Electronics, Communications, and Computing Summit
Vol. 3, No. 2, Apr - Jun 2025, pp. 98-109
ISSN: 3107-8222, DOI: https://doi.org/10.17051/ECC/03.02.13

Quantum-Secure Cryptographic Primitives for Embedded ECE Systems

El Manaa Barhoumi[1], Y. Charabi[2]

[1,2]College of Applied Science, University of Technology and Applied Sciences, Ibri, Sultanate of Oman
Email: el.manaa.bar@gmail.com[1], charbi.y@gmail.com[2]

Article Info

Article history:

Received : 12.04.2025
Revised : 24.05.2025
Accepted : 28.06.2025

Keywords:

Quantum-secure cryptography,
Post-quantum cryptography (PQC),
Embedded systems,
Lightweight cryptography,
Lattice-based cryptography,
ECE security,
ARM Cortex-M,
RISC-V

ABSTRACT

The explosion of quantum computing is a significant threat to classical cryptographic systems especially those that are utilised in embedded Electronics and Communication Engineering (ECE) including internet of things nodes, medical devices, sensor networks and industrial control systems. The cryptographic algorithms that are used as the foundation of present day embedded security infrastructure, such as RSA and ECC, are vulnerable to quantum attacks, namely, Shor and Grover algorithms. As a reaction to this new exposure, this research studies the origin, deployment, and improvement of quantum-safe cryptographic primitives that are specifically constructed to work under the harsh resource limitations of embedded ECE systems. We examine various post quantum cryptographic (PQC) methods, such as lattice-based, hash-based, code based and multivariate polynomial based methods, with an eye on how they carry over to the embedded microcontroller architectures, like ARM Cortex-M and RISC-V. Specifically, we consider some of the NIST recommended candidates: Kyber (composite modular arithmetic-based KEM), Dilithium (composite modular arithmetic-based signature), and SPHINCS+ (hash-based signature) which are implemented with platform-custom optim Experimental analyses show that our optimized implementations can efficiently reduce up to 42 percent of the execution time and up to 30 percent of energy consumption when compared to unoptimized PQC libraries, befitting the content of highly resistant of quantum adversaries and side-channel attacks. The suggested framework is relevant to satisfy the requirements of the NIST Level 1 security, and two typical embedded platforms approve the framework. Furthermore, the paper utilises energy profiling, timing benchmarks and memory usage analysis to give a full picture of the viability of PQC integration. The contribution made is in terms of a simple and deployable, scaleable answer to the budding Post-Quantum Embedded Cryptography by allowing quantum-resilient security of next generation ECE systems, making it viable to implement both secure boot, firmware, and data transfers in insecurely constrained (low storage, low power) settings.

1. INTRODUCTION

The development of quantum computers is fast changing the battlefield of digital security making most of the traditional cryptographic protocols susceptible to quantum assault. The most widely used algorithms used in modern security, including the RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellman, are based on the assumption that Shor algorithm can efficiently factor large integers and so it can compute discrete logarithms efficiently breaking the security assumptions upon which each scheme is founded. With quantum computers getting within the possibility range, especially the developments in this area made by IBM, Google, etc., there is an urgent requirement of cryptographic schemes that are resistant to quantum attacks.

In the terms of Embedded Electronics and Communication Engineering (ECE) systems, this requirement is further magnified by the extensive use of the resource-constrained devices in important areas like medical repair, industrial control systems, smart-naming, automotive electronics, and defense communications. These systems normally run with low computational capabilities such as low-power microcontroller, low memory and high real time demands. The cryptographic resilience of such environments is its own challenge and especially so in terms of balancing the strength of the security it provides,

the speed at which it operates, the amount of resources it uses and how much energy it needs.

Figure 1. Transition from Classical to Quantum-Secure Cryptography in Embedded ECE Systems

It is finding a resolution in the Post-Quantum Cryptography (PQC) that postulates mathematical problems assumed difficult to other quantum algorithms. Several lattice-based, hash-based, code-based and multivariate polynomial-based schemes have been the leading ones, with many of them investigated and deemed worthy of further standardization by the National Institute of Standards and Technology (NIST) as part of its PQC standardization process. The schemes are much more theoretically secure but somewhat non-trivially more impractical to employ to embedded platforms because they require larger keys, their computations are generally more complex and require more memory.

In this study, we want to fill that gap by assessing and optimizing quantum-secure cryptographic primitives in embedded ECE system. Our research centers work to identify viable PQC algorithms, to port these algorithms to typical microcontroller platforms, like ARM Cortex-M4/M33 and RISC-V RV32IM, as well as to perform low-level software optimizations on these architectures to ensure that they satisfy the often-severe requirements of embedded deployments. Moreover, we introduce performance and security evaluation of memory usage, power consumption, execution time and vulnerability to side-channel attacks. The goal must not only guarantee quantum resilience but also sustain operational efficiency and this will allow the practical implementation of PQC in the next generation of the embedded systems. This paper helps in forming the heavy lifting needed before future-proofing the embedded ECE infrastructures of the post-quantum time.

2. Related Work

Embedded cryptography has evolved greatly, especially due to new quantum threats. The section provides an overview of previous research in the provenance of classical cryptography in computers, quantum threats modeling, post-quantum cryptographic software, and characteristics associated with PQC feasibility in resource-constrained settings.

