Iraqi Journal of Computers, Communications, Control and Systems Engineering
Journal homepage: https://ijccce.uotechnology.edu.iq

A Review of Post-Quantum Digital Signature Schemes Applicability and Performance in Various Environments

Marwa M. Hamood[1,*], Arwa A. Moosa[2]

[1]Department of Computer Engineering, College of Engineering, Al-Iraqia University, Baghdad, Iraq.
[2]Department of Networks and Cybersecurity Engineering, College of Engineering, Al-Iraqia University, Baghdad, Iraq.
[1] marwa.m.hamood@aliraqia.edu.iq, [2]arwa.amir@aliraqia.edu.iq

DOI: https://doi.org/10.33103/uot.ijccce.25.2.4

HIGHLIGHTS

- Comprehensive of review of post-quantum digital signature schemes across diverse platforms.
- -Analyzes suitability of post-quantum schemes for real-world applications like IOT and secure communication.
- -Identify research gaps and challenges for deployment for high bandwidth-sensitive systems.

ARTICLE HISTORT

Received: 17/ March /2025

Revised: 18/ May /2025

Accepted: 01/ July /2025

Available online: 30/ October /2025

Keywords:
Communication Environment, Optical Fiber, Performance Evaluation, Post Quantum Digital Signature Algorithms.

ABSTRACT

The emergence of quantum computers, coupled with relentless advancements in technology, calls for the immediate transition from classical to modern cryptography for efficient data transfer across optic fibers. This paper assesses different proposed post-quantum signature schemes pertaining to their plausibility of being useful against quantum computers' capabilities. The ability of quantum computers to solve mathematical equations at speeds significantly faster than those of classical computers is remarkable. Existing cryptographic frameworks that depend on discrete logarithms and integer factorization are seriously threatened by this exceptional efficiency. In order to protect sensitive data in a post-quantum world, it may be necessary to reevaluate existing encryption techniques as the introduction of quantum computing has the potential to seriously compromise the security of many popular cryptographic systems. Hence, during the post-quantum epoch, the implementation of cryptographic measures to safeguard the confidentiality, integrity, and authenticity of all data amid the challenges instigated by quantum computers is an undertaking that must be addressed tactically and strategically. This document endeavors to depict the state-of-the-art methodologies in post-quantum cryptography outlining lattice, hash, code, and multivariate polynomial lattice-based schemes. By discussing their advantages, disadvantages, and implementation hurdles, this work seeks to educate academics and industry experts about the steps that must be taken to safeguard digital communications in the age of quantum technology.

I. INTRODUCTION

Digital signature schemes based on Public Key Infrastructure (PKI) currently rely on hard mathematical problems, such as discrete logarithms [1] or integer factorization mathematical problems [2]. However, with the rapid technological advancements, these traditional methods are becoming increasingly vulnerable. Quantum algorithms have the potential to solve these cryptographic problems exponentially faster than classical computers methods, posing a significant threat to existing security protocols. This emerging quantum vulnerability has led to a growing field of research knowing as Post-Quantum Cryptography (PQC). A new class of cryptographic algorithms designed to secures digital communications against quantum attacks. The National Institute of Standards and technology (NIST) is leading efforts to standardized PQC solutions to ensure strong information security in the quantum era. In this paper, examining the readiness of post-quantum digital signatures for security data across different environments. It provides an in-depth analysis of the third-round NIST PQC digital signature candidates [3], focusing on key sizes and computations efficiency. Among the selected algorithms Dilithium [4], Falcon [5], and SPHINCS+ [6] each offers unique trads-offs in terms of key size, ciphertext size and signature size, making them suitable for different use cases. Given the diverse performance and efficiency requirement across various systems, tailored cryptographies solutions may be necessary, especially in resource-constrained environments. The transition from classical cryptography to PQC presents several challenges, particularly compatibility, due to fundamental algorithmic differences. Quantum computers process computational capabilities that surpass classical computer in solving specific cryptographic problems [7]. As a results, adapting to post-quantum security frame works is essential to safeguarding digital infrastructures against further threats.

II. LITERATURE REVIEW

Extensive research has been conducted on digital signature algorithms of post-quantum cryptography, aiming to assess existing developments and will evaluate the key features that define this emerging field. The following studies provide a comprehensive understanding of a current advancements in quantum-resistant cryptographic techniques, emphasizing critical aspects such as security, efficiency, and practical implementation. The security and effectiveness of post-quantum digital signature algorithms have been extensively tested across various environments and domains. Researchers have explored different approaches to optimize these algorithms to ensure their feasibility in real-word applications. This literature review synthesizes recent finding on post-quantum digital signature schemes, focusing on their performance, security and applications in different contexts. To provide a structure overview, this review is organized into the following key categories:

A. ***Performance Analysis of Post-Quantum Algorithms-*** Evaluating computational efficiency, signature size, and key generation times.
B. ***Hardware Implementation and Optimization –*** Investigating practical deployment on different hardware architectures.
C. ***Security and Vulnerability Analysis –*** Examining resistance against classical and quantum attacks.
D. ***Standardization and Practical Application –*** Reviewing efforts by organizations like NIST to establish cryptographic standards.
E. ***Resource-Constrained Environments –*** Assessing the feasibility of post-quantum digital signatures in low-power or embedded systems.

