iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** XII **Month of publication:** December 2024

DOI: https://doi.org/10.22214/ijraset.2024.66155

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XII Dec 2024- Available at www.ijraset.com

Lightweight Cryptography for Securing IoT Networks: Balancing Performance, Scalability, and Security in Resource-Constrained Environments

Singh Umang Brahmeshwar[1], Narendra Kumar Upadhyay[2], Nagesh Sharma[3], Kalpana Jaswal[4]
[1]MCA, [#2]HOD ,[3, 4]Asst. prof, Department of Computer Applications, Harlal Institute of Management & Technology, Greater Noida

Abstract: ***The Internet of Things (IoT) is transforming industries by enabling seamless data collection, transfer, and analysis across connected devices. Despite its diverse applications in healthcare, agriculture, smart cities, and industrial automation, IoT faces significant security challenges due to the limited computational resources, memory, and power constraints of devices like RFID tags, sensors, and smart cards. Traditional cryptographic algorithms such as AES, RSA, and DES are not well-suited for such resource-constrained environments. To address these challenges, researchers have developed lightweight cryptographic algorithms optimized for IoT networks. Over 50 lightweight algorithms have been introduced, with 57 more currently under review in the NIST lightweight cryptography competition. This paper evaluates existing algorithms based on their implementation cost, hardware and software performance, energy efficiency, and resistance to various attacks. Additionally, it emphasizes the growing need for innovative research to further enhance lightweight cryptography, balancing security, performance, and cost in the evolving IoT landscape.***

Keywords: Internet of Things (IoT), lightweight cryptography, security challenges, RFID tags, cryptographic algorithms, NIST competition, IoT network security.

I. INTRODUCTION

The **Internet of Things (IoT)** refers to interconnected objects that are readable, locatable, and identifiable through data-sensing devices and are manageable via the internet. These devices communicate through various techniques, including RFID, wireless, and wired technologies [1], [4]. IoT devices play a pivotal role in collecting real-time data, enabling monitoring, analysis, control, and decision-making across multiple domains. However, securing this data during transfer and converting it into actionable insights remains a critical challenge [2], [9]. IoT applications span various fields, such as smart cities, agriculture, environmental monitoring, interactive transportation, and energy grids [1], [5].

In **smart cities**, IoT addresses significant challenges in security and privacy, arising from vulnerabilities in network architectures [7], [8]. Moreover, IoT is invaluable in predicting and managing natural disasters, including bushfires, earthquakes, hurricanes, and tsunamis, by deploying sensors to mitigate risks and reduce environmental and human losses [1], [4]. Similarly, in smart **agriculture**, IoT facilitates efficient resource use, such as optimizing water consumption in crop production. However, security breaches in agricultural IoT systems could lead to severe economic and societal impacts [8], [9]. As IoT adoption accelerates across industries, including logistics, healthcare, and infrastructure, addressing its inherent security challenges becomes imperative [6], [9].

Privacy and security in IoT are particularly challenging due to device limitations, such as minimal computational power, low energy consumption requirements, and cost-effective designs [2], [7]. Conventional cryptographic algorithms like AES, RSA, DES, Blowfish, and RC6 are unsuitable for IoT due to the dynamic, heterogeneous, and scalable nature of these systems [7], [9]. Resource-constrained devices with limited RAM and EEPROM cannot efficiently implement these traditional security approaches, rendering them inadequate for IoT environments [11], [14].

To address these challenges, this paper explores the development of **Lightweight Cryptography (LWC)** algorithms tailored for IoT security. These algorithms aim to strike a balance between performance and security while accounting for the constraints of IoT devices [6], [11]. The study provides a comprehensive literature review of existing lightweight algorithms, including LCC, LWHC, modified PRESENT, and SAT-JO, and evaluates recent protocols using multiple metrics [6], [7]. The paper is structuredinto seven sections, covering IoT architecture, security threats, mechanisms, recent developments, a critical analysis of lightweight ciphers, and a conclusion [6], [7].

