iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 Issue: V Month of publication: May 2016

DOI:

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

FPGA Implementation of Lightweight Cryptographic Algorithms-A Survey

Athmika Aravind[1], Vignesh Ballal[2] , Kiran Kumar V.G[3],Reshma[4],Megha N[5]
[1,2]M.Tech in VLSI Design & Embedded Systems, [3]Associate Professor, [4,5]Assistant Professor
[3,4,5,6]Dept. Electronics & Communication Engineering ,Sahyadri college of Engineering & Management, India

Abstract Ever-present computing is new era of computing and it needs lightweight cryptographic algorithms for security and confidentiality. Lightweight cryptography is used for resource limited devices such as radio frequency identification (RFID) tags, contactless smart cards, wireless sensor network, health care devices and internet of things (IoT). The comparative evaluations of these block ciphers on any platform is hard. In this paper comparative study of selected symmetric key lightweight block ciphers such as LED, HUMMINGBIRD, PRESENT, GRAIN-128, TEA, KTANTAN is presented.

Keywords –LFSR, keys, shift register, GEs, Encryption.

I. INTRODUCTION

In this digital era we come across the tremendous growth in digital data and communication. Mankind and hard bind data transfer have become a forgotten story. Internet has become an important part of life. Life without technology is near to impossible these days. But public networks and wireless medium are more prone to hacking and unauthorized usage. In certain fields like defense and finance any leakage of information would cause a serious issue. Adequate security and confidentiality is very much required in the aspect. So the data is only known to authorize users. Cryptographic algorithms were not very suitable for implementation .So development of new branch of cryptography called light weight cryptography was developed. In recent time advances in algorithm design and increased awareness of application is noticed. Evolution of light weight block cipher has come into picture. It doesn’t require strict classification. The requirement of algorithms is very less in target devices.

II. METHODOLOGY OF VARIOUS LIGHTWEIGHT CRYPTOGRAPHIC ALGORITHMS

A. LED

Light Encryption Device block cipher is a 64 bit block cipher that uses cryptographic key sizes varying from 64bits to 128 bits .128-bit key size and 48 rounds is performed.The figure 1 illustrates the overall structure of LED block cipher with key size of 128 bits. Initially Plain text(x) is EX-OR’ed with Key1 (K1) where K1 ranges from 0 to 63 bits of total key size. After the completion of first four rounds Key2 (K2) is EX-OR’ed, where K2 ranges from 64 to 127 bits of the total key size. K1and K2 are alternatively EX-OR’ed after every four rounds. The step function is performed 12 times for 128 bits .Hence 48 rounds of operation are involved.

The Light Encryption algorithm is described by four main operations. They are,

Add Constants- Round constants are combined with cipher using bitwise XOR.

Substitute Cells- each of the 4 bits is replaced by generated 4 bits by using Present’s S-Box

Shift Rows-ith row rotated i cell position left.

Mix-Columns serial-Column replaced by the column vector.

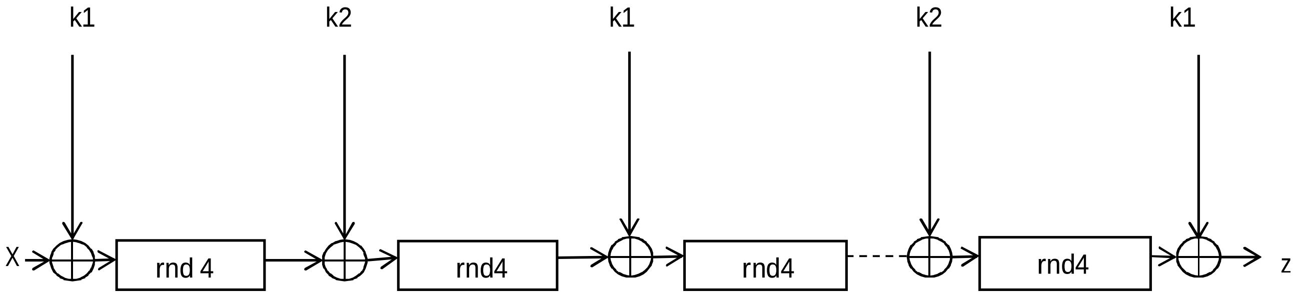


Fig.1. Block Diagram of Led Block Cipher.

B. Present

PRESENT cipher is a hardware-computed ultra-lightweight block cipher that has been designed with area and power constraints. PRESENT is an example of SPN(substitution permutation network) structure.It is a block cipher with 64 bit block size ,80 or 128 bit key size and performs 31 rounds.

Here, in the figure 2, the plaintext is Xor-ed with key register and performs the following set of operations and the last updated key is Xor-ed with P layer and we obtain the cipher text.

Each round consists of the following 3 steps

1- AddRoundKey: Key XORed with cipher.

2- Substitution: Used 4 bits S-box(shuffling of bits).

3- Permutation: Used P-layer.

