International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 5 (2018) pp. 2258-2270
© Research India Publications. http://www.ripublication.com

Lightweight Block Ciphers for IoT based applications: A Review

Deepti Sehrawat and Nasib Singh Gill

Department of Computer Science & Applications
Maharshi Dayanand University, Rohtak, Haryana, India.
E-mail: dips.scorpio@gmail.com, nasibsgill@gmail.com,

Abstract

Now-a-days Internet of Things is a novel paradigm shift in Information Technology arena. It is playing a vital role in everyone's life by bringing physical objects and living things into the sphere of the cyber world. Different tagging technologies make it possible to identify physical objects and connect everything to communicate and share information. The communication must be secured in IoT with confidentiality, integrity and authentication services. A number of new factors like limited computational power, RAM size, ROM size, register width, different operating environment and etc. constrained IoT to use traditional security measures. These constraints on IOT enabled devices results in the emergence of a new field, Lightweight Cryptography. Recently a number of software and hardware implementation of lightweight ciphers are designed for IoT applications. These are broadly classified as Hash functions, Stream ciphers, and block ciphers. Software implementations have lower cost and provide more flexibility on manufacturing and maintenance. This paper presents a comparative study of various lightweight block ciphers suitable for IoT applications along with their benefits and limitations. A number of cryptanalysis is also done over these ciphers by various cryptanalysts and their effects on the ciphers are also studied in this paper. A future dimension is also proposed to develop a good lightweight cipher.

Keywords: Lightweight, block ciphers, RFID, ciphers, SPN, Feistel, Feistel-M, GFN, IoT.

INTRODUCTION

Recently infrastructure systems like smart home, smart grid, smart city, and intelligent transportation connect our world with a concept known as Internet of Things (IoT). Internet of things connects not only the inanimate things but also the living things like plants, people and animals. In this physical or material world things are real objects that can be distinguishable by real world [1]. The concept of IoT was introduced in 1999 after the explosion of the wireless device market and the introduction of technologies like RFID (Radio Frequency Identification) and WSN (Wireless Sensor Networks). It is simple and powerful where objects in the physical world having sensors within or attached communicate with each other via wireless connectivity.

Radio Frequency Identification systems are the important components of IoT. RFID is composed of a number of RFID tags which are having a unique identifier that can distinguish them and several readers. Readers activate the transmission in tag by generating suitable signals illustrating a query for respective tag. RFID chips are used as sensors in objects to monitor some specific conditions like pressure, location, motion, temperature, vibration and etc. To provide information, sensors are connected to other sensors and systems. Sensors can use wide area connections like GPRS (General Packet Radio Service), LTE (Long-Term Evolution), GSM (Global System for Mobile communication), and 3G (Third Generation) whereas for local area connections sensors can use RFID, NFC (Near-field communication), Bluetooth, Zigbee and WiFi (Wireless Fidelity) connections. Sensor networks are used in numerous applications including health care, smart home, military, environment/ earth monitoring, intelligent transportation and many more. Sensor nodes in sensor networks communicate in a wireless multi-hop fashion. Sensor nodes generally report to special nodes called sinks [2].

Devices are interconnected via distributed sensor networks in a sophisticated dynamic system in order to transmit control instructions and valuable information. IoT-enabled objects have digital identity and connectivity to share information in a real-time or at defined intervals about their condition and surrounding environment with people, software system, and other IoT-enabled devices. Using networked embedded devices, IoT achieves intelligent monitoring and management.

With the expansion of imminent 5G technology for seamless communication, IoT is attracting more attention. IoT communication in this heterogeneous 5G environment is vulnerable to eavesdropping attack. Authors in [3] presented a secure relay communication for IoT networks to prevent from randomly distributed eavesdroppers attack. The protection of data and privacy of users has been identified as one of the key challenges in the IoT [4].

Cryptography is the main aspect of security and a cipher encrypts a plain text into cipher text and again converts cipher text to plain text. The cryptographic algorithm is generally classified as a hash function, a stream cipher or a block cipher. Block ciphers are considered to be workhorses in the cryptographic environment. In this paper, our goal is to summarize the various lightweight block ciphers with their strengths and weaknesses. We analyzed the effects of various attacks on these ciphers.

The rest of the paper is organized as follows: In section 2 we summarize security issues related to IoT based applications and a comparison among various techniques used by different lightweight ciphers. In Section 3, various existing lightweight block ciphers are summarized. After giving various security solutions for IoT based applications, we compare the various existing software implemented lightweight block ciphers. We conclude the paper with section 4.

IoT SECURITY

In IoT paradigm, many of the physical world objects will be on the network in any form creating a heterogeneous environment for Internet of Things. In such environment, there is a need to encrypt information so that chip identification can be prevented from an eavesdropper. The communication must be secured in IoT with confidentiality, integrity and authentication services. The data inside sensor nodes must be stored in an encrypted form. Along with the encryption of data; firewalls and IDC (Intrusion Detection Systems) are also required because of Internet and WSN, with which sensors are exposed.

IoT is constrained by a number of new factors like participation of a huge number of nodes; IoT devices have usually limited computational power, different operating environment. As a result, security challenges become more difficult to fulfill “one fits all” security strategy.

Cryptography is a main aspect of security. Its main functions are confidentiality, Privacy, Authentication, and Integrity. A number of security standards are available now-a-days like AES [5] and DES. These ciphers have higher gate counts and high power dissipation. For IoT enabled devices using these types of cipher are practically not possible. As small-scale embedded system uses 4-bit/8-bit processors which have a very small memory size and even cannot afford high power dissipating applications. In the global CPU market, 8-bit microcontrollers are prime contributors. These have some constraints like RAM size, ROM/Flash size, limited arithmetic capabilities, register width and clock speed. These constraints on IOT enabled devices results in the emergence of a new field, Lightweight Cryptography. Recently a number of software and hardware implementation of lightweight ciphers are designed for IoT applications like PRESENT [6], RECTANGLE [7], SIMON [8], SPECK [8], TWINE [9], HUMMINGBIRD-2 [10], PICCOLO[11], PICO [12], HISEC [13], ROADRUNNER [14], Extended-LILIPUT [15], SIT [16], SKINNY [17], MANTIS [17], CLEFIA [18], KLEIN [19], XTEA [20], LED [21] and many more. Some of these ciphers are suitable for software implementation while others have better performance in hardware implementation. Software implementations have lower cost and provide more flexibility in manufacturing and maintenance.

A cryptography algorithm is mainly of three types:

1. **Hash Function:**

By providing a digital fingerprint, hash function uses a mathematical transformation and is primarily used for message integrity.

2. **Public Key Cryptography or asymmetric encryption:**

An Asymmetric algorithm is primarily used for authentication and non-repudiation. A different key is used for encryption and decryption.

3. **Secret key cryptography or symmetric encryption**:

A Symmetric algorithm is used mainly for confidentiality and privacy and a single key is used for both encryption and decryption. Each round has some mathematical functions for confusion and diffusion. Secret key cryptography can be categorized as either block cipher algorithm or stream cipher algorithm. Stream ciphers encrypt/ decrypt a single bit at a time with continuously changing key and are well suited to real-time applications like audio and video. Block ciphers encrypt/ decrypt one block from data at a time with the same key on each block.

Block cipher is practically easier to implement, more efficient and can achieve higher diffusion and error propagation in comparison to stream ciphers. Some of the block ciphers are designed to provide security authentication or integrity protection which is not provided by any of the stream ciphers. In this paper we have summarized various existing lightweight block ciphers because of its more usefulness when the data amount is pre-known such as a data file, fields, or request protocols. Block ciphers are considered to be workhorses in the cryptographic environment.

Block Cipher

Block ciphers have fixed block size and key size. Confusion and Diffusion are two operations used in block cipher for encryption. Confusion makes complex relationship among encryption key and cipher text. Every bit of key is supposed to influences every bit of cipher text. Diffusion propagates influence of each bit in the block of plain text over a number of bits in cipher text block making cipher text oversensitive to statistical attacks [23].

Types of Block ciphers:

Block cipher can be of type; Substitution Permutation Network (SPN) and Feistel based network. Feistel networks can be further classified as classical Feistel Networks and Generalized Feistel networks.

1. Feistel structures

Feistel structure operates on only half of the data per round and generally requires more rounds in comparison to SPNs. Decryption function in the Feistel type structure do not require much implementation cost as Feistel structure use same program code for both encryption and decryption operations in order to decreases the memory requirements. CLEFIA [18], SIMON [8], PICCOLO [11], TWINE [9], SPECK [8], and XTEA [20] are some popular Feistel networks. Feistel networks have further two classifications as Classical Feistel

Structures (CFS) and Generalized Feistel structures (GFS). To provide optimum security GFS require more number of rounds.

2. Substitution Permutation Networks (SPN)

SPN has a chain of linked mathematical operations. A combination of substitution layer with permutation layer along with key mixing constitutes a round of SPN. A substitution function or confusion function provides confusion and constitutes a substitution/ confusion layer. This layer constitutes non-linear operations provided by S-boxes (Look-up-Tables based) or by using bit-slice implementation. Permutation layer has P-box and is also called diffusion layer. Permutation layer constitutes invertible linear transformations or simple fixed permutations (bit-wise or word-wise). It has extra inherent parallelism for confusion and diffusion and it requires S-box to be invertible. AES [5], PRESENT [6], KLEIN [19], LED [21] and mCrypton [22] are some latest and widely used SPN block ciphers.

Figure 1 shows the comparative use of techniques in different lightweight block ciphers by researchers against the number of publications mentioned in this paper.

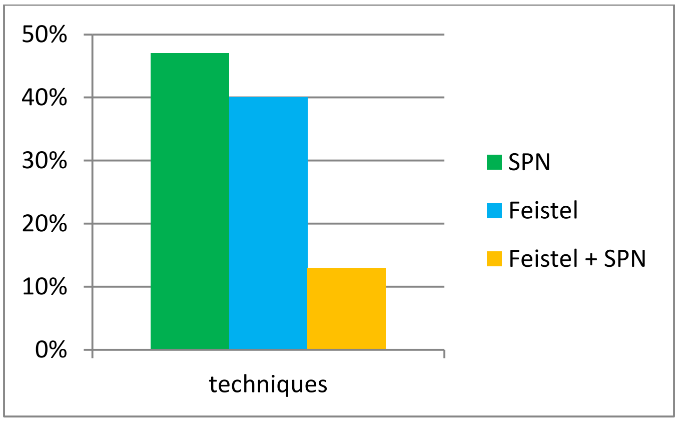

Figure 1: Comparative Use of Various Techniques in Lightweight Block Ciphers

Features of Good Lightweight Ciphers

Designing a good, memory efficient, resource efficient and robust lightweight cipher requires a number of features to be considered. The important features of a good lightweight cipher are as follows:

a) Less complexity

b) Robust architecture

c) Rich encryption standard

d) High Throughput

e) Less Execution time

f) Requires less memory, software implementation (code size, RAM size)

g) Need smaller hardware implementation

h) Consumes less power (energy consumption)

i) Good immunity against linear and differential attacks.

j) Prevent possible advance attacks like Biclique attack, Zero correlation attack, Meet-In-The-Middle attack (MITM), Algebraic attacks and etc.

SURVEY OF EXISTING TECHNIQUES

In the past two decades, Internet of Things (IoT) has emerged as a distinguishable approach and it has attracted the attention of many researchers. Security and Privacy is the major concern in IoT. Lightweight cryptography is the main aspect of security which has led to many results being published in the research literature. The following section presents some research in the field related to IoT.

Paulo S.L.M. Barreto and Vincent Rijmen (2000) presented a lightweight SPN block cipher KHAZAD that favors component reuse following WTS [24] (Wide Trail Strategy). In WTS round transformations have two invertible steps; first, local non-linear transformation (any output bit depends upon a limited number of input bits) and second, a linear mixing transformation for achieving high diffusion. KHAZAD have a 64-bits long block and its key size is 128-bits. Its S-box is randomly generated and decryption differs from encryption only in the key schedule [25].

Kazumaro Aoki *et al.* (2000) presented Camelia, a 128-bit Feistel block cipher having 128/192/256-bit keys with 18/24/24 round for Camelia-128/192/256 respectively. It uses four different 8X8 S-box in the non-linear layer, designed to minimize hardware size with additional input/output key whitening. The F-function uses SPN structure and is inserted after every 6 round [26].

Phillip Rogaway *et al.* (2001) described a parallelizable block-cipher mode of operation, named OCB for efficient Authenticated Encryption that provides privacy and authenticity. OCB is an advancement over IAPM that performs encryption on arbitrary length bit string $M \in \{0, 1\}*$ using $|M|/n\_$ + 2block-cipher invocations, where n is the block length. In it offset calculation and session setups are economical and a single cryptographic key is proposed. There is no extended-precision addition and proposed block cipher calls are most favorable [64].

William C. Barker and Elaine Barker (2004) specified TDEA **(**Triple Data Encryption Algorithm) Feistel block cipher by implementing DEA cryptographic engine. Its block size is 64-bit and key size is also 64-bit (56 bits randomly generated by the algorithm as key bits and remaining 8-bits used for error detection). Operations performed in DEA engine are initial permutation, complex key dependent computation, and inverse initial permutation. DEA engine runs in two directions – forward and reverse. It is the sequence in which the key bits are used that varies in these two directions. In TDEA forward and inverse operation is defined as a compound operation of DEA forward and inverse transformations. TDEA key consists of a key bundle, KEY with three keys. To be secure the number of blocks processed with on bundle key should be less than 232 [27].

Katsuyuki Takashima (2005) designed mCrypton (miniature of Crypton), a lightweight SPN enhancement over Crypton. It has 64-bit block size, 64/96/128-bits key size and number of rounds are 12. Round transformation has four steps: substitution (nibble-wise using four 4-bit S-boxes), bit permutation (Column-wise), transposition (Column-to-Row), and key addition. mCrypton processes 8-byte data block into 4X4 nibble array representation as in Crypton. Key scheduling consists two stages; the first stage is a key generation for round using S-boxes and the second stage is key variable update through round constant and rotations (word-wise and bit-wise). S-boxes used in key scheduling are same as that in round transformation. Decryption differs by encryption with a different key schedule [22]. There exists a MITM attack on mCrypton [28].

Francois-Xavier *et al.* (2006) designed a Feistel lightweight block cipher, SEA for software implementations on an 8-bit processor. SEA*n,b* operates on a number of blocks and key sizes. Operations performed in SEA are: bitwise Exclusive-OR; S-box in parallel; word rotation and inverse word rotation; bit rotation and; addition mod. In key scheduling, during half rounds, the master key is encrypted while during the other half rounds master key is decrypted [29].