By analyzing these aspects, this review aims to highlight the strengths and limitations of current post-quantum digital signature algorithms and their potential for widespread adoption in secure communication systems.

A. Performance Analysis of Post-Quantum Algorithms

Extensive research has been conducted on post-quantum digital signature algorithms, particularly those evaluated as part of the National Institute of Standards and Technology (NIST) standardization. One such study by **Filip Opiłka and colleagues (2024)** [8] analyzes performance of post-quantum digital signature algorithms using the liboqs library running on a Linux Debian virtual machine which compares post-quantum algorithms with the traditional RSA algorithm. Their findings highlight that Dilithium outperforms others in key generation as well as signing process. It is worth noting that Dilithium5, despite imposing a low time cost when processing larger files, proves to be a strong candidate for RSA substitution. Similarly, researchers **Marin Vidaković et al. (2023)** [9] conducted comparative analysis of Crystals-Dilithium, Falcon and SPHINCS+ on Cortex M4 and Intel Core i5-8259U CPUs. The researchers found that Dilithium is significant for low power, Falcon signature verification is faster and SPHINCS+ is generally secure but computationally expensive. Additionally, to this, **Shuzhou Sun et al. (2020)** [10] explored the parallelization of SPHINCS+, achieving 5152 signatures per second on a GeForce GTX 1080 GPU and demonstrating its applicability to high-demand applications such as social media websites. Furthermore, **Erdem Alkim et al. (2020)** [11] introduced qTESLA, a lattice-based signature scheme that offers simplicity and robust security assurances, even though its utilization of Fourier sampling methods renders it challenging to implement. These studies are summarized in in Table I, providing a deeper understanding of the trade-offs in post-quantum digital signatures. The table highlights the methods used, key findings, and strengths and weakness of each contribution.

B. Hardware Implementations and Optimization

The implementation of post-quantum algorithms on hardware platforms has also been addressed in more recent research. **Georg Land et al. (2021)** [12] analyszed the performance of Dilithium on Field-Programmable Gate Arrays (FPGAs) with significant area-time trade-offs improvements for key generation and signing processes. Their research indicates the suitability of Dilithium in low-cost and high-throughput applications. Similarly, **Quang Dang Truong et al. (2024)** [13] introduced a high-speed low-latency hardware implementation of the Module-Lattice Digital Signature Algorithm (ML-DSA), with the best latency among FPGA-based hardware. The results of their findings highlight the beneficial practicability of using ML-DSA in post-quantum digital signature schemes**.** Additionally, **Michael Schmid et al. (2023)** [14] presented the first hardware implementation of Falcon on a Zynq UltraScale+ FPGA, obtaining competitive performance for key generation and signing but with higher resource usage compared to other implementations. While, **Naina Gupta et al. (2023)** [15] developed the smallest CRYSTALS-Dilithium implementation on Zynq FPGAs, with significant area-time trade-off improvements for embedded systems. The summary of these hardware implementations, including key methods, results, and trade-offs, is presented in Table II.

C. Security and Vulnerability Assessments

Security remains a principal and critical axiom in the assumption of post-quantum algorithms. **Daniel Smith-Tone et al. (2020)** [16] investigated vulnerabilities in the Rainbow signature scheme, proposing better methods to prevent Rainbow Band Separation (RBS) attacks. Their study proposes increasing Rainbow's parameters for enhanced security, though this could impact performance. Also**, Keshav k.et al. (2023)** [17] investigates how to improve healthcare systems by integrating blockchain and quantum technologies. It demonstrates how these technologies can enhance safe data storage. Adoption is hampered by implementation issues and infrastructure needs, though. Additionally, **Alvaro Cintas Canto et al. (2023)** [18] examined implementation attacks against NIST's PQC competition winners, pointing towards the insufficiency of algorithmic security and vulnerability of cryptographic algorithms to Side-Channel Attacks (SCA). Their results confirm the need for robust countermeasures against SCAs to enhance the security of PQC algorithms. A summary of these security and vulnerability assessments, including key finding and proposed solutions, is provided in Table III.

