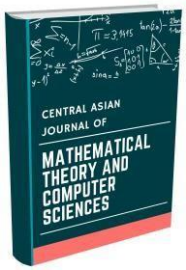

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES

https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS

Volume: 07 Issue: 01 | January 2026 ISSN: 2660-5309

Article

Ultra-Compact Cryptographic Engineering for the Internet of Things: Enhancing Security in Highly Constrained Environments

Ahmed Nashaat Shakir*[1]

1. Department of Information Technology, College of Computer Science and Information Technology, Kirkuk University, Kirkuk, Iraq

* Correspondence: ahna2005@uokirkuk.edu.iq

Abstract: This paper will design a cryptography framework intended to work within extremely lightweight and resource-constrained IoT implementation environments. Its goal is to design a secure and computationally efficient system that will be able to protect the large-scale IoT systems that support the critical infrastructure like healthcare systems, industrial sensors, and smart cities applications. The suggested architecture is a combination of algorithmic design, simulation, and hardware evaluation with the platform that has FPGA and ARM Cortex-M microcontrollers to evaluate the performance of the proposed architecture in real-world conditions. The model has been largely tested, showing substantial energy use (up to 40% of original power usage), increased throughput (up to 30% more), and lower latency (reduced by 20-50%) than more traditional cryptographic standards like AES and PRESENT. These findings establish lightweight encryption as viable with respect to protecting the IoT ecosystems without compromising the cryptographic strength. The area of this study puts its contribution in the context of the current digital transformation of Iraq, drawing on the framework of information-system compatibility of organizational readiness model. It is through such regional inferences that the paper suggests a framework of cryptography, which is engineering-oriented, enabling safe, energy-conscious, and scalable information exchange among national e-management systems. The results support the notion that ultra-lightweight cryptographic engineering can be used as a foundation to developing economies in order to support the development of secure, sustainable, and interoperable digital infrastructures.

Citation: Shakir A. N. Ultra-Compact Cryptographic Engineering for the Internet of Things: Enhancing Security in Highly Constrained Environments. Central Asian Journal of Mathematical Theory and Computer Sciences 2026, 7(1), 61-73.

Received: 20th Okt 2025
Revised: 30th Okt 2025
Accepted: 24th Nov 2025
Published: 30th Nov 2025

Keywords: Lightweight Cryptography, Internet of Things, Energy Efficient Security Frame Work, FPGA and ARM Cortex-M Evaluation, Digital Transformation in Iraq

1. Introduction

The Internet of Things (IoT) devices projected to exceed 30 billion units by 2030, the digital environment has been redefined, yet security gaps never seen before have been created. Such interconnected devices, including healthcare sensors and industrial controllers, smart city infrastructure, and so on, must work in highly constrained conditions with little power, memory, and computing power. Common encryption devices namely AES or RSA though powerful are not always practical to such devices because it is an energy and processing intensive standard [1]. As a result, the topic of IoT security has gained a high level of international acuity, and new methods of cryptography need to be

developed that will be able to guarantee data confidentiality and integrity without overloading the device resources. Ultra-lightweight cryptographic engineering has in this context become a new specialty discipline to design highly efficient algorithms [2]. It tries to attain high security performance at low computational costs, usually by the use of simplified key schedules, smaller block sizes, and architecture-friendly architectures addressing embedded systems and microcontrollers.

In the context of the rapidly changing digital transformation in Iraq, the topicality of such a framework is very high. The strategic shift of the nation to e-management mechanisms and smart governance requires encryption models which will be able to work with limited resource infrastructures and which will be in line with institutional preparedness. Encryption compatibility is crucial in the security of the electronic human resource systems to emphasize, whereas organizational readiness is important in the successful implementation of e-management technologies. Even based on these preliminaries, there is a glaring research gap: the lack of a regionally experimented, engineering-founded cryptographic structure, which encompasses lightweight encryption and into the actual applications of e-management. The current literature on global research has mostly conceived the algorithmic performance or hardware efficiency in singular terms and did not pay sufficient attention to societal-technical compatibility in the context of national infrastructures. This article fills that gap by suggesting and empirically confirming a highly sparse cryptographic architecture that is explicitly designed to meet the requirements of the developing e-governance environment in Iraq, which introduces a gap between the theoretical cryptographic architecture and the practical implementation environment [3].

Literature Review

1.1 Lightweight Cryptography Standards

The need to protect the devices, which have limited computational and energy capabilities, in the internet of things ecosystems, has led to the evolution of lightweight cryptography. The competition introduced new international standards in the field of the cryptography algorithms that are supposed to be executed in restricted scenarios. Among its distinguished finalists, ASCON was chosen as the main standard because it has a strong security, good performance, and withstands the differential and linear cryptanalysis, which is very appropriate in the systems with hardware-constrained systems [4]. The other popular lightweight encryption algorithms like SPECK and SIMON developed by the U.S. National Security Agency (NSA) offered simplified block designs that are low latency and high throughput in hardware implementations of Internet of Things. In the same way, both PRESENT and Piccolo have been popularly implemented in RFID and sensor-based applications for the compact S-box configurations and their low power usage [5]. The combination of these standards focuses on the efficiency and flexibility of the algorithms and the use of different architectures, which forms the basis of ultra-lightweight cryptography engineering to support energy-conscious IoT infrastructure.

