Energy-Efficient & Privacy-Preserving Adaptive Post-Quantum Secure Boot for Low-Power RISC-V IoT: A Hardware-Agnostic Approach with Empirical Validation

Faiza Nawaz[1,*], Hamna Mughal[1], Sumaira Safeer[1]
[1] Department of Computer Engineering, Comsats University Islamabad, Attock Campus, Pakistan

***Abstract*—The advent of cryptographically relevant quantum computers threatens the classical public-key primitives (RSA, ECC) that currently secure the boot and over-the-air (OTA) update chains of billions of low-power Internet of Things (IoT) devices. NIST has also standardized the lattice-based post-quantum cryptography (PQC) algorithms, including "ML-KEM and ML-DSA" / "ML-KEM, ML-DSA, and SLH-DSA", but PQC secure-boot solutions for embedded systems either rely on dedicated hardware roots-of-trust that add to per-unit costs, or are based on static, non-adaptive benchmarks, which are unable to establish a tangible security/benefit-cost ratio for software-only implementations. This paper proposes *AdaptivePQC-Boot* as a hardware-agnostic, hybrid classical-PQC secure-boot and OTA-update scheme for commodity RISC-V microcontrollers that (i) requires no dedicated security silicon, relying on RISC-V Physical Memory Protection (PMP) for software-based attestation, (ii) adaptively switches between classical, hybrid, and full-PQC cryptographic modes based on battery level and threat severity, retaining energy budget and device privacy guarantees, and (iii) empirically quantifies the resulting trade-offs. The verification scheme is implemented and evaluated on an ESP32-C6 RISC-V IoT board: Mean time and estimated energy cost of verification are monotonically increasing from Classical (6.46 ms, 0.155 mJ) to Hybrid (9.49 ms, 0.464 mJ) and then to Full-PQC (13.23 ms, 0.774 mJ) across n=12 repeated verification cycles. The adaptive switch-engine saves 56.7% energy compared to an always-Full-PQC baseline in a 12-cycle battery-drain simulation with 4.02 mJ versus 9.29 mJ respectively. The results place the proposed scheme as a viable, clear and energy efficient replacement to hardware-based PQC for cost-limited consumer, industrial-retrofit and privacy-sensitive IoT applications.**

***Index Terms*—RISC-V, low-power IoT, post-quantum cryptography, secure boot, over-the-air update, OTA, adaptive security, energy efficiency, privacy, zero trust**

I. Introduction

A. Background and Motivation

Public-key cryptography has underpinned digital trust for four decades, securing everything from web traffic to firmware signatures. This foundation is time-constrained as Shor's algorithm, run on a large enough fault-tolerant quantum computer, can break RSA and Elliptic Curve Cryptography (ECC) entirely. To respond, NIST released the first three PQC standards in August 2024 ("ML-KEM and ML-DSA" / "ML-KEM, ML-DSA, and SLH-DSA"), and in March 2025 picked a fourth code-based scheme, HQC, as a fallback "structural" PQC. The theoretical foundations and implementation strategies on these standards are thoroughly covered by Truong *et al.* [1] and unified architecture for combined execution of both ML-DSA and ML-KEM is proposed in the literature [2].

Corresponding author: Faiza Nawaz (email: faiza.nawaz@cuiatk.edu.pk).

The urgency is further exacerbated by the "harvest-now, decrypt-later" model, particularly for privacy-sensitive low power IoT telemetry potentially recorded today for later decryption when a cryptographically relevant quantum computer (CRQC) is available. With the advent of a CRQC, the devices deployed today via classical secure boot find themselves in a quantum threat window as shown in the above Fig. 1, which drives the urgency to move to a post-quantum boot before NIST's deprecation milestones. The estimated requirement of fewer qubits for breaking ECC in recent years (2025–2026) has narrowed migration windows, leading Google to establish an internal migration deadline of 2029 for ECC to be replaced by other schemes and NIST to set 2030 as the date after which RSA/ECC should not be used in new designs, with complete deprecation by 2035. By January of 2027, the NSA's CNSA 2.0 suite requires quantum-safe algorithms for new national-security systems, and the UK NCSC plans to require this by 2035 for critical infrastructure.