D. Standardization and Practical Applications

The standardization of post-quantum algorithms is a critical area of ongoing research. **Oleksandra Tsentseria et al. (2023)** [19] evaluated the global standardization process, and it was found that additional research is required in order to transition to quantum-safe standards. **Dr. Manish Kumar (2022)** [20] contrasted the feasibility of utilizing quantum-safe algorithms based on benchmarking criteria from the Open Quantum Safe (OQS) project, and stressed the need for fundamental protocol and hardware adjustments. In practical usage, **Joppe W. Bos et al. (2022)** [21] demonstrated Dilithium is usable in car network processors with minimal collision at boot time despite increasing installation times. **Yong-Hua Yang et al. (2021)** [22] achieved high-efficiency quantum security authentication in a city QKD network using the lattice-based Aigis-Sig algorithm, optimizing network topology and reducing cost. Table IV provide a summary of these standardization efforts and practical implementations.

E. Resource-Constrained Environments

The efficiency of post quantum digital signature algorithms in resource-constrained environments such as Internet of Things (IoT) devices has also been explored. **Matthias J. Kannwischer et al. (2024)** [23] validated NIST's other post-quantum signature contenders on Arm Cortex-M4 microcontrollers, emphasizing the significance of proper benchmarking targeted to embedded devices. Similarly, post-quantum algorithms on Raspberry Pi 4 devices are referenced by **Gregory Fitzgibbon et al. (2024)** [24]**,** who offer important details regarding their viability in Internet of Things settings. **Purvi Tandel et al. (2024)** [25] introduced a lightweight hash-based post-quantum signature scheme for IoT devices, which achieves optimal memory consumption on Raspberry Pi platforms. **Tao Liu et al. (2024)** [26] explored optimization methods for post-quantum algorithms for IoT applications, suggesting the need for further research into resource constraints. A summary of resource-constrained environments shown on Table V.

III. EMERGE DRIFT AND PROSPECTS

Additional investigation has revealed gaps and arising trends in post-quantum cryptography. Yuexi **Xu et al.** (2024) [27] gave a comprehensive review of verification techniques for post-quantum cryptography, showing the necessity of closing the gap between theoretical constructions and real implementations. **Ritik Bavdekar et al.** (2022) [28] discussed issues and future direction in post-quantum cryptography, highlight the need for summery cryptography for IoT devices and look at new mathematical approaches. Based on other studies listed in Table VI, this review highlights important findings, spots trends, and suggests future directions.

IV. IMPORTANT RESULT

A. Performance of Post-Quantum Algorithms:

- **Dilithium** all the time come out as a strong candidate for digital signatures, showing high performance in key generation and signing processes.
- **SPHINCS+** is specified for its efficiency in signature verification but has slower performance in other areas compared to competitors.
- **Falcon** is recognized for its unique advantages in specific contexts, such as IoT applications.

B. Benchmarking and Implementation:

- Studies bring out the importance of benchmarking PQC algorithms, particularly in resource-constrained environments like microcontrollers and IoT devices.
- Performance metrics are critical for evaluating the applicability of these algorithms in real-world scenarios, with many implementations lacking the needed quality.

C. Integration Challenges:

- Transitioning to PQC requires significant adjustments in existing systems, protocols, and hardware, suggesting that a continuous approach may be necessary.

- The complexity of integrating PQC into traditional systems like TLS is noted, with performance impacts being a significant approach.

D. Security weak point:

- Several studies address the weakness associated with PQC implementations, especially relative to side-channel attacks and fault injection.
- The essential for robust countermeasures against implementation attacks is highlighted, indicating that algorithmic security alone is not enough.

