Journal of Applied Engineering and Technological Science
Vol 5(2) 2024: 860-874

LIGHTWEIGHT BLOCK AND STREAM CIPHER ALGORITHM: A REVIEW

Suaad Ali Abead[1*], Nada Hussein M. Ali[2]
Department of Computer Science, College of Science for Women, University of Baghdad, Baghdad, Iraq[1]
Department of Computer Science, College of Science, University of Baghdad, Iraq[2]
suad.ali2201m@sc.uobaghdad.edu.iq[1], nada.husn@sc.uobaghdad.edu.iq[2]

Received : 24 December 2023, Revised: 18 March 2024, Accepted : 23 March 2024
**Corresponding Author*

ABSTRACT
Most of the Internet of Things (IoT), cell phones, and Radio Frequency Identification (RFID) applications need high speed in the execution and processing of data. this is done by reducing, system energy consumption, latency, throughput, and processing time. Thus, it will affect against security of such devices and may be attacked by malicious programs. Lightweight cryptographic algorithms are one of the most ideal methods Securing these IoT applications. Cryptography obfuscates and removes the ability to capture all key information patterns ensures that all data transfers occur Safe, accurate, verified, legal and undeniable. Fortunately, various lightweight encryption algorithms could be used to increase defense against various attacks to preserve the privacy and integrity of such applications. In this study, an overview of lightweight encryption algorithms, and methods, in addition, a modern technique for these algorithms also will be discussed. Besides, a survey for the algorithm that would use minimal power, require less time, and provide acceptable security to low-end IoT devices also introduced, Evaluating the results includes an evaluation of the algorithms reviewed and what was concluded from them. Through the review, we concluded that the best algorithms depend on the type of application used. For example, Lightweight block ciphers are one of the advanced ways to get around security flaws.
Keywords : *IoT security, Lightweight encryption, Block cipher, Stream cipher, Privacy, Integrity, MAC.*

1. Introduction

In recent years, the quick development of communications, wireless network technology, and computer science has led to the appearance of the new area of the Internet of Things (IoT). The IoT refers to the idea of communication between billions of physical objects that are linked to the global internet through smart devices from any location. Translating data between these devices needs robust security from any attack (Abed & Younis, 2019) (Melki et al., 2020) (Al-Alawy et al., 2018). To provide protection to IoT systems, such as confidentiality, authentication and integrity the solution is to usage a suitable cryptographical algorithm.

Cryptographic systems are used to provide security services, to keep data protected from unauthorized uses, which are classified into symmetric and asymmetric types (Fadhil et al., 2021) (Hameed et al., 2018) (George et al., 2020). In symmetric systems, the sender and receiver use identical keys in the cipher operation (Hussein Ali & Ali Abead, 2016). Two keys are used in asymmetric key cryptography, also known as public key cryptography, to encrypt and decode data.

Cryptographic algorithms are categorized into ciphers of the block and ciphers of the stream. In block ciphers, a bit block is encoded, while in stream ciphers, data are coded bit by bit by using a secure key generator (Taha & Al-Tuwaijari, 2021). Cryptosystems possess the following characteristics: confidentiality, integrity, and availability (Abdulameer et al., 2020). Cryptographic systems are intricate and require substantial computing resources, rendering them unsuitable for devices with limited resources in the IoT environment. The restrictions within IoT devices have created a demand for lightweight cryptography (LWC) to handle this problem.

Lightweight cryptography is a type of cryptography that focuses on finding solutions for applications with high growth and frequent use of energy-efficient smart devices such as IoT devices, smart cards, and RFID tags require the use of lightweight cryptographic algorithms. A significant concern in lightweight cryptography is attaining an equilibrium among security, effectiveness, and cost, striking a balance between them is one of the key challenges (Kapalova et al., 2023).The evaluation of the performance of lightweight cryptography encompasses several parameters, including latency, system energy consumption, throughput, and wait time (Kousalya & Sathish Kumar, 2019). The lightweight coding trade-offs implementation speed, cost, performance, security and energy consumption on resource-limited devices. Its aims to develop security solutions that can operate on devices with limited resources by consuming less memory, computing power, and memory. In comparison to traditional cryptography, lightweight cryptography is anticipated to be easier to use and quicker. Less security is a drawback of lightweight cryptography (Buchanan et al.,2017)

The goal of lightweight cryptography is to reduce the total cost of implementation for both hardware and software related to cryptographic building blocks, considering factors like the cycle rates, key size, number of rounds and power consumption, Gate Equivalence and throughput (Chiadighikaobi & Katuk, 2021) (Nayancy et al., 2022).

Various lightweight cryptographic methods exhibit diverse network architectures, such as Substitution-Permutation Networks, Feistel Networks, and Lai-Massey. These algorithms include block ciphers, stream ciphers, and certain hash functions, as seen in Fig.1. Numerous applications have used lightweight cryptographic methods to guarantee integrity, availability, privacy, and security (Sevin & Mohammed, 2023).

This study offers a thorough overview of the utilization of lightweight symmetric ciphers, such as lightweight blocks and stream ciphers. The main contributions of this paper are:

1- Providing review previous works that have developed algorithms to be suitable for use in applications that need to have a balance between speed and high security.
2- The most important limitations for some of the algorithms that have been developed have suffered from have also been touched upon,
3- In addition, making some comparisons between the reviewed works for metrics cited in the literature like power consumption, memory usages, throughput, execution time.
4- This research will help the researchers to choose the right lightweight algorithm for any application.

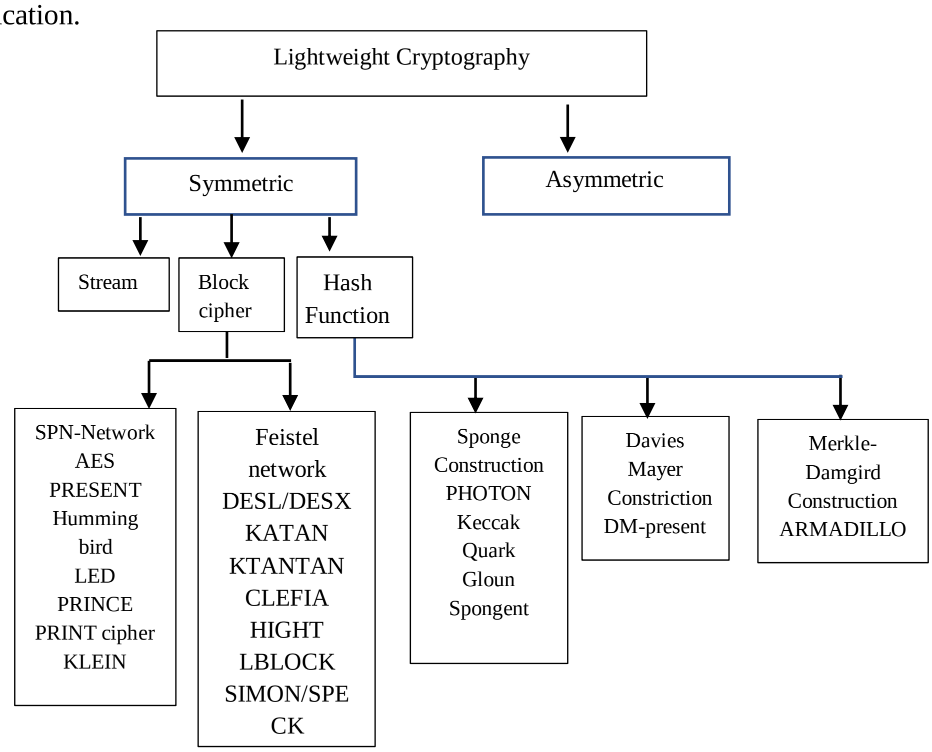

Fig. 1. Lightweight Cryptography Algorithms (Singh et al., 2017).

