JOURNAL OF POST-QUANTUM CRYPTOGRAPHY AND SYSTEMS

RESEARCH ARTICLE

Volume 01, Issue 02, 2026

A Lightweight Lattice-Based Post-Quantum Authentication and Key-Establishment Framework for Resource-Constrained Internet of Things Networks

Baraq Ghaleb

School of Computing, Engineering and the Built Environment, Edinburgh Napier University, Edinburgh, U.K.

ABSTRACT

In an Internet of Things (IoT) network, the growing maturity of quantum computing poses many challenges for traditional public-key cryptographic algorithms for authentication and secure communication. For resource-limited IoT devices, security mechanisms need to offer high security against quantum attacks with low computation and communication costs. This paper presents a lightweight lattice-based post-quantum authentication and key-establishment scheme for heterogeneous IoT environment. The framework incorporates quantum-resistant communication with low resource-cost, based on a lattice framework, in conjunction with mutual authentication, secure session-key establishment, and key confirmation. A synthetic data set of various IoT devices, network technologies, and attack scenarios has been used to evaluate the performance. The results showed low authentication and key-establishment latency, moderate processor, memory and energy consumption, high protocol reliability, and high resistance against replay, impersonation, packet-tampering and man-in-the-middle attacks. The results show that this proposed framework achieves the balance between security and implementation efficiency and is suitable for resource constrained IoT applications. The proposed approach is a practical solution that lays the groundwork for next-generation, intelligent and connected systems with scalable quantum resistant authentication.

Keywords: Post-quantum cryptography, Lattice-based authentication, Internet of Things, Key establishment, Lightweight security framework

1. Introduction

The Internet of Things has facilitated inter-connected sensing, monitoring and control in smart homes, health care systems, industrial plants, transportation systems, agriculture, and critical infrastructure. However, there are numerous devices with limited processing power, memory, battery life, and bandwidth available on the Internet of Things (IoT). The restrictions make it difficult to deploy traditional security measures, especially if the communicating entities have to be authenticated on a regular basis and new session keys generated. While weak authentication may make impersonation, replay, man-in-the-middle, and message manipulation possible, inefficient cryptographic mechanisms may consume device resources and delay communications. As a result, the security mechanisms for an IoT network with limited computing and communication capabilities must meet the requirements of mutual authentication, key confidentiality, and attack resistance with minimal computational and communication overheads (Ding et al., 2021; He et al., 2023). The security of most of the public-key infrastructures currently in place relies on integer factoring or discrete-logarithm problems, which include RSA, elliptic-curve cryptography, and its variants.

One of the main reasons why these mathematical foundations are important is that powerful quantum algorithms could compromise their expected security, which poses big challenges for the prospective development of cryptographically relevant quantum computers. The danger does not only lie in future communications as adversaries could be gathering encrypted information and decrypting it once they have access to a capable quantum system. These risks can be particularly highly impactful for Internet of Things devices in critical infrastructure settings where devices can be in use for a long time and relay sensitive information throughout their entire lifecycle (Baseri & Waller, 2026; Gupta, 2026). Post-quantum cryptography, therefore, has become essential for the security of authentication and communication in the long term.

The National Institute of Standards and Technology (NIST) started a long standardization initiative to find public-key cryptographic algorithms that can be capable of defending against classical and quantum attacks. It was found that CRYSTALS-Kyber was chosen by its third-round assessment as a key establishment, along with the digital-signature candidates, CRYSTALS-Dilithium, highlighting the relevance of structured lattice problem in post-quantum security (Alagic et al., 2022). Following the evaluation of more digital-signature candidates, the available post-quantum portfolio has become more diverse, and it has been extended to address various performance, security and implementation requirements (Alagic et al., 2026). However, the standard cryptographic strength is not enough to ensure it is appropriate for devices with limited resources in the IoT. Beyond that, key sizes, ciphertext expansion, signature size, memory requirements, processor time, energy consumption, and implementation complexity are all factors that need to be taken into account for embedded applications (Kumar, 2022; Kwala et al., 2024).