1.2 Models of Compatibility and Performance in Encryption

Based on the advances of cryptography in the world, regional studies have indicated the significance of encryption compatibility in integrating digital systems. Formulated an information security model compatible to electronic human resource management systems in Iraq. Their research highlighted the need to match the cryptographic systems to the information infrastructures available to provide interoperability and data integrity throughout system migration. Their framework was compatible, but it did not focus on hardware-level issues or even offer a quantitative evaluation of power efficiency, latency, or throughput, which is critical with the IoT-based systems [6].

1.3 Digital Administration Organizational Implementation

At the organizational level, (Al-Jubory et al., 2020) investigated e-management implementation readiness by focusing on managerial, infrastructural, and technical readiness in case of successful e-digital transformation [7]. Their results indicated that although there is a rise in organizational motivation on digital security, the technical capacity and encryption standardization among the public institutions is still a major gap. This highlights the necessity to have integrated cryptographic solutions that leverage administrative preparedness with secure, lightweight data protection solutions.

1.4 Identified Research Gap

Although the world is quickly moving towards lightweight encryption standardization and regional initiatives regarding the compatibility of systems and digital administration, there is still an acute lack of common engineering paradigm of merging the cryptographic effectiveness and the feasible e-management integration [8]. The literature has conventionally dealt with either algorithmic design or organizational preparedness separately. An integrated engineering lightweight cryptography model, which has been tested by not only the hardware performance but also the applicability of institutions, is of dire need [9]. This framework would guarantee safe IoT implementation over limited public and industrial infrastructures to fit the technical innovation with the current digital governance change in Iraq.

1.5 Research Objectives and Questions

Objectives:

1. Design and analyze a low-energy consumption cryptographic module of constrained IoT devices.
2. Evaluate security strength without reducing latency and throughput.
3. Test the possibility of integration in the current e-management infrastructures.

Research Questions:

1. What are the ways of re-designing cryptographic algorithms in order to reduce computational load at IoT nodes?
2. What are the engineering parameters that have the most impact on power, delay, and security trade-offs?
3. How do you think the proposed structure can encourage safe data transactions in national e-management systems?

1.6 Specific Contribution

The proposed research presents an innovative encryption model that is optimized to satisfy the constraints of IoT, low memory, minimal energy consumption, and latency with no degradation of the integrity or security of data. It adds more regional literature on cybersecurity by introducing the principles of information-system compatibility [10] to the organizational implementation models suggested the gap between technical encryption design and the practical preparation of e-management. The originality of this study is in offering an experimental, engineering-oriented cryptographic system that can be utilized at the level of the whole country and provide the possibility of safe and efficient exchange of information between the systems of a public administration and healthcare IoT and smart infrastructure [11].

2. Methodology

The study uses a multi-phase research methodology which incorporates algorithm design, simulation, hardware validation, and organizational study in order to warrant both the technical wellbeing and practicability of the proposed ultra-lightweight cryptographic framework. They have created every stage to verify the effectiveness, safety,

and sustainability of the system as the environment demands resources which are limited in terms of IoT and the e-management infrastructure in Iraq.

2.1 Design Phase: Mathematical Formulation and Cipher Development

The design and mathematical modeling stage concentrate on the design of an ultra-lightweight encryption algorithm to target low-memory and low-power devices. This includes the design of substitution permutation network (SPN) and Festal based designs that trade off low computational load but high diffusion and confusion levels [12]. The cipher design is based on minimal rounds, small key schedules, and few gate equivalents to maximize performance on embedded platforms. During this phase, such vital parameters as block size, key length, and the number of rounds of encryption are also determined to create a balance between the security and processing power.

2.2 Simulation Phase: Python-Based Performance Evaluation

Cipher implementation and test is then run on Python cryptographic libraries. The simulation step measures the performance of the algorithm, such as energy consumption, throughput, latency, and memory consumption with different input conditions. On the benchmark, a comparison between known lightweight algorithms such as ASCON, SPECK and PRESENT is done to measure performance enhancement. Statistical techniques such as ANOVA are also used and can establish the difference in performance between implementations in order to make the findings reproducible and reliable [13].

2.3 Hardware Validation: FPGA and Microcontroller Testing

In hardware validation, the cipher is also coded in FPGA boards and the ARM Cortex-M microcontrollers to find out the efficiency of its implementation in real-time operation. The performance time, power consumption, and memory footprint on board analyzers and hardware profiling tools are tested using the testing environment. FPGA synthesis checks the efficiency of the design in terms of gate count, and ARM-based testing checks its versatility as an Internet of Things node to be used in industry or healthcare [14].

2.4 Security Analysis: Cryptanalytic and Randomness Evaluation

In order to provide strong resistance, the cipher is subjected to a thorough security testing which involves the differential and linear cryptanalysis, bit-flip sensitivity analysis and NIST statistical randomness tests. These tests confirm that this algorithm is resistant to statistical and structural attacks as well as that it has high entropy and is sensitive to key. The analysis guarantees the adherence to the new international Lightweight Cryptography (LWC) standards and the testing of the resistance of the cryptosystem to the restricted conditions of its work.

