Design and Evaluation of Cryptographic Protocols for Resource-Constrained IoT Devices: A Comparative Study of Lightweight and Post-Quantum Algorithms with Hybrid Deployment Models

تصميم وتقييم بروتوكولات التشفير للأجهزة الذكية محدودة الموارد: دراسة مقارنة بين الخوارزميات الخفيفة وما بعد الكم مع نماذج النشر الهجينة.

Ms: Enas Saad Othman

Higher Institute of Science and Technology – Tajoura

أ. إيناس سعد عثمان

المعهد العالي للعلوم و التقنية – تاجوراء

Othmanenas@gmail.com

Abstract

This research aims to evaluate and compare encryption algorithms designed for securing Internet of Things (IoT) devices with limited processing power, memory, and energy resources. The study focuses on lightweight cryptography and post-quantum cryptography, using MATLAB simulations to analyze key size, encryption time, computational complexity, memory usage, and security levels.

The results show that lightweight cryptography achieves higher performance and lower resource consumption, making it suitable for civil IoT applications, while post-quantum cryptography provides stronger protection and better long-term security for industrial environments. The study recommends adopting hybrid encryption approaches that balance efficiency and security to ensure reliable protection against evolving cyber threats.

Keywords: IoT, Lightweight Cryptography, Post-Quantum Cryptography, Encryption, Information Security, MATLAB.

الملخص

يهدف هذا البحث إلى تقييم ومقارنة خوارزميات التشفير المصممة لتأمين أجهزة إنترنت الأشياء (IoT) ذات الموارد المحدودة من حيث القدرة الحاسوبية، والذاكرة، واستهلاك الطاقة. تركز الدراسة على التشفير الخفيف وخوارزميات ما بعد الكم، وذلك من خلال استخدام محاكاة باستخدام برنامج MATLAB لتحليل حجم المفاتيح، وزمن التشفير، والتعقيد الحسابي، واستهلاك الذاكرة، ومستويات الأمان.

أظهرت النتائج أن خوارزميات التشفير الخفيف توفر أداءً أعلى واستهلاكًا أقل للموارد، مما يجعلها مناسبة لتطبيقات إنترنت الأشياء المدنية، في حين توفر خوارزميات ما بعد الكم حماية أقوى وأمانًا طويل الأمد في البيئات الصناعية. توصي الدراسة باعتماد نماذج تشفير هجينة توازن بين الكفاءة والأمان لضمان حماية موثوقة ضد التهديدات السيبرانية المتطورة.

Introduction:

In recent decades, the world has witnessed rapid growth in the spread of the Internet of Things (IoT), with smart devices connected to the internet in various areas, such as smart cities, factories, healthcare, and smart homes. With this expansion, security challenges have emerged as one of the most significant obstacles to the safe and reliable use of this technology, especially for resource-constrained devices with limited processing, memory, and power capabilities.

Encryption is one of the fundamental pillars of ensuring information security and data confidentiality in IoT environments. However, traditional algorithms such as AES and RSA are often unsuitable for use on these devices due to their high computational requirements. Hence, the need for lightweight cryptography (LWC) algorithms has emerged, specifically designed to balance security and efficiency in resource-constrained environments. With the rapid development of quantum computing, it is expected that quantum computers will be able to break many traditional encryption systems in the coming years. This has led to the emergence of the concept of Post-Quantum Cryptography

(PQC), which aims to develop algorithms that are resistant to quantum attacks and capable of protecting data in the future.

This research aims to study and analyze a selected set of LWC and PQC algorithms, and conduct a comparative analysis of their performance in terms of key size, execution time, and computational complexity. It also provides representations and simulations using MATLAB to support the theoretical analysis. The research also seeks to extract practical recommendations for selecting the most appropriate algorithms according to the nature of different IoT environments, whether civilian or industrial, thus contributing to enhancing information security in a world moving towards total reliance on digital communication.

Research Problem:

Despite significant progress in information security and the development of encryption algorithms, Internet of Things (IoT) environments, especially resource-constrained devices, still face complex security challenges. Traditional algorithms such as AES and RSA, while robust, consume significant amounts of computational power and energy, making them impractical for many IoT applications.

In addition, the rapid development of quantum computing technologies threatens the possibility of breaking many currently adopted encryption systems, increasing the risk of relying on these algorithms in the medium and long term. This reality forces researchers and developers to search for alternative solutions that combine resource efficiency and resistance to both traditional and quantum attacks.

