Asia-pacific Journal of Convergent Research Interchange
Vol.10, No.1, January 31 (2024), pp.49-59
http://dx.doi.org/10.47116/apjcri.2024.01.05

A Study on Impact of Lightweight Cryptographic Systems on Internet of Things-Based Applications

Tai-hoon Kim[1]

[1] *Professor, School of Electrical and Computer Engineering, Yeosu Campus, Chonnam National University, Republic of Korea, taihoonn@chonnam.ac.kr*

Abstract: The Internet of Things (IoT) has become an integral part of people's daily lives with various applications such as smart homes, wearables, and industrial automation. However, these devices are often resource-constrained regarding computing power, memory, and energy. This makes deploying traditional cryptographic systems challenging, as they require significant computational resources and can lead to significant power consumption. To address this challenge, lightweight cryptographic systems have been developed that balance security and resource efficiency. This paper provides an overview of some of the most promising light cryptographic systems for IoT applications, including symmetric-key ciphers, hash functions, message authentication codes and public-key cryptosystems. The design principles and security properties of these systems and their practicality for IoT devices were discussed. The challenges associated with deploying lightweight cryptographic systems were also examined,mpotential solutions were proposed. Overall, this paper provides a comprehensive overview of impact of light cryptographic systems to IoT devices and its applications which aims to guide developers and researchers in selecting appropriate cryptographic keys for their IoT applications.

Keywords: Internet of Things(IoT), Cryptographic, Lightweight, Cyber Security, Security, IoT devices

1. Introduction

The Internet of Things (IoT) refers to the network of physical devices, vehicles, home appliances and other items embedded with sensors, software, and connectivity. These devices can collect and exchange data with other connected devices and systems over the internet[1]. The IoT has enabled a wide range of applications, including smart homes, wearables, healthcare, industrial automation, and more. However, the proliferation of IoT devices has also introduced new security challenges. These devices are often resource-constrained in terms of computing power, memory, and energy. Traditional cryptographic systems, which provide security by encrypting and decrypting messages, require significant computational resources and can lead to significant power consumption. As a result, the deployment of cryptographic systems on IoT devices has been challenging.

To address this challenge, lightweight cryptographic systems have been developed, which offer a balance between security and resource efficiency. These systems are designed to be computationally efficient and to consume minimal power. They are also designed to be resistant to attacks, ensuring that the data transmitted between IoT devices is secure[2]. There are several types of lightweight cryptographic systems that are applicable to IoT devices, including symmetric-key ciphers, hash functions, message authentication codes, and public-key cryptosystems. Symmetric-key ciphers are algorithms that use the same secret key to encrypt and decrypt messages. Hash functions are one-way

Received: September 18, 2023; 1st Review Result: October 20, 2023; Accepted: December 26, 2023

functions that map data of arbitrary size to a fixed-size output, which can be used for data integrity checks[3]. Message authentication codes are cryptographic primitives that provide data integrity and authenticity. Public-key cryptosystems are cryptographic systems that use a pair of keys, a public key, and a private key, to encrypt and decrypt messages.

The deployment of lightweight cryptographic systems on IoT devices is not without its challenges. The limited resources of these devices make it difficult to implement cryptographic algorithms that require significant computing power or memory. Additionally, there is a trade-off between security and resource efficiency, as more secure cryptographic systems often require more resources to implement. Finally, the diverse nature of IoT devices and applications means that there is no one-size-fits-all solution for deploying cryptographic systems on these devices[4]. Despite these challenges, lightweight cryptographic systems are an important tool for ensuring the security of IoT devices and applications. As the number of IoT devices continues to grow, it is essential that developers and researchers continue to develop and refine lightweight cryptographic systems that are practical and effective for use on these devices.

2. Related Work

McKay and Bassham[2] had discussed with a detailed report on lightweight cryptographic sensors and their advantages and disadvantages. They had provided a report on the lightweight cryptographic sensors and their working performance on various scenarios. They had presented the reports and results of their project entitled NIST. They had also discussed the plan for standardizing the algorithms for lightweight models. They had discussed many points regarding these lightweight cryptographic models which deals with various design requirements for the models to build and perform the operations. They had also decided to collect the feedback from the users and try to improve the performance of the algorithms they had developed for the same models in several applications and their performances.

