International Journal of Computer Engineering and Information Technology

VOL. 11, NO. 6, June 2019, 119–129
Available online at: www.ijceit.org
E-ISSN 2412-8856 (Online)

A Survey Paper of Lightweight Block Ciphers Based on Their Different Design Architectures and Performance Metrics

Sohel Rana[1], Md. Anwar Hussen Wadud[2], Ali Azgar[3] and Dr. Mohammod Abul Kashem[4]

[1, 2, 3] Lecturer, Department of CSE, Bangladesh University of Business & Technology (BUBT), Mirpur-2, Dhaka-1216, Bangladesh

[4] Professor, Department of CSE, Dhaka University of Engineering & Technology (DUET), Gazipur, Dhaka-1707, Bangladesh

[1]sohelresearch@gmail.com, [2]mahwadud@gmail.com, [3]azgor07@gmail.com, [4]drkashemll@duet.ac.bd

ABSTRACT

Now-a-days, Security in communication over Internet has turned out to be complex as technology becomes faster and more efficient rapidly especially for resources limited devices like embedded devices, wireless sensors, RFID (Radio Frequency Identification) tags, Internet of Things (IoT) devices. Lightweight cryptographic algorithms provide security for these devices to protect data from intruders. A thorough understanding of lightweight cryptography will help people develop better ways to protect valuable information as technology develops faster. But as time passes, the cryptanalyst (the science of discovering weaknesses in cryptosystems and breaking them if possible) breaks the ciphers which were known as unbreakable. This paper represents a survey of recent lightweight block cipher algorithms with performance analysis for different evaluation metrics like RAM size, Execution Cycles as well as provides modern advances in the said field and finding scopes for future research.

Keywords: *Lightweight, Small-Computing-Devices, IoT, Block-cipher, Performance-Metrics, Feistel, SPN, FELICS.*

1. INTRODUCTION

Lightweight cryptography [1] is a sub-category in the field of cryptography that intends to provide security solutions for resource-constrained devices. Cryptography means "secret writing". In computer communication we want to encrypt our information so that no unwanted entity but the expected one can decipher the information. At the core of lightweight cryptography there is a trade-off between security and light-weightiness: that is how we can achieve a good level of security in small computing devices? Recently, academic communities have been doing a significant amount of work related to lightweight cryptography; to implement conventional cryptography standards efficiently, and to design and analyze new lightweight algorithms and protocols [1].

The widespread utilization of small computing devices such as sensors nodes, Radio-Frequency Identification (RFID) tags, industrial controllers and smart cards indicates there have been massive changes in our lives. Also, technology has made our life easier and convenient with innovations. Using Internet we are connecting our devices. Smart locks are protecting our houses. Smart phones, smart TVs, video game consoles, personal computers, laptops, tablets even the refrigerator and air conditioners have gained the capability to communicate over Internet. This trend is expected to grow even exponentially and by the year 2020 it is estimated that, there will be over 50 billion objects connected to the Internet. According to that estimation each person on the earth shall have 6.6 objects online. Millions of sensors will be all around us collecting information from physical phenomena and will upload it to the Internet. Some suggestion has been made that application of IoT is yet in the early stage but is beginning to ubiquitous rapidly. IoT can be used in building automation system. Various industries are becoming more and more interested in integration of IoT.

IoT has brought in improvement opportunities in health-care. Health-care solutions through IoT can decrease costs, improve the outcome of treatment. Doctors can make informed judgment and monitor patient real time before things get of hand. It also enhances patient experience when they see improved accuracy in diagnosis, timely intervention by the physicians.

Resource constrained devices contribute in many areas. These make mining production safer and productive.

More accurate forecasting in weather and disaster will be possible. They are transforming transportation systems and automobile services. Transportation companies will be able to track and monitor their vehicles from origin to destination. If those are equipped with sensors and RFID tags [8]. Logistics industries and courier services are heavily dependent on goods tracking devices.

With so many applications looking forward to adapt the technology with the purposes to help in economy growth, transportation, healthcare facility and a better life style for the general masses, adequate security to their data is vital to encourage the adaptation process. New security and privacy considerations arise as we shift from desktop computer to small computing devices like IoT, RFID tags etc. It is challenging to implement heavyweight cryptographic standards to small devices [1], [7]. Many conventional cryptographic algorithms, was optimized for desktop and server environments. Optimization in terms of security, performance and resource requirements makes those algorithms difficult or impossible to implement in resource-constrained devices. Even if they can be implemented, they thwart the performance on the small devices. If we want the most strong and secure system we must equip our system with powerful resources.

But conventional cryptographic algorithms like RSA inherently perform well in these powerful devices; therefore lightweight algorithms are not necessary for them. Embedded systems, RFID devices and sensors networks have very limited processing capabilities and memory. Hence, Lightweight cryptography like DES [2], PRESENT [12] etc. is principally motivated for those.

Lightweight block ciphers use different design architectures to ensure enough security in Resource limited devices while keeping execution cycles as minimum as possible.

Most of the ciphers are designed by using Feistel Architecture like SIMON [6], SIT [7], TEA [17], Blowfish [11], RC5 [20], etc. or by SPN (Substitution-Permutation Network) [16] like AES [3][4], PRESENT [12], KLAIN [9] etc. or by using both Architecture like DES [2], SIMON [6] to provide enough Shannon's confusion and diffusion properties in cipher text. On the other hand, Authors of some ciphers used ARX (Addition Rotation and XOR) architecture like SPECK [6]. Each of these architectures have some Special features like Invertible (Encryption and Decryption are almost same), Round function, Security and less energy consumption etc.

Entire security of the ciphers depends on secret keys that are used in every round in the block ciphers. For that reason key scheduling in the block ciphers is performed in a secure way. In SIT algorithm [7], Authors used SP Network and 4x4 matrices to generate secret round keys in order to keep safe cipher text from unauthorized access.

