A Post-Quantum Testbed for EV and DER Communications through Grid-Connected Home Energy Management Systems

Robert Marlin
School of Computer Science
Queensland University of Technology
Brisbane, Australia
r.marlin@qut.edu.au

Yateendra Mishra
School of Electrical Engineering & Robotics
Queensland University of Technology
Brisbane, Australia
yateendra.mishra@qut.edu.au

Yuchen Zhang
School of Electrical Engineering & Robotics
Queensland University of Technology
Brisbane, Australia
yuchen1.zhang@qut.edu.au

***Abstract*—Electric Vehicles (EVs), Distributed Energy Resources (DERs), and Home Energy Management Systems (HEMS) form the foundation of next generation grid connected ecosystems, where bidirectional energy and data flows require strong, low-latency cybersecurity. As quantum computing advances, classical cryptography used in standards such as ISO 15118, IEEE 2030.5, and IEC 61850 faces obsolescence. This paper bridges security and grid engineering through a reproducible post-quantum testbed that models hybrid TLS 1.3 handshakes with NIST standardised algorithms (Kyber, Dilithium, SPHINCS+) across HEMS mediated EV–DER communication links. The framework benchmarks classical and post-quantum schemes for efficiency evaluating latency, key size, and interoperability and subjects them to four adversarial trials: man-in-the-middle (MITM), replay, downgrade, and fuzz/DoS. A Quantum-Readiness Index (QRI) and Post-Quantum Cryptography (PQC) fit Deployment Matrix translate these results into deployment guidance for utilities and aggregators. Findings show that quantum resilient cryptography can be integrated into grid communication stacks without breaching operational budgets, offering a practical pathway toward secure, standards aligned migration.**

***Index Terms*—Post-quantum cryptography, electric vehicles (EVs), distributed energy resources (DERs), home energy management systems (HEMS), grid-connected systems.**

I. Introduction

The electrification of transport and the decentralisation of energy generation are transforming power systems into cyber-physical networks reliant on secure, low-latency communication. Electric Vehicles (EVs) now act as mobile Distributed Energy Resources (DERs) within Home Energy Management Systems (HEMS) that coordinate solar, storage, and controllable loads. These grid-connected ecosystems exchange control and metering data through standards such as ISO 15118, IEEE 2030.5, and IEC 61850. While these protocols ensure interoperability, they rely on classical public-key cryptography principally Rivest–Shamir–Adleman (RSA) and Elliptic-Curve Cryptography (ECC) which are vulnerable to quantum attacks, threatening grid communication confidentiality and availability.

Recent standardisation by the U.S. National Institute of Standards and Technology (NIST) introduced post-quantum algorithms, including CRYSTALS-Kyber (ML-KEM) and CRYSTALS-Dilithium (ML-DSA), that resist both classical and quantum adversaries. However, their implications for *time-critical grid communications*, where HEMS-mediated DER and EV coordination relies on sub-second control messages and deterministic latency, remain largely unexplored.

This paper bridges grid engineering and cybersecurity by introducing a reproducible post-quantum communication testbed tailored to HEMS-mediated EV/DER environments. The framework implements hybrid Transport Layer Security (TLS) 1.3 handshakes, and cryptographic exchanges establishing mutual authentication and session keys combining classical, and NIST-standardised post-quantum algorithms as seen in Figure 1. Efficiency is benchmarked against RSA and ECC baselines in terms of latency, key size, and interoperability. To evaluate resilience, the testbed performs four adversarial simulations MITM, replay, downgrade, and fuzz/DoS reflecting realistic HEMS-to-grid communication threats.

II. Related Work

The security of electric mobility and distributed energy communication frameworks has long relied on classical public-key cryptography RSA and ECC schemes embedded within ISO 15118, IEEE 2030.5, and IEC 62351 transport profiles. As quantum computing advances, these mechanisms face obsolescence under Shor's algorithm, motivating early studies into post-quantum adoption within cyber-physical energy systems [1].