A. Bogdanov *et al.* (2007) specified a SPN block cipher PRESENT suitable for hardware implementations. PRESENT has 64-bits block size, 31 rounds and a key size of length 80/ 128 bits. Each round has XOR operation for a round key and a post-whitening key. Each round of PRESENT applies same 4-bit S-Box 16 times in parallel for non-linear substitution layer that increases confusion. Diffusion by using a bit permutation for the linear diffusion layer [6]. Due to its weak diffusion property different attacks like linear attack, weak key attack and saturation attacks are applied to PRESENT.

Taizo Shiraiet *et al.* (2007) proposed CLEFIA, a 128-bit block cipher having key sizes of 128/192/256 bits. It includes the DSM technique thereby improving flexibility and good performance for efficient implementation in H/W and S/W. It provides a good balance for security, speed, and cost. In the proposed cipher CLEFIA resistance against linear and differential attack is improved by using two different diffusion matrices by Diffusion Switching Mechanism (DSM) [18]. CLEFIA use large tables in the key scheduling, as a result, increasing memory size and requires more execution time as compared to PRESENT.

Debra Cook *et al.* (2007) introduced the concept of stretching a block cipher upto twice the size of an original block size. The newly introduced cipher is known as an elastic cipher. It provides security against attacks as an original cipher while incurring a computational workload proportional to the block size. It employs reduction method, round function as black box [30].

Olteanu Alina *et al.* (2008) proposed LCG-based 4 bytes block cipher by using Multiple Recursive Generator (MRG). MRG generate pseudo-random sequences with large periods and add noise to plaintext. Proposed cipher has 4 steps, these are: Generate 4 bytes pseudo-random number using Multiple Recursive Generator; Combining generated pseudo-random number with plaintext using addition modulo-256 byte by byte; step 3 and step 4 are concerned with pseudo-random permutation to ciphertext [31].

Zheng Gong *et al.* (2011) proposed a family of lightweight SPN block ciphers named KLEIN having 64-bit block size, 64/80/96-bit key size with 12/16/20 number of rounds for KLEIN-64/80/96 respectively. It mixes together elementary operations of AES [5] and PRESENT [6]. It uses 4X4 S-box and input/output of KLEIN are one-dimensional arrays of bytes [19]. The key schedule has a Feistel like structure designed to avoid potential related key attacks. Design of KLEIN is such that it avoids possible related-key attacks. Up to 8 rounds of KLEIN-64, there is a chosen-plaintext key-recovery attack.

Kyoji Shibutani *et al.* (2011) proposed PICCOLO, a new variant of Generalized Feistel Network (GFN) block cipher. PICCOLO supports 64-bit block cipher, 80/128-bit key size with 25/31 rounds. It uses four 16-bit whitening keys and 2r 16-bit round keys for r rounds. PICCOLO's F-function has two S-box layers that are separated by diffusion matrix by not applying key before the second layer of S-box. Standard GFN utilizes 16-bit word based cyclic shifts but PICCOLO has 8-bit word based permutation. The key schedule is permutation based for hardware efficiency [11]. GFN needs more rounds, consumes more power and has lower throughput [22].

Jian Guo *et al.* (2011) described lightweight block cipher; named LED (Light Encryption Device) based on the design principles similar to that of AES [5] and uses the S-box of PRESENT [6] cipher. LED has 64-bit block size, 64/128-bit key size, and 4 round. Each of these four rounds have operations; AddConstants, SubCells, ShiftRows, and MixColumnsSerial. It uses light key schedule and key schedule design is relatively a neglected area in LED that's why it is vulnerable to related-key attacks [21]. LED consumes high energy per bit which is power inefficient [22].

Wenling Wu and Lei Zhang (2011) proposed a new lightweight block cipher called LBlock. Its block size is 64-bit and key size is 80-bit. Round function F has substitution and permutation layers. For confusion, eight 4-bit S-boxes are used in parallel as a round function and diffusion by 4-bit word-wise permutation. Leftmost 32-bits of 80-bit master key gives round sub-key by applying simple rotation (29-bit left) and nonlinear operations. In each round, round function processes only half of the data whereas simple rotation function is applied to another half of the data. Combination of eight 4-bit S-boxes and 4-bit word-wise permutation can be considered as four 8-bit lookup tables in 8-bit oriented software implementation [32].

Tomoyasu Suzaki *et al.* (2011) presents 64-bit lightweight block ciphers, named TWINE having a key size of 80/ 128 bits. Round keys are pre-computed and only one loop is provided for two rounds by removing block shuffling between the two rounds. Compact implementation of TWINE is because of generalized Feistel network with many sub-blocks that are combined with improvement on the diffusion layer.

The speed can be further enhanced if more rounds can be combined in one loop but this increases the memory [9].

Daniel Engels *et al.* (2011) proposed an ultra lightweight encryption algorithm that operates on 16-bit blocks, named Hummingbird-2. It is a hybridized cipher by combing characteristics of both Block cipher and Stream cipher. The operations are exclusive-OR, operation on words, addition modulo and a non-linear mixing function and it uses 4X4 S-boxes. Hummingbird-2 has an initialization vector of 64-bits and it uses a secret key of 128-bits. It is not necessary that message authentication tag is generated by Hummingbird-2, it is optionally produced [10]. There exists initial key recovery attack on Hummingbird-2.

Gilles Piret *et al.* (2012) designed a Feistel block cipher which fits well with the proven masking constraints to ensure resistance to cryptanalysis methods. It is important to choose good S-box for efficient masking scheme. Maximum distance separable codes are used to construct best possible expansion layers and compression layers to circumvent the weakness of using Non-bijective S-box with Feistel network. Operations performed for key scheduling are rotations, additions (bit-wise) and selection (bit-wise) [33].

Julia Borghoff *et al.* (2012) designed lightweight block cipher PRINCE based on FX construction having a block size of 64-bits and a key size of 128-bitswith 12 rounds. Each round of PRINCE consists of key addition, S-box layer (4-bit S-box, not required to be an involution), a linear layer and the addition of a round constant. It splits key into two parts, each of 64-bits. First two sub-keys are used as whitening keys. Cipher is symmetric around middle round and therefore decryption can be implemented on top of encryption with a minimal overhead [34].

Vincent Grosso *et al.* (2012) presented a tweakable block cipher, named SCREAM inheriting tweakable key schedule from TAE [35] and extending their previously proposed block cipher Fantomas with a different L-box. The L-box choice makes sure that active S-boxes should be higher than branch number bound alone. It uses distinct values of tweak for enhancing security. In SCREAM two sets of parameters are proposed; first is single-key security known as SCREAM with 10 steps and second is related-key security known as SCREAM with 12 steps [36].

Andrey Bogdanov *et al.* (2013) proposed a nonce-based new block cipher, named as ALE (Authenticated Lightweight Encryption). It is a single pass online ALE cipher that conserves memory arrangement of data. Its operations are AES-128 key schedule, AES round transformation and 256-bit secret internal state that is dependent on both nonce and key. Its security relies on the usage of nonce. ALE uses PELICAN keyed in all rounds for computation of authentication tag and for encryption/ decryption, in every round bytes of state are leaked in away similar to LEX [37].

Manoj Kumar *et al.* (2013) proposed a software-oriented design with high efficiency, named FeW: A Feather-weight Block Cipher. FeW use 64-bit block size and 80/128 bits key size (master key) with 32 rounds. Proposed lightweight cipher is Feistel-M structure; a combination of Feistel and Generalized Feistel Structures. Key schedule of FeW is similar to PRESENT [6], Generalized Feistel based design similar to CLEFIA [18] and uses S-Box of HummingBird2 [10]. Two different functions are used in round function and are applied to two 16- bit words. Security is enhanced in FeW against linear, differential, impossible differential and zero correlation attacks [38].

Ray Beaulieu *et al.* (2013) developed two lightweight block ciphers families SIMON and SPECK. Each Speck family comprises ten different block ciphers to give support for securing applications in a controlled environment. SIMON cipher with a block size of 2*n*-bits and a key size of *mn*-bits is represented as 2*n/mn*. SPECK round function is analogous to the mixing function of THREEFISH [39]. Simon and Speck use circular shift bit permutations and a single set of rotation parameters. Tomer Ashur (2015) presents a key recovery attack by using linear approximations for Simon. The attacks on Simon64/128 needs upto 25 rounds, on Simon 32/64, Simon48/96, and Simon64/96; it requires upto 24 rounds and for Simon48/72 it requires upto 23 rounds [40].

Deukjo Honget *et al.* (2013) proposed a new lightweight block cipher LEA having simple ARX and non S-box structure for 32-bit words. Block size of LEA is 128-bits and key sizes are different; these are 128/ 192/ 256-bits having 24/28/32 rounds respectively. Operations performed in LEA algorithm are two key XORs, addition and bit-wise rotation. Non-linear function used is modulo 232 with two 32-bit inputs and one 32-bit output. For diffusion word-wise swap and bitwise rotations are used. Decryption is similar to the encryption procedure. 32-bit words array is used to represent key of LEA and key schedule generates192-bit round keys sequence without mixing the words. Constants are used to generate round keys from the hexadecimal expression of$\sqrt{766995}$, where 76, 69, and 95 are ASCII codes of ‘L,’ ‘E,’ and ‘A’ [41].

Sufyan Salim Mahmood AlDabbagh *et al.* (2013) proposed a SPN (Substitution and Permutation Network) lightweight block cipher having 64-bits block size and 80-bits key size having 31 rounds. In each round of the proposed design, 16 different S-boxes of PRESENT cipher are used. Proposed cipher presented a new method of key dependent S-box where one S-box from 16 S-boxes is selected by XORing between all the elements of a key. Key schedule extracts 64 left most bits from 80-bit master key. Design of proposed cipher is same as that of PRESENT and it has improved security in terms of linear and differential attack [42].

Deukjo Hong *et al.* (2014) presented a simplified version of LBlock [32] lightweight block cipher using a similar structure as of ALE [37]. New cipher designed is named LAC, a nonce-respecting design which uses public message number (PMN) as a nonce. With the same master key, it allows a maximum of 240 bits to be encrypted. Encryption/ Decryption is done by accepting master key of size 80-bits, a 64-bit PMN, a message *m/ cipher text c*, an associated data α, and a 64-bit authentication tag [43].

Sufyan Salim Mahmood AlDabbagh *et al.* (2014) proposed Feistel lightweight block cipher, named HISEC, an enhancement over PRESENT [6]. HISEC has 64-bit block size and 80-bit key-size with a total of 15 rounds. Characteristics of HISEC are same as that of PRESENT but Bit permutation in HISEC is different from PRESENT, it is applied on two sides and each side is of 32-bits. It has four layers with operations in each layer as XOR with key; Confusion by giving non linearity to algorithm by using single 4-bit S-box and repeating it 16 times; Diffusion by Bit permutation and last Rotation and XOR. Most right 64-bits of master-key are taken for the encryption algorithm. Proposed cipher is safe against differential, integral and boomerang attacks [13].

Nicky Mouha *et al.* (2014) proposed permutation-based Message Authentication Code (MAC) algorithm called Chaskey for 32-bit microcontrollers. Chaskey is inspired by the permutation of SipHash [44] with 32-bits instead of 64-bits. It uses ARX (Addition-Rotation-XOR) design methodology. Addition and XOR operation applied on 32-bits word. Chaskey does not follow any key schedule as key generation is done by XOR with state and key updation involves two shifts and two conditional XORs for two sub-keys. It does not require nonce and hence is secure [45].

Sufyan Salim Mahmood AlDabbagh and Imad Fakhri Taha Al Shaikhli (2014) proposed OLBCA, a 64-bit block cipher with 80-bit key size having 22 rounds. Each round in OLBCA consists of three layers each except the last round which has four layers. Three layers consist of 12 4-bit S-boxes, bit permutations, rotations, Exclusive-OR operation applied three times, and word permutation. The last layer in last round applies XOR operation on the output of third layer (all 64 bits) with 64 bits of the updated key. The master key is rotated by P-bits in key schedule, where the value of P will be incremented by 2 for next round and an initial value of P is 13 [46].

Wentao Zhanget *et al.* (2015) proposed a new hardware-friendly SPN lightweight block cipher named RECTANGLE using bit-slice techniques. It uses bit-slice technique given by SERPENT [47] and optimal 4X4 S-box given by [48]. RECTANGLE has a 64-bits block size and 80/ 128 bits key size with 25 rounds. Each round consists three operations: AddRoundkey (Bitwise XOR with round key), SubColumn (4-bit S-boxes in parallel) and last ShiftRow (each row is rotated left over different offsets). Substitution layer has 16 similar 4X4 S-boxes in parallel and permutation layer has three rotations. Due to its bit-slice implementation, it has good software speed [7]. To avoid slide attacks in key schedule different round constants are added. S-box and P-layer combination in RECTANGLE brings limited differential/ linear trails. It provides good resistance against mathematical and side-channel attacks. RECTANGLE has matrix structure like AES [5], so needs more computational cycles [22].

Gangqiang Yang *et al.* (2015) proposed a compact and an efficient family of lightweight Feistel block ciphers, named SIMECK by combing good features of both SIMON [8] and SPECK [8]. There are three block ciphers in SIMECK family; SIMECK32/64, SIMECK48/96 and SIMECK64/128.A 4n-bit key is used for encryption or decryption by SIMECK2n on 2n-bit message blocks. According to authors in [49], SIMECK is vulnerable to bit-flip fault attack and random byte fault attack.

Gaurav Bansod *et al.* (2015) proposed SPN based lightweight cipher, named PICO. PICO cipher has 64-bits block size, 128-bits key size, and 32 rounds. A large number of active S-boxes are generated in relatively fewer rounds in order to provide good immunity against linear and differential attacks. It has strong S-box which makes it robust. Key scheduling extracts 64-bits long 33 sub-keys from 128-bit master key [9]. Proposed design makes a fusion of S-box of a number of lightweight block ciphers and P-box of GRPs [50].

Hwajeong Seo *et al.* (2015) proposed improved 128, 192 and 256-bit LEA lightweight block cipher. Improved LEA uses simple ARX (Addition/ Rotation/ Exclusive-OR) operations for a low-end embedded processor. The architecture of proposed cipher is non S-box and it has 32-bit word size. LEA provides three security levels i.e. 128-bit key with 24 rounds, 192-bit key with 28 rounds and 256-bit key with 32 rounds. For an 8-bit processor, it provides 8-bit (one byte) operations. By finding and optimizing the minimum inner loops in an instruction set level, the algorithm occupies 280B to conduct LEA encryption [51].

Martin R. Albrecht *et al.* (2015) presented SPN block cipher, named PRIDE for 8-bit microcontrollers. PRIDE cipher focuses on branch number to find efficient linear layer which allows a tradeoff between security and efficiency. Its linear layer is similar to bit-sliced S-box implementation. One round of PRIDE has a number of layers including linear layer, substitution layer, branching, key-addition and key-updation by round constant [52].

Gaurav Bansod *et al.* (2015) specified a new hybrid lightweight cipher based on bit permutation instruction group operation (GRP) and S-box of PRESENT on a 32-bit processor. The proposed design uses 64-bit block size with a 128-bit key. Confusion is given by S-box of PRESENT and P-box by using GRP for 64-bit and 128-bit block size. Key generation uses GRP as it requires fewer numbers of instructions in comparison to table lookup [50].

F. Karakoçet *et al.* (2015) proposed AKF, a new Feistel lightweight block cipher scheme with alternating keys and ITUbee, software oriented scheme based on AKF. ITUbee uses S-box of AES [5] and reduce memory requirements, energy consumption and time requirements and is resistant to related-key attacks. Using alternating keys or not using a key schedule in a Feistel structure makes cipher vulnerable to related-key attacks [53]. Along with AKF scheme, ITUbee has key whitening layers, 8-bit S-Box, and cellular automation. For diffusion layer, just 15 XOR operations are required. To provide resistance against self-similarity attack (reflection, slide, and slidex) different permutations on the right-hand side are used because of round constant addition while left-hand side permutations in the round are same [54]. 16-bit constants are used to reduce the number of operations and to prevent leakage of information [55]. There exists a deterministic related-key differential distinguisher for up to eight rounds of the cipher by utilizing a self similar technique [56].

Hassan Noura *et al.* (2015) proposed a combination of dynamic structure of Artificial Neural Network (ANN) and a nonlinear function. Cipher design has three layers; these are one input layer, one hidden layer, and one output layer. It uses different dynamic invertible Weight Matrices and static Non-linear Function. Dynamic and secret synaptic matrices are different for each layer. To improve the security of cipher, numbers of hidden layers can be increased. For each validate time, first dynamic key generation process is applied then control parameters (Weight matrices) of Non-linear transformations are constructed. Subsequently, the process of encryption/ decryption can be realized. Dynamic structure of ANN resists existing attacks and parallel process of neural network ensures lower energy requirements and lesser computation complexity [57].

Sufyan Salim Mahmood AlDabbagh *et al.* (2015) enhanced OLDBCA by improving the cost factor by decreasing number of S-boxes from 12 to 8. It uses XORing of first 32-bits of the key with first 32-bits of plaintext. In enhanced OLDBCA, security decreased in terms of boomerang attack, Integral Cryptanalysis and Differential Cryptanalysis [58].

Subhadeep Banik *et al.* (2016) proposed hardware efficient MIDORI, a lightweight SPN block cipher which uses three 4-bit S-boxes and cell permutations [59].

Adnan Baysal and Sühap Sahin (2016) presented an efficient Feistel bit-slice block cipher RoadRunneR in 8- bit CPU. RoadRunneR has a block size of 64-bits and a key size of 80-bits or 128-bits requiring 10 and 12 rounds respectively. It uses S-box as proposed by the authors of [60] and implementations follow PRIDE [52]. It uses initial and final round whitening by XORing the 3 whitening keys to the left part of the state. In the final round, no swap operation is used. Round function in decryption is same but it reverses the order of whitening keys, round keys, and constants. A metric ST/A is also proposed for the first time that rank ciphers based on key length [14].

Christof Beierle *et al.* (2016) presented SKINNY and MANTIS. SKINNY is a family of tweakable block ciphers which uses SPN and follows tweakey framework as proposed in [65]. It uses a compact S-box S4 very close to S-Box of PICCOLO [11] by removing last NOT gate at the end. SKINNY has flexible block/ key/ tweak size, and sate is loaded row-wise as in AES [5]. SKINNY introduced a new sparse diffusion layer and new key schedule which is light. SKINNY uses large key size as compared to block size and lower number of rounds to provide bounds search space. The tweakable capability of SKINNY provides leakage resilient implementations [17]. MANTIS is low latency tweakable block cipher with 64-bits block size and 128-bit key size having a 64-bit tweak. It is an enhancement over MIDORI [59] by using its S-box and linear layer for fast diffusion. Mantis uses round constant of PRINCE [34], which is added row-wise. Tweak-scheduling is introduced in MANTIS to ensure a high number of active S-boxes and by increasing number of rounds security around related tweakey attack is increased. Security analysis of MANTIS is not done efficiently as it is mostly copied from its identical MIDORI [17]. There exists Related-Key Impossible-Differential Attack on Reduced-Round SKINNY and Practical Key-Recovery Attack on MANTIS-5 [62] [63].

Daniel Dinu *et al.* (2016) proposed a family of ARX (Modular Addition/ Bitwise Rotation/ XOR) based symmetric-key lightweight block cipher named SPARX and LAX. LTS employs large ARX-based S-Box called arx-box along with sparse linear layers to add nonlinearity and sufficient diffusion. ARX reduces the impact of side-channel attacks by not using table look-ups. This design strategy allows fast software implementations by minimizing operations performed. The cipher SPARX is designed according to long trail design strategy LTS (a dual of WTS [24]) and LAX complete. There are a total of 8 steps with 3 rounds in each step in Sparx-64/128 whereas Sparx-128/ 128 uses 8steps with 4 rounds in each step and Sparx-128/ 256 uses 10 steps and 4 rounds per step [53].

Ahssan Ahmed Mohammed and Dr. Abdulkareem O. Ibadi (2017) proposed a Non-Feistel block cipher with multiple of 32 bits block length, key lengths with a multiple of 48 bits which are automatically entered in variable permutation, addition function, and XOR operation. The algorithm works in single round and gives high security. Depending upon the application field, complexity, speed and cost; the algorithm performs in several block length. Permutation operation is used after each map function to propagate bits in each block and to increase confusion and diffusion operations. A number of functions are proposed like Balance function between balance fixed number and initial permutation and inverse initial permutation, maps function as a lookup table, wave function as nonlinear function. The proposed cipher design has proposed a new sub-key generation algorithm [23].

Mumthaz and Geethu (2017) introduced an optimized design of lightweight block cipher Lilliput with Extended Generalised Feistel Network (EGFN). The proposed approach has implemented the S-Box of PRESENT [6] and key schedule similar to that of key schedule of DES. Improved LILLIPUT has a 64-bit block size, 80-bit key, 30 rounds where round function acting at nibble level [15].

Subhadeep Baniket *et al.* (2017) proposed a small, fast, energy efficient and more secure SPN block cipher, named GIFT by improving PRESENT. S-box of PRESENT [6] is costly and for diffusion, bit permutation is used. GIFT improved PRESENT cipher by introducing permutation in combination with Difference Distribution Table (DDT)/ Linear Approximation Table (LAT) of the S-Box. Two proposed versions of GIFT are: GIFT-64 with 28 rounds and GIFT-128 with 40 rounds. Both versions have a key size of 128-bits. Smaller and cheaper S-box then PRESENT is used in GIFT to improve resistance against linear and differential cryptanalyst, linear hulls and clustering effect [65].

Sufyan Salim Mahmood AlDabbagh (2017) proposed a new lightweight Feistel block cipher algorithm named DLBCA (Design 32-bit Lightweight Block Cipher Algorithm) by adopting various principles and approaches given by the authors of [66]. DLBCA is designed with 32-bit blocksize and a key size of 80-bit with 15 rounds. DLBCA applies following operations on the four layers; S-box, bit-permutation, Exclusive-OR' rotation and key functions. It provides good resistance to differential and boomerang attacks [67].

Muhammad Usman *et al.* (2017) proposed SIT (Secure IoT), a lightweight 64-bit symmetric key block cipher with key size 64-bits having 5 rounds. SIT is hybridized approach that combines Feistel and SPN structure. The proposed approach uses some logical operations along with some swapping and substitution. Five rounds encryption with 5 different keys improve energy efficiency. Feistel network of substitution diffusion functions are used in SIT algorithm for confusion and diffusion. Key expansion block utilizes 64-bit cipher key as an input from the user [16]. F-function used in key generation is inspired from tweaked KHAZAD [25] block cipher. SIT does not use an actual key, key is first XORed.

Jagdish Patil *et al.* (2017) presented a new lightweight balanced Feistel block cipher "LiCi" with 64-bits block size, 128-bits key size having 31 rounds. It uses 4-bit S-boxes, XOR operation, left circular shift by 3, right circular shift by 7. Key scheduling inspired from PRESENT key scheduling and it extracts 64 LSB from 128-bits master-key and updated the master key by using left circular shift by 13. Being most lightweight cipher among existing ciphers it needs only 1944 bytes of Flash memory and 1256 bytes of RAM [68].

So far literature survey shows the interest of researchers in the field of lightweight block ciphers. In 8-bit CPUs, in order to optimize hardware implementations, some designs used building blocks and hence are not appropriate for software applications. Alternatively, some more recent designs focused on performance in software implementation. Table 1 shows few relevant lightweight block ciphers optimized for software implementations.

Table 1: Existing Lightweight Block ciphers (Software Implementation)

Cipher	**Year**	**Technique**	**Key Size** (bits)	**Block Size** (bits)	**No. of Rounds**
Improved Lilliput [15]	2017	EGFN	80	64	30
GIFT [65]	2017	SPN	128	64/128	28/40
SIT [16]	2017	Feistel + SPN	64	64	5
DLBCA [67]	2017	Feistel	80	32	15
LiCi [68]	2017	Feistel	128	64	31
SKINNY [17]	2016	SPN	64-384	64/128	32-56
MANTIS [17]	2016	SPN	128	64	10/12
SPARX [53]	2016	SPN with ARX-based S-boxes	128/256	64/128	24-40
LAX [53]	2016	SPN with ARX-based S-boxes	128/256	64/128	24-40
RoadRunneR [14]	2016	Feistel	80/128	64	10/12
PICO [12]	2015	SPN	128	64	32
RECTANGLE [7]	2015	SPN	80/128	64	25
Chaskey [45]	2014	SPN with ARX-based S-boxes	128	128	8
OLBCA [65]	2014	SPN	80	64	22
ITUBee [54]	2014	Feistel	80	80	20
HISEC [13]	2014	Feistel	80	64	15
LAC [43]	2014	Feistel	80	64	16
SIMON [8]	2013	Feistel	64/ 72/ 96/ 128/ 144/ 192/ 256	32/48/64/96/128	32/36/42/44/52/ 54/68/69/72

SPECK [8]	2013	Feistel	32/ 64/ 72/ 96/ 128	64/ 72/ 96/ 128/ 144/ 192/ 256	22/ 23/ 26/ 27/ 28/ 29/ 32/ 33/ 34
FeW [38]	2013	Feistel-M	80/128	64	32
LEA [41]	2013	SPN with ARX-based S-boxes	128/192/256	128	24/28/32
SCREAM [36]	2012	SPN	128	128	10/12
PRINCE [34]	2012	SPN	128	64	12
Hummingbird-2 [10]	2011	SPN+Feistel	128	64	4
TWINE [9]	2011	GFN	80/128	64	36
LED [21]	2011	SPN	64/128	64	32/48
LBlock [32]	2011	Feistel+SPN	80	64	32
PICCOLO [11]	2011	GFN	80/128	64	25/31
KLEIN [19]	2011	SPN	64/80/96	64	12/16/20
CLEFIA [18]	2007	Feistel	128/192/256	128	18/22/26
PRESENT [6]	2007	SPN	80/128	64	31
SEA [29]	2006	Feistel	96	96	93
mCrypton [22]	2005	SPN	64/96/128	64	12
TDEA [27]	2004	Feistel	64	64	48
Camelia [26]	2000	Feistel + SPN	128/192/256	128	18/24/24
KHAZAD [25]	2000	SPN	128	64	3

Block Size and Key Size is in number of bits; Feistel-M (Balanced GFN + SPN); Extended Generalized Feistel Network (EGFN)

Some recent surveys on lightweight block ciphers have also done to find out the performance of ciphers based on code size, cycle count, and energy consumption. Authors in [70] used FELICS tool given in [69] to compare different lightweight block ciphers. According to their survey Chaskey [41], LEA [36], PRIDE [48] and SPARX [49] are suitable for IoT Cryptography [70]. As per survey done by various researchers in [71] [72] [73] [74] [75] [76]; AES [1] is more expensive, LED [17], mCrypton [18], PRESENT [2] and KLEIN [15] have poor performances; CLEFIA [14] has high RAM requirement due to the usage of large size table in the key scheduling phase.

Some of the available ciphers are not fully optimized and can be explored further. All these ciphers have some kind of weaknesses like:

a) Weak substitution box

b) Weak permutation layer

c) Weak key scheduling

d) Susceptibility to some kind of attacks

e) Computationally complex and expensive

f) Low resource utilization

CONCLUSION

Block ciphers are one of the main primitives for cryptographic applications. In this paper, we discussed various lightweight block ciphers suitable for IoT applications. These are generally categorized as either hash functions, stream ciphers or block ciphers. A number of cryptanalysts showed that there exist numerous attacks on ciphers for which the ciphers must provide good resistance. IoT being emerging field requires lightweight cipher designs having rich encryption standards, robust architecture, less complexity, less execution time, lower power consumption, low resource utilization and good resistance against possible attacks. As a result, the design of lightweight block ciphers has fascinated attention of many researchers', especially in the last 5 years. Through our extensive literature survey over lightweight block ciphers, we found that available ciphers are not fully optimized and can be explored further. The search continues for a lightweight cipher which should fulfill the requirements of a good lightweight cipher.

REFERENCES

[1] Madakam, S., Ramaswamy, R. and Tripathi, S., 2015. Internet of Things (IoT): A literature review. *Journal of Computer and Communications*, *3*(05), p.164. {a}

[2] Hafsa Tahir, A.K. and Junaid, M., 2016. Internet of Things (IoT): An Overview of Applications and Security Issues Regarding Implementation. {b}

[3] Xu, Q., Ren, P., Song, H. and Du, Q., 2016. Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations. *IEEE Access*, *4,* pp.2840-2853. {c}

[4] Kaur, A., 2016. Internet of Things (IoT): Security and Privacy concerns. *International Journal of Engineering Sciences & Research Technology*. (pp. 161-165). DOI: 10.5281/zenodo.51013

[5] Daemen, J. and Rijmen, V., 1999. AES proposal: Rijndael.

[6] Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J., Seurin, Y. and Vikkelsoe, C., 2007, September. PRESENT: An ultra-lightweight block cipher. In *CHES* (Vol. 4727, pp. 450-466).

[7] 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.

[8] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B. and Wingers, L., 2013. The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptol ogy ePrint Archive, Report 2013/404.

[9] Suzaki, T., Minematsu, K., Morioka, S. and Kobayashi, E., 2011, November. Twine: A lightweight, versatile block cipher. In *ECRYPT Workshop on Lightweight Cryptography* (Vol. 2011).

