Lightweight Cryptography Algorithms for Internet of Things Enabled Networks. A Comparative Study

Javaria Khalid[1, a*], Rabbia Ijaz[1], Rida Fatima[2], Umer Nawaz[3]

[1]University of Engineering & Technology, Lahore, Punjab, Pakistan.

[a]Government College for Women University, Sialkot, Punjab, Pakistan

[2]Bahria University Lahore Campus (BULC).

[3]Barikat Cyber Security Qatar

***Correspondence**. javaria.khalid666@gmail.com

Citation | Khalid. J, Ijaz. R, Fatima. R, Nawaz. U, "Lightweight Cryptography Algorithms for IoT Enabled Networks. A Comparative Study", IJIST, Vol. 06 Issue. 04 pp 2124-2139, Dec 2024

Received | Nov 22, 2024 **Revised** | Dec 14, 2024 **Accepted** | Dec 20, 2024 **Published** | Dec 22, 2024.

The rapid advancement of technology has facilitated the interconnection of numerous devices, enabling the collection of vast amounts of data. Consequently, ensuring security within IoT networks has become a top priority. Cryptography is crucial in safeguarding network authentication, confidentiality, data integrity, and access control. In IoT settings, conventional cryptographic protocols frequently prove impractical owing to the limitations confronting IoT devices. Consequently, scholars have suggested multiple lightweight cryptographic algorithms and protocols customized for safeguarding data in IoT networks, aiming to overcome this hurdle. This review article delves into the most recent lightweight cryptographic protocols designed for IoT networks and furnishes a comparative evaluation of prevalent modern block ciphers. The comparative study discusses the most recent lightweight cryptographic algorithms in different evaluation parameters in terms of their performance metrics, and cryptographic features and offers in-depth analysis of their efficiency. In the concluding section, the paper discusses necessary adaptations and suggests future research directions.

Keywords. IoT, Lightweight, Lightweight Cryptography, Block Cipher, Cryptography Feature

Introduction.

The notion of the IoT involves regular items embedded with data-sensing functionalities, rendering them accessible, trackable, and controllable through the Internet. IoT gadgets employ diverse communication methods like RFID, wireless, or wired technologies. These items include not just advanced electronic devices like smartphones and cars but also everyday objects such as groceries, garments, animals, trash bins, trees, and beyond. The primary aim of IoT is to enable seamless communication between objects anytime, anywhere, utilizing any network or service available. [1].

Over recent years, there has been an immense surge in the proliferation of the IoT, which has permeated various facets of our daily existence including urban settings, agricultural practices, healthcare facilities, environmental monitoring, residential domains, and transportation networks. Typically outfitted with an array of sensors and actuators, IoT endpoints gather copious amounts of data, transmitting this information through digital channels to facilitate monitoring, analysis, control, and the derivation of diverse insights. [2]. The majority of this information constitutes real-time data crucial for informed decision-making across various service sectors. However, the secure transmission and conversion of this raw data from the Internet into comprehensible insights are essential for leveraging knowledge in areas like smart city development, agriculture, environmental management, interactive transportation, and electricity grids. As per the United Nations Food and Agriculture Organization, there is a projected requirement for a 70% increase in food production by 2050 [3]. Effective implementation of advanced agricultural techniques will be pivotal in capitalizing on the expanding market. Take, for instance, the case of Chile, where the utilization of remote sensors has resulted in a 70% reduction in water usage for blueberry cultivation. [4]. Enhancing cryptographic protocols presents a viable solution to the security challenges prevalent in IoT domains like smart cities. [5].

As per the analysis by Gartner, the IoT, excluding PCs, tablets, and smartphones, is projected to yield revenue exceeding $300 billion by the end of 2020. Additionally, the combined global market for smartphones and tablets is anticipated to encompass up to 7.3 billion units by 2020 [6] [7]. These devices will establish an extensive and intricate network wherein a vast volume of information is exchanged across the network. With the rapid expansion of IoT, various challenges emerge, including managing substantial data loads, optimizing processing capabilities while minimizing energy usage, mitigating security vulnerabilities, and implementing robust encryption methods for handling large datasets [8].

To tackle the hurdles posed by the proliferation of interconnected smart devices within an IoT framework, there is a growing need for the adoption of suitable cryptographic solutions in embedded applications. However, these smart devices typically possess restricted resources, often termed low-resource devices, characterized by their limited computational capacity, constrained battery life, diminutive size, modest memory, and restricted power provision. Consequently, traditional cryptographic primitives may prove unsuitable for such low-resource smart devices, as exemplified by the impracticability of implementing the 1204-bit RSA algorithm in RFID tags [9]. This emerging field is known as lightweight cryptography. The primary motivations for integrating novel technology into IoT systems are outlined below. Enhancing the effectiveness of end-to-end communication entails implementing lightweight symmetric key algorithms to ensure security while minimizing power usage in resource-constrained devices. The feasibility of deployment in low-resource smart devices is underscored by the smaller footprint of lightweight cryptography compared to traditional methods, potentially enabling greater network connectivity with such devices [8].

The proliferation of IoT has brought to light numerous security vulnerabilities, allowing unauthorized devices to breach networks and disrupt connectivity. Consequently, this jeopardizes both security protocols and network privacy. Moreover, IoT relies on cloud computing, presenting numerous security challenges. Additionally, resource-constrained IoT devices face limitations such as low computation power, battery life, memory, and bandwidth. Thus, there is a pressing need for security solutions that are resource-efficient and do not strain IoT resources [10]. Therefore, it is imperative to tackle and mitigate security and privacy vulnerabilities through the advocacy of effective security measures, which is essential for the advancement of IoT sectors. As interest in IoT continues to surge, the pivotal research inquiry revolves around identifying the foundational elements of streamlined cryptography aimed at resolving the myriad security concerns outlined in Figure 1 below.