1.1 Motivation

Cryptography itself is a challenging and interesting subject to study and especially to research on. We cannot think of secure data communication without cryptography. In history people won wars using cryptography as a weapon. It involves mathematics, algorithm, programming, understanding in data communication, etc. With the widespread use of small low powered devices, lightweight cryptography will play a vital role in future. A survey by HP states that more than 70% of resource-constrained devices are vulnerable [5]. It is necessary to make a balance between the security and performance.

2. DIFFERENT ARCHITECTURES FOR BLOCK CIPHERS

Different structures [14] for various ciphers have been used to provide the efficient security for thousands of years.

2.1 Feistel Architecture

It is a symmetric structure to create sufficient confusion and diffusion of information for the purpose of preventing cipher text from the attacks. It was first designed by a cryptographer named Horst Feistel who did research while working for IBM [1]. The encryption and decryption method of this architecture are similar. Feistel Network [9] is a repetitive architecture. Each loop is called a round. Steps that cover a loop in Feistel Network are as below:

- Input is divided equally into two parts (Left part and Right part).
- Right part remains unchanged and also is transformed by the round function f which receives a sub-key.
- Left part is formed by combining with the transformed input from right part using XOR operation.
- Right part and Left part are switched to obtain input for next round
- Repeat again for next round.

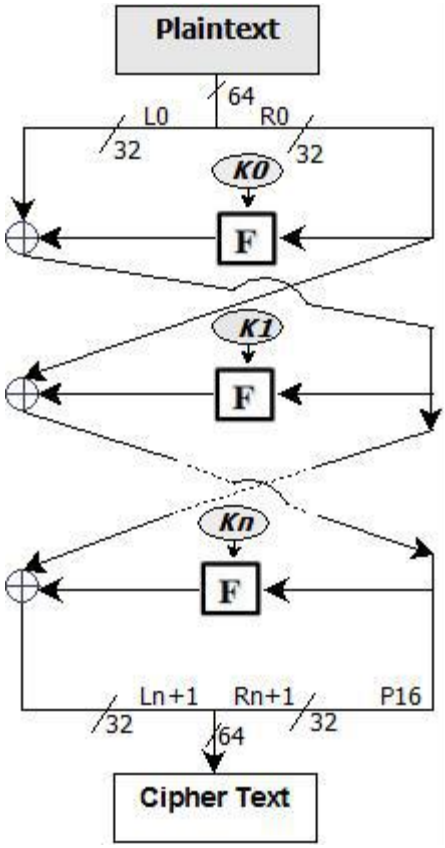

Fig. 1. Feistel Network

Feistel architecture is invertible [1] i.e., Encryption process and Decryption process are almost the same just reverse in order. This feature reduces the code size of block ciphers. Also, the F-function of this architecture is open for authors to design. It can be S-Box or P-Box or others which must be invertible also.

2.2 Substitution-Permutation Network (SPN)

SP network [1] stands for substitution and permutation network that are responsible for confusion and diffusion properties to secure the cipher text. In the SP network, substitution shows the non-linear transformation property and is called S boxes. Permutation provides the linear transformation and is called P boxes. In general, the SP network [1], [16] is used as a round function for a block cipher to achieve high security.

Let us consider an input data for S-Box is 110110. So, the corresponding output after transformed by the S-Box can be calculated as follows. The middle 4 bits of input data (110110) indicates the corresponding column of S-Box and Outer two bits (10) are for identifying the corresponding row of S-Box. Therefore, the input data corresponds to the column no of 1011 i.e., B and 10 i.e., 3rd row of S-Box. Hence, the output of S-Box is 9 i.e., 1001.

*	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	*F*	*E*	*D*	*C*	*B*	*A*	*9*	*8*	*7*	*6*	*5*	*4*	*3*	*2*	*1*	*0*
1	*3*	*F*	*C*	*0*	*9*	*E*	*A*	*D*	*B*	*4*	*6*	*8*	*2*	*7*	*5*	*1*
2	*7*	*8*	*A*	*B*	*0*	*1*	*F*	*3*	*E*	*C*	*4*	*9*	*6*	*5*	*D*	*2*
3	*2*	*D*	*9*	*6*	*5*	*4*	*C*	*E*	*3*	*F*	*1*	*0*	*B*	*A*	*8*	*7*

Fig. 2. Substitution Box.

On the other hand, P-Box just generates a different combination from the given input pattern of bits. For example, as in figure below (010000111000000) output for a binary input (1000011000010000) can be a different combination of given binary bits.

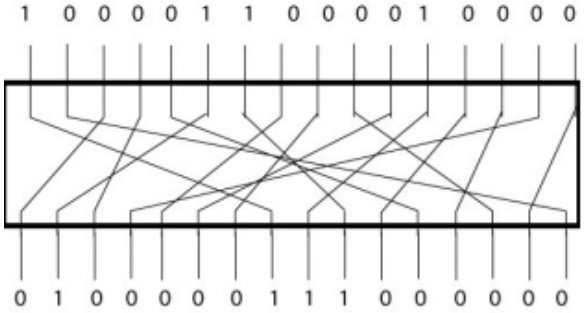

Fig. 3. Permutation Box.

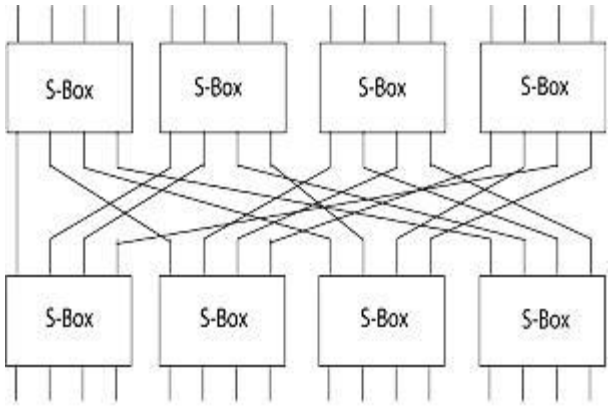

Fig. 4. Substitution-Permutation Network.

2.3 Hybrid Architecture

To avail the advantage of both SPN and Feistel architectures, some authors proposed the algorithms which are designed by using both architectures like DES (Data Encryption Standard) [2], Blowfish [11] and SIT (Secure Internet-Of-Things)[7] etc.

1. Popular lightweight block ciphers

This section illustrates the basic of some popular and recently proposed lightweight cryptographic algorithms.
Lucifer/ DES (Data Encryption Standard)
DES [2] is seemed to be the first cryptographic well-known symmetric-key block cipher which was developed at IBM in 1970 based on Feistel architecture.

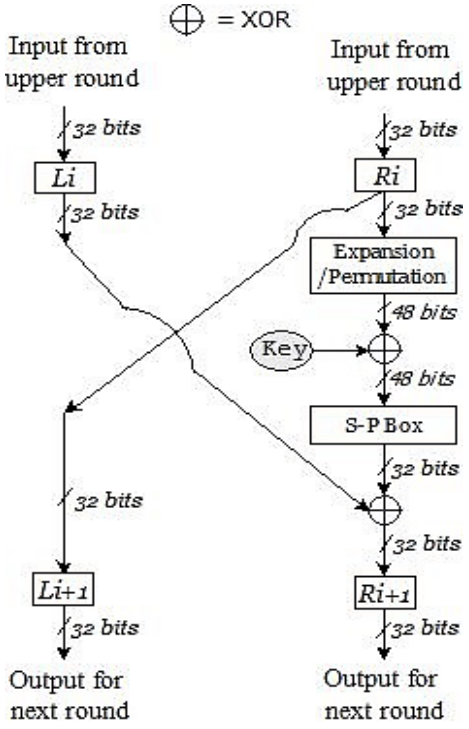

Fig. 5. One round of DES algorithm

Also, the F-function of DES algorithm consists of both S-Box(Substitution) and P-Box(Permutation). Authors of DES propose 64 bits block size, 56 bits of secret key size and 16 repeated rounds. Although Security of primary DES can easily be broken by Brute Force attack, some later version of DES like Triple-DES, G-DES and DES-X [9] etc. had become popular for providing sufficient security for small computing devices.

AES (Advanced Encryption Standard)

AES [3], [4] is now the most widely used symmetric cipher and most secure algorithm to date. DES was not secure anymore, therefore a replacement was needed, thus the advent of AES. As it uses a 128-bit key, it would take a billion years to crack a message.

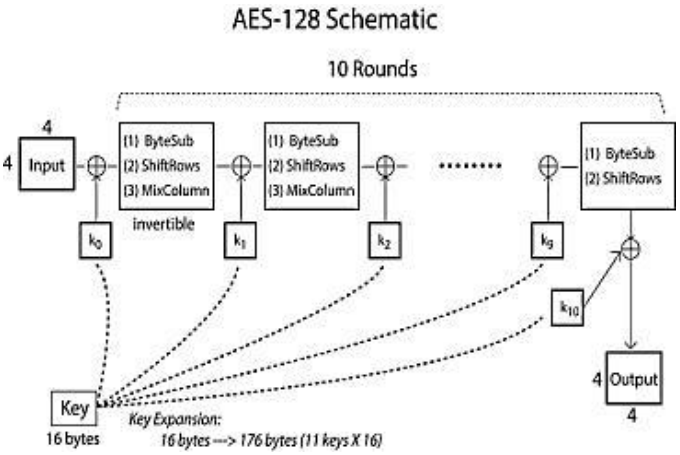

Fig. 6. AES for block size of 128 bits

It has the following attributes:

- 128-bit block size.
- 128, 192, or 256-bit key size. It has 9, 11 or 13 rounds depending on the size of the key.
- An iterative rather than a Feistel cipher.
- Treats data as 4 groups of 4 bytes.
- Each round consists of:
  - A byte substitution step (1 S-Box sued on every byte).
  - A shift rows step (shuffle the bytes between groups).
  - A mix columns step (matrix multiplication of groups with each other).
  - An add-round key step.
- All operations can be combined into XOR and table lookups - hence implementation can be very fast and efficient.

Although AES ensures enough security it hinders the performance of resource-limited devices.

Blowfish

It is a popular symmetric block cipher that was designed by Bruce Schneier in 1993. It divides the plaintext into fixed size blocks of 64 bits each. It supports the key variable size lengths that range from 32 bits to 448 bits. To implement each round of blowfish algorithm [11], S boxes and P boxes are used in F-function. P boxes are 32 bits in size and are 18 in total.