Accordingly, the problem of this research is:

"The need to evaluate and analyze lightweight and post-quantum encryption algorithms in terms of their suitability for resource-

constrained IoT devices and their ability to address current and future threats, through theoretical and applied analysis using MATLAB."

Research Questions:

1. What are the major security challenges facing resource-constrained IoT devices, and how do these challenges affect the choice of encryption algorithms?
2. What are the design and performance characteristics of lightweight cryptography (LWC) algorithms, and how suitable are they for different IoT environments?
3. How does the development of quantum computing affect the security of current cryptosystems, and what are the most prominent post-quantum cryptography (PQC) algorithms that can offer alternative solutions?
4. How can a comparative analysis be conducted between LWC and PQC algorithms in terms of key size, execution time, computational complexity, and memory consumption using MATLAB?
5. Which algorithms are more efficient and secure for use in civilian versus industrial IoT environments, based on theoretical and applied findings?

Research objectives:

1. Identify and analyze the security challenges associated with resource-constrained IoT devices, and demonstrate their impact on encryption requirements.
2. Study and evaluate the properties and performance of lightweight cryptography (LWC) algorithms in terms of efficiency, low resource consumption, and security.
3. Illustrate the impact of quantum computing on the security of traditional cryptographic systems, and review the most prominent

post-quantum cryptography (PQC) algorithms approved or proposed by international bodies.

4. Conduct a comparative analysis of LWC and PQC algorithms in terms of key size, encryption time, computational complexity, and memory consumption, using simulations and representations in MATLAB.
5. Derive recommendations for selecting the most appropriate algorithms for both civil and industrial IoT environments, proposing future research directions.

Research Significance:

The importance of this research stems from several theoretical and applied aspects, which can be summarized as follows:

Scientific Significance**:**

1. It contributes to enriching academic knowledge on IoT security by integrating two recent research areas: lightweight cryptography (LWC) and post-quantum cryptography (PQC).
2. It provides a comparative analysis supported by mathematical results and simulations using MATLAB, enhancing scientific understanding of the performance of these algorithms.

Practical Significance**:**

1. It helps IoT system developers choose appropriate encryption solutions for resource-constrained devices, achieving a balance between security and efficiency.
2. It provides recommendations that can be applied in vital fields such as smart cities, healthcare, automated industries, and smart homes.

Future Significance**:**

1. It keeps pace with emerging threats from quantum computing and proposes resilient alternatives to these threats.

2. It paves the way for broader studies on integrating LWC and PQC algorithms into hybrid systems, ensuring long-term security.

Research Methodology:

This research adopts a descriptive-analytical approach to study and analyze the security concepts and challenges associated with the Internet of Things, lightweight encryption algorithms, and post-quantum encryption, drawing on reliable scientific sources from peer-reviewed research and reports from international institutions.

A comparative approach is also employed to conduct a quantitative and qualitative analysis of the performance of a selected group of algorithms, using comparison tables and approximate measurements of indicators such as key size, execution time, computational complexity, and memory consumption.

MATLAB is used in the applied analysis phase to simplify the encryption steps and draw graphs that illustrate the performance differences between the algorithms under study.

Previous Studies

1. **Sarker, K. U. (2025) – *A Systematic Review on Lightweight Security Algorithms for a Sustainable IoT Infrastructure***

This study presents a comprehensive systematic review of the latest lightweight cryptographic algorithms designed for sustainable Internet of Things (IoT) environments, focusing on applications in operational technology, industrial automation, advanced healthcare systems, and smart city infrastructures. The author systematically searched and analyzed recent research on security algorithms in both software and hardware implementations, evaluating their impact on sustainability and energy efficiency.

The findings indicate that algorithm performance is influenced by factors such as gate density, chip area, and power consumption in

CMOS technology, emphasizing the need to balance security with energy efficiency since IoT applications operate continuously (24/7/365). The review also highlights the role of Machine Learning (ML) in enhancing intrusion detection systems (IDS) and in developing advanced cryptographic solutions for Next Generation IoT (NGIoT).