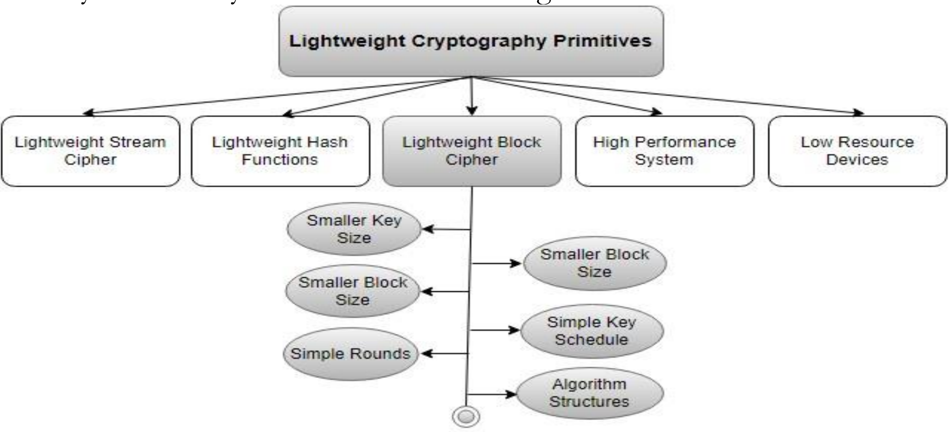

Figure 1. Lightweight Cryptography Primitives [11]

This paper examines the latest advancements in lightweight block cryptography research from 2020 onwards. It assesses recent protocols using various criteria such as block size, key length, and performance metrics to provide a comprehensive evaluation of lightweight cryptography block ciphers. The paper is structured into five sections to present an in-depth analysis of performance perspectives in this field.

IoT Architecture and Threats.

This portion explores the various tiers within the IoT architecture, distinguished by the functionalities of devices and their susceptibility to potential attacks. The vast scope of IoT domains offers abundant prospects. IoT networks bring together various devices with different operating systems and communication protocols, spanning wireless, Zigbee, and mobile technologies. Consequently, they present substantial challenges in terms of security and privacy [12]. Different OSI layers including their components and tasks are elaborated below in Table 1.

Table 1. IoT Layers Components and Tasks [13]

Layers	Components	Tasks
Application layer	Third-party applications, consoles, websites, touch panel.	Machine learning, business models, graphs, and flowcharts
Middleware layer	Vendor-specific third-party application.	Machine learning, processing, pre-processing, and real-time action.
Network layer	Nodes, gateways, firmware.	Transmit and process data, device management, process, and secure routing.
Perception layer	Sensors (temperature and humidity), actuators (relays and motor).	Transfer data, identity, monitor, acquisition, and action.

Application Layer and Security Attacks.

The highest tier within the IoT infrastructure is known as the application layer. Situated above the middleware layer, it receives data for various applications. Within this layer, IoT data is represented in formats such as business models, flowcharts, and graphs. Areas that gain advantages from automation at the application layer include smart cities, smart homes, and smart cars. Additionally, threats against this layer involve denial-of-service attacks [14], buffer overflow attacks [15], cross-site Scripting attacks [15], SQL injection attacks [16], phishing attacks [17], and concerns regarding data privacy [18].

Middleware Layer and Security Attacks.

The middleware layer oversees the execution of vendor-specific services tailored to different types of IoT node data, acting as a vital link between the network and application layers. This linkage streamlines the handling, pre-processing, and storage of IoT node information, catering to the needs of both third-party entities and the nodes themselves. [15]. An unauthorized individual has the capability to implement diverse forms of assaults within the middleware, including those pertaining to application security [19], unauthorized access attacks [20], replay attacks [21], sleep deprivation attacks [22], data security attacks [23], etc. The middleware and application tiers employ high-capacity devices capable of implementing conventional cryptographic techniques to safeguard IoT networks.

Network Layer and Security Attacks.

The transit layer, known as the network layer, manages the routing and secure transmission of data across the IoT infrastructure. It employs various protocols such as Zigbee, Bluetooth, IR, and 6LowPan for data communication. The middleware layer is relied upon by the network layer for additional processing and execution. Here are several potential attacks that can occur within this layer.

Eavesdropping. Eavesdropping, characterized as a passive assault, involves extracting message contents from network broadcasts. It involves surreptitiously monitoring, capturing, and intercepting broadcasted data, potentially leading to various forms of attack or the theft of sensitive information. [24].

Spoofing attacks. Within the context of the IoT, devices establish connections with the network either directly or via intermediary gateways. Malicious actors could potentially acquire physical access to nodes or gateways, enabling them to substitute or reprogram these components with nefarious code. To thwart such attacks, it is imperative to implement authentication mechanisms for edge devices and gateways, alongside encryption protocols to safeguard the transmitted data. [25].

The diverse characteristics and constrained resources of IoT architecture nodes render them vulnerable to potential DDoS attacks. Initially, malevolent actors acquire the credentials of the devices, thereby gaining entry to the gateways and devices. Leveraging network data, attackers can scour IoT devices and unleash a Denial-of-Service (DoS) assault by flooding the system with counterfeit packets. [26].

Man-in-the-middle attacks. Because of the diverse structure of IoT architecture, unauthorized individuals can clandestinely intercept communications between two entities to surreptitiously monitor or alter traffic passing between them.

Sinkhole attacks. Perpetrators create sinkholes to lure traffic away from IoT devices. Subsequently, they redirect this network flow to alternate destinations instead of the intended gateway. This breach undermines the privacy and confidentiality of the IoT devices involved [27].

Perception Layer and Security Attacks.

The primary function of IoT systems revolves around the collection and transmission of real-world data. As a result, the perception layer includes a range of tools that collect, analyze, and send data, such as pressure and temperature sensors, along with communication standards like Bluetooth and Zigbee. This stratum comprises two elements. (a) the sensing or controlling unit known as the perception node, and (b) the communication infrastructure, denoted as the perception network, which enables interaction with the higher tiers of the IoT framework [28]. Perceptual nodes, such as sensors and actuators, gather and manage data. The perception network plays a crucial role in facilitating the transmission of collected data to the gateway. It employs various technologies such as Zigbee, RFID, GPS, and Long-Range Wide Area Network (Lora WAN) to ensure effective communication of information [29]. In this layer, nodes may encounter threats of intrusion, compromise, or physical tampering. Typically, such compromised entities are referred to as faulty nodes. Encryption algorithms and methods for managing cryptographic keys are employed to safeguard communication within the perception layer network. Device validation utilizes a proprietary key algorithm that offers enhanced scalability and upholds system security without necessitating a convoluted key management protocol. [30]. All the mentioned layers and their security attacks and threats are summarized in Figure 2.

