EUROPEAN JOURNAL OF EMERGING REAL-TIME IOT AND EDGE INFRASTRUCTURES

Post-Quantum Cryptographic Foundations and Deployment Challenges for the Internet of Things: Integrating Code-Based, Lattice-Based, and Standardization Perspectives

Dr. Elena Kovács
Faculty of Informatics, Eötvös Loránd University, Hungary

V0LUME02 ISSUE02 (2025)
Published Date: 17 September 2025 // Page no.: - 07-11

ABSTRACT

The accelerating development of quantum computing has profoundly altered long-standing assumptions about computational hardness that underpin classical public-key cryptography. Algorithms such as Shor's polynomial-time approach to integer factorization and discrete logarithms have demonstrated, at least in theory, that cryptographic primitives based on number-theoretic problems are fundamentally vulnerable in a future where large-scale quantum computers become operational (Shor, 1997). This realization has catalyzed a global shift toward post-quantum cryptography, a domain dedicated to designing and analyzing cryptographic systems that remain secure against both classical and quantum adversaries. Within this broad transformation, the Internet of Things occupies a uniquely sensitive position. IoT ecosystems combine massive device heterogeneity, constrained computational resources, long device lifetimes, and high-stakes security requirements related to privacy, safety, and critical infrastructure. Consequently, the transition to quantum-resistant cryptography in IoT environments is not merely a matter of algorithmic substitution, but a systemic challenge involving protocol design, standardization, performance trade-offs, and long-term trust.

This article presents an extensive, theory-driven research study that examines post-quantum cryptography for IoT through three interlinked lenses: foundational cryptographic paradigms, particularly code-based and lattice-based constructions; evolving standardization efforts, especially those coordinated by the National Institute of Standards and Technology; and applied security considerations across emerging network architectures such as fifth- and sixth-generation wireless systems, edge computing, and blockchain-enabled IoT. Drawing strictly on the provided scholarly references, the article situates code-based cryptography as one of the earliest and most conceptually resilient post-quantum approaches, emphasizing its relevance to long-lived IoT deployments where conservative security margins are valued (Sendrier, 2018). At the same time, it critically evaluates lattice-based schemes that currently dominate standardization trajectories due to their versatility and comparatively efficient implementations (W. S. P., 2022; NIST, 2024a).

Methodologically, the study adopts a qualitative, interpretive research design grounded in comparative literature analysis and theoretical synthesis. Rather than presenting experimental benchmarks or numerical evaluations, it systematically interprets reported findings across surveys, protocol proposals, and standards documents to identify recurring patterns, tensions, and unresolved questions. The results section articulates how post-quantum algorithms interact with IoT-specific constraints, revealing a persistent trade-off between cryptographic robustness, computational overhead, and deployment feasibility (Boneh, 2020; Karakaya & Ulu, 2024). The discussion then deepens this analysis by engaging with scholarly debates on algorithmic diversity, cryptographic agility, and the socio-technical implications of premature or fragmented adoption.

Ultimately, the article argues that securing the IoT in the post-quantum era requires more than selecting standardized algorithms. It demands an integrated research agenda that reconciles theoretical security assurances with real-world operational contexts, anticipates future advances in both quantum computing and cryptanalysis, and aligns global standardization with local deployment realities. By offering an expansive and critical synthesis of post-quantum cryptography for IoT, this work contributes a comprehensive academic foundation for researchers, standards bodies, and practitioners navigating one of the most consequential transitions in contemporary information security.

Keywords: Post-quantum cryptography, Internet of Things security, code-based cryptography, lattice-based cryptography, cryptographic standardization, quantum-resistant protocols.