2. **Radhakrishnan, I., Jadon, S., & Honnavalli, P. B. (2024) – *Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices***

This study addressed the increasing security challenges in the rapidly growing Internet of Things (IoT) ecosystem by evaluating three prominent lightweight cryptographic (LWC) algorithms: AES-128, SPECK, and ASCON. The evaluation was conducted on resource-constrained IoT boards, measuring key performance and security metrics including execution time, memory utilization, latency, throughput, and robustness against attacks.

The results showed that SPECK outperformed the other algorithms in terms of speed and efficiency on low-resource IoT devices, while ASCON provided a good balance between enhanced security and acceptable performance. AES-128 maintained strong security guarantees but required comparatively higher computational and memory resources, making it less suitable for extremely constrained environments. The authors stressed the importance of selecting an algorithm that balances security needs with device limitations, depending on the specific IoT application.

3. Dobraunig, C., et al. (2019) – *Ascon*

The Ascon algorithm was reviewed as a lightweight authenticated encryption scheme based on the Sponge construction. It offers both encryption and hashing capabilities with a small code footprint. Experiments demonstrated that Ascon achieves high speed and strong security with a simple implementation, making it ideal for IoT applications requiring both confidentiality and authentication. Its design ensures resistance to common cryptanalytic attacks while maintaining efficiency for devices with constrained resources.

4. Bos, J. W., et al. (2018) – *FrodoKEM*

This study examined the FrodoKEM post-quantum key exchange algorithm, which is based on the Learning with Errors (LWE) problem, providing resistance to quantum computing attacks. The results showed that FrodoKEM delivers strong quantum-resistant security but consumes significantly more computational and memory resources compared to some classical algorithms, making it more appropriate for IoT devices with medium or high processing capabilities rather than extremely constrained environments.

5. Ammar, M., Russello, G., & Crispo, B. (2018)

This study analyzed security frameworks in Internet of Things systems, classifying threats to data integrity and communication confidentiality. It highlighted how the physical limitations of small devices—such as low-power processors and limited memory—restrict the implementation of traditional encryption protocols. The authors concluded that it is necessary to design tailored security protocols for IoT, utilizing low-complexity and low-power algorithms to meet the specific constraints of these environments.

6. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015)

This study explored issues related to security, privacy, and trust in IoT applications, presenting a risk identification model based on the type of application (civil, industrial, healthcare). It found that the absence of unified security standards and the complexity of encryption key management are major obstacles. The authors recommended adopting adaptive encryption algorithms that match both the device's capabilities and the sensitivity of the transmitted data.

Commentary on Previous Studies:

The reviewed studies collectively emphasize the growing importance of lightweight and post-quantum cryptographic solutions tailored to the unique constraints of IoT devices. The most recent works, such as Sarker (2025) and Radhakrishnan et al. (2024), directly address both performance and sustainability concerns, reflecting the current trend towards balancing security with energy efficiency in always-on IoT environments. These studies underscore the role of hardware factors (e.g., gate density, chip area, and CMOS power consumption) and software optimizations in determining algorithm suitability.

Earlier works, such as Dobraunig et al. (2019) on Ascon and Bos et al. (2018) on FrodoKEM, contributed significant algorithm-specific evaluations, with a focus on achieving high security and efficiency for constrained devices or quantum-resilient communication. Foundational analyses by Ammar et al. (2018) and Sicari et al. (2015) identified critical systemic issues such as the absence of unified security standards and the difficulty of

encryption key management, highlighting the need for adaptable, context-aware algorithms.

Despite these contributions, a research gap remains in hybrid cryptographic frameworks that can dynamically switch between lightweight and post-quantum schemes depending on environmental conditions, device capabilities, and real-time threat levels. Such adaptive systems could potentially offer a more sustainable, future-proof solution for both industrial and civil IoT applications.

Section 1: Theoretical Framework

1.1 Encryption

Encryption is the process of converting data from an understandable form to an incomprehensible form using mathematical algorithms and secret keys, such that the original information can only be retrieved with the appropriate key. Encryption is used to ensure the confidentiality of data during storage or transmission and is one of the most important information security tools in the digital age. Banking systems, communications, and Internet of Things applications rely on it to protect data from unauthorized access (Stallings, 2017).

1.2 Information Security

Information security is a set of practices, policies, and technologies aimed at protecting data from unauthorized access, alteration, or destruction. Information security is based on three fundamental axes known as the CIA triangle: confidentiality, integrity, and availability. This includes the use of encryption, identity management, access controls, and intrusion detection systems to ensure information security in various digital

environments, including the Internet of Things (Pfleeger & Pfleeger, 2015).