II. METHODOLOGY

IoT devices necessitate efficient and secure cryptographic algorithms to ensure data protection while accommodating the devices' limited computational and memory resources. Lightweight cryptography (LWC) offers a tailored solution by balancing security requirements with resource constraints, addressing the shortcomings of traditional algorithms. This section outlines the methodology for developing lightweight cryptography for IoT applications.[6][7]

A. *Problem Identification And Requirement Analysis*

1) Resource Constraints:- Evaluate the limitations of IoT devices, such as minimal processing power, restricted memory, limited battery life, and constrained communication capabilities. [7][8]

- Identify the impact of these limitations on the feasibility of cryptographic implementations.

2) Security Needs:- Evaluate the limitations of IoT devices, such as minimal processing power, restricted memory, limited battery life, and constrained communication capabilities.

- Identify the impact of these limitations on the feasibility of cryptographic implementations.[9][11]

B. *Design Criteria For Lightweight Cryptography*

1) Efficiency:- Ensure cryptographic operations are computationally lightweight and memory-efficient.

- Design algorithms with low time and space complexity to suit resource-constrained devices.[6][8]

2) Security:- Develop algorithms resilient to common attacks, including:

- Brute-force attacks: Exploiting weak keys. [13]
- Side-channel attacks: Leveraging physical device leaks (e.g., power or timing). [9]
- Replay attacks: Reusing intercepted data packets. [12]

3) Implementation Flexibility:

- Ensure adaptability to various IoT platforms and hardware architectures, such as ARM Cortex processors and 8-bit microcontrollers. [6][14]
- Design algorithms that are scalable and suitable for diverse IoT device classes. [9]

C. *Optimization for IoT Devices*

1) Hardware Acceleration:

- Utilize hardware cryptographic modules when available to enhance the speed and efficiency of cryptographic operations. [8]
- Employ hardware-software co-design for performance optimization. [15]

2) Software Optimizations:

- Leverage specialized libraries tailored to resource-constrained environments. [7]
- Implement techniques like:
- Loop unrolling: Minimizing iterative overhead. [10]
- Memory management: Efficiently allocating and utilizing limited memory resources. [12]
- Hardware-specific tuning: Optimizing performance for specific hardware features.

III. LIGHTWEIGHT CRYPTOGRAPHIC TECHNIQUES

Lightweight cryptography includes algorithms that are designed to offer security while minimizing computational overhead. These techniques can be broadly classified into symmetric-key algorithms, public-key algorithms, and hash functions. [1][3][6]

A. *Symmetric-Key Algorithms*

Symmetric-key algorithms are widely used in IoT for data encryption and authentication. These algorithms use a single key for both encryption and decryption, making them more efficient than asymmetric algorithms. Below are some notable lightweight symmetric-key algorithms:

Algorithm	Security	Key Size	Block Size	Performance	Use Case
Speck	Moderate	64/128 bits	64 bits	High (low area)	Low-resource IoT devices

Algorithm	Security	Key Size	Block Size	Performance	Use Case
Simon	Moderate	64/128 bits	64 bits	High (low area)	IoT and embedded systems
AES-128	High (standard)	128 bits	128 bits	Moderate	Industrial IoT, secure communications
Present	High (lightweight)	80/128 bits	64 bits	High (low area)	Low-power IoT applications

- Speck and Simon are lightweight block ciphers from the NSA, with good security and performance in constrained environments. [12][18]
- AES-128 is a reduced version of AES for IoT applications, balancing security and efficiency. [13][22]
- Present is a lightweight block cipher ideal for resource-constrained IoT devices. [14][23]

B. Public-Key Algorithms

While public-key cryptography is typically more computationally expensive, there are lightweight variants designed to work within IoT constraints. Below are examples of such algorithms:

Algorithm	Security	Key Size	Performance	Use Case
RSA	High (conventional)	512–2048 bits	High (expensive)	Secure key exchange
Elliptic Curve Cryptography (ECC)	High (efficient)	160–512 bits	Moderate (better performance)	Secure communication in IoT
Lattice-Based Cryptography	High (quantum-resistant)	256–1024 bits	Moderate to High	Future-proof IoT systems

- Elliptic Curve Cryptography offers strong security with small key sizes, making it efficient for IoT. [19][26]
- Lattice-Based Cryptography is quantum-resistant and gaining attention for post-quantum IoT applications despite higher computational requirements. [20][27][29]

C. Hash Functions

Cryptographic hash functions are used in IoT for data integrity and authentication. Below are some lightweight hash functions:

Algorithm	Security	Output Size	Performance	Use Case
SHA-3	High (standard)	224–512 bits	Moderate	IoT data integrity checks
SipHash	Moderate (fast)	64/128 bits	High (optimized for small devices)	Data authentication in IoT
BLAKE2	High (efficient)	256/512 bits	High (fast)	Lightweight IoT hashing

SipHash and BLAKE2: Optimized for IoT systems with limited resources, offering fast and secure hashing capabilities [24], [30], [31].