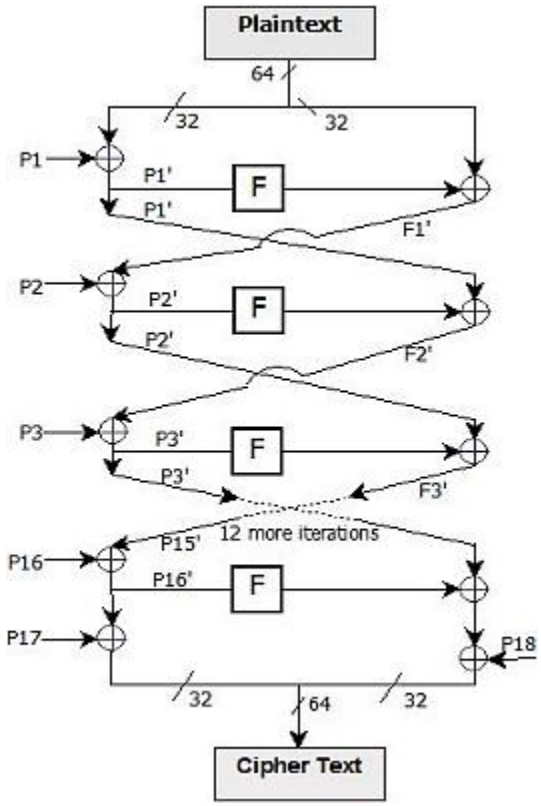

Fig. 7. Blowfish Algorithm

PRESENT

PRESENT [12] is a popular block cipher that was designed for resource-constrained environments. It takes variable key length that is either 80 bits or 128 bits. The plaintext is divided into fixed blocks of 64 bits sized. Standard SP (Substitution and Permutation) networks are used for implementing every round function. It consists of 32 rounds, each of which includes an XOR operation between key bits and plaintext, an SP network for performing linear and non-linear transformations. The key register is rotated to update the key schedule for the next round.

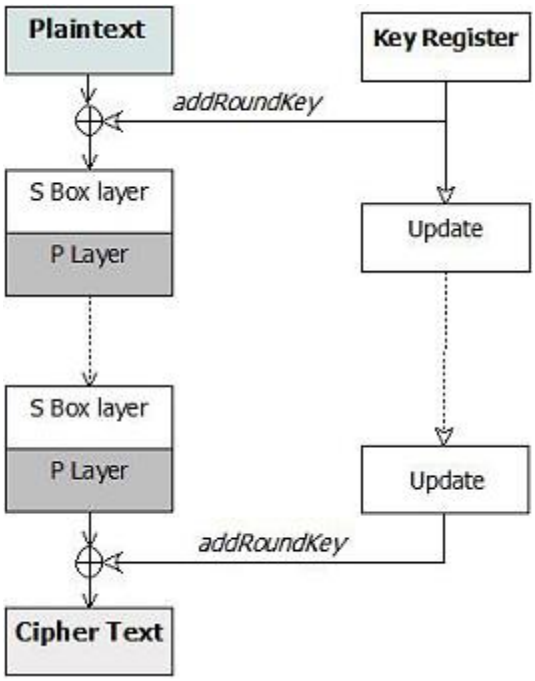

Fig. 8. PRESENT Algorithm

HIGHT

It is a popular symmetric key cryptographic algorithm that divides plaintext into fixed sized blocks of 64 bits each. It supports 128 bits key length. The encryption process of HIGHT [13] includes *Initial Transformation, Round function and Final Transformation.* The *Key Schedule* provides the functionality to generate Whitening keys (WK) and Sub-keys(SK). There are eight Whitening keys (WK_7--WK_0) for Initial and Final transformation. In total, 128 sub keys (SK_{127}- -SK_0) are used for round functions and four Sub keys per round.

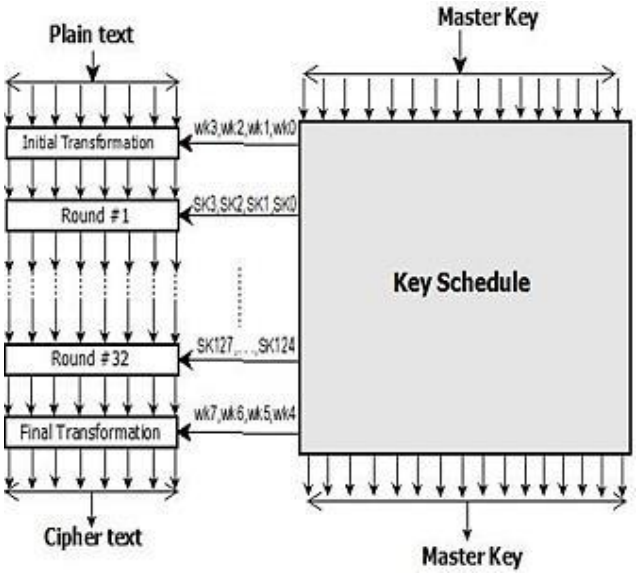

Fig. 9. HIGHT Algorithm

KLEIN

The typical Substitution-Permutation Network (SPN) is used to build KLEIN [9] structure. In KLEIN 80, the number of the round is 16. It generates a series of sub-keys from a master key. However, the complexity of the key generation must be adequate because the security depends on it. To save memory and increase performance, KLEIN generates sub-keys as transitions occur from one round to the next round.

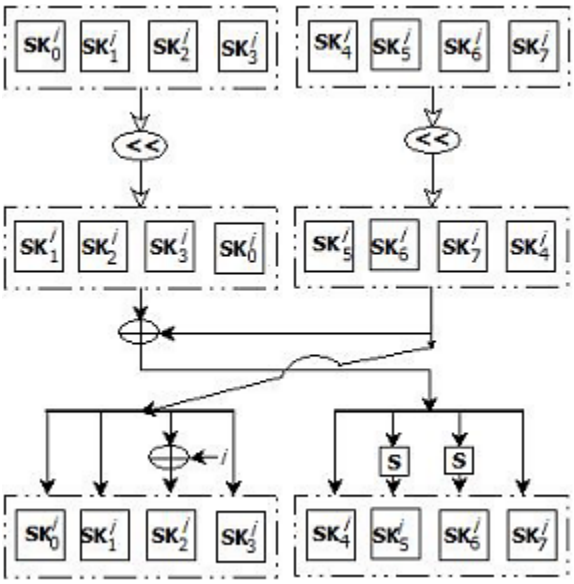

Fig. 10. KLEIN Algorithm

TEA

TEA [17] is a symmetric key cryptographic algorithm that was designed by Roger Needham and David Wheeler at the Computer Laboratory of Cambridge University. It supports 128 bits key length and 64 bits data block. It uses *Feistel Network* to implement the round functions but it uses Addition and Subtraction as reversible operators rather than XOR. Key scheduling uses the addition and the number Delta, derived from the golden number is used where $Delta = (\sqrt{5} - 1)2^{31}$. A multiple of the delta is used in each round so that no bit of the multiple will not change frequently.