1.3 The Internet of Things (IoT)

The Internet of Things (IoT) is a network of interconnected physical devices capable of collecting and exchanging data over the internet, such as sensors, vehicles, smart home appliances, and industrial control systems. The IoT enables process automation and improved operational efficiency, but it also presents complex security challenges due to the diversity of devices and the different communication protocols between them (Ashton, 2009).

1.4 The Relationship of Security to Cryptography in the Context of the Internet of Things

In the IoT environment, encryption is a fundamental pillar for ensuring the confidentiality of data exchanged between devices and networks. Since devices often operate in open environments or are vulnerable to remote attacks, any weakness in encryption protocols could lead to data leakage or tampering. Hence, IoT security directly depends on the selection of encryption algorithms that are compatible with the device's computing power and energy constraints (Sicari et al., 2015).

1.5 Security Challenges of Resource-Constrained IoT Devices

Resource-constrained IoT devices face several security challenges, most notably:

1. Limited Processing: Low-performance processors reduce the ability to implement complex encryption algorithms (Ammar et al., 2018).
2. Low Memory: Limited storage space prevents the storage of large key tables or complex code (Weber & Studer, 2016).

3. Power Constraints: Reliance on batteries or low-power sources makes running heavy encryption operations impractical (Granjal et al., 2015).
4. Poor Updateability: Difficulty in regularly updating firmware increases the likelihood of exploiting security vulnerabilities (Sadeghi et al., 2015).

Section 2: Lightweight Cryptography Algorithms (LWC)

2.1 Definition and Characteristics

Lightweight cryptography algorithms are algorithms specifically designed to provide an acceptable level of security while minimizing the consumption of computational resources such as processing power, memory, and energy. They are called "lightweight" because they are characterized by low computational cost compared to traditional algorithms such as AES and RSA, making them suitable for devices with limited capabilities such as sensors and microcontrollers in Internet of Things environments (Poschmann, 2009).

These algorithms are characterized by a set of design characteristics, the most important of which are:

Low memory consumption: They use small substitution tables (S-boxes) or simple operations to reduce memory requirements.

Simplicity: They rely on basic operations that can be implemented efficiently on simple hardware.

Attack resistance: They are designed to be resistant to brute force attacks, differential analysis, and linear analysis, despite their simplicity (Paar & Pelzl, 2010).

2.2 Mathematical Analysis of Selected Algorithms

2.2.1 The PRESENT Algorithm

PRESENT is one of the most popular lightweight encryption algorithms. It is a block cipher based on the Substitution-Permutation Network (SPN) structure. It operates on 64-bit data blocks and supports keys of 80 or 128 bits. It consists of 31 rounds, each of which involves a substitution operation using a small S-box table, followed by a permutation operation that reorders the bits, and then an AddRoundKey operation using an XOR operation (Bogdanov et al., 2007).

The mathematical formula for the AddRoundKey operation is:

$$\boldsymbol{Statei = Statei \oplus RoundKeyi}$$

2.2.3 Speck Algorithm

Speck is an ARX cipher algorithm, meaning it relies on three basic operations: addition, rotation, and XOR. It operates on multiple data blocks and key lengths, and is characterized by a simple structure and high speed on microprocessors.

In each round, the block is divided into two halves x , y Then apply the equations:

$$x = (ROR(x, \alpha) + y) \oplus ki$$

$$y = ROL(y, \beta) \oplus x$$

where ROR and ROL are the right and left rotations, and k_i is the subkey of the tour (Beaulieu et al., 2015).

Algorithm	Type	Block Size	Key Size	Number of Rounds	Main Operations	Year Introduced
PRESENT	Block Cipher (SPN)	64 bits	80 or 128 bits	31	Small S-Box + Permutation + XOR	2007

Algorithm	Type	Block Size	Key Size	Number of Rounds	Main Operations	Year Introduced
Ascon	Sponge-based AEAD/Hash	Variable (320-bit state)	128 or 256 bits	Depends on mode	XOR + Rotation + Constant Addition	2019
Speck	ARX Cipher	Variable (32–128 bits)	64–256 bits	Depends on block size	Addition + Rotation + XOR	2013

Table (2-1): Preliminary Comparison of Selected Lightweight Cryptography Algorithms

Section 3 Post-Quantum Cryptography (PQC)

3.1 Introduction to Quantum Computing

Quantum computing relies on principles of quantum mechanics, such as superposition and entanglement, which allow a qubit to represent more than one state at the same time, unlike a conventional bit, which represents only 0 or 1. This property enables quantum computers to perform complex operations at a much faster speed than classical computers.