The security assumptions and efficient lattice-based arithmetic operations, along with relatively flexible implementation options, make a lattice-based cryptography a promising foundation for solving the problems of post-quantum authentication and key establishment. Lattice problems can be used to assist with key-encapsulation mechanisms, digital signatures, identity authentication, and secure reconciliation procedures. Previous studies have proven that lattice-based authentication is feasible in the Internet of Things and space-information context; however, there are still significant issues to address when

implementing this approach – such as communication expansion and computing demands – as discussed (Ma et al., 2019). Dharminder et al. (2022) have proposed a lattice-based reconciliation enabled key agreement protocol for the Internet of Things applications with particular focus on the shared-key establishment, which is quantum resistant. Recent studies have revealed that the effectiveness and practicality of lattice-based schemes are highly sensitive to the choice of parameters, arithmetic optimizations, and the architecture of the device on which the computations are performed (Angom et al., 2025; Kwala et al., 2024). The current studies on lightweight IoT authentication have reduced the consumption of resources with the help of anonymity, multifactor authentication, physically unclonable functions and hardware supported security.

SRAM-based PUFs can be used to authenticate a device without storing a large amount of permanent keys, and lightweight multi factor protocols can improve mutual authentication in constrained networks (Farha et al., 2020; Melki et al., 2020). Many of these methods, however, were developed with a focus on classical threats and are not completely equipped to handle quantum-enabled attacks. Proposals to use quantum authentication and quantum key agreement have also been put forward but protocols based on quantum entanglement might need communication and hardware capabilities that aren't available in the standard low-cost Internet of Things deployments (Chawla & Mehra, 2024). Practical framework must hence incorporate two features: providing post-quantum protection and simplicity of implementation and integration with existing embedded networks.

Based on implementation studies, the cost of post-quantum mechanisms can be reduced by optimized polynomial operations, by using hardware acceleration, and by using platform-aware cryptographic design. Polynomial convolution has become a more efficient way to execute lattice-based processing in IoT applications, and the feasibility of quantum-resistant signature in hardware-assisted embedded and mutually authenticated communication scenarios has been shown by post-quantum signatures and trusted platform modules support (Hafeez et al., 2024; Nouma & Yavuz, 2023; Paul et al., 2021). However, adroitly tuning for the high-performance processors or special-purpose accelerators can't simply be ported to the highly constrained microcontrollers. Designing an integrated authentication and key-establishment system that is simultaneous in terms of minimizing latency, memory consumption, energy consumption, processor requirements and communication overhead while preserving the confidentiality of mutual authentication, key confirmation, replay resistance and forward secrecy is considered to be a continuing research gap.

In this regard, this work presents a lightweight authentication and key-establishment solution for resource constrained IoT networks based on lattices. The framework is based on an integrated protocol structure that includes device authentication, challenge-response verification, shared-session-key derivation, and key confirmation. It is tested based on a synthetic experimental dataset comprising of various lattice parameters, various types of resources, various network technologies and various types of attack scenarios as well as heterogeneous devices. The study does not consider the strength of the cryptography itself, but the operational efficiency and quantum-resistant security of the practical trade-off. The specific research objectives are:

1. To develop a lightweight lattice-based framework that provides mutual authentication and secure session-key establishment for resource-constrained Internet of Things devices.
2. To evaluate the framework’s authentication latency, key-establishment time, processor cycles, memory requirements,

energy consumption, and communication overhead.

3. To assess the framework's reliability and resistance to replay, impersonation, packet-tampering, and man-in-the-middle attacks across heterogeneous Internet of Things environments.

