

[2] D. Kern et al., ”QuantumCharge: Post-Quantum Cryptography for Electric Vehicle Charging,” *LNCS*, vol. 13906, pp. 85–111, 2023.

[3] T. E. Carroll Moran et al., ”Exploring the Adoption Challenges of Post-Quantum Cryptography in EV Charging Infrastructure,” Pacific Northwest National Laboratory, 2024.

[4] N. A. Ravi and L. Kumar, “Electric vehicle charging method and impact of charging and discharging on distribution system: a review,” International Journal of Electric and Hybrid Vehicles, vol. 14, no. 1/2, p. 107, 2022, doi: https://doi.org/10.1504/ijehv.2022.10050109.

[5] Capa Learning, “Why Is Quantum Computing A Threat To Cryptography? - Capa Learning,” Capa Learning, May 18, 2023. https://capalearning.com/2023/05/18/why-is-quantum-computing-a-threat-to-cryptography/ (accessed Jan. 17, 2025).

[6] D. A. Cooper, D. C. Apon, Q. H. Dang, M. S. Davidson, M. J. Dworkin, and C. A. Miller, “Recommendation for Stateful Hash-Based Signature Schemes,” Oct. 2020, doi: https://doi.org/10.6028/nist.sp.800-208.

[7] A. D. Savio and V. J. A., “Development of multiple plug-in electric vehicle mobile charging station using bidirectional converter,” International Journal of Power Electronics and Drive Systems (IJPEDS), vol. 11, no. 2, p. 785, Jun. 2020, doi: https://doi.org/10.11591/ijpeds.v11.i2.pp785-791.

[8] D. Sikeridis, P. Kampanakis, and M. Devetsikiotis, “Assessing the overhead of post-quantum cryptography in TLS 1.3 and SSH,” Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies, Nov. 2020, doi: https://doi.org/10.1145/3386367.3431305.

[9] A. Orobosade, T. Aderonke, A. Boniface, and A. J., “Cloud Application Security using Hybrid Encryption,” Communications on Applied Electronics, vol. 7, no. 33, pp. 25–31, May 2020, doi: https://doi.org/10.5120/cae2020652866.

[10] “EV Charging: Software and Grid Services — Cleantech Group,” www.cleantech.com. https://www.cleantech.com/ev-charging-software-and-grid-services/

[11] M. Torky, M. El-Dosuky, E. Goda, V. Snášel, and A. E. Hassanien, “Scheduling and Securing Drone Charging System Using Particle Swarm Optimization and Blockchain Technology,” Drones, vol. 6, no. 9, p. 237, Sep. 2022, doi: https://doi.org/10.3390/drones6090237.

[12] “Electric Vehicle Supply Equipment Standards Regulation Background and FAQs — California Air Resources Board,” Ca.gov, 2019. https://ww2.arb.ca.gov/resources/documents/electric-vehicle-supply-equipment-standards-regulation-background-and-faqs.

[13] I. T. L. Computer Security Division, “Workshops and Timeline - Post-Quantum Cryptography — CSRC — CSRC,” CSRC — NIST, Jan. 03, 2017. https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline

[14] D. Kern, Christoph Krauß, T. Lauser, Nouri Alnahawi, A. Wiesmaier, and R. Niederhagen, “QuantumCharge: Post-Quantum Cryptography for Electric Vehicle Charging,” Cryptology ePrint Archive, 2023. https://eprint.iacr.org/2023/430

[15] “Securing EV Charging Infrastructure Part 2: Game-Changing Research,” Energy.gov, 2024. https://www.energy.gov/ceser/articles/securing-ev-charging-infrastructure-part-2-game-changing-research

[16] “AFIR - Alternative Fuels Infrastructure Regulation: What you need to know,” www.virta.global. https://www.virta.global/afir-what-you-need-to-know

[17] Virta, “Vehicle-to-grid (V2G) technology: Key challenges and developments,” www.virta.global. https://www.virta.global/blog/v2g-technology-key-challenges-and-developments