These deadlines are significant for low power IoT: the devices deployed today will still be in service when CRQCs come into existence, and many will have privacy sensitive telemetry location, biometric, or usage data—that need to be kept confidential throughout that lifetime. Both reviews of PQC in consumer electronics [3] and broad surveys of quantum-resistant IoT cryptography [4], [5] agree that the major problem limiting the adoption of PQC at the edge is not algorithmic immaturity, but rather resource limitations. This condition is exacerbated in 5G-IoT as both the lattice-based and legacy ECC/RSA should coexist in a long transition period, as demonstrated by Choudhury *et al.* in [6].

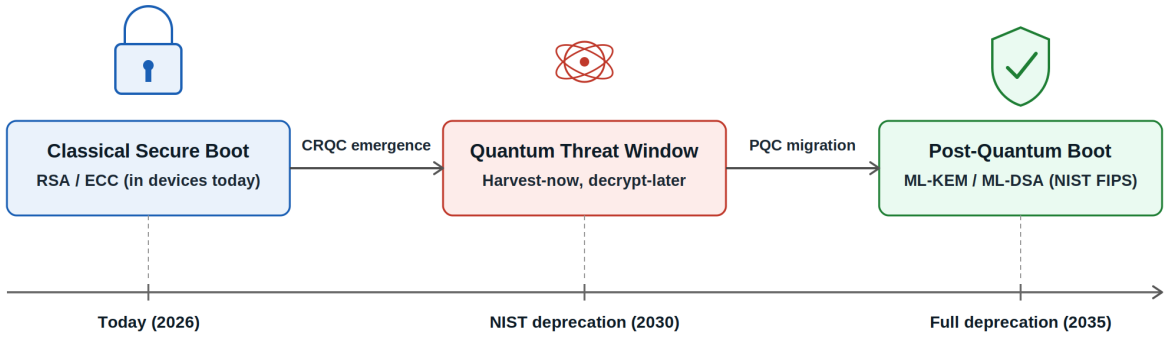

Fig. 1: Migration timeline for low power IoT to secure boot after quantum. Classical RSA/ECC secure boot devices provisioned today (2026) are vulnerable to "harvest-now, decrypt-later" once a quantum computer of cryptographic relevance emerges. The migration window has been narrowed down to the post-quantum boot, with NIST 2030 providing deprecation guidance and full deprecation 2035 [1] for its recommended post-quantum cryptographic standards (PQCS), ML-KEM/ML-DSA. AdaptivePQC-Boot focuses on the "Resource-Middle" area of this spectrum.

B. Problem Statement

There are two types of PQC-IoT solutions: The first anchors cryptographic operations in dedicated hardware, such as secure elements, PUFs, or custom extensions to the RISC-V instruction-set [7], [8], that is too costly to widely integrate into consumer IoT devices, or even into microcontroller chips that are widely deployed. The second class is composed of software-only benchmarking studies that evaluate the performance of PQC on embedded targets [9]–[12], but do not provide an energy-aware deployable framework for PQC, nor directly provide an empirical measure of the assurance gap of a hardware-agnostic approach.

While many solutions have been proposed to address the energy-versus-security trade-off in the classical-to-PQC transition, the energy cost has remained unquantified and the security has been taken as given so this leaves an unaddressed middle ground: a runtime-adaptive, hardware-agnostic hybrid classical-PQC secure-boot mechanism for low-power RISC-V IoT whose energy cost is measured, not assumed, and whose design also preserves device privacy by minimizing the attack surface exposed during the classical-to-PQC transition.

C. Contributions

The following are the contribution of this paper:

- A software-only hybrid classical-PQC secure-boot design that uses RISC-V PMP for attestation instead of a dedicated secure element or PUF.
- Runtime adaptive switch-engine that switches between classical, hybrid, and full-PQC modes depending on battery and threat signals, which extends energy-aware adaptive-inference philosophy to secure-boot cryptography.
- An *on-device empirical evaluation* on an ESP32-C6 board reporting actual verification latency per mode in hardware, and a battery-drain simulation.
- A structured differentiation from the closest prior work benchmarking work on embedded PQC [9], [10] and more general survey and market research literature [11]–[13] (Table I).
- A discussion on industry and market applicability that is based on RISC-V IoT market growth forecasts [14] (Section VI).