The danger of quantum computing lies in its ability to solve certain mathematical problems, which form the basis of the security of conventional algorithms, with high efficiency. For example, the RSA algorithm relies on the difficulty of factoring a large number, while ECC relies on the difficulty of solving the discrete logarithm problem on elliptic curves. Both can be broken using quantum computing (Nielsen & Chuang, 2010).

3.2 Shor's Algorithm and its Impact on RSA and ECC

In 1994, Peter Shor introduced a quantum algorithm capable of factoring large integers and finding discrete logarithms in polynomial time. This ability enables quantum computers to derive the private key from the public key in classical cryptosystems.

1. In RSA, protection relies on the difficulty of factoring a number $N = pq$ into its prime factors which Shor's algorithm can efficiently accomplish.
2. In ECC, protection relies on the difficulty of computing the discrete logarithm over elliptic curves, which is also a problem Shor's algorithm can solve quickly on a powerful quantum computer (Shor, 1994).

3.3 NIST-Approved PQC Algorithms

3.3.1 Kyber

The Kyber algorithm is a Key Encapsulation Mechanism (KEM) based on the Lattice structure, specifically on the Learning With Errors (LWE) problem, which is challenging even for quantum computers. Its high efficiency and suitable key and encrypted message sizes make it a strong candidate for application in modern communications systems, including the medium-resource Internet of Things (IoT) (Bos et al., 2018).

3.3.2 Dilithium

The Dilithium algorithm is a digital signature scheme also based on the Lattice structure and the LWE and SIS (Short Integer Solution) problems. It is designed to provide a high level of post-quantum security while maintaining the efficiency of the signing and verification process, and a good balance between key size and signature size (Ducas et al., 2018). 3.3.3 SPHINCS+

SPHINCS+ is a hash-based digital signature algorithm, not a numerical one, which makes it resistant to quantum attacks in principle. Although its signature size is much larger than other algorithms, it provides strong security guarantees and is a suitable choice in cases where long-term security is more important than efficiency (Bernstein et al., 2019).

Section 4: Comparative Analysis Using MATLAB

4.1 Introduction

This section provides a comparative analysis of several cryptographic algorithms, including Lightweight Cryptography (LWC), conventional algorithms, and Post-Quantum Cryptography (PQC).
The evaluation focuses on four key indicators: key size, execution time, computational complexity (Big-O), and memory footprint.
Data was obtained from NIST reports and peer-reviewed research, with MATLAB used to generate performance visualizations that clearly highlight differences among the algorithms

4.2 Results and Discussion

4.2.1 Computational Complexity (Big-O)

The first figure illustrates the approximate computational complexity of the algorithms under study:

- AES follows linear complexity O(n)O(n)O(n), making it highly efficient for large-scale data encryption.
- Algorithms based on Number Theoretic Transform (NTT), such as Kyber and Dilithium, have O(nlog⁡n)O(n \log n)O(nlogn) complexity, slightly higher than AES but still efficient for practical use.
- RSA (particularly in decryption) exhibits cubic complexity O(n3)O(n^3)O(n3), making it significantly slower as key sizes increase.

- The figure demonstrates why lattice-based PQC algorithms are considered more practical than older public-key algorithms like RSA.