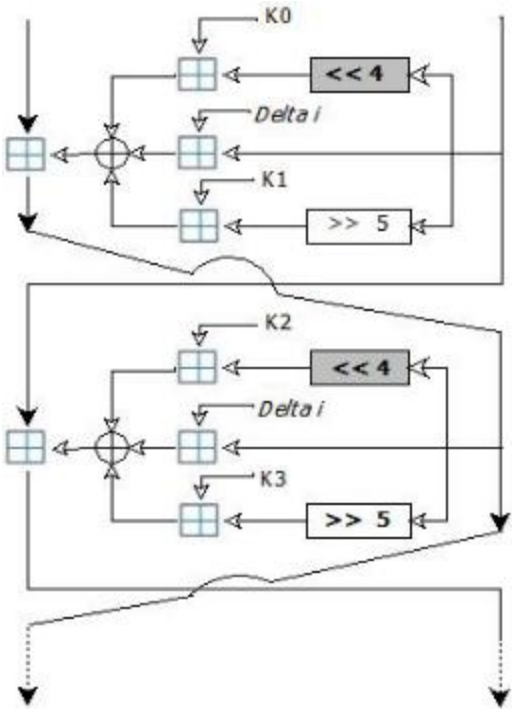

Fig. 11. Tiny Encryption Algorithm

KATAN

KATAN [15] uses 80 bits key for all types of its KATAN32, KATAN48, and KATAN64. This structure uses a counter to count the number of rounds. Also for the purpose of clocking, it uses the feedback polynomial $x_8 + x_7 + x_5 + x_3 + x_1$.

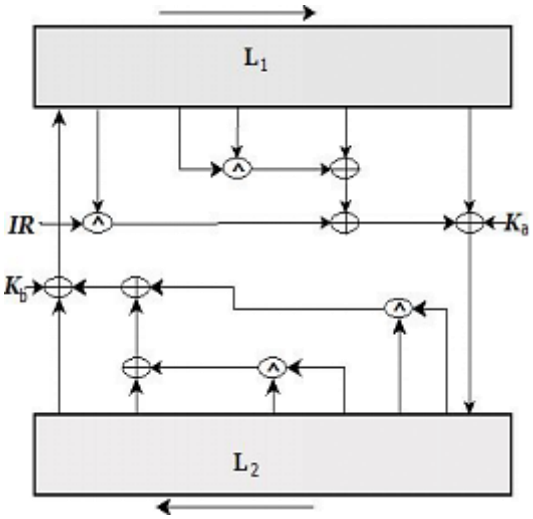

Fig. 12. KATAN Algorithm Structure

RC5

RC5 [20] is a popular block cipher with variable parameters of the block size of 32, 64, 128 bits, secret key size ranging from 0 to 2048 bits and number of rounds(1 to 255). Authors of RC5 used Feistel like network with some arithmetic and logic operators like XOR, Rotate and Addition. Although up to 12 rounds of RC5 for a block size of 64 bits is vulnerable to a *differential attack*. The successor of RC5 like RC6 [20], Akelarre is secure enough.

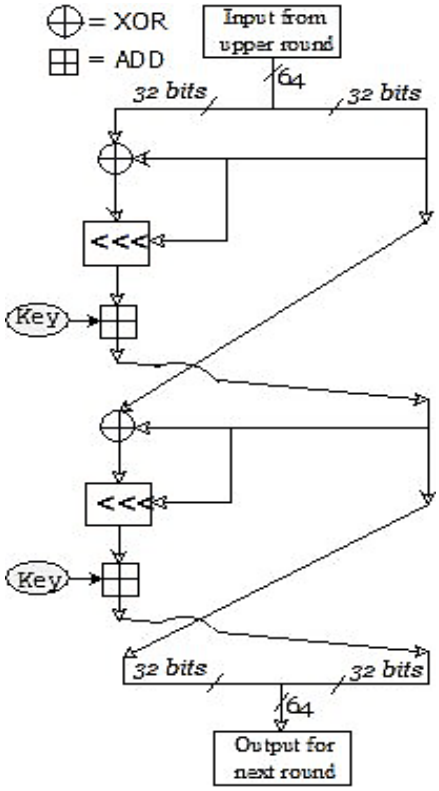

Fig. 13. One round of RC5 for 64 bits of block size

SIMON

Simon [6] is a recently released block cipher which was published by the NSA (National Security Agency) in June 2013.

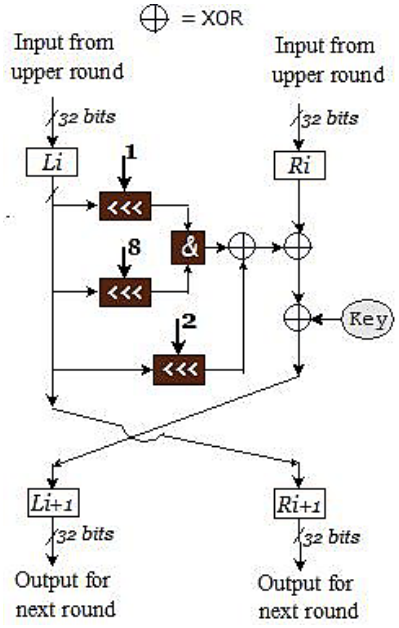

Fig. 14. One round of Simon for 64 bits of block size

Authors proposed the cipher with variable parameters of the block size of 32, 48, 64, 96 or 128 bits, the secret key size of 64, 72, 96, 128,144,192 or 256 bits and number of rounds (32 to 72). They used a balanced Feistel Architecture. Each of the repeated rounds of the cipher consists of some bit-wise and logic operators like XOR, Rotate, etc. Although the security of the cipher up to 46 rounds for the block size of 128 bits can be broken by *differential attack*, It is optimally efficient for the performance in hardware implementations.

SPECK

The authors of *Speck* proposed varieties size of the data block (multiple of 8 bits), key size and number of rounds same as like *Simon* cipher. It was also published by the NSA (National Security Agency) in June 2013. The cipher is designed with ARX (Addition, Rotation, and XOR) architecture. It is optimized for the performance in software implementations.

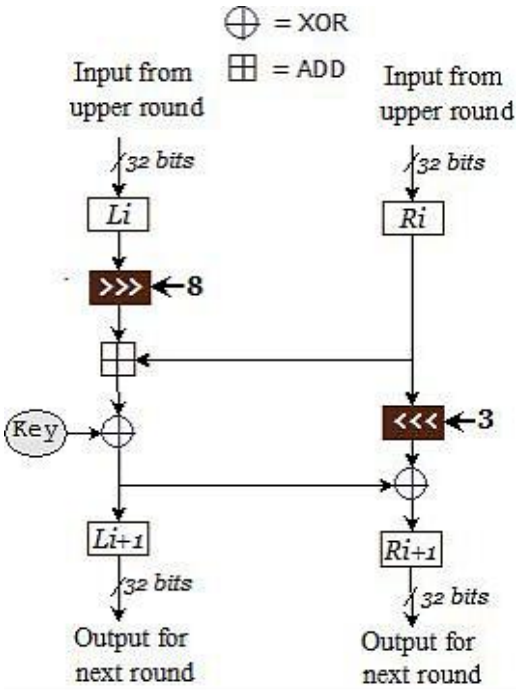

Fig. 15. One round of Speck cipher for 64 bits of block size

SIT (Secure Internet Of Things)

In 2017, the authors of SIT [3] proposed a symmetric key block cipher that uses 64-bit key over 64-bit data. Block ciphers such as AES uses a substitution-permutation (SP) network in order to integrate Shannon's confusion and diffusion properties. Other ciphers such as Blowfish and DES use Feistel architecture using the advantage of having almost the same encryption and decryption operation. Their proposal is a combination of both Feistel and SP networks using properties of the both to provide substantial security but keeping the computation complexities as minimum as possible. The algorithm has two parts: key expansion and encryption. A 64-bit key is taken as input by the user, divided into 4 blocks, supplied into F-functions, arranged in 4X4 matrices and new five unique keys are generated using some linear and non-linear transformations. The encryption process consists of logical operations, shifting, and substitutions. Although other cipher uses 10 to 20 rounds, it uses the Feistel network of 5 rounds that use the five unique generated keys but provides enough confusion and diffusion.

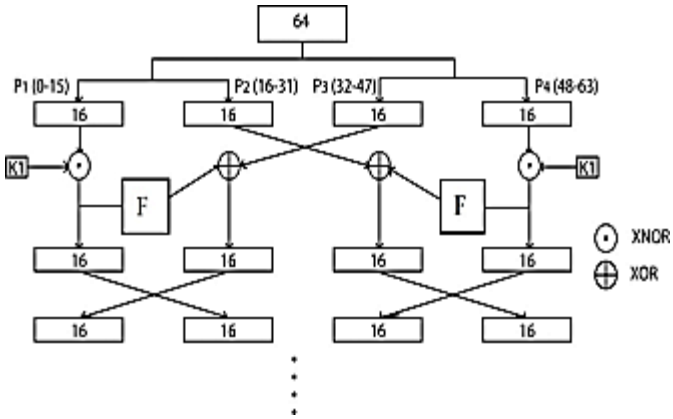

Fig. 16. One round of SIT for 64 bits of block size

3. PERFORMANCE ANALYSIS

In order to measure execution cycles and memory usage a benchmark tool called FELICS (Fair Evaluation of Lightweight Cryptographic Systems) [10] is used. It can evaluate performance on different platforms (such as AVR, MSP, ARM, and PC) and various performance matrices. It can measure execution cycles, RAM footprint, and binary code size on a specific platform. The tool is available to be downloaded. It runs on Linux Ubuntu. A virtual machine file incorporates both Linux Ubuntu and FELICS that saves us from installing all prerequisites. We use the virtual machine file and works excellently.

In this section, Five performance metrics [8] i.e., Size of RAM to execute ciphers, the Code size of ciphers, Cycles to generate rounds keys, Cycles for encryption and decryption are considered to evaluate the performance of different block ciphers.

Ciphers	Block Size in bits	Key Size in bits	Code Size in Byte	RAM Size in Byte	Cycles in Key Generation	Cycles in Encryption	Cycles in Decryption
AES	128	128	9350	388	3274	5423	5388
DES	64	56	1709	468	2166	3617	3592
HIGHT	64	128	13476	288	1412	3376	3401
PRESENT	64	80	1738	274	2570	7447	7422
KATAN	64	80	638	215	4627	14126	11239
KLEIN	64	64	1979	401	2560	6195	7659
TEA	64	128	855	196	2365	7400	7501
RC5	64	128	16044	360	11793	4616	4652
Simon	64	96	1370	188	2991	1980	1925
Speck	64	96	2552	124	1509	1179	1411
SIT	64	64	826	96	2130	876	851

Table 1: Data table for the comparison of different Lightweight Algorithms on AVR architecture