2. Lightweight cryptography Applications

There are many examples of IoT's ; which is considered a resource-constrained; usefulness in modern society's many spheres as Health care and Radio Frequency Identification(RFID) (Panahi et al., 2021). The utility control center may access and manage this technology remotely, reducing the need for manual labor (Hasan & Kadhim, 2022). It is important to safeguard these devices and information must be sent carefully in a secure manner. Hence, Lightweight cryptography methods are considered suitable for it (Panahi et al., 2021). Table 1 explains the most common lightweight application types and table 2 shows comparisons between diverse lightweight algorithms.

Table 1 - The most common lightweight applications

Ref	Application	Summary	Limitation
(Xiao-Mei & Yong, 2019)	Radio Frequency Identification and Motes	The Piccolo cipher algorithm is an occasion for RFID tags.	Serialization is an important measure of achieving lightweight
(Singh et al., 2020)	IoT Devices and Smartcards	The suggested architectures provide security with high throughput and energy-efficient architectures	Throughput complexity
(Fotovvat et al., 2021)	Industrial Sensors and Devices	A promising answer to reduce the complexity of calculations while still maintaining degree of protection for IOT	encryption time of LWC algorithms is insignificant compared to read time and transmission time.
(Hussein et al., 2022)	Wireless Sensors Networks	Improving WSN system performance by increasing network throughput	network throughput is inversely related to security. when the number of keys increases, network throughput decreases.
(Yousif & Fadahl, 2021) (Zang et al., 2023)	Mobile or User Equipment	Provide a lightweight, effective model for seatbelt detection.	slight improved when the running time is greatly reduced.
(Chaudhary & Chatterjee, 2020)	Healthcare Devices	a lightweight ciphering technique has been introduced for IoT-based-healthcare system	This technique requires low computation load and less energy consumption.
(Saadatnejad et al., 2020)	Other Battery-Powered Devices like Wearable	ECG classification algorithm is proposed for continuous cardiac monitoring on wearable devices	further increase the classification performance and improvements on single-lead ECG processing.

Table (1) introduces the most common applications that rely on lightweight encryption, in addition, a table displays algorithms and approaches with their limitations.

Table 2- Comparison of different lightweight algorithms

Ref	platform	Evaluate matrices	algorithms	summary
(Xiao-Mei & Yong, 2019)	SASEBO	DPA attack serialization	LED lightweight cryptography	Serialization can achieve, the lightweight of cryptographic algorithm, also it decreases the hardness of DPA attack.
(Panahi et al., 2021)	Raspberry Pi 3 and Arduino Mega 2560 as	memory usage (RAM and ROM), energy consumption, throughput, and execution time	AES, PRESENT, LBlock, Skipjack, SIMON, XTEA, PRINCE, Piccolo,AES	Arduino Mega 2560 needs lower processing and memory compared to Raspberry Pi 3 for all block cipher mentioned.
(Jallouli et al., 2022)	Personal computer around Intel Core (TM) i5 @2.60 GHZ with 15.6 GB under Ubuntu 14.04 Trusty	Encryption time, Energy measurement, Memory usage	Two chaotic stream ciphers (CM-SC and CS-SC)	Roughly 57% fewer cycles are required for CS-SC than for CM-SC, and CS-SC uses roughly 30% less energy and memory than CM-SC (less than 8 KB and 32 KB, respectively). CM-

(Shilpa & Chinchu, 2021)	Linux operating system. area of 1000GE.	Power consumption, complexity, throughput, memory usage, execution time	GIFT, LED RECTANGLE, PRESENT, PICO	SC offers better security characteristics than the stream cipher CS-SC. Reduced resource usage, less complexity, less area, smaller footprint, shorter execution times, and lower power consumption

Table (2) discussed a comparison between a number of lightweight encryption algorithms in terms of some criteria, including execution time, energy consumption, throughput, and memory usage, and on different implementation environments, and there was a clear improvement in these algorithms. In addition, we see that some algorithms are affected by some types of attacks, as shown below:

The GIFT cipher is susceptible to the Chosen Plaintext Attack, but RECTANGLE is resistant to side channel attacks. The PRESENT cipher is vulnerable to linear cryptanalysis. GIFT offers strong resistance against both linear and differential cryptanalysis, yet it is vulnerable to linear attacks, RECTANGLE has good security-performance tradeoff resistance against Slide attack, The PICO cipher is resistant to both differential and linear attacks, LED cipher provide robust security against wholly attacks (Shilpa & Chinchu, 2021). Efficiently satisfy the Internet of Things' RFID tag chip's security requirements for cryptographic algorithms (Xiao-Mei & Yong, 2019).

3. Lightweight cryptography methods

For applications with limited resources, the lightweight cryptographic primitives created recently perform better than traditional ciphers. A few of these primitives are the stream cipher, hash function, block cipher, and message authentication code, as shown in Fig. 2. Standard algorithms are different from lightweight primitives. To summarise, the goal of lightweight cryptography is to enable designers to achieve the best possible balance between security, performance, and cost in situations with limited resources.(Singh et al., 2020) (Mileva et al., 2021).

