KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express xxx (xxxx) xxx

www.elsevier.com/locate/icte

An Enhanced Energy Efficient Lightweight Cryptography Method for various IoT devices

Prakasam P.[a,*], Madheswaran M.[b], Sujith K.P.[c], Md Shohel Sayeed[d]

[a] *School of Electronics Engineering, Vellore Institute of Technology, Vellore, India*
[b] *Muthayammal Engineering College, Rasipuram, India*
[c] *School of Electronics Engineering, Vellore Institute of Technology, Chennai, India*
[d] *Multimedia University, Melaka, Malaysia*

Received 8 April 2020; received in revised form 15 January 2021; accepted 14 March 2021
Available online xxxx

Abstract

Internet of Things (IoT) is an auspicious technology that will connect more number of devices through an internet. The huge number of communication expected to transmit high data securely is an important problem in recent days. In this paper, an **E**nhanced **E**nergy **E**fficient **L**ightweight **C**ryptography **M**ethod which utilizes 8 bit manipulation principle (**E^{3}LCM**) has been proposed. The proposed method has been verified for speech signal using MATLAB. The hardware complexity has been validated using Sparten3E XC3S500E FPGA devices and it has been found that the proposed method consumes 202mW power and 0.9 Kbytes RAM and it outperforms other methods.

Keywords: Cryptography; Lightweight; Power consumption; Memory; Histogram; Correlation

1. Introduction

Due to the technology era in wireless communication industry, more number of different in nature next generation devices such as android mobile phones, laptops, tablets, PCs, android TVs, Video Games, smart watches, smart homes, smart biomedical equipments, air conditioners, smart cameras, smart refrigerators etc., can be connected through single network. Also, each devices may have an ability to interact with other through internet is illustrated as shown in Fig. 1. Hence, the Internet of Things (IoT) is became a popular during recent past and also an emerging area for doing research and developments [1,2]. IoT is a typical network which contains normal units with an intelligence to sense and interact with associated devices through an Internet. Due to the deployment of the broadband internet with high speed and low cost, many electronics devices and sensors are accessing and sending information through internet. Hence, this technology advancement provides the suitable policy to expand IoT further in future as Internet-of-Everything (IoE).

Since, every object can exchange the information from anywhere in the world to other devices through internet, the complexity are also increased considerably for IoT. An enlightened embedded sensors and chips within next generation devices can sense the valuable data and transmits thorough the internet. Hence, this sharing of huge valuable data through IoT platform must be transmitted more securely to another device. But normally, the IoT is using a traditional sensor, mobile and internetwork to transmit the data to other devices. Hence more recent research has been concentrated in security issues rather than reducing the complexity [3–5].

1.1. Security issues in IoT

The major safety related issues of IoT systems as compared with conventional systems is that any misuse devices for information assortment in real world will be converted as the target of cyberattacks. Let us consider a mechanical plant for which the IoT can be used improve the production in a significant manner and also for easy maintenance by

* Corresponding author.
E-mail addresses: prakasamp@gmail.com (Prakasam P.), madheswaran.dr@gmail.com (Madheswaran M.), sujith.kp2019@vitstudent.ac.in (Sujith K.P.), shohel.sayeed@mmu.edu.my (M.S. Sayeed).

Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2021.03.007

Please cite this article as: Prakasam P., Madheswaran M., Sujith K.P. et al., An Enhanced Energy Efficient Lightweight Cryptography Method for various IoT devices, ICT Express (2021), https://doi.org/10.1016/j.icte.2021.03.007.

Fig. 1. Internet of Things (IoT).

coordinating and collecting the information from the huge number of sensors deployed in the plant automatically in real time. Due to cyberattacks, if incorrect information has been received in the server leads to improper analysis which will induce the improper management and finally it leads to the major damage in a huge mechanical plant.

The measurement data as well as control data are more confidential associated with management and production process, avoiding leakages are also a vital aim in the view of competitiveness. Therefore it is more important to consider the effect of security threats while deploying on any IoT based systems.

The three major reasons for easy attack of IoT by cyber attackers are as follows. The first reason is that IoT is not having a supervisory mechanism or intelligent to identify the attackers. Secondly, since IoT uses wireless medium, the snooping is very simple. Last, the elements of IoT accept low ability in terms of energy consumption and also with low computational capability. Therefore, the designing and deployment of conventional computationally expensive security algorithms will result in the intrusion on the performance of the energy controlled devices. Hence Cryptographic algorithms play an important role in secure to provide secure situation in order to transmit the information without any information leakage for IoT. The data transferred through the internet are exposed to the risks of unauthorized access that may tamper with the control signals or issue illegal commands that would lead to abnormal operations.