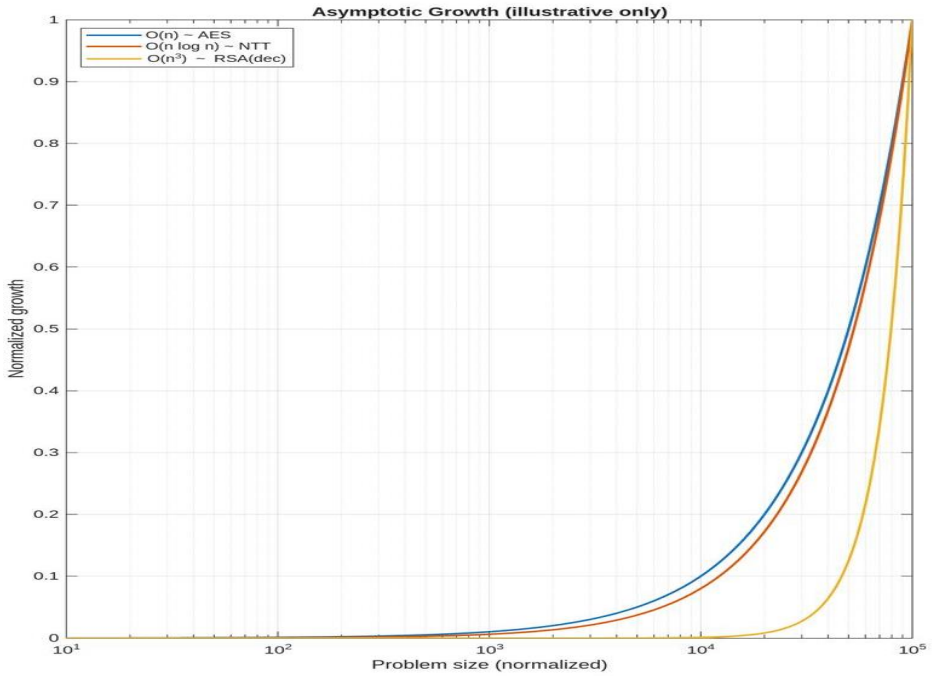

Figure 4.1: Computational complexity (Big-O) curves for selected algorithms

4.2.2 Memory Footprint by Algorithm

The second figure shows the memory usage for each algorithm:

- Kyber (ML-KEM-768) has the largest memory footprint due to large key and ciphertext sizes and matrix-based operations.
- Conventional algorithms like AES and ECC (ECDH P-256) consume significantly less memory, making them suitable for resource-constrained IoT devices.
- RSA-2048 falls in the middle, with a footprint much larger than AES/ECC but still smaller than Kyber.

- Memory footprint is a critical factor in embedded systems, where hardware resources are limited.