[10] Engels, D.W., Saarinen, M.J.O., Schweitzer, P. and Smith, E.M., 2011. The Hummingbird-2 Lightweight Authenticated Encryption Algorithm. *RFIDSec*, *11*, pp.19-31.

[11] Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T. and Shirai, T., 2011, September. Piccolo: An ultra-lightweight blockcipher. In *CHES* (Vol. 6917, pp. 342-357).

[12] Bansod, G., Pisharoty, N. and Patil, A., 2016. PICO: An Ultra Lightweight and Low Power Encryption Design for Ubiquitous Computing. *Defence Science Journal*, *66*(3).

[13] AlDabbagh, S.S.M., Shaikhli, A., Taha, I.F. and Alahmad, M.A., 2014, September. Hisec: A new lightweight block cipher algorithm. In *Proceedings of the 7th International Conference on Security of Information and Networks* (p. 151). ACM.

[14] Baysal, A. and Şahin, S., 2015, September. Roadrunner: A small and fast bitslice block cipher for low cost 8-bit processors. In *International Workshop on Lightweight Cryptography for Security and Privacy* (pp. 58-76). Springer, Cham.

[15] Mumthaz Pookuzhy Ali, Geethu T George, 2017. "Optimised Design of Light Weight Block Cipher Lilliput with Extended Generalised Feistal Network (EGFN)." International Journal of Innovative Research in Science, Engineering and Technology, Vol. 6, Issue 4. *Website: www.ijirset.com.*

[16] Usman, M., Ahmed, I., Aslam, M.I., Khan, S. and Shah, U.A., 2017. SIT: A Lightweight Encryption Algorithm for Secure Internet of Things. *arXiv preprint arXiv:1704.08688*.

[17] Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P. and Sim, S.M., 2016, August. The SKINNY family of block ciphers and its low-latency variant MANTIS. In *Annual Cryptology Conference* (pp. 123-153). Springer Berlin Heidelberg.

[18] Shirai, T., Shibutani, K., Akishita, T., Moriai, S. and Iwata, T., 2007, March. The 128-bit blockcipher CLEFIA. In *FSE* (Vol. 4593, pp. 181-195).

[19] Gong, Z., Nikova, S. and Law, Y.W., 2011. KLEIN: A new family of lightweight block ciphers. *RFIDSec*. Springer, *7055*, pp.1-18.

[20] Needham, R.M. and Wheeler, D.J., 1997. Tea extensions. *Report, Cambridge University, Cambridge, UK (October 1997)*.

[21] Guo J., Peyrin T., Poschmann A., and Matt Robshaw M.,Preneel B. and Takagi T., 2011. The LED Block Cipher. CHES 2011, In International Association for Cryptologic Research, LNCS 6917 (pp. 326–341).

[22] Lim, C.H. and Korkishko, T., 2005, August. mCrypton-a lightweight block cipher for security of low-cost RFID tags and sensors. In *WISA* (Vol. 3786, pp. 243-258).

[23] Mohammed, A.A. and Ibadi, A.O., 2017. A Proposed Non Feistel Block Cipher Algorithm.

[24] Daemen, J. and Rijmen, V., 2001, December. The wide trail design strategy. In *IMA International Conference on Cryptography and Coding* (pp. 222-238). Springer, Berlin, Heidelberg.

[25] Barreto, P.S.L.M. and Rijmen, V., 2000. The Khazad legacy-level block cipher. *Primitive submitted to NESSIE, 97.*

[26] Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J. and Tokita, T., 2000, August. Camellia: A 128-bit block cipher suitable for multiple platforms-design and analysis. In *Selected Areas in Cryptography* (Vol. 2012, pp. 39-56).

[27] Barker, W.C. and Barker, E., 2012. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher: NIST Special Publication 800-67, Revision 2.

[28] Hao, Y., Bai, D. and Li, L., 2014, October. A meet-in-the-middle attack on round-reduced mCrypton using the differential enumeration technique. In *International Conference on Network and System Security* (pp. 166-183). Springer, Cham.

[29] Standaert, F.X., Piret, G., Gershenfeld, N. and Quisquater, J.J., 2006, April. SEA: A scalable encryption algorithm for small embedded applications. In *International Conference on Smart Card Research and Advanced Applications* (pp. 222-236). Springer, Berlin, Heidelberg.

[30] Cook, D., Keromytis, A. and Yung, M., 2007, March. Elastic block ciphers: the basic design. In *Proceedings of the 2nd ACM symposium on Information, computer and communications security* (pp. 350-352). ACM.

[31] Olteanu, A., Xiao, Y., Hu, F. and Sun, B., 2008, November. A lightweight block cipher based on a multiple recursive generator. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE* (pp. 1-5). IEEE

[32] Wu, W. and Zhang, L., 2011. LBlock: a lightweight block cipher. In *Applied Cryptography and Network Security* (pp. 327-344). Springer Berlin/Heidelberg.

[33] Piret, G., Roche, T. and Carlet, C., 2012, June. PICARO-A Block Cipher Allowing Efficient Higher-Order Side-Channel Resistance. In *ACNS* (Vol. 7341, pp. 311-328).

[34] Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C. and Rombouts, P., 2012, December. PRINCE–a low-latency block cipher for pervasive computing applications. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 208-225). Springer, Berlin, Heidelberg.

[35] Liskov, M., Rivest, R.L. and Wagner, D., 2011. Tweakable block ciphers. *Journal of cryptology*, *24*(3), pp.588-613.

[36] Grosso, V., Leurent, G., Standaert, F., Varici, K., Journault, A., Durvaux, F., Gaspar, L. and Kerckhof, S., 2015. SCREAM Side-Channel Resistant Authenticated Encryption with Masking. *CAESAR submission*.

[37] Bogdanov, A., Mendel, F., Regazzoni, F., Rijmen, V. and Tischhauser, E., 2013, March. ALE: AES-based lightweight authenticated encryption. In *International Workshop on Fast Software Encryption* (pp. 447-466). Springer, Berlin, Heidelberg.

[38] Kumar, M., Pal, S.K. and Panigrahi, A., 2014. FeW: A Lightweight Block Cipher. *IACR Cryptology ePrint Archive*, *2014*, p.326.

[39] Ferguson, N., Lucks, S., Schneier, B., Whiting, D., Bellare, M., Kohno, T., Callas, J. and Walker, J., 2010. The Skein hash function family. *Submission to NIST (round 3)*, *7*(7.5), p.3.

[40] Ashur, T., 2015. Improved Linear Trails for the Block Cipher Simon. *IACR Cryptology ePrint Archive*, *2015*, p.285.

[41] Hong, D., Lee, J.K., Kim, D.C., Kwon, D., Ryu, K.H. and Lee, D.G., 2013, August. LEA: A 128-bit block cipher for fast encryption on common processors. In *International Workshop on Information Security Applications* (pp. 3-27). Springer, Cham.

[42] AlDabbagh, S.S.M. and Al Shaikhli, I.F.T., 2013, December. Improving PRESENT Lightweight Algorithm. In *Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on* (pp. 254-258). IEEE.

[43] Zhang, L., Wu, W., Wang, Y., Wu, S. and Zhang, J., 2014. LAC: A lightweight authenticated encryption cipher. *Submitted to the CAESAR competition*.

[44] Aumasson, J.P. and Bernstein, D.J., 2012, September. SipHash: A Fast Short-Input PRF. In *INDOCRYPT* (Vol. 7668, pp. 489-508). Springer.