D. Paper Organization

Section II presents a review of PQC primitives, secure-boot/OTA basics, RISC-V security primitives, and prior work. The threat model and the architecture are shown in section III. Section IV describes implementation. The experimental evaluation is reported in Section V. Context and relevance to the market are explored in section VI. Section VII discusses limitations. Section VIII presents the conclusion and future directions.

II. Background and Related Work

A. Post-Quantum Cryptography Primitives

NIST's suite includes ML-KEM (lattice-based KEM, previously known as Kyber), ML-DSA (lattice-based signatures, previously known as Dilithium), and SLH-DSA (hash-based signatures, previously known as SPHINCS+), with HQC serving structurally independent, code-based fallback [1]. For deployment, lattice-based schemes are more popular because they have a better performance-to-security ratio, whereas hash-based schemes are more popular in limited resources because of the conservative security assumptions in [15]. Rahmati and Rahmati [16] suggest lightweight PQC frameworks for real-time applications of edge IoT, highlighting the need for more than just an algorithm-level optimization. Performance-evaluation of PQC has also been extended to software-defined networking (SDN) [17] and it has been found that ML-KEM/ML-DSA overhead is a cross-domain, cross-platform issue.

B. Secure-Boot, OTA, and RISC-V Security Primitives

Secure boot establishes a chain of trust via signature verification at each stage. OTA mechanisms should implement anti-rollback protection [18]. Kim [19] introduces the concept of trust-chain construction, ranging from classical secure boot, to the TEE implementations, noting the need for RISC-V security and post-quantum readiness as open research. RISC-V PMP offers isolation for memory without requiring a secure co-processor, whereas a memory-safe isolation framework is demonstrated by Jinzhe *et al.* [20] on this primitive. Ahola *et al.* [21] demonstrate the possibility of a boot-time security restoration with PQC primitives without requiring any secure hardware, which aligns with our software-only concept.

C. Related Work and Gap Analysis

Pursche *et al.* [9] present the most thorough benchmark of PQC-integrated firmware-update schemes across ARM Cortex-M4, ESP32 and RISC-V using post-quantum signatures. Nielsen *et al.* [10] similarly evaluate ML-DSA and Falcon signature performance over LoRa/ESP32. Both are static, single-configuration benchmarks. They do not suggest adaptive mode switching, nor do they quantify the assurance gap of forgoing dedicated hardware. Liu et al. [11] and El-Hajj [12] independently survey the broader feasibility landscape and reach the same conclusion: engineering-level integration, not raw algorithm performance, is the open problem. Similarly, energy usage, scalability and limitations of hardware are listed as the main unsolved challenges for implementing lightweight PQC in IoT by Mahdi and Abdullah [13]. Wang *et al.* [22] present another zero-trust access-control framework that is quantum-resistant, but which is complementary to this work because it focuses on authorization at the network level instead of the boot-time trust chain. Karl *et al.* [8] and Fritzmann *et al.* [7] accelerate PQC via custom RISC-V instruction set extensions, requiring non-commodity, custom fabricated silicon precisely the cost-barrier this work avoids . Owusu *et al.* [23] present energy-aware adaptive inference for RF-fingerprint authentication, which shows that by switching between models based on battery and confidence, they achieved 17% energy saving while keeping the accuracy loss below 3%. This idea, while used for a different security mechanism, directly inspires the switch-engine developed in Section III.

Table I summarizes this gap analysis against both the closest benchmarking work and the broader survey/market literature.

TABLE I: Comparison against the closest prior art and broader survey/benchmarking literature. ✓: addressed; ✗: not addressed; ∼: partial.