INTRODUCTION

The history of modern cryptography is deeply intertwined with assumptions about computational infeasibility, assumptions that have traditionally been grounded in the practical limits of classical computing architectures. Public-key cryptography, in particular, has relied on the perceived hardness of mathematical problems such as integer factorization and discrete logarithms, which for decades resisted efficient solution despite intense scrutiny from the cryptographic community (Shor, 1997). These assumptions enabled the

widespread deployment of cryptographic protocols that now underpin global digital infrastructure, from secure web communications to authentication mechanisms in embedded systems. However, the theoretical emergence of quantum algorithms capable of solving these problems in polynomial time has destabilized this foundation, prompting a fundamental reassessment of what it means for a cryptographic system to be secure in the long term (Boneh, 2020).

The implications of this reassessment are particularly acute for the Internet of Things. IoT systems are characterized by pervasive connectivity, massive scale, and deep integration into physical and social environments. Devices range from simple sensors with minimal processing capabilities to complex embedded systems controlling industrial processes, healthcare equipment, and urban infrastructure. Many such devices are expected to remain operational for years or even decades, during which time cryptographic mechanisms chosen today must withstand future adversarial capabilities, including those enabled by quantum computing (Mansoor et al., 2025). This temporal mismatch between device lifetimes and cryptographic obsolescence creates a pressing need for post-quantum solutions that are not only theoretically secure but also practically deployable in constrained environments.

Post-quantum cryptography encompasses a diverse set of approaches based on mathematical problems believed to be resistant to quantum attacks. Among these, code-based cryptography occupies a historically significant position. Originating in the late twentieth century with the McEliece cryptosystem, code-based schemes have withstood decades of cryptanalytic efforts without fundamental breaks, leading some researchers to view them as conservative yet highly reliable candidates for long-term security (Sendrier, 2018). Despite their strong security record, code-based schemes have often been criticized for large key sizes, a property that poses nontrivial challenges for IoT devices with limited memory and bandwidth. Nevertheless, renewed interest in code-based cryptography has emerged as the cryptographic community seeks diversity beyond lattice-centric solutions, particularly in scenarios where long-term confidentiality is paramount.

In parallel, lattice-based cryptography has risen to prominence due to its flexibility and efficiency across a wide range of cryptographic primitives, including key exchange, encryption, and digital signatures. Lattice problems such as Learning With Errors have been shown to admit reductions from worst-case hardness assumptions, providing strong theoretical security guarantees that extend to the quantum setting (W. S. P., 2022). These properties, combined with comparatively moderate key sizes and efficient implementations, have positioned lattice-based schemes at the center of international standardization efforts. The National Institute of Standards and Technology has played a pivotal role in this process, coordinating a multi-round evaluation that culminated in the selection of lattice-based and hash-based algorithms for standardization (NIST, 2022; NIST, 2024a).

The intersection of post-quantum cryptography and IoT has therefore become a focal point of contemporary security research. Scholars have examined post-quantum authentication protocols for cellular networks, physical-layer security schemes for next-generation wireless systems, and blockchain-based security architectures for distributed IoT applications (Yadav et al., 2025; Abdallah, 2024; Gharavi et al., 2024). These studies collectively underscore that the adoption of post-quantum algorithms cannot be decoupled from broader architectural considerations. Network latency, energy consumption, trust models, and regulatory compliance all influence which cryptographic solutions are viable in practice.

Despite this growing body of work, significant gaps remain in the literature. Much existing research focuses on performance comparisons or protocol-specific optimizations, often treating post-quantum algorithms as interchangeable components rather than as elements of a complex socio-technical system. Moreover, there is a tendency to privilege lattice-based approaches due to their alignment with current standards, potentially underestimating the strategic value of alternative paradigms such as code-based cryptography in achieving cryptographic resilience through diversity (Sendrier, 2018; Karakaya & Ulu, 2024). This article addresses these gaps by providing an expansive, integrative analysis that situates post-quantum cryptography for IoT within its broader theoretical, historical, and standardization contexts.

By synthesizing insights from foundational cryptographic research, standardization documents, and applied IoT security studies, this work seeks to articulate a coherent framework for understanding both the promise and the limitations of post-quantum cryptography in resource-constrained, long-lived environments. The introduction thus establishes the central problem: how to reconcile the theoretical imperatives of quantum-resistant security with the practical realities of IoT deployment, a challenge that demands sustained scholarly attention and interdisciplinary collaboration (Boneh, 2020; Mansoor et al., 2025).