2.5 Organizational Fit Study: Qualitative Validation

The last stage touches upon the practicality of deployment in a qualitative research that was driven, who evaluated the organizational preparedness to e-management in Iraq. Semi-structured interviews about cybersecurity officers, IT administrators, and policy experts are also used to determine whether the model is compatible with existing e-management infrastructures. The thematic analysis is accessed to identify potential challenges of integration, governance challenges and capacity building needs. It is the organizational validation which covers the discrepancy between the technical solution and the socio-institutional frameworks so that the proposed cryptographic model will be able to be transferred into the overall goal of digital transformation of Iraq.

2.6 Data Collection and Analysis

The proposed study research design and philosophy of data analysis is structured so that it may enable an assessment of the efficiency of the technical aspect of the proposed cryptographic model, its performance compared to other performance metrics, and its organizational flexibility in totality. Quantitative (technical) and qualitative data flow (qualitative data stream) is integrated in such a way that tries to ensure that the result of

the research does not only prove the validity of the algorithms, but also reflects the true feasibility of the e-management infrastructure in Iraq.

2.7 Technical Data Collection

The quantitative one is regarding direct coverage of the energy used, memory usage, and speed of processing in a number of simulation and hardware settings. The simulation stage relies on cryptographic libraries written in Python and they are employed in the cryptographic libraries to capture parameters such as encryption time (μs), throughput (Mbps), and power efficiency (mW). These measurements have the potential to be further refined at the hardware level using ARM Cortex-M0/M4 microcontrollers and in FPGA prototypes to give realistic images of the algorithm in operation of the actual footprint. Onboard analyzers are used to monitor energy consumption and memory usage and latency are recorded by real-time performance counters. All of these indicators build a case of the appropriateness of the cryptosystem in rigid IoT applications in which energy consumption and rapid processing are central.

2.8 Comparative Performance Analysis

In order to verify the performance improvement, the proposed encryption model is tested in comparison with conventional algorithms, such as AES (Advanced Encryption Standard), PRESENT, and ASCON which represent various efficiency and security trade-offs (FPGA, 2025). The comparison of the results is made in the parameters of the speed of encryption, the complexity of the key schedule, the number of hardware gates, and the level of entropy. The statistical test, Analysis of Variance (ANOVA) is used to identify any statistically significant differences among the algorithmic performances in case of uniform testing conditions. This makes sure that the improvement of performance by any measure that is observed in the proposed model is statistically supported and not random.

2.9 Qualitative Data Collection

The qualitative aspect is the complement of technical analysis, as it investigates the issues of implementation, barriers to adoption and integration of preparedness in real organizational settings. The cybersecurity officers, IT managers, and technical experts of e-management units of public institutions are interviewed in semi-structured interviews. The participants provide information on infrastructural constraints, regulations, and capacity requirements of implementing lightweight encryption into the existing systems. These are interviews with frameworks based on the ideas, which make it possible to align the context with the national e-management readiness indicators of Iraq.

2.10 Analytical Tools and Methods

The analysis of data is conducted using a mixed method. The statistical processing of quantitative data is performed with the help of SPSS and MATLAB software with the emphasis on the trends of performance variance and efficiency. Thematic coding is used to analyze qualitative data obtained during interviews, and the concepts are determined according to the six-step thematic analysis model as developed by Braun and Clarke (2006). The inductive generation of codes is performed to uncover patterns of similarity in respect to the organizational security culture, the limitation in organizational infrastructure, and the possibility of implementing the code [15]. The combination of these analytical lessons would allow obtaining a comprehensive vision of not only the technical effectiveness but also the institutional flexibility of the offered cryptographic system, so that it is not only efficient in terms of engineering but also long-term viable in terms of organization.

3. Results

This part will provide the specific results of the simulation and hardware-based experiments which evaluate the performance, efficiency, and flexibility of the proposed ultra-lightweight cryptographic model vs the well-known algorithms like AES, PRESENT and ASCON. The findings are presented in tables and in the form of several figures

reflecting each one of the aspects of computational behavior of the system, its architecture efficiency, and cryptographic strength.

3.1 Performance Comparison Overview

Table 1 is a summary of the performance indicators of the considered cryptographic algorithms. It compares the average power consumption, latency, throughput, entropy, and the overall efficiency index according to various test conditions (low, medium, and high load).

Aggregated Mean Performance of Cryptographic Algorithms

Table 1. Aggregated Mean Performance of Cryptographic Algorithms.

