Lightweight Block Cipher for Resource Constrained IoT Environment—An Survey, Performance, Cryptanalysis and Research Challenges

M. Abinaya and S. Prabakeran

Abstract Nowadays IoT (Internet of Things) is becoming a more popular environment and has a variety of applications like Smart Home, Smart Healthcare, Vehicles, and many Industries. There is plenty of information shared among the devices with the use of the internet. Due to this importance of data sharing, there is a possibility of security attacks, and threats. IoT environments have many security challenges including Providing Confidentiality, Integrity, and Availability in addition Privacy, Authentication. These challenges can be fulfilled by many cryptographic algorithms. Since IoT has limited memory, resources, power, those cryptographic primitives may not be suitable. The best solution for this problem is lightweight cryptographic algorithms. This paper presents the importance of lightweight cryptography algorithms. We analysed the performance of current algorithms in terms of throughput, latency, ROM/RAM, software efficiency, and energy. We are comparing the cryptanalysis of some popular algorithms. Also, we are discussing the research challenges and research gaps in the area of lightweight cryptography for providing better performance, cost and software implementation without affecting high security.

Keywords Internet of Things · Security issues · Lightweight block Cipher · Performance metrics. Cryptanalysis

1 Introduction

This is a fast-moving field known as the Internet of Things. By 2024, there are expected to be 50 billion gadgets on the market, and it is imperative that we understand what it will take to get there.

M. Abinaya (✉) · S. Prabakeran
Department of Networking and Communication, SRMIST, Chennai, India
e-mail: am8580@srmist.edu.in

S. Prabakeran
e-mail: prabakes@srmist.edu.in

P. P. Joby et al. (eds.), *IoT Based Control Networks and Intelligent Systems*,
Lecture Notes in Networks and Systems 528,
https://doi.org/10.1007/978-981-19-5845-8_25

The Internet of Things (IoT) is an environment that encompasses connecting devices to the internet and using that connection to facilitate remote monitoring or control of those objects [15]. No substantial security concerns were raised when the Internet of Things (IoT) technologies were first built by linking small devices equipped with sensors, as was the case when they were first developed.

The Internet of Things (IoT) is becoming increasingly significant in terms of security as more and more devices are connected to exchange private and sensitive information. Each stage of the Internet of Things design lifecycle has a distinct set of security and research issues.

IoT devices are classified into two types. One has many resources, while the other does not. Servers, personal computers, tablets, and smartphones are examples of high-resource devices. On the other hand, insufficient resources are sensor nodes, RFID tags, actuators. These resource-constrained devices have some security flaws. Every smart device must be protected and maintained as new vulnerabilities are discovered.

Confidentiality, Integrity, Availability, Privacy, Authenticity, and Lightweight Solutions are all well-known security objectives. During any transfer, confidentiality is a way of securing all information from unauthorised nodes [52]. It may be performed by the sender and recipient exchanging safe keys. In addition, encrypt the data before delivering it to the recipient and then decode the data after receiving it using this key to obtain the original information. It is imperative that data stored in the cloud remain private.

The integrity of the transmission guarantees that it does not alter throughout transmission. When it comes to data transport, a symmetric cryptographic approach is frequently employed to generate signatures. Another function is the Message Integrity Check, which checks to see if the data received is correct before displaying it. The system must be capable of displaying the route if a change is detected and an activity log must be created in order to demonstrate the change. They may be held locally or centrally, for a short period of time or for an extended period of time, and for any reason at all.

Availability ensured that authorized users could always access IoT services and applications. When the connected things are needed, they should be available and functional. It is essential that the system has the ability to protect itself and heal itself in the case of a failure or an attack. Hierarchical organisation of Internet of Things nodes can help to improve scalability.

Privacy is the ability of an individual or a group to separate information about themselves or themselves and thereby selectively express themselves. To keep the nodes flexible and consider a wide range of IoT applications, RFID tags provide robust privacy. The personal information of other users should not be used to create profiles by unidentified individuals. An IoT device's current or previous location can't be revealed.

Lightweight solutions is a novel characteristic for IoT devices since IoT devices are generally computationally lightweight and have limited memory.

For Internet of Things devices, authenticity is essential since it enables them to verify and authenticate the active users of the connection. User authentication, context

authentication, and device authentication all need to be confirmed for a user to be authenticated in the context of a given system. Secondly, there's Trust Management, which focuses on IoT security and network performance in general. It further states that IoT devices and the central unit must validate a user's identity on their own, without the assistance of a third party.

Hardware is more important to execute the algorithm in faster. In IoT environment all the hardware devices are very small having low energy and its working based upon the battery power. Devices used in IoT environment is execute only RISC and CISC oriented architecture. So, the size of the algorithm should be minimized with the consideration of high security.

Let us consider a resource-constrained device like IoT. The best solution for security achievement is light cryptography algorithms. LWC (Lightweight Cryptography) is encryption with a tiny footprint or low computing complexity. When developing a security solution for devices with limited resources, lightweight cryptography aims to use less memory, computing resources, and power than classical encryption in order to provide a more reliable security solution. When compared to traditional encryption, lightweight cryptography is believed to be less complicated and faster to implement than the latter.

In this article, we will discuss in Sect. 2 of related work from various research papers and our contribution towards our research, in Sect. 3 on lightweight block ciphers, in Sect. 4 on performance metrics for lightweight block ciphers, in Sect. 5 Cryptanalysis of Various Algorithms, in Sect. 6, the discussion of research gaps and challenges in Sect. 7 will be the conclusion.