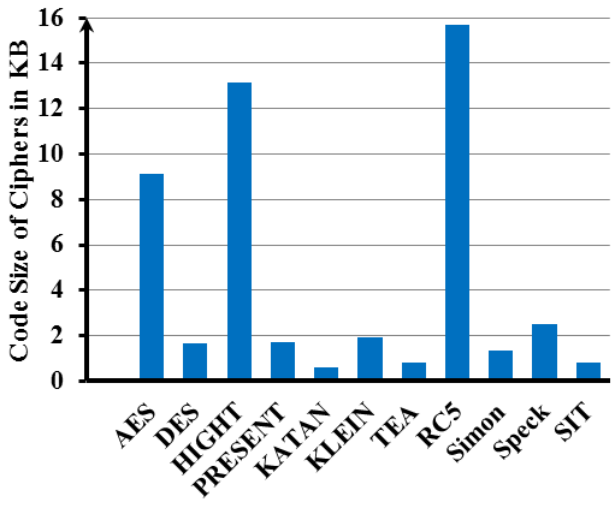

Fig. 4.1. Comparison on Code Size of different Ciphers

The code size of ciphers affects the performance on the light-weight device. Now-a-days, most of the height-weight devices like embedded devices, microcontroller chips, RFID tags, etc. have enough ROM in range of MB to store cryptographic algorithm. Above figure shows the maximum code size of cipher like RC5 is 15KB. On the other-hand, ciphers like KATAN, TEA, and SIT have less code size as shown in the above figure.

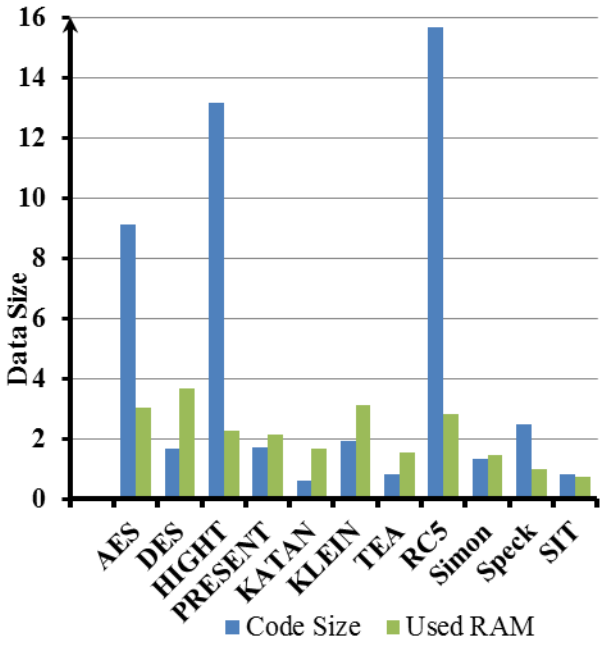

Fig. 4.2. Comparison between RAM and program data size used by different Ciphers

On the other-hand, used RAM size of the ciphers is very important for performance of a light-weight device because RAM of those devices is very limited. So the ciphers which used minimum RAM while executing is the efficient one. Like SIT, Simon, KATAN and TEA. Another case is that some of the ciphers have little code size while these ciphers waste too much physical memory to perform encryption and decryption. Because these ciphers have higher number of round. Typically, the round of a light-weight cipher should be in between 5 to 20. In above graph, DES has little code size while it requires Maximum RAM. On the other-hand, AES needs less RAM while its code size is too high. Since Energy consumption is directly related to size of used RAM while executing instructions. So, AES is better than DES due to using less physical memory. There is an issue that security strength of a cipher depends on complexity of computations. In general, higher rounds ensure high security. But there is a trade-of between security and complexity. In light-weight devices, ciphers of heavy computation hinder the performance for the sake of limitation of resources. So, it is not feasible to implement the heavy ciphers on light-weight devices. On the other-hand, ciphers of light-weight computation are easy to break.

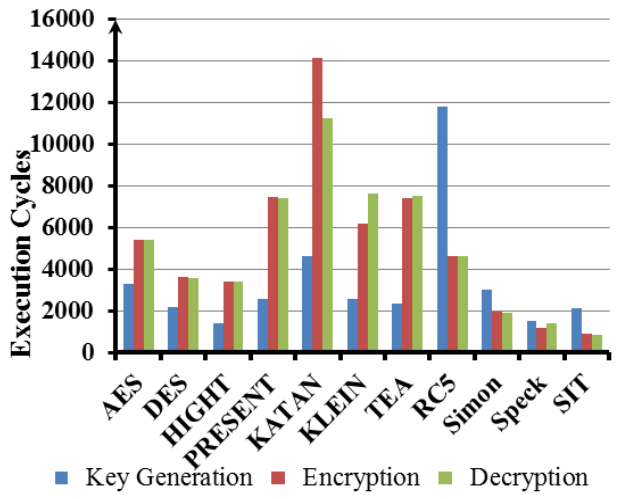

Fig. 4.3. Comparison of execution cycles for Key generation, Encryption and Decryption among different block ciphers

The above figure demonstrates that Execution cycles require for key generation, encryption and decryption. The execution cycle of ciphers is directly related to Energy consumption. Since the resource-limited devices are low powered battery operated. Hence, Energy consumption should be as less as possible while the strength of security for ciphers should be up to the security level. In short, there is a trade-off between light-weightiness and security. The entire security of a cipher directly depends on keys are used to encrypt and decrypt each block of message. So, generation of keys should be enough complex. Once keys are generated then these keys can be used for all blocks of data as well as all round of cipher. Hence, Complex computation of key generation doesn't effect on the performance of devices like Encryption and Decryption phases of ciphers. In the above chart, SIT has enough secured key distribution technique to ensure the security of keys. For that reason, SIT requires more cycles than that of HIGHT, Speck, etc. For KLEIN, PRESENT, and AES has less key scheduling cycles than Encryption and decryption cycles. On the other hand, KATAN has low execution for key scheduling cycles but Encryption and decryption are high. So, on average Simon, Speck, SIT, DES are more energy efficient.