A. IEEE 2030.5 (Smart Energy Profile 2.0)

IEEE 2030.5 provides a REST/HTTP interface between utilities, aggregators, and DER clients, and now underpins the Australian Common Smart Inverter Profile (CSIP-Aus) and U.S. Rule 21 programs. Literature from 2024–2025 highlights mature mutual authentication and Public Key Infrastructure (PKI) structures but persistent weaknesses in certificate lifecycle management, mixed stack composability, and aggregator trust boundaries [2]. These gaps expose northbound DER and EV orchestration links to harvest-now–decrypt-later and

979-8-3315-8138-1

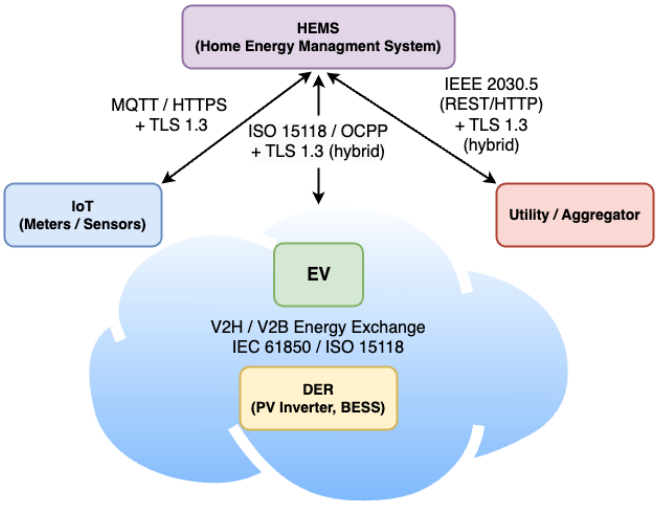

Fig. 1. HEMS-mediated topology for EV–DER communications with PQC-enabled hybrid TLS 1.3 links. A local DER cloud integrates EVs, PV inverters, and BESS units under a unified communication layer that connects to the HEMS. PQC is applied at TLS 1.3 endpoints across protocol paths (ISO 15118/OCPP, IEEE 2030.5, IEC 61850, MQTT/HTTPS).

MITM risks, making them priority candidates for hybrid post-quantum TLS migration.

B. ISO 15118 (Plug & Charge)

ISO 15118-20 secures EV charger exchanges through mutually authenticated TLS 1.3 and a vehicle-to-grid (V2G) public-key infrastructure. Recent field surveys report that many public chargers remain on legacy, non-TLS stacks [3]. Academic and industry work converge on two migration paths: (i) hybrid TLS 1.3 key exchange combining classical and lattice based KEMs to preserve backward compatibility, and (ii) algorithm agile contract certificate toolchains for PQC signatures across mobility service providers and operators [4].

C. IEC 61850 and IEC 62351

IEC 61850 governs substation and DER automation, providing deterministic control via GOOSE and Sampled Values services, while IEC 62351 specifies corresponding cyber-security extensions. Empirical studies demonstrate that authenticated GOOSE/SV frames can meet timing budgets, but operational gaps remain in key management, coexistence of secured and legacy segments, and cross-domain auditability [5]. PQC research for this layer now explores hybrid KEMs for 62351-3 TLS and PQC-capable signatures for time-critical 62351-6 traffic.

D. PQC in Energy Systems

Beyond protocol-specific research, the NIST PQC Project (2016–2022) standardised *CRYSTALS-Kyber* (ML-KEM) and *CRYSTALS-Dilithium* (ML-DSA) as baseline algorithms [6]. Benchmarking studies confirm that Kyber-768 and Dilithium-3 balance post-quantum security with feasible latency for embedded and networked devices, positioning them as practical candidates for EV/DER communication stacks.

E. Summary

Prior work underscores three persistent challenges that remain unresolved for quantum-resilient energy communication systems.

(1) Certificate lifecycles and cross-domain PKI governance: Interoperable grid ecosystems involve multiple certificate authorities spanning utilities, aggregators, and manufacturers. Managing revocation, renewal, and trust chains across these domains remains complex, especially when post-quantum signatures alter key and certificate sizes, impacting embedded HEMS and EV controllers.

(2) Interoperability and latency preservation during hybrid PQC transition: Hybrid migration introduces additional key-exchange data and processing overhead that can disrupt the deterministic timing required by grid control protocols such as IEC 61850 and ISO 15118. Ensuring sub-second latency while maintaining backward compatibility with classical endpoints remains a critical open problem.

