International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Survey on Lightweight Cryptographic Algorithms in IoT

K. Prathapchandran[1], Abhijith P[2], Alen Britto[3]

[1]Assistant Professor, Department of Computer Applications, Nehru Arts and Science College, Coimbatore – 641195, Tamilnadu, India
[2,3]Student, Department of Computer Applications, Nehru Arts and Science College, Coimbatore – 641195, Tamilnadu, India

Abstract
The Internet of Things (IoT) represents a paradigm shift in computing, enabling ubiquitous connectivity among heterogeneous devices. It has revolutionized sectors including healthcare, transportation, agriculture, and smart cities. However, the proliferation of IoT devices introduces critical security challenges, primarily due to their resource-constrained nature and the scale of their deployment. Traditional cryptographic algorithms, designed for high-performance computing environments, are often ill-suited for IoT systems. This paper presents a comprehensive survey of lightweight cryptographic algorithms developed specifically for IoT applications. It categorizes these algorithms into symmetric, asymmetric, and hash-based techniques, analyzing them based on performance metrics such as computational efficiency, energy consumption, and memory footprint. Furthermore, this survey outlines the current research challenges, recent advancements, and open issues in the design and deployment of secure, efficient, and scalable IoT systems.

Keywords: Internet of Things, Cryptographic, Symmetric. Asymmetric, Hash

1. Introduction

The Internet of Things (IoT) is a transformative ecosystem comprising interconnected smart devices capable of data collection, processing, and communication with minimal human intervention. As IoT devices are widely deployed in sensitive domains—such as health monitoring systems, industrial automation, and vehicular networks—securing these networks becomes paramount (Roman et al., 2018). Ensuring data confidentiality, integrity, and authentication is essential to protect against cyber threats, data breaches, and unauthorized access.

Traditional cryptographic protocols such as RSA and AES, though robust, are computationally intensive and demand significant energy and memory resources, making them unsuitable for low-power IoT devices (Zhou et al., 2018). To address this gap, researchers have proposed lightweight cryptographic algorithms that maintain a trade-off between computational overhead and security assurance.

2. Background and Motivation

Cryptographic security in conventional systems assumes the availability of significant computational and energy resources. However, IoT nodes typically operate under severe resource constraints—limited

CPU power, restricted RAM, non-rechargeable batteries, and constrained bandwidth—making them susceptible to performance degradation if traditional algorithms are used (Paar & Pelzl, 2010).

The motivation for lightweight cryptographic research stems from the need to enable secure communication in environments where energy and computation are premium commodities. By optimizing algorithmic structures for efficiency without compromising core security principles, lightweight cryptography becomes a foundational element in IoT security architectures.

3. Categories of Lightweight Cryptographic Algorithms

3.1 Symmetric Key Algorithms

Symmetric key algorithms use the same key for both encryption and decryption. They are favored in IoT due to their relatively low computational complexity and fast execution times.

- **PRESENT**: A hardware-optimized block cipher with a 64-bit block size and key sizes of 80 or 128 bits. PRESENT is highly efficient in constrained environments, achieving ISO/IEC standardization for lightweight encryption (Bogdanov et al., 2007).
- **LED (Lightweight Encryption Device)**: An AES-like cipher tailored for hardware-constrained systems, emphasizing low-area cost and power efficiency (Guo et al., 2011).
- **Simon and Speck**: Developed by the NSA, these ciphers offer tunable configurations for both hardware and software implementations and are optimized for versatility across devices (Beaulieu et al., 2015).

3.2 Asymmetric Key Algorithms

Asymmetric cryptography employs public-private key pairs, providing robust security guarantees but at higher computational costs.

- **Elliptic Curve Cryptography (ECC)**: Provides equivalent security to RSA with much smaller key sizes (e.g., 160-bit ECC ≈ 1024-bit RSA), significantly reducing memory and processing needs (Liu & Ning, 2008).
- **NTRUEncrypt**: A lattice-based cryptosystem known for its post-quantum resistance and suitability for constrained devices due to polynomial-time operations (Hoffstein et al., 1998).

3.3 Lightweight Hash Functions

Hash functions are essential for verifying message integrity and authentication in resource-constrained environments.