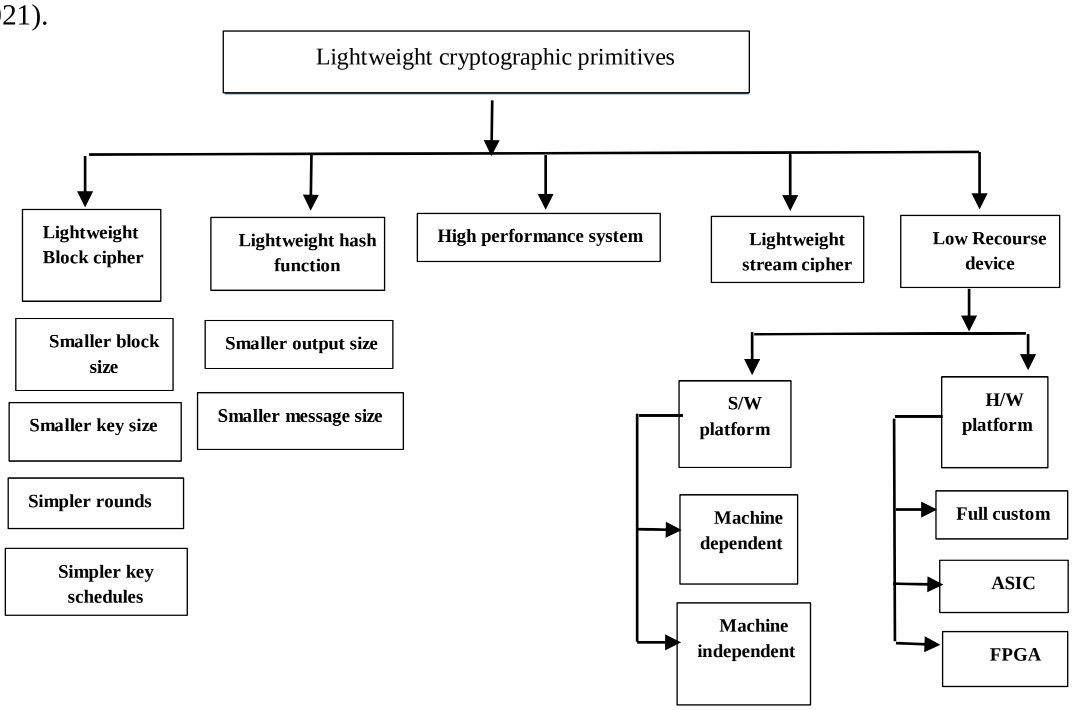

Fig. 2. Lightweight cryptographic primitives (Badr et al., 2019)

3.1 Block Ciphers

Block ciphers use a secret key and several rounds of encryption to convert one block of plaintext bits at a time to a block of cipher text bits. Every cycle consists of a series of straightforward changes that produce disarray and dissemination. A key schedule technique is used to obtain the round key, which is utilized in each round, from the secret key. some option make block cipher is preferable for resource-constrained environment such as : Small block length, Small key length , Simple round function , Simple key generation and Minimal implementations (Singh et al., 2020) (Mileva et al., 2021).

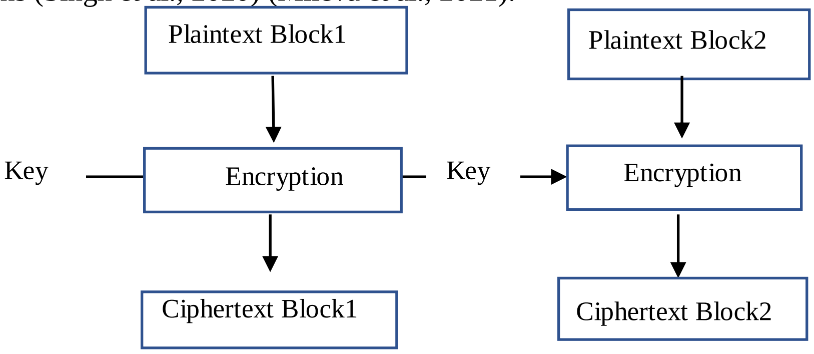

Fig. 3. describes the block cipher mechanism (Cusick & Stanica, 2017)

3.2 Stream Ciphers

Stream ciphers are cryptographic algorithms that operate on individual or multiple bits of data sequentially, encrypting them in tiny increments. The generation of a pseudorandom key stream is facilitated by the utilization of a secret key. This key stream is subsequently merged with the plaintext bits, resulting in the production of the corresponding cipher text bits. The combining function commonly employed is the bitwise XOR operation, leading to the classification of such systems as binary additive stream ciphers. In the context of stream ciphers, it is imperative to adhere to the fundamental security principle of avoiding the encryption of two distinct messages.

Utilizing an identical combination of key and Initialization Vector (IV). Consequently, stream ciphers often have a long key stream duration; after the time expires, a new key and/or IV need to be employed. A certain number of rounds, or clock cycles, are typically used in the initialization phase of each stream cipher. This is followed by an encryption phase. There are some factors that contribute to the design of lightweight stream cipher: Shorter LFSR length, Small inner state length, Small initialization length and Pseudorandom number generator (Singh et al., 2020) (Mileva et al., 2021). Fig. 4 shows stream cipher operation.

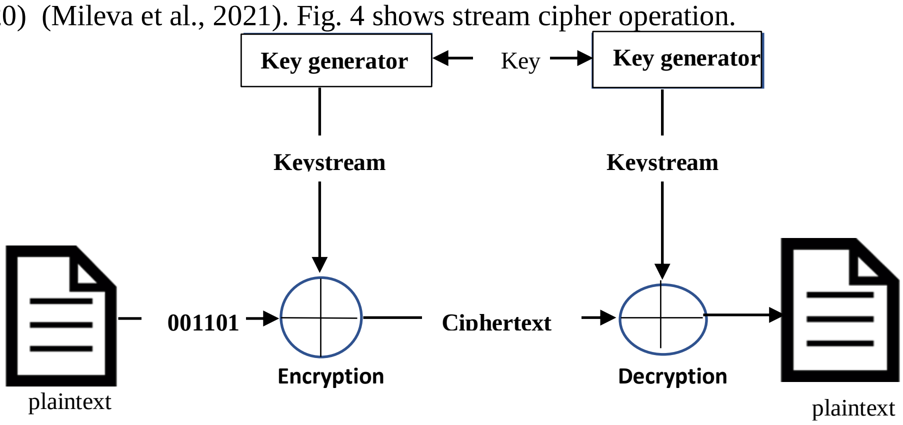

Fig. 4. General Structure of a stream cipher (Asaad et al., 2017)

3.3 Hash Functions

A hash function, also known as a message digest, is a cipher procedure that converts a changeable-length input message into a stable message called a hash message. We may create random generators or authentication systems that support digital signatures and data integrity using the capabilities of hash functions (Ghareeb & Gbashi, 2022). Cryptographic hash functions are required to possess the properties of preimage resistance (one-wayness), second preimage resistance, and collision resistance. Typically, the message undergoes a process of padding before being partitioned into blocks of a certain length. The performance of lightweight hash functions is superior to that of traditional hash algorithms due to many design choices, including: minor block size, Fewer number of input blocks, simple compression function. (Singh et al., 2020) (Mileva et al., 2021). The diagram is presented in Fig. 5. Illustrates the Hash Function.

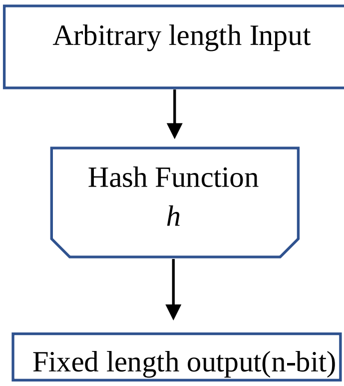

Fig. 5. A Hash Function (Tiwari, 2017).