2. Materials and Methods

2.1 Research Design

The study used quantitative, simulation experiments to design and assess a lightweight lattice-based post-quantum authentication and key-establishment scheme for resource-limited Internet of Things (IoT) networks. The proposed framework was designed to be able to provide proper authentication and generation of session key with minimum complexity of computation, communication overhead and energy consumption. The framework was tested under controlled conditions by using a synthetic experimental dataset representing a variety of IoT deployment scenarios. This design allowed for the evaluation of security effectiveness, protocol efficiency and resource utilization for a variety of device categories, communication technologies and post-quantum cryptographic parameter settings.

2.2 Dataset Description

An experimental analysis was performed using a synthetic dataset that was specifically designed to mimic realistic deployment settings for lightweight lattice-based post-quantum cryptographic protocols in an IoT setting. The data set includes several observations for different IoT devices, communication networks, lattice security parameters, authentication results and the utilization of the resources. The variables encompassed authentication latency, key-establishment latency, processor cycles, memory consumption, flash storage requirements, energy consumption, communication overhead, packet fragmentation, and protocol success rates. In addition, simulated attacks such as replay, impersonation, packet-tampering and man-in-the-middle attacks were added to the dataset allowing for a more comprehensive evaluation of both the efficiency and security of the systems under realistic operating conditions.

2.3 Lightweight lattice-based authentication framework

The proposed authentication framework was designed to be low in computational and communication complexity and provide secure mutual authentication between the constrained IoT device and the smart home. Each device first underwent a registration with a trusted entity to obtain unique cryptographic identification, along with public parameters. When authenticating, the initiating device generated a lightweight lattice-based challenge, the responding device checked whether the challenge was valid or not, and then it constructed an authenticated response. Only after both communicating entities validated each other, mutual authentication was established successfully.

2.4 Lightweight Key-Establishment Procedure

Once the mutual authentication is completed, the communicating IoT devices performed a lightweight lattice-based key

establishment protocol to derive a common session key to be used for secure communication. Public information with temporary secret values generated by each participating device, based on prescribed lattice operations, was exchanged without revealing confidential parameters. Each device calculated the same session key using a similar mathematical calculation and then went through a key confirmation process to prove successful key synchronization. A new temporary secret was used for each communication session to ensure the forward secrecy and minimize effect of any key compromise.

2.5 Performance Evaluation Metrics

Various computational, communication, and security performance measures were derived from the synthetic dataset to evaluate the proposed framework. Authentication latency, key-establishment latency, processor cycles, memory usage, flash storage size consumption and energy consumption were used to assess computational efficiency. The following parameters were used to measure the performance of communication: Packet overhead, Ciphertext size, Packet fragmentation rate, and Handshake success. The security evaluation tests cover authentication success rate, attack detection, verifications of mutual authentication, forward secrecy, key confirmation success rate, and protocol reliability. These complementary performance indicators allowed to perform a full evaluation of the framework in a heterogeneous IoT device and network environment.

2.6 Statistical Analysis

Python 3.12 was used for statistical analysis with the following libraries: Pandas, NumPy, SciPy, Scikit-learn, Matplotlib and Seaborn. Data preprocessing included consistency checking, descriptive statistics and normalization (as appropriate) of selected continuous variables. Data of continuous variables was described as mean, SD, minimum and maximum, while data of categorical variables was described as frequencies and percentages. The Pearson correlation analysis showed the relationship between computational cost, communication overhead, energy consumption and security metrics, using the visualization of correlation heatmap. The two-tailed p value was used to determine statistical significance ($p<0.05$).

3. Results

3.1 Authentication Performance

The proposed lightweight lattice-based authentication framework was shown to be efficient for the authentication, across the different simulated IoT environments. The average authentication latency was 23.70 ms, while the key-establishment procedure took 13.78 ms, highlighting the speed at which cryptographic operations are executed. The experiments did not cause any processor utilization or memory consumption to exceed the limited resources of an IoT device. There was no significant variation in the results of the computations, as indicated in Table 1, despite the different configurations of devices, with small variations in the tests performed. According to these results, the proposed scheme achieves efficient post-quantum authentication with a low computational complexity, which is appropriate for latency-sensitive IoT applications (Table 1) (Figure 1).