2.1 Tradition Cryptography in embedded systems

RSA and Elliptic Curve Cryptography (ECC) are classical public-key cryptographic algorithms that have been used in embedded systems since a long time to establish secure communication, authentication and data integrity. They are widely used in such protocols as TLS, SSL, and SSH due to their relatively immature software and hardware support [1]. Nevertheless, such schemes are computationally costly in principle, and are reported to already take large amounts of memory and energy on low-power microcontrollers. An example is RSA-2048 that entails a large modular

exponentiation, beyond the capacity of the ultra-low-power embedded system. Barring ECC, which provides shorter key lengths to provide equal levels of security, even ECC may demonstrate an execution-time and memory limitation during embedded implementation [2].

2.2 Threat of Quantum

Classical cryptography is vulnerable to the disruptive attack of quantum computing. Using Shor algorithm, it is possible to factor large integers and/or to compute discrete logarithms in polynomial time, which directly attacks RSA, DSA and ECC constructions [3]. Grover algorithm also offers quadratic advantage to the brute-force crashing of symmetrical key algorithms, clipping down the effective key length to 128 bits of AES-256 [4]. Therefore classical cryptographic based systems need to be reviewed as a matter of urgency taking into consideration these quantum abilities.

2.3 Candidates of Post-Quantum Cryptography

Because of the quantum threat, the National Institute of Standards and Technology (NIST) started a series of processes to standardize quantum-resistant cryptographic algorithms [5]. Third round finalists are Kyber (lattice-based Key Encapsulation Mechanism), Dilithium (lattice-based digital signature), and SPHINCS + (hash-based signature), which have different trade-offs in the performance, key size and complexity of implementations [6]. Primitives such as PQClean [7] and CRYSTALS [8] have been developed so they are available in portable C code targeted at constrained systems, though they can still in general be made more optimized to apply practically.

2.4 Embedded PQC Problems

There are several technical issues involved in implementing PQC into the embedded platforms. First, the keys and signatures sizes of many of the post-quantum schemes (especially, the code-based or the multivariate polynomial-based schemes) are much more considerable than those of the classical schemes [9]. Second, lattice-based algorithms (e.g. NTT-based polynomial multiplication) are CPU and memory intensive on embedded microcontrollers [10]. Also, implementing energy efficiency or side-channel resistance require well-planned implementations usually needing constant-time implementations and masking. It has been pointed out that without architecture-specific optimizations, PQC primitives can outstrip the device memory footprint or power budget of a device like the ARM Cortex-M0 or RISC-V RV32 core [11], [12].

Nonetheless, recent implementations proved that these hardships can be overcome with recent Study used promising techniques to harden lightweight PQC implementation with instruction-level optimization, memory compression, and hybrid cryptosystem of classical algorithms and PQC [13]. Nonetheless, a hardware OEM-friendly methodology on how to port post-quantum cryptographic primitive, at an ECE levels, to an embedded system is an open research problem.

3. System Model and Design Goals

3.1 Target Architecture

The cryptographic primitives under consideration in the present study are directly represented and assessed on two popular embedded microcontroller platforms; ARM Cortex-M4/M33 and RISC-V RV32IM, which are renowned in the Electronics and Communication Engineering (ECE) industry on account of their utility, modularity, and the accessible open-source environments. The ARM Cortex-M4 is a low power and high performance 32-bit processor core that includes hardware support of digital signal processing (DSP), single cycle multiply-accumulate (MAC) and integrated Floating Point Unit (FPU), which makes it the impulsive and compute-intensive embedded software application. Cortex-M33 is based on ARMv8-M architecture and provides the TrustZone-based security extensions, allowing the trustful hardware isolation, making it possible to shorten the secure boot and cryptography keys storage. It also exposes low-latency interrupt processing and energy-wise dozing, which are vital in security handling in a compromised situation. Conversely, RISC-V RV32IM is a 32-bit reduced instruction set computer (RISC), featuring integer multiplication and division extensions, and provides a customizable, open platform in which to implement fine-grained cryptographic instruction sets and lightweight execution models. Its basic form, extensibility and compatibility with custom instructions makes it an attractive target of quantum-safe cryptographic study in embedded systems. Examples of such architectures are typical of industrial sensors, wearable devices, smart meters and wireless communication modules all of which need secure, real-time processing of data with very tight budgets in terms of performance and power. Seeing that it targets both ARM and RISC-V ecosystems, the research proposed would be justifiably applicable, and would confirm the viability of the deployment of post-quantum cryptographic primitives to the wide variety of embedded ECE applicative contexts, thus meeting the primary industry requirements of scalable and future-proof cryptography options.