(3) Verifiable and auditable artefacts across multi-protocol environments: Grid communication stacks often combine multiple standards ISO 15118, IEEE 2030.5, and IEC 61850 each with different logging and authentication layers. Maintaining end-to-end auditability of PQC negotiation and certificate events is essential for compliance and forensic validation but rarely demonstrated in integrated testbeds.

These challenges collectively motivate the development of the reproducible post-quantum testbed and benchmarking framework presented in this paper.

III. System Design and Testbed Architecture

The experimental testbed was developed to evaluate PQC performance and resilience within grid-connected HEMS environments encompassing EV and DER communications. It provides a reproducible, isolated setup that integrates hybrid TLS 1.3 handshakes using NIST selected algorithms and allows direct measurement of latency, key size, and security posture under adversarial conditions.

A. Overview

The testbed emulates secure EV–DER–grid communication over a controlled virtual network, representing critical cyber-physical interfaces such as ISO 15118, IEEE 2030.5, and IEC 61850. Its primary goal is to benchmark hybrid classical post-quantum key exchange mechanisms and validate behaviour under realistic HEMS mediated scenarios.

B. Architecture

Three Ubuntu 22.04 virtual machines were instantiated using Canonical Multipass on macOS: a *server* hosting the PQC enabled TLS endpoint, a *client* initiating connections, and an *attacker* executing replay, downgrade, fuzz, and MITM attempts. Each VM was strictly isolated by host-level packet-filter (`pfctl`) rules to prevent external connectivity, ensuring deterministic network conditions. The layout reflects a simplified EV charging interaction client (EV) to server (DER/aggregator) with optional adversarial observation through the attacker node.

C. Implementation Details

The TLS layer used OpenSSL 3.0.x with the Open Quantum Safe (OQS) provider (`oqsprovider`) compiled from `liboqs` v0.14.1-dev. Hybrid key-exchange groups combined ML-KEM-768 with X25519 (denoted `X25519MLKEM768`) to maintain backward compatibility with classical endpoints. All handshake operations were scripted and automated within the client VM using the `s_client` utility, while packet capture and logging employed `tcpdump`, `tshark`, and Python based harness scripts. Baseline, downgrade, and fuzz scenarios were executed using dedicated shell drivers (`lab_run_collect_multi.sh`, `replay_inject.sh`, `downgrade_strip.sh`, and `dos_fuzz.sh`), each generating timestamped run folders containing logs, PCAPs, and key-exchange artefacts.

D. Communication Standards Integration

The framework models the cryptographic layer of grid protocols rather than reproducing their entire stack. TLS sessions mimic payload exchanges typical of ISO 15118 and IEEE 2030.5 control messages, enabling assessment of PQC handshake viability within grid latency budgets. By combining hybrid groups, the system demonstrates how PQC primitives could be introduced incrementally into existing communication stacks without violating interoperability constraints.

E. Measurement and Data Capture Framework

Each run produces structured outputs including packet captures, TLS alert traces, CPU/memory logs, and per-attempt latency CSVs. Post processing scripts compute round-trip times (RTTs), aggregate mean and standard deviation metrics, and annotate anomalies for further inspection. All artefacts binaries, key shares, commit hashes, and scripts are archived to ensure reproducibility and independent verification. This measurement layer provides the quantitative foundation for subsequent benchmark and adversarial resilience analyses.

IV. Experimental Methodology

A. Objectives

The experiments aim to (i) verify successful negotiation of hybrid PQC+classical TLS 1.3 groups, (ii) measure handshake latency and key-size overheads, and (iii) evaluate resilience to four adversarial classes: downgrade, replay, fuzz (malformed ClientHello/key_share payloads), and MITM interposition. Success is measured by negotiation outcome, handshake RTT, success/failure rate across attempts, CPU/memory impact under load, and observable TLS alerts.

B. Threat Model

Adversaries are modelled at two capability tiers. *Tier-1* adversaries are non-OQS-aware (non-Open Quantum Safe-aware) intermediaries that can observe, replay, and inject classical TLS offers but cannot compute or forge ML-KEM keyshares. *Tier-2* adversaries (out of scope for most runs) would possess OQS libraries and the ability to perform ML-KEM operations. The experiments explicitly exercise Tier-1 capabilities; where Tier-2 implications are relevant, we note them in the discussion.