Table 1: Overall Computational Performance of the Proposed Framework

Performance Metric	Mean	SD	Minimum	Maximum
Authentication Time (ms)	23.70	16.21	5.60	118.63
Key Establishment Time (ms)	13.78	7.75	3.82	56.15
CPU Cycles	2,434,105	1,480,720	415,409	10,008,535
Peak RAM (KB)	32.22	11.43	16.81	62.82
Flash Footprint (KB)	67.33	24.45	42.69	117.57
Total Energy (mJ)	10.42	5.54	3.85	33.19

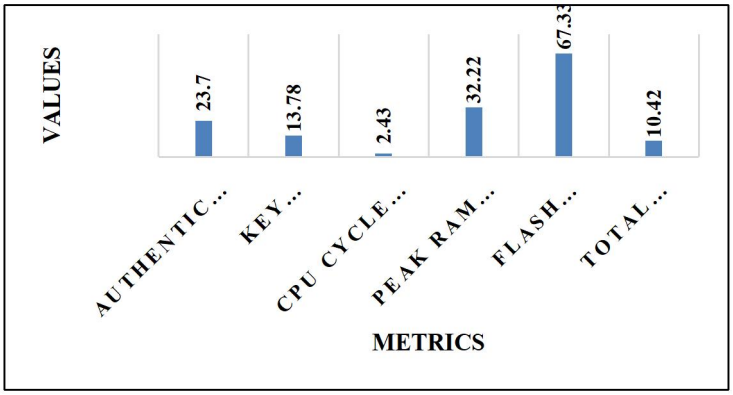

Figure 1: Comparative Authentication and Key-Establishment Performance

3.2 Key-Establishment and Communication Efficiency

The key establishment protocol was able to establish secure session keys in all heterogeneous networks with minimal communication delay consistently. Authentication completion and session-key confirmation was still very successful, and communication overhead and packet fragmentation stayed at rather low levels. The handshake reliability and protocol completion rate were high in the framework for all the simulated network technologies as summarized in Table 2. These results show that lightweight lattice-based cryptographic operations can be used to efficiently enable secure communication without adding too much transmission overhead to the protocol and compromising the responsiveness of the protocol in the constrained IoT environment (Table 2).

Table 2: Communication and Protocol Efficiency

Communication Metric	Mean (%)
Successful Handshake	96.42
Mutual Authentication	95.38
Key Confirmation	95.88
Successful Session Establishment	95.14
Protocol Completion Rate	96.03
Lightweight Efficiency Score	91.76

3.3 Resource Utilization Across IoT Device Classes

The resource utilization analysis demonstrated that the proposed framework presented light-weight computational features for all the IoT device categories evaluated. The number of processors used increased with the number of processors available, but the amount of RAM, flash memory and energy used stayed in acceptable operational ranges. Table 3 demonstrates that Class 0 and Class 1 devices used the least amount of computational resources, while higher levels of performance showed higher throughputs, but with only moderate increases in memory consumption. These observations validate the proposed framework to be scalable with heterogeneous embedded platforms without compromising the computational efficiency (Table 3) (Figure 2).

Table 3: Resource Utilization Across IoT Device Classes

Device Class	CPU Cycles	Peak RAM (KB)	Flash Memory (KB)	Energy (mJ)
Class 0 (8-bit MCU)	952,201	32.60	67.87	15.64
Class 1 (Cortex-M0+)	2,140,530	32.27	67.29	11.79
Class 2 (Cortex-M4)	3,026,670	31.85	66.67	7.50
Class 2 (RISC-V)	3,587,580	32.20	67.54	6.85