3.4 Message Authentication Codes

Through the creation of a tag from the message and a secret key, a MAC safeguards the integrity and validity of a particular communication. Block ciphers, such as OCB-MAC [504] or CBC-MAC (part of the ISO/IEC 9797-1:1999 standard), cryptographic hash functions, such as HMAC (RFC 2104), etc., can be used to create MAC schemes. Certain design factors allow lightweight MAC algorithms to outperform traditional MAC algorithms in terms of performance: Little internal state, Lesser key length, minor number of rounds, Small MAC output. (Singh et al., 2020) (Mileva et al., 2021) For many online services, authentication has been utilized to solve unique security issues (Majeed & Rokan, 2020). Fig. 6 displays the creation of MAC.

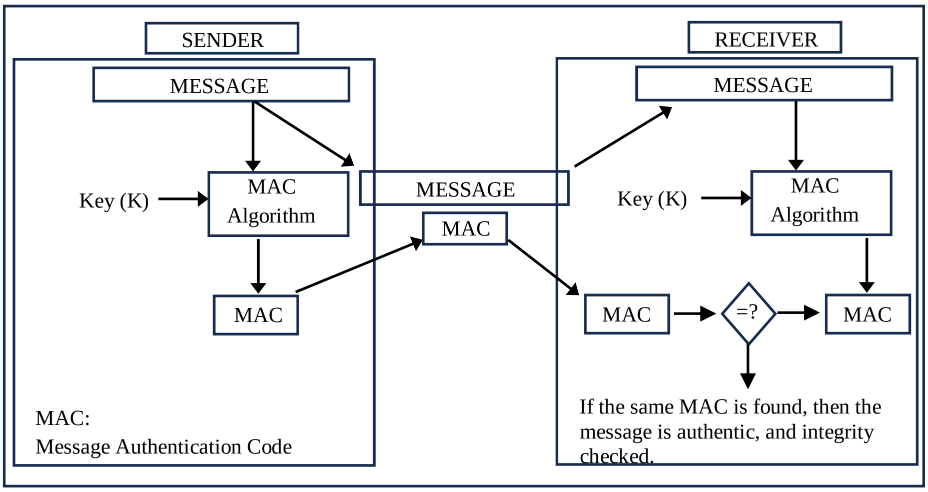

Fig. 6. Message Authentication Codes (Abdalsatir & Abboud, 2019).

3.5 Authenticated Encryption Schemes

AE schemes integrate the functionalities of ciphers and MACs into a single primitive, hence offering the combined benefits of secrecy, integrity, and authentication for a specific communication. In addition to the plaintext and secret key, AEAD methods often accommodate changeable length Associated Data, a public nonce, and a facultative secret nonce. The inclusion of the AD component within a message serves the purpose of ensuring authentication but excluding encryption (Mileva et al., 2021). Confidentiality is a protective measure employed to restrict access to information solely to individuals who possess the necessary authorization (Zhao et al., 2023). The authentication encryption scheme is depicted in Fig.7.

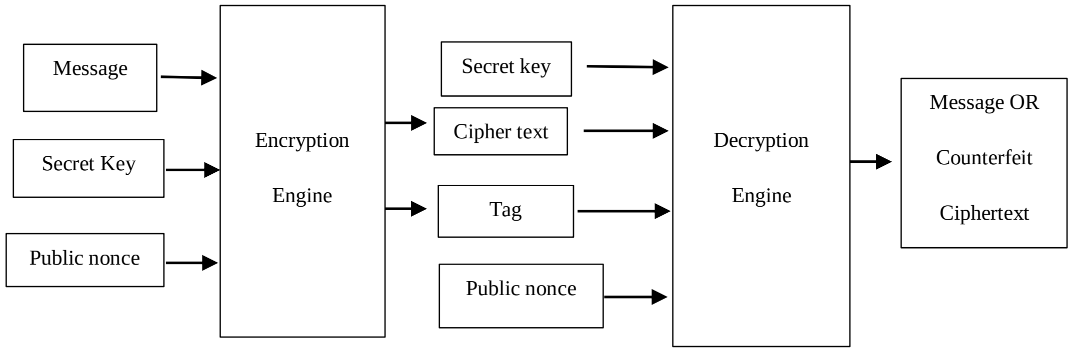

Fig. 7. Authentication encryption schema (Aljabri et al., 2023).

4. Literature Review

In the last years, many lightweight encryption algorithms have been proposed:

Alassaf et al. (2019) suggested a SIMON-based lightweight cryptographic algorithm for potential use in an IoT of Things environment. The proposed algorithm has been in contrast to the AES technique and the original block cipher SIMON techniques in execution time and memory use. The findings indicate that the enhanced SIMON algorithm shows improvement percentages between 20% and 26% across all block versions. However, it is worth noting that block size 64 has a slightly lower enhancement percentage of about 13%.

In Chen et al. (2019) the researchers present a new kind of hiding reversible data in encrypted images by using multi-secret sharing as the underlying encryption and lightweight cryptographic techniques to apply compression to create shared-one-key (SOK). It provides a full description of the SOK scheme from the share no secret keys (SNK) schemes. This proposed system is a top contender for maintaining efficiency and security in equal measure.

Almalkawi et al. (2019) lightweight and efficient security scheme based on chaotic algorithms to efficiently encrypt digital images was proposed. The two stages of the suggested scheme's handling are image encryption and image compression. Discrete Cosine Transform (DCT) is used to compress pictures during the compression stage. While the hybrid chaotic maps are used to safeguard images in four phases during the encryption process. The suggested chaotic image security system produces complex and random-looking cipher images while withstanding the majority of cryptanalysis and cryptography assaults, as confirmed by simulation results and security analysis. Saddam et al. (2020) proposed a lightweight coding algorithm called Stable IoT (SIT), Low complexity coding symmetry block cipher algorithm called Stable Power with Affine Shift for protecting sensitive data. The computation presented in this context employs a hybrid approach that relies on both Feistel and Square Switch Network (SP). The Blowfish algorithm is employed to encode the image matrix. The findings of the test demonstrate that the algorithm yields favorable outcomes, hence establishing its suitability for employment in IoT applications. Modifying a solitary bit in either the key or plain text results in a 49% alteration in the cipher bits, a proportion that closely approximates the ideal change of 50%.

Anwar & Maha (2020) Present hybrid cryptographic scheme, AES and Modified Playfair Cipher (AMPC), strengthen the security of WSN (Wireless sensor network). It uses the cryptographic schemes AES (Block Cipher) and Playfair (Stream Cipher) to encrypt data, while Diffie-Hellman is another technique used to secure the key exchange procedure. AMPC has addressed the constraints of WSN, providing higher security with less computational latency, and needs less operating time. It also transmits data quickly and consumes less energy.