[45] Mouha, N., Mennink, B., Van Herrewege, A., Watanabe, D., Preneel, B. and Verbauwhede, I., 2014, August. Chaskey: an efficient MAC algorithm for 32-bit microcontrollers. In *International Workshop on Selected Areas in Cryptography* (pp. 306-323). Springer, Cham.

[46] Aldabbagh, S.S.M. and Al Shaikhli, I.F.T., 2014, December. OLBCA: A New Lightweight Block Cipher Algorithm. In *Advanced Computer Science Applications and Technologies (ACSAT), 2014 3rd International Conference on* (pp. 15-20). IEEE.

[47] Biham, E., Anderson, R. and Knudsen, L., 1998. Serpent: A new block cipher proposal. In *Fast Software Encryption* (pp. 222-238). Springer Berlin/Heidelberg.

[48] Zhang, W., Bao, Z., Rijmen, V. and Liu, M., 2015, March. A New Classification of 4-bit Optimal S-boxes and its Application to PRESENT, RECTANGLE and SPONGENT. In *International Workshop on Fast Software Encryption* (pp. 494-515). Springer, Berlin, Heidelberg.

[49] Nalla, V., Sahu, R.A. and Saraswat, V., 2016, January. Differential Fault Attack on SIMECK. In *Proceedings of the Third Workshop on Cryptography and Security in Computing Systems* (pp. 45-48). ACM.

[50] Bansod, G., Raval, N. and Pisharoty, N., 2015. Implementation of a new lightweight encryption design for embedded security. *IEEE Transactions on Information Forensics and Security*, *10*(1), pp.142-151.

[51] Seo, H., Liu, Z., Choi, J., Park, T. and Kim, H., 2015, August. Compact implementations of LEA block cipher for low-end microprocessors. In *International Workshop on Information Security Applications* (pp. 28-40). Springer, Cham.

[52] Albrecht, M.R., Driessen, B., Kavun, E.B., Leander, G., Paar, C. and Yalçın, T., 2014, August. Block ciphers–focus on the linear layer (feat. PRIDE). In *International Cryptology Conference* (pp. 57-76). Springer, Berlin, Heidelberg.

[53] Dinu, D., Perrin, L., Udovenko, A., Velichkov, V., Großschädl, J. and Biryukov, A., 2016. Design strategies for ARX with provable bounds: Sparx and LAX. In *Advances in Cryptology–ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I 22*(pp. 484-513). Springer Berlin Heidelberg.

[54] Karakoç, F., Demirci, H. and Harmancı, A.E., 2013, May. ITUbee: a software oriented lightweight block cipher. In *International Workshop on Lightweight Cryptography for Security and Privacy* (pp. 16-27). Springer, Berlin, Heidelberg.N5

[55] Karakoç, F., Demirci, H. and Harmancı, A.E., 2015. AKF: A key alternating Feistel scheme for lightweight cipher designs. *Information Processing Letters*, *115*(2), pp.359-367.

[56] Soleimany, H., 2014. Self-similarity cryptanalysis of the block cipher ITUbee. *IET Information Security*, *9*(3), pp.179-184.

[57] Noura, H., Samhat, A.E., Harkouss, Y. and Yahiya, T.A., 2015, October. Design and realization of a new neural block cipher. In *Applied Research in Computer Science and Engineering (ICAR), 2015 International Conference on* (pp. 1-6). IEEE.

[58] Al-Dabbagh, S.S.M., Al Shaikhli, I.F.T., Al-Enezi, K.A. and Alyaqoup, M.J., 2015, December. Enhancing Lightweight Block Cipher Algorithm OLBCA through Decreasing Cost Factor. In *Advanced Computer Science Applications and Technologies (ACSAT), 2015 4th International Conference on*(pp. 159-164). IEEE.

[59] Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T. and Regazzoni, F., 2014, December. Midori: A block cipher for low energy. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 411-436). Springer, Berlin, Heidelberg.

[60] Ullrich, M., De Canniere, C., Indesteege, S., Küçük, O., Mouha, N. and Preneel, B., (2011) Finding Optimal Bitsliced Implementations of 4 χ 4-bit S-boxes.

[61] Jean, J., Nikolić, I. and Peyrin, T., 2014, December. Tweaks and keys for block ciphers: the TWEAKEY framework. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 274-288). Springer, Berlin, Heidelberg.

[62] Dobraunig, C., Eichlseder, M., Kales, D. and Mendel, F., 2017. Practical key-recovery attack on mantis5. *IACR Transactions on Symmetric Cryptology*, *2016*(2), pp.248-260.

[63] Ankele, R., Banik, S., Chakraborti, A., List, E., Mendel, F., Sim, S.M. and Wang, G., 2017, July. Related-key impossible-differential attack on reduced-round SKINNY. In *International Conference on Applied Cryptography and Network Security* (pp. 208-228). Springer, Cham.

[64] Rogaway, P., Bellare, M. and Black, J., 2003. OCB: A block-cipher mode of operation for efficient authenticated encryption. *ACM Transactions on Information and System Security (TISSEC)*, *6*(3), pp.365-403.

[65] Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M. and Todo, Y., 2017, September. GIFT: a small PRESENT. In *International Conference on Cryptographic Hardware and Embedded Systems* (pp. 321-345). Springer, Cham.

[66] Panasenko, S. and Smagin, S., 2011. Lightweight cryptography: Underlying principles and approaches. *International Journal of Computer Theory and Engineering*, *3*(4), p.516.

[67] AlDabbagh, S.S.M., 2017. Design 32-bit Lightweight Block Cipher Algorithm (DLBCA). *International Journal of Computer Applications*, *166*(8).

[68] Patil, J., Bansod, G. and Kant, K.S., 2017, February. LiCi: A new ultra-lightweight block cipher. In *Emerging Trends & Innovation in ICT (ICEI), 2017 International Conference on*(pp. 40-45). IEEE.

[69] Dinu, D., Biryukov, A., Großschädl, J., Khovratovich, D., Corre, Y.L. and Perrin, L., 2015, July. Felics–fair evaluation of lightweight cryptographic systems. In *NIST Workshop on Lightweight Cryptography*.

[70] Biryukov, A. and Perrin, L.P., 2017. State of the Art in Lightweight Symmetric Cryptography.

[71] Eisenbarth, T., Gong, Z., Güneysu, T., Heyse, S., Indesteege, S., Kerckhof, S., Koeune, F., Nad, T., Plos, T., Regazzoni, F. and Standaert, F.X., 2012, July. Compact implementation and performance evaluation of block ciphers in ATtiny devices. In *International Conference on Cryptology in Africa* (pp. 172-187). Springer, Berlin, Heidelberg.

[72] Cazorla, M., Marquet, K. and Minier, M., 2013, July. Survey and benchmark of lightweight block ciphers for

wireless sensor networks. In *Security and Cryptography (SECRYPT), 2013 International Conference on* (pp. 1-6). IEEE.

[73] Eisenbarth, T. and Kumar, S., 2007. A survey of lightweight-cryptography implementations. *IEEE Design & Test of Computers*, *24*(6).

[74] Matsui, M. and Murakami, Y., 2013, March. Minimalism of software implementation. In *International Workshop on Fast Software Encryption* (pp. 393-409). Springer, Berlin, Heidelberg.

[75] Avanzi, R., 2016. A Salad of Block Ciphers. *IACR Cryptology ePrint Archive*, p.1171.

[76] Vermesan, O. and Friess, P. eds., 2014. *Internet of things-from research and innovation to market deployment* (Vol. 29). Aalborg: River Publishers.