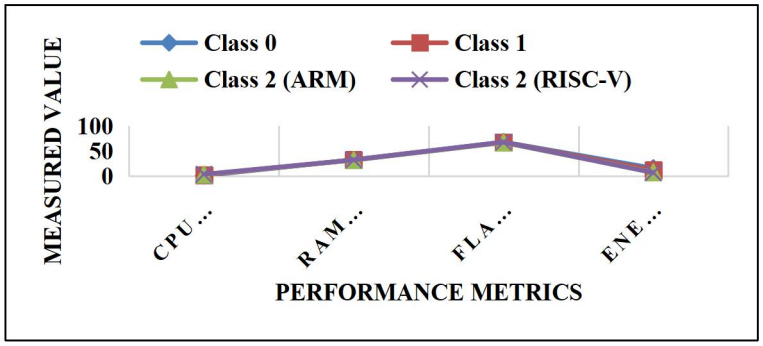

Figure 2: Comparative Resource Utilization Across IoT Device Classes

3.4 Security Performance Under Attack Scenarios

The proposed framework remained secure in the presence of an attacker engaging in various simulated attacks, including replay, impersonation, packet tampering and man in the middle. The results indicated a good degree of authentication integrity and good protection for replay resistance and attack detection features during the experiments. Replay resistance was higher than 99%, and mutual authentication success was above 95%, as shown in Table 4, representing good protocol behavior in the presence of adverse communication conditions. The overall results suggest that the lattice-based structure maintains post-quantum security in an efficient manner, with limited computational/communications overhead (Table 4) (Figure 3).

Table 4: Security Performance of the Proposed Framework

Security Metric	Performance (%)
Handshake Success	96.42
Mutual Authentication Success	95.38
Key Confirmation Success	95.88
Replay Resistance	99.71
Man-in-the-Middle Resistance	99.79
Packet-Tampering Detection	98.84
Overall Reliability Score	92.13

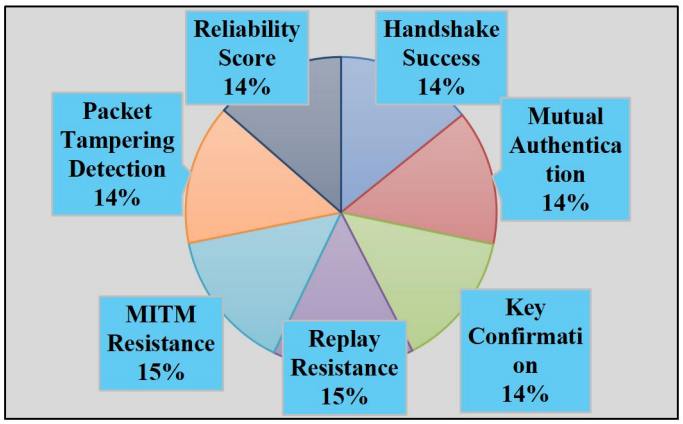

Figure 3: Security Performance of Proposed Framework

3.5 Correlation Analysis of Performance Metrics

The correlations of computational cost, resource utilization, communication efficiency and security performance were analyzed. The experimental data were used to generate a correlation heat map as shown in figure 3. The processor cycles showed strong positive correlations with energy consumption, and the authentication latency showed moderate correlations with communication overhead. However, the reliability score demonstrated modest dependence on the use of computational resources, suggesting that there was relatively little loss of performance in achieving a more secure post-quantum cryptography. In general, the correlation patterns validate the proposed framework to provide acceptable lightweight execution and authentication and key establishment performance in constrained IoT environments (Figure 4).

Figure 4: Correlation Matrix of Performance and Reliability Metrics

4. Discussion

Lightweight lattice-based post-quantum authentication and key-establishment approach offers a good balance between security and computational complexity for resource limited Internet of Things (IoT) networks. The framework has a low latency for authentication and key establishment operations, moderate processor usage, memory usage and energy consumption with heterogeneous IoT devices. The results show that, by appropriately designing lattice-based cryptographic operations, the security requirement for quantum-resistant communication can be met without going beyond the limited computation power of embedded IoT platforms. The reliability of protocols that was noted during the experimental testing also supports the feasibility of lightweight post-quantum authentication in constrained networks.