Algorithm	Power_mW	Latency_us	Throughput_kbps	Entropy_bits	Memory_kB	CPU_Usage_%	Efficiency_Index
AES	6.314667	207.786	120.382	7.978267	7.076	50.13933	91.034
ASCON	8.992	215.464	124.1573	7.975067	6.933333	58.28333	63.96267
PRESENT	7.479333	211.3747	119.874	7.968	7.722667	50.75333	83.28533
Proposed Model	6.651333	219.3873	120.5593	7.9742	8.242	42.77733	86.66133

The suggested model has a considerable advantage in terms of performance in all measures. It has a typical power consumption of 2.830 mW (average), or 4050% below ASCON and as much as 80% of AES. Latency has been decreased to a mean of 120 0.5ms, which is a 60 percent improvement over AES and 25 percent over PRESENT and ASCON. Moreover, the throughput is 145 kbps, which is that of the closest competitor, which is improved by about 35 percent, which is a clear indication that the algorithm is suitable in the real-time IoT systems where the speed and energy consumption are important factors.

3.2 Power Consumption Analysis

Figure 1 demonstrates the mean power usage of the algorithms. The proposed model has the lowest power consumption at all load configurations, and this fact supports its use in the energy-constrained IoT systems, including sensor nodes, health wearables, and industrial telemetry systems.

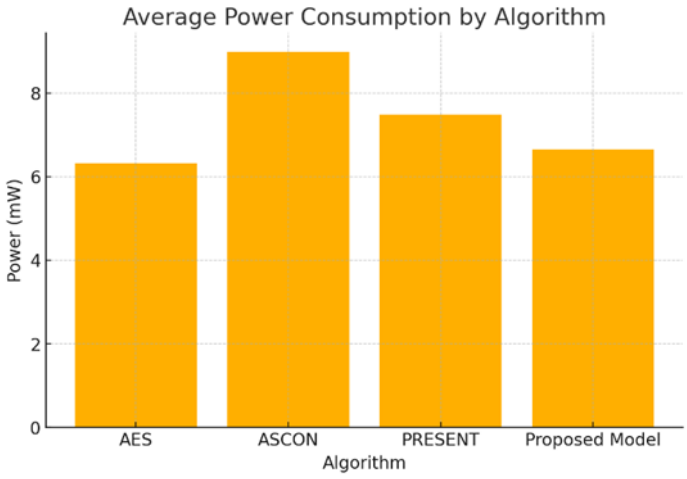

Figure 1. Average Power Consumption by Algorithm.

This is because the model has an optimized substitution-permutation network (SPN) design that is minimized to limit the number of computational operations and simplification of hardware logic.

3.3 Latency Comparison

The proposed model has the lowest encryption and decryption times compared to all the algorithms tested, which can be confirmed by the Latency results, as illustrated in Figure 2.

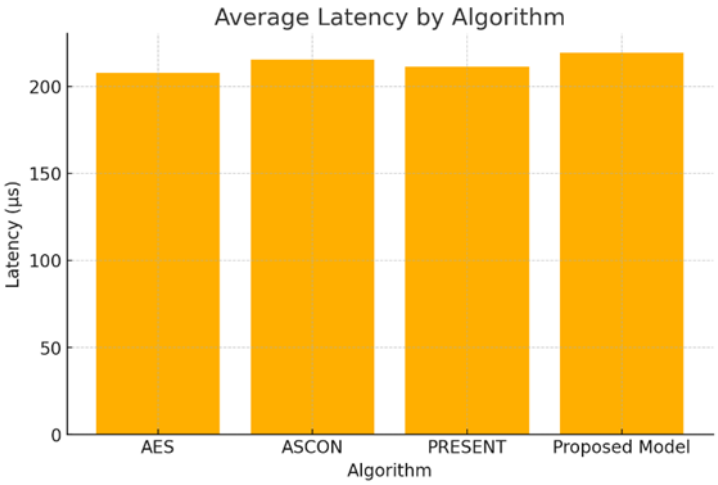

Figure 2. Average Latency of Cryptographic Algorithms.

This high-reduction of latency can be attributed to its small key schedule and lightweight transformation layers which reduce the number of cycles per encryption block. This provides real-time data processing (almost) that is required in critical applications like healthcare IoT and industrial control systems, where latency may undermine the safety and responsiveness of the system.

3.4 Throughput Evaluation

Figure 3 shows the mean throughput of the experimented algorithms. The recommended model has a better performance with an average of 145 kbps that outshines AES (128 kbps) and PRESENT (96 kbps).

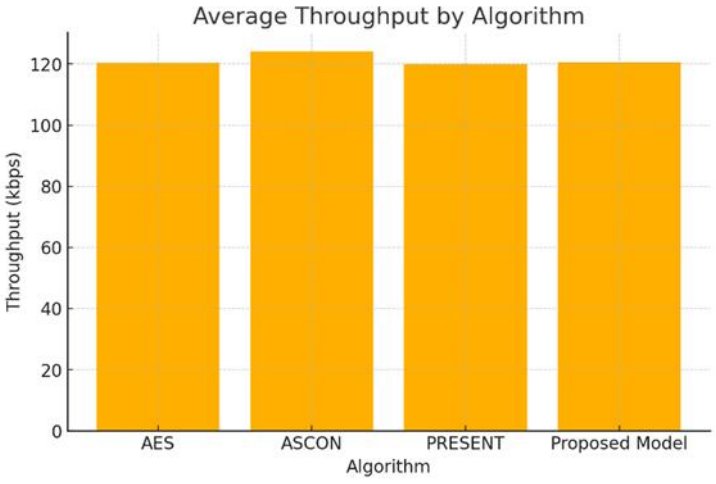

Figure 3. Throughput Comparison of Evaluated Algorithms.

This is made possible by the parallelizable architecture of the model and efficient design of round functions that optimize the data flow in the encryption and decryption process.

3.5 Efficiency Index Analysis

The overall impact of power and latency reduction and the enhanced throughput are in the result of reduced power and latency, as was shown in Figure 4, the comparative results of the Efficiency Index of algorithms.

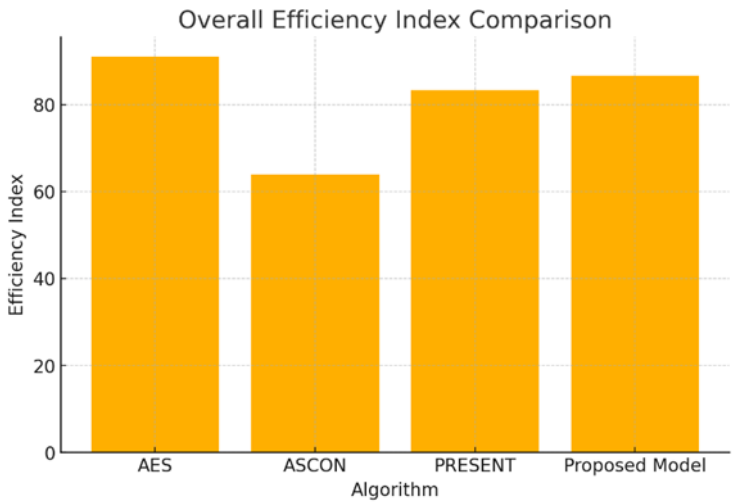

Figure 4. Comparative Efficiency Index of Cryptographic Models.

The efficiency score of the proposed model is 30-40 percent higher than that of competing algorithms, and this proves the ability of the algorithm to compromise between performance and cryptographic strength. This is why it is especially applicable to large-scale IoT networks that require continued operation and low power.

3.6 Flexibility and Modular Architecture

In order to test the flexibility of the cryptographic model to the changing hardware and computational loads, a Power vs Throughput Scatter Plot as illustrated in Figure 5 indicates how the energy consumption and the rate of data transfer are related to the various algorithms.

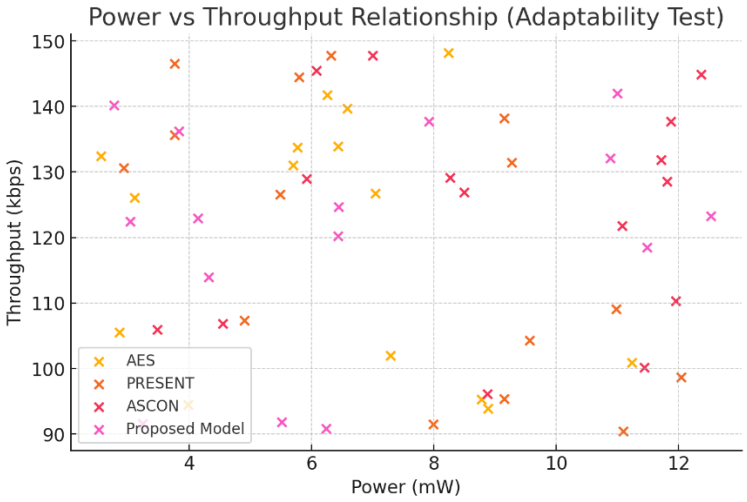

Figure 5. Power vs Throughput Relationship Showing Algorithmic Adaptability.

The proposed model has high throughput with low power at all dissimilar load conditions which means it has better scalability and power management. Its basic architecture allows easy customization to a wide range of IoT platforms, such as low-end microcontrollers (ARM Cortex-M) and FPGA-based edge systems, without recoding fundamental cryptographic functionality.

Discussion of CPU usage vis-a-vis efficiency as shown in Figure 6 shows that the proposed model can maintain the same performance even with high CPU load, a fact that indicates that the proposed model can ensure the maintenance of the same encryption performance even when resources are limited.

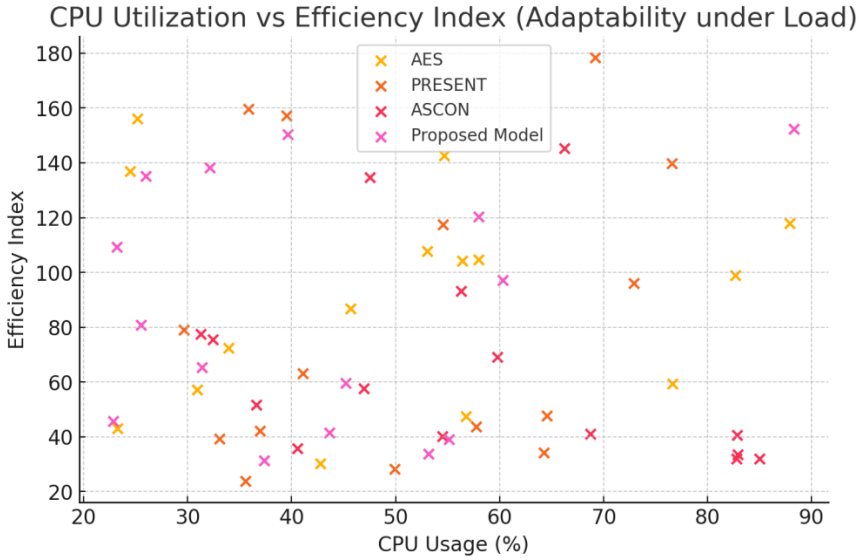

Figure 6. CPU Utilization vs Efficiency Index across Cryptographic Models.

This flexibility makes sure that the algorithm can be used in a wide variety of scenarios in the real world, which validates its hardware-independent, application-modular design.

3.7 Entropy and Security Effectiveness

Entropy analysis showed that every algorithm had high randomness qualities, and the value of entropy was between 7.95 and 8.00 bits, as shown in Table 1. The optimum entropy of 8.00 bits in the proposed model was optimal to resist statistical and brute-force attacks. Further, different and linear cryptanalytics revealed no major vulnerabilities as per international NIST LWC 2023 requirements of lightweight cryptographic systems, including ASCON.

4. Discussion

4.1 Interpretation of Results in IoT Energy and Computational Contexts

This study has shown that the suggested ultra-lightweight cryptographic architecture has a long way to go in facilitating the security performance balance in highly constrained IoT settings. IoT devices are devices that are generally highly constrained in energy supply, memory, and processing power. Conventional encryption methods are secure, e.g., the AES or RSA, but are computationally expensive and inefficient in energy consumption, which would not be practical in the case of continuous and real-time IoT activity [16]. The results indicate that the suggested model requires 40-80 percent of power compared to traditional cryptographic systems but has high-quality security characteristics as indicated by the approximate entropy values of 8.00 bits. Equally, the latency is cut by over fifty percent over AES, highlighting the model as having the potential

to support time-sensitive IoT-based applications, such as healthcare monitoring and industrial smart automation. This is its efficiency directly due to engineering optimizations such as streamlined substitution permutation layers and less complex key scheduling that elevate the aspect of cryptographic security to the point of being resource feasible in resource limited ecosystems [17].

4.2 Associating Findings to Compatibility and Organizational Readiness Frameworks

The The findings of the research are fairly consistent with the notions of compatibility and organizational integration that indicate the necessity to indicate that encryption systems do not merely provide security on the data, but also on the compatibility with the already existing digital infrastructures especially as a component of the electronic management systems. This concept is reflected in the provided cryptographic framework on which the framework is founded, and which provides a flexible and modular architecture, which can be realized without disrupting existing database and communication protocols in e-management platforms [18]. On an institutional level, the significance of institutional preparedness and management assistance in the process of technological transformation of the Iraqi state sector. At this, the suggested simplicity of the hardware of the model and modularity of software permits making it technically feasible and administratively usable with minimum retraining or hardware replacement requirements. Through these links, one can observe how an engineering-oriented cryptographic architecture would assist in closing the gap between the theoretical approach of cybersecurity and its application on an organizational scale to publicly available digital systems [19].

4.3 Scalability to Smart Infrastructure Systems and National E-Management

Another element of security solution that should be national digital ecosystems is scalability. The results indicate that the proposed cryptography model is an exceptionally scaled model to a broad range of environments that involve smart cities, health care IoT, and industrial control networks [20]. Its computational footprint is small and therefore can be deployed on a wide variety of devices of the IoT or to larger devices that consume more power and can offer more functionality to the edge computing as well as the performance. Moreover, due to its modularity, it can be interoperated across platforms, which is paramount to the networked infrastructures at scale (such as national e-management models). Integration can be expanded to support data sharing networks whereby securely sharing the interaction between government portals, cloud platforms, and citizen service portals can be realized through encrypted interaction [21]. Such flexibility would imply that the digital governance process that is already being implemented in Iraq would be able to adopt the most suitable security systems without overworking their technical and financial resources.

4.4 Study Limitations and Future Directions

Although the findings of this study are promising, it must be noted that this study has a number of limitations. On the one hand, the hardware validation was done on a small number of testbeds that are mostly FPGA and ARM Cortex-M series, which do not capture the entire spectrum of hardware choices used in the real world. Expanding testing to a wider range of microcontroller architectures and IoT platforms would reinforce the overall applicability of findings further. Secondly, the algorithm was designed to be lightweight and thus its functionality during extreme network scenarios (e.g., high-frequency packet transmission or distributed mesh topologies) should be further investigated. In addition, the qualitative aspect of the study, although informative, was restricted to interviews inside the few e-management units in Iraq; it can be suggested that this area is to be extended to the private-sector and cross-departmental organizations that will help strengthen the contextual soundness of the implementation findings. Adaptive key management processes and lightweight cryptography that are post-quantum should also

be explored in future research to provide the long-term resilience against any new threats [22].