TABLE I. SUMMARY OF TRADE-OFFS IN POST-QUANTUM DIGITAL SIGNATURES

Title	Author	Objectives	Method	Results	Discussion & Conclusions	Strongest	Weakness
Performance Analysis of PQC Algorithms for Digital Signature	Filip Opiłka et al./2024	The paper aims to conduct a comprehensive performance analysis of various post-quantum cryptographic algorithms due to their specific use in digital signatures	The paper utilized the liboqs library for conducting the performance tests on a VMware-based virtual machine running Linux Debian, with comparison tests against the RSA algorithm	The findings indicate that Dilithium excels in the signing and key generation processes, while SPHINCS+ excels at signature verification. Notably, Dilithium5 proves to be a viable alternative to RSA with some time overhead.	The paper concludes that Dilithium5 is the most suitable for digital signatures because of its level of performance and small signature size compared to other algorithms. However, particular application requirements should determine the choice of the algorithm.	Dilithium5 is more efficient in key generation and signing and has smaller signature sizes than SPHINCS+.	It is somewhat slower in signature verification than some of its counterparts and incurs a time overhead over RSA with larger file sizes.
Performance and Applicability of Post-Quantum Digital Signature Algorithms in Resource-Constrained Environments	Marin Vidaković et al./2023	The article is a comparative examination of the Crystals-Dilithium, Falcon, and Sphincs+ digital signature algorithms based on key performance indicators.	The study involved the comparison of execution speed on the Cortex M4 and Intel Core i5-8259U CPU.	The results indicate that Dilithium is more amenable to low-power use cases, Falcon offer higher-speed signature verification, and Sphincs+ offer good security but at higher computational costs. computational demands.	All algorithms have their own merits based on specific demands of deployment contexts; Dilithium and Falcon are deemed more suitable for IoT application, while larger signature size of Sphincs+ may render it less desirable for extremely resource-constrained environments.	Dilithium is said to be simple to implement, while Falcon provides shorter signatures.	Sphincs+'s slower speed and larger signature sizes could make it more difficult to implement in environments with limited resources.
Efficient Parallelism of Post-Quantum Signature Scheme SPHINCS	Shuzhou Sun et al/2020	This work seeks to accelerate the signing speed of SPHINCS, a stateless, quantum-resistant hash-based signature scheme, that now only generates a few hundred signatures per second.	The article presents highly parallel and optimized implementation of SPHINCS on multi-core platforms, starting with a baseline implementation on x86/64 processors and extending to GPUs	The implementation achieves a throughput of 5152 signatures per second on a GeForce GTX 1080, with a 7.88 speedup over recent FPGA implementations, with further gains on TITAN Xp GPUs	The findings indicate the optimized implementations provide significant improvement in throughput with tolerable latency, which makes SPHINCS viable for high-demand environments like social media websites	The parallel implementations significantly enhance the efficiency of SPHINCS, which enables it for high-throughput environments	The complexity of the implementation could be higher due to the need for GPU resources and optimization approach
The Lattice-Based Digital Signature Scheme qTESLA	Erdem Alkim et al/2020	The article presents qTESLA, a family of post-quantum digital signature schemes offering simplicity and strong security guarantees against quantum adversaries, with inherent side-channel and fault attack protection	using about 300 lines of C code only AVX2-optimized assembly implementations are also provided with a factor of 1.5 speedup	The results indicate that qTESLA boasts strong security features while maintaining a compact codebase, which makes it suitable for various applications	the use of Fourier sampling methods' complexity and floating-point arithmetic support makes implementation cumbersome, especially in devices lacking such support, complicates protection against side-channel and fault attacks	The scheme's simplicity and strong security guarantees make it an attractive option for post-quantum applications	The use of complicated methods could be the reason for potential limited adoption due to complications in implementation

TABLE II. SUMMARY OF HARDWARE IMPLEMENTATIONS

Title	Authors	Objectives	method	Results	Discussion & Conclusions	strongest	weakness
A Hard Crystal - Implementing Dilithium on Reconfigurable Hardware	Georg Land et al.2021	This article aims to analyze the performance of lattice-based cryptography within low-cost and high-throughput configurations	The work presents FPGA implementations for Dilithium and evaluates their performance metrics	The research achieved significant improvements in area-time trade-offs for key generation and signing processes.	The findings demonstrate that the proposed design is suitable for low-cost and high-throughput applications, enhancing the practicality of Dilithium in various contexts	The design efficiently utilizes hardware resources for the Dilithium algorithm	Implementation complexity may increase for certain configurations.
Efficient Low-Latency Hardware Architecture for Module-Lattice-Based Digital Signature Standard	Quang Dang Truong et al.2024	This paper presents an efficient low-latency hardware architecture for the (ML-DSA).	The research involved designing flexible arithmetic and hash modules tailored for ML-DSA, emphasizing efficient operation scheduling	The study achieved the best latency among FPGA-based implementations of ML-DSA.	The findings underscore the practical applicability of the proposed architecture for digital signature cryptosystems in the post-quantum era.	The architecture achieves low latency and high efficiency in digital signature operations	Specific hardware configurations may be required to optimize performance
Lightweight Hardware Accelerator for Post-Quantum Digital Signature CRYSTALS-Dilithium	Naina Gupta et al.2023	This work reports the smallest implementation of CRYSTALS-Dilithium, a finalist candidate for post-quantum digital signatures, aiming to optimize its performance for embedded applications.	The implementation leverages parallelism, pre-computation, and memory access sharing, fitting into one of the smallest Zynq FPGAs. Evaluations were conducted on three different hardware platforms, comparing results with software implementations	The design achieves improvements of about 36.7%, 35.4%, and 42.3% in Area×Time (LUTs×s) trade-off for KeyGen, Sign, and Verify operations respectively over state-of-the-art implementations. On ASIC using TSMC 65nm technology, the design occupies 0.227mm² and operates at 1.176 GHz, requiring 53.7µs, 96.9µs, and 57.7µs for KeyGen, Sign, and Verify operations in the best-case scenario	The results demonstrate the feasibility of deploying CRYSTALS-Dilithium in resource-constrained environments, highlighting the potential for practical applications in embedded systems. Further optimizations could enhance performance, making it a viable choice for post-quantum security in various applications	The implementation's small footprint and efficiency make it suitable for embedded applications requiring post-quantum security	The complexity of optimizations may increase the design time and implementation challenges.
Falcon Takes Off - A Hardware Implementation of the Falcon Signature Scheme	Michael Schmid et al.2023	This publication describes the first hardware implementation for Falcon signing and key generation, aiming to evaluate its performance on FPGA platforms.	The implementation on a Zynq UltraScale+ FPGA, and measures latency and throughput for signing and key generation processes.	H/W for signing requires 45,223 LUTs, 41,370 FFs, and 182 DSPs, achieving a signature in 8.7 ms. Key generation takes 320.3 ms with higher resource requirements.	Falcon as a viable candidate for post-quantum signature, demonstrating its efficiency compared to CPU implementations.	promising performance for embedded devices, enhancing Falcon in real-world scenarios	Higher resource demands may limit deployment options in constrained environments

TABLE III. SUMMARY OF SECURITY AND VULNERABILITY ASSESSMENTS

Title	Authors	Objectives	Method	Results	Discussion & Conclusions	strongest	weakness
Rainbow Band Separation is Better than we Thought	Daniel Smith-Tone et al.2020	This paper aims to improve methods for solving the Rainbow Band Separation attack.	The research presents an enhanced method for solving RBS systems using a modified Extended Linearization strategy.	The study recommends increasing parameters for Rainbow to enhance its security against RBS attacks.	The findings highlight the necessity for adjustments in Rainbow's parameters to ensure resilience against emerging cryptographic threats.	The research enhances the understanding of cryptographic weaknesses associated with Rainbow	Performance may suffer as a result of the suggested parameter increases.
Demystifying Quantum Blockchain for Healthcare	Keshav k.et al.2023	Analyze the importance of blockchain and quantum technologies in healthcare systems for data acquisition, monitoring, and security.	Literature review and comparative analysis of existing technologies and their applications in healthcare.	Quantum blockchain can enhance security, privacy, and efficiency in healthcare data management and patient monitoring.	The integration of quantum computing with blockchain can revolutionize healthcare by ensuring data integrity and accessibility.	Innovative application of quantum technologies in healthcare.	Challenges in implementation and the need for robust infrastructure.
Algorithmic Security is Insufficient: A Comprehensive Survey on Implementation Attacks Haunting Post-Quantum Security	Alvaro Cintas Canto et al.2023	it explores implementation attacks targeting NIST's PQC competition winners, emphasizing the insufficiency of algorithmic security and the vulnerabilities of cryptographic algorithms to Side-Channel Attacks (SCA)	The study reviews various types of SCAs, including passive differential power analysis (DPA), active differential fault analysis (DFA), and deep-learning-based SCAs, highlighting their implications for PQC	The findings underscore the need for robust countermeasures against SCAs to enhance the security of PQC algorithms, providing insights into current advancements and challenges	The research calls for a comprehensive approach to securing PQC against implementation attacks, emphasizing the importance of addressing both theoretical and practical vulnerabilities	This survey provides a thorough examination of the vulnerabilities associated with PQC implementations.	The focus on implementation attacks may overlook other significant aspects of cryptographic security

TABLE IV. SUMMARY OF STANDARDIZATION AND PRACTICAL IMPLEMENTATIONS

Title	Authors	Objectives	Method	Results	Discussion & Conclusions	Strongest	Weakness
THE STATE OF STANDARDIZATION OF POSTQUANTUM CRYPTO-ALGORITHMS AT THE GLOBAL LEVEL	Oleksandra Tsentseria et al.2023	The aim of the research is to analyze the actual process of post-quantum cryptographic algorithm standardization.	Research was conducted using the PRISMA model, reading existing literature on quantum cryptography and computing	The results provide insight into algorithms' status while they are transitioning to quantum-proof standards.	The study concludes that there is not yet any known quantum algorithm to replace existing cryptographic systems entirely today; further research and development are needed	The study emphasizes the ongoing process of post-quantum cryptographic algorithm standardization	The timeline of implementation of change in standards remains uncertain
PQC Algorithm's Standardization and Performance Analysis	Dr. Manish Kumar.2022	he aim of this analysis is to determine the feasibility of utilizing quantumresistant cryptographic algorithms.	Performance analysis was done by leveraging the benchmarking statistics of the Open Quantum Safe (OQS) project on AWS.	Results indicate that there needs to be a significant shift in protocols and hardware towards quantum-resistant algorithms	the study emphasizes that transitioning to quantum-resistant cryptography will require significant modifications in a number of systems and may even be difficult for existing infrastructures.	This paper highlights the need to prepare for future quantum attacks on cryptographic systems	The shift may pose significant challenges to current systems and protocols.
Post-Quantum Secure Boot on Vehicle Network Processors	Joppe W. Bos et al.2022	This paper examines the practical implications of PQC deployment on vehicle network processors	the study entailed developing a low-memory fault attack-resilient implementation of Dilithium signature verification algorithm	The results indicate negligible impacts on boot time regardless of increased installation time due to signature verification processes.	The findings show that switching to a post-quantum secure boot is feasible while maintaining an achievable installation latency.	This work demonstrates the feasibility of adding PQC to real-world systems	Installation times may increase when transitioning to post-quantum secure boot processes.
All Optical Metropolitan Quantum Key Distribution Network with PQC Authentication	YONG-HUA YANG et al.2021	The purpose of this study is to achieve high-efficiency quantum security authentication of QKD using the lattice-based post-quantum digital signature algorithm Aigis-Sig, demonstrating its excellence in simplifying the MAN network structure and new user entry.	The metropolitan QKD network of the Jinan field included 14 user nodes and 5 optical switching nodes, verifying the feasibility and excellence of the PQC algorithm and the excellence of substituting trusted relays with optical switching.	The QKD system used was acommercial unit with polarization encoding on the decoy-stateBB84 protocol and a secret key rate of 10 kbps at 10 dB channel loss. Integration of the PQC with ARM chip of QKD simplified the authentication process.	Replacement of trusted relay: an optical switch simplified the network topology, reduced security dependence on the trusted relay, reduced construction cost, and improved interoperability between QKD nodes.	The method eliminates the vulnerability of pre-sharing symmetric keys, providing quantum-resistant security.	Implementational complexity of optical switches may prove to be difficult in certain environments

TABLE V. A SUMMARY OF RESOURCE-CONSTRAINED ENVIRONMENTS

Title	Authors	Objectives	Method	Results	Discussion & Conclusions	Strongest	Weakness
pqm4: Benchmarking NIST Additional Post-Quantum Signature Schemes on Microcontrollers	Matthias J. Kannwischer et al.2024	The goal of this paper is to measure the performance and appropriateness of NIST's additional post-quantum signature contenders on Arm Cortex-M4 microcontrollers.	PQC Algorithm's standardization and performance analysis	The findings highlight the importance of intensive benchmarking of post-quantum cryptographic schemes that are designed for embedded platforms, noting issues of quality in the majority of submissions.	Future work would involve substituting existing implementations with better ones.	This paper emphasizes the relevance of performance benchmarking in PQC embedded implementations.	Various implementations were found to be substandard in terms of required quality and efficiency.
Constrained Device Performance Benchmarking with the Implementation of Post-Quantum Cryptography	Gregory Fitzgibbon et al.2024	the study aims to provide quantitative handshake and benchmark performance for post-quantum algorithms on IoT devices	The study involved testing on Raspberry Pi 4 hardware to simulate existing IoT environments, compared to previous benchmarking results	The results compiled post-quantum algorithm performance measures on constrained devices and described their applicability in real-world use	The results indicate the necessity of performance benchmarks in low-resource environments, pointing to the necessity of using post-quantum algorithms in real-world use	This study illuminates key insight into post-quantum algorithm performance in IoT use	hardware limitations can constrain the generalizability of the study.
Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization	Tao Liu et al.2024	The researcher canvasses literature regarding the performance of post-quantum cryptography on resource-constrained devices in a bid to gauge the scope of challenges that emanate	The paper discusses recent suggestions for optimizing post-quantum cryptography for constrained environments	The research indicates trends and research gaps in existing research, offering an outline of directions for future work in the utilization of optimized post-quantum cryptography for IoT	The paper emphasizes the urgency of optimizing post-quantum cryptography for use in IoT, setting the foundation for future innovation in this field	This research offers a full overview of the optimization of post-quantum cryptography	The scope can be narrowed to specific algorithms, missing out on other advancements.
Secure Authentication Framework for IoT Applications Using a Hash-Based Post-Quantum Signature Scheme	Purvi Tandel et al.2024	A real-world client-server deployment case for IoT applications is presented where the application of hash-based post-quantum digital signatures is emphasized	Demonstration of model structure is made using Raspberry Pi 3 and Pi 0 as servers supported by ESP32 as client systems with a memory usage optimization rate of 32.83%. The results of the proposed architecture to facilitate post-quantum signatures in IoT systems and its potential scalability and robust security.	The results demonstrate the effectiveness of the proposed architecture in integrating post-quantum signatures into IoT systems, highlighting the potential for scalability and robust security.	The suggested architecture can support 256 users and further optimizations in lightweight operations to improve speed and lower memory usage, making it a template for a variety of IoT applications.	The addition of post-quantum signatures brings enhanced security to IoT usage	The design may be further enhanced in a bid to address best performance and memory problems.

TABLE VI. A SUMMARY OF FUTURE DIRECTIONS BASED ON OTHER STUDIES

Title	Authors (Year)	Key Findings	Comparative Analysis	Synthesis & Future Implications
Formal Verification Techniques for Post-Quantum Cryptography: A Systematic Review	Yuexi Xu et al.2024	- Focus on formal verification. - Quantum-resistant protocols.	**Similarity**: Both papers emphasize NIST standards. **Difference**: Xu focuses on verification, Bavdekar on lightweight crypto.	**Trend**: Growing need for standardization. **Gap**: Lack of real-world implementation studies.
Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research	Ritik Bavdekar et al.2022	- NIST standardization. - Lightweight crypto for IoT.	**Overlap**: Both stress NIST's role. **Divergence**: IoT focus vs. formal methods.	**Challenge**: Balancing security & efficiency. **Future Work**: Cross-disciplinary solutions needed.

E. Quantum Communication progression:

- Representation in quantum key distribution, including twin-field QKD, demonstrate **significant improvement in long-distance secure communication.**

- Prototype results indicate the feasibility of integrating quantum technologies with existing infrastructure, alignment the way for future developments in quantum networks.

V. TRENDS

• **Increased Emphasis on Embedded Systems**: With the trend towards lightweight cryptography solutions, additional emphasis is on improving PQC algorithms for embedded systems, especially for IoT.

• **Hybrid Approaches**: To provide better security and enable more seamless transitions, some studies suggest hybrid approaches that incorporate PQC with conventional cryptographic operations.

•**Performance Optimization**: Research focuses on performance optimization of PQC algorithms with different studies investigate hardware implementations that affect parallelism and special-purpose architectures.

•**Standardization efforts**: One topic that continues to resurface is the ongoing standardization of PQC algorithms by organizations such as NIST, who applaud the imperative of getting into agreement on practical and secure cryptographic techniques**.**

VI. FUTURE DIRECTIONS

A. *Continuing Benchmarking*: future research will have to prioritize earnest benchmarking of PQC algorithms across multiple platforms to confirm their efficiency and reliability across various applications.

B. *Good Security Practices*: formulating concrete security frameworks accounting for theoretical as well as practical vulnerability will be important as PQC picks up more widespread application.

C. *Focus on open Solutions*: with IoT and other resource-constrained applications growing dramatically, there will be a need for lightweight cryptographic algorithms that do not compromise security at the cost of performance.

D. *Integration with Existing Systems*: work should explore methods for integrating PQC into complete cryptographic ecosystem, by focusing on minimizing confusion and performance on high.

E. *Survey of New Algorithms*: To keep ahead of potential quantum attacks, continuous research into new cryptographic schemes is required, particularly those based on various mathematical problems.

F. *Facing Real-World Challenges*: Quantcast challenges, such as noise and loss in quantum communication systems, need more search to enhance the return of quantum technologies in real-world applications.

VII. CONCLUSIONS

The field PQC continues to evolve rapidly, marked by significant advancements and ongoing challenges in the quest for quantum-resistant solutions. Researchers in this domain emphasize the complexities of balancing security requirements with practical performance and implementation feasibility. Collaboration among cryptographers, developers, and standards organizations has become essential to navigating these obstacles and accelerating the adoption of quantum-safe cryptographic techniques. As quantum computing technology progresses, future-proof encryption grows increasingly urgent. The future of PQC will depend on a combination of theoretical innovation, algorithmic optimization, and efficient real-world deployment. Furthermore, continuous evaluation and standardization efforts will play a critical role in ensuring trust and compatibility. By addressing these multifaceted challenges, the cryptographic community can pave the way for a secure transition into the quantum era. Ultimately, sustained investment in research and cross-industry cooperation will be key to safeguarding digital infrastructure against emerging threats.

REFERENCES

[1] M. Ekerå and J. Gärtner, "Extending Regev's factoring algorithm to compute discrete logarithms," in *International Conference on Post-Quantum Cryptography*, Springer, 2024, pp. 211–242.

[2] J.-M. De Koninck and W. Verreault, "On the tower factorization of integers," *Am. Math. Mon.*, vol. 131, no. 6, pp. 511–518, 2024.

[3] G. Alagic *et al.*, "Status report on the third round of the NIST post-quantum cryptography standardization process," 2022.

[4] L. Ducas *et al.*, "Crystals-dilithium: A lattice-based digital signature scheme," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, pp. 238–268, 2018.

[5] D. F. Aranha and M. Medwed, "IACR Transactions on Cryptographic Hardware and Embedded Systems," 2023.

[6] M. Barbosa, F. Dupressoir, A. Hülsing, M. Meijers, and P.-Y. Strub, "A Tight Security Proof for SPHINCS+, Formally Verified," in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, 2024, pp. 35–67.

[7] J. J. Tom, N. P. Anebo, B. A. Onyekwelu, A. Wilfred, and R. E. Eyo, "Quantum computers and algorithms: a threat to classical cryptographic systems," *Int. J. Eng. Adv. Technol*, vol. 12, no. 5, pp. 25–38, 2023.

