IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13511

Advancing IoT Security: A Comprehensive Survey of Lightweight Cryptography Solutions

Karthik S[1], **Dr. A. Rengarajan**[2]

Student of MCA, Department of CS & IT, Jain (Deemed-to-be-University), Bengaluru, India[1]

Professor, Department of CS & IT, Jain (Deemed-to-be-University), Bengaluru, India[2]

Abstract: A comprehensive survey of lightweight cryptography (LWC) solutions tailored to address the security challenges inherent in Internet of Things (IoT) environments. Evaluating various cryptographic primitives, including block ciphers, stream ciphers, hash functions, and elliptic curve cryptography, the study highlights the efficacy of AES and ECC in resource-constrained IoT devices. Emphasizing the necessity of lightweight cryptographic solutions amidst real-world constraints, the paper underscores ongoing research efforts and identifies future directions to fortify the security posture of IoT ecosystems. Through meticulous analysis and synthesis of findings, this survey advocates for the critical role of LWC in ensuring the resilience of IoT technologies.

Keywords: Lightweight Cryptography; Internet of Things (IoT); Security Challenges; Cryptographic Primitives; Resource-Constrained Devices.

I. INTRODUCTION

IoT has brought a new sense of connectivity, but it has also initiated colossal security concerns. While very powerful on a system with a lot of processing power and memory, these cryptographic methods in the past, such as AES, SHA-256, and RSA, had problems with scalability to resource limitations in devices from IoT. This will require that research be conducted on the identification of lightweight cryptography solutions that would be applicable to the peculiar challenges thrown up by IoT environments. This paper comprehensively surveys lightweight cryptographic primitives within several techniques, such as: block ciphers, stream ciphers, hash functions, and variants of elliptic curve cryptography (ECC), up to year 2019. The study carefully evaluates all these primitives on the basis of chip area, energy consumption, hardware, and software efficiency, throughput, latency, and figure of merit. We find that both AES and ECC are prime candidates to be considered as lightweight cryptographic primitives. Further, the paper discusses the existing challenges toward IoT deployment, with special emphasis on devices that are truly resource-constrained at the extreme, for example, RFID tags and sensors. This means that secure lightweight cryptographic schemes must be put in place for devices subjected to real-world constraints, especially in the area of energy, memory, and processing power.

It discusses recent advances in lightweight AES and trade-offs in hardware versus software implementation. The paper in summary believes that lightweight cryptography plays an instrumental role in the security of IoT ecosystems, and the main research directions to take would be emerging challenges in this area.

II. BACKGROUND AND CONTEXT

The specialized zone of cryptographic techniques is lightweight cryptography, meant for serving light devices under several resource constraints, most generally in embedded systems, IoT devices, and the like with low-power computing environments. These are generally small processor power, limited memory, small energy resources, and physical size. LWC aims to enable efficient cryptographic security techniques specially designed to fit the required characteristics of the device being used without degrading security.

Lightweight cryptosystems encrypt and decrypt messages securely, and provide

1. Efficiency: LWC algorithms pay great attention to efficiency in terms of computational complexity, memory use, and energy. They are designed to carry out cryptographic operations with low resource overhead.
2. Security: While being a very lightweight scheme, the LWC algorithms must provide a very high order security level against most of the cryptographic attacks, such as brute force, differential, and side channel attacks. Therefore, this is one of the most major challenging parts in the design of LWC.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024
DOI: 10.17148/IJARCCE.2024.13511

3. Scalability: The LWC techniques should be scalable for supporting diversified application scenarios and the quickly evolving technological landscape. They have to retain effectiveness both in the sense of rising numbers of connected devices and in the sense of evolution of computational resources.

Examples of lightweight cryptography historical developments and trends:

1. Early Efforts: Small, resource-constrained devices, such as smart cards or RFID tags, gained momentum during the 1990s. Early research oriented itself toward adapting pre-existing cryptographic algorithms to minimize the small resource requirement.
2. Specialized algorithms: With an increased demand for lightweight cryptography, researchers continued to design specialized algorithms developed for the particular constraints that correspond to embedded systems and IoT devices. Most of these algorithms incorporate novel design techniques for effectiveness and safety.
3. Standardization Efforts: In consideration of the extensive use of lightweight cryptography in emerging technologies, standardization activities for lightweight cryptographic algorithms by leading standardization bodies such as the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) have been started. These efforts will support interoperability and promote a wide adoption of light solutions that are secure.

4. Ongoing Research: Lightweight cryptography research is continually evolving under the pressure of hardware design, cryptographic theory, and emerging application domains, such as wearable devices and edge computing. Research has been devoted to creating lightweight, secure, and efficient cryptographic techniques for the new challenges and opportunities that emerge in the digital landscape. Such lightweight cryptography is important for enabling secure communication and data protection even in resource-constrained environments. To progress the IoT, embedded systems, and other recent technologies, there is a substantial role that lightweight cryptography plays in enabling safe communication and data protection under resource-constrained environments.

III. LITERATURE REVIEW

The skyrocketing number of Internet of Things (IoT) devices has put forward serious issues regarding the security and privacy of data, especially in resource-constrained environments where typical cryptographic methods, like AES and SHA, become highly infeasible due to a high dependency on processing power, physical space, and battery consumption. Several lightweight cryptography primitives have been designed with these challenges in mind, specifically for the IoT and embedded systems.

Both national (NIST) and international (ISO/IEC) organizations have set up specific methods for lightweight cryptography, showing that the nature of the requirements for IoT and RFID devices is very different from those of conventional computer systems, due to the diverse range of computational capabilities across the whole spectrum from servers and smartphones to embedded systems and sensor networks.