2 Related Work

In [1], authors described light cryptography algorithms to secure the IoT environment. Discussed about the security level, chip area, throughput, latency time, hardware and software efficiency, and figure of merit are all the important factors for validating the encryption algorithm. Based upon these metrics, they concluded that AES is the most competitive algorithm which provides high-level security. They also indicated that ECC is still a viable solution for providing authentication and non-repudiation.

The creators of [2] offered a new Speck version, dubbed Speck-R, to the world. Here dynamic substitution layer had been introduced to improve security level of encryption algorithm Speck-R. The ARX (Addition, Rotation, and XOR) method of encryption is used to secure this Speck–R. The most significant contribution of this study is the number of rounds of original Speck algorithm is reduced from 26 to 7 and also high level of safety is satisfied.

In [3], the authors discuss the common and well-known attacks and threats that are affecting the different IoT design, as well as the problems identified with them. Eavesdropping on the sender's messages, identity theft, unauthorised access, trojans, and malicious software insertion into the code are all examples of risks. As a result of their research, they developed SDN-based Internet of Things designs.

The authors concentrate on the end-to-end security model, which allows the end nodes to communicate securely over an unprotected channel, as described in [4]. An IoT security middleware that is adaptable may safeguard intermittent network devices when they are connected as well as convert security protocols between cloud and edge networks in this configuration. No matter whether one of the devices is an active communication node or not, it ensures a secure connection between the two.

According to the authors of [5] the era of Internet of Things (IoT), its supporting technologies, and a complicated security strategy in conjunction with the conventional internet were offered. Many security attacks, threats, and reactions have been examined, as well as their consequences. Finally, they came to the conclusion that Internet of Things (IoT) Availability is essential. The discussion has come to a conclusion with regard to current approaches, implementation challenges, and future research objectives.

The authors of [6] presented a lightweight security system (LSS) for IoT in their paper. LSS protects the Internet of Things while lowering energy consumption. LSS is divided into three stages: The system was made immune to CPA attacks by generating secret compressed samples during the key generation, key exchange, and compression with encryption stages. The success of their technique is that it extends the network lifetime compared to existing encryption algorithms.

The authors of [7] concentrate on the security of resource-constrained systems, indicating the need for lightweight cryptographic methods. Lightweight cryptography, which is a realistic way for securing communication by modifying data, may be beneficial for Internet of Things devices with little resources. The well-defined LWC characteristics are compared and contrasted with one another. This paper highlights the research gaps and outstanding research problems that have been identified. They concluded that the block ciphers PRESENT and CLEFIA are acceptable. SIMON and SPECK are the most suitable encryption algorithms for hardware and software implementations respectively.

The performance of ten lightweight block cyphers is investigated and evaluated in the work of [8] researchers using the Raspberry Pi 3 and the Arduino Mega 2560 devices, respectively. The performance of encryption and decryption operations on payloads is measured in terms of memory usage, execution time, throughput, and energy consumption, with memory utilisation being the most important factor to consider. This research is really beneficial in establishing the most appropriate setting and encryption approach for us.

In [9], the authors proposed an algorithm that is based upon a symmetric key block cipher with a 64-bit key. Every symmetric key strategy has a number of encryption rounds, and the process of encrypting data is one of them. It is necessary to use custom substitution-permutation networks and the Feistel architecture in this case. Two fundamental concepts are applied through the usage of the Genetic Algorithm. When it comes to measurement, FELICES, a Linux-based benchmark application, is employed, whereas MATLAB is used when it comes to encryption quality testing.

Key scheduling can be used to construct the encryption keys needed for IoT devices in medical care to increase the security of data transferred in healthcare environments, according to the author of [10]. First, a unique input is transformed

into a 128-bit input key separated into four 4-bit segments. The Fibonacci scrambling algorithm is used to generate the encryption key sequences in the second stage.

A review of the many lightweight solutions and the security dangers they pose to the authentication and data integrity of the Internet of Things application can be found in [11]. The main application area of the Internet of Things has been discussed. In their examination, researchers discovered that the main security part of these protocols is to execute with the least amount of computing in order to avoid attacks such as "man in the middle," "replay attacks," "denial of service attacks," "forgery," and "chosen-ciphertext attacks," among others. The article demonstrates how to use Microsoft's threat modelling tool for the safe development life cycle of IoT-based applications.

In [12], a brief summary of the evolution of the Internet of Things with an emphasis on security vulnerabilities and countermeasures is proposed. Several innovative approaches to enhancing IoT security are discussed in this study, which includes cloud-fog, lightweight algorithms, block chain, machine learning, SDN/NFV, PUF, and neural networks. A discussion of cybersecurity issues such as privacy concerns, limited resources, vulnerabilities, trust management, access control, and several lightweight cryptographic techniques is provided in this work.

It is discussed in [13] how DDoS assaults inflict substantial harm to an existing system and how available solutions are utilised to fight these attacks. It also looks at resource limits in the context of resource-constrained devices and how to overcome them.

[14], proposes the unique taxonomy for IoT vulnerabilities, attacks and threats, security impacts on IoT and research impact related to security on IoT. The research contributions were discussed, covering several security issues of the IoT paradigm. This paper elaborates on the IoT vulnerabilities, Taxonomy Overview, Layers of IoT.

[15], elaborates the effects of security and privacy for some IoT features and available research challenges to be solved. This article provides up-to-date information on a variety of industries and highlights the most recent Internet of Things security research as well as how IoT aspects influence existing security research.

A simple and successful model for lightweight cipher performance measurements was devised in [16]. The devices can encrypt communications in low-energy mode using this paradigm. The algorithm balanced the encryption throughput, energy, and execution time. Their next task will be to keep an eye on unusual behaviour in the gadgets.

