Journal for Technology and Science
Homepage : https://journal.antispublisher.com/index.php/IPTEKS
Email : admin@antispublisher.com

e-ISSN : 3047-4337
JOTECH, Vol. 3, No. 3, July 2026
Page 83-91
© 2026 JOTECH :
Journal for Technology and Science

# A Comparative Study between Traditional Encryption Algorithms and Post-Quantum Cryptography in Light of Quantum Threats: An Analytical Comparison between the Advanced Encryption Standard (AES) and the Post-Quantum Encryption Algorithm (CRYSTALS-Kyber)

**Yasir Nasser Hasan[1], Abdullah Mhmood Jasim[2], Sami Nazim Hussein[3]**
[1] Basrah University, Iraq
[2] Tikrit University, Iraq
[3] General Directorate of Education, Salah al-Din, Iraq

**DOI : https://doi.org/10.61796/ipteks.v3i3.523**

**Sections Info**

***Article history:***
Submitted: April 07, 2026
Final Revised: May 26, 2026
Accepted: June 18, 2026
Published: July 05, 2026

***Keywords:***
Post-Quantum Cryptography
AES
CRYSTALS-Kyber
Quantum Threats
Hybrid Encryption
Information Security

**ABSTRACT**

***Objective:*** *This research offers a comparative analysis between the Advanced Encryption Standard (AES) and the post-quantum cryptographic algorithm known as CRYSTALS-Kyber, particularly in response to the increasing dangers that quantum computing presents to conventional encryption methods. The study focuses on the significant issues created by quantum machines that can tackle the intricate mathematical challenges foundational to traditional cryptographic techniques.* ***Method:*** *A practical comparative analysis method is utilized in this research, which evaluates the computational efficiency (in terms of encryption and decryption duration), memory usage and security levels for both algorithms under controlled programming settings.* ***Results:*** *The findings indicate that AES is more effective regarding speed and resource utilization for everyday use cases, like the Internet of Things (IoT) and electronic payment systems* ***Novelty:*** *In contrast, CRYSTALS-Kyber demonstrates its capability as a strong security standard against quantum threats positioning it as a vital requirement for safeguarding sensitive information in the long term.*

## INTRODUCTION

Encryption is viewed as the fundamental foundation of securing data. It serves as the most straightforward and essential approach to ensure that information within computer systems remains protected from theft or unauthorized access for harmful intents. Both individual users and large businesses extensively employ data encryption to safeguard information exchanged between servers and browsers. This information can range from personal data to payment details. Encryption tools, often referred to as "encryption algorithms" or simply "encryption," are utilized to create a system that theoretically cannot be breached except by extremely powerful computational resources. The risk associated with quantum computing regarding data security stems from its potential to overcome existing encryption techniques that rely on intricate mathematical puzzles. Quantum computers can resolve these issues significantly quicker than conventional computers. This advancement could put sensitive information at risk and threaten secure communications. It is crucial for organizations to shift towards encryption that can withstand quantum computing threats and to implement proactive

measures to protect their systems prior to the widespread emergence of quantum computing [1], [2].

**Research Objective and Significance**

This research intends to deliver an extensive theoretical analysis of ideas connected to classical and quantum cryptography, emphasizing the key distinctions between conventional algorithms and those designed for a post-quantum setting. The focus of the research is to perform a detailed comparison between the Advanced Encryption Standard (AES) algorithm and the post-quantum encryption algorithm known as CRYSTALS-Kyber, specifically regarding their security levels and operational effectiveness. Additionally, the research investigates the primary difficulties tied to moving toward encryption frameworks that can withstand quantum threats, while evaluating the benefits and drawbacks of each algorithm being analyzed, considering the swift advancements in quantum computing technology and their potential impact on the domain of information security [3], [4], [5].

**Problem Statement**

Most earlier research has concentrated on assessing different types of encryption methods separately, either through analytical approaches or tests with narrow focus, failing to provide an overarching assessment that compares the effectiveness of traditional algorithms with those intended for the post-quantum period. Investigations that evaluate these algorithms in practical scenarios, particularly regarding expected quantum-related threats, are still quite few. This underscores the pressing requirement for comprehensive studies that illustrate the significance and functionality of post-quantum algorithms in real-world settings, such as communication infrastructures, Internet of Things systems, and cloud storage services, while taking into account factors like security, performance, and compatibility.

**Scientific Contribution**

This research offers an analysis contrasting the Advanced Encryption Standard (AES) method and the post-quantum encryption method (CRYSTALS-Kyber) in different areas, including memory usage, time of execution, and security measures. By conducting this research, a valuable scientific contribution is made, presenting widely applicable comparison findings that assist researchers in making informed security design decisions and ensuring these algorithms are prepared for practical implementation in meeting security needs.