Al-Husainy and Al-Shargabi (2020) proposed a lightweight encryption model to secure data transmission for IoT surveillance cameras. The suggested encryption scheme is compliant with the processor speed, memory capacity, and power consumption limitations of Internet of Things devices. The experimental findings demonstrate that, in comparison to other methods, the suggested algorithm achieves lower processing times and memory requirements while maintaining a high degree of data security. The suggested model's key size is sufficiently big to make it difficult for an attacker to crack. Mohandas et al. (2020) a new lightweight stream cipher A4 using one Linear Feedback Shift Register and One Feedback with Carry Shift

Register is proposed. The primary level of security is ensured by the LFSR's clocklike function. A seed box with 256 values serves as the pseudo-random source of the LFSR seed value. Each bit length is 128. It generates the key stream for server-side and client-side encryption and decryption, respectively, by clocking the FCSR. Additionally, it can withstand simple cryptographic assaults. Further LFSRs, FCSRs, or both can be added to further increase A4's security. However, it might lead to more implementation difficulty.

Roy et al. (2021) introduced a lightweight image encryption technique using 2-D Von-Neumann Cellular Automata (VCA), called IEVCA. The feature of IEVCA ascertain its robustness and resistance against various security attacks, Runtime faster as compared to its existing counterparts. The technique Traverse all the randomness tests of NIST and DIEHARD test suites.

Thabit et al. (2021) suggest A novel lightweight cryptographic algorithm (NLCA) for enhancing data security was proposed in the paper, which may be utilized to safeguard cloud computing systems. It is a block cipher designed to increase encryption complexity, influenced by Feistel and SP architectural techniques. Using a range of parameters, the suggested method evaluated its performance against other common cryptographic algorithms. The NLCA algorithm is considerably more efficient for cloud computing, according to experimental data, and it has a strong security level and cheap processing cost. (Khashan et al., 2021) adopted an automated lightweight cryptographic symmetric scheme called FlexCrypt for WSNs. It enables both flexible lightweight cryptography techniques and mobility across sensor nodes. The findings demonstrate that, in comparison to previous ciphers, the suggested method offers a considerable improvement in power consumption and network lifespan, a notable reduction in latency and encryption time, and the capacity to withstand well-known WSN attacks.

Al-Husainy et al. (2021) proposed a novel lightweight encryption system designed specifically for Internet of Things (IoT) devices. It is suitable for resource constrained IoT devices. It employs robust substitution and transposition operations to effectively encrypt and decrypt data. The encryption system demonstrated superior performance in encryption time when compared to AES. The use of Deoxyribonucleic Acid (DNA) sequences to produce cryptographic keys is also employed. Furthermore, the suggested scheme successfully produced desirable levels of confusion and dispersion effects. avalanche test value of 50%, indicating its resilience against statistical analysis attacks. Hasan et al. (2021) proposed a secure, lightweight algorithm encryption technology to protect patients' medical images' privacy. Two permutation strategies are used in the suggested lightweight encryption method to protect medical photos. featured a discussion of the various encryption algorithms currently in use as well as different security metrics. When it comes to the execution time of medical picture encryption, the suggested solution performs more efficiently than traditional approaches.

Abd Zaid & Hassan (2022) introduced the proposed framework of lightweight security algorithms for cryptography primitives. The resources, time, memory, and lifetime of relevant sensors must all be taken into account in the proposed system encryption. They have made several adjustments to their algorithm for the stream cipher and block cipher. The (NIST) statistical tests for test randomness, greater processing speed, reduced memory use, and higher throughput than conventional algorithms were all passed by all of the lightweight algorithms that were generated.

Mohammed (2023) In order to determine the confusion/diffusion qualities and look into the functional aspects, this research recommends developing a lightweight authentication encryption technique for Internet of Things applications based on stream cipher and chaotic maps with sponge structure. Text data is used in the proposed method for permission and encryption. The suggested system is random and secure, as shown by randomness tests, and demonstrates the system's quick performance and low memory requirements. Tawalbeh et al. (2022) proposed a new lightweight crypto algorithm called the Mypher algorithm to provide security to IoT devices. The functioning of the system involves the integration of a substitution box, a permutation box, and cyclic key shifting. The algorithms aim to provide a level of security that is deemed to be reasonable while minimizing the associated expenses. The results indicated that there exists considerable variation in performance even across IOT devices. Consequently, selecting an algorithm for such devices is not a universally applicable solution, particularly when considering resource-constrained devices. Singh et al. (2023) proposed two hardware architectures for KLEIN block cipher to encrypt variant sets of images under resource-constrained implementations. The two-hardware serial and pipelined architectures is observed. The security analysis showed stronger encryption. The simulation results confirmation robust resistance against a wide range of statistical and differential assaults.

Mahlake et al. (2023) A new security method called Lightweight Security Algorithm (LSA) was developed by merging the Security Protocol for Sensor Networks (SPINS) with the Secure IoT (SIT) encryption method. This combination results in the highest level of perplexity and burstiness in data. Additionally, the LSA has a lower number of rounds, reducing energy consumption and improving overall security for Wireless Sensor Networks (WSNs). This advancement aims to reduce the risk of cyber-attacks while also minimizing power usage and maintaining network efficiency.

Table 3 demonstrates in brief the aforementioned researches for block cipher algorithms. It includes the enhancement domain based on the key size, entropy method and conventional methods.

Table 3 - Classification Lightweight Block Ciphers

NO./Years	Methodology	Performance Metric	Result evaluation
(Alassaf et al., 2019)/2018	A lightweight cryptography algorithm based on SIMON	Execution time, memory consumption	An enhancement from 20% to 26% for all block sizes is expected; 64 shows a percentage close to 13%. no attacks surpass 70% of any variety of SIMON
(Almalkawi et al., 2019)/2019	A lightweight encryption technique using chaotic algorithms.	Key space and key sensitivity, entropy, histogram, statistical analysis, differential attacks analysis, time consumption, processing complexity	Resisting most existing attacks (statistical attacks and differential attacks), proposed algorithm surpassed the performance of other current techniques.
(Saddam et al., 2020)/2020	A lightweight coding algorithm (SIT).	Histogram, MSE (mean square error), memory consumption. encryption /decoding execution cycles	Optimal change of 50%.
(Al-Husainy et al., 2021)	Lightweight encryption model for surveillance cameras.	Peak Signal to Noise Ratio (PSNR), Histogram, encryption time	Shorter encryption time 170.7 ms for an 80-bit key. A 7.7 PSNR and a large key make it difficult for attackers to crack.
(Roy et al., 2021)/2020	A lightweight, called IEVCA algorithm	National Institute of Standards and Technology (NIST) DIEHARD1. “Unified Average Changing Intensity (UACI), Energy consumption, entropy, MSE, histogram, PSNR, Correlation, differential analysis.	Traverse all NIST and DIEHARD test, can stop a variety of cryptanalysis attacks, including those that use brute force, known plaintext, chosen plaintext, known ciphertext, and chosen cipher text.
(Thabit et al., 2021)/2021	A Lightweight encryption algorithm (NLCA)	Execution time, block size, key length, possible key, mathematical operations, cipher type, and security power.	Quick processing, cheap calculation costs, and strong security
(Khashan et al., 2021)/2021	A Lightweight cryptographic scheme Flex Crypt.	Encryption time, power consumption, network lifetime.	Reduction in power consumption, 66%. Extension in network lifespan, improvements of 86%, 94%, and 90%. resist various attacks (brute-force, eavesdropping, man-in-the-middle and replay).
(Al-Husainy et al., 2021)/2021	A flexible lightweight encryption system.	PSNR, Histogram, Entropy, avalanche test, memory usage, execution time.	Given that the avalanche test value was greater than 50%, both real-time and statistical analysis attacks are prevented. reduce the amount of RAM used and the encryption time.
(M. K. Hasan et al.,	A Lightweight algorithm	Entropy, MSE, execution time,	Minimal computations, maximum