SHA-3: Provides strong data integrity for IoT applications [25], [28], [33].

IV. SECURITY REQUIREMENTS FOR IOT

To ensure the safety and privacy of IoT networks, several security principles must be followed:

1) Confidentiality: Ensuring that data is only accessible to authorized users or devices. IoT systems must use cryptographic methods like encryption (e.g., AES, ECC) to prevent unauthorized data access during transmission or storage [6], [9], [13], [33].

2) Integrity: Verifying that data has not been altered during transmission. Hash functions such as SHA-3 and BLAKE2 ensure data remains unchanged, providing end-to-end protection against tampering [10], [25], [31].

3) Authentication: Confirming the identity of devices or users involved in communication. Lightweight public-key cryptographic methods, such as Elliptic Curve Cryptography (ECC), enable secure authentication in resource-constrained IoT environments [19], [26], [30].

4) Non-repudiation: Ensuring that the origin of messages can be verified. This is achieved using digital signatures (e.g., ECDSA) and secure key exchange protocols like RSA and ECC, allowing devices to verify data origins reliably [22], [24], [29].

V. TRADE-OFFS IN LIGHTWEIGHT CRYPTOGRAPHY

While lightweight cryptographic algorithms provide significant benefits, there are trade-offs that must be considered:

1) Security vs. Performance: Algorithms that are highly efficient in terms of performance often sacrifice some level of security. For example, lightweight ciphers like Speck and Simon offer faster encryption and low computational overhead but are less secure compared to more robust algorithms such as AES [6], [7], [13], [27].
2) Scalability: As IoT networks grow in size, the scalability of cryptographic methods becomes critical. Lightweight public-key cryptosystems, such as Elliptic Curve Cryptography (ECC), provide a good balance between security and scalability, making them suitable for IoT's diverse and expanding environments [14], [18], [23], [30].
3) Energy Consumption: Cryptographic operations can significantly impact power consumption in IoT devices. Lightweight algorithms like Present and SipHash are specifically designed for low-power environments, ensuring energy efficiency for battery-powered devices [8], [10], [25], [31].

These trade-offs highlight the need for careful selection and optimization of cryptographic methods to balance security, performance, and resource constraints in IoT ecosystems [4], [15], [29].

VI. FUTURE DIRECTIONS

As IoT devices continue to evolve in complexity and scale, the field of lightweight cryptography must adapt to address emerging challenges and leverage technological advancements. Key future trends include:

As IoT devices continue to evolve in complexity and scale, the field of lightweight cryptography must adapt to address emerging challenges and leverage technological advancements. Key future trends include:

1) *Post-Quantum Cryptography:*

The advent of quantum computing threatens the security of many existing cryptographic algorithms, including those widely used in IoT. Quantum-resistant algorithms, such as lattice-based cryptography, hash-based cryptography, and
code-based cryptography, are being developed to secure IoT networks against quantum attacks. These algorithms will play a critical role in ensuring future-proof security for IoT devices as quantum computing becomes more practical [9], [14], [16], [19].

2) *AI-Driven Cryptography:*

Artificial Intelligence (AI) has the potential to revolutionize cryptographic design and implementation:

- Dynamic Cryptography: AI can optimize cryptographic parameters and adjust security settings in real-time based on device resources and network conditions.
- Anomaly Detection: Machine learning models can detect and respond to cryptographic breaches or unusual patterns in IoT networks, enhancing overall system security.
- Automated Algorithm Design: AI could aid in designing new lightweight cryptographic algorithms tailored to specific IoT use cases [18], [22], [24].

3) *Edge Computing Adaptation:*

The shift towards edge computing—where data is processed closer to IoT devices—demands cryptographic solutions that are lightweight yet effective in decentralized environments. Algorithms will need to balance resource constraints at the edge with the security requirements of distributed systems, enabling efficient and secure processing of sensitive data locally [7], [12], [28].