Embedded systems generally use microcontrollers with very feeble processing abilities, therefore, exerting some real-time demands that cannot be met easily with the usual cryptography methods. Furthermore, RFID and the sensor network devices operate under very tight strictures in terms of the available gates for security and power consumption. In this respect, AES and all of its standard specifications are not that applicable to the devices of such natures.

Lightweight cryptography shows this by using smaller block sizes, shorter keys, and less complex rounds—usually 64 or 80-bit block sizes and keys smaller than 90 bits. However, this sort of trade-off can easily bring in weaknesses, for example, with respect to the successful break-ins due to differential power analysis and correlation power analysis on 128-bit AES key Arduino boards in 30 minutes.

While IoT promises to enable new applications, on the other hand, it brings new security challenges, particularly in cryptographic security, credentialing, and identity management. The main issue faced is how to ensure security and privacy protection when connected devices are resource-constrained and can't carry out any standard cryptographic computation.

A new twist in lightweight symmetric and asymmetric cryptography has given promise of yielding solutions to the security of IoT. Lightweight block ciphers, such as Quark, Marvin, and stream ciphers like PRESENT and SPONGENT, have provided an effective alternative to traditional methods. Asymmetric techniques such as ECC and post-quantum cryptography will, in turn, allow key exchange and authentication to be made secure in such IoT environments.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024
DOI: 10.17148/IJARCCE.2024.13511

IV. METHODOLOGY

Selecting and evaluating Literature for a survey paper in Lightweight Cryptography:

1. Selection Criteria: The selection of literature is based on relevance to lightweight cryptography, recency, quality, diversity of sources, and contribution to the field.

2. Search Process: All relevant databases like IEEE Xplore, ACM Digital Library, and Google Scholar are searched using keywords like "lightweight cryptography," "embedded systems security," and specific algorithm names. Use of Boolean operators and snowballing techniques for refinements of search queries and further literature identification.

In this report, only those literatures related to lightweight cryptography and meeting predefined criteria are going to be included. It will include peer-reviewed articles, conference papers, and reputable caliber journals.

3. Procedures for Review: Selected literature is reviewed based on relevance, quality, methodology, results, and contributions. This involves comparative analysis, which points out all common themes, trends, and also discrepancies, and thus draws conclusions for the survey paper.

All this structured procedure assures high-quality, relevant literature for a reader, literature that importantly contributes to the comprehensive realization of lightweight cryptography.

V. ANALYZING AND COMPARING THE FINDINGS

Trends and Features in the Field

Concern of Resource Constrained: All over, in the presented literature, is a concern that the IoT devices have minimum processing power, memory, and energy resources. The lightweight cryptographic techniques are being given the focus as a necessity to provide secure communication and data protection.

Evaluation Metrics: State-of-the-art literature commonly evaluates lightweight cryptographic primitives with metrics like chip area, energy consumption, hardware and software efficiency, throughput, latency, and figure of merit. AES and ECC generally turn out to be promising candidates because of good figures of merit in these metrics.

Security Issues: Security is a primary concern in the implementation of IoT, where the main thrust is in securing lightweight, resource-constrained devices, such as RFID tags and sensors, from common threats of eavesdropping, tampering, and data breaches. Lightweight cryptography is regarded as a vital ingredient in the security recipe of IoT.

Dependencies And Limitations:

• Heterogeneity in Evaluation Metrics: Even though some consensus can be found about the general importance of evaluation metrics, specifically which evaluation metrics are used and to what extent they are prioritized are found to be represented quite heterogeneously. As such, direct comparisons between the studies become very difficult. It really calls for standardization in evaluation methodologies.

◦ Emerging Technique Blindness: In all likelihood, established cryptographic primitives AES and ECC will be the focus of some studies, ignoring emerging techniques and recent advances. This may thus create a gap in understanding the full scope of the available solutions.

◦ Lack of Deployment Studies in the Real World: Though theoretical and technical details of lightweight cryptography are well covered by the literature, there are relatively few studies related to the real-world deployment and practical implications of the techniques. More research needs to be done to evaluate the effectiveness and scalability of lightweight cryptography within different IoT applications and environments.

VI. CONCLUSION

The paper is a comprehensive survey of the critical role of lightweight cryptography in addressing security challenges posed by IoT ecosystems. The rapid increase in the number of IoT devices has rendered classical cryptographic schemes, such as AES, SHA-256, and RSA, hard-pressed to adapt to the inherent resource constraints in these devices. Consequently, lightweight cryptographic solutions are required for dealing with these challenges.

REFERENCES

1. Chakrabarti, S., Saha, H. N., University of Nevada, Institute of Electrical and Electronics Engineers. Region 1, Institute of Electrical and Electronics Engineers. Region 6, IEEE-USA, & Institute of Electrical and Electronics Engineers. (n.d.). 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) : 7th-9th January, 2019, University of Nevada, Las Vegas, NV, USA.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13511

2. Buchanan, W. J., Li, S., & Asif, R. (2017). Lightweight cryptography methods. Journal of Cyber Security Technology, 1(3–4), 187–201. https://doi.org/10.1080/23742917.2017.1384917
3. Dhanda, S. S., Singh, B., & Jindal, P. (2020). Lightweight Cryptography: A Solution to Secure IoT. Wireless Personal Communications, 112(3), 1947–1980. https://doi.org/10.1007/s11277-020-07134-3
4. Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. A. (2021). Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. IEEE Access, 9, 28177–28193. https://doi.org/10.1109/ACCESS.2021.3052867