2021)/2021	encryption medical images.	correlation, PSNR,	security, and more effective techniques
(Tawalbeh et al., 2022)/2022	A Lightweight crypto algorithm Mypher	Key Size, Block Size, Performance Tests.	There can be widely varying performance among IoT devices.
(Singh et al., 2023)/2023	Two hardware implementations for the KLEIN block cipher.	Entropy, MSE, PSNR, NPCR, UACI, Histogram variance analysis, correlation ,Key space anlaysis, Differential attack analysis, Known-plaintext attack (KPA) and chosen-plaintext attack (CPA) analysis, Chi-square test analysis	While pipelined architecture produced high throughput and increased processing speed, serial architecture required less space for hardware. robust defense against multiple statistical and differential assaults.

Table (4) presents the aforementioned researches that proposed an approach to enhanced stream cipher. The developed work is based on image encryption, chaotic map simultaneously

Table 4 - Classification of Lightweight Stream Ciphers

NO./Years	Methodology	performance metric	Result evaluation
Mohandas et al. 2020)	A new lightweight stream cipher A4.	Security analysis.	little computational price, attacks that are conceivable on MAC tags will not work on A4: (Meet in the middle, algebraic, brute force, differential, correlation) attacks.
(Mohammed, 2023)/2022	Lightweight encryption technique combination of stream cipher and chaotic maps, using a sponge structure	NIST randomness tests, execution time, memory space, and functional features.	Fewer memory spaces and good rapidity.

Table 5 - Classification Lightweight Stream Ciphers and block cipher

NO/Years	Methodology	Performance metric	Result evaluation
(Roy et al., 2021)/2020	A lightweight algorithm called (IEVCA).	(NIST, DIEHARD) statistical test, Energy consumption, statistical test suit (STS), Differential analysis, Analysis of histogram, MSE Correlation coefficient analysis, PSNR.	Encryption procedure that passes all randomness tests, uses very little resources, runs faster, and is resilient to a variety of security threats.
(Abd Zaid & Hassan, 2022)/2022	The framework lightweight security methods.	NIST, Nist statistical tests, avalanche effect. measuring time and memory used.	better processing time, less memory usage, higher throughput, more cost-effective, faster
(Mahlake et al., 2023)/2023	Lightweight Security Algorithm (LSA)	Energy consumption Packet Drop Ratio (PDR). key expansion time, key expansion time.	Decrees power consumption by an average of 411.2uJ, (PDR) was between 90 and 99%, decrees the key obstetrics time by 102mS, enhancement the security by 99%.

Table (5) displays the proposed work that developed an approach is based on combining the stream and block with limitation.

5. Analysis and Discussion

Over the past few years, several lightweight block ciphers have been introduced. Some notes from Table2 could be noticed as in follow:

- Their contribution enhanced the encryption performance while preserving an optimal tradeoff between security, performance and memory cost.

- Achieve performance from a practical perspective, more security with minimum computational delay.
- It successfully tackles all NIST and DIEHARD tests.
- These techniques are highly applicable to cloud computing, it can be implemented in serial and pipelined architecture, and a significant extension of in-network longevity.
- Lightweight block algorithm is capable of withstanding the majority of current attacks, various statistical and differential.

In the Table3: a lightweight stream cipher scheme is at least a candidate to preserve both efficiency and security. it is faster than others since this relied on exclusive OR operation, less memory space and can resist most attacks such as Meet in the middle, algebraic, brute force, differential, correlation attacks.

Finally, in the Table4: a hybrid cryptographic scheme is presented, consisting of block cipher and stream cipher, it facilitates fast data transmission with lower energy consumption
It concluded that the block cipher algorithms are most suitable to be implemented as a lightweight algorithm. This is done through enhancement of the Key size, and block size, and reducing the number of encryption rounds. In addition, the improvement also replaces some steps as in block cipher by stream cipher methods or combined to form a hybrid algorithm

Summary of the result:

- To measure the performance of algorithms, there is some performance metrics, such as execution time, memory usage, encryption/decryption speed, security features:
- Assessment of Robustness and measure the strength of encryption. There are types of attacks must be measured, such as brute-force attacks, differential cryptanalysis, linear cryptanalysis, and statistical attacks
- How can contribution enhance encryption performance while preserving an optimal tradeoff between security, performance, and memory cost?

6. Conclusion and Future Works

The most important requirement for the needed algorithms is to reduce storage, power consumption, latency, and execution time, especially with resource-constrained devices. we can apply lightweight encryption algorithms to achieve this requirement. The factors that were reviewed, when reduced, greatly affect the security of the transmitted data, and this certainly leads to many problems. Therefore, the use of lightweight encryption algorithms must strike a balance between security and speed, and this is done either with hybrid algorithms between block and stream or by increasing the degree of complexity of the encryption key after modifying the original algorithm. In addition, the block size can be controlled while maintaining the degree of security or reducing the number of rounds to improve the algorithm and maintain the degree of complexity, especially the feature confusion/diffusion qualities. Effective and safe algorithms exist for all Internet of Things application. As future work, we can expand outcomes for more block and stream ciphers, compare their performance with other enciphering techniques such as hybrid algorithms between block and stream, and do tests over a new IoT testbed.

References

Abd Zaid, M., & Hassan, S. (2022). Proposal Framework to Light Weight Cryptography Primitives. *Engineering and Technology Journal, 40*(4), 516–526. https://doi.org/10.30684/etj.v40i4.1679

Abdalsatir, A. T., & Abboud, A. J. (2019). Integrity Checking of Several Program Codes. *Journal of Engineering and Applied Sciences, 14*(13), 4435–4441. https://doi.org/10.36478/jeasci.2019.4435.4441

Abdulameer, S. A., Kashmar, A. H., & Shihab, A. I. (2020). A cryptosystem for database security based on TSFS algorithm. *Baghdad Science Journal, 17*(2), 567–574. https://doi.org/10.21123/bsj.2020.17.2.0567

Abed, M. M., & Younis, M. F. (2019). Developing load balancing for IoT - Cloud computing based on advanced firefly and weighted round robin algorithms. *Baghdad Science Journal, 16*(1), 130–139. https://doi.org/10.21123/bsj.2019.16.1.0130

Ahmed Faiq Al-Alawy, Al-Abod, E. E., & Raya Mohammed Kadhim. (2018). Journal of engineering. *The Journal of Engineering, 2019*(16), 2597–2603. https://digital-library.theiet.org/content/journals/10.1049/joe.2018.8601