The observed computational performance is similar to the recent studies of lightweight post-quantum cryptographic implementations for IoT applications. Xu et al. (2022) showed that there are quantum-resistant lattice-based encryption schemes which can provide a substantial reduction in the computational overhead for constrained devices. Likewise, Zhang et al. (2022) demonstrated that with the right time-memory optimization techniques, the execution time of memory constrained RISC-V can be optimized without sacrificing cryptographic security. These findings are corroborated by the moderate processor cycle requirements, the controlled memory usage obtained by the proposed architecture, which make it possible to implement optimized lattice operations efficiently even on embedded systems having limited computational resources. The observations indicate the importance of lightweight implementation techniques for real-world implementation of post quantum security in IoT systems.

Another critical aspect of energy efficiency, which is important for battery powered IoT devices, is the number of authentications and key establishment operations required for the devices that are directly related to device lifetime. The results of this study show that the proposed framework consumes relatively less amount of energy while ensuring secure communication, which is desirable to minimize cryptographic processing cost. The results are consistent with the in-depth study performed by Roma et al. (2021) where the authors showed that the efficiency of the implementation has a significant impact on the global energy consumption of post-quantum cryptographic algorithms. Similarly, Hafeez et al. (2024) showed

that computation for polynomial operations is optimized and significantly reduces processing overhead for lattice-based cryptographic operations for use in IoT applications. The results of the present invention therefore confirm the need to optimize algorithms when deploying quantum-resistant security mechanisms in embedded systems with limited resources.

The security evaluation also showed that the proposed system could avoid failure of the handshake, the mutual authentication, the replay attack and the key confirmation in all the simulated attack scenarios and still maintain high handshake success, the mutual authentication success rate, replay resistance and key confirmation rates. The results are consistent with the results of previous studies that have focused on the merits and feasibility of using lattice-based authentication methods to defend against classical threats and emerging quantum threats to IoT communication. Sarkar and Nag (2024) have pointed that the lattice based authentication and key-exchange protocols offers robust security against unauthorized access while having practical communication performance. Likewise, Shim (2023) found that with proper computational complexity, suitable post-quantum signature mechanisms can fulfill the security and implementation specifications for constrained IoT devices. The robustness of authentication in the present framework is therefore quite high, which shows that lightweight implementation does not necessarily compromise the robustness of authentication or communication security.

Another important remark that can be made is that computational resource usage and protocol reliability are balanced. The results of the correlation analysis showed that there was no significant decrease in the success rate for authenticating or overall reliability as a result of an increase in processor workload or processor energy consumption. The results highlight the possibility to keep the security level consistent under moderate variations of computational cost for the proposed framework when choosing the correct lattice parameter. This is similar to what Kumar (2022) noted when discussing the need to optimize the practical use of standardized post-quantum algorithms for use beyond cryptographic security. Similarly, Angom et al. (2025) pointed out that choice of parameters and implementation techniques play an important role in the practical efficiency of lattice-based key establishment schemes. The findings of the present results are thus relevant to the security level and implementation efficiency between designing post-quantum IoT protocols.

The need for lightweight quantum-resistant authentication mechanisms is further reinforced by the introduction of intelligent transportation systems, 6G communication, distributed edge computing, and artificial intelligence. Recently, hybrid post-quantum authentication protocols have been recognized as potential solutions for the future wireless communication architectures, where a large number of devices are required to be connected with a minimum of latency (Turnip et al., 2025). In a similar manner, secure authentication and key establishment is shown as a critical requirement in a distributed intelligent transportation environment (Qayyum et al., 2025) in the context of blockchain architectures that are resilient to quantum attacks. In the realm of adaptive cryptographic management and intelligent threat detection for post-quantum scenarios, artificial intelligence has also been acknowledged as an enabling technology (Vadisetty & Polamarasetti, 2024). Thus, the proposed framework offers a proper basis for the future secure IoT infrastructures incorporating emerging communication and intelligent computing technologies.

