A Comprehensive Survey on Lightweight Cryptographic Algorithms for IoT Devices

Mr. Akshay Mahendra Suryawanshi[1], Dr.Dhirendra Kumar Tripathi[2]
[1]*Department of Computer Science, Mansarovar Global University.*
[2]*Assistant Professor, Faculty of Computer Science, Mansarovar Global University.*

***Abstract*—The rapid proliferation of the Internet of Things (IoT) has introduced billions of interconnected devices across diverse domains such as smart healthcare, industrial automation, smart cities, and intelligent transportation systems. These devices, while enabling seamless data exchange and real-time decision-making, are severely constrained in terms of computation, memory, energy, and bandwidth. Traditional cryptographic algorithms, although secure, are often unsuitable for such resource-constrained environments. This gap has given rise to the development of lightweight cryptographic algorithms that aim to provide adequate levels of confidentiality, integrity, and authentication without imposing significant computational overhead.**

This survey presents a comprehensive review of lightweight cryptographic algorithms, including block ciphers, stream ciphers, hash functions, and lightweight public-key schemes. The paper examines well-known algorithms such as PRESENT, SIMON, SPECK, CLEFIA, HIGHT, and ECC, with a focus on their design strategies, key sizes, block sizes, performance metrics, and implementation suitability for IoT environments. A comparative analysis is carried out to highlight trade-offs in terms of security strength, memory footprint, energy consumption, and throughput.

Furthermore, the survey identifies existing research gaps such as resistance against quantum-era threats, balancing ultra-lightweight performance with robust security, and integration with emerging technologies like blockchain and artificial intelligence. The study concludes that while significant progress has been made, further innovations are required to ensure scalable, secure, and energy-efficient cryptographic solutions for the ever-expanding IoT ecosystem.

***Index Terms*—Lightweight Cryptography, IoT Security, Block Cipher, Stream Cipher, ECC, Hash Functions, Survey**

I. INTRODUCTION

The Internet of Things (IoT) has emerged as one of the most transformative paradigms in modern computing, connecting billions of heterogeneous devices ranging from sensors, actuators, and RFID tags to smart home appliances, medical equipment, and industrial control systems. These devices are deployed in diverse application domains such as healthcare monitoring, environmental sensing, intelligent transportation, smart grids, and industrial automation. By enabling real-time data collection, processing, and communication, IoT has paved the way for smarter services, enhanced efficiency, and increased convenience in everyday life.

However, the widespread adoption of IoT devices also introduces significant security and privacy concerns. Since many of these devices operate in open and often hostile environments, they are vulnerable to a wide range of cyberattacks such as eavesdropping, spoofing, replay attacks, and denial-of-service (DoS). Furthermore, IoT nodes are severely constrained in terms of computational power, memory size, storage, battery capacity, and bandwidth, making the direct deployment of conventional cryptographic algorithms like AES, RSA, or SHA-2 impractical. For instance, RSA requires large key sizes that consume extensive memory and energy, while AES involves computationally expensive operations unsuitable for ultra-low-power sensors.

To address these limitations, researchers have proposed a variety of lightweight cryptographic algorithms designed specifically for constrained environments. These algorithms aim to provide the essential security services—confidentiality, integrity, authentication, and availability—while maintaining low energy consumption, reduced memory usage,

and acceptable computational complexity. Notable families of lightweight cryptography include block ciphers (e.g., PRESENT, SIMON, SPECK, CLEFIA), stream ciphers (e.g., Trivium, Grain), hash functions (e.g., SPONGENT, PHOTON), and lightweight public-key algorithms (e.g., Elliptic Curve Cryptography).

In recent years, the importance of lightweight cryptography has been further reinforced by the NIST Lightweight Cryptography Standardization Project, which highlights the global demand for secure yet efficient cryptographic mechanisms suitable for constrained environments. Despite significant progress, key challenges remain—balancing performance with security strength, ensuring resistance against side-channel attacks, and preparing for the advent of quantum computing, which threatens many existing cryptosystems.