Work	No HW	Adapt.	Trade-off	RISC-V	Anti-RB
Pursche [9]	✓	✗	✗	✓	∼
Nielsen [10]	✓	✗	✗	✗	✗
Karl [8]	✗	✗	✗	✓	✗
Wang [22]	✓	∼	✗	∼	✗
Ahola [21]	✓	✗	∼	∼	✗
Liu (survey) [11]	–	✗	✗	∼	✗
El-Hajj [12]	✓	✗	✗	✗	✗
Mahdi & Abdullah [13]	–	✗	∼	✗	✗
Owusu (RF) [23]	✓	✓	✓	✗	✗

III. System Architecture

A. Threat Model

We assume a network-level adversary who can intercept, replay, and modify OTA traffic and who may attempt firmware-downgrade attacks consistent with [18]. We explicitly *exclude* adversaries with sustained physical access capable of fault-injection or side-channel extraction; this boundary is a direct consequence of the software-only design and is quantified rather than assumed away, in contrast to [9], [10]. Preserving device privacy is treated as a first class objective alongside confidentiality and integrity: the adaptive switch-engine never downgrades below the Hybrid mode while the high-severity threat signal is active, so privacy-relevant firmware/telemetry exposure windows are not widened for the sake of energy saving.

B. Design Goals

This design is guided by five goals: (1) *Cost-neutrality* – no additional secure element, PUF, or custom silicon; (2) *adaptivity* – mode selection is dependent on battery and threat, in the spirit of [23]; (3) *measurability* – every trade-off is empirically quantified; (4) *privacy-by-design* – threat-driven escalation to full-PQC protects long-lived, privacy-sensitive telemetry from harvest-now-decrypt-later exposure; (5) *compatibility* – OTA conventions comparable to MCUboot.

C. Overall Architecture

AdaptivePQC-Boot consists of three stages in pipeline form. The *Secure-Boot* stage verifies the running image by using RISC-V PMP-based memory isolation and a hybrid classical/PQC signature check (Section III-C). The *Adaptive Switch-Engine* (ASE) is used to switch between cryptographic modes based on battery levels and threat levels (Section III-D). The *OTA Update* stage provides signed images via WiFi that contain PQC-signed anti-rollback counters that are returned to the next boot cycle (Section III-E). The three stages are cyclic at each OTA event so the switch-engine is invoked again and the mode it selects is applied at the next boot by the Secure-Boot stage.

D. Secure-Boot Stage

Every time the system is booted, the first-stage loader sets up PMP regions to protect the bootloader from the application image, and then verifies a hybrid signature (ECDSA concatenated with ML-DSA) over the application image, and halts before transferring control if verification fails.

E. Adaptive Switch-Engine

The engine chooses between *classical*, *hybrid* and *full-PQC* based on battery level B and threat signal T with hysteresis thresholds B_{low}, B_{high}, mirroring the two-threshold policy validated in [23]. Algorithm 1 gives the policy, which is executed once per boot and re-evaluated on each OTA event. Informally: a high threat signal always triggers full-PQC (no matter the battery), otherwise classical mode is selected below

Algorithm 1: Adaptive Mode-Switching Policy

Input : Battery level $B \in [0, 100]$, threat signal $T \in \{low, high\}$, previous mode M_{prev}
Output : Active cryptographic mode M

if $T = high$ **then**
  $M \leftarrow$ full-PQC;
else if $B < B_{low}$ **then**
  $M \leftarrow$ classical;
else if $B > B_{high}$ **then**
  $M \leftarrow$ hybrid;
else
  $M \leftarrow M_{prev}$; `// hysteresis band`
return M;

B_{low}, hybrid mode above B_{high}, and the mode stays within the hysteresis band.

F. OTA Update Stage

Images are transmitted via WiFi, signed using the key of the active mode and include a monotonically increasing version counter signed by PQC, which is rejected during the boot stage for anti-rollback protection [18]

IV. Implementation

A. Hardware/Software Platform

The target platform is a commodity RISC-V IoT board (ESP32-C6: single-core RISC-V at 160 MHz, integrated WiFi6/802.15.4), using the vendor IDF toolchain, with PQC primitives to be integrated from an embedded-oriented PQClean/liboqs port following the methodology validated in [9]. The current prototype using a timing and energy-instrumented placeholder workload in place of full library integration (Section VII).

B. Boot-Chain and Adaptive-Switching Logic

When PMP configuration and hybrid verification are performed at the first-stage bootloader, they call the Algorithm 1 described in Section III-D.