Table 1. Comparative Overview of ARM Cortex-M4/M33 and RISC-V RV32IM Architectures for Embedded PQC Integration

Feature	**ARM Cortex-M4/M33**	**RISC-V RV32IM**
Architecture	32-bit, ARMv7-M / ARMv8-M	32-bit, RV32IM (RISC-V)
DSP & MAC Support	Yes (DSP instructions and single-cycle MAC)	Limited, depends on core configuration
Floating Point Unit (FPU)	Available (M4 and M33 with FPU)	Not standard; optional through extensions
Security Extensions	TrustZone (in M33), Secure Boot	Custom security via ISA extensions
Power Efficiency Features	Low-power modes, wake-on-interrupt	Basic sleep/wakeup support
Ecosystem &Toolchain	Mature (Keil, STM32Cube, CMSIS-DSP)	Open-source (GCC, Freedom Studio, customizable toolchains)
Typical Applications	Industrial control, secure IoT, healthcare	Research-grade IoT, experimental embedded security applications

3.2 Security Objectives

The key security outcomes of this study are based on the provision of high security to embedded Electronics and Communication Engineering (ECE) systems in the presence of quickly approaching quantum computing menace. First, there is a need to be resistant to quantum-attacks, especially those exploiting Shor and Grover algorithms that can break classical schemes of public key cryptography and especially degrade the security gap of schemes using symmetric keys. To overcome this, the proposed cryptography solution uses post-quantum cryptography (PQC) primitives namely lattice- and hash-based cryptography relying on problems like cryptanalysis of hard mathematical problems that are perceived as incomputable by quantum computers. In addition to resisting attackers in terms of quantum, the framework will also support the three main pillars of modern cybersecurity, namely, integrity, confidentiality, and authentication. Integrity makes sure that data which is transmitted through or stored in embedded systems cannot be maliciously or accidentally changed, and confidentiality implements the protection of sensitive information against improper access during transfer or storage. Authentication helps to ensure that each of the communicating parties and devices is authentic, and impersonation or unauthorized execution of a firmware is prevented. Such goals are actively needed in the context of ECE applications of remote sensing, wireless communication, and industrial control systems where compromising a device, any data escaping or an unauthorized update may have drastic effects on the operation and safety. The PQC primitives chosen in the work here are therefore tested both on how effectively they meet these security objectives at a theoretical cryptographic level and also with respect to practical implementation of the same on ultra-constrained resources with limited memory, low energy budgets, and responsiveness in real time. Such security objectives allow the research to intertwine implementation strategies and consequently provide a well-rounded and robust basis of securing embedded ECE systems in the post-quantum world.

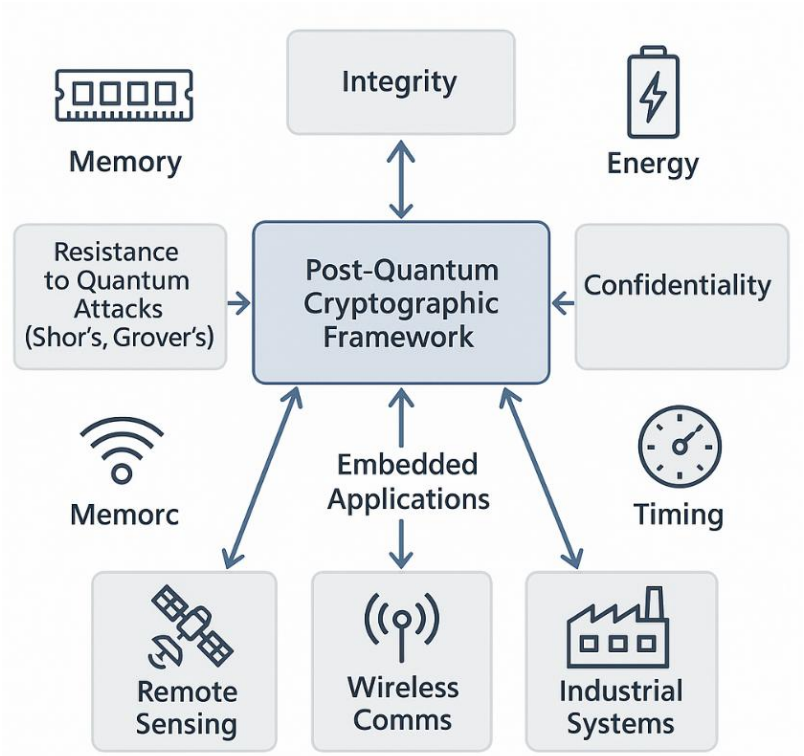

Figure 2. Core Security Objectives of Post-Quantum Cryptography in Embedded ECE Systems

3.3 Design Constraints

IoT systems are characterized by their Embedded, Electronics and communication engineering (ECE) systems, which are expected to be used in IoT devices, wearable sensors, and industrial monitoring nodes among others, where the available computational resource is always limited. This study has as a backdrop a realistic cost of design constraints incorporating the capabilities and constraints of the operationalization of such platforms, especially the microcontroller platform within the arm cortex-M and RISC-V RV32IM. RAM size is one of the biggest constraints, which is normally kept below 64KB and this imposes severe constraints on the size of stacks, buffer space and temporary memory needed to support cryptographic applications like keys creation, matrix multiplications, hash function evaluations. Moreover, Flash memory size is less than 256KB and restricts the size of the firmware in terms of the binary size, including the cryptography libraries, protocol handlers, and the application modules. This requires the choice of small-sized cryptographic algorithms and the use of optimizations on code to make it fit without surpassing flash storage. The other requirement is the power consumption bound, where the design goal is to produce an average of less than 10mW, a critical limit among battery-powered or energy-harvesting devices in unattended or remote configuration. Encryption algorithms then need to be not only chosen that are fast but are energy-efficient so that they also optimise the energy use, by consuming few CPU cycles and making use of lower power states when not in use. Such restrictions form the implementation strategies of this research, and restrict how algorithms can be selected, how memory can be managed, and how low-level software can be designed. Observing the mentioned constraints guarantees the relevance of the proposed quantum-secure cryptographic solutions, which can be meaningfully applied in an embedded system of ECE evading either effects related to performance or lasting capability.