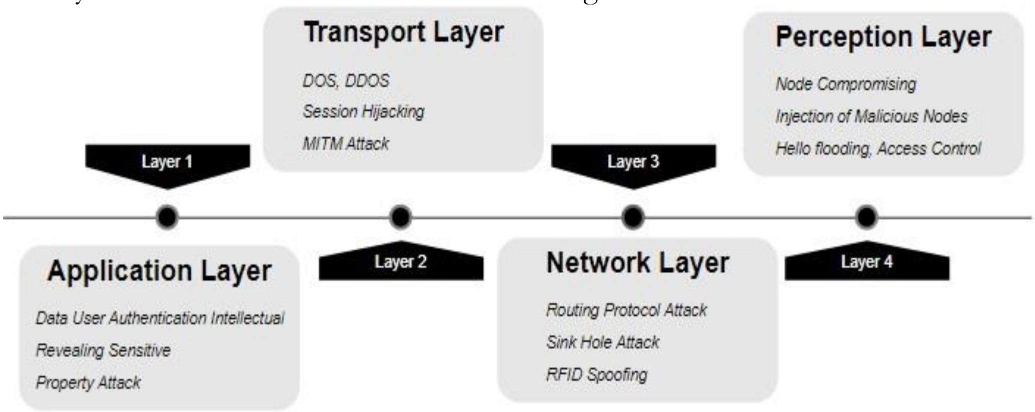

Figure 2. Targeting Attacks on IoT layer3 Literature Review

This paper explores recent progress in lightweight cryptographic primitives applied on platforms with limited resources. These primitives present unique benefits in contrast to traditional cryptographic standards. The adoption of specific new technologies in such environments is motivated by two primary factors. Firstly, the efficiency of lightweight symmetric key algorithms enables the achievement of end-to-end communication security while minimizing energy consumption. Additionally, lightweight algorithms have smaller footprints compared to classical cryptographic ones, enabling low-resource devices to establish more network connections. [31]. Lightweight cryptographic algorithms are categorized into two groups which are symmetric and asymmetric ciphers, as outlined here in Fig. 3.

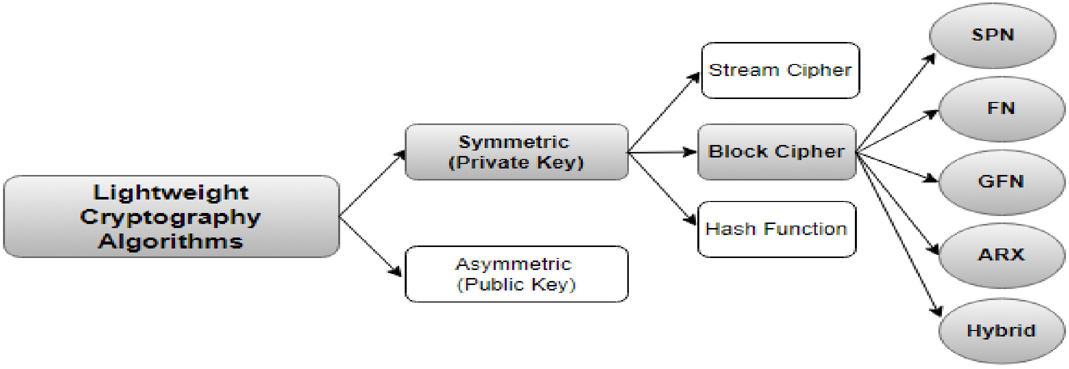

Figure 3. Lightweight Cryptographic Algorithm Structure & Classification

Symmetric Lightweight algorithms for IoT utilize a single key for both encrypting and decrypting data, ensuring a balance between security and efficiency. While symmetric key encryption is known for its speed and reliability, it lacks inherent authentication measures, making it vulnerable if the key is compromised. Symmetric ciphers encompass block, stream, and hash functions [32].

In recent years, numerous techniques have been introduced and adopted in lightweight block ciphers to optimize performance for low-resource smart devices like the Advanced Encryption Standard (AES-128) [33], built on a structure called a Substitution Permutation Network (SPN). It operates with block lengths of 128 bits and accommodates various key sizes.

128 bits with 10 rounds Next is, DESL [34]. The cipher is essentially a streamlined version of the classical DES, aiming to boost its efficiency. In the DESL round function, instead of employing eight separate S-boxes, it operates with a single one, thereby reducing the complexity of hardware gates. The findings in [35] indicate that when compared to DES, DESX, DESXL, and AES, DESL demonstrates superior suitability for RFID tags, boasting the lowest gate equivalence at 35%. PRESENT [36] follows the SPN structure and employs either an 80-bit or 128-bit key, comprising 31 rounds, and operates on blocks of 64 bits. It stands as one of the earliest ultra-lightweight block ciphers crafted specifically for ensuring robust security within resource-constrained hardware environments. However, its software implementation faces challenges due to the substitution layer's high cycle consumption, particularly in processing 4 bits of input and the subsequent S-box output. As a remedy, an enhanced variant known as the RECTANGLE cipher has been introduced. [37]. RECTANGLE [38] and PRESENT share similarities, with RECTANGLE being comprised of only 25 rounds, making it highly efficient for hardware and software implementations with limited resources.

CLEFIA [39], utilizing the Feistel network, operates with 128-bit block sizes and key lengths of 128, 192, and 256 bits, requiring approximately 6K gates for implementation. It claims superior hardware performance compared to other block ciphers. HIGHT [40] (High Security and Lightweight), which also utilizes the Feistel network structure, employs basic operations such as modulo 28 addition or XOR. It functions with a block size of 64 bits and a key size of 128 bits, spanning 32 rounds. CAMELLIA [41], designed for both software and hardware implementations, operates with a block size of 128 bits and keys of 256 bits. TEA [42] and XTEA utilize an ARX architecture, characterized by straightforward round structures, making them ideal for resource-limited software environments. SIMON [43] and SPECK [44], unveiled in June 2013, present encryption solutions tailored for efficient hardware and software deployments, respectively. They exhibit efficiency surpassing AES in heterogeneous network scenarios. TWINE [45], another Feistel-based algorithm, offers both hardware and software adaptability. It comes in two variants, TWINE and TWINE8, both featuring a 64-bit block size and 36 rounds. Recently and most frequently used block ciphers are summarized in Table 3.