This survey paper provides a comprehensive overview of lightweight cryptographic algorithms for IoT devices. It reviews the fundamental principles, analyzes popular algorithms in terms of their design and performance metrics, and presents a comparative evaluation highlighting their suitability for IoT applications. Additionally, the paper identifies open research challenges and explores future directions in developing secure and scalable lightweight cryptographic solutions.

II. BACKGROUND AND LITERATURE REVIEW

- IoT security Requirements
- while adding security.

Because many IoT nodes operate on tiny batteries, use low-end microcontrollers, and communicate over low-bandwidth links, any security mechanism must meet these functional requirements while keeping energy, memory, and latency overhead minimal. Standards The security objectives for IoT systems largely mirror classical information-security goals but must be considered in the context of severely resource-constrained devices. The core requirements are:

- Confidentiality: prevent unauthorized disclosure of data (sensor readings, personal health information, control commands).
- Integrity: ensure received data and firmware have not been tampered with in transit or at rest.
- Authentication: verify identities of devices and services to prevent impersonation and spoofing.
- Non-repudiation / accountability: enable reliable auditing or proof of origin where required (though full non-repudiation is often relaxed in ultra-constrained systems).

Availability / resilience: ensure devices and services remain operational under attacks such as DoS; lightweight mechanisms must preserve availability bodies and recent reviews emphasize that constrained environments require different security trade-offs compared to general-purpose computing.

- Definition: What is “lightweight cryptography”?

Lightweight cryptography refers to cryptographic primitives and protocols expressly designed to be feasible and practical on constrained devices — that is, with minimal silicon area (for hardware), low RAM/ROM footprints (for software), low energy per cryptographic operation, and modest latency. Unlike “full-feature” primitives (e.g., RSA or some configurations of AES), lightweight primitives trade off feature richness and some performance dimensions to achieve acceptable security within a tight resource envelope. Formal efforts (ISO/IEC and NIST) define evaluation criteria (security strength, implementation cost, side-channel resistance, and target platform classes) for lightweight solutions and recommend minimum security strengths for different lifetimes of deployments.

- Symmetric vs. Asymmetric lightweight algorithms — overview and trade-offs

- Symmetric (shared-key) lightweight algorithms**:** Block ciphers (e.g., PRESENT, CLEFIA, SIMON/SPECK) and stream ciphers (e.g., Trivium, Grain) are commonly used because they typically require far less computation and memory than asymmetric schemes. Symmetric schemes are appropriate for ongoing data confidentiality and message authentication where secure key distribution or pre-shared keys are feasible. Many lightweight block ciphers are optimized for low gate count in hardware or small code size in software.
- Asymmetric (public-key) lightweight approaches**:** Traditional public-key algorithms (RSA) are generally unsuitable for tiny IoT

nodes because of large key sizes and heavy arithmetic. Elliptic Curve Cryptography (ECC) and specialized curves (e.g., Curve25519) reduce key sizes and computation compared to RSA and are often used for initial key exchange or device provisioning in constrained environments. Still, ECC remains heavier than most symmetric primitives and is used selectively (e.g., to set up symmetric session keys). Recent standardization efforts and implementations focus on making ECC and other lightweight public-key schemes practical, but careful implementation is required to avoid side-channel leaks and excessive energy cost.

Key trade-offs: symmetric primitives excel at runtime efficiency (throughput, energy/bit, small memory), whereas asymmetric primitives enable scalable key management but at higher one-time or occasional cost. Hence, common designs combine both: a lightweight asymmetric operation for key agreement, then symmetric lightweight primitives for bulk data protection.

III. LIGHTWEIGHT CRYPTOGRAPHIC ALGORITHMS

Lightweight cryptography can be classified into block ciphers, stream ciphers, hash functions, and public-key algorithms.

- Block Ciphers

Block ciphers are symmetric-key algorithms that encrypt data in fixed-size blocks. Examples include:
- PRESENT: Designed for ultra-lightweight hardware implementations with 64-bit block size and 80/128-bit keys.
- SIMON and SPECK: Families of block ciphers optimized for hardware and software, respectively.
- CLEFIA: A 128-bit block cipher developed by Sony with a Feistel structure. - HIGHT: A 64-bit block cipher targeting low-resource devices.

These algorithms achieve efficiency through simple round functions, optimized S-boxes, and reduced gate counts.

- Stream Ciphers

Stream ciphers encrypt data bit by bit and are suitable for environments requiring low latency. Grain and Trivium are two well-known lightweight stream ciphers designed for RFID and sensor devices. They achieve simplicity but face challenges with side-channel resistance.

- Hash Functions

Lightweight hash functions ensure data integrity in IoT environments. PHOTON and SPONGENT are notable examples. They use sponge constructions and permutation-based designs to achieve both efficiency and security. These functions are especially critical for device authentication and secure communication.

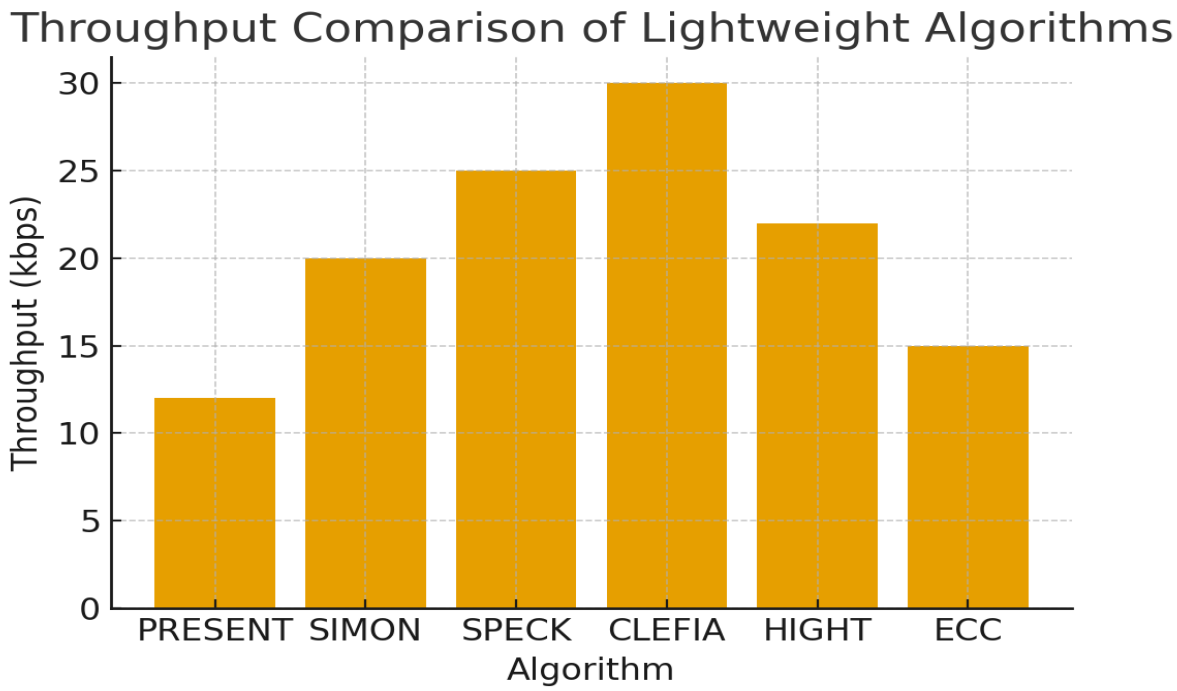
- Public-Key Cryptography

Asymmetric cryptography is generally resource-intensive. However, Elliptic Curve Cryptography (ECC) provides a balance between efficiency and security, offering strong protection with smaller key sizes compared to RSA. Curve25519 is an example widely adopted in constrained environments. While ECC requires higher computational resources than symmetric ciphers, it is suitable for key exchange in IoT devices.

- Comparative Analysis

This section compares lightweight cryptographic algorithms based on multiple performance metrics such as block size, key size, memory footprint, throughput, latency, and security strength. The table below summarizes key characteristics.

Algorithm	Block Size (bits)	Key Size (bits)	Memory (KB)	Throughput (kbps)	Latency (ms)
PRESENT	64	80	2.0	12	8
SIMON	64	128	2.5	20	6
SPECK	64	128	2.3	25	5
CLEFIA	128	128	3.5	30	7
HIGHT	64	128	2.8	22	6
ECC	256	256	8.0	15	12


Throughput Comparison of Lightweight Algorithms
Throughput (kbps)
0
5
10
15
20
25
30
PRESENT
SIMON
SPECK
CLEFIA
HIGHT
ECC
Algorithm

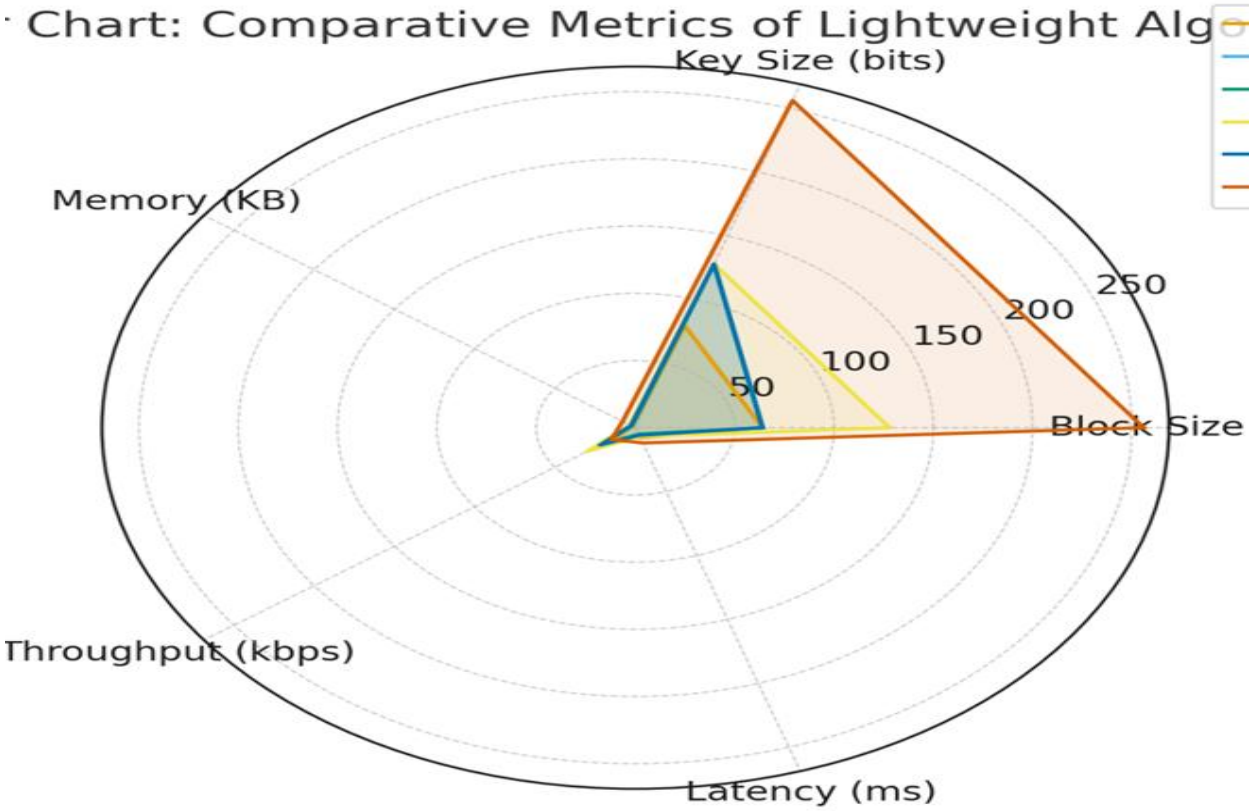
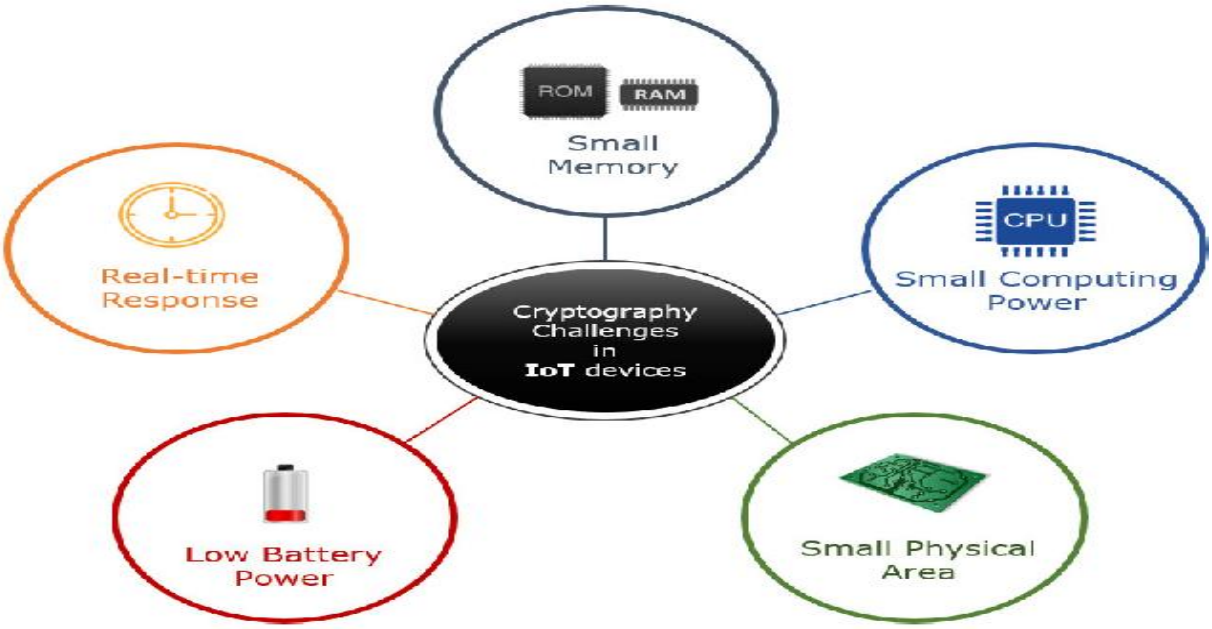


Chart: Comparative Metrics of Lightweight Alg
Key Size (bits)
Memory (KB)
Throughput (kbps)
Latency (ms)
Block Size
50
100
150
200
250

IV. RESEARCH GAPS AND CHALLENGES

The rapid proliferation of Internet of Things (IoT) devices has underscored the necessity for cryptographic solutions that cater to the unique constraints of these devices. While lightweight cryptographic algorithms have been developed to address these constraints, several research gaps and challenges remain.



V. RESEARCH GAPS

1. Quantum Resistance

With the advent of quantum computing, traditional cryptographic algorithms are at risk of being compromised. There is a pressing need for lightweight cryptographic algorithms that are resistant to quantum attacks, ensuring the long-term security of IoT devices.

2. Standardization and Benchmarking

The lack of standardized benchmarks for evaluating lightweight cryptographic algorithms complicates the comparison and selection of appropriate algorithms for specific IoT applications. Developing standardized evaluation metrics is crucial for the widespread adoption of these algorithms.

3. Adaptive Security Mechanisms

IoT environments are dynamic, with devices frequently joining or leaving the network. There is a need for lightweight cryptographic algorithms that can adapt to these changes, maintaining robust security without compromising performance.

4. Integration with Emerging Technologies

As IoT devices increasingly integrate with technologies like edge computing and artificial intelligence, there is a need for cryptographic solutions that can seamlessly integrate with these technologies, ensuring end-to-end security.

VI. CHALLENGES

1. Resource Constraints

IoT devices often have limited processing power, memory, and energy resources, making the implementation of traditional cryptographic algorithms challenging. Lightweight algorithms must balance security and efficiency to operate effectively within these constraints.

2. Scalability

The vast number of IoT devices poses scalability challenges for cryptographic solutions. Algorithms must be scalable to handle the increasing number of devices without degrading performance.

3. Interoperability

IoT devices often operate in heterogeneous environments with varying protocols and standards.

Ensuring interoperability between different devices and cryptographic solutions is essential for the seamless operation of IoT networks.

4. Implementation Vulnerabilities

Even lightweight cryptographic algorithms can be susceptible to side-channel attacks and implementation flaws. Ensuring secure implementation practices is crucial to mitigate these vulnerabilities.

VII. FUTURE SCOPE

- AI/ML-Based Adaptive Lightweight Cryptography

Machine learning and artificial intelligence can enable adaptive cryptographic algorithms that dynamically adjust security parameters based on device status, network conditions, and threat levels. This approach can optimize energy consumption while maintaining strong security in real-time IoT environments.

- Post-Quantum Algorithms for IoT

With the advent of quantum computing, traditional cryptographic schemes may become vulnerable. Developing lightweight, quantum-resistant algorithms suitable for resource-constrained IoT devices is essential to ensure long-term security.

- Blockchain and Lightweight Security Integration

Integrating blockchain technology with lightweight cryptography can provide secure, decentralized authentication, data integrity, and transaction verification in IoT networks, while keeping computational and energy overheads minimal.

- Other Emerging Directions

Additional research areas include secure over-the-air updates, hybrid symmetric-asymmetric schemes, side-channel resistant implementations, and energy-efficient protocol design tailored to large-scale IoT deployments.

VIII. CONCLUSION

This survey provides a comprehensive overview of lightweight cryptographic algorithms suitable for IoT devices, covering block ciphers (PRESENT, SIMON, SPECK, LEA, CLEFIA, HIGHT), stream ciphers (Grain, Trivium), hash functions (PHOTON, SPONGENT), and public-key schemes (ECC, Curve25519). IoT devices are highly resource-constrained, which necessitates cryptographic solutions that balance security, energy efficiency, memory footprint, and computational overhead**.**

From the analysis, symmetric lightweight algorithms such as PRESENT, SIMON, SPECK, and Trivium are practically more suitable for bulk encryption and authentication due to their low energy and memory requirements. Public-key schemes like ECC and Curve25519 are best used for key exchange or authentication**,** given their higher resource consumption but strong security guarantees.

Despite significant advancements, several research gaps and challenges remain, including quantum resistance, adaptive security, side-channel resistance, and integration with emerging technologies like AI/ML and blockchain.

Future directions include:

- AI/ML-based adaptive lightweight cryptography for dynamic threat and resource management.
- Post-quantum lightweight algorithms to secure IoT against future quantum attacks.
- Integration with blockchain to enhance decentralized security and data integrity.

In conclusion, lightweight cryptography is essential for the secure and efficient operation of IoT networks, and ongoing research will continue to optimize these algorithms for scalability, resilience, and emerging threats.

REFERENCES

[1] A. Sevin, "Implementation of a Data-Parallel Approach on a Lightweight Hash Function for IoT Devices," Sustainability, vol. 15, no. 4, pp. 3552, 2025. [Online]. Available: https://www.mdpi.com/2071-1050/15/4/3552

[2] R. Bharathi and N. Parvatham, "Light-Weight Present Block Cipher Model for IoT Security on FPGA," Int. J. Appl. Sci. Comput. Eng., vol. 33, no. 1, pp. 46134, 2021. [Online]. Available: https://www.techscience.com/iasc/v33n1/46134/html

[3] V. Arribas, S. Nikova, and V. Rijmen, "Guards in Action: First-Order SCA Secure Implementations of Ketje Without Additional Randomness," in Proc. 21st Euromicro Conf. Digital Syst. Design (DSD), Prague, Czech

Republic, 2018, pp. 492–499. [Online]. Available: https://www.mdpi.com/2410-387X/6/3/45

[4] N. Noura, A. Chehab, L. Sleem, and M. M. Mansour, "One Round Cipher Algorithm for Multimedia IoT Devices," J. Comput. Sci. Technol., vol. 33, no. 1, pp. 46134, 2018. [Online]. Available: https://www.researchgate.net/figure/List-of-recent-lightweight-cryptographic-algorithms_tbl1_322499033

[5] W. J. Buchanan, R. Asif, and N. Gunathilake, "Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications," in Proc. Int. Conf. Comput. Commun. Technol., 2019, pp. 1–6. [Online]. Available: https://www.researchgate.net/figure/Lightweight-Cryptography-LWC-Classification_fig2_331298498

[6] M. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia, "Quark: A Lightweight Hash," J. Cryptol., vol. 26, no. 2, pp. 313–339, 2013. [Online]. Available: https://link.springer.com/article/10.1007/s12652-017-0494-4

[7] S. Al Salami, J. Baek, K. Salah, and E. Damiani, "Lightweight Encryption for Smart Home," in Proc. 11th Int. Conf. Availability, Reliab. Secur., 2016, pp. 382–388. [Online]. Available: https://link.springer.com/article/10.1007/s12652-017-0494-4

[8] J. P. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia, "Quark: A Lightweight Hash," J. Cryptol., vol. 26, no. 2, pp. 313–339, 2013. [Online]. Available: https://link.springer.com/article/10.1007/s12652-017-0494-4

[9] S. Babbage and M. Dodd, "The MICKEY Stream Ciphers," in New Stream Cipher Designs, Springer, Berlin, 2008, pp. 191–209. [Online]. Available: https://link.springer.com/article/10.1007/s12652-017-0494-4

[10] H. Manifavas, G. Hatzivasilis, K. Fysarakis, and I. Papaefstathiou, "A Survey of Lightweight Stream Ciphers for Embedded Systems," J. Comput. Sci. Technol., vol. 33, no. 1, pp. 46134, 2015. [Online]. Available: https://www.researchgate.net/figure/Lightweight-Cryptography-LWC-Classification_fig2_331298498

[11] H. Manifavas, G. Hatzivasilis, K. Fysarakis, and I. Papaefstathiou, "A Survey of Lightweight Stream Ciphers for Embedded Systems," J. Comput. Sci. Technol., vol. 33, no. 1, pp. 46134, 2015. [Online]. Available: https://www.researchgate.net/figure/Lightweight-Cryptography-LWC-Classification_fig2_331298498

[12] H. Manifavas, G. Hatzivasilis, K. Fysarakis, and I. Papaefstathiou, "A Survey of Lightweight Stream Ciphers for Embedded Systems," J. Comput. Sci. Technol., vol. 33, no. 1, pp. 46134, 2015. [Online]. Available: https://www.researchgate.net/figure/Lightweight-Cryptography-LWC-Classification_fig2_331298498

[13] H. Manifavas, G. Hatzivasilis, K. Fysarakis, and I. Papaefstathiou, "A Survey of Lightweight Stream Ciphers for Embedded Systems," J. Comput. Sci. Technol., vol. 33, no. 1, pp. 46134, 2015. [Online]. Available: https://www.researchgate.net/figure/Lightweight-Cryptography-LWC-Classification_fig2_331298498