In [17], the authors introduced a new Fuzzy with Black Widow for cluster the query solution and Spider Monkey Optimization Algorithms query optimization. This proposed model solve privacy preserving in crowdsourcing for minimizing the cost and latency effectively. This model expresses optimal communication and computation time efficiency.

The authors in [18], presented a HCPDS (Hybrid Chaotic Particle Dragonfly Swarm Algorithm) based system for detection of DDoS attacks in VANETs. In the HCPDS approach, the dragonfly algorithm is added for enhancing the PSO updating algorithm and also, the performance metrics like processing delay, network accuracy, false alarm detection ratio and communication overhead are evaluated.

The research article [19] authors presented a hybrid crypto model for satisfying privacy and security for the cloud data. They use Elliptic Curve Cryptography (ECC) with Homomorphic for encryption. The process includes first implementing ECC at level 1 then implementing Homomorphic Algorithm. To provide more security the encryption process is done at 2 levels. After that the cipher text has been stored in the cloud. However, the implementation of this model seeks high cost.

Apart from these literature survey, our contribution of this article has summarized below,

- Our research addresses the important of the lightweight block cipher for IoT Security for providing better security without affecting the resource constraint.
- A comparison of the performance of different lightweight block cipher algorithms based on latency, throughput, chip area, security, power, and energy efficiency.
- Based on several assaults, cryptanalysis of some lightweight block cipher algorithms

3 Lightweight Block Cipher Algorithms

The majority of IoT devices have limited storage size, are small in size, and have limited resources. The following are the significant obstacles to implementing traditional cryptography algorithms:

- Limited memory
- Reduced battery power
- Real time response

RFID tags, sensors, contactless smart cards, and healthcare equipment need a lightweight cryptography method or protocol for deployment in limited contexts [20]. Hundreds of billions of heterogeneous lightweight gadgets will be connected in the future.

Lightweight cryptography is a specialty of cryptography that focuses on the optimization of encryption algorithms based on the fundamental cryptographic primitives such that they can run on small devices that have limited resources [21]. There are several types of cryptography, including:

Lightweight Block Cipher: Lightweight block cipher focuses on implementing a lightweight version of existing block ciphers and inventing new and secure cipher specifically for memory constrained devices [22]. There are two types of designs for block ciphers: Substitution-Permutation Networks and Feistel Networks.

Lightweight Stream Cipher: Lightweight stream cipher generates a key for a input data with a secret key and initialization vector. A stream cipher with low battery power low computational complexity and high level of security is called as lightweight stream cipher. Chacha and FSR (Feedback shift register)-based designs are two famous lightweight stream ciphers [21].

In order to accomplish encryption, Block Cipher makes use of Electronic Code Block (ECB) and the Cipher Block Chaining (CBC), whereas Stream Cipher makes

use of Output Feedback (OFB) and Cipher Feed-back (CFB). On the other hand, decryption of the block cipher is more difficult than decryption of the stream cipher. The implementation of the block cipher is carried out using the Feistel cipher, while the stream cipher is carried out using the Vernam cipher. The structure of a block cipher is straightforward, whereas the structure of a stream cipher is more involved.

The National Institute of Standards and Technology (NIST) has announced that FIPS 197, The Advanced Encryption Standard (AES), has been approved. The United States Government has full confidence in AES, which results in a very high level of security. In addition, it employs 192-bit and 256-bit keys for its heavy-duty encryption function [26].

When developing cryptographic algorithms for extremely low-resource devices, it is important to consider design criteria that are distinct from those used for more common devices. Despite the fact that no specific criteria for lightweight cryptography algorithms have been established, the features typically include any one or more of the following:

- the lowest feasible implementation cost
- the highest possible level of security
- the smallest size of the memory necessary for hardware implementation
- the low computing capability of microprocessors or microcontrollers

The length of the key is related to the cost and security of cryptographic algorithms, while the number of rounds in encryption provides security, performance, and hardware architecture for cryptographic algorithms that use these algorithms as well as for other algorithms that don't use cryptographic algorithms. Key length is also related to the cost of implementing cryptographic algorithms [50].

Cryptography includes two basic characteristics: To make the cipher more intriguing, Claude Shannon introduced confusion and diffusion. The link between cipher text and key is as complicated as employing a substitution box because of the ambiguity. Diffusion, on the other hand, indicates that plaintext merely generates cipher text. If a single letter in the plaintext is changed, the cipher text is completely transformed. Stream ciphers rely primarily on the property of confusion, whereas block ciphers incorporate both confusion and diffusion principles [23].

For the reasons stated above, a block cipher is favoured over a stream cipher. The focus of this research paper is on lightweight block cipher methods. Symmetric block cipher designed by the structures categorized by Feistel Network, Substitution-Permutation Network, Add-Rotate-XOR, General Feistel Network, Non-Linear Feedback Shift Register, Hybrid. Table 1 shows the structure-based categorization of several algorithms [4].

Table 1 Structure wise category of algorithms

Structure type	Description	Algorithms
SPN	The data is tweaked with the use of a set of substitution boxes and a permutation table, and the procedure is repeated defined no. of rounds	AES, Present, SKINNY, mCrypton, Iceberg, SAFER, SHARK, Square, Prince, Klein
FN	Divides the input into equal halves and applies diffusion to one half in each round	DESL/DESXL, TEA, Simon, SEA, Lblock, ITUbee, RC2, Skipjack
GFN	Splits the input data into a number of sub-blocks, with each pair of sub-blocks being applied to the Feistel function as a result of this division	CLEFIA, Piccolo, Twis, Twine, HISEC
ARX	For generating ciphertext, it combines the operations of addition, rotation, and XOR	Speck, IDEA, HIGHT, BEST-1, LEA
NLFSR	Current state is obtained from earlier state in both stream and block ciphers	KeeLoq, KATAN/KTANTAN, Halka
Hybrid	Any three types of ciphers or combination of block and stream cipher combined	Hummingbird, Present-GRP

4 Performance Metrics and Cryptanalysis

In this part of the article, we will evaluate and contrast a large number of lightweight cryptographic techniques based on a predetermined set of performance standards. In this part, we will evaluate a large number of lightweight cryptographic algorithms by contrasting them against a predetermined set of performance standards. In this part, we will evaluate a large number of lightweight cryptographic algorithms by contrasting them against a predetermined set of performance goals. The performance metrics details as follows,

- Security performance: It is measured in bits and can be assessed against several forms of assaults. The key size that measured in bits is the deciding factor for the security level
- Throughput: It is evaluated in bits and can be weighed against a variety of potential dangers. The amount of security is proportional to the key length, which is measured in bits. If it is at the maximum, then it is satisfactory. It is possible to calculate it using the formula T = (B F)/N, where T is throughput, B is the amount of data in bits that is encrypted or decrypted, F denoted as frequency, and N is the number of cycles take place in each block [3].

  If any security attack occurs, the receiver can compute throughput from the security constraints and the channel states during the reception of the frame. The link adaptive scheme can be presented for the optimization between security and throughput.

- Latency: measured in terms of the number of clock cycles needed to process a single block of plaintext during encryption and cypher text during decryption. It is the equivalent of seconds. It is denoted by the equation L = k tcycle, in which k represents the number of clock cycles required to compute one block of cypher text and tcycle represents the number of clock cycles required to compute one block of cypher text.

  Latency can be measured in two ways: i) One Way Latency is the time taken for data to travel in one direction and it is used to diagnose the network problem. ii) Two-Way Latency is the time taken for the round-trip time for the data packet and it used to calculate Mean Opinion Score. It also called as round-trip latency.
- Power and energy consumption: The power and energy consumption of 8-bit and 16-bit microprocessors that operate at 4 MHz frequency with 0.9 V voltage are measured by taking the average power of the processors into consideration [3].

$$\text{Energy [J]} = \big(\text{Latency}\left[\text{number of cycles per block}\right] * \text{Power [W]}\big)/\text{block size [bits]} \quad (1)$$

  The quantity of clock cycles needed to encrypt a block, the amount of power used by the hardware or software implementation, and the number of bits contained in a block of data are all described in terms of latency and power respectively.
- Efficiency: It indicates a balance achieved between performance and implementation size.

$$\text{Efficiency} = \text{Throughput}\left[\text{Kbps}\right]/\text{Code size [KB]} \quad (2)$$

4.1 Comparative Analysis

Over the past few years, many different types of work have been done to compare various analyses in order to determine which one is the best suitable for providing security to resource-constrained Internet of Things devices.

To optimize the encryption algorithm, we need to compare the algorithms based upon their speed, efficiency, performance and how it is to be secure the protected data against attacks. There are so many efficient new edition encryption algorithms available to decrease the security threats. The various optimization algorithms like Binary Particle Swarm Optimization, Swarm Intelligence Based Approach, Ant Colony Optimization are used for encryption algorithm to improve the performance and security.

These investigations are based on a number of trials carried out on several platforms, including NXP, AVR, and ARM microcontrollers [23]. We consider some popular lightweight block cipher algorithms and figure out their latency, throughput, security, power, and energy efficiency. The software implementation on an 8/16/32 bit microcontroller is summarised in Table 2.

Table 2 Performance metrics analysis of various algorithm

lwc algorithms	Key size	Block size	No. of. rounds	Rom	Ram	Latency	Energy	Through put	S/W efficiency
AES [26] [27]	128, 192, 256	128	10,12,14	918	0	4192	16.7	122	132.9
KLEIN [37]	64, 80, 96	64	12,16,20	2980	50	7901	10.6	32.4	10.87
LED [41]	64,128	64	32,48	2164	368	35,161	-	7.28	3.36
NOEKEON [47]	128	128	16	364	32	23,517	95.9	21.7	59.62
PRIDE [28]	128	64	20	266	0	1514	6	169	635.34
mCrypton [42]	64,96,128	64	12	1076	28	16,457	68	15.5	14.41
PRINCE [35]	128	64	12	1108	0	3614	14.4	70.8	63.9
ITUbee [30]	80	80	5	716	0	2607	10.4	122.7	171.37
SPECK [24]	64 72/94 96/128 96/144 128/192 156	32 48 64 96 128	22 22/23 26/27 28/29 32/33/34	134	0	408	1.6	750.5	3511.19
SIMON [24]	64 72/96 96/128 96/144 128/192/256	32 48 64 96 128	32 36 42/44 52/54 68/69/72	170	0	594	2.3	323	1900
HIGHT [36]	128	64	32	5718	47	6377	25.5	40.14	7.02
GOST [52]	256	64	32	4748	190	10,240	13.8	25	5.27
PICCOLO [52]	128,80	64	25,31	966	70	21,448	28.9	11.93	12.35
LEA [31]	128/192/256	128	24/28/32	590	32	5231	-	97.8	165.76

(continued)

Table 2 (continued)

lwc algorithms	Key size	Block size	No. of. rounds	Rom	Ram	Latency	Energy	Through put	S/W efficiency
CLEFIA [33]	128/192/256	128	18,28,26	1920	78	3646	4.9	140.42	73.14
LBLOCK [45]	80	64	32	976	58	18,988	25.6	13.48	13.81
SEA [38]	96	96	93	426	24	41,604	173.7	9.2	21.6
TEA [39]	128	64	30	648	24	7408	30.3	34.5	53.24
BORON	80/128	64	25	140	0	500	2.3	350.25	2344.20

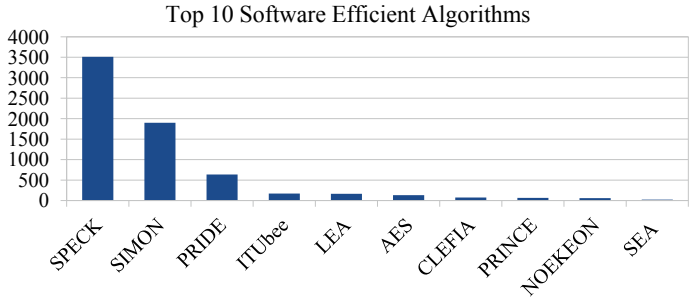

Fig. 1 Software efficient algorithms

Based upon the Fig. 1, software efficiency of various algorithms, we conclude that Speck is the best solution for IoT security. Memory power for various LWC algorithms has been shown in the Fig. 2. Again, Speck has won the competition. Other essential metrics like latency, throughput is shown in the Fig. 3, Fig. 4. Again, Speck has the lowest latency and high throughput.

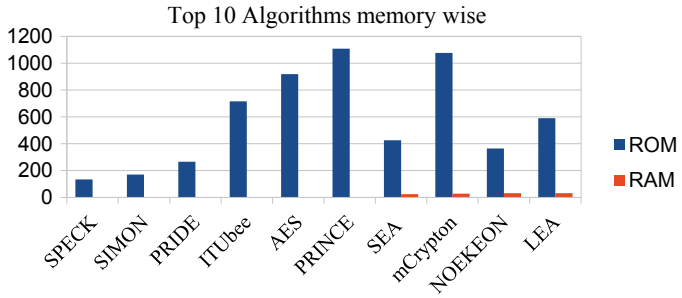

Fig. 2 Memory wise algorithms

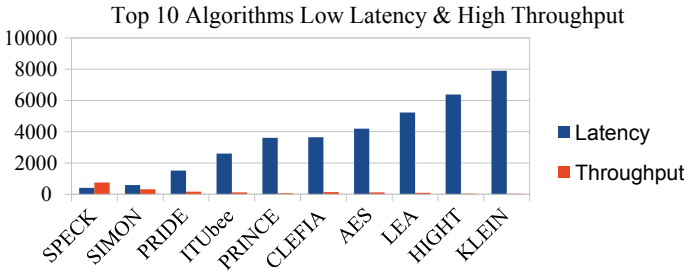

Fig. 3 Low latency and high throughput algorithms

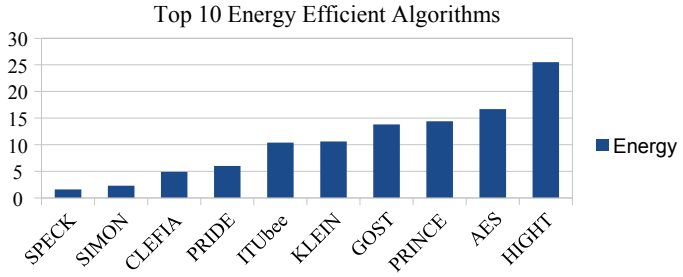

Fig. 4 Energy efficient algorithms

Table 3 Types of cryptanalysis

Cryptanalysis	Description
Differential cryptanalysis	Analysis of output against various types of inputs
Linear cryptanalysis	Experimenting with plaintext, ciphertext, and the secret key in a linear way
Integral cryptanalysis	It's especially useful for block ciphers that use the Substitution and Permutation Network
Algebraic cryptanalysis	Based upon solving the mathematical equation

4.2 Cryptanalysis of LWC Algorithms

Security is one of the most important factors, along with performance and cost. Every LWC has a certain amount of assault resistance. However, in order to acquire our information, the attacker devises a new type of assault. As a result, examining the security element of algorithms is critical. We can get the information of security efficiency through cryptanalysis. The Table 3 depicts the many types of cryptanalysis.

These cryptanalysis employ on Cipher text Only, Known Plaintext, Chosen Plaintext, and Chosen Cipher text with Man-In-The-Middle, Brute Force, and Side Channel Attacks. Related Key Attack, Boomerang Attack, Biclique Attack, and Algebraic Attack are some of the other attacks [22]. In Table 4 the various popular algorithms are analysed based upon varous attacks and also covered merits of those algorithms discussed.

5 Research Challenges and Research Gap

The main challenge in the IoT environment is security. It has a high demand in Confidentiality, Integrity, Availability, and Authentication. Many researchers depict that cryptographic algorithms will be effective to provide security. The problem of cryptographic algorithms requires large resource allocation, large memory usage,

Table 4 Cryptanalysis of popular algorithms

Ref No	LWBC Algorithm	Merits	Attacks/Analysis
[25]	SIMON	Provides support for many key sizes and executes effectively on hardware	Attacks based on differential faults and assaults on reduced version
[25]	SPECK	Performs better in software, high security	Key recovery, Boomerang attack
[27]	AES	Excellent Security, Flexible	Related key attack, Boomerang, Biclique
[28]	PRIDE	Low Latency and low energy consumption	Differential Related Key attack on 17^{th} round,
[29]	PRESENT	Ultra-Lightweight cipher, Energy Efficient	Attacks such as truncated differential cryptanalysis, integral bottleneck assaults, and statistical saturation attacks
[30]	ITUbee	It provides 80-bit security against related key models as well as single level attack types. algorithm aimed toward software	Self-similarity cryptanalysis on 8-round
[32]	LEA	Fast encryption on common processors, small code size and low power	Boomerang attack on $15,16,17^{th}$ round, truncated differential attack
[34]	CLEFIA	Efficient encryption on a variety of processors, a compact code footprint, and low power consumption	In the 10th round, an attack on key recovery and saturation cryptanalysis
[35]	PRINCE	Low Latency in hardware, low energy consumption	Key recovery attack and truncated differential attack on 7^{th} round
[36]	HIGHT	Ultra lightweight, offers exceptional security, and is suitable for RFID tagging	Impossible differential attack on 27^{th} round, Integral attack is on 9th round
[37]	Klein	High software-based performance,	Biclique attack of the full round, key recovery attack up to 8^{th} round
[38]	SEA	Low-cost encryption, low memory, small code size,	Slide attack, Related key attack, algebraic attack
[42]	mCrypton	Cost and Energy Efficient	Related Key Attack
[48–50]	BORON	Ultra-Lightweight Cipher, Secure against DPA attack	Key Recovery attack on 8^{th} round, Related key attack on 10^{th} round

high battery power since IoT is a resource constrained environment. NIST standards represent AES as the most competitive block cipher algorithm among other algorithms. But it has a larger block size, larger rounds, and S-Box. Considering memory and computational power the traditional block cipher algorithm is not suitable for the IoT environment.

Based upon these challenges, we came to know some problem,

- Confusion is one of the two fundamental features of cryptographic algorithms, and it can be created by the use of the S-Box method. Nonetheless, S-Box takes a significant investment of time and resources.
- Larger block sizes like 128 bits, 256 bits are slowing down the computational power.
- Cryptographic algorithms are only as secure as their keys, and the key plays the most critical role in this. The goal is to produce random subkeys from the starting key for all rounds while utilising the same initial key as the first round.
- Some cryptographic algorithms have many rounds for ensuring security. But increasing the no. of rounds will affect the performance and cost. So, the problem is how to reduce the no of rounds without affecting security.

6 Future Work

To provide better security, we should think about those comparative statements and performance analysis. From the study, performance comparison and cryptanalysis we conclude that SPECK and AES have better security and limited Resource consuming, higher software efficiency. According to cryptanalysis this algorithm has some attacks. To overcome this problem, we plan to implement a reduced version of SPECK named SPECK-R. To enhance the security of this algorithm, we plan to introduce a new key scheduling algorithm. Additionally, research is going on for authentication purposes.

7 Conclusion

Nowadays IoT has become an important one in our day-to-day life. There is plenty of sensitive information that has been shared among the devices. There are many challenges for securing the IoT environment. The main security goals are Confidentiality, Integrity, and Availability. Lightweight cryptography algorithms are much better compared with traditional cryptographic algorithms since IoT devices are resource-constrained devices. Based on performance and cryptanalysis measures, we've analysed the various methods in this research study. Research difficulties and gaps in research have been addressed in this work. With a new ultra-lightweight block cipher approach to be launched in the not-too-distant future, it will be possible

to substantially increase IoT device security while still consuming little power and memory.

References

1. Dhanda SS, Singh B, Jindal P (2020) LightWeight cryptography - a solution to secure IoT. Wirel Pers Commun 112:1947–1980
2. Sleem L, Couturie R (2020) Speck-R: an ultra light-weight cryptographic scheme for internet of things. Multimedia Tools Appl 80:17067–17102
3. Iqbal W, Abbas H, Daneshmand M, Rauf B, Abbas Y (2020) An in-depth analysis of IoT security requirements, challenges and their countermeasures via software defined security. IEEE int Things j 7:10250–10276
4. Thakor V, Razzaque MA, Khandaker M (2020) Lightweight cryptography for IoT: a state-of-the-art
5. Khanam S, Ahmedy IB, Idris MYI, Jawarad MH, Sabri AQB (2020) A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things. IEEE Access 8:219709–219743
6. Aziz A, Singh K (2019) Lightweight security scheme for internet of thing. Springer Science
7. Thakori VA, Razzaque MA, Khandaker MRA (2021) Lightweight cryptography algorithms for resource-constrained IoT devices: a review, comparison and research opportunitie. IEEE Access 9:28177–28193
8. Panahi P, Bayılmış C, Çavuşoğlu U, Kaçar S (2021) Performance evaluation of lightweight encryption algorithms for IoT-based applications. Springer, Arabian Journal For Science And Engineering
9. RanaS Hossain S, Shoun HI, Kashem MA (2018) An effective lightweight cryptographicalgorithm to secure resource-constrained devices. (IJACSA) Int J Adv ComputSci Appl 9(11):267–275
10. PoojariA Nagesh H, Kiran KVG, Sangharama RC (2020) A novel key scheduling algorithmfor lightweight cryptographic applications. Int J Adv Trends Comput Sci Eng 9:682–684
11. Rao V, Prema KV (2020) A review on lightweight cryptography for internet of things based applications. J Am Intell Human Comput 12:8835–8857. https://doi.org/10.1007/s12652-020-02672-x
12. Ali M A Abuagoub (2019) IoT security evolution: challenges and countermeasures review. Int J Commun Netw Inf Secur (IJCNIS)
13. Al-Hadhrami Y, Hussain FK (2021) DDoS attacks in IoT networks: a comprehensive systematic literature review. World Wide Web 24:971–1001. https://doi.org/10.1007/s11280-020-00855-2
14. Neshenko N, Bou-Harb E, Crichigno J, Kaddoum G, Ghani N (2019) Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet scale IoT exploitations. IEEE Commun Surv Tutor
15. Zhou W, Jia Y, Peng A, Zhang Y, Lia P (2018) The effect of IoT new features on security and privacy: new threats, existing solutions and challenges yet to be solved. IEEE Int Things J
16. Bassam JM, Hayajneh T (2018) Light weight block ciphers for IoT: energy optimization and survivability techniques. IEEE Access, Special Section on Survivability Strategies for Emerging Wireless Networks
17. Prabakeran S (2021) Fuzzy with black widow and spider monkey optimization for privacy-preserving-based crowdsourcing system. Soft Computing
18. Prabakeran S, Sethukarasi T (2020) Optimal solution for malicious node detection and prevention using hybrid chaotic particle dragonfly swarm algorithm in VANETs. Wireless Networks
19. Saravanan P, Kumar RH, Arvind T, Narayanan B (2019) Hybrid crypto system using homomorphic encryption and elliptic curve cryptography. i-Manager's J Comput Sci