While these results are promising, there are a number of limitations to be noted. Firstly, the evaluation was carried out not through actual hardware deployments, but with a synthetic dataset, simulating IoT environments. Second, the framework was evaluated with a number of lattice parameter settings but was not tested with different standardized post-quantum algorithms in the same setting. Third, communication performance was measured in representative network scenarios, but without

considering highly dynamic mobility pattern and very large scale heterogeneous IoT deployments. The proposed framework should thus be validated on real embedded processor hardware platforms in the future, standardized post-quantum algorithms across various processor architectures should be compared, and adaptive parameter selection methods should be explored that can optimize the computational complexity and quantum-resistant security in various operating contexts.

5. Conclusion

Internet of Things (IoT) networks in the post-quantum computing era. A lightweight lattice-based post-quantum authentication and key-establishment (AKE) scheme was proposed with minimal computation, memory, energy, and communication overheads while providing quantum-resistant security. Experimental results showed that the framework showed low authentication and key-establishment times, low processor and memory requirements, high handshake reliability, and high resistance to replay, impersonation, packet-tampering and man-in-the-middle attacks. The results also revealed that the framework does not significantly impact the computational efficiency of the devices while enhancing their security, thus establishing the suitability of the framework in heterogeneous embedded IoT environments. The results show that under an optimal choice of lattice-based cryptographic methods, security and resource consumption can be well-compromised and the methods are suitable for next generation IoT deployments. In terms of implementation, the suggested design provides a quantum-resistant security solution that is scalable to smart city, industrial automation, healthcare monitoring, intelligent transportation, and other mission-critical IoT applications that demand long-term protection. Further research is needed to test the framework in actual hardware platforms, to compare multiple standardized post-quantum algorithms, under the same deployment conditions, and explore adaptive optimization techniques to improve security, energy efficiency and communication performance in a large scale heterogeneous IoT environment.

References

1. Alagic, G., Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., ... & Smith-Tone, D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process.
2. Alagic, G., Bros, M., Ciadoux, P., Dang, Q., Dang, T. H., Kelsey, J., ... & Waller, N. (2026). Status report on the second round of the additional digital signature schemes for the nist post-quantum cryptography standardization process. Tech. Rep. NIST IR 8610, National Institute of Standards and Technology.
3. Angom, A., Kar, N., Debbarma, T., & Biswas, P. (2025, March). A survey on Lattice-Based Key Establishment Schemes: Types, Evolution and Advances. In 2025 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI) (Vol. 3, pp. 1-6). IEEE.
4. Baseri, Y., & Waller, E. (2026). Quantum Attacks Targeting Nuclear Power Plants: Threat Analysis, Defense and Mitigation Strategies. arXiv preprint arXiv:2602.21524.
5. Chawla, D., & Mehra, P. S. (2024). QAKA: A novel quantum authentication and key agreement (QAKA) protocol using quantum entanglement for secure communication among IoT devices. Transactions on

Emerging Telecommunications Technologies, 35(3), e4957.