1.2. Lightweight cryptography

The symmetric cryptography method is essential to achieve an end to end security in IoT systems. Also for the low powered devices, the cryptographic process with a restricted amount of energy consumption is very important [2]. The application of light-weight is bilateral key rule permits lower energy consumption for end devices. A lightweight cryptography algorithmic rule achieves improvement of any of the parameters for e.g. Memory size, Latency, Energy and circuit size. Applying encoding to detector devices suggests that the deployment of knowledge guard for privacy and reliability, may be an efficient measure in contradiction of the threats. Lightweight cryptography as shown in Fig. 2 has the utility of enabling the appliance of secure encoding, even for nodes with restricted resources. Encryption is exists previously applied as normal on the information link layer of communication schemes like the radiophone. In that case also an encryption is an effective process which is providing end to end information security between the devices and the server to ensure security independently. The factors that are to be considered while deploying the light-weight cryptography are energy, power consumption, size, delay and processing speed. The energy is particularly necessary with the RFID and energy harvest devices whereas the ability of consumption is vital with battery powered nodes. A high outturn is important for devices with massive knowledge transmissions like a smart camera or a vibration detector, whereas a high processing speed is vital for the time period monitoring process of a car-control system, etc. Since the ability is greatly gripped with the hardware size or the processor in use and energy consumption, the size and energy becomes the important factor for lightweight encryption technique. The energy and power consumption is reliant on the delay and the processing speed, hence computations count which determines the processing speed will also to be considered as an important index of lightweight encryption. The outturn depends significantly on the multiprocessing ability.

2. Literature review

Kitsos et al. [3] planned a hardware-based performance comparison of light-weight block ciphers. It surveys concerning the ciphers that area unit appropriate for frequency Identification security applications. It is also suitable for other security applications with restrictions in area. Chenhui Jin et al. [4] proposed a new lightweight stream cipher family well-known as Welch–Gong considered 80 bit for both secret key and for initial vector also. There exist Key-IV pairs to generate keystreams. The keystreams are propagated to generate key for the next round. Swarnendu Jana et al. [5] planned a light-weight even cipher. It is evaluated based on hardware and software implementations. Traditional encryption methods are not suitable for wireless sensor networks due to the limitations on memory, power and energy. Wenling Wu and Lei Zhang [6] developed a brand new cipher known as L Block for light-weight applications. It uses a 64 bits and 80 bits for block and key sizes respectively. Evaluation of security shows that LBlock can do security margins against attacks.

Christophe De Canniere et al. [7] developed the cipher which utilizes 32, 48 and 64 bit block size and share 80 bit key. In KATAN cipher, the key is burnt into the device. The copy of plaintext is loaded into register. Julia Borghoff et al. [8] designed the cipher PRINCE which uses 64 and 128 bits for block size and key respectively. The cipher unfolds the key throughout the plaintext and prevents cryptologic attacks.

Deukjo Hong et al. [9] developed the cipher which also uses 64 and 128 bits for block size and key respectively. The basic structure is a Feistel Network. Simple XOR and shift operations are used in the functions F0 and F1. Ray Beaulieu et al. [10] proposed the ciphers with different block size and key size. This cipher has been designed to improve the hardware and software system structure on the processors. This cipher uses modulo addition, XOR operation, left circular shift and right circular shift. The survey on light weight cryptography was discussed by Kong Jia Hao et al. [10].

Gauravm Bansod [11] explained PRESENT-GRP hybrid method. The block of input data has been distributed through the S-box of PRESENT and the output data has been passed to the permutation layer after mapping and encrypting using PRESENT GRP algorithm. S-box of PRESENT GRP has been designed with 4×4 box in order to reduce the complexity and the energy consumption. For the 64 bit operation, the design has been carried such that it used only 16 four bit S-boxes of PRESENT and the output of PRSENT is passed to GRP for permutation. The hybrid structure of PRESENT-GRP has terribly less memory demand as compared to the existing algorithms. P-box of GRP uses seven stages so as to cut back gate equivalent. The bits are grouped such as first group contains 0th bit and 64th bit, second group will be 1st bit and 65th bit and so on. Light weight implementation of block ciphers in hardware and software was discussed by George Hatzivasilis et al. [12].