Table 3. Summary of Recent Lightweight Cryptographic Block Ciphers

Year	Algorithm	Performance metrics	Results	Applications
[46] 2021	Speck-R, based on Speck with a key-dynamic substitution layer, reduces the number of rounds from 26 to 7.	Reduction in execution time, security testing (including statistical tests), real hardware implementation on IoT devices, and comparison with Speck.	Speck-R achieves a minimum of an 18% decrease in execution time on constrained devices, resulting in a 77% reduction compared to Speck, all while upholding a stringent level of security.	Appropriate for compact devices like IoT gadgets, where minimizing processing time and ensuring top-notch security are paramount.
[47] 2021	Ten lightweight block ciphers. AES, PRESENT, LBlock, Skipjack, SIMON, XTEA, PRINCE, Piccolo, HIGHT, RECTANGLE.	Memory consumption (RAM and ROM), power usage, data transfer rate, and processing duration for both encryption and decryption methods.	Evaluation of performance metrics for each algorithm, providing insights into their suitability for IoT applications.	IoT network development. Secure data transmission over cloud networks
[48] 2021	Compression algorithm (not specified), lightweight cryptography based on the Vernam cipher principle.	Bandwidth utilization, transmission security, and system resource usage.	Achieved reduction in data transmission volume. Enhanced bandwidth efficiency. Improved transmission security with lightweight cryptography.	IoT communication systems where bandwidth and transmission security are critical. Situations where maximizing existing infrastructure is essential.
2021 [49]	Shadow cipher, a combination of generalized Feistel structure and ARX operations, is designed to improve diffusion speed.	Avalanche effect, FPGA implementation, ASIC implementation, security analysis.	Shadow cipher demonstrates compactness in IoT nodes and high security against cryptanalysis.	Suitable for securing data transmission in IoT networks. Potential application in other contexts where efficient and secure encryption is required.
2021 [50]	Not specified	Not applicable (as the paper focuses on security threats, requirements, challenges, and existing solutions rather than specific algorithms or performance metrics).	Identification and discussion of security threats, requirements, challenges, and existing solutions in IoT security.	Provides insights for developing and implementing secure IoT systems. Useful for researchers, developers, and practitioners in the field of IoT security.
2021 [51]	Enhanced Energy Efficient Lightweight Cryptography Method utilizing 8-bit manipulation principle (E3LCM).	Power consumption, RAM usage, and comparison with other methods.	The method under consideration utilizes 202 milliwatts of power and requires 0.9 kilobytes of RAM. It surpasses alternative approaches in terms of hardware intricacy.	Ensuring the safe transfer of large data volumes in IoT contexts is viable for devices with limited resources like IoT devices.

2023 [52]	Shadow cipher, a combination of generalized Feistel structure and ARX operations, designed to improve diffusion speed.	Avalanche effect, FPGA implementation, ASIC implementation, security analysis.	The Shadow cipher showcases efficiency in IoT nodes and strong resistance against cryptanalysis.	Suitable for securing data transmission in IoT networks. Potential application in other contexts where efficient and secure encryption is required.
2023 [53]	Lightweight symmetric ciphers	Speed, cost, energy efficiency, latency	Evaluation of various encryption techniques across varying block and key sizes, comparing their operational efficiency on Arduino and Raspberry Pi platforms, while also examining the performance of second-round NIST candidates in terms of latency and energy consumption efficiency.	Fields such as IoT networks, cyber-physical systems, distributed control systems, vehicular systems, wireless sensor networks, telemedicine, smart grid, and similar domains rely on devices with limited resources, necessitating secure communication.
2023 [54]	Lightweight block ciphers, stream ciphers, hybrid ciphers, and other cryptographic algorithms are used in IoT security.	Performance, robustness, computational complexity of cryptographic algorithms.	Comparative analysis of cryptographic algorithms in terms of performance, robustness, and computational complexity. Discussion of IoT security challenges, threats, attacks, and mitigation techniques.	Guidance for implementing secure IoT systems. Awareness of IoT security challenges and mitigation strategies.
[32] 2023	Lightweight cryptography algorithms	Cost of implementation, hardware and software capabilities and resistance to attacks are among the properties to consider.	Comparative analysis of existing lightweight cryptography algorithms, identification of strengths and weaknesses in terms of security and performance, discussion on potential research directions for optimizing cost, performance, and security balance.	Ensuring the protection of IoT devices with limited resources, like RFID tags, sensors, and smart cards, across diverse sectors such as healthcare, industrial automation, smart cities, agriculture, etc.

Comparative Study of Recent Lightweight Cryptographic Block Cipher.

In recent years, the field of lightweight cryptographic block ciphers has seen significant advancements, driven by the demand for efficient and secure encryption solutions in resource-constrained environments such as IoT devices and embedded systems. These lightweight ciphers prioritize minimal hardware and software requirements while maintaining a high level of security against various attacks. In this comparative study, we analyze some of the most recent lightweight cryptographic block ciphers, considering their merits, demerits, targeted attacks, and performance in terms of power consumption and throughput. This examination aims to provide insights into the strengths and weaknesses of these algorithms, aiding in the selection of appropriate cryptographic solutions for specific application scenarios. The comparative table of lightweight cryptographic block ciphers and their evaluation metrics are discussed in Tab. 3.

Discussion on Lightweight Cryptographic Block Cipher Algorithms.

In assessing the "best" algorithm among the options listed, several key factors come into play, including security strength, efficiency, resilience to attacks, and adaptability. Algorithms such as PRESENT-256, SHADOW, and SPECK-R stand out for their robust security guarantees, offering protection against a wide array of potential attacks, including differential and algebraic cryptanalysis. Conversely, algorithms like TED, T-Twine, and 3D-RECTANGLE excel in competence and performance, possessing low overhead and high throughput, making them suited for resource-constrained environments. Temporarily, LRBC, UBRIGHT, and IVLBC highlight resilience against side-channel attacks, crucial for safeguarding IoT devices and vulnerable systems. Finally, ACT and LAO-3D exhibit compliance and scalability, with lightweight designs and low resource consumption, theoretically suitable for a varied range of applications. Eventually, the determination of the "best" algorithm centers on the specific requirements of the anticipated use case, evaluating factors such as security needs, resource constraints, and performance considerations.

Conclusion.

The IoT has been rapidly integrating into our modern existence, seeking to increase our daily practices by connecting numerous smart devices, technologies, and applications. Its goal is to usher in a scope of full automation in our environment. Despite significant research already conducted on the IoT, there remains a vast frontier yet to be investigated. The increasing attention from industries and governments has ignited extensive research efforts, returning numerous successful projects. Safeguarding IoT devices while ensuring they meet resource constraints is a serious and challenging task. Including many block ciphers available, selecting the absolute ones for specific applications presents a significant design challenge. This paper offers a detailed examination and evaluation of various lightweight block ciphers, considering discrete design principles. Certain attributes of IoT, such as the broader architecture, security, and privacy concerns, have garnered significant spotlight, while factors like the availability, reliability, and performance of smart devices require further investigation.

Table 4. Comparative Analysis of Recent Lightweight Block Ciphers [23]

	Block Cipher Features								**Performance Metrics**	
Proposed	**Structure**	**Key size**	**Block size**	**Rounds**	**Cipher**	**Merit**	**Demerit**	**Targeted Attacks**	**Power Consumption**	**Throughput**
ACT (2020) [55]	SPN	80	64	31	Block	Lightweight, Efficient	Susceptible to Linear Cryptanalysis	Differential Cryptanalysis	Moderate	High
ILEA [56]	SPN	128	64	12	Block	Simple Design, Low Resource Consumption	Vulnerable to Differential Cryptanalysis	Algebraic Attacks	Low	Moderate
Improved Simeck [57]	FN	64/128	32/64	32/44	Block	Improved Security	Limited Key Length	Algebraic Cryptanalysis	Low	High
LRBC (2020) [52]	HYBRID	16	16	24	Block	Resilient to Side-Channel Attacks	May not Scale Well with Larger Key Sizes	Power Analysis Attacks	Moderate	Moderate
LWE (2020) [58]	HYBRID	64	64	3	Block	Security Based on Hard Mathematical Problem	Computationally Intensive Key Generation	Lattice-Based Attacks	High	Low
TED (2020) [59]	FN	128	64	26	Block	Lightweight, Low Overhead	Vulnerable to Differential Cryptanalysis	Statistical Attacks	Low	High
T-Twine (2020) [60]	GFN	80/128	64	36	Block	High-Security Margin	Limited Analysis in Practice	Differential Cryptanalysis	Moderate	Moderate
UPRIGHT (2020) [61]	GFN	80	32	22	Block	Robustness Against Side-Channel Attacks	Limited Cryptanalysis Efforts	Power Analysis Attacks	Moderate	Moderate
3D-RECTANGLE [62]	SPN	128	64	25	Block	Efficient in Hardware Implementations	Vulnerable to Linear Cryptanalysis	Differential Cryptanalysis	High	Moderate
LBC-IOT [63]	FN	80	32	32	Block	Designed for IoT Devices	Vulnerable to Known Attacks	Side-Channel Attacks	Low	High

LAO-3D [64]	SPN	128	64	20	Block	Lightweight, Low Resource Consumption	Limited Analysis Efforts	Differential Cryptanalysis	Moderate	High
SHADOW [49]	GFN	64/128	32/64	16/32	Block	High-Security Margin	Limited Cryptanalysis Efforts	Algebraic Cryptanalysis	High	Low
IVLBC [65]	SPN	80/128	64	29	Block	Efficient Implementation	Limited Analysis Efforts	Side-Channel Attacks	Moderate	High
SPECK-R [46]	FN	80	64	30 or min	Block	High Performance in Resource-Constrained Devices	Reduced Security Margin	Differential Cryptanalysis	High	High
PRESENT-256 [66]	SP	128	64	64	Block	Strong Security Guarantees	Increased Computational Complexity	Differential Cryptanalysis	High	Low
SCENERY [67]	FN	80	64	28	Block	Lightweight, Low Resource Consumption	Vulnerable to Differential Cryptanalysis	Statistical Attacks	Low	Moderate
SLIM [68]	FN	80	32	21	Block	Efficient for Low-Resource Environments	Vulnerable to Known Attacks	Differential Cryptanalysis	Low	High
IIOTBC [69]	SPN	128	64	10	Block	Optimized for IoT environments	Limited security analysis	Brute Force, Side-Channel Attacks	Low	Moderate

References.

[1] A. Hameed and A. Alomary, "Security issues in IoT: A survey," *2019 Int. Conf. Innov. Intell. Informatics, Comput. Technol. 3ICT 2019*, Sep. 2019, doi: 10.1109/3ICT.2019.8910320.

[2] J. Lee, J. Kim, and J. Seo, "Cyber attack scenarios on smart city and their ripple effects," *2019 Int. Conf. Platf. Technol. Serv. PlatCon 2019 - Proc.*, Mar. 2019, doi: 10.1109/PLATCON.2019.8669431.

[3] and T. A. K. Demestichas, N. Peppes, "Survey on security threats in agricultural IoT and smart farmingSurvey on security threats in agricultural IoT and smart farming," *Sensors*, vol. 20, no. 22, p. 6458, 2020, doi: https://doi.org/10.3390/s20226458.

[4] M. K. and S. Moriai, "Lightweight cryptography for the internet of things," *Proc. Futur. Technol. Conf.*, vol. 3, pp. 780–795, 2020, doi: https://doi.org/10.1007/978-3-030-63092-8_52.

[5] and Y. Y. L. Cui, G. Xie, Y. Qu, L. Gao, "Security and Privacy in Smart Cities: Challenges and Opportunities," *IEEE Access*, vol. 6, pp. 46134–46145, 2018, doi: 10.1109/ACCESS.2018.2853985.

[6] M. Dr. Molly M. Jahn, William L. Oemichen, Dr. Gregory F. Treverton, Scott L. David, B. B. A. Rose, Max A. Brosig, Dr. Buddhika "Jay" Jayamaha, William K. Hutchison, and Rimestad, "Cyber Risk and Security Implications in Smart Agriculture and Food Systems," *White Pap. Jahn Res. Group, Univ. Wisconsin–Madison, Coll. Agric. Life Sci.*, pp. 1–20, 2019, [Online]. Available: https://jahnresearchgroup.webhosting.cals.wisc.edu/wp-content/uploads/sites/223/2019/01/Agricultural-Cyber-Risk-and-Security.pdf

[7] J. Laufs, H. Borrion, and B. Bradford, "Security and the smart city: A systematic review," *Sustain. Cities Soc.*, vol. 55, p. 102023, 2020, doi: https://doi.org/10.1016/j.scs.2020.102023.

[8] and J. M. A. Gissinga, M. Timmsa, S. Browninga, R. Cromptona, "Compound natural disasters in Australia: a historical analysis," *Environ. Hazards*, pp. 159–173, 2021, doi: https://doi.org/10.1080/17477891.2021.1932405.

[9] T. Bhattasali, "Licrypt: Lightweight cryptography technique for securing smart objects in internet of things environment," *CSI Commun.*, pp. 26–36, 2013.

[10] S. K. and S. M. M. Gupta, M. Abdelsalam, "Security and Privacy in Smart Farming: Challenges and Opportunities," *IEEE Access*, vol. 8, pp. 34564–34584, 2020, doi: 10.1109/ACCESS.2020.2975142.

[11] E. R. Naru, H. Saini, and M. Sharma, "A recent review on lightweight cryptography in IoT," *Proc. Int. Conf. IoT Soc. Mobile, Anal. Cloud, I-SMAC 2017*, pp. 887–890, Oct. 2017, doi: 10.1109/I-SMAC.2017.8058307.

[12] S. S. Dhanda, B. Singh, and P. Jindal, "Lightweight Cryptography: A Solution to Secure IoT," *Wirel. Pers. Commun.*, vol. 112, no. 3, pp. 1947–1980, Jun. 2020, doi: 10.1007/S11277-020-07134-3/METRICS.

[13] V. Rao and K. V. Prema, "Comparative Study of Lightweight Hashing Functions for Resource Constrained Devices of IoT," *CSITSS 2019 - 2019 4th Int. Conf. Comput. Syst. Inf. Technol. Sustain. Solut. Proc.*, Dec. 2019, doi: 10.1109/CSITSS47250.2019.9031038.

[14] and F. A. F. A. Alabaa, M. Othmana, I. A. T. Hashema, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, 2017, doi: 10.1016/j.jnca.2017.04.002.

[15] and K. K. V. Varadharajan, U. Tupakula, "Study of Security Attacks Against IoT Infrastructures," *Tech. Rep. TR1 ISIF ASIA Funded Proj.*, pp. 1–36, 2018, [Online]. Available: https://www.newcastle.edu.au/__data/assets/pdf_file/0020/552017/TR1-ISIF-ASIA.pdf

[16] M. Mahbub, "Progressive researches on IoT security: An exhaustive analysis from the

perspective of protocols, vulnerabilities, and preemptive architectonics," *J. Netw. Comput. Appl.*, vol. 168, p. 102761, 2020, doi: https://doi.org/10.1016/j.jnca.2020.102761.

[17] S. N. Swamy, D. Jadhav, and N. Kulkarni, "Security threats in the application layer in IOT applications," *Proc. Int. Conf. IoT Soc. Mobile, Anal. Cloud, I-SMAC 2017*, pp. 477–480, Oct. 2017, doi: 10.1109/I-SMAC.2017.8058395.

[18] A. Aggarwal, W. Asif, H. Azam, M. Markovic, M. Rajarajan, and P. Edwards, "User Privacy Risk Analysis for the Internet of Things," *2019 6th Int. Conf. Internet Things Syst. Manag. Secur. IOTSMS 2019*, pp. 259–264, Oct. 2019, doi: 10.1109/IOTSMS48152.2019.8939265.

[19] M. A. Imran Makhdoom and W. N. Abbas, Haider, "Blockchain's adoption in IoT: The challenges, and a way forward," *J. Netw. Comput. Appl.*, vol. 125, pp. 251–279, 2019, doi: https://doi.org/10.1016/j.jnca.2018.10.019.

[20] B. C. Chifor, I. Bica, and V. V. Patriciu, "Mitigating DoS attacks in publish-subscribe IoT networks," *Proc. 9th Int. Conf. Electron. Comput. Artif. Intell. ECAI 2017*, vol. 2017-January, pp. 1–6, Dec. 2017, doi: 10.1109/ECAI.2017.8166463.

[21] M. Saadeh, A. Sleit, K. E. Sabri, and W. Almobaideen, "Hierarchical architecture and protocol for mobile object authentication in the context of IoT smart cities," *J. Netw. Comput. Appl.*, vol. 121, pp. 1–19, 2018, doi: https://doi.org/10.1016/j.jnca.2018.07.009.

[22] H. P. Alahari and S. B. Yelavarthi, "Performance Analysis of Denial of Service DoS and Distributed DoS Attack of Application and Network Layer of IoT," *Proc. 3rd Int. Conf. Inven. Syst. Control. ICISC 2019*, pp. 72–81, Jan. 2019, doi: 10.1109/ICISC44355.2019.9036403.

[23] F. A. Bakhtiar, E. S. Pramukantoro, and H. Nihri, "A lightweight IDS based on j48 algorithm for detecting DoS attacks on IoT middleware," *2019 IEEE 1st Glob. Conf. Life Sci. Technol. LifeTech 2019*, pp. 41–42, Mar. 2019, doi: 10.1109/LIFETECH.2019.8884057.

[24] I. G.-M. and J. L. M. M. Nasralla, "Defenses Against Perception-Layer Attacks on IoT Smart Furniture for Impaired People," *IEEE Access*, vol. 8, pp. 119795–119805, 2020, doi: 10.1109/ACCESS.2020.3004814.

[25] Y. M. Tukur and Y. S. Ali, "Demonstrating the Effect of Insider Attacks on Perception Layer of Internet of Things (IoT) Systems," *2019 15th Int. Conf. Electron. Comput. Comput. ICECCO 2019*, Dec. 2019, doi: 10.1109/ICECCO48375.2019.9043248.

[26] R. Kanagavelu and K. M. M. Aung, "A Survey on SDN Based Security in Internet of Things," *Adv. Intell. Syst. Comput.*, vol. 887, pp. 563–577, 2019, doi: 10.1007/978-3-030-03405-4_39.

[27] A. K. Mishra, A. K. Tripathy, D. Puthal, and L. T. Yang, "Analytical Model for Sybil Attack Phases in Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 379–387, Feb. 2019, doi: 10.1109/JIOT.2018.2843769.

[28] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017, doi: 10.1109/JIOT.2017.2694844.

[29] R. Yugha and S. Chithra, "A survey on technologies and security protocols: Reference for future generation IoT," *J. Netw. Comput. Appl.*, vol. 169, p. 102763, 2020, doi: https://doi.org/10.1016/j.jnca.2020.102763.

[30] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wirel. Networks*, vol. 20, no. 8, pp. 2481–2501, Oct. 2014, doi: 10.1007/S11276-014-0761-7.

[31] and N. M. K. McKay, L. Bassham, M. Snmez Turan, "Report on Lightweight

Cryptography," *NISTIR*, pp. 1–27, 2016, doi: https://doi.org/10.6028/NIST.IR.8114.

[32] M. A. R. and M. R. A. K. V. A. Thakor, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," *IEEE Access*, vol. 9, pp. 28177–28193, 2021, doi: 10.1109/ACCESS.2021.3052867.

[33] and M. I. H. A. Khattak, M. A. Shah, S. Khan, I. Ali, "Perception layer security in Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 100, pp. 144–164, 2019, doi: https://doi.org/10.1016/j.future.2019.04.038.

[34] and K. S. G. Leander, C. Paar, A. Poschmann, "New Lightweight DES Variants," *Springer, Berlin, Heidelb.*, pp. 196–210, 2007, doi: https://doi.org/10.1007/978-3-540-74619-5_13.

[35] A. Shah and M. Engineer, "A Survey of Lightweight Cryptographic Algorithms for IoT-Based Applications," *Adv. Intell. Syst. Comput.*, vol. 851, pp. 283–293, 2019, doi: 10.1007/978-981-13-2414-7_27.

[36] A. Bogdanov *et al.*, "PRESENT: An ultra-lightweight block cipher," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 4727 LNCS, pp. 450–466, 2007, doi: 10.1007/978-3-540-74735-2_31.

[37] I. Bhardwaj, A. Kumar, and M. Bansal, "A review on lightweight cryptography algorithms for data security and authentication in IoTs," *4th IEEE Int. Conf. Signal Process. Comput. Control. ISPCC 2017*, vol. 2017-January, pp. 504–509, Sep. 2017, doi: 10.1109/ISPCC.2017.8269731.

[38] W. Zhang, Z. Bao, D. Lin, V. Rijmen, B. Yang, and I. Verbauwhede, "RECTANGLE: A bit-slice lightweight block cipher suitable for multiple platforms," *Sci. China Inf. Sci.*, vol. 58, no. 12, pp. 1–15, Dec. 2015, doi: 10.1007/S11432-015-5459-7/METRICS.

[39] T. A. and H. Hiwatari, "Very compact Hardware Implementations of the Block cipher CLEFIA," *Sel. Areas Cryptogr. Lect. Notes Comput. Sci. Springer*, pp. 278–292, 2012, doi: https://doi.org/10.1007/978-3-642-28496-0_17.

[40] D. Hong, "HIGHT: A New Block Cipher Suitable for Low Resource Device," *Cryptogr. Hardw. Embed. Syst. CHES 2006 Lect. Notes Comput. Sci. Springer*, pp. 46–59, 2006, doi: https://doi.org/10.1007/11894063_4.

[41] A. S. and S. Morioka, "Hardware-Focused Performance Comparison for the Standard Block Ciphers AES, Camellia, and Triple-DES," *Lect. Notes Comput. Sci. Inf. Secur. Springer*, pp. 252–266, 2003, doi: https://doi.org/10.1007/10958513_20.

[42] D. J. W. & R. M. Needham, "TEA, a tiny encryption algorithm," *Proceeding Int. Work. Fast Softw. Encryption", Springer, Berlin*, pp. 363–366, 1995, doi: https://doi.org/10.1007/3-540-60590-8_29.

[43] R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith, and L. Wingers, "The SIMON and SPECK lightweight block cIPhers," *Proc. - Des. Autom. Conf.*, vol. 2015-July, Jul. 2015, doi: 10.1145/2744769.2747946.

[44] A. V. Duka and B. Genge, "Implementation of SIMON and SPECK lightweight block ciphers on programmable logic controllers," *2017 5th Int. Symp. Digit. Forensic Secur. ISDFS 2017*, May 2017, doi: 10.1109/ISDFS.2017.7916501.

[45] and E. K. T. Suzaki, K. Minematsu, S. Morioka, "TWINE: A Lightweight Block Cipher for Multiple Platforms," *Springer*, pp. 339–354, 2012, doi: https://doi.org/10.1007/978-3-642-35999-6_22.

[46] L. Sleem and R. Couturier, "Speck-R: An ultra light-weight cryptographic scheme for Internet of Things," *Multimed. Tools Appl.*, vol. 80, no. 11, pp. 17067–17102, May 2021, doi: 10.1007/S11042-020-09625-8/METRICS.

[47] P. Panahi, C. Bayılmış, U. Çavuşoğlu, and S. Kaçar, "Performance Evaluation of Lightweight Encryption Algorithms for IoT-Based Applications," *Arab. J. Sci. Eng.*, vol.

46, no. 4, pp. 4015–4037, Apr. 2021, doi: 10.1007/S13369-021-05358-4/METRICS.

[48] and Ľ. C. I. Sokol, P. Hubinský, "Lightweight Cryptography for the Encryption of Data Communication of IoT Devices," *Electron.*, vol. 10, no. 21, p. 2567, 2021, doi: https://doi.org/10.3390/electronics10212567.

[49] Y. Guo, L. Li, and B. Liu, "Shadow: A Lightweight Block Cipher for IoT Nodes," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 13014–13023, Aug. 2021, doi: 10.1109/JIOT.2021.3064203.