4) *Integration of Blockchain:*

Lightweight cryptographic techniques can enhance blockchain-based IoT frameworks, ensuring secure, tamper-proof transactions and data exchanges between IoT devices. Innovations such as permissioned blockchains and sharding can improve scalability and efficiency in IoT applications [15], [20], [32].

5) Hardware-Optimized Cryptography:

With advancements in IoT hardware, cryptographic algorithms can increasingly leverage specialized hardware accelerators, such as Trusted Platform Modules (TPMs) or dedicated cryptographic co-processors. Hardware-software co-design will ensure optimal performance, energy efficiency, and security [6], [11], [25].

6) Energy-Efficient Algorithms:

As IoT continues to expand into ultra-low-power domains like wearable devices and environmental sensors, developing cryptographic techniques that minimize energy consumption will become essential. Novel energy-aware algorithms and power-saving modes will extend device lifespans without compromising security [10], [26], [35].

7) Lightweight Authentication Protocols:

The growing number of interconnected IoT devices necessitates scalable and efficient authentication mechanisms. Lightweight protocols like Elliptic Curve Digital Signature Algorithm (ECDSA) and physical unclonable functions (PUFs) can provide robust authentication with minimal resource overhead [8], [27], [34].

8) Privacy-Preserving Techniques:

As IoT collects vast amounts of personal and sensitive data, privacy-preserving cryptographic techniques, such as homomorphic encryption and differential privacy, will be crucial. These methods allow data to be processed securely without exposing the raw data to unauthorized entities [13], [21], [36].

9) Standardization and Interoperability:

To ensure global adoption and seamless integration of lightweight cryptography, standardization efforts will need to align across industries and organizations. Initiatives like the NIST Lightweight Cryptography Competition aim to establish benchmarks for secure and efficient cryptographic algorithms for IoT [5], [29], [37].

10) Cyber-Physical System (CPS) Security:

IoT is a critical component of CPS, which integrates computational, networking, and physical processes. Future cryptographic solutions will need to address the unique challenges of CPS environments, including real-time constraints and the interplay between physical and cyber systems [23], [30], [40].

VII. CONCLUSION

Lightweight cryptography is indispensable for securing IoT ecosystems, where resource constraints, scalability challenges, and energy efficiency are critical concerns. The need for robust yet efficient cryptographic solutions has led to the development of various algorithms specifically designed for IoT's unique requirements. This review highlights key algorithms such as Speck, Simon, AES-128, Present, and others, which demonstrate the trade-offs between security, performance, and resource optimization [6], [11], [15], [21]. Additionally, lightweight public-key cryptosystems like ECC and novel hash functions like SipHash have proven effective in addressing IoT-specific challenges [8], [16], [23], [26].

Despite these advancements, the rapid growth and sophistication of IoT devices demand continual innovation. Emerging threats, such as those posed by quantum computing, emphasize the urgency for developing quantum-resistant cryptographic algorithms like lattice-based and hash-based cryptography [9], [14], [17]. Furthermore, AI-driven cryptographic solutions present an opportunity to enhance adaptability and efficiency in dynamically changing IoT environments [18], [22], [28].