Scope of research on block ciphers:

- Most of the block ciphers developed up to the day ensures security based on the complexity of number theory or different logic operation. The neural network [18] is a good choice for designing a security cipher.
- Architecture used in block ciphers is either SP Network (e.g., AES, PRESENT) or Feistel Architecture like DES, Simon, etc. or both (Blowfish, SIT, etc.). Some features of GAs(Genetic Algorithms) like Crossover operators and Mutation [19] are the good option to design the architecture of block ciphers.
- Entire Security of the ciphers depends on keys. So key scheduling should be designed not only based on number theory rather than it can be designed by applying advanced theories like Gas [19], neural network [18], etc.

4. CONCLUSION AND FUTURE WORK

In the era of internet, the light-weight cryptographic algorithm has become essential to ensure security for resource-constrained devices like wireless Network sensors, RFID tags, and embedded device, etc. The collected data table for performance evaluation is tested on AVR architecture by FELICS (A Benchmark to evaluate block ciphers on different metrics). In the near future, these ciphers will be tested on more architectures on more performance metrics. Besides the performance of ciphers, the strength of security should be up to the mark. So for further improvement and analysis, these ciphers will be tested on different security aspects like Entropy, Co-relation, etc.

REFERENCES

[1] Kerry A. McKay, Larry Bassham, Meltem Sönmez Turan, Nicky Mouha. "Report on Lightweight Cryptography", National Institute of Standards and Technology (NIST), USA, March 2017.

[2] Harshali D. Zodpe ; Prakash W. Wani ; Rakesh R. Mehta."Design and Implementation of Algorithm for DES Cryptanalysis". 2012 12th International Conference of IEEE on Hybrid Intelligent Systems (HIS), DOI: 10.1109/HIS.2012.6421347 , Pune, India, January 2013.

[3] National Institute of Standards and Technology (NIST), "The Advance Encryption Standard (AES)", Federal Information Processing Standard Publication 197, November 26, 2001.

[4] S. Mangard, M. Aigner, and S. Dominikus, "A highly regular and scalable AES hardware architecture" IEEE Transactions on Computers,52(4):483–491, April 2003.

[5] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in Internet of Things: Challenges, solutions and future directions", in 2016 49th Hawaii International Conference on System Sciences (HICSS), IEEE, 2016, pp.5772-5781.

[6] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L. "The SIMON and SPECK families of lightweight block ciphers". in Cryptology ePrint Archive, Report 2013/404.

[7] Muhammad Usman, Irfan Ahmed, M. Imran Aslam, Shujaat Khan and Usman Ali Shah. "SIT: A

Lightweight Encryption Algorithm for Secure Internet of Things" Iqra University, Defence View and Department of Electronic Engineering. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, 2017.

[8] MOJTABA ALIZADEH, * MAZLEENA SALLEH, MAZDAK ZAMANI, + JAFAR SHAYAN, + SASAN KARAMIZADEH."Security and Performance Evaluation of Lightweight Cryptographic Algorithms in RFID", Faculty of Computer and Information Systems, + Advanced Informatics School Universiti Teknologi Malaysia.

[9] William Stallings . "Cryptography and Network Security Principles and Practices", Fourth Edition, Publisher: Prentice Hall, November 16, 2005

[10] https://www.cryptolux.org/index.php/FELICS

[11] Ms NehaKhatri – Valmik, Prof. V. K Kshirsagar." Blowfish Algorithm" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 80-83, India, 2008.

[12] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y.Seurin, and C. Vikkelsoe."PRESENT: An Ultra-Lightweight Block Cipher," Horst-G¨ortz-Institute for IT-Security, Ruhr-University Bochum, Germany

[13] Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee. "HIGHT: A New Block Cipher Suitable for Low-Resource Device." Center for Information Security Technologies (CIST), Korea University, Seoul, Korea

[14] Morris Dworkin" Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality", NIST Special Publication 800-38C, USA, May 2004

[15] Vikash Kumar Jha," Cryptanalysis of Lightweight Block Ciphers" Aalto University School of Science Degree Programme of Computer Science and Engineering, Master's Thesis, November 18, 2011

[16] Hristina Mihajloska, Danilo Gligoroski." A NEW APPROACH INTO CONSTRUCTING S-BOXES FOR LIGHTWEIGHT BLOCK CIPHERS," 8th Conference on Informatics and Information Technology with International Participation (CIIT 2011)

[17] Hernández, Julio César; Sierra, José María; Isasi, Pedro; Ribargorda, Arturo. "Finding efficient distinguishers for cryptographic mappings, with an application to the block cipher TEA". Proceedings of the 2003 Congress on Evolutionary Computation. 3. pp. 2189–2193. doi:10.1109/CEC.2003.1299943. ISBN 978-0-7803-7804-9.

[18] Prof. P.S Revankar, D.T.Rathod. "Cryptography Using Neural network".Conference: International Conference on Sensor and Related Networks, At VIT University, Vellore, India, December 2009

[19] S. Dutta, T. Das, S. Jash, D. Patra, Dr. P. Paul, "A Cryptography Algorithm Using the Operations of Genetic Algorithm & Pseudo Random Sequence Generating Functions", International Journal of Advances in Computer Science and Technology, ISSN 2320 – 2602, Volume 3, No.5, May 2014

[20] Asma Belhaj Mohamed ; Ghada Zaibi ; Abdennaceur Kachouri ."Implementation of RC5 and RC6 block ciphers on digital images". 8th International Multi-Conference of IEEE on Systems, Signals & Devices , DOI: 10.1109/SSD.2011.5767447, 22-25 March 2011 in Sousse, Tunisia.