[50] and V. V. L. M. Shamala, G. Zayaraz, K. Vivekanandan, "Lightweight cryptography algorithms for internet of things enabled networks: An overview," *J. Phys. Conf. Ser.*, vol. 1717, no. 1, p. 012072, 2021, doi: 10.1088/1742-6596/1717/1/012072.

[51] and M. S. S. P. Prakasam, M. Madheswaran, K. P. Sujith, "An Enhanced Energy Efficient Lightweight Cryptography Method for various IoT devices," *ICT Express*, vol. 7, no. 4, pp. 487–492, 2021, doi: https://doi.org/10.1016/j.icte.2021.03.007.

[52] A. Biswas, A. Majumdar, S. Nath, A. Dutta, and K. L. Baishnab, "LRBC: a lightweight block cipher design for resource constrained IoT devices," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 5, pp. 5773–5787, May 2023, doi: 10.1007/S12652-020-01694-9/METRICS.

[53] and A. F. M. El-Hajj, H. Mousawi, "Analysis of lightweight cryptographic algorithms on iot hardware platform," *Futur. Internet*, vol. 15, no. 2, p. 54, 2023, doi: https://doi.org/10.3390/fi15020054.

[54] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, and H. A. Alkhzaimi, "Cryptography Algorithms for Enhancing IoT Security," *Internet of Things (Netherlands)*, vol. 22, Jul. 2023, doi: 10.1016/j.iot.2023.100759.

[55] K. B. Jithendra and T. Kassim Shahana, "ACT: An ultra-light weight block cipher for internet of things," *Int. J. Comput. Digit. Syst.*, vol. 9, no. 5, pp. 921–929, 2020.

[56] P. Jha, H. Y. Zorkta, D. Allawi, and M. R. Al-Nakkar, "Improved lightweight encryption Algorithm (ILEA)," *2020 Int. Conf. Emerg. Technol. INCET 2020*, Jun. 2020, doi: 10.1109/INCET49848.2020.9154170.

[57] and A. A. H. P. C. Encarnacion, B. D. Gerardo, "Modified round function of SIMECK 32/64 block cipher," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 1–3, pp. 1–9, 2020, doi: https://doi.org/10.30534/ijatcse/2020/3991.32020.

[58] and A. H. Z. S. Toprak, A. Akbulut, M. A. Aydın, "LWE: An energy-efficient lightweight encryption algorithm for medical sensors and IoT devices," *Istanbul Univ. - J. Electr. Electron. Eng.*, vol. 20, no. 1, pp. 71–80, 2020, doi: 10.5152/electrica.2020.19082.

[59] and B. J. C. Thorat, V. Inamdar, "TED: A LIGHTWEIGHT BLOCK CIPHER FOR IoT DEVICES WITH SIDE-CHANNEL ATTACK RESISTANCE," *Int. J. Inf. Technol. Secur.*, vol. 12, no. 2, p. 83, 2020, [Online]. Available: https://openurl.ebsco.com/EPDB%3Agcd%3A9%3A1547961/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A143815102&crl=c&link_origin=www.google.com

[60] K. Sakamoto *et al.*, "Tweakable TWINE: Building a Tweakable Block Cipher on Generalized Feistel Structure," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. E103.A, no. 12, pp. 1629–1639, Dec. 2020, doi: 10.1587/TRANSFUN.2019EAP1141.

[61] D. Sehrawat and N. Gill, "Ultra BRIGHT: a tiny and fast ultra lightweight block cipher for IoT," *Int. J. Sci. Technol. Res.*, vol. 9, p. 1063, 2020.

[62] N. H. Z. and M. D. A. A. Zakaria, A. H. Azni, F. Ridzuan, "Extended RECTANGLE Algorithm Using 3D Bit Rotation to Propose a New Lightweight Block Cipher for IoT," *IEEE Access*, vol. 8, pp. 198646–198658, 2020, doi: 10.1109/ACCESS.2020.3035375.

[63] and M. E. R. A. Ramadan, B. W. Aboshosha, K. Yadav, I. M. Alseadoon, M. J.

Kashout, “LBC-IoT: Lightweight Block Cipher for IoT Constraint Devices,” *Comput. Mater. Contin.*, vol. 67, no. 3, pp. 3563–3579, 2021, doi: https://doi.org/10.32604/cmc.2021.015519.

[64] and M. D. A. A. Zakaria, A. H. Ab Halim, F. Ridzuan, N. H. Zakaria, “LAO-3D: A Symmetric Lightweight Block Cipher Based on 3D Permutation for Mobile Encryption Application,” *Symmetry (Basel).*, vol. 14, no. 10, p. 2042, 2022, doi: https://doi.org/10.3390/sym14102042.

[65] and J. Y. X. Huang, L. Li, “IVLBC: An involutive lightweight block cipher for Internet of Things,” *IEEE Syst. J.*, vol. 17, no. 2, pp. 3192–3203, 2023, doi: 10.1109/JSYST.2022.3227951.

[66] R. B. and N. Parvatham, “Light-Weight Present Block Cipher Model for IoT Security on FPGA,” *Intell. Autom. Soft Comput.*, vol. 33, no. 1, pp. 13–34, 2022, doi: https://doi.org/10.32604/iasc.2022.020681.

[67] J. Feng and L. Li, “SCENERY: a lightweight block cipher based on Feistel structure,” *Front. Comput. Sci.*, vol. 16, no. 3, pp. 1–10, Jun. 2022, doi: 10.1007/S11704-020-0115-9/METRICS.

[68] A. E.-S. and M. M. D. B. Aboushosha, R. A. Ramadan, A. D. Dwivedi, “SLIM: A Lightweight Block Cipher for Internet of Health Things,” *IEEE Access*, vol. 8, pp. 203747–203757, 2020, doi: 10.1109/ACCESS.2020.3036589.

[69] L. L. Juanli Kuang, Ying Guo, “IIoTBC: A Lightweight Block Cipher for Industrial IoT Security,” *KSII Trans. Internet Inf. Syst.*, vol. 17, no. 1, 2023, doi: 10.3837/tiis.2023.01.006.