[14] H. Manifavas, G. Hatzivasilis, K. Fysarakis, and I. Papaefstathiou, "A Survey of Lightweight Stream Ciphers for Embedded Systems," J. Comput. Sci. Technol., vol. 33, no. 1, pp. 46134, 2015. [Online]. Available: https://www.researchgate.net/figure/Lightweight-Cryptography-LWC-Classification_fig2_331298498

[15] H. Manifavas, G. Hatzivasilis, K. Fysarakis, and I. Papaefstathiou, "A Survey of Lightweight Stream Ciphers for Embedded Systems," J. Comput. Sci. Technol., vol. 33, no. 1, pp. 46134, 2015. [Online]. Available: https://www.researchgate.net/figure/Lightweight-Cryptography-LWC-Classification_fig2_331298498

[16] H. Manifavas, G. Hatzivasilis, K. Fysarakis, and I. Papaefstathiou, "A Survey of Lightweight Stream Ciphers for Embedded Systems," J. Comput. Sci. Technol., vol. 33, no. 1, pp. 46134, 2015. [Online]. Available: https://www.researchgate.net/figure/Lightweight

-Cryptography-LWC-Classification_fig2_331298498
[17] H. Manifavas, G. Hatzivasilis, K. Fysarakis, and I. Papaefstathiou, "A Survey of Lightweight Stream Ciphers for Embedded Systems," J. Comput. Sci. Technol., vol. 33, no. 1, pp. 46134, 2015. [Online]. Available: https://www.researchgate.net/figure/Lightweight-Cryptography-LWC-Classification_fig2_331298498
[18] H. Manifavas, G. Hatzivasilis, K. Fysarakis, and I. Papaefstathiou, "A Survey of Lightweight Stream Ciphers for Embedded Systems," J. Comput. Sci. Technol., vol. 33, no. 1, pp. 46134, 2015. [Online]. Available: https://www.researchgate.net/figure/Lightweight-Cryptography-LWC-Classification_fig2_331298498
[19] H. Manifavas, G. Hatzivasilis, K. Fysarakis, and I. Papaefstathiou, "A Survey of Lightweight Stream Ciphers for Embedded Systems," J. Comput. Sci. Technol., vol. 33, no. 1, pp. 46134, 2015. [Online]. Available: https://www.researchgate.net/figure/Lightweight-Cryptography-LWC-Classification_fig2_331298498
[20] H. Manifavas, G. Hatzivasilis, K. Fysarakis, and I. Papaefstathiou, "A Survey of Lightweight Stream Ciphers for Embedded Systems," J. Comput. Sci. Technol., vol. 33, no. 1, pp. 46134, 2015. [Online]. Available: https://www.researchgate.net/figure/Lightweight-Cryptography-LWC-Classification_fig2_331298498
[21] H. Manifavas, G. Hatzivasilis, K. Fysarakis, and I. Papaefstathiou, "A Survey of Lightweight Stream Ciphers for Embedded Systems," J. Comput. Sci. Technol., vol. 33, no. 1, pp. 46134, 2015. [Online]. Available: https://www.researchgate.net/figure/Lightweight-Cryptography-LWC-Classification_fig2_331298498
[22] H. Manifavas, G. Hatzivasilis, K. Fysarakis, and I. Papaefstathiou, "A Survey of Lightweight Stream Ciphers for Embedded Systems," J. Comput. Sci. Technol., vol. 33, no. 1, pp. 46134, 2015. [Online]. Available: https://www.researchgate.net/figure/Lightweight-Cryptography-LWC-Classification_fig2_331298498
[23] H. Manifavas, G. Hatzivasilis, K. Fysarakis, and I. Papaefstathiou, "A Survey of Lightweight Stream Ciphers for Embedded Systems,"