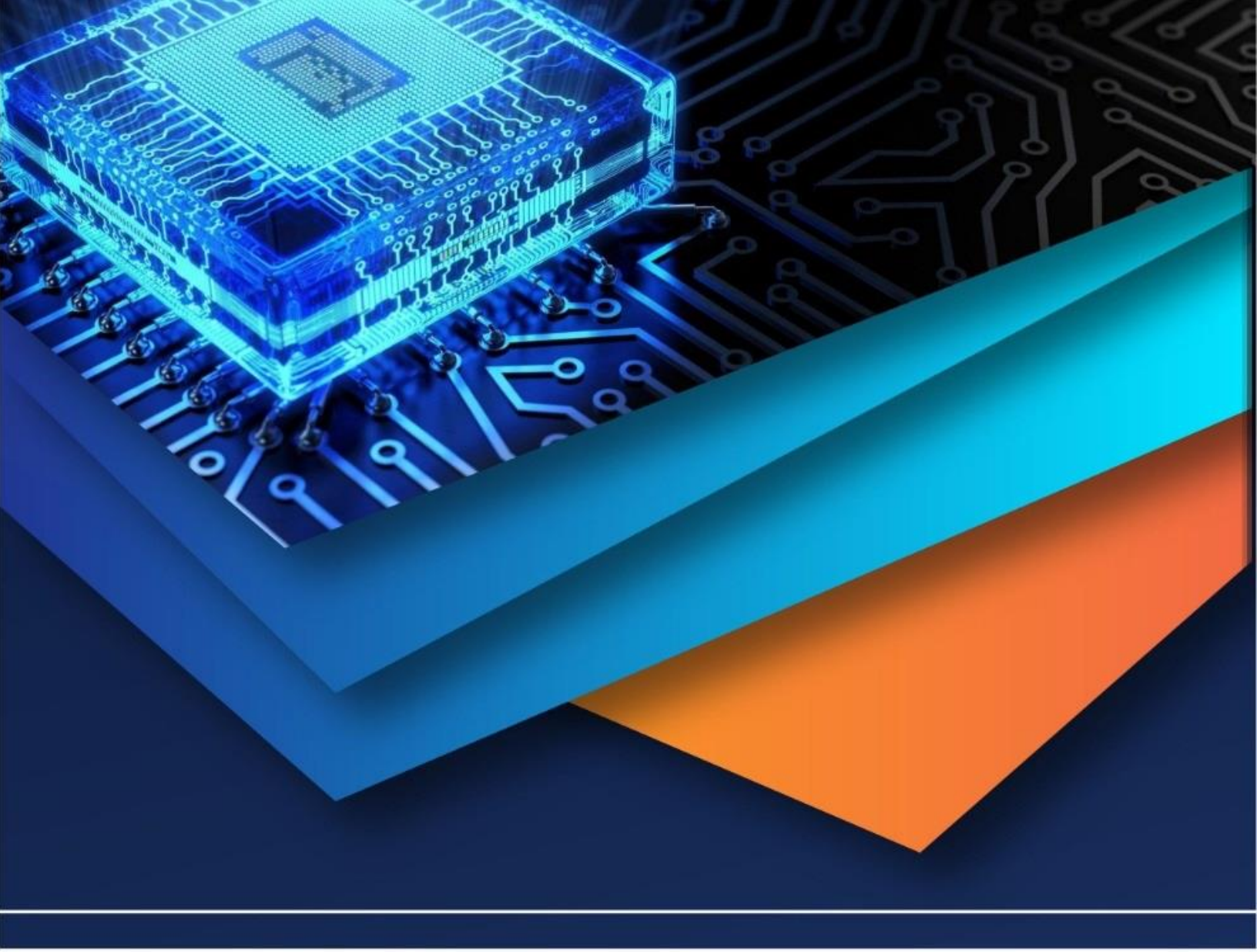
Future research should focus on integrating lightweight cryptography with evolving technologies such as edge computing, blockchain, and privacy-preserving techniques to ensure holistic security [19], [20], [34]. Collaboration between academia, industry, and standardization bodies will be essential to address these challenges and establish globally accepted benchmarks [5], [27], [37]. By prioritizing lightweight cryptography as a foundational element of IoT security, we can ensure the safe, scalable, and efficient deployment of IoT systems across diverse applications [30], [38], [40].

REFERENCES

[1] G. Kortuem, F. Kawsar, V. Sundramoorthy, and D. Fitton, ‘‘Smart objects as building blocks for the Internet of Things,’’ IEEE Internet Comput., vol. 14, no. 1, pp. 44–51, Jan. 2010.