[8] F. Opiłka, M. Niemiec, M. Gagliardi, and M. A. Kourtis, "Performance Analysis of Post-Quantum Cryptography Algorithms for Digital Signature," *Appl. Sci.*, vol. 14, no. 12, 2024, doi: 10.3390/app14124994.

[9] M. Vidaković and K. Miličević, "Performance and applicability of post-quantum digital signature algorithms in resource-constrained environments," *Algorithms*, vol. 16, no. 11, p. 518, 2023.

[10] S. Sun, R. Zhang, and H. Ma, "Efficient parallelism of post-quantum signature scheme SPHINCS," *IEEE Trans. Parallel Distrib. Syst.*, vol. 31, no. 11, pp. 2542–2555, 2020.

[11] E. Alkim, P. S. L. M. Barreto, N. Bindel, J. Krämer, P. Longa, and J. E. Ricardini, "The lattice-based digital signature scheme qTESLA," in *International Conference on Applied Cryptography and Network Security*, Springer, 2020, pp. 441–460.

[12] G. Land, P. Sasdrich, and T. Güneysu, "A hard crystal-implementing dilithium on reconfigurable hardware," in *International Conference on Smart Card Research and Advanced Applications*, Springer, 2021, pp. 210–230.

[13] Q. D. Truong, P. N. Duong, and H. Lee, "Efficient Low-Latency Hardware Architecture for Module-Lattice-Based Digital Signature Standard," *IEEE Access*, 2024.

[14] M. Schmid, D. Amiet, J. Wendler, P. Zbinden, and T. Wei, "Falcon takes off-a hardware implementation of the falcon signature scheme," *Cryptol. ePrint Arch.*, 2023.

[15] N. Gupta, A. Jati, A. Chattopadhyay, and G. Jha, "Lightweight hardware accelerator for post-quantum digital signature CRYSTALS-Dilithium," *IEEE Trans. Circuits Syst. I Regul. Pap.*, vol. 70, no. 8, pp. 3234–3243, 2023.

[16] D. Smith-Tone and R. Perlner, "Rainbow band separation is better than we thought," *Cryptol. ePr. Arch*, 2020.

[17] K. Kaushik and A. Kumar, "Demystifying quantum blockchain for healthcare," *Secur. Priv.*, vol. 6, no. 3, p. e284, 2023.

[18] A. C. Canto, J. Kaur, M. M. Kermani, and R. Azarderakhsh, "Algorithmic Security is Insufficient: A Comprehensive Survey on Implementation Attacks Haunting Post-Quantum Security," 2023. [Online]. Available: http://arxiv.org/abs/2305.13544.

[19] O. Tsentseria, K. Hleha, A. Matiyko, and I. Samoilov, "The state of standardization of post-quantum crypto-algorithms at the global level," *Autom. Technol. Bus. Process.*, vol. 15, no. 2, pp. 66–71, 2023.

[20] M. Kumar, "Post-quantum cryptography Algorithm's standardization and performance analysis," *Array*, vol. 15, no. April, p. 100242, 2022, doi: 10.1016/j.array.2022.100242.

[21] J. W. Bos, B. Carlson, J. Renes, M. Rotaru, D. Sprenkels, and G. P. Waters, "Post-Quantum Secure Boot on Vehicle Network Processors," 2022. [Online]. Available: https://eprint.iacr.org/2022/635.

[22] Y.-H. Yang *et al.*, "All optical metropolitan quantum key distribution network with post-quantum cryptography authentication," *Opt. Express*, vol. 29, no. 16, p. 25859, 2021, doi: 10.1364/oe.432944.

[23] M. J. Kannwischer, M. Krausz, R. Petri, and S.-Y. Yang, "pqm4: benchmarking NIST additional post-quantum signature schemes on microcontrollers," *Cryptol. ePrint Arch.*, 2024.

[24] G. Fitzgibbon and C. Ottaviani, "Constrained Device Performance Benchmarking with the Implementation of Post-Quantum Cryptography," 2024. doi: 10.3390/cryptography8020021.

[25] P. Tandel and J. Nasriwala, "Secure authentication framework for IoT applications using a hash-based post-quantum signature scheme," *Serv. Oriented Comput. Appl.*, pp. 1–12, 2024.

[26] T. Liu, G. Ramachandran, and R. Jurdak, "Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization," 2024. [Online]. Available: http://arxiv.org/abs/2401.17538.

[27] Y. Xu, Z. Li, N. Dong, V. Kuchta, Z. Hou, and D. Liu, "Formal Verification Techniques for Post-quantum Cryptography: A Systematic Review," in *International Conference on Engineering of Complex Computer Systems*, Springer, 2025, pp. 346–366.

[28] R. Bavdekar, E. J. Chopde, A. Bhatia, K. Tiwari, S. J. Daniel, and Atul, "Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research," 2022, [Online]. Available: http://arxiv.org/abs/2202.02826.