METHODOLOGY

The methodological approach adopted in this study is intentionally qualitative and interpretive, reflecting the theoretical and conceptual nature of the research problem under investigation. Rather than conducting empirical experiments or implementing cryptographic algorithms in controlled testbeds, the study systematically analyzes and synthesizes existing scholarly literature and standards documents to derive insights into post-quantum cryptography for the Internet of Things. This approach is particularly appropriate given the forward-looking nature

of quantum threats and the ongoing evolution of both cryptographic research and standardization processes (W. S. P., 2022).

The first methodological component involves comprehensive source selection and delimitation. Only the references explicitly provided form the evidentiary basis of the analysis, ensuring that all claims and interpretations are grounded in a defined and coherent corpus of authoritative work. This corpus spans foundational theoretical contributions, such as analyses of quantum algorithms and post-quantum primitives, applied studies addressing IoT and wireless networks, and formal standardization documents issued by recognized institutions (Shor, 1997; Sendrier, 2018; NIST, 2024a). By restricting the scope in this way, the study avoids speculative extrapolation beyond the established literature while enabling deep engagement with each selected source.

The second component consists of thematic coding and comparative analysis. Each reference was examined to identify recurring themes, including assumptions about adversary capabilities, performance constraints in IoT environments, and the role of standardization in shaping cryptographic adoption. For example, works focusing on lattice-based protocols for cellular authentication were compared with studies emphasizing physical-layer security or blockchain integration, allowing the identification of shared concerns and divergent priorities (Yadav et al., 2025; Abdallah, 2024; Gharavi et al., 2024). Code-based cryptography, as articulated in Sendrier's work, was analyzed not in isolation but in relation to these broader themes, highlighting both complementarities and tensions within the post-quantum landscape (Sendrier, 2018).

A third methodological element involves critical discourse analysis of standardization texts. Documents produced by the National Institute of Standards and Technology were treated not merely as technical specifications but as artifacts reflecting institutional priorities, risk assessments, and implicit trade-offs (NIST, 2022; NIST, 2024a; NIST, 2024b). This perspective enables a nuanced understanding of how certain cryptographic paradigms gain prominence and how others may be marginalized despite their theoretical merits. Such analysis is particularly relevant for IoT, where compliance with standards often determines market adoption and regulatory acceptance (Mansoor et al., 2025).

The methodology also explicitly acknowledges its limitations. By relying exclusively on existing literature, the study does not generate new empirical performance data or validate protocol implementations under real-world conditions. As a result, conclusions about feasibility and efficiency are necessarily interpretive, derived from reported findings rather than direct measurement (Opiłka et al., 2024). Nevertheless, this limitation is consistent with the study's objective, which is to provide a comprehensive theoretical synthesis rather than a narrowly focused technical evaluation.

Finally, reflexivity forms an integral part of the methodological framework. Throughout the analysis, attention is paid to the assumptions embedded in different strands of the literature, including implicit notions of technological progress, threat timelines, and device capabilities. By making these assumptions explicit and subjecting them to critical scrutiny, the study aims to avoid uncritical endorsement of dominant narratives, particularly the presumption that current standardization outcomes represent a definitive solution to post-quantum security challenges (Boneh, 2020; Karakaya & Ulu, 2024).

RESULTS

The interpretive analysis of the selected literature reveals several interconnected findings regarding the role of post-quantum cryptography in securing the Internet of Things. One prominent result is the consistent recognition that quantum threats fundamentally alter the risk calculus for IoT security, transforming what were once considered long-term or hypothetical concerns into immediate design considerations (Shor, 1997; Boneh, 2020). Across diverse application domains, authors converge on the view that cryptographic mechanisms embedded in IoT devices must be evaluated not only for current adversarial models but also for their resilience against future quantum-enabled attacks.