20. Bansod G, Raval N, Pisharoty N (2015) Implementation of a new lightweight encryption design for embedded security. IEEE Trans. Inf. Forensics Secur 10(1):142–151
21. Philip MA, Vaithiyanathan (2018) A survey on lightweight block Ciphers for IoT Devices. In: Proceedings IEEE region conference, October 2018. pp 1784–1789
22. Hatzivasilis G, Fysarakis K, Papaefstathiou I, Manifavas C (2018) A review of lightweight block ciphers. J Cryptograph Eng 8(2):141184
23. Dinu D, Biryukov A, Groÿschädl J, Khovratovich D, Corre YL, Perrin L (2015) Felics fair evaluation of lightweight cryptographic systems. In: Proceedings NIST Workshop Light Cryptograph, p 128
24. Beaulieu R, Shors D, Smith J, Treatman-Clark S, Weeks B, Wingers L (2015) The simon and speck: block ciphers for internet of things. DAC 2015, 07–11 June 2015. San Francisco
25. Abed F, List E, Lucks S, Wenzel J (2015) Differential cryptanalysis of round-reduced Simon and Speck. International Association of Cryptologic Research
26. Pub N (2001) 197: Advanced encryption standard (AES). Federal Inf Process Standards 197(441):0311
27. Verma A, Kaur S, Chhabra B (2016) Improvement in the performance and security of advanced encryption standard using AES algorithm and comparison with blowfish. Int Res J Eng Technol (IRJET) 03(10):10–14
28. Albrecht MR, Driessen B, Kavun EB, Leander G, Paar C, Yalçn T (2014) Block Ciphers – Focus on the Linear Layer (feat. PRIDE). In: Garay JA, Gennaro R (eds) Advances in Cryptology – CRYPTO 2014, vol 8616. Lecture Notes in Computer Science. Springer, Heidelberg, pp 57–76. https://doi.org/10.1007/978-3-662-44371-2_4
29. Z'aba MR, Jamil N, Rusli ME, Jamaludin MZ, Yasir AAM (2014) I-PRESENT: An involutive lightweight block cipher. J Inf Secur 2014:25
30. Karakoç F, Demirci H, Harmanc AE (2013) ITUbee: A software oriented lightweight block cipher. In: Avoine G, Kara O (eds) Lightweight Cryptography for Security and Privacy, vol 8162. Lecture Notes in Computer Science. Springer, Heidelberg, pp 16–27. https://doi.org/10.1007/978-3-642-40392-7_2
31. Hong D, Lee J-K, Kim D-C, Kwon D, Ryu KH, Lee D-G (2014) LEA: A 128-bit block cipher for fast encryption on common processors. In: Kim Y, Lee H, Perrig A (eds) Information Security Applications, vol 8267. Lecture Notes in Computer Science. Springer, Cham, pp 3–27. https://doi.org/10.1007/978-3-319-05149-9_1
32. Kim Y, Yoon H (2014) First experimental result of power analysis attacks on a FPGA implementation of LEA. Proc IACR 2014:999
33. Pyrgas L, Kitsos P (2019) A very compact architecture of CLEFIA block cipher for secure IoT systems. Euromicro Conference on Digital System Design (DSD)
34. Tezcan C (2010) The improbable differential attack: Cryptanalysis of reduced round CLEFIA. In: Gong G, Gupta KC (eds) Progress in Cryptology - INDOCRYPT 2010, vol 6498. Lecture Notes in Computer Science. Springer, Heidelberg, pp 197–209. https://doi.org/10.1007/978-3-642-17401-8_15
35. Borghoff J, Canteaut A, Güneysu T, Kavun EB, Knezevic M, Knudsen LR, Leander G, Nikov V, Paar C, Rechberger C, Rombouts P, Thomsen SS, Yalç T (2012) PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications. In: Wang X, Sako K (eds) Advances in Cryptology – ASIACRYPT 2012, vol 7658. Lecture Notes in Computer Science. Springer, Heidelberg, pp 208–225. https://doi.org/10.1007/978-3-642-34961-4_14
36. Hong D, Sung J, Hong S, Lim J, Lee S, Koo B-S, Lee C, Chang D, Lee J, Jeong K, Kim H, Kim J, Chee S (2006) Hight: A new block cipher suitable for low-resource device. In: Goubin L, Matsui M (eds) Cryptographic Hardware and Embedded Systems - CHES 2006, vol 4249. Lecture Notes in Computer Science. Springer, Heidelberg, pp 46–59. https://doi.org/10.1007/11894063_4
37. Gong Z, Nikova S, Law YW (2012) KLEIN: A new family of lightweight block ciphers. In: Juels A, Paar C (eds) RFID. Security and Privacy, vol 7055. Lecture Notes in Computer Science. Springer, Heidelberg, pp 1–18. https://doi.org/10.1007/978-3-642-25286-0_1