Alassaf, N., Gutub, A., Parah, S. A., & Al Ghamdi, M. (2019). Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications. *Multimedia Tools and Applications*, *78*(23), 32633–32657. https://doi.org/10.1007/s11042-018-6801-z

Al-Husainy, M. A. & & Al-Shargabi, B. (2020). Secure and lightweight encryption model for IoT surveillance camera. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(2), 1840–1847. https://doi.org/10.30534/ijatcse/2020/143922020

Al-Husainy, M. A. F., Al-Shargabi, B., & Aljawarneh, S. (2021). Lightweight cryptography system for IoT devices using DNA. *Computers and Electrical Engineering, 95*(August 2020), 107418. https://doi.org/10.1016/j.compeleceng.2021.107418

Aljabri, Z., Abawajy, J., & Huda, S. (2023). A Comprehensive Review of Lightweight Authenticated Encryption for IoT Devices. *Wireless Communications and Mobile Computing*, 2023. https://doi.org/10.1155/2023/9071969

Almalkawi, I. T., Halloush, R., Alsarhan, A., Al-Dubai, A., & Al-karaki, J. N. (2019). A lightweight and efficient digital image encryption using hybrid chaotic systems for wireless network applications. *Journal of Information Security and Applications, 49*, 102384. https://doi.org/10.1016/j.jisa.2019.102384

Anwar, M. N. Bin, & Maha, M. M. (2020). AMPC: A Lightweight Hybrid Cryptographic Algorithm for Wireless Sensor Networks. *International Journal of Innovative Science and Research Technology, 5*(6), 1142–1146. https://doi.org/10.38124/ijisrt20jun975

Asaad, R. R., Abdurahman, S. M., & Hani, A. A. (2017). Partial image encryption using RC4 stream cipher approach and embedded in an image. *Academic Journal of Nawroz University*, *6*(3), 40-45. https://doi.org/10.25007/ajnu.v6n3a76

Badr, A. M., Zhang, Y., & Ahmad Umar, H. G. (2019). Dual authentication-based encryption with a delegation system to protect medical data in cloud computing. *Electronics*, *8*(2), 171. https://doi.org/10.3390/electronics8020171

Buchanan, W. J., Li, S., & Asif, R. (2017). Lightweight cryptography methods. *Journal of Cyber Security Technology,* *1*(3-4), 187-201.https://doi.org/10.1080/23742917.2017.1384917

Chaudhary, R. R. K., & Chatterjee, K. (2020). An efficient lightweight cryptographic technique for iot based E-healthcare system. *2020 7th International Conference on Signal Processing and Integrated Networks,* SPIN 2020, 991–995. https://doi.org/10.1109/SPIN48934.2020.9071421

Chen, Y. C., Hung, T. H., Hsieh, S. H., & Shiu, C. W. (2019). A New Reversible Data Hiding in Encrypted Image Based on Multi-Secret Sharing and Lightweight Cryptographic Algorithms. *IEEE Transactions on Information Forensics and Security, 14*(12), 3332–3343. https://doi.org/10.1109/TIFS.2019.2914557

Chiadighikaobi, I. R., & Katuk, N. (2021). A scoping study on lightweight cryptography reviews in IoT. *Baghdad Science Journal*, *18*(2), 989–1000. https://doi.org/10.21123/bsj.2021.18.2(Suppl.).0989

Cusick, T. W., & Stanica, P. (2017). *Cryptographic Boolean functions and applications*. Academic Press.

Fadhil, M. S., Farhan, A. K., & Fadhil, M. N. (2021). A lightweight aes algorithm implementation for secure iot environment. *Iraqi Journal of Science*, *62*(8), 2759–2770. https://doi.org/10.24996/ijs.2021.62.8.29

Fotovvat, A., Rahman, G. M. E., Vedaei, S. S., & Wahid, K. A. (2021). Comparative Performance Analysis of Lightweight Cryptography Algorithms for IoT Sensor Nodes. *IEEE Internet of Things Journal*, *8*(10), 8279–8290. https://doi.org/10.1109/JIOT.2020.3044526

George, L. E., Hassan, E. K., Mohammed, S. G., & Mohammed, F. G. (2020). Selective image encryption based on DCT, hybrid shift coding and randomly generated secret key. *Iraqi Journal of Science, 61*(4), 920–935. https://doi.org/10.24996/ijs.2020.61.4.25

Ghareeb, Y. A., & Gbashi, E. K. (2022). A Lightweight Hash Function Based on Enhanced Chaotic Map Algorithm(Keccak). *Iraqi Journal of Computer, Communication, Control and System Engineering, 22*(2), 53–62. https://doi.org/10.33103/uot.ijccce.22.2.5

Hameed, S. M., Sa'adoon, H. A., & Al-Ani, M. (2018). Image encryption using DNA encoding and RC4 algorithm. *Iraqi Journal of Science, 59*(1B), 434–446. https://doi.org/10.24996/IJS.2018.59.1B.24

Hasan, M. K., Islam, S., Sulaiman, R., Khan, S., Hashim, A. H. A., Habib, S., Islam, M., Alyahya, S., Ahmed, M. M., Kamil, S., & Hassan, M. A. (2021). Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications. *IEEE Access, 9*, 47731–47742. https://doi.org/10.1109/ACCESS.2021.3061710

Hasan, M. Y., & Kadhim, D. J. (2022). Efficient Energy Management for a Proposed Integrated Internet of Things-Electric Smart Meter (2IOT-ESM) System. *Journal of Engineering, 28*(1), 108–121. https://doi.org/10.31026/j.eng.2022.01.08

Hussein Ali, N. M., & Ali Abead, S. (2016). Modified Blowfish Algorithm for Image Encryption using Multi Keys based on five Sboxes. *Journal of Science, 57*(4C), 2968–2978.

Hussein, S. N., Obaid, A. H., & Jabbar, A. (2022). Encryption Symmetric secret Key in Wireless Sensor Network Using AES Algorithm. *Iraqi Journal of Science, 63*(11), 5037–5045. https://doi.org/10.24996/ijs.2022.63.11.38

Jallouli, O., Chetto, M., & Assad, S. El. (2022). Lightweight Stream Ciphers based on Chaos for Time and Energy Constrained IoT Applications. *2022 11th Mediterranean Conference on Embedded Computing*, MECO 2022. https://doi.org/10.1109/MECO55406.2022.9797087

K, S., & A, C. (2021). A Review on Lightweight Block Ciphers. *SSRN Electronic Journal*, 146–150. https://doi.org/10.2139/ssrn.3794162

Kapalova, N., Algazy, K., & Haumen, A. (2023). Development of a New Lightweight Encryption Algorithm. *Eastern-European Journal of Enterprise Technologies, 3*(9(123)), 6–19. https://doi.org/10.15587/1729-4061.2023.280055

Khashan, O. A., Ahmad, R., & Khafajah, N. M. (2021). An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. *Ad Hoc Networks*, *115*(October 2020), 102448. https://doi.org/10.1016/j.adhoc.2021.102448