Bogdanov and Knudsen[4] had discussed the working of a new model of AES block cipher. They had discussed in detail the need and usage of the new cipher block such that the performance can be monitored and can be improved further for the same models. The new proposed AES cipher block is going to be the source and choice for almost all types of users who are using the similar type of applications in the market and also in the research domain. The usage of this model works well in several cases and applications, but it also has some disadvantages. The proposed new cipher block is not being used mostly for the applications like the sensor networks and other RFID models. The reason for the development of this new cipher is that the need for advancement of both hardware and software are equally important and needed.

Leander and Paar[6] proposed DES lightweight new cipher block which was based on the previous cipher block DES. The current new cipher block works on the basis of S box which works on single repeated times which equals to eight. The designed special S box can be used for the previous models of cipher blocks and also to other blocks of similar S boxes. The newly designed cipher block is very strong on several types of serious attacks and some other common attacks. The implementation results on various scenarios and various models have given a clear performance dominance with respect to the previous models of the DES cipher blocks.

Xuanxia Yao[8] discussed in detail the IoT, which was an emerging and most promising technology being used by most people today. As the usage of these devices and technology growa, society is converting to the name of smart society or the smart devices. As these devices are used by the public in their daily lives, providing security to such devices is an important and key requirement from the manufacturers. As the technology is heterogeneous, providing security to the devices under this technology is a very challenging task. The authors developed a non-pairing unit called the ABE

scheme which works on elliptic curve cryptography which works to deal with the security and privacy issues on the devices working and connected with IoT based units. The results showed that the proposed model is working better in comparison with the previous models with respect to operational and development costs and efficiency of the models.

Singh[9] discussed the importance of IoT and its related block ciphers. The authors also diswcussed the latest technologies and the latest cipher blocks which were developed to improve the performance of the IoT based devices. They also discussed the hash functions and stream ciphers which play a key role in the development of various IoT based environmental devices. The authors analysed the performance of these proposed ciphers with several inputs and their resources like the size of the block, rounds in count and structure of the models, etc.

2.1 Research Gaps

While there has been significant progress in the development of lightweight cryptographic systems for the Internet of Things (IoT), there are still several research gaps that need to be addressed in order to fully secure IoT devices and applications. One research gaps is the need for standardized security protocols and frameworks for IoT devices. While there are many lightweight cryptographic systems available, there is no widely accepted standard for securing IoT devices. This lack of standardization can make it difficult for developers to implement secure systems, and can lead to interoperability issues between devices.

Another research gap is the need for lightweight key management systems for IoT devices[8]. Key management is a critical component of any cryptographic system, as it is responsible for securely generating, storing, and distributing keys. However, many key management systems are designed for more powerful devices and are not well-suited for IoT devices, which have limited resources. There is a need for lightweight key management systems that can provide secure key generation, storage, and distribution on resource-constrained devices. A third research gap is the need for lightweight cryptographic systems that can provide security in dynamic environments. IoT devices are often deployed in environments where network connectivity can be intermittent or unreliable, and where devices may be added or removed from the network frequently. Lightweight cryptographic systems that can provide security in these dynamic environments are needed.

Finally, there is a need for research on the trade-off between security and resource efficiency in lightweight cryptographic systems. While lightweight cryptographic systems are designed to be efficient, there is a trade-off between security and efficiency. As the level of security increases, the computational and memory requirements of the cryptographic system also increase. There is a need for research that can quantify this trade-off and provide guidelines for choosing the appropriate level of security for different IoT applications. Overall, there are still several research gaps that need to be addressed in the field of lightweight cryptographic systems for the IoT. Addressing these gaps will be critical for ensuring the security and privacy of IoT devices and applications.

2.2 Problem Description

One area of related work is the development of lightweight symmetric-key ciphers, which are algorithms that use the same secret key for both encryption and decryption. Examples of lightweight symmetric-key ciphers include SIMON, SPECK, and LEA[5]. These ciphers are designed to be computationally efficient and to have a small memory footprint, making them well-suited for deployment on IoT devices.

Another area of related work is the development of lightweight hash functions, which are one-way functions used for data integrity checks. Examples of lightweight hash functions include SipHash,

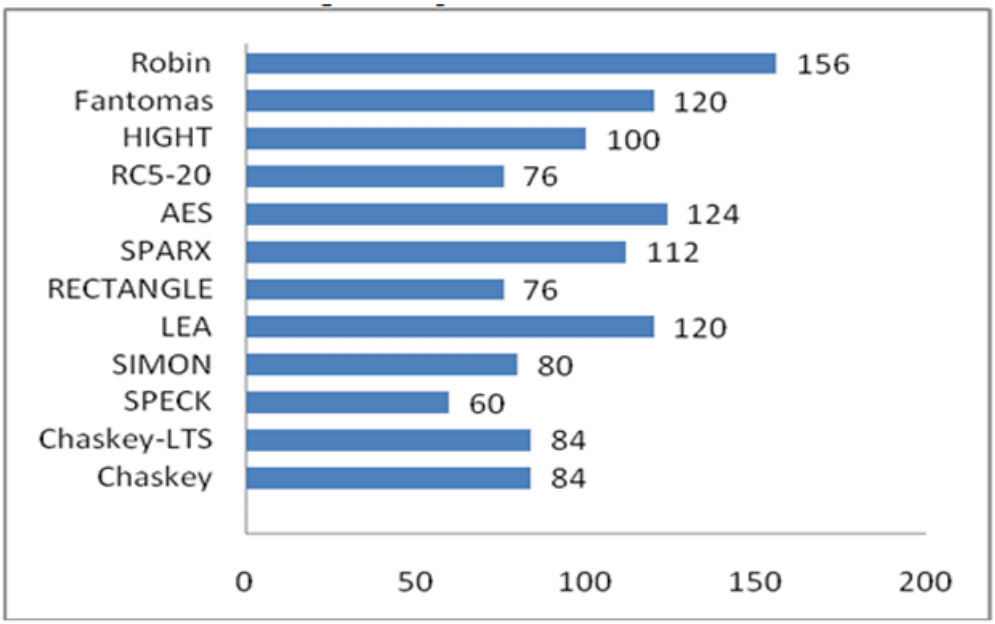
PHOTON, and Ascon-Hash. These hash functions are designed to be fast and secure, making them well-suited for IoT applications.

Research on lightweight message authentication codes (MACs)[6] is another area of related work. MACs are cryptographic primitives that provide data integrity and authenticity. Examples of lightweight MACs include Gimli-Hash-based MAC, Skinny-AEAD-MAC, and Poly1305. These MACs are designed to be computationally efficient and to have a small memory footprint, making them suitable for deployment on resource-constrained devices. Finally, there is related work on lightweight public-key cryptosystems, which are cryptographic systems that use a pair of keys, a public key, and a private key, to encrypt and decrypt messages. Examples of lightweight public-key cryptosystems include NTRU and FrodoKEM. These cryptosystems are designed to be computationally efficient and to have a small memory footprint, making them well-suited for deployment on IoT devices.

Overall, there is a significant amount of related work in the field of lightweight cryptographic systems for the IoT. Researchers and developers are actively working to design[7] and implement cryptographic primitives and protocols that are both efficient and secure for use in resource-constrained environments.