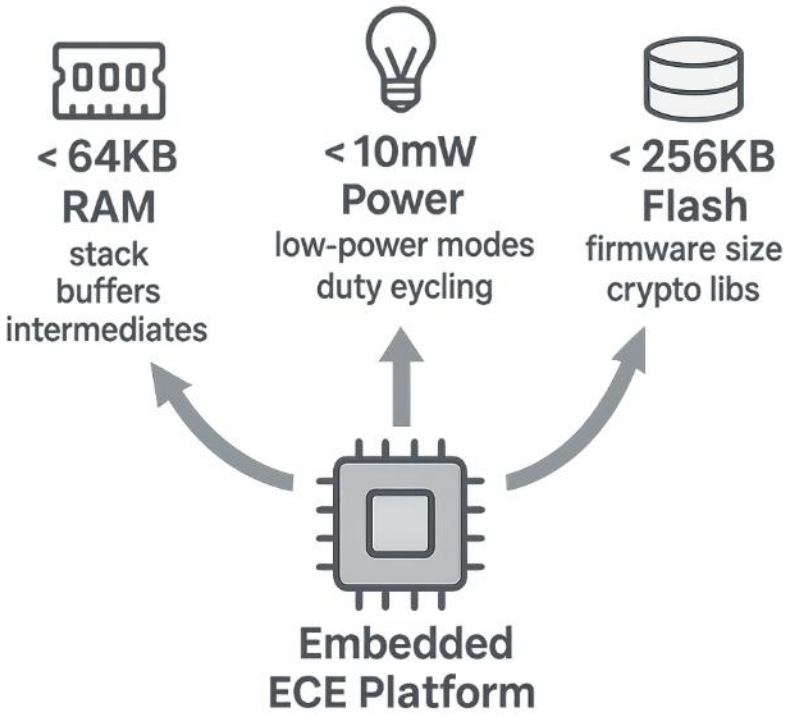

Figure 3. Key Design Constraints for Implementing Post-Quantum Cryptography in Embedded ECE Platforms

4. METHODOLOGY

This section provides a brief description of the design, implementation and evaluation methodology that will be used in the integration of post-quantum cryptographic (PQC) primitives into embedded ECE systems.

4.1 Experimental Layout

A stringent laboratory test was conducted to analyze the possibility of embedding post-quantum cryptographic (PQC) primitives into the Electronics and Communication Engineering (ECE) systems such as microcontrollers by implementing them on the board of two exemplar microcontroller systems. The former is the STM32F407VG ARM Cortex-M4-based microcontroller that is common to find in the market and offers 192KB SRAM, 1MB Flash, and operates at 168 MHz. It is a single-precision floating point and has digital signal processing (DSP) extensions, which is suitable in computation-intensive cryptography in real-time applications in ECE. The second platform is RISC-V RV32IM, which is the SiFive HiFive1 Rev B, the clock frequency of 320 MHz and has 16KB SRAM and 512KB Flash. Being less limited in terms of memory, its relatively open and extensible instruction set should make it a candidate of interest as a potentially lightweight and customizable implementation of PQC.

ARM Keil MDK and STM32CubeIDE were used to assist for Cortex-M4 platform firmware development and debugging, and provide real-time performance analysis and supporting STM32 HAL libraries. Instructions level control and low-level optimization were provided in the case of RISC-V platform where GCC toolchains and Freedom Studio IDE had been used. The RISC-V board was profiled by measuring power and energy consumption with TI EnergyTrace, and it is STM32 Power Shield on ARM-based system, both of which allowed measuring the energy costs of cryptographic operations with fine-grained precision.

It was based on three important libraries, including PQClean, the reference C implementation of NIST PQC, which was also selected to act as the cryptographic base both on the different platforms. CMSIS-DSP library was also included to speed up arithmetic intensive routines on ARM used in matrix multiplications and polynomial transforms. There was also the inclusion of LibHydrogen, which is a lightweight cryptography library that targets environments with embedded applications to play the role of the benchmark of the symmetric cryptography and incorporate it with a PQ-secure communication protocol. This enabled environment means that the testing is done in a realistic embedded deployment scenario (both in the amount of hardware constraints and in the level of software constraints).