A second key finding concerns the comparative positioning of different post-quantum cryptographic paradigms. Lattice-based schemes emerge as the most widely studied and practically oriented solutions, particularly in the context of authentication protocols, digital signatures, and secure key exchange for networked devices (Yadav et al., 2025; Karakaya & Ulu, 2024). Their prominence is reinforced by standardization outcomes, which lend institutional legitimacy and encourage early adoption. However, the literature also highlights that this dominance is not purely the result of superior security properties but is shaped by considerations of implementation efficiency, versatility, and alignment with existing protocol architectures (W. S. P., 2022; NIST, 2024a).

In contrast, code-based cryptography is frequently discussed in terms of its exceptional security longevity. Sendrier emphasizes that decades of cryptanalysis have failed to produce practical breaks against well-parameterized code-based systems, a track record that few other post-quantum candidates can claim (Sendrier, 2018). The result of this analysis is a nuanced appreciation of code-based schemes as highly conservative options that may be particularly well-suited for IoT deployments requiring long-term confidentiality, such as archival data protection or critical infrastructure monitoring. At the same time, concerns about key size and communication overhead are consistently identified as barriers to widespread adoption in highly constrained devices

(Boneh, 2020).

Another significant finding relates to the interaction between post-quantum cryptography and emerging network architectures. Studies on fifth- and sixth-generation wireless systems reveal that integrating quantum-resistant algorithms into authentication and key management protocols introduces new performance trade-offs, including increased signaling overhead and computational latency (Yadav et al., 2025; Abdallah, 2024). These trade-offs are not uniformly negative; in some cases, the literature suggests that careful protocol redesign can mitigate overhead while enhancing security properties such as perfect forward secrecy. Nonetheless, the results indicate that post-quantum adoption in IoT is inseparable from broader architectural innovation.

Finally, the analysis reveals a growing emphasis on standardization as both an enabler and a constraint. NIST's selection of specific post-quantum algorithms provides clarity and direction, reducing uncertainty for developers and manufacturers (NIST, 2022). At the same time, scholars caution that overreliance on a narrow set of standardized algorithms may create systemic risks if unforeseen vulnerabilities emerge, underscoring the importance of cryptographic agility and diversity (Sendrier, 2018; Karakaya & Ulu, 2024).

DISCUSSION

The findings outlined above invite deeper theoretical reflection on the trajectory of post-quantum cryptography for the Internet of Things. At the most fundamental level, they highlight a tension between the desire for definitive solutions and the inherently provisional nature of cryptographic security. Quantum computing represents not merely a new class of attack tools but a paradigm shift that challenges long-standing intuitions about hardness assumptions and adversarial capabilities (Shor, 1997; Boneh, 2020). In this context, post-quantum cryptography should be understood not as a final destination but as an evolving response to an uncertain technological future.

One of the most salient issues emerging from the discussion is the role of algorithmic diversity. The literature's emphasis on lattice-based schemes reflects practical considerations, yet it also risks creating monocultures that may prove brittle over time (Sendrier, 2018). Code-based cryptography offers a compelling counterpoint, embodying a philosophy of conservatism grounded in empirical cryptanalytic history. From a theoretical perspective, incorporating multiple cryptographic paradigms into IoT security architectures can enhance systemic resilience by reducing the likelihood that a single breakthrough compromises an entire ecosystem (Karakaya & Ulu, 2024).

Standardization processes occupy a complex position within this debate. On one hand, coordinated efforts by institutions such as NIST are essential for achieving interoperability, regulatory acceptance, and economies of scale (NIST, 2022). On the other hand, standardization can inadvertently ossify design choices, discouraging experimentation and delaying the adoption of alternative approaches that may prove advantageous in specific contexts (Boneh, 2020). For IoT, where deployment environments vary widely and device capabilities are heterogeneous, a one-size-fits-all approach to post-quantum cryptography is particularly problematic (Mansoor et al., 2025).

