TEST Engineering & Management

November-December 2019
ISSN: 0193-4120 Page No. 3747 - 3760

Comprehensive Analysis on Lightweight Cryptographic Algorithms for Low Resource Devices

[1]M. Girija, [2]P. Manickam, [3]M. Ramaswami
[1]*Assistant Professor, Department of Computer Science, The American College, Madurai, India*
[2]*Assistant Professor, Department of Computer Science, Thiagarajar College, Madurai, India*
[3]*Professor, Department of Computer Applications, Madurai Kamaraj University, Madurai, India*

Article Info
Volume 81
Page Number: 3747 - 3760
Publication Issue:
November-December 2019

Article History
Article Received: *5 March 2019*
Revised: *18 May 2019*
Accepted: *24 September 2019*
Publication: *18 December 2019*

Abstract:
Lightweight cryptography is a prominent research area in network security. It provides high security and is ideal for resource constrained based smart devices in smart environment. Smart gadgets such as RFID, Sensor Networks, and embedded systems form the smart environment and it helps in sharing information among objects at anytime, anywhere. Contribution of lightweight security algorithms and schemes in smart objects are great due to their properties such as computational power, memory size, etc. This paper presents the merits and demerits of lightweight ciphers. This paper also presents complete information about existing lightweight cryptography algorithms and the structure of lightweight cryptography.

Keywords: *Lightweight cryptography, Block cipher, RFID, Sensor Networks, Smart System*

I. Introduction

Internet of Things (IoT) is a new emerging technology which is the next generation of the network. In this network, resource constrained devices like smart gadgets are connected and they share the information with each other using the internet. IoT is the extension of internet and collection of networked interconnection of everyday objects of different types such as digital and electro mechanical instruments. This emerging technology facilitates the communication among people and things, and among things themselves. IoT establishes the connection with any gadget at anytime and anywhere, in the absence of human interactions.

Internet of Things (IoT) [1] is applicable invariably in all fields such as Industries, traffic and parking systems, Environmental monitoring (Temperature, Climate and Monsoon) systems, Health care systems (Temperature, Blood Pressure and etc.), Home Automation, Smart City, and Agriculture.

In IoT paradigm, different types of physical objects form a wireless network and heterogeneous environment and are able to provide the communication. In such an environment, there is a demand to provide enough security to the information [33-39]. This method helps to prevent the eavesdropper accessing the information. Since the environment is heterogeneous, the communication needs to be secured in smart systems with confidentiality, integrity, and authentication.

The successful operation of an IoT in terms of secure communication depends on number of factors like participation of devices, devices types, memory, processing power, and different operating environment, and open environment also. So,

November-December 2019
ISSN: 0193-4120 Page No. 3747 - 3760

providing security to such open environment with heterogeneous devices is a major challenge. This paper explains the security concepts, classification of cryptography methods, and existing lightweight cryptographic techniques. This paper is organized as follows: Section II presents the lightweight cryptography and its classification. Section III presents the performance metrics of lightweight cipher schemes. Section IV explains the existing lightweight cryptography schemes. Section V presents the discussion over existing lightweight security schemes and the last section presents the conclusion of the paper.

II. Lightweight Cryptography

Cryptography is a technique which is based on mathematical concepts and provides security to the communication in the open networking environment. There are two processes in cryptography such as Key Generation and Encryption/Decryption process. Each security system must supply some security processes that ensure the secrecy of the system [68-73]. The success of cryptography depends upon complex mathematical problems like prime number factors, key length, and number of rounds [56-60]. The impression of this problem is the computation, which can be easily performed in direct direction, but tedious in the opposite direction [61-66]. The result of multiplying two numbers is not difficult; but the challenge is to find prime factors of a number. Cryptographic algorithms can be classified into three types, such as

- Symmetric cryptography
- Asymmetric cryptography
- Hash Function

- **Symmetric cryptography**

In symmetric cryptography, we use only one key for both encryption and decryption, called symmetric encryption. It is used for privacy and confidentiality. Sender encrypts the plaintext into cipher text using this key. The receiver applies the same key for decryption over cipher text in order to get plain text. Many of the lightweight block cipher algorithms are designed using this type of cryptography. Examples are DES, AES, TDEA, Camellia, etc.

- **Asymmetric cryptography**

Asymmetric cryptography uses double keys instead of a single key. Of these two keys, one key is for encryption operation and the other is for decryption operation. One key is used for converting plain text into cipher text and another key is used in converting back the cipher text to plain text. It is used in cryptographic function such as authentication, non-repudiation, and key exchange. Example: RSA, ECC, etc.

- **Hash Function**

Hash Function is based on mathematical concepts which read messages of arbitrary size, processes the message, and produces the output as fixed size. The scheme will calculate fixed length Hash value based on the plain text. It plays a vital role in integrity, message digest, and one-way encryption. It will provide a digital fingerprint of a file’s contents. Examples are MD5, SHA, etc.

Lightweight cryptography is a new type of cryptography and is developed for the resource constrained devices like limited storage capacity, processing capability, display system, and so on. Lightweight cryptography will be implemented on smart systems such as smart objects, embedded systems, RFID, Sensor nodes and devices which are exclusively designed for IoT. Salient features of a good lightweight cryptography [20][28][30-32] are as follows:

- Minimum complexity
- Smaller block size and key size
- Low memory and hardware
- Takes Simple rounds
- Consumes less power and execution time

Lightweight cryptography algorithms [2-4] [9] [12] [18, 19, 21, 29] [40-44] are categorized into

TEST Engineering & Management
November-December 2019
ISSN: 0193-4120 Page No. 3747 - 3760

different types such as Stream cipher, Block cipher, and Hash Function as shown below.

- **Stream Cipher**

Stream Cipher algorithm encrypts and decrypts the messages as one byte at a time. Due to this, stream cipher introduces delay to produce the cipher text. Its implementation is based on vernam cipher and works on the algorithm such as Cipher Feedback and Output Feedback. It can support Confusion method only.

- **Block Cipher**

Block Cipher [10][11][13] [14-16] processes the messages and breaks it into a fixed size of blocks. It converts the message into a block at a time. Block cipher is a simple design when compared to stream cipher. Its implementation is based on Feistel Cipher and has two algorithms, such as Electronic Code Book and Cipher Block Chaining. It can support both Confusion and Diffusion methods [10][17] [18][22][25][26]. Lightweight Block ciphers can be classified into following types:

- Substitution Permutation Networks (SPNs)
- Feistel structures
- Generalized Feistel Network
- Add-Rotate-XOR (ARX)
- Non Linear Feedback Shift Register
- Hybrid

Substitution Permutation Networks (SPNs)

Substitution Permutation Network is a type of block cipher and it has several rounds. In SPN, each round has a substitution, permutation, and addition of generating key operations. We can derive the subsequent keys from a single key. The keys are known as key schedule, and the derived keys are known as round keys. In this type, plain text and keys are used as input and applied in a number of rounds in order to generate cipher text.