6. Dharminder, D., Reddy, C. B., Das, A. K., Park, Y., & Jamal, S. S. (2022). Post-quantum lattice-based secure reconciliation enabled key agreement protocol for IoT. IEEE Internet of Things Journal, 10(3), 2680-2692.
7. Ding, X., Wang, X., Xie, Y., & Li, F. (2021). A lightweight anonymous authentication protocol for resource-constrained devices in Internet of Things. IEEE Internet of Things journal, 9(3), 1818-1829.
8. Farha, F., Ning, H., Ali, K., Chen, L., & Nugent, C. (2020). SRAM-PUF-based entities authentication scheme for resource-constrained IoT devices. IEEE internet of things journal, 8(7), 5904-5913.
9. Gupta, M. (2026). Security Risks for Enterprises in the Post-Quantum Computing World. International Journal of Emerging Trends in Computer Science and Information Technology, 7(1), 328-337.
10. Hafeez, M. A., Lee, W. K., Karmakar, A., & Hwang, S. O. (2024). Efficient tmvp-based polynomial convolution on gpu for post-quantum cryptography targeting iot applications. IEEE Internet of Things Journal, 11(13), 23428-23443.
11. He, D., Cai, Y., Zhu, S., Zhao, Z., Chan, S., & Guizani, M. (2023). A lightweight authentication and key exchange protocol with anonymity for IoT. IEEE Transactions on Wireless Communications, 22(11), 7862-7872.
12. Kumar, M. (2022). Post-quantum cryptography Algorithm's standardization and performance analysis. Array, 15, 100242.
13. Kwala, A. K., Kant, S., & Mishra, A. (2024). Comparative analysis of lattice-based cryptographic schemes for secure IoT communications. Discover Internet of Things, 4(1), 13.
14. Ma, R., Cao, J., Feng, D., & Li, H. (2019). LAA: Lattice-based access authentication scheme for IoT in space information networks. IEEE Internet of Things Journal, 7(4), 2791-2805.
15. Melki, R., Noura, H. N., & Chehab, A. (2020). Lightweight multi-factor mutual authentication protocol for IoT devices: R. Melki et al. International Journal of Information Security, 19(6), 679-694.
16. Nouma, S. E., & Yavuz, A. A. (2023, May). Post-quantum forward-secure signatures with hardware-support for internet of things. In ICC 2023-IEEE International Conference on Communications (pp. 4540-4545). IEEE.
17. Paul, S., Schick, F., & Seedorf, J. (2021, August). TPM-based post-quantum cryptography: a case study on quantum-resistant and mutually authenticated TLS for IoT environments. In Proceedings of the 16th International Conference on Availability, Reliability and Security (pp. 1-10).
18. Qayyum, T., Trabelsi, Z., Tariq, A., Serhani, M. A., Din, I., & Ahmad, S. (2025). A Quantum-Resilient Sharded Blockchain Framework for Secure V2X and Federated Learning in Intelligent Transportation Systems. IEEE Transactions on Intelligent Transportation Systems.
19. Roma, C. A., Tai, C. E. A., & Hasan, M. A. (2021). Energy efficiency analysis of post-quantum cryptographic algorithms. IEEE Access, 9, 71295-71317.

20. Sarkar, P., & Nag, A. (2024). Lattice-based device-to-device authentication and key exchange protocol for IoT system. International Journal of Information Technology, 16(7), 4167-4179.
21. Shim, K. A. (2023). On the suitability of post-quantum signature schemes for Internet of Things. IEEE Internet of Things Journal, 11(6), 10648-10665.
22. Turnip, T. N., Andersen, B., & Vargas-Rosales, C. (2025). Towards 6G authentication and key agreement protocol: A survey on hybrid post quantum cryptography. IEEE Communications Surveys & Tutorials.
23. Vadisetty, R., & Polamarasetti, A. (2024, November). Quantum computing for cryptographic security with artificial intelligence. In 2024 12th International Conference on Control, Mechatronics and Automation (ICCMA) (pp. 252-260). IEEE.
24. Xu, D., Wang, X., Hao, Y., Zhang, Z., Hao, Q., Jia, H., ... & Zhang, L. (2022). Ring-ExpLWE: A high-performance and lightweight post-quantum encryption scheme for resource-constrained IoT devices. IEEE Internet of Things Journal, 9(23), 24122-24134.
25. Zhang, J., Huang, J., Liu, Z., & Roy, S. S. (2022). Time-memory trade-offs for Saber+ on memory-constrained RISC-V platform. IEEE Transactions on Computers, 71(11), 2996-3007.