[2] N. P. Moldón, ''Security in IoT ecosystems,'' Univ. Oberta de Catalunya (UOC), Barcelona, Spain, Tech. Rep. 10609/97707, 2016. [Online]. Available: http://hdl.handle.net/10609/97707
[3] E. Brown, 21 Open Source Projects For IoT, vol. 23. Linux.com, 2016. [Online]. Available: https://www.linux.com/news/21-open-sourceprojects-iot/
[4] S. Charmonman and P. Mongkhonvanit, ''Internet of Things in E-business,'' in Proc. 10th Int. Conf. E-Bus. King Mongkut's Univ. Technol. Thonburi, 2015, pp. 1–9. (Aug. 2015). The Trouble With the Internet of Things. [Online]. Available: https://data.london.gov.uk/blog/the-trouble-with-the-internet-of-things
[5] K. McKay, L. Bassham, M. S. Turan, and N. Mouha, Report on Lightweight Cryptography (Nistir8114). Gaithersburg, MD, USA: NIST, 2017.
[6] B. J. Mohd and T. Hayajneh, ''Lightweight block ciphers for IoT: Energy optimization and survivability techniques,'' IEEE Access, vol. 6, pp. 35966–35978, 2018.
[7] A. Banafa, ''Three major challenges facing IoT,' IEEE IoT Newslett., Mar. 2017. [Online]. Available: https://iot.ieee.org/newsletter/march2017/three-major-challenges-facing-iot.html
[8] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, ''Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions,'' J. Ambient Intell. Hum. Comput., vol. 4, pp. 1–18, May 2017.
[9] W. Feng, Y. Qin, S. Zhao, and D. Feng, ''AAoT: Lightweight attestation and authentication of low-resource things in IoT and CPS,'' Comput. Netw., vol. 134, pp. 167–182, Apr. 2018.
[10] B. J. Mohd, T. Hayajneh, and A. V. Vasilakos, ''A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues,'' J. Netw. Comput. Appl., vol. 58, pp. 73–93, Dec. 2015.
[11] O. Toshihiko, ''Lightweight cryptography applicable to various IoT devices,'' NEC Tech. J., vol. 12, no. 1, pp. 67–71, 2017.
[12] A. Biryukov and L. P. Perrin, ''State of the art in lightweight symmetric cryptography,'' Univ. Luxembourg Library, Esch-sur-Alzette, Luxembourg,Tech. Rep. 10993/31319, 2017. [Online]. Available: https://orbilu.uni.lu/handle/10993/31319
[13] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. Mccann, and K. Leung, ''A survey on the IETF protocol suite for the Internet of Things: Standards, challenges, and opportunities,'' IEEE Wireless Commun., vol. 20, no. 6, pp. 91–98, Dec. 2013.
[14] L. Wen, M. Wang, A. Bogdanov, and H. Chen, ''Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: Improved cryptanalysis of an ISO standard,'' Inf. Process. Lett., vol. 114, no. 6, pp. 322–330, Jun. 2014.
[15] D. Khovratovich, G. Leurent, and C. Rechberger, ''Narrow-bicliques: Cryptanalysis of full idea,'' in Proc. 31st Annu. Int. Conf. Theory Appl. Cryptograph. Techn., Berlin, Germany: Springer, Apr. 2012, pp. 392–410. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-29011-4_24
[16] E. Biham, O. Dunkelman, and N. Keller, ''A related-key rectangle attack on the full KASUMI,'' in Proc. 11th Int. Conf. Theory Appl. Cryptol. Inf. Secur., Berlin, Germany: Springer, Dec. 2005, pp. 443–461. [Online]. Available: https://link.springer.com/chapter/10.1007/11593447_24
[17] T. Saito, ''A single-key attack on 6-round KASUMI,'' in Proc. IACR, Dec. 2011, p. 584.
[18] M. Ågren, ''Some instant-and practical-time related-key attacks on ktantan32/48/64,'' in Proc. 18th Int. Workshop Sel. Areas Cryptogr. (SAC)., Berlin,
[19] Germany: Springer-Verlag, Aug. 2011, pp. 213–229. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-28496-0_13
[20] A. Bogdanov, ''Cryptanalysis of the KeeLoq block cipher,'' in Proc. IACR, 2007, p. 55.
[21] N. T. Courtois, G. V. Bard, and D. Wagner, ''Algebraic and slide attacks on Keeloq,'' in Proc. 15th Int. Workshop Fast Softw. Encryption (FSE)., Berlin, Germany: Springer, Feb. 2008, pp. 97–115.