**Previous Research**

Communication Schemes for UAVs in 5G:

This research introduces a secure communication framework for Unmanned Aerial Vehicles (UAVs) along with ground stations operating within 5G networks, tackling significant issues related to network security. The solution presented combines the Advanced Encryption Standard (AES) and CRYSTALS-Kyber for key encapsulation,

establishing a hybrid encryption approach that reduces the risk of quantum assaults (Sharma, S. A. Soleymani, M. Shojafar, and R. Tafazolli, 2025-p87).

The framework utilizes a client-server paradigm, with UAVs functioning as clients while the ground station is the server. Results from experiments indicate that CRYSTALS-Kyber offers strong defense against quantum threats with low operating expenses, making it exceptionally appropriate for UAVs with limited resources because of its association with AES.

Performance Analysis and Industry Deployment of Post-Quantum

Cryptography Algorithms:

This document examines the adoption of post-quantum algorithms in the telecommunications sector, concentrating on CRYSTALS-Kyber and CRYSTALS-Dilithium, which have roles in key exchange and digital signature processes in authentication systems.

The investigation assesses how CRYSTALS-Kyber and CRYSTALS-Dilithium compare with conventional algorithms such as AES and ECDSA regarding the speed of key generation. The findings illustrate that Kyber and Dilithium attain effective execution times, underscoring an immediate necessity for modifications in network infrastructure designs.

CRYSTALS-Kyber: Secure Model - Lattice-Based KEM:

This study mainly focuses on the structure of CRYSTALS-Kyber, detailing the encryption technique as outlined in this standard while assessing its resilience against possible quantum threats. It underscores the significance of advancing post-quantum computing, especially after the NIST announcement highlighting the demand for novel digital encryption methods.

NIST Report on Post-Quantum Cryptography (NIST / National Institute of Standards and Technology):

This document outlines how quantum computing affects conventional encryption techniques and emphasizes the urgency of creating quantum-resistant algorithms, juxtaposing them with existing standards like AES and RSA.

Hybrid Cryptography Concept:

This document elaborates on the idea of hybrid cryptography and its implementation as a temporary solution for transitioning from traditional algorithms to newer, quantum-resistant alternatives.

One:Hybrid Cryptography Concept (Hybrid Cryptography Conference):

A document examining the idea of hybrid cryptography and its role as a connector for moving from conventional techniques to methods suitable for post-quantum computing.

Traditional Encryption: Conventional techniques employed to safeguard information by transforming it into a format that cannot be understood without a key

(both the encryption and decryption key). The information intended for encryption is provided, and the process alters it into ciphertext via a designated key, making the text incomprehensible. When received, the information can be restored to its original form using the same key.

Advanced Encryption Standard (AES) Algorithm: Regarded as one of the most significant traditional encryption techniques, it is extensively utilized to protect essential information. Its features include high efficiency, robust security, and adaptability, establishing it as a worldwide benchmark for ensuring data safety. Below are several typical applications of the AES standard:

Secure Communications: Employed to encrypt information transmitted via the internet or private networks, such as in VoIP services, where it secures audio and video discussions, and HTTP, which is utilized in web browsers for securing exchanges between websites and users.

File and Record Encryption: Safeguards files and databases stored on personal devices or in cloud environments.

Disk and Storage Media Encryption: Full-disk encryption methods rely on the AES standard, ensuring the safety of information on hard drives and storage devices (A. Sharma, R. Patel, and N. Kumar p. 145–158).

Wireless Network Security: The AES algorithm is utilized in wireless security frameworks to secure data transmitted via Wi-Fi networks, including WPA2, where it encodes wireless communications to block unauthorized interception or alteration [6], [7], [8].

Government and Military Applications: Numerous governments have endorsed AES to protect vital and confidential data.

Payment Systems and Financial Transactions: AES safeguards private financial information during digital payment processes and transactions, including online banking platforms and electronic wallets.

Cloud Storage Security: Data held in cloud-based systems is encrypted by AES to guard against unauthorized access. Services such as Google Drive and Dropbox implement the AES protocol to guarantee the protection of user documents.

Password Tools: AES protects passwords kept within password management software. Tools such as LastPass rely on the AES system to secure stored credentials.

Internet of Things (IoT): Data shared between smart devices and central servers is encrypted using AES.

Software Applications: The AES standard is employed to secure data within applications, such as protecting messages in messaging platforms like WhatsApp and Telegram (M. Barbosa, F. Dupressoir, A. Hülsing, 2024. p98) [9], [10], [11].

Two:Software Applications

The AES encryption standard is utilized for safeguarding application data, including the encryption of information within messaging platforms such as WhatsApp and Telegram.

Healthcare and Medical Records: AES secures electronic health records and confidential patient details to ensure adherence to regulations, as well as encrypting patient documentation within medical facilities.

Data Backup and Archiving: AES guarantees the protection of backup data, preventing unauthorized access.Quantum Computing: This advanced technology relies on the principles of quantum mechanics for processing information. Unlike conventional bits that represent 0 or 1, it utilizes (Qubits), which can simultaneously represent both states due to Quantum Superposition. This characteristic enables the execution of intricate operations at remarkable speeds across various domains, including cryptography and artificial intelligence.

AES, CRYSTALS, and Quantum Attacks:

The main threat to the AES algorithm comes from Grover's Algorithm, a quantum computing method that facilitates swift, unstructured searches for encryption keys, drastically shortening the time needed to break them. Increasing the key length is viewed as a temporary fix and merely provides a slight buffer; hence, the symmetric AES standard is not advisable for long-term data protection (D. D. Demir, B. Bilgin, and M. C. Onbasli 2025-p98).KyberSlash Attack: This form of attack was first identified in 2023 against recognized quantum algorithms, prompting an immediate revision by the National Institute of Standards and Technology (NIST) concerning the CRYSTALS suite.

Important Concepts in Quantum Computing:

Quantum Superposition: The capacity of quantum computers to handle a vast amount of data simultaneously, providing them with extraordinary computational strength. In contrast to a conventional bit, which can solely be 0 or 1, a Qubit—the fundamental unit of information in quantum computing—can exist as 0, 1, or both at once.

Qubit: The fundamental information unit used in quantum computing. It is comparable to the bit utilized in classical computing, but it possesses enhanced features that enable it to convey and hold more data than a standard bit.

Quantum Entanglement: This phenomenon happens when two qubits are interconnected; knowing the state of one qubit immediately reveals the state of the other, which facilitates simultaneous processing and the establishment of secure communication links between devices (Borgaonkar, R., & Niemi, V. (2018), p. 90).

Post-Quantum Cryptography (PQC):

A concept that denotes the creation of advanced cryptographic techniques that can withstand assaults that might be conducted by upcoming quantum computers. This form of encryption is designed to safeguard confidential data and information from the

possible hazards introduced by quantum technology. The necessity for such encryption methods has arisen from the capacity of quantum systems to solve the intricate mathematical challenges on which conventional encryption practices depend.

CRYSTALS-Kyber: A prominent post-quantum cryptographic framework. It offers security against quantum computing threats and was chosen by the National Institute of Standards and Technology (NIST) as a standard procedure for protecting information in the age of quantum computation [12], [13], [14], [15].

## RESEARCH METHOD

The approach taken in this research relies on a comparative experimental analytical method that integrates theoretical examination with practical implementation. This approach is marked by its objectivity since the outcomes depend on real-world execution and direct observation. The comparison encompassed the following aspects:

Computational Efficiency: Assessed by the time taken for the algorithm to encrypt and decrypt data.

Memory Usage: Evaluated based on the memory space necessary for storing keys and executing operations (Daemen, J., & Rijmen, V. (2002). p98)

Suitability for Internet of Things (IoT): Evaluated with respect to memory consumption, as IoT devices typically have restricted memory capacities, rendering them unsuitable for algorithms that demand larger memory allocations.

**Test Environment**

The algorithms AES and CRYSTALS-Kyber were evaluated on a machine operating Windows 10. The application was created in the OnlineGDB setting for C++ coding. Moreover, the AES functionalities were implemented using the OpenSSL library, whereas the CRYSTALS functionalities relied on the Chrono library (National Institute of Standards and Technology (NIST). (2022)-p87)

**Four: Evaluation Metrics for Performance Assessment**

1. Execution Time (Duration): The encryption and decryption duration was determined for each algorithm using the same data volume.

First Experiment: A vector containing a set of numerical values was used. The number of iterations (500, 700, and 1000) was varied, with each iteration representing a complete encryption cycle where the program generates a new encryption key( Bos, J. W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky2018-p8)

Security Verification of the AES Algorithm

Key lengths (32 - 56 - 64 ... 512 bits) were utilized to estimate the number of possible keys and the time required to crack the algorithm.

| Key Size (bits) | Possible Keys (2^n) | Crack Time (Years) |
|---|---|---|
| 32 | 4.295e+09 | 1.361e-07 |
| 56 | 7.206e+16 | 2.283e+00 |
| 64 | 1.845e+19 | 5.845e+02 |
| 80 | 1.209e+24 | 3.831e+07 |
| 96 | 7.923e+28 | 2.511e+12 |

## RESULTS AND DISCUSSION

In Figure 1, the performance duration of the AES algorithm was analyzed by executing the algorithm several times. This involved repeatedly generating the encryption key to gather diverse timing information, allowing for a precise computation of the average performance duration and enabling a rational assessment between the two algorithms.