Jaber Hossein Zadeh and Abbas Ghaemi Bafghi [13] surveyed the various lightweight encryption ciphers in terms of their speed, performance and cost. It analyzed the ciphers which is suitable for hardware implementation. Saurabh singh et al. [14] discussed a advanced lightweight encryption ciphers, stream ciphers, high performance nodes for IoT applications. Secure IoT (SIT) light weight block cipher was proposed by Muhammad Usman et al. [15]. Architecture uses a combined structure of feistel network and a normal permutation substitution network. Based on the above literature review it has been observed that enhanced security lightweight cryptography method is essential to transmit the data in a secure way for various IoT devices.

3. Proposed enhanced energy efficient lightweight cryptography method

The block diagram of the proposed Enhanced Energy Efficient Lightweight Cryptography method (E^3LCM) is shown in Fig. 2. The immunity of symmetric key block ciphers extensively depends on the cryptographic potent of the S-boxes (Substitution boxes). To reduce the area, the design of S-Box is marginally altered and constructed using Multi-sequence Linear Feedback Shift Register (MLFSR). The main prevalence of using MLFSR is that the design occupies much less area with optimal speed and power consumption. MLFSR uses registers, simple XOR operation and a shifting operation to generate a sequence of cyclic binary states. MLFSR updates the current state through direct computation.

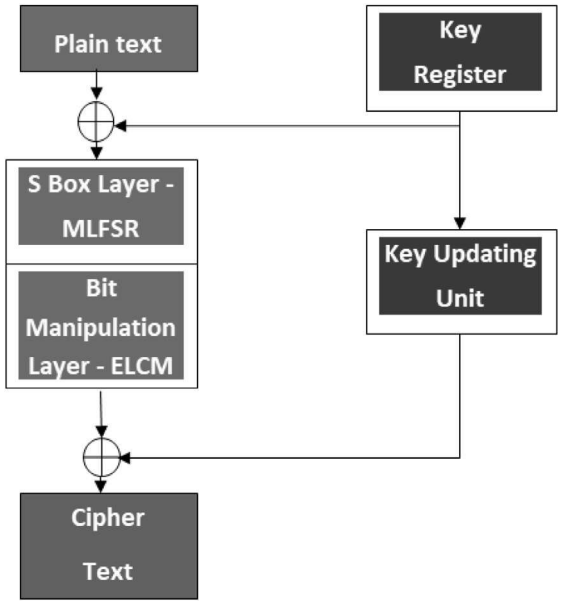

Fig. 2. Block diagram of proposed E^3LCM method.

In order to implement the proposed encryption method in a better way, a new 8 bit manipulation method (E^3LCM) is proposed and shown in Fig. 3. E^3LCM takes 2 inputs, one as "data bits" and other as "control bits" and gives only single output. The control words square measure generated by control bit generation unit in E^3LCM. Based on the control bits the input data is swapped. Grouping between bits is finished in keeping with E^3LCM algorithmic rule. The groups are (A_7, A_3), (A_6, A_2), (A_5, A_1) and (A_4, A_0). For swapping, the corresponding control bits are checked. The basic operation of E^3LCM which takes input as 8 bits of data and respective 8 bits of control words. This algorithm is implemented through combination of 2 input multiplexers. Mux0 and Mux1 generated output is depending on the control bit. Input sequence is fed to the series of multiplexers.

Based on the control words generated by SGRP, the structure can swap the info. Two set of multiplexers are available, 4 multiplexers denoted by Mux0 and another 4 multiplexers denoted by Mux1. For example, every group of bits are applied to Mux0 and Mux1. For example in the first group (A_7, A_3), if the corresponding control bits are 0 and 1, it is not swapped. For the other group (A_6, A_2), corresponding control bits are 0 and 1, it is swapped. The E^3LCM implementation is shown in Fig. 4. The encrypted data is shown at the output of third stage. Three stages square measure ruled by 3 totally different control words generated from E^3LCM formula for specific bit positions. If arrangements of knowledge bits position is modified the formula will generate 3 totally different control words. It is also used for key generation. Control words that square measure generated from E^3LCM is used as totally different keys for doing science method of changing plain text to cipher text. It offers a minimum delay once enforced as a hardware structure. For decryption, encrypted data is given as input to decrypted module and control words are applied in

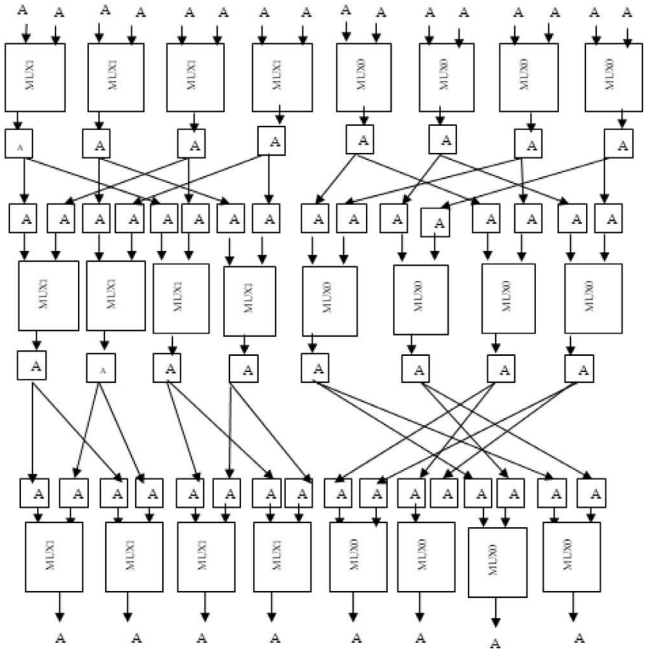

Fig. 3. Implementation of E^{3}LCM operation for 8 bit.

reverse order to get the desired output. The original data is received in order after completion of the process.

4. Results and discussion

The proposed E^{3}LCM method has been simulated and tested using MATLAB v2019. In order to evaluate various the performance metrics like power consumption, latency, memory required etc,. the encryption and decryption operations of the proposed E^{3}LCM method are implemented in Spartan3E XC3S500E FPGA. Using this Sparten3E FPGA tool, the performance of the various existing common lightweight cryptographic techniques like AES, DES, PRESENT, CLEFIA, KATAN and SIT have been implemented and compared with the proposed E^{3}LCM method. The VHDL has been used for the design of the proposed E^{3}LCM method and it is synthesized and simulated using XILINX ISE 14.7 and ModelSim respectively. The various cryptography algorithms has been implemented using Spartan3E FPGA processor and the various parameters obtained has been tabulated in Table 1.

From Table 1, it has been found that the proposed E^{3}LCM method outperforms with less power consumption, less memory occupation and low end-to-end delay. The encryption and decryption performance of the proposed E^{3}LCM method has been verified and validated for speech signal as shown in Fig. 4 using MATLAB. The key size has been selected as 64, the original speech signal is encrypted and again decrypted using the proposed E^{3}LCM method. The decrypted speech signal is shown in Fig. 5.

The performance of the proposed E^{3}LCM method has been verified and validated using correlation and histogram parameters. The Correlation is an efficient toll which is used

Table 1
Comparison of hardware implementation.

Methods	Key size	Memory		Delay (ns)	Power (mW)
		Flash memory (kB)	RAM (kB)		
AES	128	3.7	2	11.98	290
DES	128	10	4.6	21.10	267
CLEFIA	128	4.5	1.4	11.56	251
PRESENT	128	2.9	1.3	10.34	240
KATAN	80	2.8	1.3	8.5	234
SIT	64	2.7	1.1	7.6	221
E^{3}LCM	**64**	**2.4**	**0.9**	**5.4**	**202**

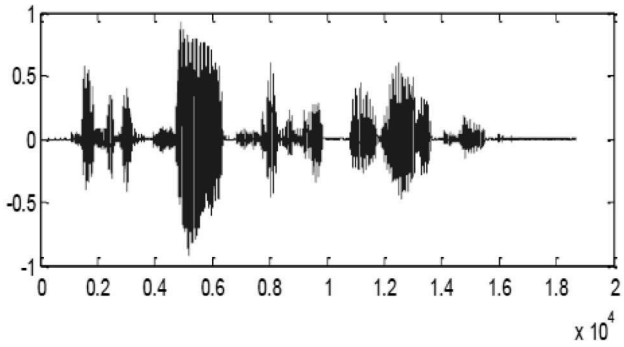

Fig. 4. Original speech signal.