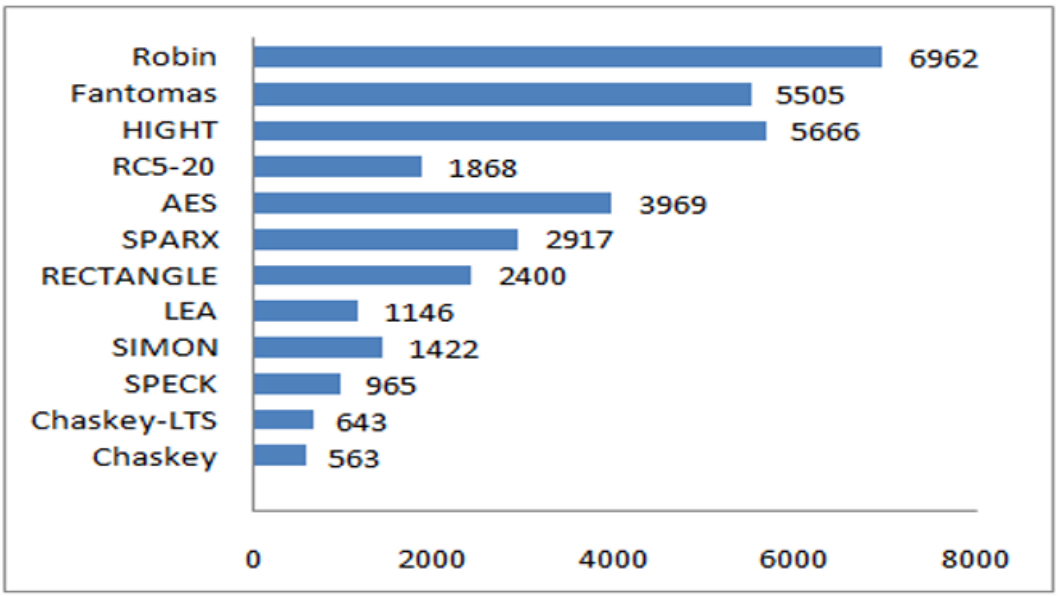
3. Materials and Methods

Lightweight cryptography, often known as LWC, is an area of cryptography that focuses on the creation of security protocols that are both effective and uncomplicated, with the goal of replacing more complicated and expensive options[4][10]. The idea behind lightweight alternatives is that they are speedier, need less memory, and have smaller key sizes than their heavier counterparts. This indicates that more lightweight systems can make do with a lower amount of resources than their more robust counterparts[9]. The size of the key, the size of the block, the code measures, the clock cycles, and many other factors are given precedence, but any lightweight solution may be used. In this study, in order to build a lightweight algorithm, it was important to make concessions in a number of different areas, including the speed of the technique, the performance requirements, and the level of cryptographic strength as shown in the [Fig. 1].



[Fig. 1] Showing the Comparision of the Code Size

It is essential to have an understanding of the effectiveness of lightweight block ciphers in order to achieve the optimum balance possible between cost, speed, and security. Lightweight ciphers are meant to be more efficient in terms of resources and processing power than their more resource-intensive counterparts, while still offering an appropriate level of security. Each encryption method was assessed according to how effectively it satisfies the requirements that have been laid forth. This section describes lightweight symmetric block ciphers[4] that are often built as software and are used by a large number of people. The FELICS scores for encrypting 128-bit messages in counter mode are shown in [Table 3], and the software-based lightweight block ciphers designed for the security of IoT devices are shown in the [Fig. 2].



[Fig. 2] Showing the Consumption of the RAM

It was possible to determine the code's length by looking at the machine's instruction set. Chaskey was the best option since it is recognized for quick thinking and has a smaller profile than the other options.

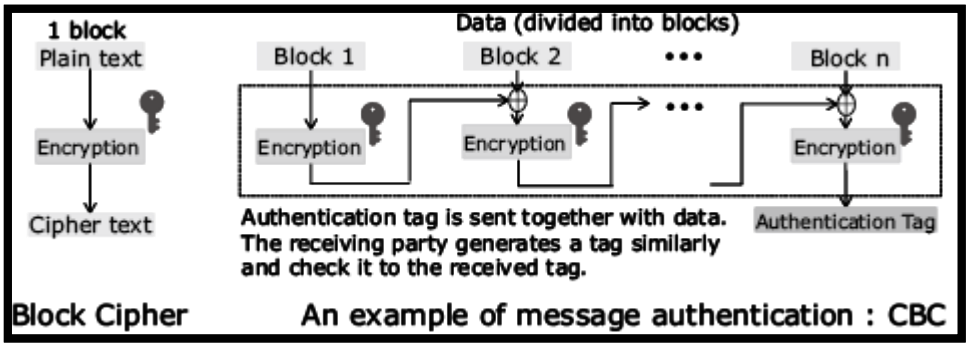
3.1 Proposed Model

The two primary categories of encryption are public key and symmetric key. In symmetric key cryptography, data is secured and decrypted using a single key. The data being processed undergoes verification procedures to ensure its authenticity and security. In the context of cryptographic systems, the use of public key cryptography, as opposed to private key cryptography, involves the utilization of a publicly available key for the encryption process, while a confidential key is employed for the decryption process. This significantly increases the difficulty of determining the secret key. Public key cryptography is used for the transmission of the secret key and digital signature in the context of symmetric key encryption, despite its much higher operational expenses. The lack of balance in public key encryption enables this possibility.

Private passwords may already be established in the control system of a plant or an automobile. The attainment of reliable and accurate data protection is contingent upon the use of symmetric key cryptography. In contrast, public key cryptography serves as a valuable tool for establishing secure communication channels with unfamiliar entities in a dynamic manner, such as when two vehicles engage in intercommunication. Acquiring public keys is comparatively more convenient than

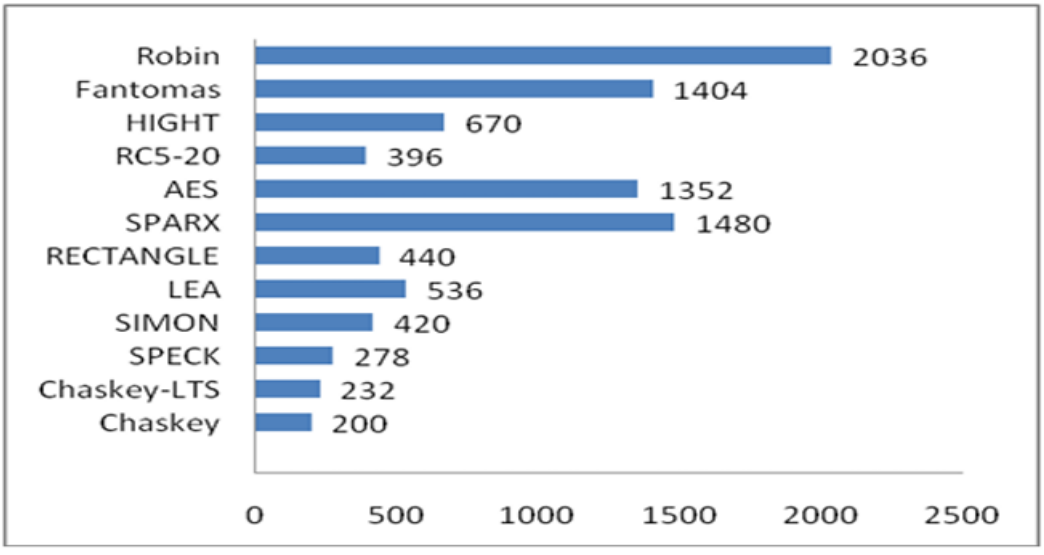
obtaining private keys.

The primary focus of this paper is on symmetric key cryptography due to its widespread use as a means of safeguarding information in resource-constrained environments. Various methods of operation and distinct categories of block ciphers are used within the realm of symmetric key cryptography to ensure the confidentiality and integrity of data packets. These entities are also referred to as cryptographic primitives. The acronym CBC-MAC refers to Cipher Block Chaining Message Authentication Code, as shown in [Fig. 4]. In order to enhance the universality of cryptography, it is important to improve the efficacy of both the block cipher mode and the secure primitives.



[Fig. 3] Basic Lightweight Architecture used in the proposed Work

The code size measure places a particular emphasis on the bits of RAM and ROM that are designated explicitly for block cipher encryption. The greater the quantity of data that is being encrypted, the greater the efficacy of a lightweight cipher will be. This is determined by the number of XOR operations that are carried out and the number of changes that are applied. The memory needs of several ciphers are shown by the graph; Robin requires the least amount of memory, with just 583 bytes, while Chaskey requires the most significant capacity, with 6,962 bytes, as shown in [Fig. 3].



[Fig. 4] Showing the Execution Time

The time it takes to finish a job and how efficiently the central processing unit operates is directly linked to the amount of power used. The greater the number of calculations performed, the more

secure an encryption will be. The total number of cycles in each block is considered while determining it. This encryption is shown to be more effective regarding the time it takes to execute, as seen in [Fig. 4]. Chaskey makes use of an ARX structure and a method that is based on resilient diffusion in order to simplify the data. This makes the procedure easier to complete at that precise time. Chaskey, RC5-20, SIMON, SPECK, and even RECTANGLE could work when the code size is crucial. When everything is considered, Chaskey emerges as the most valuable staff member.

3.2 Design Requirements of the Light Weight Model

Internet-of-Things cryptography and ultra-lightweight encryption are critical subcategories under "lightweight cryptography." The first category should only include low-powered gadgets with a poor level of security. The high cost that is often associated with cryptographic primitives and low-power processors in the modern day is an illustration of the former. The more things are dependent upon one another, the greater the likelihood that they will keep you secure. To restate this in another way, "an ultra-lightweight cryptography algorithm works on devices that are very cheap, do not connect to the internet, are easy to replace, and do not last very long." These methods may be used in various Internet of Things (IoT) devices, including radio frequency identification (RFID) tags, smart cards, rain tags, memory encryption, remote vehicle keys, and many more. It is not a good idea to protect these devices by attaching them to a global platform and protecting that platform with an 80-bit key. Encryption of data sent across the IoT could be helpful here. IoT devices can perform a diverse set of functions, despite the fact that they do not have the same amount of computing power as higher-end devices. Because of this, IoT needs a base that can be easily molded. Appliances connected to the IoT need encryption because it enables various essential features, including the authentication of manufacturer updates and user interactions.

The security of an ultraportable device just requires a single layer. One of the most important distinctions is the level of protection each offers. The improved transmission rate may be attributed to a more vital link to the network. An example would be rogue devices connected to the IoT, which might be exploited to launch a denial of service attack. Because of this, a significantly increased level of caution is required. The industry norm of 80 bits for the length of a secret key is insufficient in many situations; 128 bits are needed instead. A low-power gadget linked to a worldwide network, such as the Internet, is compatible with a secure approach to the Internet of Things. Because they are all connected to the same network, Internet of Things devices should, in an ideal world, all utilize the same "primitive" protocol. In light of the fact that some of these devices are readily available, it is of the utmost importance that Side Channel Attack (SCA) countermeasures be easy to implement. IoT devices will soon achieve more than one thing thanks to multipurpose microcontrollers, which will replace electrical circuits in cryptographic processes. For the protection of the Internet of Things, it is essential that software be lightning-fast. Many other algorithms may be used, some of which are Chaskey, RECTANGLE, Lea, SPECK, and Sparx. In order to guarantee that the program functions appropriately, the guidelines for IoT security primitives are provided in [Table 1].

[Table 1] Design Requirements of the light Weight Model

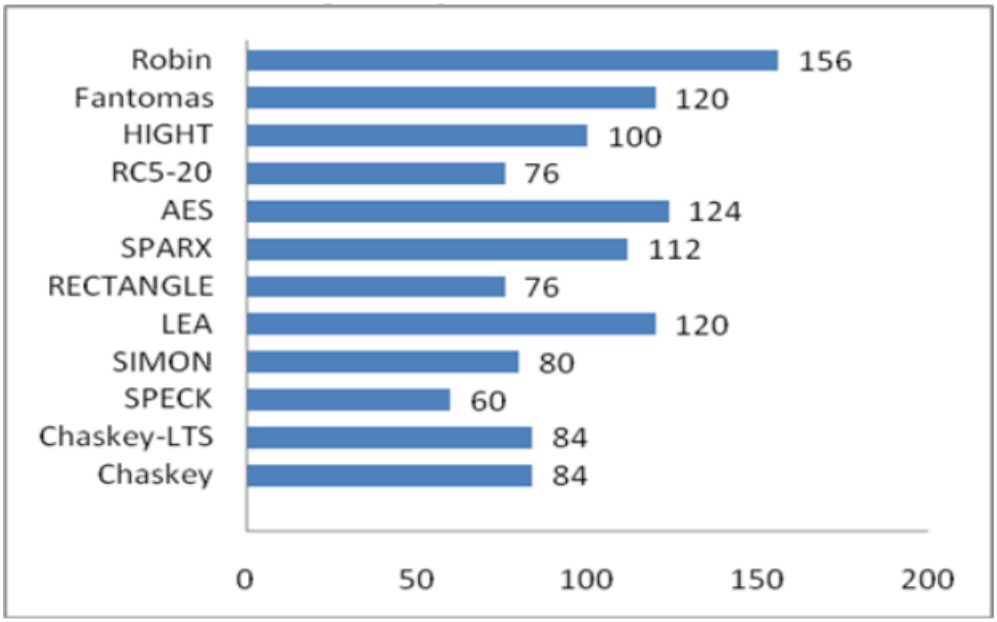
Design Requirements	Description
Type	Block Cipher or Sponge. IoT Devices perform multiple tasks; a versatile primitive is needed
Block Size	96 bits is the minimum; larger sizes must be preferred.
Key Size	At least 128 bits since more minor keys may give access to opponents
Relevant Attacks	Same as traditional ciphers
Target Platform	Microcontrollers and low-end processors
SCA Resilience	Implement a Counter Measures
Functionalities	Hashing
Flexibility	Microcontrollers

4. Results and Discussions

It is necessary to improve the success rate of lightweight block ciphers to improve their ability to balance cost, performance, and security. Lightweight ciphers aim to enhance safety while decreasing the resources (including computational power) needed to achieve this goal. The efficiency of every cipher can be judged in accordance with the parameters that have been listed. In this paper, we have explained and contrasted several software implementations of lightweight symmetric block ciphers that are widely used. In [Table 1], the various software-based lightweight block ciphers currently used to secure IoT devices have their respective FELICS scores displayed for encoding 128-bit messages in counter mode.

[Table 2] Cipher Name of the Proposed Model

Cipher Name	Block Size	Key Size	No.of Rounds	Code Size	Ram in Terms of Bytes	Execution Time
Robin	156	128	8	200	84	563
Fantomas	120	128	12/16	278	84	643
Hight	100	128	27	440	60	965
RC5-20	76	128	44	1480	80	1422
AES	124	128	24	396	112	1146
SPARX	112	128	25	670	120	2917
Rectangle	76	128	27	440	60	965
Lea	120	128	44	1480	80	1422
Simon	80	128	24	396	112	1146
Speck	60	128	25	670	120	2917
Chaskey-LTS	84	128	24	396	112	1146
Chaskey	84	128	25	670	120	2917



[Fig. 5] Comparison of Code Size

4.1 Non-Linear Operations

It is very critical that the algorithm for cryptography does not follow a linear progression. By using S-Boxes and other non-linear mathematical techniques, this characteristic can be achieved. After that,

the algorithms based on the S-Box are separated into two distinct categories. The second group uses the bit-slice, in contrast to the first group, which uses look-up tables (LUT). When performing mathematical operations, primitives in ARX only consider modular additions since this is how the system was designed. The use of lookup tables and S-Boxes are required in order to implement LUT procedures.S-Boxes are employed in a manner that is very similar to that of bit slice-based techniques; however, in order to calculate the S-Box layer, table lookups are not necessary. Utilizing bitwise operations on words, such as AND and XOR, may make the S-Box computation more amenable to parallelization. According to the Felics framework, the most effective ciphers for microcontrollers are those that are ARX-based. Each time along the iteration process, lightweight algorithms choose bits from master keys and round constants. A key schedule is an illustration of what an Even-Mansour arrangement looks like. During the process of encryption, distinct parts of the master key might sometimes do double duty as subkeys. The act of creating a subkey by using the bits of the master key as building blocks is referred to as "key schedule selection."

4.2 Key Schedule

The fact that employing such a key schedule needs less logic to calculate round keys is the biggest benefit that comes from doing so. In addition, the key state does not need to be changed, which is an expensive hardware operation. This eliminates the requirement for that step. Establishing a basic key schedule may be done in a simple manner by changing the key state while simultaneously reprocessing important components of the round function. In this particular scenario, the round function may be used in its full or in part. Either way, the results will be the same. Adjustments and keys are only ever utilized in tandem in very few instances in modern lightweight algorithms. Modification is the factor that contributes to the availability of variability. Because of the update to the public variable, the user is now able to make use of more complex action strategies.

5. Conclusion

In conclusion, developing lightweight cryptographic systems applicable to the IoT is an active area of research. While significant progress has been made in developing efficient and secure cryptographic primitives and protocols for resource-constrained devices, there are still several research gaps that need to be addressed. Standardization of security protocols and frameworks for IoT devices, the development of lightweight critical management systems, security in dynamic environments, and the trade-off between security and resource efficiency are some areas that require further research. Addressing these research gaps will be critical for ensuring the security and privacy of IoT devices and applications, as well as for enabling the widespread adoption of IoT technologies. With the increasing importance of IoT in various domains, including healthcare, transportation, and smart cities, it is essential to continue exploring lightweight cryptographic systems that can provide secure and efficient communication in these resource-constrained environments.

6. Future Work

Future work in the field of lightweight cryptographic systems applicable to the Internet of Things (IoT) could focus on several areas:

First is the development of standard security protocols and frameworks for IoT devices: As IoT devices become more ubiquitous, there is an increasing need for standardized security protocols and frameworks to ensure interoperability and compatibility between devices from different manufacturers. Future work could focus on developing standardized security protocols and

frameworks for IoT devices based on lightweight cryptographic primitives and protocols.

Second is the development of lightweight key management systems: Key management is a critical component of any cryptographic system, and there is a need for lightweight critical management systems that can provide secure key generation, storage, and distribution on resource-constrained devices. Future work could focus on the development of light key management systems that are specifically designed for IoT devices.

Third is establisnging security in dynamic environments: IoT devices are often deployed where network connectivity can be intermittent or unreliable, and widgets may be added or removed from the network frequently. Future work could focus on developing lightweight cryptographic systems that can provide security in these dynamic environments by incorporating adaptive key exchange, revocation, and secure device registration.

Fourth is integrating machine learning and artificial intelligence: Integrating machine learning and artificial intelligence (AI) with lightweight cryptographic systems could provide enhanced security and privacy for IoT devices and applications. Future work could focus on exploring the potential benefits of combining machine learning and lightweight cryptography and developing new cryptographic techniques that are specifically designed for use with machine learning and AI.

Finally, explorating of new cryptographic primitives and protocols: While significant progress has been made in developing lightweight cryptographic primitives and protocols for IoT devices, there is still room for innovation. Future work could focus on exploring new cryptographic primitives and protocols that can provide enhanced security and efficiency for IoT devices while considering the resource constraints of these devices.

7. Acknowledgments

This study was financially supported by Chonnam National University (Grant number: 2023-0926)

References

[1] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Computer networks, (2010), Vol.54, No.15, pp.2787-2805.

[2] K. McKay, L. Bassham, M. Sönmez Turan, N. Mouha, Report on lightweight cryptography, National Institute of Standards and Technology, (2017)
Available from: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf

[3] F. Li, Z. Zheng, C. Jin, Secure and efficient data transmission in the Internet of Things, Telecommunication Systems, (2016), Vol.62, pp.111-122.
DOI: 10.1007/s11235-015-0065-y

[4] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, C. Vikkelsoe, PRESENT: An ultra-lightweight block cipher, International workshop on cryptographic hardware and embedded systems, (2007).
DOI: 10.1007/978-3-540-74735-2_31

[5] J. W. Bos, D. A. Osvik, D. Stefan, Fast Implementations of AES on Various Platforms, IACR Cryptolgy ePrint Archive, (2009)
Available from: https://eprint.iacr.org/2009/501.pdf

[6] G. Leander, C. Paar, A. Poschmann, K. Schramm, New lightweight DES variants, International Workshop on Fast Software Encryption, Springer, (2007).
DOI: 10.1007/978-3-540-74619-5_13

[7] F. A. Alaba, M. Othman, I. A. T. Hashem, F. Alotaibi, Internet of Things security: A survey, Journal of Network and Computer Applications, (2017), Vol.88, pp.10-28.
DOI: 10.1016/j.jnca.2017.04.002

[8] X. Yao, Z. Chen, Y. Tian, A lightweight attribute-based encryption scheme for the Internet of Things, Future Generation Computer Systems, (2015), Vol.49, pp.104-112.
DOI: 10.1016/j.future.2014.10.010

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

[10] S. Panasenko, S. Smagin, Lightweight cryptography: Underlying principles and approaches, International Journal of Computer Theory and Engineering, (2011), Vol.3, No.4, pp.516-520.