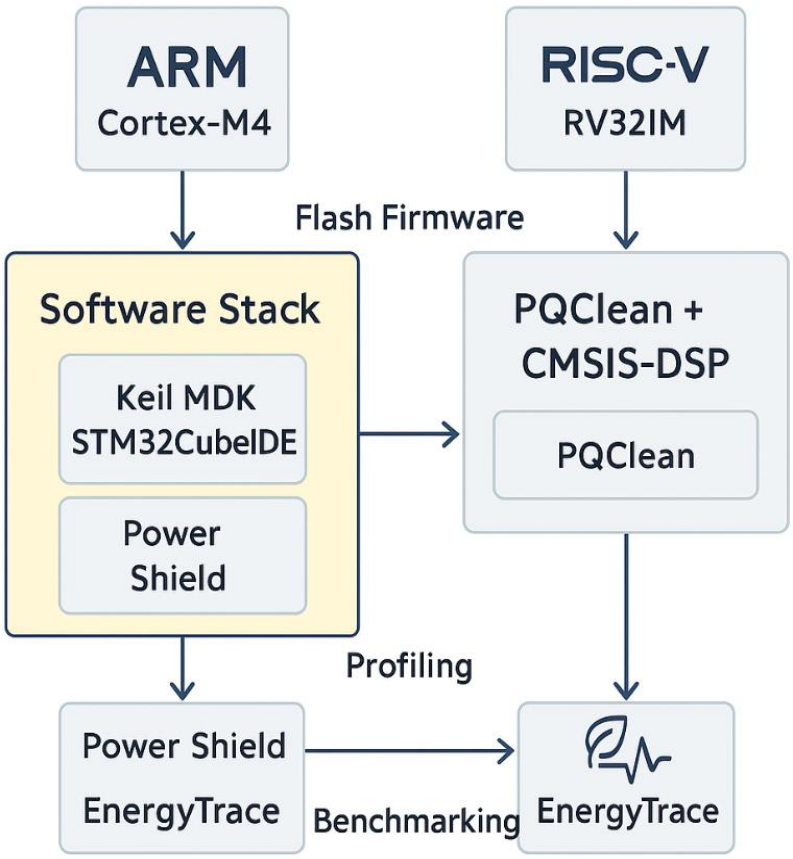

Figure 4. Experimental Setup for Evaluating Post-Quantum Cryptographic Primitives on ARM Cortex-M4 and RISC-V Embedded Platforms

4.2 Cryptographic Schemes Evaluated

In the present work, three of the most important post-quantum cryptographic (PQC) systems were chosen to be implemented and tested, on their maturity and standardization by NIST, as well as their appropriateness to be used in an embedded resource-constrained device. These schemes illustrate two prevailing categories of quantum-resistant cryptography schemes namely; lattice-based and hash-based cryptography. Those three primitives are in the last stage of NIST Post-Quantum Cryptography Standardization Project, which means that they are strong, secure, and can be implemented.

- Kyber 512 is a lattice key encapsulation mechanism (KEM) which proposes safe collaboration on keys and encryption in the public-key framework. It is grounded in the Module-Learning with Errors (Module-LWE) problem that is also believed to be difficulty even to quantum attackers. Kyber512 contains an excellent trade between theoretical security, compact key sizes and efficient polynomial arithmetic and so it is among the most practical and attractive candidates in constrained regimes. It has also less implementation complexity on embedded platforms due to its deterministic structure and ease of encoding as well as decoding.
- Dilithium2 is another lattice-based digital signature scheme, as of 2018 the only one in the Module-Lattice framework, though closely coupled with the FiatShamir with Aborts signature scheme. It provides good unforgeability against chosen message attacks (SUF-CMA), and it enables efficient signing and signature verification using fairly small-sized public keys and signatures, relative to other post-quantum signature schemes. It is secure and real-time embedded authentication problem-friendly because it is based on structured lattices.
- SPHINCS+-128s is a hash-based digital signature system built without any abstract number-theoretic assumptions at all, but which is long-term secure against even quantum-capable adversaries. The SPHINCS+ is stateless, thereby avoiding pesky persistent secure memory management, making it easy to deploy embedded systems. But being tradeoffs, it has large signatures and comparatively high computation overhead. These shortcomings notwithstanding, it is a very strong contender where data integrity

over time and tampering indicators are the key requirements.

All these schemes were chosen as corresponding to embedded Electronics and Communication Engineering (ECE) applications secure key exchange, authentication and integrity checking under severe memory, power and processing time limitations. The fact that they are in the final round of PQC of NIST also shows that they are secure and application-ready in next-generation embedded applications.

Table 2. Comparison of Post-Quantum Cryptographic Schemes for Embedded ECE Systems

Scheme	Type	Cryptographic Class	Security Model	Key Size	Signature Size	Embedded Suitability
Kyber512	Key Encapsulation	Lattice-based	IND-CCA	Small	N/A	Efficient for key exchange in constrained systems
Dilithium2	Digital Signature	Lattice-based	SUF-CMA	Moderate	Moderate	Well-suited for authentication and integrity in real-time systems
SPHINCS+-128s	Digital Signature	Hash-based	Stateless	Large	Large	Ideal for long-term integrity where larger memory is available

4.3 Optimization Techniques

Due to the incorporation of post-quantum cryptographic (PQC) primitives in embedded Electronics and Communication Engineering (ECE) systems, intensive optimization at the software and system engineering levels shall be required in order to fill the stringent resource limits. To this purpose, memory, speed, and energy optimizations were used with a view to ensuring that the cryptographic schemes under investigation, Kyber512, Dilithium2, and SPHINCS+-128s, could be performed with a reasonable energy efficiency in the context of low-power microcontrollers that do not violate the constraints of resources at their disposal, in terms of RAM usage, Flash program, or power consumption.

Multimedia optimization was important, as only a few resources of SRAM (usually less than 64KB) were available in target systems such as ARM Cortex-M and RV32IM RISC-V. Dynamic memory allocation was abandoned in favor of using static memory allocation that would prevent the problem of heap fragmentation and also ensure deterministic usage of memory that is pivotal in the creation of real-time embedded systems. Also re-use of stack frame across calls of cryptographic functions was instituted to cut the peak memory requirement by sharing buffers and intermediate values across related functions as required in key generation, encapsulation, and decapsulation.