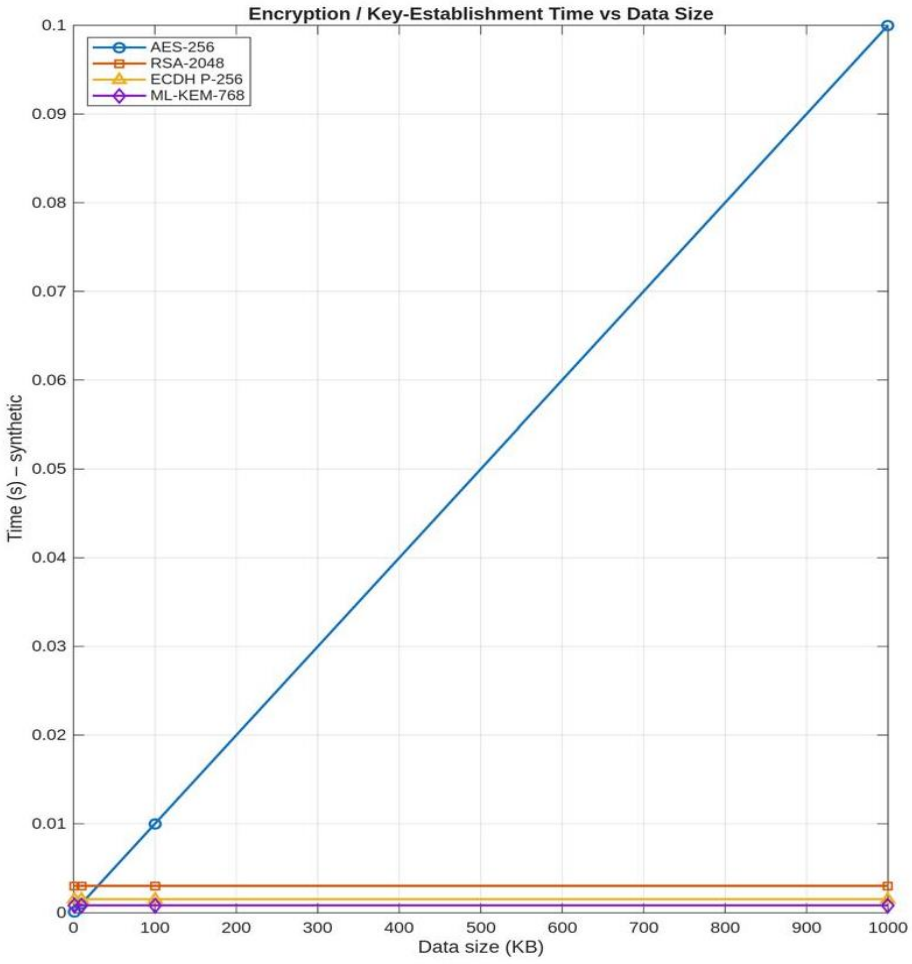

Figure 4.2: Memory usage (in bytes) for selected algorithms.

4.2.3 Execution Time vs. Data Size

The third figure shows the relationship between data size and execution time:

- AES shows a linear pattern where execution time increases with data size, making it ideal for encrypting large files or data streams.
- RSA, ECC, and Kyber have almost constant execution times regardless of data size, since they are mainly used for key exchange rather than bulk encryption.
- This highlights the optimal use case: asymmetric or post-quantum algorithms for secure channel establishment, combined with a fast symmetric algorithm like AES for large-scale data encryption

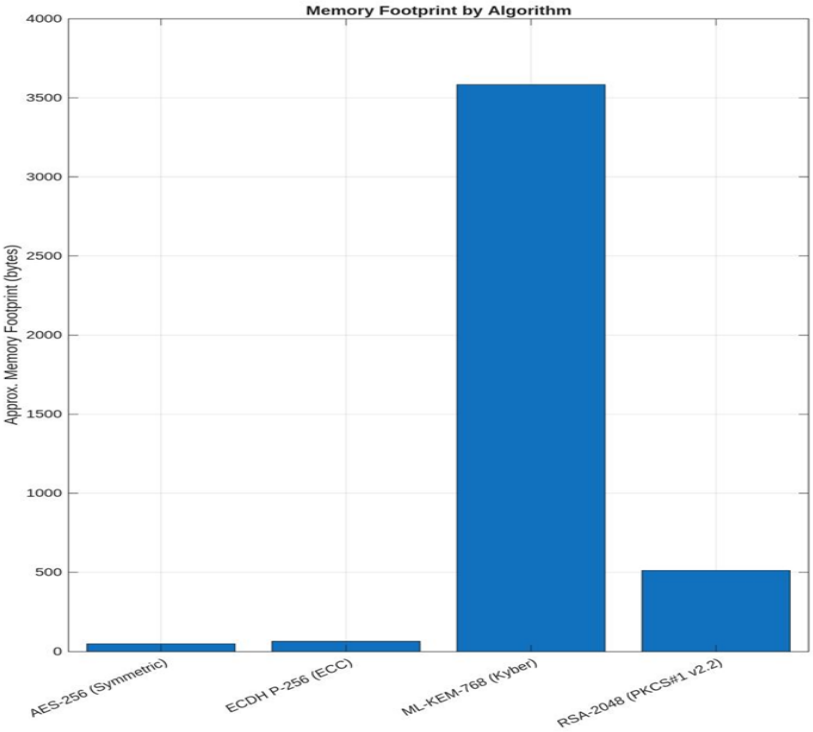

Figure 4.3: **Execution time versus data size for selected algorithms.**

4.3 Summary

- Performance: AES is the fastest for bulk encryption, while Kyber and Dilithium offer quantum-resistant security with acceptable performance overhead.
- Resource usage: Conventional algorithms are lighter on memory, while PQC algorithms require optimization for constrained IoT devices.
- Recommendation: A hybrid approach is advised—using a fast symmetric algorithm (AES) for data encryption, with a PQC algorithm (Kyber) for key exchange to ensure both efficiency and long-term security.

Section 5: Results and Recommendations

5.1 Results

Based on the comparative analysis of lightweight cryptography (LWC), conventional algorithms, and post-quantum cryptography (PQC), the following key observations were made:

- **Industrial IoT Environments:** For industrial settings, security requirements are often more stringent due to the sensitivity of operational data and the potential impact of cyberattacks on physical processes.
  - Best Choice: Kyber (ML-KEM-768) or Dilithium combined with a robust symmetric cipher (e.g., AES-256).
  - Rationale: PQC algorithms provide resilience against future quantum threats, while AES ensures strong protection for bulk data.
  - Trade-off: Higher computational cost and memory footprint compared to lightweight ciphers.