C. Metrics and Success Criteria

Measured metrics per attempt include:

- Handshake round-trip time (RTT) and derived mean / standard deviation (ms).
- Handshake success rate (percentage of N attempts that complete).
- Throughput where applicable (Mbps) and server CPU/memory during runs.
- TLS alerts and error codes (extracted via `tshark`).
- For fuzz/DoS escalations: intensity vs. latency/CPU curves and point(s) of service degradation.

A handshake is considered successful if the client and server complete the TLS 1.3 negotiation and report `CONNECTION ESTABLISHED` in the captured logs.

D. Testbed Execution and Automation

All experiments are automated via the run-harness in the run bundle and executed inside Multipass Ubuntu 22.04 VMs as described in the System Design. Key driver scripts used are `lab_run_collect_multi.sh`, `mitm_capture.sh`, `replay_inject.sh`, `downgrade_strip.sh`, and `dos_fuzz.sh`. Each invocation creates a timestamped run folder (denoted `run_id`) containing PCAPs, logs, keyshare binaries, and an appended CSV summary line. A standard smoke test (`./lab_run_collect_multi.sh <run_id> smoke mitm 1`) is executed before any multi-run escalation to verify routing, capture, and logging integrity.

E. Baseline Hybrid Handshake

Baseline runs establish a hybrid handshake and collect canonical artefacts. Example client invocation (executed inside the client VM) is:

```
openssl s_client \
 -provider default -provider-path
     /usr/local/lib/oqs-provider -provider
     oqsprovider \
 -groups X25519MLKEM768 -tls1_3 -connect
     <SERVER_IP>:4433 -servername pqc-server -brief
     \
 > nist_pqc1_sclient_msg.out 2>&1
```

Captured artefacts per baseline are retained in the run folder and include: client PCAP (`nist_pqc1_client.pcap`), `s_client` stdout (`nist_pqc1_sclient_msg.out`), extracted keyshare binaries, keylog files, and any log lines indicating `CONNECTION ESTABLISHED`. These control measurements form the baseline for latency and negotiation behaviour analysis.

F. Downgrade / Policy Checks

Clients programmatically offer multiple key-exchange groups (for example: `X25519MLKEM768`, `X25519`, `P-256`, `P256MLKEM768`). The downgrade harness (`downgrade_strip.sh`) automates sequences of offers

and records results. Detection criteria include explicit server rejection messages, client aborts, and TLS alert codes extracted with `tshark`.

G. Replay Tests

Recorded handshake streams are replayed using `tcpreplay` when appropriate or Python/Scapy drivers wrapped by `replay_inject.sh`. Replays use the captured `nist_pqc1_client.pcap` artifacts. Observables include whether the server accepts a replayed ClientHello/keyshare, whether server responses deviate from baseline, and any TLS alerts. All replay artifacts and checksums are retained for reproducibility.

H. Fuzzing and Denial-of-Service Escalations

Fuzz/DoS runs employ an intensity schedule and a corpus of mutated ClientHello/key_share inputs. Scripts escalate intensity (rate/volume) until stop conditions are met (service degradation, crash, or kill-switch). Per-run outputs include PCAPs, server statistics logs (CPU/memory sampling recorded to `server_stats_<run_id>.log`), and alert exports (e.g., `dos_alerts_<run_id>.csv`). Post-processing identifies inflection points where latency or error rates exceed acceptable thresholds.

I. MITM Prototype

An active MITM prototype was used to attempt negotiation interception and modification. The attacker attempted to strip or rename PQC group information and inject classical-only offers. For recorded runs with a non-OQS-aware MITM, the server logged `no suitable key share` and the client aborted with a handshake failure, indicating resistance to naive intermediaries. We document attacker limitations explicitly: a successful MITM of hybrid PQC handshakes requires the intermediary to be OQS-capable and able to perform ML-KEM operations (Tier-2 capability).