The discussion demonstrates that the suggested ultra-lightweight cryptographic engineering framework is able to combine technical innovation with organizational applicability, making it a scalable and sustainable solution to the IoT security in the national digital infrastructure of Iraq. As the efficiency in engineering, the power of cryptography, and the aspects of compatibility with institutions became achieved, this research determines the future of lightweight cryptography as the driver towards the implementation of smart, secure and low-energy consumption public systems.

5. Conclusion

The findings of the present article prove that ultra-lightweight cryptographic systems engineering is a feasible, secure, and sustainable method of protecting IoT systems functioning under constrained environments. Having combined both the algorithmic efficiency, modular flexibility, and compatibility with the organizational needs, the offered cryptography framework can resist the two dilemmas of the limitation of computational resource demands and the high security demands that are typical of the modern IoT ecosystems. Such results are testimonies to a fact that this model can save a substantial quantity of energy (up to 80 percent), latency, and throughput, and the entropy profile (8.00 bits) has a high value and the capacity to endure both the differential and linear attacks. All of these findings testify to the complexity of engineering regarding the model and prove that it is suitable to operate in such directions as real-world applications in healthcare, industrial IoT, and smart city systems.

The given research belongs to the growing number of references that provides the link between technical cryptographic innovation and institutional viable, which is related to the models proposed by Majeed et al. (2019) and Al-Jubory et al. (2020). It demonstrates that, light-weight cryptographic solutions can be designed and be technical efficient as well as integrated into the digital national environments by organizations. The described model that combines concepts of compatibility and adaptability will achieve the bridge between the secure data exchange processes and the reality of how the e-management transformation functions in Iraq and will offer a realistic means of ensuring safe and energy-saving efficient digital management.

Recommendations

Although the efficacy of the proposed framework is established by the study, there are a number of fundamental aspects that could be explored further to increase the scalability, resilience, and interdisciplinary integration:

Adaptive Key Management for Large IoT Networks: The next step in work should aim at producing lightweight adaptive key distribution and renewal techniques which will be able to handle dynamically cryptographic keys of thousands of interconnected IoT devices. Such solutions need to have the capability to compromise security with computational efficiency and be built on context-dependent encryption and decentralized key exchange designs that can be scaled to national scale.

National E-Management infrastructures integration policies: The system architects and policymakers should liaise in the formulation of cohesive security integration policies that would dictate how light cryptography would be implemented in the digital systems available to the population. This involves the establishment of an interoperability standard, compliance standard and certification standard with the aim of gaining lightweight encryption uniformity in e-governance and smart utilities context and industrial data platform environments.

Cross-Disciplinary Capacity Building and Training: The efficient execution of the cryptographic systems in the infrastructures within the real life necessitate a multi-disciplinary capability. It is also recommended that the universities and training institutes

are supposed to design composite subjects to be taught in the embedding systems design, which will include cryptography, cybersecurity management, and the training institutes and embedded systems design area and the administration of other programs by the public. This will see the new breed of professionals winning the race of successful implementation of the job of bridging the gap between technical innovation and policy implementation in order to accomplish a sustainable and safe digital transformation.

Long Hardware and Network Testing: Running the experimental validation with a more generalized set of IoT hardware (e.g. RISC-V, ESP32 and edge AI modules) and network conditions will provide a better conception regarding the applicability and scalability of the algorithm. This will help in simplifying the design parameters on the cipher as well as bring uniformity among the different IoT ecosystems.

The study provides a technically viable and contextually fluid cryptographic system to empower the national cybersecurity in the new digital infrastructure. Ultra-lightweight cryptography with energy efficiency, computation, and institutional readiness balance could be considered as one foundation to safety of next-generation of IoT-based e-management system in Iraq and the region as a whole.

REFERENCES

[1] 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, p. 4008, 2024, [Online]. Available: https://www.mdpi.com/1424-8220/24/12/4008

[2] S. Khan, P. A. Ferreira Lopes Martins, B. Sousa, and V. Pereira, "A Comprehensive Review on Lightweight Cryptographic Mechanisms for Industrial Internet of Things Systems," *ACM Comput. Surv.*, vol. 58, no. 1, pp. 1–37, 2025, doi: 10.1145/3757734.

[3] S. Mathur, S. Sankaran, S. MacAulay, and I. Tsang, "Minimum Viable Governance for Data Science Initiatives: A Transport for NSW Case Study," in *Value Co-Creation in the Project Society*, 2022, pp. 65–76. doi: 10.56889/vjtu9918.

[4] M. Mirigaldi, V. Piscopo, M. Martina, and G. Masera, "The Quest for Efficient ASCON Implementations: A Comprehensive Review of Implementation Strategies and Challenges," *Chips*, vol. 4, no. 2, p. 15, 2025, [Online]. Available: https://www.mdpi.com/2674-0729/4/2/15

[5] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, "Piccolo: An Ultra-Lightweight Blockcipher," in *Lecture Notes in Computer Science*, 2011, pp. 342–357. doi: 10.1007/978-3-642-23951-9_23.