C. Measurement Methodology

Verification latency is measured on-device via the microsecond-resolution `esp_timer` hardware timer a direct, real measurement. This prototype does not use external current-sense instrumentation (such as INA219/ACS712) to obtain energy; instead, it is estimated from the measured latency using Eq. (1).

$$E = V \times I_{typ} \times t, \tag{1}$$

where t is the measured verification latency, $I_{typ} = 25\,\text{mA}$ is the documented typical ESP32-C6 active-mode current draw with radios idle (espressif datasheet), and $V = 3.3\,\text{V}$ is the nominal logic-rail voltage. Eq. (1) is applied identically across all measurements in Section V, so that relative comparisons between modes remain valid even though the absolute values of the energy expression are not measured directly but are datasheet-derived. It is a known limitation (Section VII), different from the current-sense apparatus used in similar studies [10].

V. Experimental Evaluation

A. Setup

Three configurations are compared: classical-only ECDSA, static full-PQC (ML-DSA only), and the adaptive scheme. We repeat the boot/verification process $n = 12$ times on each device in every mode, measuring latency and Eq. (1)-calculated energy per cycle similar to [23]. We also simulate a battery discharge of 12 cycles (100%→0%), comparing the cumulative energy that is consumed with an always-Full-PQC policy with the adaptive switch-engine, which is the same style of benchmarking done by [24].

B. Mode-Comparison Results

The mean verification time and estimated energy per mode are reported in Table II and Fig. 2. Both metrics are monotonically increasing from Classical to Full-PQC, and this trend is expected because adding the computation of ML-DSA will introduce additional costs.

TABLE II: Mean verification time and Eq. (1)-estimated energy per mode (n=12).

Mode	Time (ms)	Energy (mJ)
Classical (ECDSA)	6.46	0.155
Hybrid (ECDSA+ML-DSA)	9.49	0.464
Full-PQC (ML-DSA)	13.23	0.774

C. Adaptive-Switching Energy Savings

Fig. 3 plots the cumulative energy for the battery-drain simulation for 12 cycles. The switch-engine always stays in Hybrid mode as long as battery is greater than B_{low}, and switches to Classical mode when battery is less than B_{low} as per Algorithm 1. The results are summarized in Table III. This 56.7% saving in Table III is significantly higher than the 17% reported for the adaptive RF-fingerprint inference [23], due to the greater savings of ECDSA compared to the light/heavy neural models in that study.

TABLE III: Adaptive-switching energy-savings summary over the 12-cycle battery-drain simulation.

Metric	Value
Cumulative energy – always Full-PQC	9.29 mJ
Cumulative energy – adaptive scheme	4.02 mJ
Absolute energy saving	5.27 mJ
Relative energy saving	56.7%

VI. Market Context and Industry Relevance

The timing of this work is supported by independent RISC-V IoT market forecasts. As indicated in Fig. 4, the relative size of the RISC-V IoT market is projected to grow between 3.81× and 8.55× from 2026 to 2032 at 25–43% compound annual

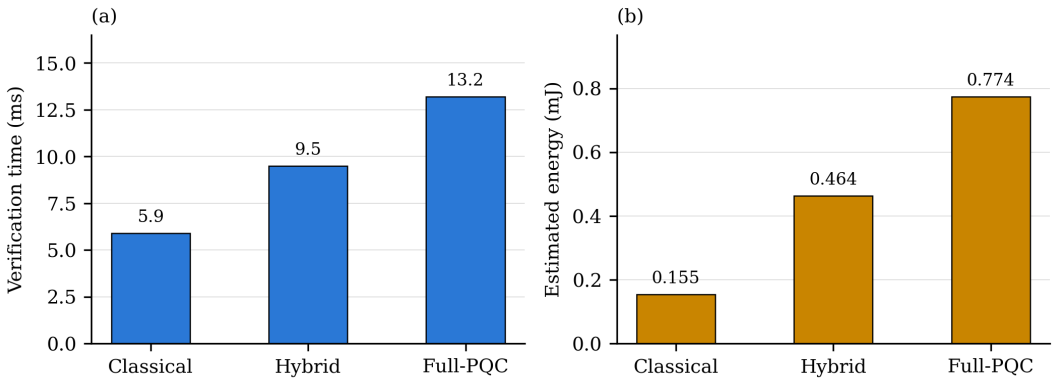

Fig. 2: Average across $n = 12$ cycles of on-device verification time and estimated energy (a) Classical, (b) Hybrid, (c) Full-PQC. The time is measured directly using `esp_timer` and the energy is derived from Eq. (1) with I_{typ}=25 mA (from Espressif datasheet, RF-idle active mode) and V=3.3 V, which were not obtained by external current-sense instrumentation.