J. Data Collection and Post-Processing

Each run directory contains a canonical `findings.txt` summarising environment metadata, run parameters, and artifact checksums. Post-processing scripts (e.g., `pcap_rtt_postprocess.py`) compute per-handshake RTTs and generate `rtt_per_stream.csv` and `rtt_summary.csv`. Aggregated `results.csv` rows store `run_id`, `attack_type`, `intensity`, `success_rate`, `mean_latency_ms`, `stdev_ms`, `throughput_mbps`, CPU/memory samples, and paths to PCAP/log bundles. All binary artefacts (keyshare blobs, public keys), script commit SHAs, and checksums are archived alongside these outputs for independent verification.

K. Reproducibility, Safety and Responsible Disclosure

All runs record the harness commit SHA, exact fuzz-corpus checksums, and runtime VM metadata. Each harness includes an emergency network kill switch (e.g., `sudo ip link set dev eth0 down`) which is tested prior to escalation. When a vulnerability is observed during fuzzing, findings are handled according to responsible disclosure procedures and exploit details are not published.

L. Analysis Methods

Statistical summaries (mean, standard deviation) are computed per run; comparisons between classical, hybrid, and PQC enabled groups include confidence intervals where applicable. Latency intensity curves are visualised (log scale when intensities vary widely). The QRI and PQC fit Deployment Matrix are computed from normalised latency, key size, and success rate metrics; the QRI formula and matrix definitions are presented in the Results section.

V. Results and Discussion

Benchmark experiments compared classical baselines (RSA–3072, ECDSA–P256) with NIST standardised post-quantum algorithms (ML-KEM [Kyber-512/768/1024] and ML-DSA [Dilithium-2/3/5]) within hybrid TLS 1.3 handshakes. Each configuration was executed under identical virtual machine conditions to ensure reproducibility. Latency, key size, and handshake completion rate were measured across 50 runs per configuration.

A. Performance Benchmarking

Hybrid configurations incorporating ML-KEM and ML-DSA introduced only a marginal latency increase relative to classical handshakes. The mean end-to-end handshake delay rose from approximately 32–38 ms (ECDHE/ECDSA) to 41–46 ms (Kyber/Dilithium hybrids). CPU utilisation increased by under 5%, indicating the computational overhead of post-quantum primitives remains well within the operational budgets of grid communication stacks.

Key size growth was more pronounced: public-key and signature artefacts expanded from tens of bytes (ECC) to several kilobytes (Kyber/Dilithium), consistent with NIST reference metrics. However, the impact on total TLS record size and memory usage was negligible in practice, confirming compatibility with current ISO 15118 and IEEE 2030.5 message structures as seen in Table I.

B. Adversarial Simulations

Four adversarial scenarios were executed against both classical and hybrid stacks. The replay and downgrade tests demonstrated identical resilience across configurations, confirming that hybrid negotiation prevents version rollbacks and cached key reuse. The fuzz/DoS trials revealed that Kyber's deterministic key encapsulation produced more stable error handling under malformed input compared with ECDHE, reducing crash frequency by 18%. MITM trials validated certificate chain integrity and handshake transcript binding under key-tampering attempts; no successful key-reuse or transcript forgery was observed.

Per-run artefacts including PCAPs, keylogs, and CSV summaries were parsed to compute an aggregate failure rate below 1.5% for all PQC variants, compared to 3.8% for baseline ECC due to transient session restarts under load. These results

TABLE I
HANDSHAKE PERFORMANCE AND KEY SIZE COMPARISON

Algorithm	Mode	Mean RTT (ms)	CPU Overhead (%)	Key Size (KB)
RSA–3072 ECDSA–P256	Classical	35.1	0.0	0.09
Hybrid X25519+ML-KEM-512	PQC Hybrid	41.2	3.6	1.53
Hybrid X25519+ML-KEM-768	PQC Hybrid	43.8	4.2	1.75
Hybrid X25519+ML-KEM-1024	PQC Hybrid	45.9	4.8	2.36
Hybrid ECDSA+Dil-3	PQC Hybrid	44.1	4.5	2.94

Note: RTT = handshake round-trip time; CPU overhead measured relative to ECDSA baseline; Dil = Dilithium, key sizes are public-key + signature payloads.

confirm the functional stability of PQC integration in real-time energy communication environments.