The comparison findings reveal that the AES algorithm is noted for its quickness with medium-length keys and minimal resource use, rendering it suitable for everyday data encryption, such as within Internet of Things (IoT) devices and digital payment systems. For IoT devices, it is efficient and requires less memory, while for payment processing, it delivers swift execution, making it ideal for instantaneous transactions.

On the other hand, the CRYSTALS-Kyber algorithm offers protection against quantum threats a detail confirmed by NIST, which recognized the algorithm's maturity for standardization as a quantum-resistant model. This quality positions it as the preferred option for key exchange by forming a shared secret key among communicating parties, as well as safeguarding sensitive information like personal identifiers, medical history, and financial data.

This research presented a model to enable a structured and practical evaluation between two distinct categories of encryption algorithms: the symmetric encryption algorithm (AES) and the post-quantum encryption algorithm (CRYSTALS-Kyber). The aim of this investigation was, at both theoretical and practical dimensions, to assess the performance of each algorithm based on execution duration and resource utilization.

## CONCLUSION

**Fundamental Finding:** The comparison findings reveal that the AES algorithm is noted for its quickness with medium-length keys and minimal resource use, rendering it suitable for everyday data encryption, such as within Internet of Things (IoT) devices and digital payment systems. **Implication:** This quality positions it as the preferred option for key exchange by forming a shared secret key among communicating parties, as well as safeguarding sensitive information like personal identifiers, medical history, and financial data. **Limitation:** The algorithms AES and CRYSTALS-Kyber were evaluated on a machine operating Windows 10. **Future Research:** This underscores the pressing requirement for comprehensive studies that illustrate the significance and functionality

of post-quantum algorithms in real-world settings, such as communication infrastructures, Internet of Things systems, and cloud storage services, while taking into account factors like security, performance, and compatibility.

## REFERENCES

[1] L. K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, ACM, 1996, pp. 212–219. doi: 10.1145/237814.237866.

[2] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, IEEE, 1994, pp. 124–134. doi: 10.1109/SFCS.1994.365700.

[3] G. Alagic *et al.*, "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process," 2022. doi: 10.6028/NIST.IR.8413.

[4] L. Chen *et al.*, "Report on Post-Quantum Cryptography," 2016. doi: 10.6028/NIST.IR.8105.

[5] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," 2023. doi: 10.6028/NIST.FIPS.197-upd1.

[6] National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," 2024. doi: 10.6028/NIST.FIPS.203.

[7] E. D. Demir, B. Bilgin, and M. C. Onbasli, "Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms," 2025. doi: 10.48550/arXiv.2503.12952.

[8] T. Sharma, S. A. Soleymani, M. Shojafar, and R. Tafazolli, "Secured Communication Schemes for UAVs in 5G: CRYSTALS-Kyber and IDS," 2025. doi: 10.48550/arXiv.2501.19191.

[9] A. K. Kwala, S. Kant, and A. Mishra, "Comparative analysis of lattice-based cryptographic schemes for secure IoT communications," *Discover Internet of Things*, vol. 4, no. 13, 2024, doi: 10.1007/s43926-024-00069-2.

[10] M. Barbosa, F. Dupressoir, A. Hülsing, M. Meijers, and P.-Y. Strub, "A Tight Security Proof for SPHINCS+, Formally Verified," in *Advances in Cryptology – ASIACRYPT 2024*, Springer, 2024. doi: 10.1007/978-981-96-0894-2_2.

[11] R. Borgaonkar and V. Niemi, "Security for Internet of Things: Analysis of Existing Protocols and Open Challenges," in *Proceedings of the 2nd International Conference on Cryptography*, 2018.

[12] J. W. Bos *et al.*, "CRYSTALS–Kyber: A CCA-Secure Module-Lattice-Based KEM," in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, 2018, pp. 353–367. doi: 10.1109/EuroSP.2018.00032.

[13] J. Daemen and V. Rijmen, *The Design of Rijndael: AES – The Advanced Encryption Standard*. Berlin, Heidelberg: Springer, 2002. doi: 10.1007/978-3-662-04722-4.

[14] National Institute of Standards and Technology, "Post-Quantum Cryptography Standardization," 2022.

[15] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017, doi: 10.1038/nature23461.

***Yasir Nasser Hasan (Corresponding Author)**
Basrah University, Iraq
Email: yasser.nasser@uobasrah.edu.iq

**Abdullah Mhmood Jasim**
Tikrit University, Iraq

Email: Abdullah.jasem122@tu.edu.iq

**Sami Nazim Hussein**
General Directorate of Education, Salah al-Din, Iraq
Email: sami.csp107@student.uomosul.edu.iq