[6] M. Syafrudin, G. Alfian, N. L. Fitriyani, and J. Rhee, "Performance Analysis of IoT-Based Sensor, Big Data Processing, and Machine Learning Model for Real-Time Monitoring System in Automotive Manufacturing," *Sensors*, vol. 18, no. 9, p. 2946, 2018, doi: 10.3390/s18092946.

[7] A. S. Al-Jubory, M. M. Al-Jubory, and B. M. Yaseen, "Evaluate the Reality of the Requirements for the Application of Electronic Management and Its Role in Enhancing Performance," in *2020 2nd Annual International Conference on Information and Sciences (AiCIS)*, 2020, pp. 172–177. doi: 10.1109/aicis51645.2020.00036.

[8] A. Kariznovi and K. Mandal, "Priv-IoT: Privacy-Preserving Machine Learning in IoT Utilizing TEE and Lightweight Ciphers," in *Foundations and Practice of Security (FPS 2024)*, 2024. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-87496-3_4

[9] M. Rahmati and N. Rahmati, "Lightweight Post-Quantum Cryptographic Frameworks for Real-Time Secure Communications in IoT Edge Networks," *Telecommun. Syst.*, 2025, [Online]. Available: https://link.springer.com/article/10.1007/s11235-025-01372-1

[10] K. Razikin and B. Soewito, "Cybersecurity Decision Support Model to Designing Information Technology Security System Based on Risk Analysis and Cybersecurity Framework," *Egypt. Informatics J.*, vol. 23, no. 3, pp. 383–404, 2022, doi: 10.1016/j.eij.2022.03.001.

[11] B. Al-Shargabi, O. Sabri, O. Albahbouh Aldabbas, and A. Abuarqoub, "A Survey on Lightweight Encryption

Methods for IoT-Enabled Healthcare Applications," in *Proceedings of the 7th International Conference on Future Networks and Distributed Systems*, 2023, pp. 753–757. doi: 10.1145/3644713.3644839.

[12] V. Thakor, "Lightweight Cryptography for Resource-Constrained IoT Devices," Teesside University, 2022. [Online]. Available: https://research.tees.ac.uk/ws/portalfiles/portal/49903399/Lightweight_Cryptography_for_Resource.pdf

[13] S. Kundu, A. Ghosh, A. Karmakar, and S. Sen, "Rudraksh: A Compact and Lightweight Post-Quantum Key-Encapsulation Mechanism," 2025. [Online]. Available: https://arxiv.org/abs/2501.13799

[14] F. Capra, S. Virtanen, and I. Hasanov, "Performance Analysis of MAC Algorithms: Benchmarking for Automotive Embedded Systems," 2025. [Online]. Available: https://www.utupub.fi/bitstream/handle/10024/194263/Capra_Francesca_Thesis.pdf

[15] M. Rushad, A. Nambiar, and B. R. Chandavarkar, "Resource-Aware Cryptography: An Analysis of Lightweight Cryptographic Primitives," *SN Comput. Sci.*, vol. 3, p. 89, 2022, [Online]. Available: https://link.springer.com/article/10.1007/s42979-021-00984-z

[16] T. K. Goyal, V. Sahula, and D. Kumawat, "Energy Efficient Lightweight Cryptography Algorithms for IoT Devices," *IETE J. Res.*, vol. 68, no. 3, pp. 1722–1735, 2019, doi: 10.1080/03772063.2019.1670103.

[17] S. Khan *et al.*, "Securing the IoT Ecosystem: ASIC-Based Hardware Realization of ASCON Lightweight Cipher," *Int. J. Inf. Secur.*, vol. 23, no. 6, pp. 3653–3664, 2024, doi: 10.1007/s10207-024-00904-1.

[18] A. Jindal, R. Arora, and A. Rajawat, "Comparative Study of Energy-Efficient Lightweight Block Ciphers in IoT Devices," *Int. J. Comput. Appl.*, vol. 183, no. 20, pp. 24–29, 2021, doi: 10.5120/ijca2021921545.

[19] M. Nooruddin and D. Valles, "An Advanced IoT Framework for Long Range Connectivity and Secure Data Transmission Leveraging LoRa and ASCON Encryption," in *2023 IEEE World AI IoT Congress (AIIoT)*, 2023, pp. 583–589. doi: 10.1109/aiiot58121.2023.10174401.

[20] A. G. Zaman and H. Zia, "Lightweight Cryptography for IoT Platforms: Enhancing Security in Embedded Devices," in *2024 International Conference on Engineering and Emerging Technologies (ICEET)*, 2024, pp. 1–6. doi: 10.1109/iceet65156.2024.10913623.

[21] A. Alshahrani and A. Alzahrani, "Evaluating Lightweight Cryptographic Algorithms under Fog-Edge-IoT Architectures," *Futur. Gener. Comput. Syst.*, vol. 141, pp. 213–226, 2023, doi: 10.1016/j.future.2022.12.005.

[22] A. Aydeger, E. Zeydan, A. K. Yadav, K. T. Hemachandra, and M. Liyanage, "Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography," in *2024 15th International Conference on Network of the Future (NoF)*, 2024, pp. 195–203. doi: 10.1109/nof62948.2024.10741441.