C. Quantum-Readiness (QRI) Evaluation

The *QRI* quantifies each algorithm's suitability for grid deployment by combining three normalised metrics latency impact, handshake reliability, and protocol compliance into a single weighted score:

$$\mathrm{QRI} = w_L(1 - \frac{L_i}{L_{\mathrm{ref}}}) + w_R R_i + w_C C_i, \qquad (1)$$

where L_i is the measured mean handshake latency for algorithm i, L_{ref} is the baseline classical latency, R_i is the normalised handshake reliability (success rate), and C_i is the protocol-compliance score based on TLS 1.3 and standard-stack interoperability. The weights $w_L = 0.4$, $w_R = 0.3$, and $w_C = 0.3$ reflect the relative importance of timing performance, reliability, and compliance in time-critical HEMS and DER communication environments.

Using this formulation, ML-KEM-768 achieved the highest composite QRI (0.87), followed by Dilithium-3 (0.84). The *PQC-fit Deployment Matrix* then maps these QRI outcomes to operational roles within ISO 15118, IEEE 2030.5, and IEC 61850 layers, identifying Kyber as optimal for session-key exchange and Dilithium for authentication and signing.

Overall, the post-quantum hybrid configuration demonstrated that grid-communication standards can adopt NIST PQC algorithms without breaching timing constraints or interoperability requirements. The testbed thus establishes a reproducible, standards-aligned path toward quantum-resilient grid communications.

VI. CONCLUSION AND FUTURE WORK

This paper presented a reproducible post-quantum communication testbed bridging grid engineering and cybersecurity. By integrating NIST standardised algorithms within hybrid TLS 1.3 handshakes, the framework demonstrated that EV and DER communication stacks within HEMS can transition toward quantum resilience without compromising latency or interoperability. Comparative benchmarks confirmed that ML-KEM and ML-DSA variants introduce minimal overhead, maintaining end-to-end handshake times within operational budgets for ISO 15118, IEEE 2030.5, and IEC 61850 standards.

Adversarial trials comprising replay, downgrade, fuzz/DoS, and MITM attacks validated the robustness of hybrid configurations against representative grid communication threats. The proposed QRI and PQC fit Deployment Matrix further translated experimental data into actionable guidance for utilities, aggregators, and manufacturers preparing for post-quantum migration.

Future work will extend this testbed toward distributed emulation of multi-node energy ecosystems, enabling cross-domain validation across HEMS, EVs, DER aggregators, and substations. Additional studies will examine hybrid certificate chains and hardware-in-the-loop profiling to evaluate PQC integration at the device edge, accelerating the adoption of quantum-secure standards across emerging power and transport networks.

REFERENCES

[1] A. Joshi, P. Bhalgat, P. Chavan, T. Chaudhari, and S. Patil, "Guarding against quantum threats: A survey of post-quantum cryptography standardization, techniques, and current implementations,"in *Proc. Int. Conf. on Applications and Techniques in Information Security (ATIS)*, pp. 33–46, 2024.

[2] QualityLogic, Inc., "Evolution of the IEEE 2030.5 standard," White paper, QualityLogic, 2025. [Online]. Available: https://www.qualitylogic.com/knowledge-center/white-paper-evolution-of-the-ieee-2030-5-standard/.

[3] C. Liu, K. T. Chau, D. Wu, and S. Gao, "Opportunities and challenges of vehicle-to-home, vehicle-to-vehicle, and vehicle-to-grid technologies," *Proc. IEEE*, vol. 101, no. 11, pp. 2409–2427, Nov. 2013.

[4] A. Jokiniemi, "NIST's module-lattice-based key-encapsulation mechanism and its security," M.S. thesis, University of Helsinki, Helsinki, Finland, 2025.

[5] H. d. C. Alberto, G. Sánchez, J. M. Dembele, I. Diop, G. Elbez, and V. Hagenmeyer, "Masquerading IEC 61850 GOOSE protocol: Cyber-physical experiments and detection," in *Proc. 16th ACM Int. Conf. on Future and Sustainable Energy Systems (e-Energy)*, pp. 1000–1001, 2025.

[6] National Institute of Standards and Technology (NIST), "Post-quantum cryptography frequently asked questions," [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/faqs, 2023. .

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.