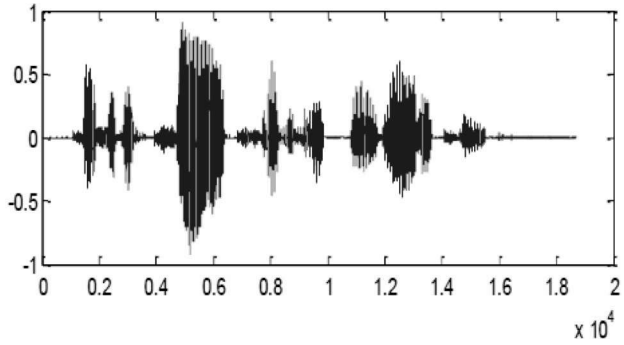

Fig. 5. Decrypted speech signal using E^{3}LCM method.

to measure the degree of a cryptography method. The correlation quantifies the amount of dependency between two signals/texts. For an ideal cipher, the cipher text of plaintext should not have any dependency on its original data. The correlation has been computed using MATLAB for both encrypted data and the original data in order to measure the similarity.

The obtained graph is illustrated in Fig. 6. The original data in this proposed work is the original speech image. The image shown in Fig. 6(a) is heavily correlated and keeping a high value for the correlation coefficient. It has been observed from Fig. 6(b) that the correlation coefficient of encrypted signal is almost zero and it is not having any correlation.

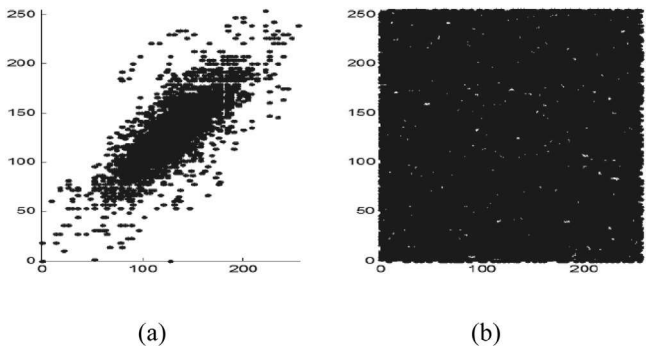

Fig. 6. Correlation of original speech signal (a) and the encrypted signal (b).

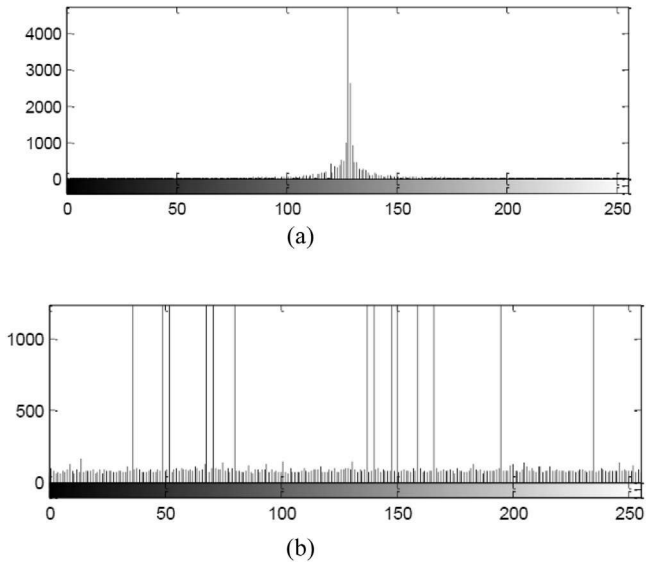

Fig. 7. Histogram representation of original speech signal (a) and encrypted signal (b).

The desired security of the encrypted signal has been validated by computing the histogram for the original signal and the encrypted signal which is also used as tool to measure the quality. A histogram can measure the arbitrariness while encrypting an image. The cryptography methods refer to enough secure if the computed histogram is uniform after encryption The simulated histogram using MATLAB for the proposed E^{3}LCM method is shown in Fig. 7.

In Fig. 7, x axis refers the intensity value and y axis represents the number of pixels occurred in the particular intensity value. It has been observed from Fig. 7(a) and (b) that after the encryption process, the histogram plot has a uniform distribution which ensures the desired security.