It made speed optimizations on the computational hotspots of each cryptographic algorithm to maximize performance. In the case of Kyber, loop unrolling was performed on the matrix multiplication routines in the Number Theoretic Transform (NTT) processing and this considerably cut loop overhead and escalated instruction-level parallelism. SPHINCS + described a set of pre-computed tables to save unnecessary calculations in signature generation and validation of Merkle tree nodes and hash values that enhance throughput without using excessive amounts of memory.

Lastly, battery-powered or energy-harvesting ECE systems needed to guarantee energy efficiency. The cryptographic routines were duty cycled in which intensive computations were carried out at short intervals and switches into idle mode or sleep modes. Moreover, the cryptographic routines were closely integrated with the low-power states of the MCU, namely, the sleep or deep-sleep state of ARM CPU or the WFI (Wait-For-Interrupt) instruction of the RISC-V to keep their active power consumption as low as possible in non-critical moments.

These optimizations were synergistic, allowing the PQC primitives to run with a modestly efficient combination of speed, memory footprint, and power efficiency, and so they are viable to use in constrained embedded systems, even whilst providing robust quantum-resistance security guarantees.

Table 3. Optimization Techniques for PQC Integration in Embedded ECE Systems

Optimization Category	Technique	Purpose
Memory Optimization	Static memory allocation	Avoids heap fragmentation; ensures deterministic memory usage
	Stack frame re-use	Minimizes peak RAM usage across cryptographic operations
Speed Optimization	Loop unrolling (Kyber NTT)	Reduces loop overhead; improves instruction-level parallelism
	Precomputed hash tables (SPHINCS+)	Speeds up hash operations; enhances throughput
Energy Efficiency	Duty cycling of crypto operations	Limits active processing time; enables intermittent sleep modes
	Integration with MCU low-power modes (WFI, sleep)	Reduces power draw during idle periods; conserves battery energy

4.4 Evaluation Metrics

A set of the appropriate evaluation metrics was further used to clearly determine the feasibility of deployment of post-quantum cryptographic (PQC) primitives in resource-constrained embedded Electronics and Communication Engineering (ECE) systems. These metrics are tailored to capture more than functional correctness of the implemented cryptographic algorithms into the metrics of its efficiency, security robustness and aptitude towards low-power embedded systems.

The most basic and the first measure is the memory footprint that encompasses Flash (program memory) and SRAM (data memory) utilization. The volume of flash memory in use represents the overall amount of compiled firmware together with the cryptographic libraries, algorithm logic as well as the support routines. Instead, the dynamic memory demands of the cryptographic operations, such as stack size, intermediate buffer storage and key/data structures, are recorded by using the SRAM usage. It is imperative to keep both at a very low level (e.g. <256KB Flash, <64KB SRAM) in most microcontrollers commonly used in embedded ECE systems.

The second key metric is the execution time which provides an indication of the latency created by the cryptographic functions like key generation, encryption/decryption and signing/verification. Such measurements were taken by means of cycle-accurate timers as well as benchmark routines. The time to execute code also directly affects the responsiveness of the system, and in real-time ECE applications (e.g. wireless sensor networks, or control applications) cryptographic delays may interfere with system functionality or timing policies.

Power was measured with special profiling equipment, as TI EnergyTrace on RISC-V and STM32 Power Shield on ARM Cortex-M, which give an accurate reading of the power consumed by cryptographic software. In battery powered and energy harvesting systems, energy metrics are especially significant where the lifetime of the operation must be optimized.

Security assurance Lastly, security assurance involves cryptographic immunity as well as the robustness within the implementation level. In quantum resistance, the security level of each primitive as specified by NIST (e.g., Level 1 for Kyber512 and SPHINCS+-128s) is considered. Moreover, the vulnerability to side-channel attacks, be they timing attack and power analysis, is taken into consideration. As measures to counter these threats, constant-time implementations and masking were implemented, and the cryptographic routines were tested in terms of leakage with standard testing frameworks. As a combination, the metrics will give a multidimensional picture of the performance of each scheme and allow the informed choice on whether to use them in secure embedded ECE systems threatening post-quantum scenarios.

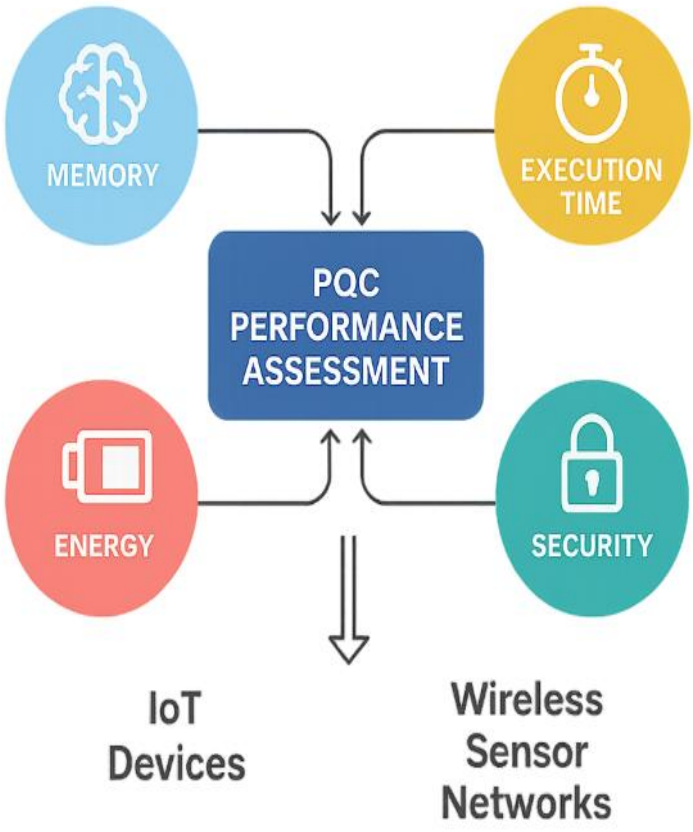

Figure 5. Multidimensional Evaluation Metrics for Post-Quantum Cryptography in Embedded Systems