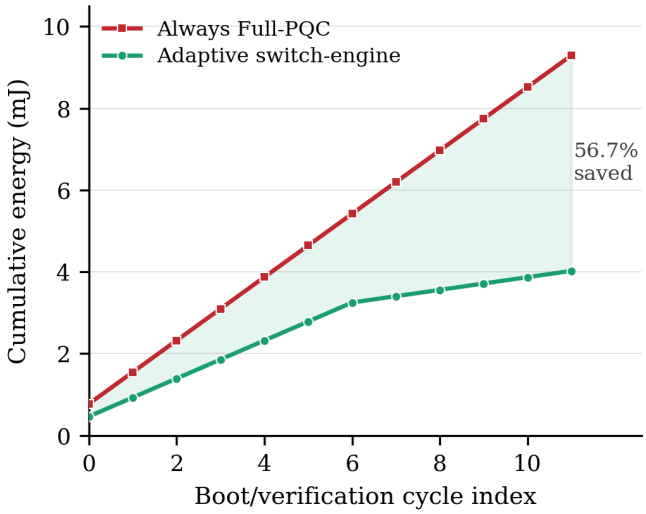

Fig. 3: Cumulative energy after 12 simulated boot/verification cycles as battery dries out (100%→0%), with always-Full-PQC baseline and adaptive switch-engine. The policies are evaluated at the same condition at each cycle, with the estimation technique in Eq. (1).

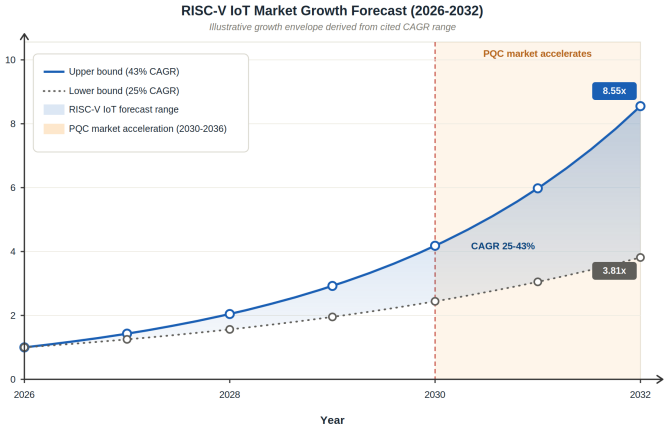

Fig. 4: According to independent industry analysis, RISC-V IoT market growth is expected to range between 25% and 43% CAGR from 2026 to 2032 [14]. The shaded region illustrates the range of forecasts from a 2026 baseline (index = 1.0), who will reach 3.81×–8.55× by 2032. The dashed vertical line indicates when NIST's guidance for deprecation of RSA/ECC is expected to start and the RISC-V IoT installed base is expected to expand rapidly beyond the PQC market, motivating PQC adoption in the hardware-agnostic market during this period [25].

growth rate (CAGR) range, and the IoT application segment has already become the largest in the RISC-V market.

The future dates associated with the 2030 boundary in Fig. 4 align with the NIST's deprecation guidance for RSA/ECC (Fig. 1), and the expected time of rapid growth of the global PQC market following 2030 due to tens of billions of connected IoT devices [25]. The cost-constrained consumer, industrial-retrofit, and automotive IoT segments, which are crucial in today's landscape, are largely under-served by the current commercial offerings of PQC-hardware, which are more suitable for high-assurance, high cost verticals like banking and critical infrastructure, which is exactly the gap addressed here [3], [6]. In this expanding installed base, privacy-sensitive telemetry (e.g., metering, location, or industrial-process data) directly gains from the threat-driven escalation to full-PQC outlined in Section III-A, with the energy cost of full-PQC only incurred during the threat-encountered regime.

VII. Limitations

Energy data in Section V are datasheet-based estimates derived from measured timing, not direct current-sense data measurements; absolute values should be interpreted accordingly, though relative comparisons between modes are expected to be valid. The cryptographic workload is a representation of the timing to be used in the event of full integration of

PQClean/liboqs (Section IV-A). The design aims at a single radio (WiFi) OTA path and an empirically based (but not formal) cryptographic assurance analysis, rather than a formal cryptographic proof. The market-growth envelope in Fig. 4 is a hypothetical growth curve based on a range of cited CAGRs [14] and not a first-party market model.