5. Conclusion

In this paper, an enhanced energy efficient lightweight cryptography method which is utilizing 8 bit manipulation (E^{3}LCM) has been proposed. The proposed method has been simulated and tested for speech signal. Also it has been verified and validated with existing cryptography methods. From the validation, it has been found that proposed E^{3}LCM method consumes 10.39% less power and 18.18% less memory as compared with other reported methods. The comparisons and results show that the proposed system has an optimum area and power performance along with lesser delay. Due to the low weight and high security nature, the proposed E^{3}LCM cyber text method can be integrated in real time high secured applications like electronic money transfer, authentication scheme, time stamping, encryption in WhatsApp, histogram etc. In the near future, the proposed method can be verified, validated and tested for different real time applications for further enhancing its performance metrics.

CRediT authorship contribution statement

Prakasam P.: Conceptualization, Methodology, Formal analysis, Draft paper writing. **Madheswaran M.:** Investigation, Data curation, Supervision. **Sujith K.P.:** Conceptualization, Software, Validation, Formal analysis. **Md Shohel Sayeed:** Re-writing, Editing, Project administration.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] T. Velmurugan, P. Prakasam, V. Noor Mohameed, K. Saravanan, Smart garbage monitoring and navigation system using IoT, Int. J. Innov. Technol. Expl. Eng. 8 (11) (2019) 3992–3996.

[2] P. Prakasam, T.R. Suresh Kumar, T. Velmurugan, S. Nandakumar, Efficient power distribution model for IoT nodes driven by energy harvested from low power ambient RF signal, Microelectron. J. (2019) http://dx.doi.org/10.1016/j.mejo.2019.104665.

[3] Paris Kitsos, Nicolas Sklavos, Maria Parousi, Athanassios N. Skodras, A comparative study of hardware architectures for lightweight block ciphers, Comput. Electr. Eng. 38 (1) (2012) 148–160.

[4] Lin Ding, Chenhui Jin, Jie Guan, Qiuyan Wang, Cryptanalysis of lightweight WG-8 stream cipher, IEEE Trans. Inf. Forensics Secur. 9 (4) (2014) 645–652.

[5] Swarnendu Jana, Jaydeb Bhaumik, Manas Kumar Maiti, Survey on lightweight block cipher, Int. J. Soft Comput. Eng. 3 (5) (2013) 183–187.

[6] Wenling Wu, Lei Zhang, Lblock : A lightweight block cipher, in: Applied Cryptography and Network Security, in: Springer LNCS, vol. 6715, 2011, pp. 327–344.

[7] Christophe De Canniere, Orr Dunkelman, Miroslav Knezevic, KATAN and KTANTAN-a family of small and efficient hardware-oriented block ciphers, in: Cryptographic Hardware and Embedded Systems-CHES 2009, in: Springer LNCS, vol. 5747, 2009, pp. 272–288.

[8] J. Borghoff, et al., PRINCE–a low-latency block cipher for pervasive computing applications, in: Advances in Cryptology–ASIACRYPT, in: Springer LNCS, vol. 7658, 2012, pp. 208–225.

[9] Ray Beaulieu, Douglas Shors, Jason Smith, StefanTreatman Clark, Bryan Weeks, Louis Wingers, The SIMON and SPECK families of lightweight block ciphers, IACR Cryptology ePrint Archive (2013).

[10] Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, HIGHT: A new block cipher suitable for low-resource device, in: Cryptographic Hardware and Embedded Systems-CHES 2006, Vol. 4249, Springer Berlin Heidelberg, 2006, pp. 46–59.

[11] Gaurav Bansod, Nishchal Raval, Implementation of a new lightweight encryption design for embedded security, IEEE Trans. Inf. Forensics Secur. 10 (1) (2015) 142–151.

[12] George Hatzivasilis, Konstannious Fysarakis, Ioannis papaestathi, Harrymani favas, Review of light weight block ciphers, J. Cryptogr. Eng. 8 (2) (2017) 141–184.

[13] Jaber Hossein Zadeh, Abbas Ghaemi Bafghi, Evaluation of lightweight block ciphers in hardware implementation: A comprehensive survey, in: Proc. 1st International Conference on New Research Achievements in Electrical and Computer Engineering, 2017, arXiv:1706.03878.

[14] Saurabh singh, Pradip KumarSharma, Seo Yeon moon, Jong Hyuk Park, Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions, J. Ambient Intell. Human. Comput. (2017) 01–18.

[15] Muhammad Usman, Irfan Ahmedy, M. Imran Aslamy, Shujaat Khan, Usman Ali Shahy, SIT: A lightweight encryption algorithm for secure internet of things, Int. J. Adv. Comput. Sci. Appl. 8 (1) (2017) 01–08.