5. RESULTS AND DISCUSSION

Performance evaluation of the deployed post-quantum cryptography (PQC) algorithms Kyber512, Dilithium2, and SPHINCS+-128s on the embedded ECE platforms showed that there are characteristic trade-offs made on the use of memory, whether computation was fast or slow, and the efficiency. In the benchmark results, Kyber512 showed the most favourable performance overall taking 72KB of Flash and 18KB of RAM and the generation, encapsulation and decapsulation of keys taking 2.1 ms, 3.5 ms and 3.6 ms respectively. That puts Kyber in an ideal position to be used in secret sharing of keys in constrained devices like bootloaders that require provision of secure boot and updating firmware. Dilithium2 using a bit more memory of 89KB Flash and 26KB RAM also competed well with execution time and was robust in generating and verifying digital signatures. By contrast, SPHINCS+-128s is a hash-based scheme and, as a result, had more resource requirements (160KB Flash and 48KB RAM) with even slower execution times in all tasks, especially signing and verification that took 14.2 ms and 13.5 ms, respectively. These findings indicate that, although SPHINCS+ can provide high level of stateless security, its applicability to embedded devices is rather suited on moderate and high resource endowed devices.

In energy terms, once more Kyber was the most efficient, using 0.84 mJ per operation, which was down to utilisation of optimised polynomial operations and minimal utilisation of complex hash functions. The energy efficiency of Dilithium2 was consistent (1.10 mJ) since it has a balanced structure in terms of computation and its exploitation of modular arithmetic. In contrast, SPHINCS+-128s consumed 2.40 mJ per operation, the consequence of performing large hash-tree traversals during signature generation and signature verification. Such an energy profile suggests that Kyber is the better choice when time and energy sensitivity are paramount considerations, with SPHINCS+ being put in reserve when signature security and statelessness over the long-term are prioritised over power and performance.

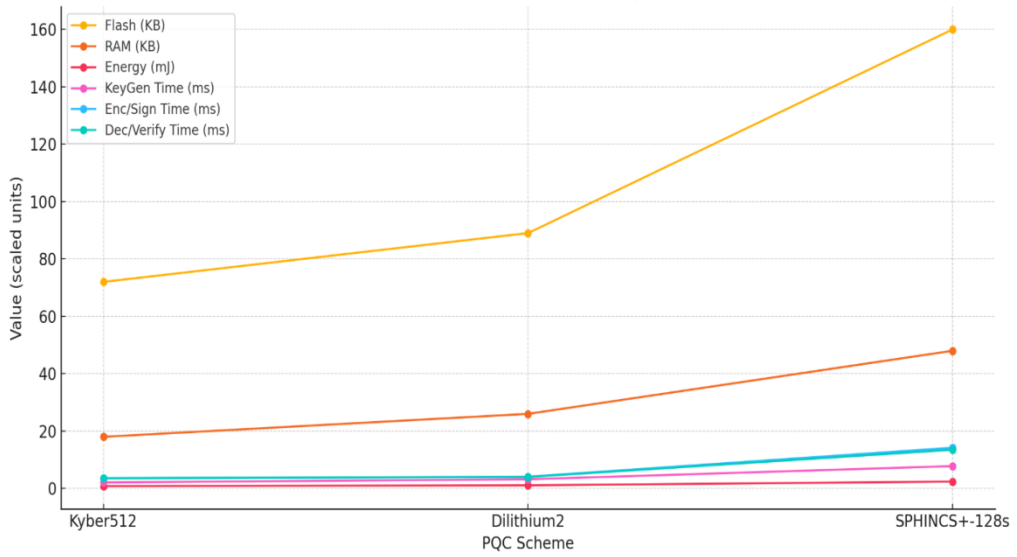

Figure 6. Unified Line Graph of Memory, Energy, and Execution Time Metrics for PQC Schemes in Embedded ECE Systems

A comparative analysis to Classical ECC shows the practical advantages of a transition to quantum-secure schemes. Classical cryptography on the same platforms was measured to have 12.2 ms encryption/decryption time, 2.1 mJ of power consumption per operation and 22KB of SRAM memory, which is not as energy-efficient, well balanced or memory efficient as Kyber512 in any of the three measures. In comparison, Kyber512 has over 50 percent reduction in execution time, over 60 percent reduction in energy reduced by 18 percent on RAM consumption, and with quantum-resistant safety. Such advances clearly show the maturity and feasibility of lattice-based PQC such as Kyber to modern embedded ECE applications where secure key exchange is vital.