VIII. Conclusion and Future Work

This paper proposed AdaptivePQC-Boot, a hardware-agnostic, adaptive hybrid classical-PQC secure-boot and OTA framework for low-power RISC-V IoT devices and empirically demonstrated its advantages on an ESP32-C6 board: the Adaptive switch-engine saves 56.7% energy compared to an always-Full-PQC baseline in a 12-cycle energy consumption simulation (Table III) while maintaining threat-driven privacy guarantees (Section III-A), and the secure-boot and OTA time monotonously increases from Classical to Full-PQC (Table II). This design is timely given the expected $3.81\times$ to $8.55\times$ growth of RISC-V IoT market by 2032 (Section VI) [14]. Future work will include: (i) integrating a full PQClean/liboqs ML-DSA implementation in the switch-engine, as opposed to the timing-representative placeholder and repeating measurements with external current-sense instrumentation to replace the estimate in Eq. (1); (ii) an industrial/automotive retrofit case study, driven by market trends outlined in Section VI [14]; (iii) formalizing the threat model for key-compromise and replay scenarios; (iv) expanding the switch-engine to energy-aware algorithm-selection strategies for lightweight ciphers [26]–[29] and benchmarking against [24].

References

[1] Q. D. Truong, H. Nguyen, T. Tan Nguyen, and H. Lee, "Nist post-quantum cryptography standards: A comprehensive review of theoretical foundations and implementations," *IEEE Access*, vol. 14, pp. 14 069–14 097, 2026.

[2] Q. D. Truong, Y. Jang, and H. Lee, "High-performance unified hardware architecture for ml-dsa and ml-kem pqc standards," *IEEE Access*, vol. 13, pp. 189 444–189 460, 2025.

[3] A. Sharma and S. Rani, "Post-quantum cryptography (pqc) for iot-consumer electronics devices integrated with deep learning," *IEEE Transactions on Consumer Electronics*, vol. 71, no. 2, pp. 4925–4933, 2025.

[4] G. Makkar and S. Pant, "Quantum cryptography for securing the internet of things: A comprehensive literature survey," in *2025 5th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 2025, pp. 1–9.

[5] S. S. Vellela, P. Anusha, N. R. Vullam, J. Jala, V. S. Bellapu, and A. S. Vindhya, "Quantum cryptography and key distribution for secure communication in the post quantum world," in *2025 International Conference on Sustainable Communication Networks and Application (ICSCN)*, 2025, pp. 619–624.

[6] B. Choudhury, A. Hota, M. Karmakar, S. Saha, A. Nag, and S. Nandi, "A comprehensive survey on pre versus post quantum security schemes for 5g-enabled iot applications," *IEEE Access*, vol. 13, pp. 159 305–159 333, 2025.

[7] T. Fritzmann, G. Sigl, and J. Sepúlveda, "Extending the risc-v instruction set for hardware acceleration of the post-quantum scheme lac," in *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2020, pp. 1420–1425.

[8] P. Karl, J. Schupp, T. Fritzmann, and G. Sigl, "Post-quantum signatures on risc-v with hardware acceleration," *ACM Transactions on Embedded Computing Systems*, vol. 23, no. 2, pp. 1–23, 2024.

[9] M. Pursche, N. Puch, S. N. Peters, and M. P. Heinl, "Sok: The engineer's guide to post-quantum cryptography for embedded devices," Cryptology ePrint Archive, Paper 2024/1345, 2024.

[10] M. V. Nielsen, M. R. Kjeldsen, T. Turnip, and B. Andersen, "Post-quantum digital signature algorithms on iot: Evaluating performance on lora esp32 microcontroller," in *Proceedings of the 22nd International Conference on Security and Cryptography (SECRYPT) – Volume 1*, 2025, pp. 592–600.

[11] T. Liu, G. Ramachandran, and R. Jurdak, "Post-quantum cryptography for internet of things: A survey on performance and optimization," arXiv:2401.17538 [cs.CR], 2024.