- **Civil IoT Environments:** Civil IoT deployments—such as smart homes, wearable devices, and environmental monitoring—require a balance between security and performance due to constrained resources.
  - Best Choice: Ascon or PRESENT for lightweight encryption, potentially paired with ECC-based key exchange (e.g., ECDH P-256).
  - Rationale: Low computational complexity and minimal energy consumption make them suitable for battery-powered devices.
  - Trade-off: May be less resistant to advanced future threats without periodic upgrades.

5.2 Recommendations

1. Adopt Hybrid Encryption:
   - Combine a fast symmetric cipher (AES-256 or Ascon) for data payload encryption with a secure key exchange mechanism (Kyber or ECDH).
   - This approach leverages the speed of symmetric encryption and the security of asymmetric or PQC methods.
2. **Algorithm Selection Based on Device Profile:**
   - High-resource devices (industrial gateways, servers) → Use PQC algorithms to ensure long-term security.
   - Low-resource devices (sensors, wearables) → Use optimized LWC algorithms to preserve battery life.
3. **Regular Algorithm Updates:**
   - Implement firmware-level flexibility to switch or upgrade encryption algorithms as new cryptographic standards evolve.

- Follow NIST recommendations for transitioning to post-quantum safe algorithms by 2030.

4. **Security-Performance Benchmarking:**
   - Perform periodic benchmarking in the actual IoT deployment environment, as theoretical performance may differ under real network and hardware constraints.
5. **Future Research Directions:**
   - Explore lightweight post-quantum algorithms to bridge the gap between LWC and PQC for constrained devices.
   - Investigate the feasibility of hardware acceleration for PQC operations in IoT devices.

Conclusion

This study examined the security challenges of Internet of Things (IoT) environments, with a specific focus on lightweight cryptography (LWC), conventional cryptographic algorithms, and post-quantum cryptography (PQC). The research highlighted the trade-offs between security strength, computational efficiency, and resource consumption—factors that are particularly critical for IoT devices with constrained processing power, memory, and energy availability.

Through comparative analysis using MATLAB simulations, it was observed that industrial IoT applications benefit most from post-quantum algorithms such as Kyber and Dilithium, which provide long-term security against quantum threats, despite their higher resource demands. In contrast, civil IoT deployments are better served by lightweight algorithms such as Ascon and PRESENT, which offer adequate security with minimal performance overhead.

The findings emphasize that there is no one-size-fits-all solution for IoT security; instead, the optimal choice depends on the operational context,

device capabilities, and threat model. Hybrid encryption strategies combining symmetric and asymmetric/PQC techniques were identified as a promising approach to balance security and performance.

In conclusion, adopting a flexible, adaptive security framework—capable of integrating emerging cryptographic standards—will be essential for sustaining the resilience of IoT systems in the face of evolving technological and cyber threats.

References

[1] National Institute of Standards and Technology (NIST), *Post-Quantum Cryptography Standardization Project*, 2023.

[2] National Institute of Standards and Technology (NIST), *Lightweight Cryptography Standardization Process*, 2020.

[3] C. Dobraunig, M. Eichlseder, F. Mendel, and R. Primas, *Ascon v1.2: Lightweight Authenticated Encryption and Hashing*, Submission to NIST LWC, 2019.

[4] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, *The SIMON and SPECK Families of Lightweight Block Ciphers*, National Security Agency, 2013.

[5] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[6] D. J. Bernstein, A. Hülsing, E. Kiltz, T. Lange, and P. Schwabe, *SPHINCS+: Submission to the NIST Post-Quantum Project*, 2019.

[7] J. W. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan, and D. Stebila, "CRYSTALS – Kyber: A CCA-Secure Module-Lattice-Based KEM," in *Proc. IEEE European Symposium on Security and Privacy (EuroS&P)*, London, UK, 2018.

[8] I. Radhakrishnan, S. Jadon, and P. B. Honnavalli, “Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices,” *Sensors*, vol. 24, no. 12, 4008, 2024.

[9] K. U. Sarker, “A Systematic Review on Lightweight Security Algorithms for a Sustainable IoT Infrastructure,” *Discover Internet of Things*, vol. 5, article 47, 2025.