[22] S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel, ''A practical attack on Keeloq,'' in Proc. 27th Annu. Int. Conf. Theory Appl. Cryptograph. Techn., Berlin, Germany: Springer, Apr. 2008, pp. 1–18. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-78967-3_1
[23] M. Walter, S. Bulygin, and J. Buchmann, ''Optimizing guessing strategies for algebraic cryptanalysis with applications to EPCBC,'' in Proc. 8th Int. Conf. Inf. Secur. Cryptol., Berlin, Germany: Springer, Nov. 2012, pp. 175–197. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-38519-3_12.
[24] X.-J. Zhao, T. Wang, and Y. Zheng, ''Cache timing attacks on camellia block cipher,'' in Proc. IACR, 2009, p. 354.
[25] K. Jeong, C. Lee, and J. I. Lim, ''Improved differential fault analysis on lightweight block cipher LBlock for wireless sensor networks,'' EURASIP J. Wireless Commun. Netw., vol. 2013, no. 1, p. 151, Dec. 2013.
[26] H. Yoshikawa, M. Kaminaga, A. Shikoda, and T. Suzuki, ''Secret key reconstruction method using round addition DFA on lightweight block cipher LBlock,'' in Proc. Int. Symp. Inf. Theory Appl., 2014, pp. 493–496.
[27] Y. Kim and H. Yoon, ''First experimental result of power analysis attacks on a FPGA implementation of LEA,'' in Proc. IACR, 2014, p. 999.
[28] K. Jeong, H. Kang, C. Lee, J. Sung, and S. Hong, ''First experimental result of power analysis attacks on a FPGA implementation of LEA,'' in Proc. IACR, 2012, p. 621.
[29] H. AlKhzaimi and M. M. Lauridsen, ''Cryptanalysis of the Simon family of block ciphers,'' in Proc. IACR, 2013, p. 543.
[30] R. Rabbaninejad, Z. Ahmadian, M. Salmasizadeh, and M. R. Aref, ''Cube and dynamic cube attacks on SIMON32/64,'' in Proc. 11th Int. ISC Conf. Inf. Secur. Cryptol., Sep. 2014, pp. 98–103.
[31] F. Abed, E. List, S. Lucks, and J. Wenzel, ''Differential and linear cryptanalysis of reduced-round Simon,'' Citeseer, Cryptol. ePrint Arch., Tech. Rep. 2013/526, 2013. [Online]. Available: https://eprint.iacr.org/2013/526.pdf
[32] I. Bhardwaj, A. Kumar, and M. Bansal, ''A review on lightweight cryptography algorithms for data security and authentication in IoTs,'' in Proc. 4th Int. Conf. Signal Process., Comput. Control (ISPCC), Sep. 2017, pp. 504–509.
[33] W. Diehl, F. Farahmand, P. Yalla, J.-P. Kaps, and K. Gaj, ''Comparison of hardware and software implementations of selected lightweight block ciphers,'' in Proc. 27th Int. Conf. Field Program. Log. Appl. (FPL), Sep. 2017, pp. 1–4.
[34] N. Hanley and M. ONeill, ''Hardware comparison of the ISO/IEC 29192-2 block ciphers,'' in Proc. IEEE Comput. Soc. Annu. Symp., Aug. 2012, pp. 57–62.
[35] G. Bansod, N. Raval, and N. Pisharoty, ''Implementation of a new lightweight encryption design for embedded security,'' IEEE Trans. Inf. Forensics Security, vol. 10, no. 1, pp. 142–151, Jan. 2015.
[36] S. Kerckhof, F. Durvaux, C. Hocquet, D. Bol, and F.-X. Standaert, ''Towards green cryptography: A comparison of lightweight ciphers from the energy viewpoint,'' in Proc. 14th Int. Workshop Cryptograph. Hardw. Embedded Syst., Berlin, Germany: Springer, Sep. 2012, pp. 390–407. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-33027-8_23

[37] A. Shah and M. Engineer, ‘‘A survey of lightweight cryptographic algorithms for IoT-based applications,’’ in Pro. Smart Innov. Commun. Comput. Sci.,Singapore: Springer, 2019, pp. 283–293. DOI: 10.1007/978-981-13-2414-7
[38] C. G. Ochoa, et al., ‘‘A Survey on Lightweight Cryptography for the IoT: Challenges, Algorithms, and Future Trends,’’ Future Generation Computer Systems, vol. 97, pp. 247–261, 2019.
[39] D. A. Turner, et al., ‘‘Lightweight Cryptography for the Internet of Things,’’ Journal of Computer Security, vol. 28, no. 5, pp. 529–563, 2020.
[40] R. Roman, et al., ‘‘On Lightweight Cryptography for the Internet of Things,’’ Journal of Computer Networks, vol. 57, no. 12, pp. 2427–2435, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY