 http://dx.doi.org/10.14500/aro.11007

Modern and Lightweight Component-based Symmetric Cipher Algorithms: A Review

Samar A. Qassir[1], Methaq T. Gaata[1], and Ahmed T. Sadiq[2]

[1]Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq

[2]Department of Computer Science, University of Technology - Iraq, Baghdad, Iraq

***Abstract*—Information security, being one of the corner stones of network and communication technology, has been evolving tremendously to cope with the parallel evolution of network security threats. Hence, cipher algorithms in the core of the information security process have more crucial role to play here, with continuous need for new and unorthodox designs to meet the increasing complexity of the applications environment that keep offering challenges to the current existing cipher algorithms. The aim of this review is to present symmetric cipher main components, the modern and lightweight symmetric cipher algorithms design based on the components that utilized in cipher design, highlighting the effect of each component and the essential component among them, how the modern cipher has modified to lightweight cipher by reducing the number and size of these components, clarify how these components give the strength for symmetric cipher versus asymmetric of cipher. Moreover, a new classification of cryptography algorithms to four categories based on four factors is presented. Finally, some modern and lightweight symmetric cipher algorithms are selected, presented with a comparison between them according to their components by taking into considerations the components impact on security, performance, and resource requirements.**

***Index Terms*—Information security, Lightweight Symmetric Cipher, Modern Symmetric Cipher, Symmetric cipher components.**

I. Introduction

The collection of the steps and processes designed to protect and secure data which is one of the most important commodities of this era from any unauthorized access or alterations whether in the more static storage status or in the more dynamic transmission phase between one location to another, is defined collectively as Information security (abbreviated to "InfoSec"). Because knowledge has become one of the most valuable commodities in the 21st century, efforts to keep data secure have become increasingly vital (Soomro, Shah, and Ahmed, 2016).

The phrase "information security" is usually used to refer to data secrecy, this confidentiality can be achieved with help of cryptography. Cryptography as a term came from the Greek word "kryptos" which defines "Hidden" or "Secrets" (Anand, et al., 2016; Pachghare, 2019). Cryptography is skill/discipline of transforming a plain/original data into coded data (Lakhtaria, 2011) and again reconverting that plain text into its original data, providing protection for this data from unauthorized access and manipulation both in storage and transfer circumstances. Fig. 1 shows cryptography process which involves two processes: Encryption and decryption (Stallings, et al., 2012; Bagane and Sirbi, 2021).

Plain text refers to the original information, whereas cipher text refers to the coded form. Cipher is an algorithm for converting original text to coded text. Key is information which is used in cipher known only to sender/recipient to encode or decode the information (Qadir and Nurhayat, 2019; Forouzan and Mukhopadhyay, 2015). Encryption which is also known as an encipherment is a process of converting original data into coded one. Nowadays, encryption is available by default often without the user even being aware of it. Decryption which is also known as decipherment can be defined as the recovery system of cipher text from plain text. The cryptography can be summarized as learning of encryption theory or techniques (Stallings, et al., 2012; Sharma, et al., 2022).

This paper presents a review of cipher categories, symmetric main components units, explanation for their properties and effect on security, and the symmetric advantages versus asymmetric cipher category, also comparison among the two types of the symmetric cipher category, in addition to gathering and discussing some common types of stream, block, and lightweight ciphers algorithm.

Due to the importance of encryption algorithms in the field of information security, many of researches and studies are being conducted and presented. Certain of these studies have been done for performance evaluation (Sallam and Beheshti, 2018), cipher design analysis (Hamza and Kumar, 2020), and summarization the various weaknesses of a particular

ARO-The Scientific Journal of Koya University
Vol. X, No. 2 (2022), Article ID: ARO.11007. 17 pages
DOI: 10.14500/aro.11007
Received 18 June 2022; Accepted: 07 November 2022
Regular review paper: Published: 08 December 2022
Corresponding author's e-mail: samarqassir@uomustansiriyah.edu.iq

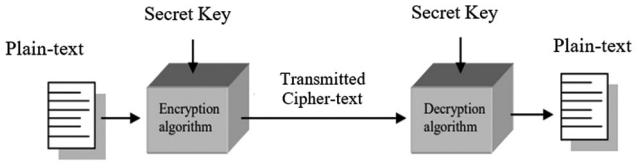

Fig. 1. General Model of Cryptography Process.

algorithm (Brahmjit, 2015). In the next section of this review, some of these studies will explain. For this review, which represent the first analysis study for the components that used in symmetric cipher algorithms design, the new contribution explains through these three points: First, a new classification of encryption is presented. This comprehensive classification is the first of its kind that give the insight idea about all types of encryption according to their chronological sequence and components, which shows how the development of encryption algorithms done depended mainly on the types and size of components used in algorithm design. Second, analysis of the design of modern and lightweight symmetric ciphers based on their main components used, focusing on the impact of each component on cipher design; the component that appears primarily in symmetric cipher design shows how these components give the properties of symmetric versus asymmetric cipher characteristics. Third, by selecting and analyzing 13 symmetric cipher algorithms of both types (stream and block), it was shown the lightweight that used today in smart devices they result from a reduction in the number and in the size of essential cipher components, which shows the importance of reviewing and analyzing all cipher components and knowing the basic one, in addition of its impact on the strength of the cipher algorithm design. The objectives of this analytical study for the basic symmetric cipher components are giving a more insight and comprehensive to developers in the field of encryption for designing new cipher algorithms.

The next sections of this review presents related work and new taxonomy of cryptography categories respectively; whereas section 4 discusses the theoretical background that demonstrates the categories of symmetric key cipher; additionally, the main components used in symmetric key cipher's types have explained. Some selected modern and lightweight cipher algorithms are explained in sections 5 and 6, whereas the last 2 sections (7 and 8) involve the discussion and conclusion.

II. Related Work

Sharma, et al. (2022) introduced a review study about the concept of cryptography, beginning with its history, definitions, security functions, and historical methods for symmetric and asymmetric encryption, as well as homomorphic encryption, and the Goldwasser_Micali encryption scheme. This investigation focused on several different kinds of cryptography computations, including AES, DES, 3DES, IDEA, RSA, ECC, homomorphic, and blowfish. This study has demonstrated that cryptography plays a crucial role in achieving the main goals of security objectives, such as acceptance, rectification, safety, and repudiation. Cryptographic calculations are performed to accomplish these goals. To provide reliable, amazing, and strong association and data protection, cryptography is strongly motivated.

A comparative study between conventional cryptographic algorithms and evolutionary algorithms for cyber security was presented by Bagane and Sirbi (2021). Based on Darwinian evolutionary theories of natural selection and genetics, genetic algorithm (GA) is organized as random search algorithm. Moreover, the skill of creating secret codes is known as cryptography. This study comes to the conclusion that using a genetic algorithm-based cryptosystem is more safe and impenetrable than a conventional cryptosystem. The recommendation was to experiment with several sophisticated ciphers, such as AES and DES, to improve the performance of genetic algorithm.

Hamza and Kumar (2020) proposed a review for three algorithms DES, AES, and RSA. This study evaluated and listed the aforementioned algorithms in a sequential order, making clear how they relate to one another. For instance, how symmetric and asymmetric algorithms, those with secret keys, and those with key pairs relate to one another by examining the DES, AES, and RSA algorithms, they were able to highlight the advantages and disadvantages of both symmetric and asymmetric encryption techniques. This study might reveal some of the areas for future scholarly research in the area of cryptography.

The evolution of stream ciphers, their classification, and the design concepts of this cipher type were reviewed by Jiao, Hao and Feng (2020). In addition, a brief analysis of their advantages and shortages was done to stimulate additional study on this cipher type's implementation and security. This study shown that this cipher design focuses primarily on the cipher structure and the fundamental operations used, which must ensure the security that resists all categories of current attacks.

A survey of recent developments in the field of lightweight cryptographic algorithms was given by George Hatzivasilis, et al. (2018). Hardware and software designs for symmetric key block ciphers'' lightweight implementations have been studied. Three hundred and sixty implementations and 52 block ciphers were compared in terms of their security, cost, and adaptability to various types of embedded devices. The most significant cryptanalysis relating to these ciphers was also mentioned. The research offered, in the authors' opinion, will help designers create reliable systems and architectures, enabling a safe transition to this new world and the Internet of Things.

III. Cipher Classification

The cryptography fundamentals can be categorized in four main ways/categories according to several factors including number of keys, type of cipher operation, way of processing plain text, and, finally, the chronological order; as shown in Fig. 2. The first categorization method depends on the number

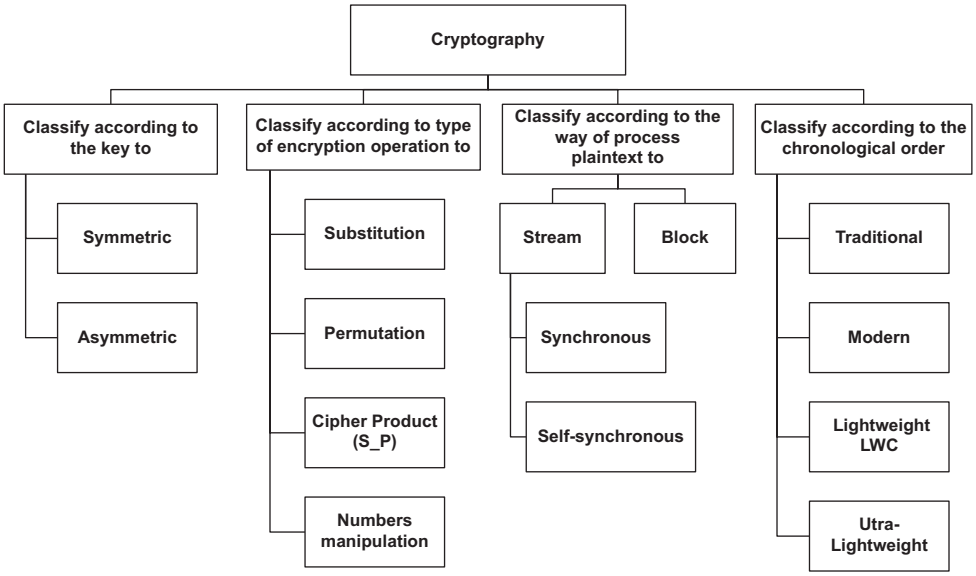

Fig. 2. The cipher classifications.

of keys: Symmetric versus asymmetric (Wahid, et al., 2018), whereas the second categorization method involves the type of cipher operation: Substitution (S-Box), permutation (P-Box), cipher product (S-P), and numbers manipulation. The third categorization method takes into consideration the way of processing plain text into two main categories: Stream (which is further sub-categorized into synchronous and self-synchronous) and block ciphers (Mewada, Sharma and Gautam, 2016). The last categorization method depends on the chronological order: Beginning with the traditional, into modern, the most recent lightweight and ultra-lightweight (Hasan, et al., 2021).

The cipher algorithm can involve more than 1 of the above-mentioned categorization methods; for example, the algorithm may be symmetric key using (s-p) in encryption, processing plain text as blocks, and lightweight type (Chiadighikaobi and Katuk, 2021).

IV. Basic Principles

In this section, the basic principles of symmetric cipher of its two types (stream and block) are covered. The main components that used in symmetric cipher algorithm design are explained in details and finally the different between symmetric ciphers algorithms according to their chronological order are presented.

A. Symmetric Cipher

As explained in the previous section, there are two cipher types based on number of key used: Symmetric and asymmetric. Table I shows direct comparison between these two categories. On a basis of processing way of plain text, a symmetric encryption schemes classified into main categories: The first one is stream cipher and the second one is block cipher (Hussain and Shah, 2013), (Forouzan and Mukhopadhyay, 2015). The first cipher, as explained in Fig. 3, is the most important encryption system. It is generally used for its speed

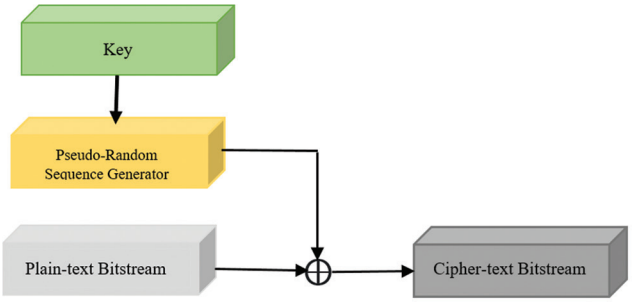

Fig. 3. Stream cipher encryption process.

and simplicity of implementation in hardware, they have less complex hardware circuitry. The characteristic feature of this cypher system is the continue change of the keys for every bit of the plain text resulting in the production of different cipher text even for plain text of repetitive blocks, this becomes very applicable and handy for unknown length plain text like a secure wireless connection, limited buffering, when individual processing of characters is a must on reception, in addition to, military applications, and in strategic sectors.

Due to merit of having limited or no error propagation, and where transmission errors are highly probable, this stream cipher has a prominent advantage. It is classified into synchronous stream ciphers (SSC) and self-synchronizing stream cipher (SSSC) where due to design problems, SSSC is less used in practice (Sharma, et al., 2022; Jindal and Singh, 2015).

Random key streaming that ensures the computational security of the cipher is the major selling point for this cipher system where its solidity and robustness against attacks and unauthorized access is based on complex keystream created to secure text and images transmitted digitally through open networks such as phones and emails. This defines its efficacy as a major property of this cipher system.

Many studies aiming to improve the stream ciphers took interest on the randomness and complexity of the keystream (Bagane and Sirbi, 2021).

The second category, based on how plain text is processed, is block type, in which the original text is divided into chunks of bits at a time (Hussain and Shah, 2013). High versatility, high diffusion, and robust resistance to attempts of concealed tampering attempts, and possessing very similar and identical encryption and decryption methods, all those merits grant this cipher system its advantages making its implementation with lesser resources is a genuine possibility. However, speaking about advantages cannot be completed without mentioning possible disadvantages such as slower encryption speed as a result of need to capture the entire block for encryption/decryption. Another negative point is the possibility of breeding errors due to the fact that a mistake in just one symbol could alter the whole block. As shown in Fig. 4, this cipher contains a set number of bits and multiple stages of transformation that is defined by a symmetric key (De Canniere, Biryukov and Preneel, 2006). Table II shows a comparison of block and stream cipher types.

B. Components Used in Symmetric Cipher

There are many properties of symmetric cipher such as its faster speed compared with asymmetric cipher, the need to use minimal resources only, suitability for today's constrained environmental resources such as low chip area or low-power supply, and being ideal for most of today's applications and for encoding large amounts of data.

The reason behind all those above-mentioned properties of the symmetric cipher is its design which is based on components that are different from the asymmetric cipher. Whereby, the design of symmetric cipher is based on substitution, permutation, XOR, and many other components which are much faster compared to the asymmetric cipher's design due to the application of mathematical functions to numbers (Kumar, Suneetha, and Chandrasekhar, 2012; Szaban and Seredynski, 2011).

Fig. 5 shows that illustration of the components of the two types of the symmetric cipher is shown in addition to

TABLE I
COMPARISON FOR THE TWO MAIN CIPHERS CATEGORIES SYMMETRIC AND ASYMMETRIC (DUTTA, GHOSH AND BAYOUMI, 2019)

Criteria	Symmetric – Cipher	Asymmetric –Cipher
No. of key	Sharing secrecy (one key)	Personal secrecy (two key)
Operation type	Based on substation, permutation	Numbers manipulation
Algorithm speed	Faster	Requires more time
Main ciphering aim	Provides confidentiality and authentication	Provides confidentiality
Algorithm utilization	For ciphering huge amounts of data, files and also for communication paths	For all key operations like ciphering, distributing
Algorithm design based on	Arithmetic and logic components	Mathematical computation
Hardware implementation difficulty	Less difficulty	More difficulty
For lightweight applications	Used a lot	Less used

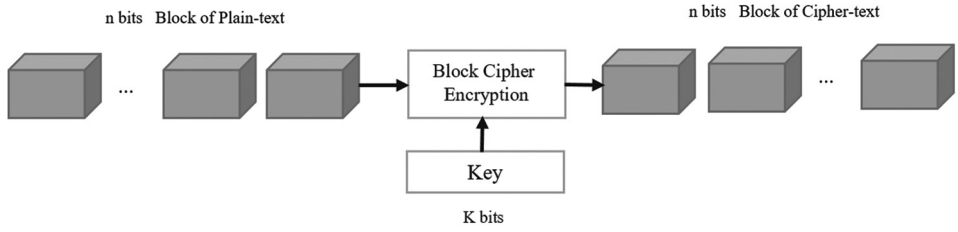

Fig. 4. Simple diagram for block cipher.

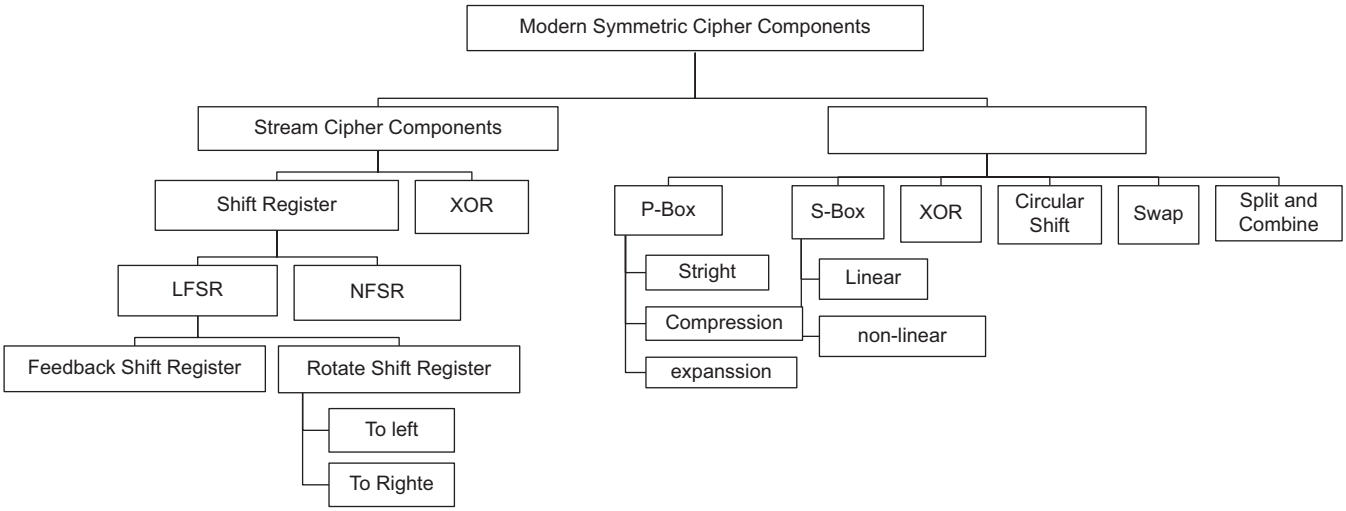

Fig. 5. Modern symmetric cipher components.

http://dx.doi.org/10.14500/aro.11007

TABLE II
COMPARISON FOR THE TWO CATEGORIES OF SYMMETRIC CIPHER (MOHAMMAD, 2021)

Criteria	Block type	Stream type
The length of data	Big (64,128,256) bit	Little (1) bit
The length of key	Fixed	Variable
Count of rounds	Big	-
Usage of resources	Big	Little
Implementations speed	Less than stream	More rapid and easier
Security	Less than stream	Maximum security
Error-resistant robustness	Little	Big
Applications	For big message	For small message
Shannon principles	Confusion and diffusion	Only confusion
Algorithm design based on	S-Box, P-Box, XOR, swap, circular shift, split, and combined	All types of shift registers and XOR

the difference between the components used in each type of symmetric cipher: Stream and block. In the modern stream symmetric cipher, the algorithm is based on two main components only; feedback shift register (FSR) and XOR. They effectively utilize linear and non-linear feedback shift register (LFSR and NFSR). Whereas in modern block symmetric cipher, the algorithms are very versatile as a result of being designed to provide properties of modern cipher, such as diffusion and confusion by being constructed not as a single unit.

This modern cipher is made of a combination of different components such as S-Box, P-Box, Exclusive-Or, circular shift, swap, split, and combine. Some of these components will be explained in the next subsections (Easttom, 2021), (Bardis, Markovskyy and Andrikou, 2004).

1. S-Box and P-Box

Substitution box (S-Box) and permutation box (P-Box) are crucial components of every modern block cipher. The prime purpose of an S-Box is to prevent the output from being easily transformed back into the input by creating confusion between the cipher text and the secret key, this purpose of this component making it as the heart of every block cipher cryptosystem (Hussain and Shah, 2013). P-Box, on the other hand, is responsible for diffusion. To further maximize the difficulty of analyzing the cipher and increase its robustness, modern block ciphers actually use several different S-Boxes. Fig. 6 illustrates the S-Box in DES algorithm.

According to the number of output bits compared to those of the input bits, P-Boxes are classified as compression (less), expansion (greater), and straight (equal), where only the later ones are invertible (Chugunkov, et al., 2020), as shown in Fig. 7.

2. Exclusive_Or

Ciphers that are more sophisticated have a very common component operator considered the to be the mysterious recipe behind modern encryption, known as Exclusive_Or "XOR," where a cipher text is created by combining a key with a plain text through this operator, while restoring the original plain text by XOR-ing to same key to the cipher text. This operator is based on what is known as a truth table, in which 0 represents "false" and 1 represents "true."

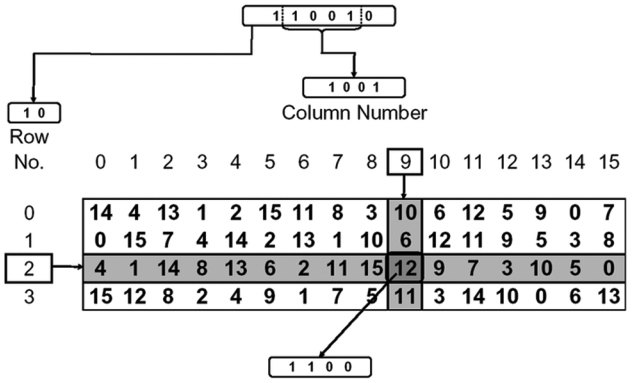

Fig. 6. S-Box in DES algorithm.

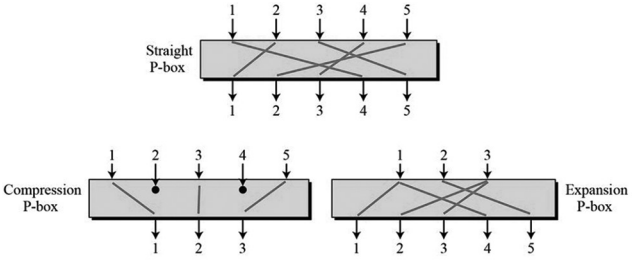

Fig. 7. The three types of P-Boxes.

When one of two bits is 1, the other two bits are regarded true (or 1), however, when both bits are 0 or 1, they XOR to 0. For a really random key bit, this operation creates an ideal equilibrium in which the cipher text outcome is equally likely to be 0 or 1 for a given plain text input. This ideal/perfect balance is the main reason why this operator is so useful in cryptography. In this section, the five essential properties of XOR (Dreier, et al., 2018) that make use of it are presented in Table III:

3. Circular shift

When parts fall off at one end and are put back at the other end, this is defined as "circular shift" with bits falling off at the left end being put back at the right end in a left rotation and bits falling off at the right end being put back at the left in a right rotation (Muchsin, Sari and Rachmawanto 2019). Fig. 8 depicts a circular shift to the left.

C. Symmetric Cipher Algorithms depending on Chronological Order

In classification of cipher algorithms as shown in section and Fig. 2, according to the chronological order, there are traditional, modern, lightweight, and ultra-lightweight algorithms ciphers. In the traditional, which is the oldest type, character oriented, can be reasonably computed by hand and based on using two only of operations types: Substitutions and permutation. In modern and lightweight ciphers, which are bit oriented, they are usually easy to decode using recent technology with product cipher (S-P) and many other components such as S-Box, P-Box, XOR, swap, circular shift, split, and combined. One of the main different between modern, lightweight, and ultra-lightweight cipher is in the number and size of components used in cipher algorithm design. This lightweight referred to as lightweight

TABLE III
THE ESSENTIAL PROPERTIES OF XOR

S. No.	Property	Its symbolization	Its description
1	Associative	U ⊕ (V⊕Z) = (U⊕V) ⊕ Z	The operations can be chained together without effect on the result
2	Closure	-	It is guarantees exclusive-or's result of two n-bits is completely different n-bit
3	Commutative	U⊕V = V⊕U	The sequence in which the two inputs are entered is irrelevant
4	Identity element	U⊕0 = U	Any value that XOR'd with zero is still the same unaffected
5	Self-inverse	U⊕U = 0	Any value XOR'd with itself the result is zero

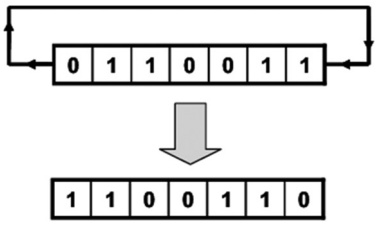

Fig. 8. Left circular shift.

cryptography (LWC), it is considering as a new cryptography type, to give adequate secure algorithms for restricted devices by reducing the length of key, the rate of each the cycle and the throughput, also the power consumption. Thus, for dealing with all parameters of computing devices to a minimal level, in lightweight and ultra-lightweight cipher system is strongly desired (Kousalya and Kumar, 2019; Sallam and Beheshti, 2018; Sliman, et al., 2021; Raza, et al., 2020). Table IV illustrates the main differences between the modern and the lightweight block ciphers:

V. *Modern Symmetric Cipher Algorithms*

A quick overview of common modern symmetric key (stream and block) cipher algorithms is presented. Three stream cipher algorithms and four vital block cipher are presented with concentration on basic components used in cipher algorithm design without describing the key schedule.

A. Modern Stream Cipher Algorithms

1. Rivest Cipher 4 (RC4)

Designed in 1984 and containing a basic component XOR, this modern stream cipher is one of the simplest and widely adopted ciphers, yet it is this simplicity that make this cipher covulnerable to security attacks (Brahmjit, 2015). As per functionality, for key creation, this cipher has two essential components: The Key Scheduling Algorithm (KSA) and the Pseudo Random Number Generator (PRGA), the latter of which generates a pseudorandom output sequence (bytes) from the permuted internal state, which is a random sequence. For the cryptanalyst, the statistical inadequacies of the output sequence are the focus of their investigation (Madarro-Capó, et al., 2021). Fig. 9 depicts functionality.

2. Salsa20

Being a family of 256 bits ciphers, this cipher is designed as another modern stream cipher and recommended for typical cryptographic applications due to its speed (faster than AES) while for applications where speed is more important than confidence, the faster, more reduced-round ciphers

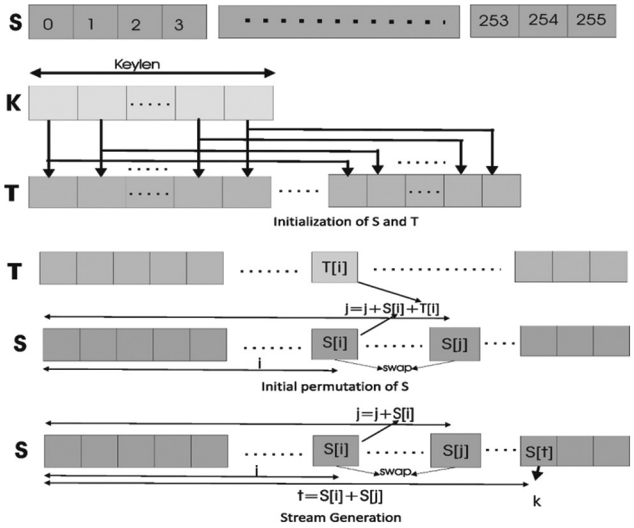

Fig. 9. Fundamental of RC4.

Salsa20/12 and Salsa20/8 are recommended. Functionality wise, this cipher encryption consists of a long chain of three simple operations on 32-bit words: Modular addition, XOR, and left shift rotation. Fig. 10 shows the quarter-round (Afdhila, Nasution and Azmi, 2016; Fukushima, et al., 2017).

3. A5/1

This cipher algorithm having two main components: The first is LFSR and the second is XOR, this algorithm is considered one of very fast stream cipher algorithms. The cipher design comprises three LFSRs: The first is R1 with length 19 bits, the second is R2 with length 22 bits, and the last is R3 with length 23 bits, this cipher designed for yield a randomly binary stream of bits with along cycle (Ekdahl and Johansson, 2003; Jiao, Hao and Feng, 2020).

The tap bits that select to achieve primitive polynomial are: 18, 17, 16, and 13 for the first register; 21 and 20 for the second one, and 22, 21, 20, and 7 for the last register (Amiri, Mahdavi and Mirzakuchaki, 2009; Sadkhan and Jawad, 2015). Fig. 11 provides illustration for the cipher design.

B. Modern Block Cipher Algorithms

1. Data encryption standard (DES)

This algorithm cipher is the first one of modern symmetric of block type. Its key and block length are (56, 64-bits), respectively, put by the NSA (Patil, et al., 2016). The design of this cipher based on 16 rounds, the main components that used in the design of each round are: S-Box, permutation, XOR, swap, split, and combined (Yihan and Yongzhen,

http://dx.doi.org/10.14500/aro.11007

TABLE IV
COMPARISON FOR THE TWO CHRONOLOGICAL ORDER OF BLOCK CIPHERS: MODERN AND LIGHTWEIGHT

Criteria	Modern block cipher	Lightweight block cipher
Components number and its size	More than lightweight	Less than modern
Number of round	Less	More
The block size	64, 128, and 256 bits	32, 48, or 64 bits
Key sizes	128 bits or more	80 or 128 bits

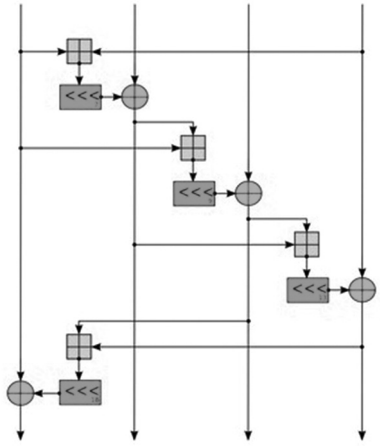

Fig. 10. Salsa20 quarter-round.

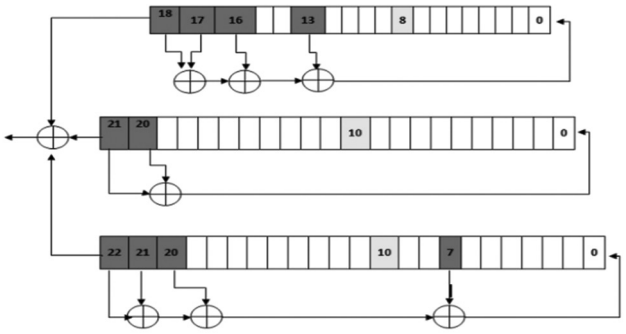

Fig. 11. The basic of A5 cipher algorithm that based on three LFSRs.

2021); the algorithm general structure with its round and its function are illustrated in the Fig. 12 below:

2. Advanced Encryption Standard (AES)

This cipher algorithm is designed as a solution for previous one. It is also modern symmetric of block type and its standard version has simple structure, based on substitution-permutation network (SPN) (Zhao, Ha and Alioto, 2015) its design comprises: Non-linear substitution step; permutation step; XOR; split; and combined components. Its key length is: (128 or 192, or 256-bits), respectively, and can be encrypted/decrypted for 128 bits of data length, as shown in Fig. 13.

The cipher design also having numbers round of plain text transformation, the number of round in this cipher depends on key length, the longer the key length, the more number of round used (10 for the 128 bits, 12 for the192 bits, and finally 14 for the 256 bits). It is flexible for hardware implementations, also this cipher algorithm can be tailored for low-volume loads or can be improved for applications required high throughput (Kumar and Rana, 2016; Qiao, El-Assad and Taralova, 2020).

3. Blowfish

With variable key length from (32 to 448 bits) and block size of (64 bits), this modern symmetric cipher algorithm of block type is designed by Brice Schneier in 1993, with 16-round Feistel structure, intended as a replacement for cipher algorithm like DES or IDEA (faster than DES when implemented on 32 bits microprocessors). It is suitable for both domestic and commercial use due to its variable length key, most notably for applications such as communication links or file encryptors where the key does not change frequently, whereas it is unsuitable for other applications such as packet switching or smart cards that require even more compact ciphers (Schneier, 1993; Hussaini, 2020; Ghosh, 2020). The main components that used in each round are: S-Box, XOR, swap, split, and combined, as shown in Fig. 14.

4. International Data Encryption Algorithm (IDEA)

Operating on 64 bits data blocks length with 128 bits long key, the IDEA is another modern symmetric block cipher, the design principle of which depends on mixing of arithmetical operations (the three of which are: XOR, addition modulo 2^{16}, and multiplication modulo $2^{10}+1$) that are easily implemented both in hardware and software (Basu, 2011; Patil and Bhusari, 2014). The much needed non-linearity of this cipher is derived from the addition modulo 2^{16} and multiplication modulo $2^{10}+1$ arithmetical operation, whereas explicit S-Box is not used. This cipher designed base on modular additions, modular multiplications, and XOR, swap, split, and combined, as shown in Fig.15.

VI. LIGHTWEIGHT AND ULTRA-LIGHTWEIGHT SYMMETRIC CIPHER ALGORITHMS

This section presents the main of lightweight and ultra-lightweight symmetric cipher algorithms for two types (stream and block), three lightweight stream ciphers algorithms and 10 lightweight block ciphers, all these cipher algorithms are covered from many points of view (number and size of components, security, and performance).

A. Lightweight Stream Cipher Algorithms

1. Fruit-v2

It introduced informally in 2016 on the web page of IACR. This cipher was designed as ultra-lightweight symmetric stream cipher with smaller state, introduced for hardware applications in the eSTREAM project (Wang, et al., 2019), new ideas were introduced to show the possibility of shortening the size of the internal state size by exploiting a secret key not only in the initialization but also in the keystream generation (Naser and Naif, 2022), thus succeeding in reaching a formula that is able to resist attacks such as the classical time-memory data trade-off attack.

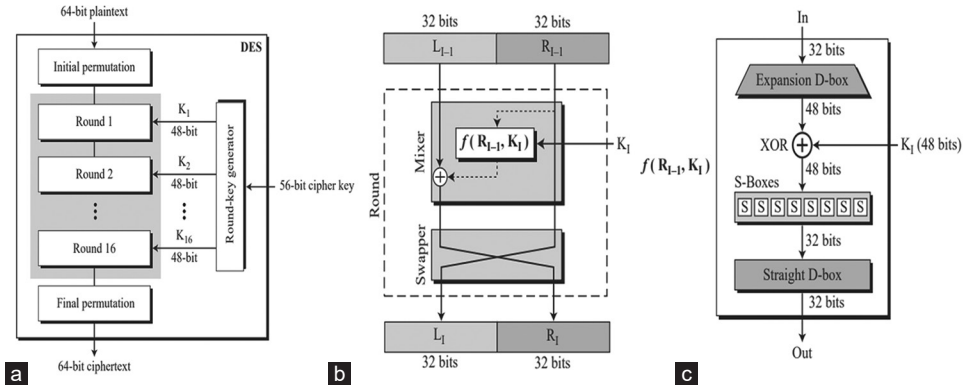

Fig. 12. (a) The general structure of DES, (b) A round in DES (encryption site), and (c) DES function.

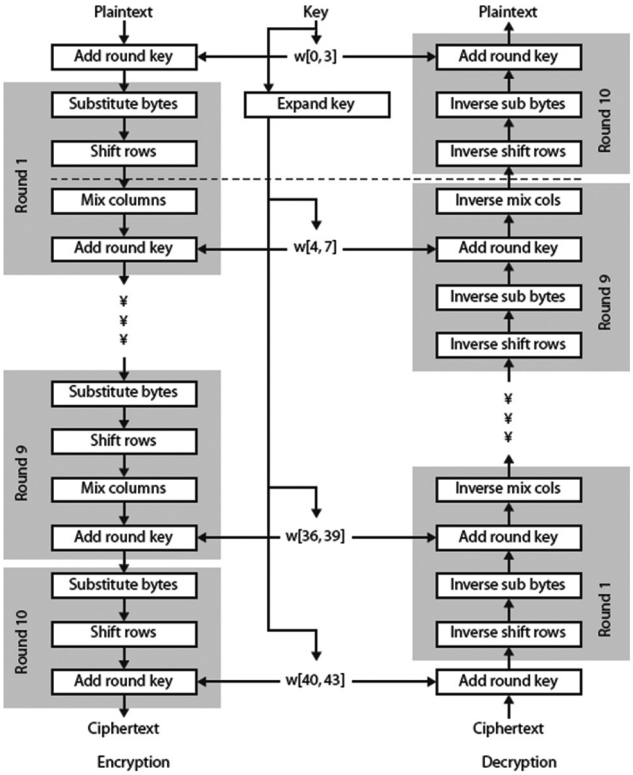

Fig. 13. AES encryption and decryption process.

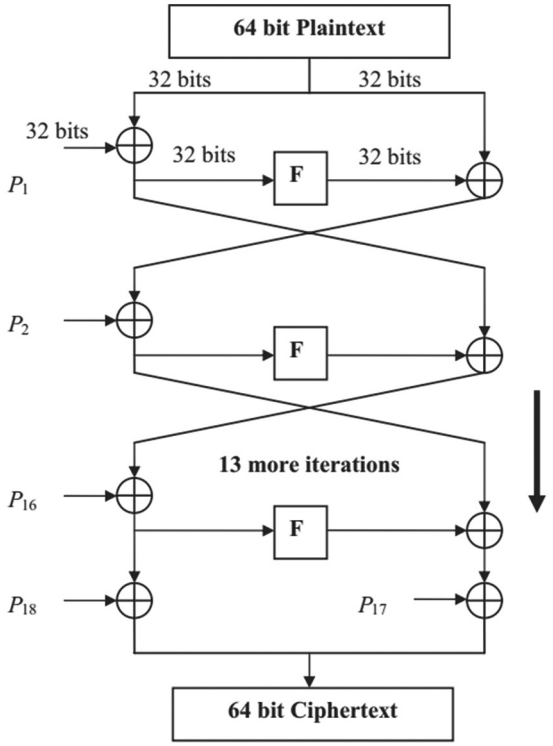

Fig. 14. A round structure.

Its structure, as shown in Fig. 16, involved of LFSR and NFSR, the size of these both FSR in Fruit-v2 is only 80 bits (Wang, et al., 2022).

2. LOGIC

Published in 2019, this cipher algorithm was introduced as a lightweight symmetric stream cipher behind a main idea of combining a chaotic system and two NFSRs. This cipher design is leading to the formation of a new cipher that is hardware-oriented and can be used efficiently in certain circumstances such as in resource constrained devices or environments (Ding, et al., 2019). As shown in Fig. 17, this algorithm has a secret key of 80 bits (40 bits for each one of the NFSR) also with three multiplexers; a filter function and logistic chaotic system. Regarding security of this cipher is considered good in resisting many essential attacks due to the high nonlinearity and the good elasticity of the function used beside the existence of the two NFSRs (Ding, et al., 2019).

3. A4

This algorithm is lightweight symmetric stream cipher, published in 2020, its cipher design depend on two kinds of FSR: The first is LFSR and the second is FCSR (Mohandas, et al., 2020). This algorithm can be describing as two parts: The first one is encryption procedure and the second is decryption procedure, and a seed box exists between these two procedures with 128 bits key length. The characteristic of this algorithm is ensuring security to big extent and easy to implement. The LFSR acts as a clock thereby ensuring primary level of security. Robustness of this cipher against attacks like the algebraic, brute force, and differential is merited to the arrangement of LFSR and FCSR. Its time and space

http://dx.doi.org/10.14500/aro.11007

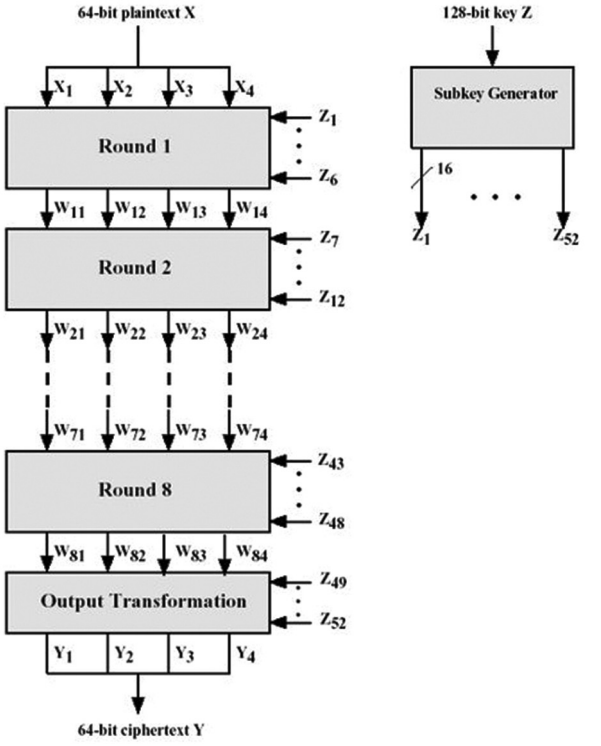

Fig. 15. IDEA encryption structure.

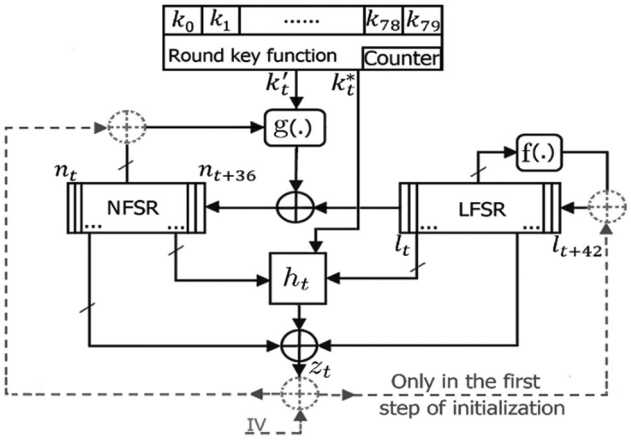

Fig. 16. The FRUIT-v2 cipher design.

consuming consider minimal if compared to other ciphers (Jassim and Farhan, 2021).

B. Lightweight Block Cipher Algorithms

1. Lightweight Data Encryption Standard (DESL)

Presented in 2006, this cipher, being a descendant from DES design, is the first DES variant (Poschmann, et al., 2006). By replacing the eight original S-Boxes of DES with a single new one (eliminating seven S-Boxes as well as the multiplexer implementation) achieving a reduction in the DES's gate complexity, through decreasing the chip by about 20% (1850 [GE] vs. 2310 [GE]).

Another leverage of the DESL on DES is being lighter merited to discarding the initial and final permutation of

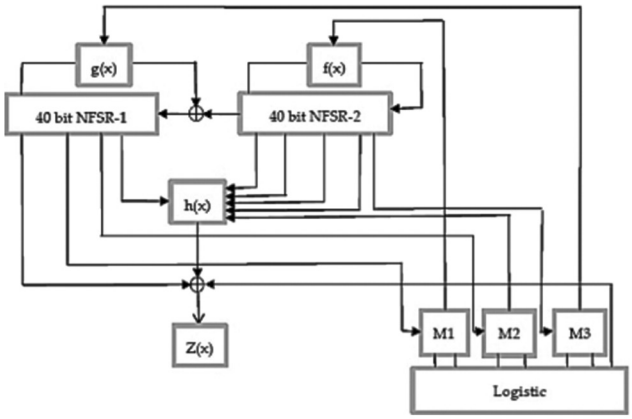

Fig. 17. LOGIC cipher algorithm design.

DES (Kitsos, et al., 2012). The ability of this DESL to resist common attacks such as linear and differential cryptanalysis and the Davies-Murphy attack is attributed to the careful selection and prime optimization of the S-Box, reaching a level of security that is acceptable and suitable for many applications. Further robustness of the cipher can be achieved by applying key whitening, making way to the formation of the "DESXL" cipher, with a security level of approximately 118 bits. DESXL requires 2168 area (GE) compare to the DES 2309, to make it lighter.

2. Lightweight Advanced Encryption Standard (AES)

On top of being the most well-studied block cipher algorithm (Dutta, Ghosh and Bayoumi, 2019), this algorithm continues to the be subject of further studying past, present, and future optimizing its applicability for today's needs based on the intensely growing environmental demands in every single aspect of modern life with an ultimate goal of achieving sustainability. Moreover, it is through reducing the consumption of power and energy, a compact AES circuit design was proposed by Lu, et al., 2018. Only one S-Box is used in the cipher design, this one S-Box is utilized in key expansion process and data encryption process. This reduction in components achieves less latency in encryption process; and small area with high energy and throughput as a circuit design. In Mathew, et al., 2015, this cipher design based on one 8-bit S-Box with shift rows to compute all rounds, its aim to reduce the power of AES in encryption and decryption processes.

3. LBlock

Presented in 2011, and with (64, 80 bits) block size and key size, respectively, this is an ultra-lightweight symmetric block cipher algorithm (Wu and Zhang, 2011). In hardware, it occupies 1320 (GE), requiring 3955 clock cycles to encrypt a single block (Aljazeera, Nandakumar and Ershad, 2016). This cipher can be implemented effectively in hardware and software. As shown in Fig. 18, the structure of its round function based on substitution-permutation network (SPN), in which a small 4 × 4 S-Boxes is used with simple 4 bits word for permutation. Decent level of security in the face of attacks such as differential cryptanalysis and linear cryptanalysis can be established through the full 32 round LBlock.

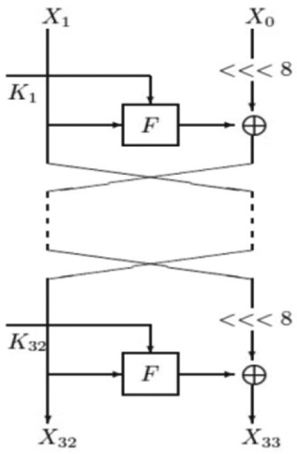

Fig. 18. LBlock Block Cipher.

4. TWINE

Presented in 2012 by Suzaki, et al., 2011, this cipher algorithm is a lightweight symmetric block cipher with 64 bits block size along with variable key length of 80 and 128 bits. The hardware implementation is 1866 (GE). It is a Classical Feistel Network (GFN) and carries out encryption and decryption operations simultaneously. It was subjected to numerous comparable choices to LBlock previous algorithm, aiming to achieve equilibrium performance on both states (hardware and software), nevertheless, the number of S-Boxes and the permutation process remain two of the most important differences between the two ciphers, whereby, the cipher based on using one 4 bits S-Box and a 4 bits XOR, as shown in Fig. 19. Security wise, this cipher algorithm claims a high level of protection, significantly against differential and saturation attacks (Ménétrey, et al., 2021). Whereas, in Yoshikawa, Nozaki and Asahi, 2016, where an electromagnetic analysis attack method directed experimentally toward TWINE, results exposed TWINE's vulnerability when it is implemented as hardware.

5. Simon and Speck

Proposed publicly in 2013 by a group of researchers in the US National Security Agency's Research Directorate (Beaulieu, et al., 2017), Simon and Speck are two ciphers lightweight symmetric block algorithms.

With an n-bits word, the Simon cipher algorithm is used, where n need to be 16, 24, 32, 48, or 64. Simon2n/mn will be referred to as Simon2n with an m-word (mn-bits) key. Simon64/128, for example, is a variation of Simon that works with 64 bits plain text blocks and a 128 bits key. XOR, AND, mod 2n addition, and left circular shift are the Speck component units. For security, Simon and Speck employ simple round functions that are iterated as many times as necessary. In comparison, other algorithms (like as AES) use more sophisticated round functions but require fewer rounds. Because the algorithms use basic round functions, they have small realizations and are well suited for application on limited platforms. The general round of speck (Beaulieu, et al., 2013; Beaulieu, et al., 2015) is depicted in Fig. 20:

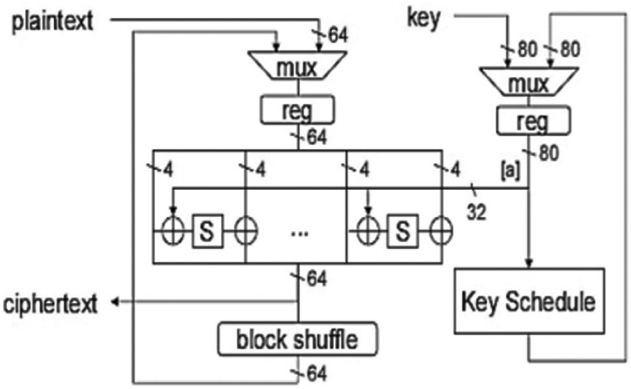

Fig. 19. The cipher design of Twine.

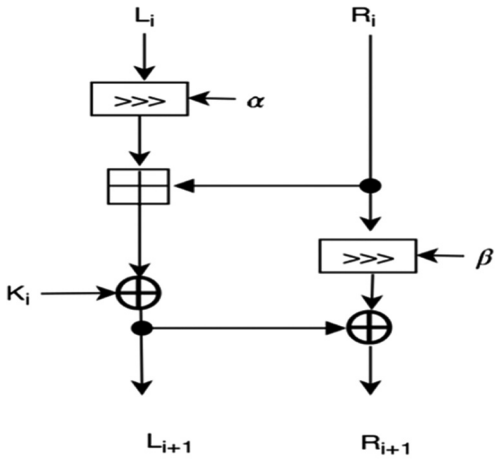

Fig. 20. General round of speck cipher.

6. RECTANGLE

This cipher algorithm, proposed by Zhang, et al., 2015, in 2014, is an ultra-lightweight block cipher with a block size of 64 bits, a variable key of 80 or 128 bits, and iterating based on SPN, as shown in Fig. 21, with a substitution mostly have of 16 (4×4) S-Boxes connected in parallel and a permutation layer consisting of three rotations. It has been demonstrated to have excellent hardware and software performance, enabling for a wide range of IOT applications (Philip, 2017).

This cipher algorithm, proposed by Zhang, et al., 2015, in 2014, is an ultra-lightweight block cipher with a block size of 64 bits, a variable key of 80 or 128 bits, and iterating based on SPN, as shown in Fig. 21, with a substitution mostly have of 16 (4×4) S-Boxes connected in parallel and a permutation layer consisting of three rotations. It has been demonstrated to have excellent hardware and software performance, enabling for a wide range of IOT applications (Philip, 2017; Philip, et al.,2018).

7. QTL

Proposed by Li, Liu and Wang 2016, in 2016, structurally as Generalized Feistel Network (GFN), this cipher algorithm is an ultra-lightweight block cipher designed for gadgets with restricted resources, with 64 bits of block size, variable key length of 64 or 128 bits iterating through 16, 20 rounds, respectively, and having a lot of S-Boxes in the encryption

http://dx.doi.org/10.14500/aro.11007

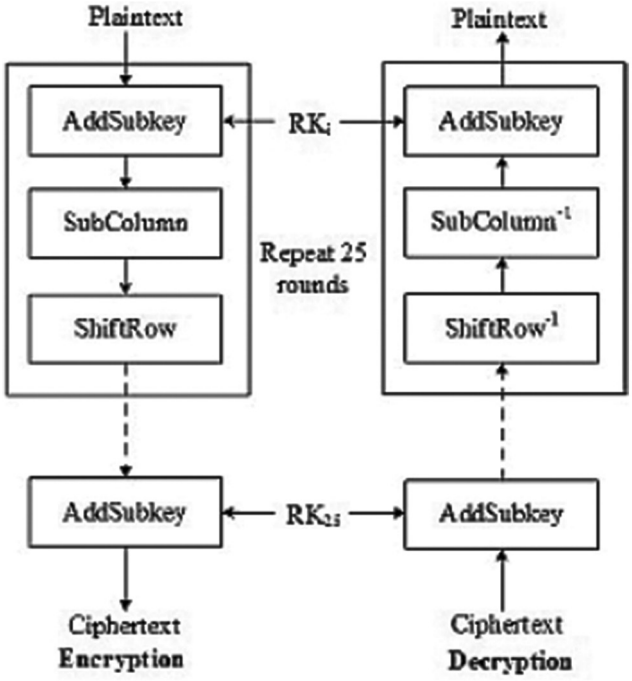

Fig. 21. The cipher design of RECTANGLE algorithm.

process. Improving the security of this cipher that has a Feistel structure was done using SPNs diffusion in the design, whereas not using a key schedule was intended to minimize hardware implementation's energy consumption (Shrivastava, Singh and Acharya, 2020). Compact HW implementation and high security as in Çoban, Karakoç and Özen, 2016, both can be achieved with QTL, a diagram of which is shown in Fig. 22.

8. BORON

Proposed by Bansod, Pisharoty and Patil, 2017, in 2017, this cipher algorithm that uses SPN, operating on a 64 bits block, supporting two key length of 80 and 128 bits, respectively, and having a total of 25 rounds, it is an ultra-lightweight block cipher with a compact structure, with higher throughput, and less power compared to other existing SPN ciphers (Sutar, 2018), and good performance concerning hardware and software platforms. It has three important components: Shift register, round permutation layers, and XOR component, as illustrated in Fig. 23 (Sutar, 2018). Opposing and deterring linear and differential attacks with this cipher are merited to the production of a high number of active S-Boxes in a small number of rounds that are possible due to its unique architecture.

9. NLBSIT

This cipher which was presented by Alahdal, et al., 2020, in 2020, designed as a new lightweight block cipher for resource restricted IOT computers due to consumption of less energy than other algorithms (encryption/decoding cycles) and less memory. Through integrating the benefits of both Feistel and SPN designs with an extra linear box idea, an increase in data security was possible to be achieved in this cipher. Structurally, it uses a key of 64 bits to encode 64 bits block size, it also uses uncomplicated mathematical

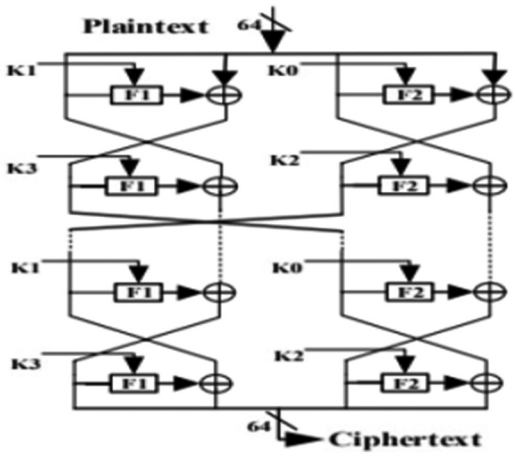

Fig. 22: QTL block cipher.

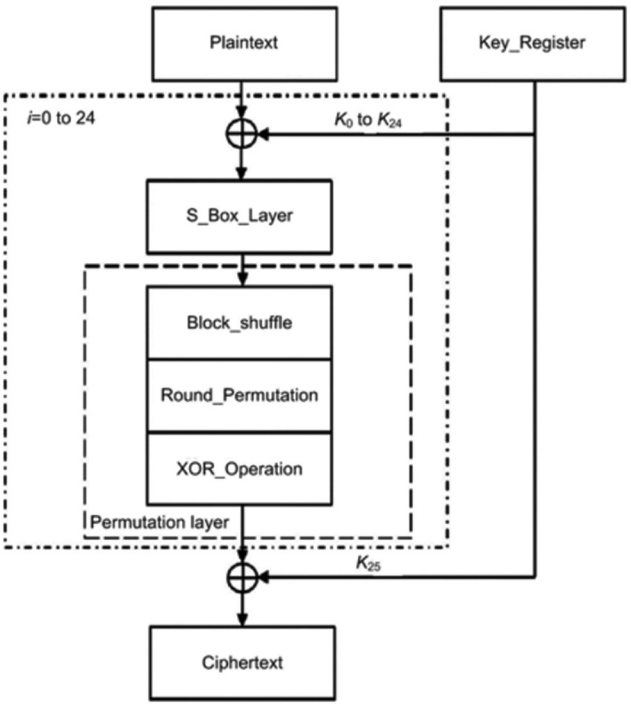

Fig. 23. BORON block cipher block diagram.

operations with fewer rounds XOR, XNOR, shifting, and swapping, as illustrated in Fig. 24. High speed and high level of security resisting all known attacks achieved by the usage of both the SPN and Feistel architectures in the creation of NLBSIT are considered among the several advantages of this cipher, in addition to the less memory and less energy consumption mentioned earlier (Alahdal, et al., 2020).

10. SAND

SAND-64 and SAND-128 are two AND-RX block ciphers having a Feistel structure. They accept 128 bits keys and have block sizes of 2n, where n refers to the branch length (n = 32 for SAND-64 and n = 64 for SAND-128). Strong security bounds and competitive performance viewed as merits of its novel design, are achieved by admitting an equivalent S-Box-based representation and thus supporting S-Box-based

TABLE V
MODERN SYMMETRIC CIPHER ALGORITHMS

Cipher name	Cipher classification	Block size	Key size	Rounds numbers	Cipher structure	S-Box
RC4	Modern stream cipher	-	-	-	-	-
Salsa20	Modern stream cipher	-	-	-	-	-
A5/1	Modern stream cipher	-	-	-	-	-
DES	Modern block cipher	64 bits	56 bits	16	Feistel based	8 S-Box
AES	Modern block cipher	128 bit	128, 192, 256 bits	10, 12, 14	SPN based	8 S-Box
Blowfish	Modern block cipher	64 bits	32–448 bits	16	Feistel based	4 S- Boxes
IDEA	Modern block cipher	64 bits	128 bit	8	Mixing of arithmetical operations	-

TABLE VI
LIGHTWEIGHT AND ULTRA-LIGHTWEIGHT SYMMETRIC CIPHER ALGORITHMS

S. No.	Cipher name	Cipher classification	Block size	Key size	Rounds numbers	Cipher structure	S-Box	P-Box
1	Fruit-v2	Ultra-lightweight stream cipher	-	-	-	-	-	-
2	LOGIC	Lightweight stream cipher	-	-	-	-	-	-
3	A4	Lightweight stream cipher	-	-	-	-	-	-
4	DESXL	Lightweight block cipher of DESX	64 bits		16	Feistel		-
5	DESL	Lightweight block cipher of DES	64 bits	56 bits	16	Feistel	Single (6 * 4 bits) S-Box 8 times	-
6	LBlock	Lightweight block cipher	64 bits	80 bits	32	Based on both Feistel and SPN	4×4 S-boxes	Permutations operate on 32bit
7	TWINE	Lightweight block cipher	64 bits	80 and 128-bit	36	Type-2 GFS	nonlinear substitution layer One 4-bit	Permutation operate on 4bits
8	Simon	Lightweight block cipher	32	64	32	Feistel Based	-	-
9	Speck	Lightweight block cipher	32	64	22	Feistel Based	-	-
10	RECTANGLE	Lightweight block cipher	64 bits	80 or 128 bits	25	SPN	16 4 bits S-Boxes	(P-layer) is composed of 3 rotations
11	QTL	Lightweight block cipher	64 bits	64 bits 128 bits	16 for 64, 20 for 128	Feistel –Based and SPNs	4×4 S-Box	Permutation operate on 16bits
12	BORON	Lightweight block cipher	64	80 bits 128 bits	25	SPN	4×4 S-Box nonlinear layer S-Box	Three sub-permutation layers Operate on 16bit
13	NLBSIT	Lightweight block cipher	64	64	5	Feistel –Based and SPN	4 S-Box	-
14	SAND-64	Lightweight block cipher	64	128	48	AND-RX block ciphers	4×8 synthetic	-

security evaluation approaches. Seeking for an easier S-Box-based cryptanalysis, the AND-RX-based design with several 4×8 S-Boxes provides a new way for the designing of AND-RX-based cipher in the future. The round function of this cipher algorithm (Chen, 2022) is explained in Fig. 25:

VII. DISCUSSION

Information security being subfield from computer science that comprises each of computer and network security, has attracted a lot of attention by several developers and scholars who's working on technologies that used every day, like smart mobile application, cloud service, and the new lifestyle using IOT.

This review presented a new classification of cryptographic, comparison between symmetric versus asymmetric cipher, comparison between stream versus block cipher, the main concepts about the components used in symmetric cipher, and finally some of selected modern and lightweight symmetric cipher algorithms are presented based on analysis its components. This review aims to illustrate how the cipher algorithms design and its properties are depending basically on the type, number, and size of components used in algorithm design.

In cryptographic fundamentals, after researched and studied many research work about cryptographic mechanism, this review present new classification that classify the cipher according to four criteria's: The number of keys that used,

http://dx.doi.org/10.14500/aro.11007

TABLE VII
CHRONOLOGICAL ORDER, PROPERTIES, VULNERABILITY, AND BASIC COMPONENTS FOR ALL CIPHER ALGORITHMS PRESENTED IN THIS REVIEW

S. No.	Cipher name	Proposed in	Chronological order	Properties	Vulnerability	Basic components
1	RC4	1984	Modern	It is simple to use and fast, strong in coding and straightforward to implement, does not require extra memory, and can handle enormous streams of data when compared to other ciphers. Frequently used	A bit-flipping attack is possible	XOR
2	Salsa20	2005	Modern	Based on ARX for keystream generator, the ChaCha cipher is closely related.	There are no differential characteristics with a probability>2^{-130}.	Modular addition, XOR, Left shift rotation
3	A5/1	2000	Modern	Flexible, common algorithms, Widely used	Hardware-based attacks are possible	XOR and 3 LFSR
4	DES	1970	Modern	Common algorithm	Not particularly secure, but very adaptable	XOR, permutation, substitution
5	AES	1977	Modern	Flexible and common algorithm	Excellent security	XOR, addition, multiplication, mixing, substitution, shifting
6	Blowfish	1993	Modern	Flexible common algorithms	Excellent security	XOR, shifting, mixing, substitution, S-Boxes
7	IDEA	1991	Modern	Less common algorithm	Vulnerable against MITM Meet-in-the-middle attack.	XOR, swap, multiplication modulo, addition modulo 2^{16}, 2^{10}+1, split, and combined
8	Fruit-v2	2016	Ultra-lightweight	The cipher design includes a new round key function as well as a new initialization strategy. Increase the LFSR's size.	More resistant to traditional time and memory-data trade-offs than other ciphers.	1 LSFR and 1 NSFR
9	LOGIC	2019	Lightweight	Suited for devices with a limited amount of resources.	a security margin that is too tiny	2 NFSRs
10	A4	2020	Lightweight	Low computational cost	Fundamental cryptographic attacks resistant.	1 LFSR and 1 FCSR
11	DESL	2006	Lightweight	DESL encryption is more power efficient than DES, requiring 20% fewer gate equivalences and 25% less DES implementation.	More secure against specific types of cryptanalyses, including linear and differential because of the S-Box's non-linearity, it is more resistant to the Davies-Murphy attack, more size optimized, and more power efficient than DES.	XOR, S-Box, permutation
12	LBlock	2011	Lightweight	Improve hardware performance while also increasing software efficiency.	More secure against differential and linear, related key, integral attack.	XOR, S-Box, permutations, left cyclic shift, right cyclic shift, concatenation
13	TWINE	2012	Lightweight	Its primarily intended to fit into very small hardware.	Its security naturally needs to be studied further.	XOR, S-Box, permutation, split, and combined
14	Simon	2013	Lightweight	Simplicity, ease of implementation, and efficient implementations, attractive for homomorphic encryption, as does support for a broad 12 range of block and key sizes.	a security margin that is too tiny	Exclusive-OR, AND, left circular shift
15	Speck	2013	Lightweight	Simplicity, easy to implement, efficient implementations, attractive for homomorphic encryption, support for a broad 12 range of block and key sizes	A security margin that is too tiny	Exclusive-OR, addition modulo 2^n, left and right circular shifts
16	RECTANGLE	2014	Lightweight	By leveraging bit-slice techniques, the primary purpose of this cipher design is to allow for lightweight and rapid implementations.	Differential and linear distinguisher; Statistical Saturation Attack are all impossible to build. Also offers adequate protection to withstand integral cryptanalysis and key schedule assaults	XOR, S-Box, row rotated, permutation

(*Contd...*)

TABLE VII
(*Continued*)

S. No.	Cipher name	Proposed in	Chronological order	Properties	Vulnerability	Basic components
17	QTL	2016	Lightweight	suited for devices with a limited amount of resources.	achieves a high level of security. Differential, linear, algebraic, and related-key attacks are all safe.	Permutation operate on 16 bits, S-Box layer, exclusive-OR
18	BORON	2017	Lightweight	Low-power encryption with excellent performance on both the software and hardware platforms.	Linear, differential, key scheduling, and key collision attacks are all resistant.	Shift, permutation layers, exclusive-OR
19	NLBSIT	2020	Lightweight	Using simple mathematics, requires less energy and memory.	Linear, differential, Weak Key, Related keys, and square attack resistance.	XOR, XNOR, shifting and swapping
20	SAND-64	2020	Lightweight	One of the most lightweight primitives available in software	All of its variants are resistant to MITM (Meet-in-the-Middle) attack	AND, rotation, and XOR

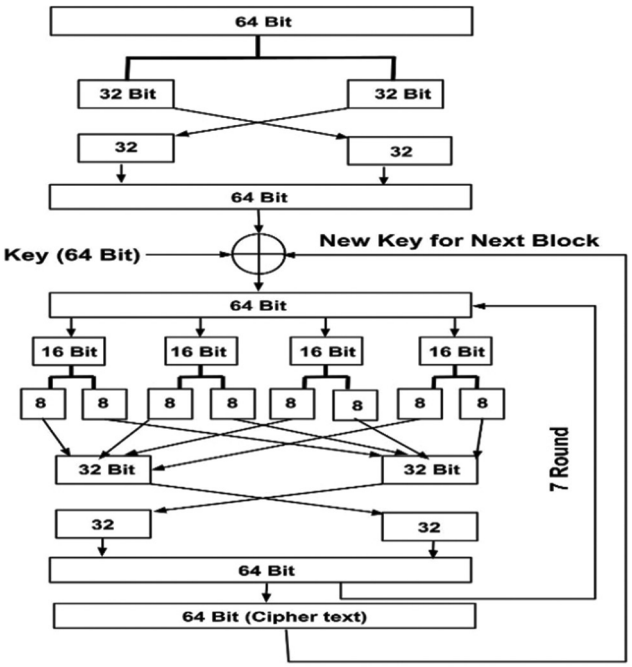

Fig. 24. The encipherment of NLBSIT algorithm.

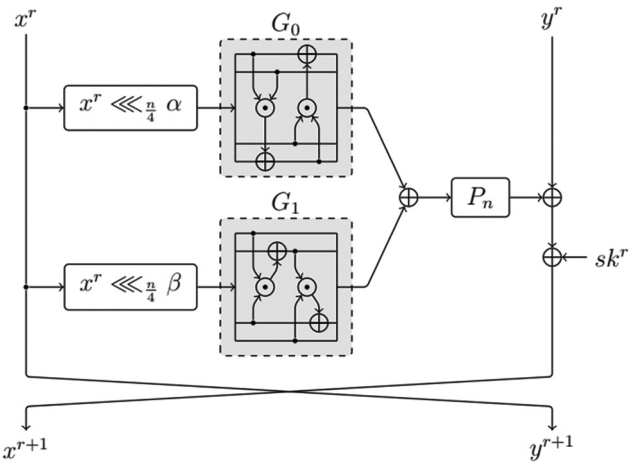

Fig. 25. Round function of SAND.

the type of encryption operation, the way of processing the plain text, and finally classifies according to chronological order. Farther more the cipher algorithm can classify to more than 1 type as illustrate in Section 2, these new classifications help to give fast and comprehensive understanding for cryptographic fundamentals.

In first comparison presented in this review between symmetric and asymmetric cipher, the conclusion was: That the two most important properties, the fast and less complex for symmetric cipher are due to the component units used in cipher algorithm design like XOR, S-Box, P-Box, circular shift, swap, split, and combined that used in cipher algorithm design, which different from asymmetric cipher that depending on numbering manipulation in cipher algorithm design. Furthermore, these properties make the symmetric cipher type the best solution for lightweight cipher applications. The second comparison presented is between the stream cipher and block cipher, the main types of symmetric cipher, the different of stream from block is not only in the way of processing the plain text but also the components that used in algorithm design are different, it is depends basically on FSR and XOR components, whereas in block cipher, the algorithm design depends on using other components such as S-Box, P-Box, split, and combine as mention previously. It is important to mention that these collection of components made the used of block cipher more versatile than stream ciphers, where used in many of lightweight cipher applications.

From the review of modern, lightweight and ultra-lightweight symmetric cipher algorithms in this research; 3 modern stream ciphers, 4 modern block ciphers, 3 lightweight stream ciphers, and 10 lightweight/ultra-lightweight block ciphers are presented, studied, and listed in Tables V and VI, respectively, based on chronological order classification. The conclusion from studying these cipher algorithms is: The type of cipher algorithm whether if it is modern or lightweight is basically depending on the type, the number, and size of components that used in cipher algorithm design. The number and size of components in lightweight type are less than those of conventional ciphers. Hence, the conclusion,

the type, number, and the size of component will effect in obtain new cipher algorithm that is more suitable solution for today information security applications. In addition, the final conclude is that the important and basic component that used in all types of symmetric cipher is XOR, due to the important properties of this component as illustrate in Section 3.2.2. Another important and basic component used in symmetric block cipher is S-Box that achieves confusion between the cipher text and the secret key.

In the end of this section, Table VII summarizes the major characteristics, chronological order, vulnerability, and basic components of each cipher algorithm presented in this review research.

VIII. Conclusion

This review is providing an overview of cryptography fundamental, theoretical background of symmetric ciphers with its two main types (stream and block), main concepts of the components used in symmetric cipher and finally some of selected modern and lightweight symmetric algorithms are presented. The present review was attempt to present the cipher algorithm depending on the basic components that used in cipher design, and explain how these components kind's, number, and size effect on the classification of cipher algorithm and on performance, area, and its weight. Better understating of various algorithms following their establishment, design, function, and field of application can be found in this study, with futuristic aspirations for more analysis and development that can lead to improvement of pre-existing new encryption algorithms or the evolution of new ones.

References

Afdhila, D., Nasution, S.M. and Azmi, F., 2016. Implementation of stream cipher Salsa20 algorithm to secure voice on push to talk application. In: *2016 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob)*. IEEE, United States. pp.137-141.

Alahdal, A., AL-Rummana, G.A., Shinde, G.N. and Deshmukh, N.K., 2020. NLBSIT: A new lightweight block cipher design for securing data in IOT devices. *International Journal of Computer Sciences and Engineering*, 8(10), p.13.

Aljazeera, K.R., Nandakumar, R. and Ershad, S.B., 2016. Design and characterization of L Block cryptocore. In: *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES*). IEEE, United States. pp.166-172.

Amiri, M.A., Mahdavi, M. and Mirzakuchaki, S., 2009. QCA implementation of A5/1 stream cipher. In: *2009 Second International Conference on Advances in Circuits, Electronics and Micro-Electronics*. IEEE, United States. pp.48-51.

Anand, A., Raj, A., Kohli, R. and Bibhu, V., 2016, Proposed symmetric key cryptography algorithm for data security. In: *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*. IEEE, United States. pp.159-162.

Bagane, P. and Sirbi, D.K., 2021. Comparison between traditional cryptographic methods and genetic algorithm based method towards Cyber Security. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, 12(2), pp.676-682.

Bansod, G., Pisharoty, N. and Patil, A., 2017. BORON: An ultra-lightweight and low power encryption design for pervasive computing. *Frontiers of Information Technology and Electronic Engineering*, 18(3), pp.317-331.

Bardis, N.G., Markovskyy, A.P. and Andrikou, D.V., 2004. Method for designing pseudorandom binary sequences generators on Nonlinear Feedback Shift Register(NFSR). *WSEAS Transactions on Communications*, 3(2), pp.758-763.

Basu, S., 2011. International data encryption algorithm (Idea)-a typical illustration. *Journal of Global Research in Computer Science*, 2(7), pp.116-118.

Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B. and Wingers, L., 2017. Notes on the design and analysis of SIMON and SPECK.

Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B. and Wingers, L., 2013. *Implementation and Performance of the Simon and Speck Lightweight Block Ciphers on ASICs*. Unpublished Work.

Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B. and Wingers, L., 2015. The SIMON and SPECK lightweight block ciphers. In: *Proceedings of the 52nd Annual Design Automation Conference.* pp.1-6.

Chen, S., Fan, Y., Sun, L., Fu, Y., Zhou, H., Li, Y., Wang, M., Wang, W. and Guo, C., 2022. SAND: An AND-RX Feistel lightweight block cipher supporting S-box-based security evaluations. *Designs, Codes and Cryptography*, 90(1), pp.155-198.

Chiadighikaobi, I.R. and Katuk, N., 2021. A scoping study on lightweight cryptography reviews in IOT. *Baghdad Science Journal*, 18(2), pp.989-1000.

Chugunkov, I.V., Kliuchnikova, B.V., Riakhovskaia, I.S., Chernikova, E.A. and Chugunkov, V.I., 2020. Improvement of P-box efficiency. In: *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. IEEE, United States. pp.274-276.

Çoban, M., Karakoç, F. and Özen, M., 2016. Cryptanalysis of QTL Block cipher. In: *International Workshop on Lightweight Cryptography for Security and Privacy*. Springer, Cham. pp.60-68.

De Canniere, C., Biryukov, A. and Preneel, B., 2006. An introduction to block cipher cryptanalysis. *Proceedings of the IEEE*, 94(2), pp.346-356.

Ding, L., Liu, C., Zhang, Y. and Ding, Q., 2019. A new lightweight stream cipher based on chaos. *Symmetry*, 11(7), p.853.

Dreier, J., Hirschi, L., Radomirovic, S. and Sasse, R., 2018. Automated unbounded verification of stateful cryptographic protocols with exclusive OR. In: *2018 IEEE 31st Computer Security Foundations Symposium (CSF).* IEEE, United States. pp.359-373.

Dutta, I.K., Ghosh, B. and Bayoumi, M., 2019. Lightweight cryptography for internet of insecure things: A survey. In: *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, United States. pp.0475-0481.

Easttom, W., 2021. S-box design. In: *Modern Cryptography.* Springer, Cham. pp. 187-204.

Ekdahl, P. and Johansson, T., 2003. Another attack on A5/1. *IEEE Transactions on Information Theory*, 49(1), pp.284-289.

Forouzan, B.A. and Mukhopadhyay, D., 2015. *Cryptography and Network Security*. Vol. 12. McGraw Hill Education (India) Pvt Ltd., New York, NY, USA.

Fukushima, K., Xu, R., Kiyomoto, S. and Homma, N., 2017. Fault injection attack on Salsa20 and ChaCha and a lightweight countermeasure. In: *2017 IEEE Trustcom/BigDataSE/ICESS*. IEEE, United States. pp.1032-1037.

Ghosh, A., 2020. Comparison of encryption algorithms: AES, Blowfish and Twofish for security of wireless networks. *International Research Journal of Engineering Technology*, 7, pp.4656-4658.

Hamza, A. and Kumar, B., 2020, A review paper on DES, AES, RSA encryption standards. In: *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART).* IEEE, United States. pp.333-338.

Hasan, M.K., Shafiq, M., Islam, S., Pandey, B., Baker El-Ebiary, Y.A., Nafi, N.S., Rodriguez, R.C. and Vargas, D.E., 2021. Lightweight cryptographic algorithms

for guessing attack protection in complex internet of things applications. *Complexity*, 2021, 5540296.

Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I. and Manifavas, C., 2018. A review of lightweight block ciphers. *Journal of Cryptographic Engineering*, 8(2), pp.141-184.

Hussain, I. and Shah, T., 2013. Literature survey on nonlinear components and chaotic nonlinear components of block ciphers. *Nonlinear Dynamics*, 74(4), pp.869-904.

Hussaini, S., 2020. Cyber security in cloud using blowfish encryption. *International Journal of Information Technology*, 6(5).

Jassim, S.A. and Farhan, A.K., 2021. A survey on stream ciphers for constrained environments. In: *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*. IEEE, United States. pp.228-233.

Jiao, L., Hao, Y. and Feng, D., 2020. Stream cipher designs: A review. *Science China Information Sciences*, 63(3), pp.1-25.

Jindal, P. and Singh, B., 2015. RC4 encryption-a literature survey. *Procedia Computer Science*, 46, pp.697-705.

Kitsos, P., Sklavos, N., Parousi, M. and Skodras, A.N., 2012. A comparative study of hardware architectures for lightweight block ciphers. *Computers and Electrical Engineering*, 38(1), pp.148-160.

Kousalya, R. and Kumar, G.S., 2019. A survey of light-weight cryptographic algorithm for information security and hardware efficiency in resource constrained devices. In: *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN).* IEEE, United States. pp.1-5.

Kumar, D.S., Suneetha, C.H. and Chandrasekhar, A., 2012. A block cipher using rotation and logical XOR operations. *arXiv preprint arXiv:1202.1898.*

Kumar, P. and Rana, S.B., 2016. Development of modified AES algorithm for data security. Optik, 127(4), pp.2341-2345.

Lakhtaria, K.I., 2011. Protecting computer network with encryption technique: A study. In: *International Conference on Ubiquitous Computing and Multimedia Applications.* Springer, Berlin, Heidelberg. pp.381-390.

Li, L., Liu, B. and Wang, H., 2016. QTL: A new ultra-lightweight block cipher. *Microprocessors and Microsystems*, 45, pp.45-55.

Lu, M., Fan, A., Xu, J. and Shan, W., 2018. A compact, lightweight and low-cost 8-bit datapath AES circuit for IOT applications in 28nm CMOS. In: *2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE).* IEEE, United States. pp.1464-1469.

Madarro-Capó, E.J., Legón-Pérez, C.M., Rojas, O. and Sosa-Gómez, G., 2021. Information theory based evaluation of the RC4 stream cipher outputs. *Entropy*, 23(7), p.896.

Mathew, S., Satpathy, S., Suresh, V., Anders, M., Kaul, H., Agarwal, A., Hsu, S., Chen, G. and Krishnamurthy, R., 2015. 340 mv-1.1 v, 289 gbps/w, 2090-gate nanoaes hardware accelerator with area-optimized encrypt/decrypt GF (2 4) 2 polynomials in 22 nm tri-gate CMOS. *IEEE Journal of Solid-State Circuits*, 50(4), pp.1048-1058.

Ménétrey, J., Pasin, M., Felber, P. and Schiavoni, V., 2021. Twine: An embedded trusted runtime for webassembly. In: *2021 IEEE 37th International Conference on Data Engineering (ICDE).* IEEE, United States. pp.205-216.

Mewada, S., Sharma, P. and Gautam, S.S., 2016. Classification of efficient symmetric key cryptography algorithms. *International Journal of Computer Science and Information Security*, 14(2), p.105.

Mohandas, N.A., Swathi, A., Abhijith, R., Nazar, A. and Sharath, G., 2020. A4: A lightweight stream cipher. In: *2020 5th International Conference on Communication and Electronics Systems (ICCES).* IEEE, United States. pp.573-577.

Muchsin, H.N., Sari, D.E. and Rachmawanto, E.H., 2019. Text encryption using extended bit circular shift cipher. In: *2019 Fourth International Conference on Informatics and Computing (ICIC)*. IEEE, United States. pp.8138-8143.

Naser, N.M. and Naif, J.R., 2022. A systematic review of ultra-lightweight encryption algorithms. *International Journal of Nonlinear Analysis and Applications*, 13(1), pp.3825-3851.

Pachghare, V.K., 2019. *Cryptography and Information Security*. PHI Learning Pvt. Ltd., New Delhi.

Patil, P., Narayankar, P., Narayan, D.G. and Meena, S.M., 2016. A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and blowfish. *Procedia Computer Science*, 78, pp.617-624.

Patil, S. and Bhusari, V., 2014. An enhancement in international data encryption algorithm for increasing security. *International Journal of Application or Innovation in Engineering and Management*, 3(8), pp.64-70.

Philip, M.A., 2017. A survey on lightweight ciphers for IOT devices. In: *2017 International Conference on Technological Advancements in Power and Energy (TAP Energy).* IEEE, United States. pp.1-4.

Philip, M.A., Vaithiyanathan, V. and Jain, K., 2018. Implementation analysis of rectangle cipher and its variant. In: *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology (RTEICT).* IEEE, United States. pp.474-479.

Poschmann, A., Leander, G., Schramm, K. and Paar, C., 2006. A Family of Light-Weight Block Ciphers Based on DES Suited for RFID Applications. Vol. 6. *Workshop on RFID Security-RFIDSec.*

Qadir, A.M. and Nurhayat, V., 2019. A review paper on cryptography. *International Symposium on Digital Forensics and Security (ISDFS)*. IEEE, United States. pp.1-6.

Qiao, Z., El Assad, S. and Taralova, I., 2020. Design of secure cryptosystem based on chaotic components and AES S-Box. *AEU-International Journal of Electronics and Communications*, 121, p.153205.

Raza, A.R., Mahmood, K., Amjad, M.F., Abbas, H. and Afzal, M., 2020. On the efficiency of software implementations of lightweight block ciphers from the perspective of programming languages. *Future Generation Computer Systems*, 104, pp.43-59.

Sadkhan, S.B. and Jawad, N.H., 2015. Simulink based implementation of developed A5/1 stream cipher cryptosystems. *Procedia Computer Science*, 65, pp.350-357.

Sallam, S. and Beheshti, B.D., 2018. A survey on lightweight cryptographic algorithms. In: *TENCON 2018-2018 IEEE Region 10 Conference*. IEEE, United States. pp.1784-1789.

Schneier, B., 1993. Description of a new variable-length key, 64-bit block cipher (Blowfish). In: *International Workshop on Fast Software Encryption*. Springer, Berlin, Heidelberg. pp.191-204.

Sharma, D.K., Singh, N.C., Noola, D.A., Doss, A.N. and Sivakumar, J., 2022. A review on various cryptographic techniques and algorithms. *Materials Today: Proceedings*, 51, pp.104-109.

Shrivastava, N., Singh, P. and Acharya, B., 2020. Efficient hardware implementations of QTL cipher for RFID applications. *International Journal of High Performance Systems Architecture*, 9(1), pp.1-10.

Sliman, L., Omrani, T., Tari, Z., Samhat, A.E. and Rhouma, R., 2021. Towards an ultra-lightweight block ciphers for Internet of Things. *Journal of Information Security and Applications*, 61, p.102897.

Soomro, Z.A., Shah, M.H. and Ahmed, J., 2016. Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), pp.215-225.

Stallings, W., Brown, L., Bauer, M.D. and Howard, M., 2012. *Computer Security: Principles and Practice*. Vol. 2. Pearson, Upper Saddle River.

Sutar, S.A., 2018. Differential power attack analysis of ultra-lightweight block cipher

BORON. In: *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*. IEEE, United States. pp. 365-370.

Suzaki, T., Minematsu, K., Morioka, S. and Kobayashi, E., 2011. Twine: A Lightweight, Versatile Block Cipher. Vol. 2011. In: *ECRYPT Workshop on Lightweight Cryptography*.

Szaban, M. and Seredynski, F., 2011. Designing cryptographically strong S-boxes with use of ID cellular automata. *Journal of Cellular Automata*, 6(1).

Wahid, M.N., Ali, A., Esparham, B. and Marwan, M., 2018. A comparison of cryptographic algorithms: DES, 3DES, AES, RSA and blowfish for guessing attacks prevention. *Journal Computer Science Applications and Information Technology*, 3(2), pp.1-7.

Wang, S., Liu, M., Lin, D. and Ma, L., 2019. Fast correlation attacks on grain-like small state stream ciphers and cryptanalysis of plantlet, fruit-v2 and fruit-80.

Wang, S., Liu, M., Lin, D. and Ma, L., 2022. On grain-like small state stream ciphers against fast correlation attacks: Cryptanalysis of plantlet, fruit-v2 and fruit-80. *The Computer Journal,* bxac016.

Wu, W. and Zhang, L., 2011. L Block: A lightweight block cipher. In: *International Conference on Applied Cryptography and Network Security*. Springer, Berlin, Heidelberg. pp.327-344.

Yihan, W. and Yongzhen, L., 2021. Improved design of DES algorithm based on symmetric encryption algorithm. In: *2021 IEEE International Conference on Power Electronics, Computer Applications (ICPECA)*. IEEE, United States. pp. 220-223.

Yoshikawa, M., Nozaki, Y. and Asahi, K., 2016. Electromagnetic analysis attack for a lightweight block cipher TWINE. In: *2016 IEEE/ACES International Conference on Wireless Information Technology and Systems (ICWITS) and Applied Computational Electromagnetics (ACES*). IEEE, United States. pp.1-2.

Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B. and Verbauwhede, I., 2015. RECTANGLE: A bit-slice lightweight block cipher suitable for multiple platforms. *Science China Information Sciences*, 58(12), pp.1-15.

Zhao, W., Ha, Y. and Alioto, M., 2015. AES architectures for minimum-energy operation and silicon demonstration in 65nm with lowest energy per encryption. In: *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, United States. pp.2349-2352.