- **SPONGENT**: Based on sponge construction and supporting multiple hash sizes (88, 128, 160 bits), it is designed for small-area hardware and low energy consumption (Bogdanov et al., 2011).
- **Quark**: A family of hash functions (U-Quark, D-Quark, S-Quark) focused on ultra-lightweight security with strong resistance to known attacks (Aumasson et al., 2010).
- **Photon**: Offers strong diffusion, compact implementation, and resistance to cryptanalysis, making it suitable for RFID and sensor applications (Guo et al., 2011).

4. Comparative Analysis

Algorithm	Type	Key Size (bits)	Block Size	Energy Efficiency	Suitability for IoT
PRESENT	Symmetric	80/128	64	High	High
ECC	Asymmetric	160+	Variable	Medium	High
SPONGENT	Hash	N/A	88/128/160	High	High

Algorithm	Type	Key Size (bits)	Block Size	Energy Efficiency	Suitability for IoT
Simon	Symmetric	Various	Various	High	High
RSA	Asymmetric	1024+	Variable	Low	Low

This table illustrates the trade-offs between algorithm types. Symmetric key algorithms provide the best performance-to-security ratio for constrained IoT environments, whereas ECC stands out as the most practical asymmetric solution.

5. Challenges and Open Issues

- **Key Management**: One of the most pressing challenges in lightweight cryptography is the development of scalable and secure key distribution methods suitable for large-scale, dynamic IoT networks (Sicari et al., 2015).
- **Post-Quantum Cryptography**: Quantum computing poses a threat to many current cryptographic systems. There is a growing need for lightweight cryptographic schemes that are resistant to quantum attacks (Chen et al., 2016).
- **Standardization**: Despite progress, there is no universally accepted standard for lightweight cryptography, resulting in interoperability issues across devices and platforms (Barker et al., 2017).
- **Side-Channel Attacks**: Many IoT devices are susceptible to side-channel attacks (e.g., power analysis, electromagnetic attacks) due to inadequate physical protection (Mohan et al., 2013).

6. Conclusion

This survey underscores the importance of lightweight cryptographic solutions for securing IoT environments. It presents an overview of key algorithm categories, evaluating their strengths and limitations. Despite notable progress, critical challenges remain in areas such as secure key exchange, resistance to quantum threats, and defense against side-channel exploits. Future research should emphasize adaptive, context-aware cryptographic models capable of scaling across diverse IoT infrastructures while ensuring robust security and resource efficiency.

References

1. Aumasson, J. P., Meier, W., Phan, R. C. W., & Henzen, L. (2010). Quark: A lightweight hash. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 1–15). Springer.
2. Barker, E., Chen, L., & Roginsky, A. (2017). *Recommendation for the Transitioning of Cryptographic Algorithms and Key Lengths* (NIST Special Publication 800-131A Rev. 2). National Institute of Standards and Technology.
3. Beaulieu, R., Shors, D., Smith, J., et al. (2015). The SIMON and SPECK lightweight block ciphers. In *Proceedings of the 52nd Annual Design Automation Conference* (pp. 1–6).
4. Bogdanov, A., Knudsen, L. R., Leander, G., et al. (2007). PRESENT: An ultra-lightweight block cipher. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 450–466). Springer.
5. Bogdanov, A., Knežević, M., Leander, G., Toz, D., Varici, K., & Verbauwhede, I. (2011). SPONGENT: A lightweight hash function. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 312–325). Springer.

6. Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on Post-Quantum Cryptography* (NISTIR 8105). NIST.
7. Guo, J., Peyrin, T., & Poschmann, A. (2011). The PHOTON family of lightweight hash functions. In *Annual Cryptology Conference* (pp. 222–239). Springer.
8. Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. In *International Algorithmic Number Theory Symposium* (pp. 267–288). Springer.
9. Liu, A., & Ning, P. (2008). TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. In *Proceedings of the 7th International Conference on Information Processing in Sensor Networks* (pp. 245–256).
10. Mohan, N., Saxena, N., & Soh, B. (2013). Secure implementation of cryptographic protocols on constrained devices. In *International Conference on Security and Privacy in Communication Systems* (pp. 556–571). Springer.
11. Paar, C., & Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer.
12. Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, 78, 680–698.
13. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164.
14. Zhou, W., Zhang, Y., Liu, P., & Liu, L. (2018). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, 6(2), 1606–1616.