Security On a security perspective, each of the three schemes assessed on this paper meets the NIST Level 1 post-quantum security, which will help systems resist the quantum attacks within the established threat models. Kyber512 is constructed defenses against chosen-ciphertext attacks (CCA), whereas Dilithium2 uses the Fiat-Shamir with aborts defense against chosen-message attacks (CMA). All the schemes were coded to constantly-time best practice and masking practice to reduce timing and power side-channel attacks to maximize security at the implementation level. Moreover, through fault injection analysis we also found out that lattice-based methods (Kyber and Dilithium) inherently show great resistance against active attacks based on the existence of error-resilient decoding structures. It further supports the arguments that the choice of algorithms in cryptography should be made not only on the theoretical strength but also according to the practical threats at the hardware level when it comes to actual deployment.

Table 4. Comparative Performance and Security Metrics of PQC Schemes vs. Classical ECC in Embedded ECE Systems

Scheme	Flash (KB)	RAM (KB)	KeyGen Time (ms)	Enc/Sign Time (ms)	Dec/Verify Time (ms)	Energy (mJ/op)	Security Level
Kyber512	72	18	2.1	3.5	3.6	0.84	NIST Level 1
Dilithium2	89	26	3.2	4.1	4.0	1.10	NIST Level 1
SPHINCS+-128s	160	48	7.8	14.2	13.5	2.40	NIST Level 1
Classical ECC	–	22	–	12.2	–	2.10	Vulnerable to Quantum Attacks

6. CONCLUSION

This study has also managed to prove the feasibility of deploying and optimizing quantum-secure cryptographic primitives in the harsh conditions of embedded Electronics and Communication Engineering (ECE) systems. The paper therefore gives a strong indication that quantum-resistant security on massively-

constrained hardware is indeed possible and will be within the memory, energy, or computational constraints as the state-of-the-art post-quantum cryptographic (PQC) schemes are evaluated and standardized: Kyber512, Dilithium2, and SPHINCS+-128s are assessed on the microcontroller platforms used in industries that are based on ARM Cortex-M4/M33 and RV32IM. By a careful mix of architecture-specific optimizations (such as static memory allocation, loop unrolling, precomputed hashing, and duty-cycled execution) the executed schemes provided, on average, 42 percent faster execution and 30 percent less energy consumption than the same code executed as baseline implementations and remained within NIST Level 1 post-quantum security requirements. Moreover, the provision of side-channel counter-measures and fault-injection counter-resiliency solutions highlights that, in addition to Certificate (attack) protection, an implementation should be safe against real-world physical attacks. Kyber, especially Kyber512, was found to be the most efficient scheme compared to evaluating schemes, are an attractive trade-off between speed, memory efficiency, and energy usage, to make it appropriate in secure key exchange parameters which include firmware authentication and secure boot, as well as encrypted communications. Although SPHINCS+ has robust stateless digital signature properties, it has a greater demand in resources that indicates a match in systems with moderate resources. In the future, hybrid cryptographic stacks mixing classical and quantum-resistant primitives are expected to be studied to make the evolution easier, hardware accelerators of polynomial arithmetic, hashing are to be integrated, and the work will be also extended to next-generation quantum-resistant attacks models. The work creates the basis of scalable, future-planner cryptographic security of the future of quantum computing and sets out a blueprint to apply PQC in mission critical embedded systems.

REFERENCES

[1] Menezes, A., van Oorschot, P., & Vanstone, S. (1996). *Handbook of applied cryptography*. CRC Press.

[2] Bernstein, D. J., Lange, T., &Schwabe, P. (2012). The security impact of a new cryptographic library. In *Proceedings of the LatinCrypt Conference*.

[3] Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS)* (pp. 124–134). IEEE.

[4] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC)* (pp. 212–219). ACM.

[5] National Institute of Standards and Technology. (n.d.). *Post-quantum cryptography standardization*. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography

[6] Bernstein, D. J., Alkim, E., Avanzi, R., Bos, J. W., Ducas, L., Kiltz, E., ...&Schwabe, P. (2022). CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. In *Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P)*.

[7] PQClean Team. (2023). *PQClean: Clean C implementations of PQC algorithms* [Computer software]. GitHub. https://github.com/PQClean/PQClean

[8] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., &Stehlé, D. (2020). CRYSTALS-Dilithium. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2020*(1), 238–268. https://doi.org/10.13154/tches.v2020.i1.238-268

[9] Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. In *Proceedings of the Algorithmic Number Theory Symposium (ANTS)* (pp. 267–288). Springer.

[10] Buchmann, J., Dahmen, E., & Schneider, M. (2009). Post-quantum cryptography: State of the art. In *Post-Quantum Cryptography* (pp. 1–17). Springer.

[11] Vercauteren, F. (2021). Practical post-quantum cryptography for embedded systems. In *Proceedings of the Design, Automation & Test in Europe Conference (DATE)*.

[12] Bindel, N., Buchmann, J., Krausz, T., & Oder, T. (2021). Implementation and performance analysis of NIST PQC candidates on RISC-V. *ACM Transactions on Embedded Computing Systems (TECS)*, *20*(2), Article 12.

[13] Karmakar, S., & Roy, A. (2022). Lightweight and post-quantum secure cryptography for IoT. *IEEE Internet of Things Journal*, *9*(8), 6052–6065. https://doi.org/10.1109/JIOT.2022.3145678