- **Feistel Network (FN)**

Feistel Network is a basic model from which many different types of block ciphers are introduced. Entire plain text is split into two halves – left L and right R. No change in right block; but left half depends on the R and the encryption key. We apply some efficient function of two inputs such as key K and R; it generates the output and it will be XOR with an output of a mathematical function with L. This type will make several rounds (series of substitution and permutation) to previous steps. After completing the last round, cipher text is the concatenation of final left half L and right half R.

- **Generalized Feistel networks (GFN)**

GFN generates the cipher text by several iterations of the network transformation with the key. In this scheme, the input word is split into two or more sub-words, part of which is converted at each round based on a rule.

- **Add-Rotate-XOR (ARX)**

It performs addition, rotation and XOR without S box. Example: IDEA, HIGHT, SPECK, LEA.

- **Non Linear Feedback Shift register (NLFSR)**

NLFSR is more applicable in lightweight cryptography algorithms. It has a shift register which works based on stream cipher and NLFSR is implemented in RFID and sensor networks. NLFSR is resistant to many cryptanalytic attacks compared to Linear Feedback Shift Registers.

- **Hybrid**

It combines the features of above mentioned classifications in order to achieve better throughput. Hybrid type combines either Generalized Feistel Networks with ARX or Feistel with L-box and S-box. Example: HIGHT, Hummingbird.

Various lightweight block cipher schemes belonging to above classification are proposed and shown in Fig. 1.

November-December 2019
ISSN: 0193-4120 Page No. 3747 - 3760

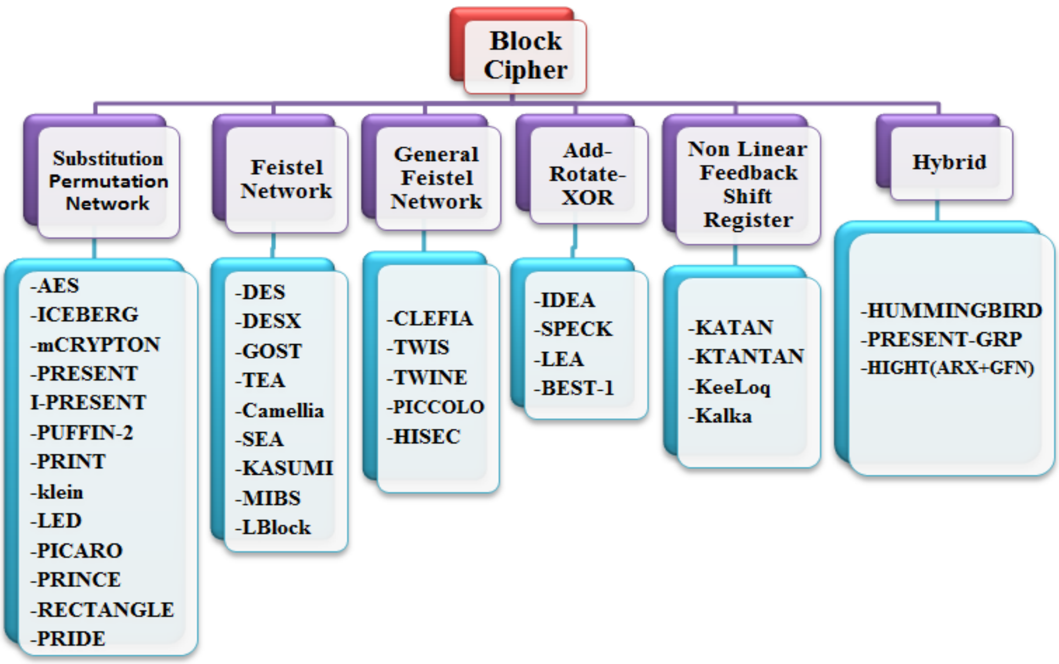

Fig. 1 Lightweight Block Cipher Schemes

III. Performance Metrics

Several lightweight block cipher schemes have been proposed (as shown in Fig.1) and compared based on performance metrics. Performance of proposed block ciphers can be measured by both software and hardware like RAM, ROM, and Gate. Performance of any proposed cipher algorithms can be measured by energy consumption, latency, and throughput.

Throughput:

Throughput is the quantity of data processed by operations such as encryption/decryption at a specific time or frequency. The proposed cipher should generate throughput at the maximum level in order to speed up the process.

Latency:

Latency denotes the numbers of cycles which are needed to process a single block of information.

Power and Energy Consumption

Energy is an important parameter while developing lightweight cipher, because these devices are operating by limited battery energy. Energy consumption will be calculated for hardware and software components as,

$$\text{Energy } [\mu J] = (\text{Latency } [\text{cycles/block}] \times \text{Power } [\mu W]) \,/\, \text{block size } [\text{bits}]$$

Latency is the time difference between conversions of plain text into cipher text. Block size is number of bits of data that are processed for encryption or decryption operation. Gate area is Resource needed for hardware platform, that is, collection of field programmable gate arrays.

$$\text{Hardware Efficiency} = \text{Throughput } [\text{Kbps}] \,/\, \text{Complexity } [\text{KGE}]$$

Throughput is number of bits used for encryption and decryption operation achieved at some frequency. Resource requirements of software applications can be measured in terms of number of registers, size (bytes) of RAM, and ROM.

$$\text{Software Efficiency} = \text{Throughput}[\text{Kbps}] \,/\, \text{Code size}[\text{KB}]$$

In Software Efficiency, throughput is the number of bits done for cryptographic operation at some frequency and code; size is the size of the executable code in KB.

IV. LIGHTWEIGHT CRYPTOGRAPHIC SCHEMES

Lightweight Cryptography is one of the most

November-December 2019
ISSN: 0193-4120 Page No. 3747 - 3760

refined cryptographic algorithms used over resource limited devices like RFID tags, sensor systems, smart cards and medical domain devices. This section discusses various Lightweight Cryptography schemes proposed by researchers. Table 1 shows the classifications of various Lightweight Cryptography Schemes.

Table 1. Classifications of Lightweight Cryptography Schemes

Cipher Name	Structure	Block Size (bits)	Key Size (bits)	No. of Rounds	Year
GOST	FN	64	256	32	1989
IDEA	Lai–Massey	64	128	8.5	1991
TEA& Versions	ARX	64	128	64	1994, 1997, 1998
DES	FN	64	56	16	1999
AES	SPN	128	128, 192, 256	12	2000
Camellia	FN	128	128/192/ 256	18/24/	2000
mCrypton	SPN	64	64/96/128	13	2005
HIGHT		64	128	32	2006
CLEFIA-128/192/ 256	FN	128	128/ 192/ 256	18/22/ 26	2007
DESX	FN	64	184	16	2007
ICEBERG	SPN	64	128	16	2008
PUFFIN	SPN	64	128	16	2008
TWINE-80 /128	FN	64	80/128	36	2011
LED-64/128	SPN	64	64/128	32/48	2011
PICCOLO	GFN	64	80/128	25/31	2011
LBlock	SPN	64	80	22	2011
TDEA	FN	64	56	32	2012
PRINCE	SPN	64	128	12	2012
LEA-128, 192 ,256	ARX	32	128, 192 ,256	24/28/ 32	2013
SIMON-32 , 48/72,64	FN	32, 48,64	64,72/96 ,96	32,36, 42	2013
SIMON-64	FN	64	128	44	2013
SIMON-96 , 128	FN	96,128	96/144,128/192/256	52/54, 68/69/ 72	2013
OLBCA	ARX	64	80	22	2014
KLEIN 64/80/96	SPN	64	64/80/ 96	12/16/ 20	2014
FeW	FN+GFN	4	80/128	32	2014
I-PRESENT	SPN	64	80/128	30	2014
PRESENT - GRP	SPN	64	128	31	2014
PRESENT	SPN	64	80/128	31	2014
RECTANGLE	SPN	64	80/128	25	2014
SIMECK 64/ 128	FN	64	64/128	32	2015
RoadRunneR	FN	64	80	12	2015
PICCOLO	GFN	64	80/128	25/31	2015
PICO	SPN	64	128	32	
SIT	FN+SPN	64	64	5	2017
GIFT -64/128 (DDT+ LAT)	SPN	64/ 128	128	28/40	2017

X. Lai et al.(1991) designed IDEA (International Data Encryption Algorithm) which performs encryption/decryption operation with 128-bits as key size, 64-bit blocks in 8.5 rounds. IDEA [75] does not use S-box and P-box to efficiently use the memory and to avoid unnecessary overhead. The IDEA has many operations like addition, XOR, and modular multiplication operations. IDEA has been designed

TEST Engineering & Management

November-December 2019
ISSN: 0193-4120 Page No. 3747 - 3760

exclusively for high-speed networks with complete cryptographic functions in order to provide the secure communication.

D. Wheeler and R. Needhan (1994) developed TEA (Tiny Encryption Algorithm) cipher which has key size as 128-bit keys, 64-bit blocks with 64 rounds. This cipher is applicable invariably in various applications due to its simple implementation and since it consumes minimum energy for processing. XTEA (eXtended TEA or Block TEA) is an extension of TEA and it addresses the weakness of TEA.

XTEA is ARX architecture and works on arbitrary size of data units but uses extra complicated key generation process and key management procedure. XTEA is suffered by a related-key rectangle attack. XXTEA (Corrected Block TEA) has proposed next to XTEA to address the issues of XTEA.

DES (1999) is designed for real smart systems and takes 56-bit as key size. DES generates cipher text of 64-bit blocks in 16 rounds. Its key size is small (56 bits) and its associated with AES. Since the cipher key of DES [74] is lesser, hackers easily break it. So it does not provide enough security to real time or sensitive applications. Also, it suffers from Linear Cryptanalysis. DESX is the variation of DES and it uses 184-bits as key size, and several rounds. DESL (DES Lightweight) and DESXL are two new versions of DES and DESX. With the advantage of DESL, single one will be used instead of 8 S-boxes, which minimizes space. Also, 7 S-boxes and one multiplexer are replaced. The S-box is designed to address various attacks such as linear, differential, and the Davis-Murphy attacks.

AES (Advanced Encryption Standard) (2000) cipher was developed by NIST and this cipher is an important, greatest, and familiar cipher. This cipher works data block of size 128-bits and has three different key lengths such as 128/192/256 bits. As we have seen previously, AES algorithm supports larger key size than DES. AES has three major methods such as Add Round Key, Byte substitution, Shifting of Rows, and Mixing Columns. AES has ten rounds and first nine rounds have the above mentioned methods and last round does not include the Mix Column transformation. AES algorithm will be applicable in numerous applications such as embedded systems and smart systems to protect the information from unauthorized access.

Axel poschmann et al. (2000) developed Feistel Network based GOST (Government Standard). It uses a key 256 bits as size and process a data unit whose size is 64 bits. It uses 32 rounds in order to create the cipher text. It has many functions like rotation operation, left rotation, in addition to basic operations.

Kazumaro Aoki (2000) developed Camellia, a block cipher. Camellia uses 128, 192, and 256 bit as key size and 128-bit as block size and it provides Advanced Encryption Standard (AES) specifications. As per design, Camellia contains 8x8 S-boxes in addition to necessary functions and operations. Hence, it will be device on tiny devices like smart cards with size of 8-bits and computers with size of 32/64-bits processors in personal computers. Camellia has been designed to support different systems of 32-byte RAM of 128-bit keys size and 64-byte RAM of 192/256-bit key size. It exists in two different versions to produce the cipher text such as Feistel structure with 18-round and 128-bits as key size, and 24-round with 192/256-bits as key size. It has some additional input/output whitening and FL-function.

Chae Hoon Lim et al. (2005) designed a cipher mCrypton (miniature crypton) with 64/96/128 bits as key sizes with 64-bit block. It is a specially designed and applied in tiny devices, such as RFID and sensors. It needs about 3500 to 4100 gates for cryptographic operations.

D.Hong et al.(2006) introduced block cipher HIGHT[80]. It uses key size of 128-bits and

November-December 2019
ISSN: 0193-4120 Page No. 3747 - 3760

operates on 64-bit blocks and produces cipher on 32 rounds. HIGHT uses a compact round function even without using S-boxes. It is applicable and suitable for simple computations and performs all operations and needs 2608GE to implement its hardware.

Debra Cook et al.(2007) proposed the scheme known as elastic cipher [46] which increases the size of cipher to twice the size of an original block cipher. Elastic cipher has operations such as reduction method, round function, etc. Elastic cipher provides security measures against various attacks and threats.

Taizo Shirai et. al.(2007) designed a lightweight block cipher CLEFIA[14] which belongs to Feistel cipher and it is suitable for efficient hardware and software implementations. It does not need registers due to its architecture which is a serialized one. CLEFIA operates on 128-bit data units with 128/192/256 bit as key size in 18/22/26 rounds. CLEFIA's implementations have 2488GE for encryption only of 128-bit Key and 116GE for decryption. CLEFIA has been designed in order to minimize the multiplexers count by using clock gating techniques. Also, designers have used scan flip flops and MUX in order to minimize the gate area.

Bogdanov et al. (2**007**) designed a SPN based ultra-lightweight cipher PRESENT[5] and it is the cipher designed for ultra-light weight devices with almost 1000GE. PRESENT [27] uses key size as 80/128-bit and converts 64-bit data blocks in 31 rounds. It needs 1030GE to implement 80-bit keys size on cryptographic operations. Also, it is used to combine AES and used in lightweight block ciphers. ISO/IEC 29192-*2:2012* is the project of PRESENT light weight cipher. PRESENT is an efficient hardware part since PRESENT is serialized architecture and designed using wired diffusion layer free from algebraic unit.

Huiju Cheng and Howard M.Heys (2008) developed ICEBERG [81] cipher and it produces cipher text fast. It uses 128-bit keys to produce cipher text size of 64-bit Blocks over 16 rounds. Its work is different from other cipher and provides better performance to the maximum level since it alters the key value in all the clock cycle free from loss of data. ICEBERG has implemented using 5800 gates and results 400 Kbps of throughput with efficient combinations of encryption/decryption. The overall design provides low-cost encryption/decryption functionality.

A Block cipher named PUFFIN was developed by **Huiju Cheng (2008)** for smart and embedded applications. PUFFIN uses 128-bit key with 64-bit block size for cryptographic operations. PUFFIN produces the cipher text using permutations and substitutions operations. PUFFIN has 4x4 S-boxes and produces optimal results. Also, it is applicable for 0.18-micron CMOS technology. PUFFIN has three operations such as substitution, bitwise XOR, and transposition. It uses substitution, addition of round key, and permutation operations to produce the cipher text.

T. Suzaki et al.(2011) designed a TWINE and it is GFN based lightweight block cipher. It has an 80-bit and 128-bit as key sizes for 64-bit block cipher and produces cipher text in 36 rounds. TWINE and L Block have similar characteristics with little differences. TWINE cipher is modernized cipher since it uses only one S-box while L Block has ten S-boxes. Moreover, TWINE has different permutation such as nibble instead of bit permutation. TWINE cipher can be compromised by the attack like meet-in-the-middle attacks due to its simplified key scheduling operation.

Kyoji Shibutani et al. (2012) developed the block cipher algorithm known as PICCOLO [23] [8], a type of Generalized Feistel Network (GFN). It uses key size as 80/128-bit with 25/31 rounds and works for 64-bit block cipher. It produces cipher text using four 16-bit key as whitening. A diffusion matrix separates the PICCOLO's F-function which

November-December 2019
ISSN: 0193-4120 Page No. 3747 - 3760

has two S-box layers. PICCOLO has a permutation technique which is 8-bit word.

Wenling Wu et al. (2012) developed a new block cipher known as L Block [24]. This cipher has round function F which has 2 layers such as substitution and permutation and it is designed for 64-bit block size. Also, L Block has round function and rotation function. In L Block, confusion and diffusion are existing and L Block has master key of 80-bit size. L Block cipher generates round sub-key by using simple rotation on left most with 32-bits of master key. Four 8-bit lookup tables can be formed by eight S-boxes and operation like word-wise permutation; both are of size of 4-bit.

William C. Barker et al. (2012) designed Feistel Network based block cipher known as Triple Data Encryption Algorithm (TDEA) and TDEA works based on DEA cipher [47] with some differences. TDEA cipher is designed for block and key size of 64-bits. While generating key, 56 bits are randomly generated. TDEA has two operations such as forward and inverse operation which are similar to DEA's operations such as forward and inverse transformations.

Borghoff et al. (2012) designed PRINCE[25] cipher which generates cipher text in 12 rounds. PRINCE cipher is designed for 64-bit data blocks with 128-bit as key size and with minimum energy consumption. It needs 2953GE to implement the cipher about 533.3 Kbps of throughput.

Light Encryption Device (LED)[48] cipher was developed by **Jian Guo et al. (2013),** a lightweight block cipher. Light Encryption Device combines the concepts of AES and S-box of PRESENT [5][27] cipher. LED produces the cipher text

in 4 rounds, block size as 64-bit, and 64/80/96128-bit as key size. It has no key scheduling process for the row-wise processing and the mix column process of previously mentioned ciphers such AES and PHOTON. But, it may be vulnerable to biclique cryptanalysis.

Ray Beaulieu et al. (2013) designed two lightweight block ciphers SIMON [7] and SPECK. SPECK [49] cipher consists of ten different block ciphers in order to ensure secure applications in a controlled environment. Also, SPECK works similar to the mixing function of THREE FISH. SIMON cipher designed for 2n-bits of block size, mn-bits as key size is represented as 2n/mn. SIMON and SPECK have the operations such as permutations and rotation. SIMON supports 64/72/96/128/144/192/256 bits for key, 32/48/64/96/128 for block and 32/36/42/44/ 52/54/68/69/72 bits for round numbers. SIMON presents differential fault attacks and dynamic cube attacks.

Sufyan Salim et al. (2014) developed a new block cipher known as Optimized Lightweight Block Cipher Algorithm (OLBCA)[50]. OLBCA produces cipher text in 22 rounds for 64-bit data with 80-bit key size. In OLBCA, each round has

Operations such as bit permutations, rotations, XOR, and word permutation, except the last round.

Gong et al. (2014) designed a lightweight cipher named KLEIN [20] which is SPN type. KLEIN combines the features of AES and PRESENT. KLEIN generates cipher text of 64-bit block size, 64/80/96-bit as key size in 12/16/20 number of rounds for KLEIN-64/80/96 and KLEIN uses 4x4 S-box. KLEIN's I/O is arrays of single dimensional arrays of bytes. It works against the potential related key attacks.

Manoj Kumar et al. (2014) developed block cipher named Feather Weight (FeW)[79]. Few combine Feistel and Generalized Feistel Structures principles. FeW generates cipher text of over 4-bit data block with 80/128 bits as key size in 32 rounds. FeW uses S-Box of HummingBird2 , Key schedule of PRESENT and Generalized Feistel based design similar to CLEFIA. Few designed to meet various attacks such as linear, differential attacks.

November-December 2019
ISSN: 0193-4120 Page No. 3747 - 3760

M.R. Zaba et.al (2014) designed PRESENT based cipher known as I-PRESENT [82]. I-PRESENT uses data block and key size similar to PRESENT and generates cipher text in 30 rounds. It differs from PRESENT in one aspect – PRESENT performs 31 rounds. It also uses the PRINCE scheme concepts. In this scheme, S-box layer has two additional 4x4 S-boxes and executes for 16 times. This scheme needs 2769GE to implement hardware for cryptographic operations. I-PRESENT generates cipher text after 15-round function and 15-round involute function. In I-PRESENT, both encryption and decryption are similar except that they use the round subkeys.

Gaurav Bansod et al. (2015) proposed a new lightweight block cipher, a hybrid approach which is based on group operation (GRP) [55] and S-box of PRESENT cipher. This cipher operates on 64-bit blocks, 128-bit as the key size with confusion. Confusion has S-box of PRESENT and P-box by using GRP for 64-bit and 128-bit block size. The proposed cipher uses GRP for key generation. GRP combines S-box of PRESENT and confusion property. It is an efficient cipher since it consumes minimum memory and gate equivalents. Also, it is tested and confirmed on LPC2129 processor. GRP ensures that it is a compact implementation in hardware, in addition to ensuring to achieve the expected avalanche effect.

Wentao Zhanget et al. (2015) proposed a novel SPN based lightweight block cipher known as RECTANGLE[6]. RECTANGLE cipher uses bit-slice techniques to generate the cipher text. RECTANGLE cipher generates cipher with 80/ 128 bits as key size for 64-bits block in 25 rounds. RECTANGLE cipher performs three major operations such as AddRoundkey , Substitution of Column, and last Row shift.

Gangqiang Yang et al. (2015) developed a lightweight block cipher named SIMECK. Actually, SIMECK [51] is a hybrid approach which combines the two different ciphers, SIMON [7] and SPECK. Three different types of SIMECK are available, such as SIMECK32/64, SIMECK48/96, and SIMECK64/128. SIMECK uses 4n-bit key as size to produce the cipher text.

Adnan Baysal et al. (2015) designed Feistel bit-slice block cipher RoadRunneR [12]. The proposed cipher works with 64-bits of data, 80/128-bits as key size in 10/12 rounds respectively. It combines S-box and PRIDE. Road Runner does not use swap operation in the final round.

Gaurav Bansod et al. (2015) developed SPN based ultra-lightweight cipher known as PICO cipher[77]. This cipher generates cipher text with 64-bits block size, 128-bits as key size in 32 rounds. Each round consists of the operations such as AddRoundkey, SubColumn, and Bit_Shuffle. PICO has a large number of active S-boxes in order to meet the linear and differential attacks. PICO has been designed using S-box of lightweight block ciphers and P-box of GRPs.

Hwajeong Seo et al. (2016) introduced lightweight block cipher LEA [52] in three different 128, 192, and 256-bits. The proposed cipher has three different operations like Addition, Rotation, and XOR (ARX) operations for smart systems. LEA cipher generates different types of ciphers which depend on different key sizes (bits) and rounds such as 128/ 24,192/28,256/32. This cipher does not have S-box and word size is 32-bit.

Muhammad Usman et al. (2017) proposed an hybrid approach Secure IoT (SIT)[78] which is a Feistel and Substitution Permutation Networks. It is a symmetric key block cipher which uses 64-bit as key size and generates the cipher text. SIT was designed to minimize the number of rounds.

Ahssan Ahmed Mohammed et al. (2017) designed a Non-Feistel block cipher [53] which generates cipher over multiple of 32 bits data with multiples of 48 bits as key size. The proposed cipher has different operations such as addition,

November-December 2019
ISSN: 0193-4120 Page No. 3747 - 3760

permutation, and XOR operation, Balance function, maps function, and wave function.

Subhadeep Baniket et al. (2017) developed SPN based block cipher known as GIFT [54]. GIFT is an improvement of PRESENT block cipher which is a small and a fast cipher. GIFT is a hybrid approach which has two tables such as Difference Distribution Table (DDT) and Linear Approximation Table (LAT) of the S-Box. GIFT generates cipher text with two different versions such as GIFT-64 in 28 rounds and GIFT-128 in 40 rounds with 128-bits as key size. They are called as GIFT-64 and GIFT-128 and both uses 128-bit as key length. In GIFT, each round of GIFT has 3 phases such as substitution, permutation, and Addition of Round Key.

V. DISCUSSION

IDEA was designed using XOR, addition and modular operation instead of using S-box and P-box in order to ensure the memory consumption. But, it is not secure and not suitable for real time data transfer and embedded devices. DES is not suitable for today's real time applications because it has 56-bit key. Twine algorithm used nibble permutation and single S box and suffers for attack. PICCOLO uses GFN in such a way that GFN needs 16-bits word and more rounds to produce the cipher key. It considerably increases more power consumption as well as produces low throughput only. RECTANGLE's computations are more complex because it has more cycles. SIMECK is compromised in security aspects because it is vulnerable to various attacks like Random-Byte Fault Attack and Bit-Flip Fault Attack. Since, SIMECK is a combination of SIMON and SPECK ciphers. RECTANGLE, SPECK, and I-PRESENT suffer from security vulnerabilities.

CLEFIA cipher needs extra care to store and process the intermediate key of key scheduling part. It is not apt for embedded systems like RAM size of 64 bytes. Also, CLEFIA's constants consume 384 bytes which need extra ROM size. So, to device this scheme with a ROM size as 512 bytes is a cumbersome process. In LED, each round performs operations like AddConstants, SubCells, ShiftRows, and MixColumns Serial. It consumes considerable energy per bit for these operations.

PRINCE cipher was developed to improve the processing speed by increasing RAM size of 128 bytes. Also, it is designed to improve the execution by using two pieces of S-box. PRINCE needs larger ROM in smart systems due to its functions. It also produces some additional overheads due to key schedule processing in addition to cryptographic functions and PRINCE's constants are large in matrix operation code.

PRESENT has to maintain two different tables of size of 256-byte and is used for the cryptographic operations. Also, PRESENT is vulnerable to side-channel attack and related-key attack. In I-PRESENT, S-box layer has two additional 4x4 S-boxes and executes for 16 times. This scheme needs 2769GE to implement hardware for both encryption and decryption processes. Because of this, I-PRESENT consumes additional power to implement this scheme. Camellia has been designed in a conservative model and need to focus on sensitivity applications.

GOST cipher needs some additional MUX to choose the round key for serialized implementation and effective operations. It takes some area for serialized implementation and key schedule. Also, it needs additional 256 flip-flops for storing intermediate results while cipher text is generated. It also needs the key to be updated. Another limitation of this cipher is complexity will be varied based on applications.

PUFFIN cipher introduced some additional key selection steps in the key schedule procedure in order to select 64 bits out of 128 bits to perform the encryption or decryption process. Also, PUFFIN cipher includes an additional number of rounds to every bit of the 128-bit key selection process. The software application of PRESENT-GRP needs

TEST Engineering & Management

November-December 2019
ISSN: 0193-4120 Page No. 3747 - 3760

large RAM size than existing schemes. Hence, it is not a good technique to select the optimal solution under resource constrained situation, like memory.

To ensure security in algorithms S-boxes are introduced and the number of rounds is increased. It is a tradeoff between introducing S-boxes and power consumption. Based on the investigation studies, existing lightweight block ciphers are still developing to meet the International standard and also to meet the current requirements. After reviewing the existing schemes and considering them inadequat, it becomes necessary to develop a novel light weight cryptography scheme to minimize the power consumption and provide better security. The proposed scheme should minimize the number of rounds, ensure the code reusability, and reuse the storage area. Hence the proposed scheme should consider all the above discussed factors and ensure the security to resource constrained devices.

VI. CONCLUSION

Lightweight cryptography plays a predominant role in resource constrained devices like smart devices to ensure the security. We have highlighted the concepts of Internet of Things and its applications in diverse domains such as smart enterprise, smart education, smart health care system, etc.

We presented the principles of lightweight cryptography, its salient features and its classifications in general – the concepts of block cipher schemes and their roles in smart devices in particular. Data structures of existing lightweight cryptography algorithms and schemes have been completely mentioned in this paper. This paper emphasizes the contribution and significance of light weight cryptographic algorithms in smart objects in order to provide secure communication in open environment. This paper also talks about attacks and vulnerabilities of existing lightweight cipher schemes. Additionally, this paper presents the comprehensive investigation of the light weight cryptographic algorithms of all sorts of classifications such as SPN, Feistel Cipher, GFN, ARX, NLFSR, and Hybrid. Moreover, we have presented complete information of all lightweight cryptographic schemes up to recent works. Obviously, this paper will be useful for the researchers to know the existing lightweight cipher schemes and propose the new cryptographic scheme for the smart systems.

REFERENCES

[1] S. A. Kumar, T. Vealey, and H. Srivastava, “Security in internet of things: Challenges, solutions and future directions”, 49th Hawaii International Conference on System Sciences (HICSS). IEEE, 2016, pp. 5772–5781.

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

[3] Daniele Miorandi, Sabrina Sicari , Francesco De Pellegrini , Imrich Chlamtac, “Internet of things: Vision, applications and research challenges”, Elsevier, Ad Hoc Networks 10, 2012, pp 1497–1516.

[4] D. Guinard, V. Trifa, F. Mattern, E. Wilde, “From the Internet of Things to the Web of Things: Resource Oriented Architecture and Best Practices”, Springer, New York, Dordrecht, Heidelberg, London, 2011 (Chapter 5).

[5] Bogdanov et al., “PRESENT: An ultra-lightweight block cipher”. In CHES ,Vol. 4727, September, 2007, pp. 450-466.

[6] Zhang et al., “RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms”, Science China Information Sciences, 58(12), 2015,pp.1-15.

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

[8] Suzaki, T., Minematsu, K., Morioka, S. and Kobayashi, E., “Twine: A lightweight, versatile block cipher”, ECRYPT Workshop on Lightweight Cryptography , November, 2011.

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

[10] Shibutani K, Isobe T, Hiwatari H, Mitsuda A, Akishita T and Shirai, T, “Piccolo: An ultra-lightweight blockcipher”, in CHES Vol. 6917, pp. 342-357, September 2011.

[11] AlDabbagh, S.S.M., Shaikhli, A., Taha, I.F. and Alahmad, M.A., “Hisec: A new lightweight block cipher algorithm”, Proceedings of the 7th International Conference on Security of Information and Networks, ACM, September 2014, pp.151.

[12] Baysal, A. and Şahin, S., “Roadrunner: A small and fast bitslice block cipher for low cost 8-bit processors”,

International Workshop on Lightweight Cryptography for Security and Privacy, Springer, September, 2015 , pp. 58-76.

[13] Beierle et al, “The SKINNY family of block ciphers and its low-latency variant MANTIS”, in Annual Cryptology Conference, Springer Berlin Heidelberg, August, 2016, pp. 123-153.

[14] Shirai T, Shibutani K, Akishita, T., Moriai, S. and Iwata, T., “The 128-bit block cipher CLEFIA”, FSE 2007, March. Vol. 4593, pp. 181-195.

[15] Daemen, J. and Rijmen, V., “The wide trail design strategy”, in IMA International Conference on Cryptography and Coding, Springer, Berlin, Heidelberg, December, 2001, pp. 222-238.

[16] Standaert, F.X., Piret, G., Gershenfeld, N. and Quisquater, J.J., “SEA: A scalable encryption algorithm for small embedded applications”, International Conference on Smart Card Research and Advanced Applications, Springer, April 2006, pp. 222-236.

[17] J. Lee, K. Kapitanova, and S. H. Son, “The price of security in wireless sensor networks,” Computer Networks, 2010, vol. 54, no. 17, pp. 2967–2978.

[18] S. Chen, G. Yang, and S. Chen, “A security routing mechanism against sybil attack for wireless sensor networks”, International Conference on Communications and Mobile Computing (CMC), IEEE, 2010, vol 1, pp. 142–146.

[19] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, “A survey of lightweight-cryptography implementations”, IEEE Design & Test of Computers, 2007,vol. 24, no. 6, pp. 522–533.

[20] Zheng Gong, Svetla Nikova and Yee-Wei Law, “KLEIN: A New Family of Lightweight Block Ciphers”, Cryptography and Communications, Springer, April 2015, vol. 02, no.1.

[21] Isha and Ashish Kr. Luhach, “Analysis of Lightweight Cryptographic Solutions for Internet of Things”, Indian Journal of Science and Technology, July 2016, vol. 56, no. 1

[22] Matsui, M, “New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis”, Springer, Heidelberg, FSE 1996. LNCS, Nov 2015, vol. 1039, pp. 205–218,.

[23] Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo ShiraiB. Preneel and T. Takagi, “Piccolo: An Ultra-Lightweight Blockcipher”, International Association for Cryptologic Research, LNCS 6917, Dec 2012, pp. 342–357.

[24] W. Wu and L. Zhang, “LBlock: A Lightweight Block Cipher Applied Cryptography and Network Security”, Springer Berlin / Heidelberg, , August 2012,Vol. 6715, pp. 327-344.

[25] J. Borghoff, et al., “PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications”, Advances in Cryptology – ASIACRYPT, Springer Berlin Heidelber , July 2013, vol. 7658, pp. 208-225.

[26] L. Knudsen, et al., "PRINTcipher: A Block Cipher for IC-Printing," in Cryptographic Hardware and Embedded Systems, Springer Berlin Heidelberg, March 2010, CHES 2010. vol. 6225, pp. 16-32

[27] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher Cryptographic Hardware and Embedded Systems – CHES”, in Springer Berlin / Heidelberg, Vol. 4727, March 2013, pp. 450-466.

[28] A. Poschmann, G. Leander, K. Schramm, and C. Paar, “New light-weight crypto algorithms for RFID,” in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), May 2007, pp.1843–1846.

[29] T. Eisenbarth and S. Kumar, “A survey of lightweight-cryptography implementations”, IEEE Des. Test. Computer, vol. 24, no. 6, Nov./Dec. 2007, pp. 522–533.

[30] Wentao Zhang et al. “RECTANGLE: A bit-slice lightweight block cipher suitable for multiple platforms”, Science China Information Sciences, 2015, 58(12),1–15.

[31] Long Wen, Meiqin Wang, Andrey Bogdanov, and Huaifeng Chen., “Multidimensional zero-correlation attacks on lightweight block cipher hight: Improved cryptanalysis of an iso standard”, Elsevier, Information Processing Letters, 2014,114(6), pp. 322 – 330.

[32] A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang, “Pushing the limits: A very compact and a threshold implementation of AES”, Eurocrypt’11, LNCS 6632, Springer-Verlag, 2011, pp. 69–88.

[33] H. J. Ban, J. Choi, and N. Kang, “Fine-grained support of security services for resource constrained internet of things,” International Journal of Distributed Sensor Networks, vol. 2016, 2016.

[34] Pan Wang et al., “The internet of things: a security point of view”, Internet Research, 2016, vol.26, no.2, pp. 337–359.

[35] M. Ebrahim, S. Khan, and U. Khalid, “Security risk analysis in peer 2 peer system: an approach towards surmounting security challenges,” arXiv preprint arXiv:1404.5123, 2014.

[36] J. Wang, G. Yang, Y. Sun, and S. Chen, “Sybil attack detection based on RSSI for wireless sensor network”, International Conference on Wireless Communications, Networking and Mobile Computing. IEEE, 2007, pp. 2684–2687.

[37] Neelima Saini &Sunita Mandal, “Review paper on cryptography”, International Journal of Research (IJR), May 2015 , e-ISSN: 2348-6848, p- ISSN: 2348-795X, Volume 2, Issue 05.

[38] Coron, J.-S, “What is cryptography?”, Security & Privacy, IEEE 2006, Vol.4, Issue 1, pp. 70- 73.

[39] Salah A. k. Albermany, Fatima RadiHamade ,“Survey: Block cipher Methods”, International Journal of Advancements in Research & Technology, Volume 5, Issue 11, November-2016 11 ISSN 2278-7763.

[40] William stalling, “Cryptography and Network Security”, Prentice Hall. Pub Date: November 16, 2005.

[41] T. Eisenbarth, Z. Gong, T. Guneysu, S. Heyse, S. Indesteege, S. Kerckhof, F. Koeune, T. Nad, T. Plos, F. Regazzoni et al., “Compact implementation and

performance evaluation of block ciphers in attiny devices", International Conference on Cryptology in Africa, Springer, 2012, pp. 172–187.

[42] S. Panasenko and S. Smagin, "Lightweight cryptography: Underlying principles and approaches", International Journal of Computer Theory and Engineering, vol. 3, pp. 516-520, 2011.

[43] S. S. M. Aldabbagh, et al., " Lightweight Block Cipher Algorithms: Review Paper", International Journal of Enhanced Research in Science, Technology & Engineering ISSN: 2319-7463, Vol. 5 Issue 5, May-2016.

[44] Levent Ertaul, Arnold Woodall, "IoT Security: Performance Evaluation of Grain,MICKEY, and Trivium - Lightweight Stream Ciphers", International Conference on Security and Management ,SAM'17, ISBN: 1-60132-467-7, CSREA Press.

[45] D. Salama, H. A. Kader and M. Hadhoud, "Studying the Effects of Most Common Encryption Algorithms," International Arab Journal of e-Technology, 2011, vol. 2, no. 1.

[46] Debra Cook et. Al, "Elastic Block Ciphers: The Basic Design", ASIACCS'07, March 20-22, 2007, Singapore.

[47] William C. Barker, " Triple Data Encryption Algorithm (TDEA) Block Cipher", NIST Special Publication, January 2012.

[48] Jian Guo, Thomas Peyrin, Axel Poschmann and Matt Robshaw, "The LED Block Cipher", CHES 2011 Nara, Japan.

[49] Ray, S. Douglas, S. Jason, T. Stefan, W. Bryan, and W. Louis, "The simon and speck families of lightweight block ciphers," Cryptology ePrint Archive, Report./404, Tech. Rep., 2013.

[50] Sufyan Salim Mahmood Aldabbagh ; Imad Fakhri Taha Al Shaikhli, "OLBCA: A New Lightweight Block Cipher Algorithm", 3rd International Conference on Advanced Computer Science Applications and Technologies,IEEE, 2014

[51] Gangqiang Yang, Bo Zhu, Valentin Suder, Mark D. Aagaard, and Guang Gong, "The Simeck Family of Lightweight Block Ciphers", Sept 15, 2015.

[52] Hwajeong Seo ,Zhe Liu , Jongseok Choi , Taehwan Park , and Howon Kim, "Compact Implementations of LEA Block Cipher for Low-End Microprocessors". Jan2016

[53] Ahssan Ahmed Mohammed, Dr.Abdulkareem O. Ibadi, "A Proposed Non Feistel Block Cipher Algorithm", QALAAI ZANIST JOURNAL, 2017,Vol. 2, No. 2.

[54] Subhadeep Banik et al., "GIFT: A Small Present", Cryptographic Hardware and Embedded Systems – CHES 2017,Springer, pp 321-345|

[55] 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.

[56] Shankar, K. and Eswaran, P., 2016. RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique. Journal of Circuits, Systems and Computers, 25(11), p.1650138.

[57] Rajesh, M., Kumar, K.S., Shankar, K. and Ilayaraja, M., Sensitive Data Security In Cloud Computing Aid Of Different Encryption Techniques. Journal of Advanced Research in Dynamical and Control Systems, 18.

[58] Avudaiappan, T., Balasubramanian, R., Pandiyan, S.S., Saravanan, M., Lakshmanaprabu, S.K. and Shankar, K., 2018. Medical Image Security Using Dual Encryption with Oppositional Based Optimization Algorithm. Journal of Medical Systems, 42(11), p.208.

[59] Shankar, K. and Eswaran, P., 2015. Sharing a secret image with encapsulated shares in visual cryptography. Procedia Computer Science, 70, pp.462-468.

[60] K. Karthikeyan, R. Sunder, K. Shankar, S. K. Lakshmanaprabu, V. Vijayakumar, Mohamed Elhoseny, Gunasekaran Manogaran. Energy consumption analysis of Virtual Machine migration in cloud using hybrid swarm optimization (ABC–BA), The Journal of Supercomputing. 2018.https://doi.org/10.1007/s11227-018-2583-3

[61] Mohamed Elhoseny, HamdyElminir, AlaaRiad, Xiaohui Yuan, "A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption", Journal of King Saud University - Computer and Information Sciences, Elsevier, 28(3):262-275, 2016 (http://dx.doi.org/10.1016/j.jksuci.2015.11.001)

[62] Shankar, K., and P. Eswaran. "An Efficient Image Encryption Technique Based on Optimized Key Generation in ECC Using Genetic Algorithm." Artificial Intelligence and Evolutionary Computations in Engineering Systems. Springer, New Delhi, 2016. 705-714.

[63] M Elhoseny, X Yuan, HK ElMinir, and AM Riad, " An energy efficient encryption method for secure dynamic WSN", Security and Communication Networks, Wiley, 9(13): 2024-2031, 2016 (Doi: 10.1002/sec.1459)

[64] Pandi Selvam Raman, K.Shankar, Ilayaraja M, "Securing cluster based routing against cooperative black hole attack in mobile ad hoc network", International Journal of Engineering & Technology, Volume. 7, Issue. 9, page(s): 6-9, 2018.

[65] I. Ramya Princess Mary, P. Eswaran, K.Shankar, "Multi Secret Image Sharing Scheme based on DNA Cryptography with XOR", International Journal of Pure and Applied Mathematics, Volume 118, No. 7, page(s) 393-398, February 2018.

[66] Nur Aminudin, Andino Maseleno, K.Shankar, S. Hemalatha, K. Sathesh kumar, Fauzi, Rita Irviani, Muhamad Muslihudin, "Nur Algorithm on Data Encryption and Decryption", International Journal of Engineering & Technology, Volume. 7, Issue-2.26, page(s): 109-118, June 2018.

[67] Sriti Thakur, Amit Kumar Singh, Satya Prakash Ghrera, Mohamed Elhoseny, Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications, Multimedia Tools andApplications, June 2018 (DOI: https://doi.org/10.1007/s11042-018-6263-3).

[68] P.Manickam,T.GuruBaskar,M.Girija,Dr..Manimegalai,"Performance comparisons of Routing protocols in Mobile Ad hoc Networks", International Journal of Wireless and

November-December 2019
ISSN: 0193-4120 Page No. 3747 - 3760

Mobile Networks (IJWMN), Vol.3, No. 1 Feb 2011, DOI:10.5121/ijwmn.2011.3109 pp:98-106.

[69] P.Manickam, Dr. D. Manimegalai,"A Highly Adaptive Fault Tolerant Source Routing Protocol for Energy Constrained Mobile Ad Hoc Networks", International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10, No.7 (2015), pp. 16885-16897.

[70] P.Manickam, Dr. D. Manimegalai,"A Highly Adaptive Fault Tolerant Routing Protocol for Energy Constrained Mobile Ad hoc Networks", Journal of Theoretical and Applied Information Technology, ISSN: 1992-8645, E-ISSN: 1817-3195,Nov. 2013. Vol.57,No.3

[71] P.Manickam, et al., "Routing Schemes and Protocols For Internet of Things: A Review", International Journal of Theoretical and Applied Sciences, Jan-June 2018, Special Issue, ISSN No.(Print):0975-1718, (Online): 2249-3247, 10(1): pp. 81-85.

[72] P.Manickam et al., "Comprehensive Approach in Studying the Behaviour of Contiki RPLProtocol in Diverse Data Transmission Ranges", Int. J. Sc. Res. in Network Security and Communication, June 2018, ISSN: 2321-3256, Volume-6, Issue-3, pp 37-42.

[73] M Elhoseny, X Yuan, Z Yu, C Mao, H El-Minir, and A Riad, " Balancing Energy Consumption in Heterogeneous Wireless Sensor Networks using Genetic Algorithm", IEEE Communications Letters, IEEE, 19(12): 2194 -2197, 2015.

[74] Standard, NIST FIPS, Data Encryption standard(DES), Federal Information Processing Standards Publication, ,1999,46-3

[75] X.Lai and J.L Massey, "A proposal for a new block encryption standard, Advances in Cryptology", ICISC 2010, Springer, LNCS, 473,1991, 00.4967

[76] D.Wheeler and R.Needhan "TEA, a Tiny Encryption Algorithm, Fast Software Encryption" (FSE 1994), Springer, LNCS, 1008, 1994, pp.363366

[77] Gaurav Vijay Bansod ,"PICO: An Ultra lightweight and Low power encryption design for pervasive computing", Frontier of Information Technology & Electronics Engineering June 2015

[78] Muhammad Usman, Ifram Abmed, M.Imran Aslam, Shujaat Khan, a EolutiveLightWeight Encryption Algorithm for Secure Internet of Things, International Journal of Advanced Computer Science and Applications. Vol.8,No.1,2017

[79] Manoj Kumar, Saibal K.Pal and Anupama Panigrahi,Few: A Lightweight Block Cipher,

[80] D. Hong et.al., "HIGHT: A New Block Cipher Suitable for Low-Resources. Cryptographic hardware and embedded system." Ches 206, Springer, LNCS,4249,2006

[81] Huiju Cheng, Howard M.Heys , "Compact ASIC implementation of the ICEBERG block cipher with concurrent error detection",IEEE symposium on circuits

[82] M.R. z'aba, N.Jamil, M.E. Rusli, M.Z Jamaludinm, and A.A.M.Yasir, "I-PRESENT: An Involutive Lightweight Block, Cipher", Journal of Information Security, Scientific Research Vol.5,2014,pp.114-122