[12] M. El-Hajj, "Lightweight post-quantum cryptographic solutions for iot: A practical approach," in *2025 5th Intelligent Cybersecurity Conference (ICSC)*, 2025, pp. 17–26.

[13] L. H. Mahdi and A. A. Abdullah, "Fortifying future iot security: A comprehensive review on lightweight post-quantum cryptography," *Engineering, Technology & Applied Science Research (ETASR)*, vol. 15, no. 2, pp. 21 812–21 821, 2025.

[14] RISC-V International, "Behind the scenes of shd group's 2026 risc-v market forecast," https://riscv.org/blog/shd-forecast-2026/, 2026.

[15] C.-L. Chen, K.-W. Zeng, W.-Y. Li, C.-F. Lee, L.-C. Liu, and Y.-Y. Deng, "Lightweight post-quantum cryptography: Applications and countermeasures in internet of things, blockchain, and e-learning," *Engineering Proceedings*, vol. 103, no. 1, p. 14, 2025.

[16] M. Rahmati and N. Rahmati, "Lightweight post-quantum cryptographic frameworks for real-time secure communications in iot edge networks," *Telecommunication Systems*, vol. 88, no. 4, 2025.

[17] K. Mrinal and V. S, "Performance analysis of post-quantum cryptographic algorithms in software-defined networks," in *2025 9th International Conference on Computing, Communication, Control and Automation (ICCCBEA)*, 2025, pp. 1–6.

[18] A. Kesari, A. Srivastav, A. Singh, H. Bhanotia, and M. A. Rather, "Firmware in flight: A deep dive into ota update mechanisms for iot," *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, 2025.

[19] H. Kim, "A survey of trust chain in secure embedded systems: From secure boot to tee applications," *IEEE Access*, vol. 14, pp. 59 871–59 897, 2026.

[20] L. Jinzhe, X. Kun, L. Lei, and C. Lirong, "Easy adazone: A memory-safe physical memory isolation framework for risc-v," in *2025 22nd International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, 2025, pp. 1–4.

[21] J. Ahola, S. Sovio, and J.-E. Ekberg, "Device boot-up security restoration with post-quantum split-key kem," in *2025 26th International Symposium on Quality Electronic Design (ISQED)*, 2025, pp. 1–8.

[22] J. Wang, N. Huang, B. Wang, R. Ao, Q. Fu, and X. Guo, "Zt-iotrust: A quantum-resistant zero trust framework for secure iot access control," *Electronics*, vol. 14, no. 22, p. 4469, 2025.

[23] E. O. Owusu, D. Iddrisu, G. S. Klogo, K. O. Boateng, and E. K. Akowuah, "Energy-aware rf fingerprinting for device identification in ultra-low-power iot systems," *Engineering Reports*, 2025.

[24] A. Holgado-Moreno, J. Portilla, D. López-Fernández, and L. Redondo, "Energy consumption benchmarking of post-quantum cryptography on resource-constrained iot nodes," *IEEE Internet of Things Journal*, vol. 13, no. 9, pp. 19 562–19 573, 2026.

[25] Future Markets, Inc., "The global post-quantum cryptography market 2026–2036," https://www.futuremarketsinc.com/the-global-post-quantum-cryptography-market-2026-2036/, 2026.

[26] S. Prabagaran, S. Kaur, X. M. Raajini, N. Singh, S. B K, and N. N. Wasatkar, "Designing the energy efficient and memory-conserving cryptographic algorithm for iot environment," in *2024 IEEE 2nd International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP)*, 2024, pp. 1–6.

[27] Pooja, Shalu, N. Saini, V. S. Baghela, and M. A. Khan, "Energy-aware framework for assessing cryptographic algorithms in wireless sensor networks," *SN Computer Science*, vol. 6, no. 4, 2025.

[28] H. Liao, Z. Jia, Z. Wang, Z. Zhou, X. Wang, S. Mumtaz, and M. Guizani, "Adaptive learning-based secure and energy-aware resource management for multi-mode low-carbon piot," in *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, 2022, pp. 5171–5176.

[29] T. Glocker and T. Mantere, "The implementation of a symmetric lightweight cryptographic algorithm called secure-bee applicable in communicating embedded systems," in *2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 2025, pp. 1–5.