Kousalya, R., & Sathish Kumar, G. A. (2019). A Survey of Light-Weight Cryptographic Algorithm for Information Security and Hardware Efficiency in Resource Constrained Devices. *Proceedings - International Conference on Vision Towards Emerging Trends in Communication and Networking, ViTECoN 2019*, 1–5. https://doi.org/10.1109/ViTECoN.2019.8899376

Mahlake, N., Mathonsi, T. E., Du Plessis, D., & Muchenje, T. (2023). A Lightweight Encryption Algorithm to Enhance Wireless Sensor Network Security on the Internet of Things. *Journal of Communications, 18*(1), 47–57. https://doi.org/10.12720/jcm.18.1.47-57

Majeed, G. H., & Rokan, J. (2020). Internet of Things Authentication Based on Chaos-Lightweight Bcrypt Internet of Things Authentication Based on Chaos-Lightweight Bcrypt chaos-Blowfish (Jolan Rokan Naif Informatics. *February,* 35–50.

Melki, R., Noura, H. N., & Chehab, A. (2020). Lightweight multi-factor mutual authentication protocol for IoT devices. *International Journal of Information Security, 19*(6), 679–694. https://doi.org/10.1007/s10207-019-00484-5

Mileva, A., Dimitrova, V., Kara, O., & Mihaljević, M. J. (2021). Catalog and Illustrative Examples of Lightweight Cryptographic Primitives. *Security of Ubiquitous Computing Systems: Selected Topics*, 21–47. https://doi.org/10.1007/978-3-030-10591-4_2

Mohammed, R. S. (2023). Design a Lightweight Authentication Encryption Based on Stream Cipher and Chaotic Maps with Sponge Structure for Internet of Things Applications.

International Journal of Intelligent Engineering and Systems, 16(1), 532–547. https://doi.org/10.22266/ijies2023.0228.46

Mohandas, N. A., Swathi, A., Abhijith, R., Nazar, A., & Sharath, G. (2020). A4: A lightweight stream cipher. In *2020 5th international conference on communication and electronics systems (ICCES) (pp. 573-577)*. IEEE. https://doi.org/10.1109/ICCES48766.2020.9138048

Nayancy, Dutta, S., & Chakraborty, S. (2022). A survey on implementation of lightweight block ciphers for resource constraints devices. *Journal of Discrete Mathematical Sciences and Cryptography, 25*(5), 1377–1398. https://doi.org/10.1080/09720502.2020.1766764

Panahi, P., Bayılmış, C., Çavuşoğlu, U., & Kaçar, S. (2021). Performance Evaluation of Lightweight Encryption Algorithms for IoT-Based Applications. *Arabian Journal for Science and Engineering, 46*(4), 4015–4037. https://doi.org/10.1007/s13369-021-05358-4

Roy, S., Shrivastava, M., Pandey, C. V., Nayak, S. K., & Rawat, U. (2021). IEVCA: An efficient image encryption technique for IoT applications using 2-D Von-Neumann cellular automata. *Multimedia Tools and Applications, 80*(21–23), 31529–31567. https://doi.org/10.1007/s11042-020-09880-9

Saadatnejad, S., Oveisi, M., & Hashemi, M. (2020). LSTM-Based ECG Classification for Continuous Monitoring on Personal Wearable Devices. *IEEE Journal of Biomedical and Health Informatics, 24*(2), 515–523. https://doi.org/10.1109/JBHI.2019.2911367

Saddam, M. J., Ibrahim, A. A., & Mohammed, A. H. (2020). A Lightweight Image Encryption and Blowfish Decryption for the Secure Internet of Things. *4th International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT 2020 - Proceedings*. https://doi.org/10.1109/ISMSIT50672.2020.9254366

Sevin, A., & Mohammed, A. A. O. (2023). A survey on software implementation of lightweight block ciphers for IoT devices. *Journal of Ambient Intelligence and Humanized Computing, 14*(3), 1801–1815. https://doi.org/10.1007/s12652-021-03395-3

Shilpa, K. & Chinchu. A. (2021). A review on lightweight block ciphers. *Proceedings of the International Conference on Systems, Energy & Environment (ICSEE) 2021*. http://dx.doi.org/10.2139/ssrn.3791092

Singh, P., Acharya, B., & Chaurasiya, R. K. (2020). Lightweight cryptographic algorithms for resource-constrained IoT devices and sensor networks. In *Security and Privacy Issues in IoT Devices and Sensor Networks*. Elsevier Inc. https://doi.org/10.1016/B978-0-12-821255-4.00008-0

Singh, P., Agrawal, B., Chaurasiya, R. K., & Acharya, B. (2023). Low-area and high-speed hardware architectures of KLEIN lightweight block cipher for image encryption. *Journal of Electronic Imaging, 32*(01). https://doi.org/10.1117/1.jei.32.1.013012

Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing,* 1-18. https://doi.org/10.1007/s12652-017-0494-4

Taha, M. H., & Al-Tuwaijari, J. M. (2021). Improvement of Chacha20 algorithm based on tent and Chebyshev chaotic maps. *Iraqi Journal of Science, 62*(6), 2029–2039. https://doi.org/10.24996/ijs.2021.62.6.29

Tawalbeh, L., Alicea, M., & Alsmadi, I. (2022). New and Efficient Lightweight Cryptography Algorithm for Mobile and Web Applications. *Procedia Computer Science, 203*(2019), 111–118. https://doi.org/10.1016/j.procs.2022.07.016

Thabit, F., Alhomdy, A. P. S., Al-Ahdal, A. H. A., & Jagtap, P. D. S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. *Global Transitions Proceedings, 2*(1), 91–99. https://doi.org/10.1016/j.gltp.2021.01.013

Tiwari, H. (2017). Merkle-Damgård construction method and alternatives: a review. *Journal of Information and Organizational Sciences, 41*(2), 283-304.

Xiao-Mei, L., & Yong, Q. (2019). Research on LED lightweight cryptographic algorithm based on RFID tag of Internet of things. *Proceedings of 2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference*, ITAIC 2019, Itaic, 1717–1720. https://doi.org/10.1109/ITAIC.2019.8785584

Yousif, S. T., & Fadahl, Z. A. (2021). Proposed Security Framework for Mobile Data Management System. *Journal of Engineering*, *27*(7), 13–23. https://doi.org/10.31026/j.eng.2021.07.02

Zang, Y., Yu, B., & Zhao, S. (2023). Lightweight seatbelt detection algorithm for mobile device. *Multimedia Tools and Applications, 82*(16), 24505–24519. https://doi.org/10.1007/s11042-023-14555-2

Zhao, J., Hu, H., Huang, F., Guo, Y., & Liao, L. (2023). Authentication Technology in Internet of Things and Privacy Security Issues in Typical Application Scenarios. *Electronics (Switzerland)*, *12*(8), 1–21. https://doi.org/10.3390/electronics12081812