38. Standaert F-X, Piret G, Gershenfeld N, Quisquater J-J (2006) SEA: A scalable encryption algorithm for small embedded applications. In: Domingo-Ferrer J, Posegga J, Schreckling D (eds) Smart Card Research and Advanced Applications, vol 3928. Lecture Notes in Computer Science. Springer, Heidelberg, pp 222–236. https://doi.org/10.1007/11733447_16
39. Andrews B, Chapman S, Dearstyne S (2020) Tiny encryption algorithm (TEA) cryptography 4005.705. 01 graduate team ACD _nal report, Rochester Inst. Technol., Rochester, NY, USA, Tech. Rep. 33695183. https://www.coursehero.com/_le/33695183/TEApdf/
40. Sekar G, Mouha N, Velichkov V, Preneel B (2011) "Meet-in-the-Middle Attacks on Reduced-Round XTEA", The Cryptographers' Track at the RSA Conference 2011. CA, USA, San Francisco
41. Guo J, Peyrin T, Poschmann A, Robshaw M (2011) The LED block cipher. In: Preneel B, Takagi T (eds) Cryptographic Hardware and Embedded Systems – CHES 2011, vol 6917. Lecture Notes in Computer Science. Springer, Heidelberg, pp 326–341. https://doi.org/10.1007/978-3-642-23951-9_22
42. Lim CH, Korkishko T (2006) mCrypton – A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors. In: Song J-S, Kwon T, Yung M (eds) Information Security Applications, vol 3786. Lecture Notes in Computer Science. Springer, Heidelberg, pp 243–258. https://doi.org/10.1007/11604938_19
43. Standaert F-X, Piret G, Quisquater J-J(2003) Cryptanalysis of block ciphers: a survey. UCL Crypto Group Laboratoire de Microelectronique Universite Catholique de Louvain
44. Mala H, Dakhilalian M, Shakiba M (2011) Cryptanalysis of mCrypton—A lightweight block cipher for security of RFID tags and sensors. Int J Commun Syst
45. Wu W, Zhang L (2011) LBlock: A lightweight block cipher. In: Lopez J, Tsudik G (eds) Applied Cryptography and Network Security, vol 6715. Lecture Notes in Computer Science. Springer, Heidelberg, pp 327–344. https://doi.org/10.1007/978-3-642-21554-4_19
46. Knudsen L, Leander G, Poschmann A, Robshaw MJB (2010) PRINTcipher: A Block Cipher for IC-Printing. In: Mangard S, Standaert F-X (eds) Cryptographic Hardware and Embedded Systems, CHES 2010, vol 6225. Lecture Notes in Computer Science. Springer, Heidelberg, pp 16–32. https://doi.org/10.1007/978-3-642-15031-9_2
47. Daemen J, Peeters M, Assche G, Rijmen V (2000) The Noekeon block cipher. In Proceedings 1st Open NESSIE Workshop pp 1–5
48. Bansod G, Pisharoty N, Patil A (2013) BORON: an ultra-lightweight and low power encryption design for pervasive computing. Front Inf Technol Electron Eng 18:317–331
49. Liang H, Wang M (2019) Cryptanalysis of the lightweight block cipher BORON. Secur Commun Netw volume 2019, article ID 7862738
50. Teha JS, Thama LJ, Jamilc N, Yapd W-S (2021) New differential cryptanalysis results for the lightweight block cipher BORON. J Inf Secur Appl
51. Alizadeh M, Salleh M, Zamani M, Shayan J, Karamizadeh S (2015) Security and performance evaluation of lightweight cryptographic algorithms in RFID. Recent Researches in Communications and Computers
52. Aldabbagh SSM, Fakhri I, Shaikhli T, Sulaiman AG (2016) Lightweight Block Cipher Algorithms: Review Paper. In: International Journal of Enhanced Research in Science, Technology & Engineering, vol 5 issue 5, ISSN: 2319–7463
53. Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B (2019) A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access 7:5–10
54. Prabakaran S (2021) Pulmonary disease diagnosis using African vulture optimized weighted support vector machine approach. International Journal of Imaging Systems and Technology (IMA)
55. Indumathi V, Prabakeran S (2021) A Comparative Analysis on Sensor-Based Human Activity Recognition Using Various Deep Learning Techniques. In: Pandian AP, Fernando X, Islam SMS (eds) Computer Networks, Big Data and IoT, vol 66. Lecture Notes on Data Engineering and Communications Technologies. Springer, Singapore, pp 919–938. https://doi.org/10.1007/978-981-16-0965-7_70

56. Prabakeran S (2021) Women's mental health chatbot using seq2seq with attention. Turkish J Comput Math Educ 12(10):919–938
57. Saravanan P, Sethukarasi T, Indumathi V (2018) An efficient software defined network based cooperative scheme for mitigation of distributed denial of service (DDoS) attacks. J Comput Theor Nanosci 15:2221–2226
58. Saravanan P, Sethukarasi T, Indumathi V (2018) Authentic novel trust propagation model with deceptive recommendation penalty scheme for distributed denial of service attacks. J Comput Theor Nanosci 15:2383–2389
59. Saravanan P, Sekar S, Kulam S, Selvaraj S (2018) An automatic helmet detection and penalty system using image descriptors and classifiers. J Comput Theor Nanosci 15:2245–2250
60. Murugeshwari B, Sudharson K, Panimalar SP, Shanmugapriya M, Abinaya M (2020) SAFE – secure authentication in federated environment using CEG key code (A Novel Method to Enhance Cloud Security). The Mattingley Publishing Co, Inc
61. Chatterjee R, Chakraborty R, Mondal JK (2019) Design of lightweight cryptographic model for end-to-end encryption in IoT domain. IRO J Sustain Wireless Syst 1(4):215–224
62. Dhaya R (2021) Light weight CNN based robust image watermarking scheme for security. J Inf Technol Digital World 3(2):118–132