The discussion also underscores the importance of viewing post-quantum cryptography through a socio-technical lens. Security mechanisms do not exist in isolation; they are embedded in organizational practices, economic incentives, and regulatory frameworks. Decisions about which algorithms to deploy are influenced by vendor support, compliance requirements, and perceived risk, as much as by theoretical security properties (Gharavi et al., 2024). Recognizing these factors is crucial for developing realistic transition strategies that balance ideal security goals with practical constraints.

Another critical dimension concerns performance and resource constraints. IoT devices often operate at the margins of computational feasibility, making even modest increases in cryptographic overhead significant (Opiłka et al., 2024). The literature suggests that while post-quantum algorithms are becoming more efficient, their integration into large-scale IoT systems will require careful optimization and, in some cases, architectural redesign (Abdallah, 2024). This raises broader questions about whether security should be treated as an add-on feature or as a core design principle shaping system architecture from the outset.

Finally, future research directions emerge naturally from this discussion. Scholars have called for longitudinal studies examining the real-world deployment of post-quantum cryptography in IoT, as well as interdisciplinary collaborations that bring together cryptographers, network engineers, and policy experts (Yadav et al., 2025; Mansoor et al., 2025). Such efforts are essential for translating theoretical robustness into sustainable security practices that can endure in the face of rapid technological change.

CONCLUSION

The transition to post-quantum cryptography represents one of the most significant challenges and opportunities in the contemporary evolution of information security. For the Internet of Things, this transition is particularly consequential, given the scale, longevity, and societal impact of connected devices. Through an extensive analysis grounded in established scholarly and standardization literature, this article has shown that post-quantum security for IoT is not reducible to the selection of a single algorithm or standard. Instead, it is a multidimensional problem involving theoretical assurance, practical feasibility, institutional coordination, and long-term adaptability (Sendrier, 2018; Boneh, 2020;

NIST, 2022).

By critically examining code-based and lattice-based cryptographic paradigms alongside emerging deployment contexts, the study underscores the need for balanced and diversified approaches. As quantum technologies continue to mature, the decisions made today regarding IoT security will shape digital trust for decades to come. A reflective, theoretically informed, and context-sensitive approach to post-quantum cryptography is therefore not only desirable but essential.

REFERENCES

1. National Institute of Standards and Technology. (2024). Stateless Hash-Based Digital Signature Standard (FIPS PUB 205).
2. Gharavi, H., Granjal, J., & Monteiro, E. (2024). Post-quantum blockchain security for the Internet of Things: Survey and research directions.
3. Sendrier, N. (2018). Code-based cryptography for post-quantum security.
4. Abdallah, W. (2024). A physical layer security scheme for sixth generation wireless networks using post-quantum cryptography.
5. Boneh, T. (2020). Cryptographic trends in IoT.
6. Opiłka, F., Niemiec, M., Gagliardi, M., & Kourtis, M. A. (2024). Performance analysis of post-quantum cryptography algorithms for digital signature.
7. Yadav, A. K., Choudhary, E., Garg, O., & Liyanage, M. (2025). Post-quantum secure lattice-based authentication protocol resistant to malicious serving networks with perfect forward secrecy.
8. National Institute of Standards and Technology. (2022). Selected algorithms.
9. Karakaya, A., & Ulu, A. (2024). A survey on post-quantum based approaches for edge computing security.
10. Mansoor, K., Afzal, M., Iqbal, W., et al. (2025). Securing the future: exploring post-quantum cryptography for authentication and user privacy in IoT devices.
11. National Institute of Standards and Technology. (2024). Module-lattice-based digital signature standard (FIPS PUB 204).
12. Shajahan, R., Jain, K., & Krishnan, P. (2024). A survey on third round post-quantum digital signature algorithms.
13. Althobaiti, O. S., & Dohler, M. (2021). Quantum-resistant cryptography for the Internet of Things based on location-based lattices.
14. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.