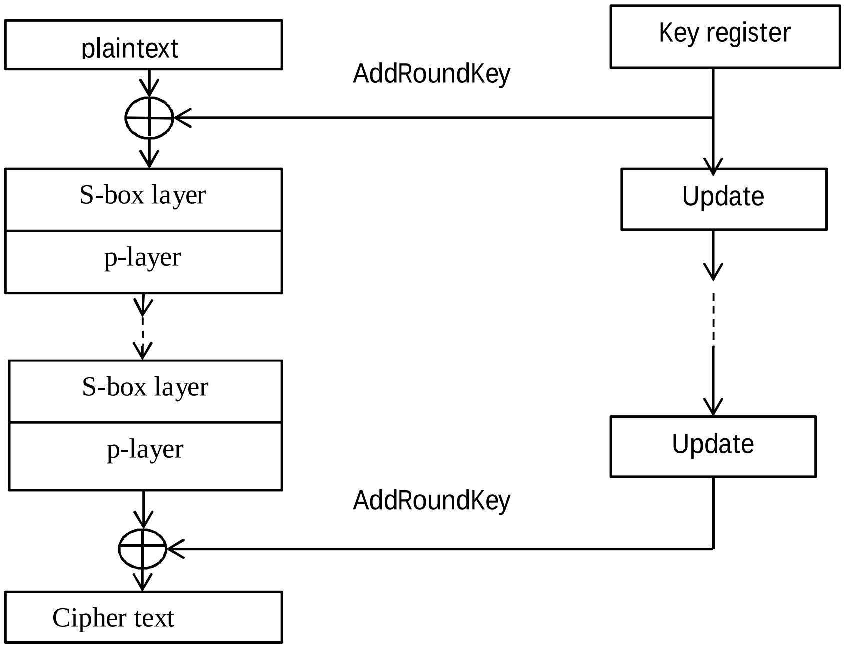


Fig. 2. Block diagram of present cipher

C. Grain 128

Grain 128 is stream cipher with 128 bit key size and internal vector of 96 bits. Grain is cryptographically efficient and very simple to implement on FPGA.

Figure 3 illustrates the overall structure of GRAIN 128 cipher and steps are described as follows

The cipher consists of three main building blocks, namely an linear feedback shift register(LFSR), an Nonlinear feedback shift register (NFSR) and an output function .

The content of the LFSR is denoted by si, si+1, . . . , si+127. Similarly, the content of NFSR is denoted by bi, bi+1, . . . , bi+127.

The feedback polynomial of the LFSR, denoted b(x), is a primitive polynomial of degree 128.

Before key stream is generated the cipher must be initialized with the key and the IV.

The 128-bit NFSR elements are loaded with the key bits, 4the first 96-bit LFSR elements are loaded with the IV bits . The last 32 bits of the LFSR is filled with ones.

After loading key and IV bits, the cipher is clocked 256 times without producing any key stream.

Instead the output function is fed back and Ex-ORed with the input, both to the LFSR and to the NFSR.

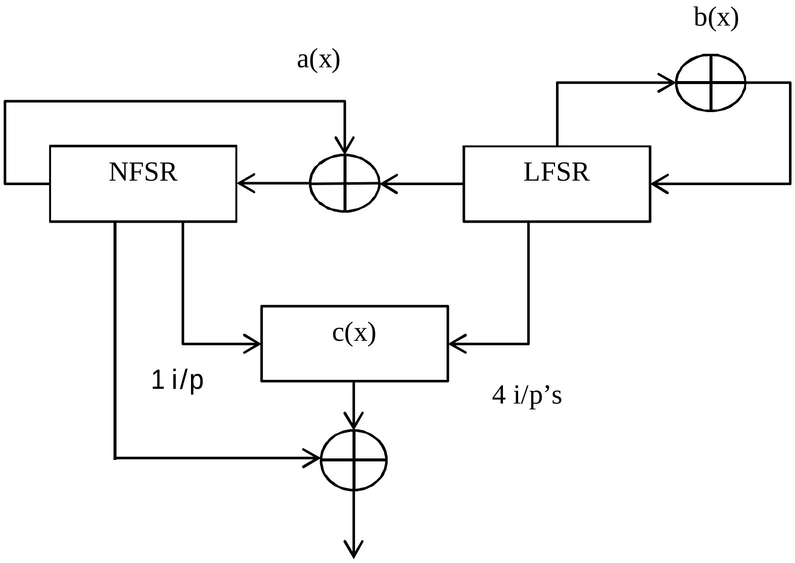


Fig..3. Block diagram Grain 128

D. Tiny Encryption Algorithm

The Tiny Encryption Algorithm (TEA) is cryptographically strong. Tiny Encryption Algorithm (TEA) is a block cipher is simple for its implementation. It requires minimum storage space.Figure 4 illustrates the encryption process of TEA cipher,wherein TEA uses 64 (block size) data bits time with128-bit key and performs 32 round of operation. TEA is a looping cipher, where each round i has plain text inputs S0 [i-1] and S1 [i-1],is obtained by previously generated round and added with key K

The one half S1 [i-1] is shifted 4 time left and 5 time right respectively. Sub key Ko and K1 is then added with left and right shifted block cipher and added with delta value

The results are then Ex–ORed and added with the other half of the block cipher S0[i-1] for next loop.

Same operation is performed on next loop.

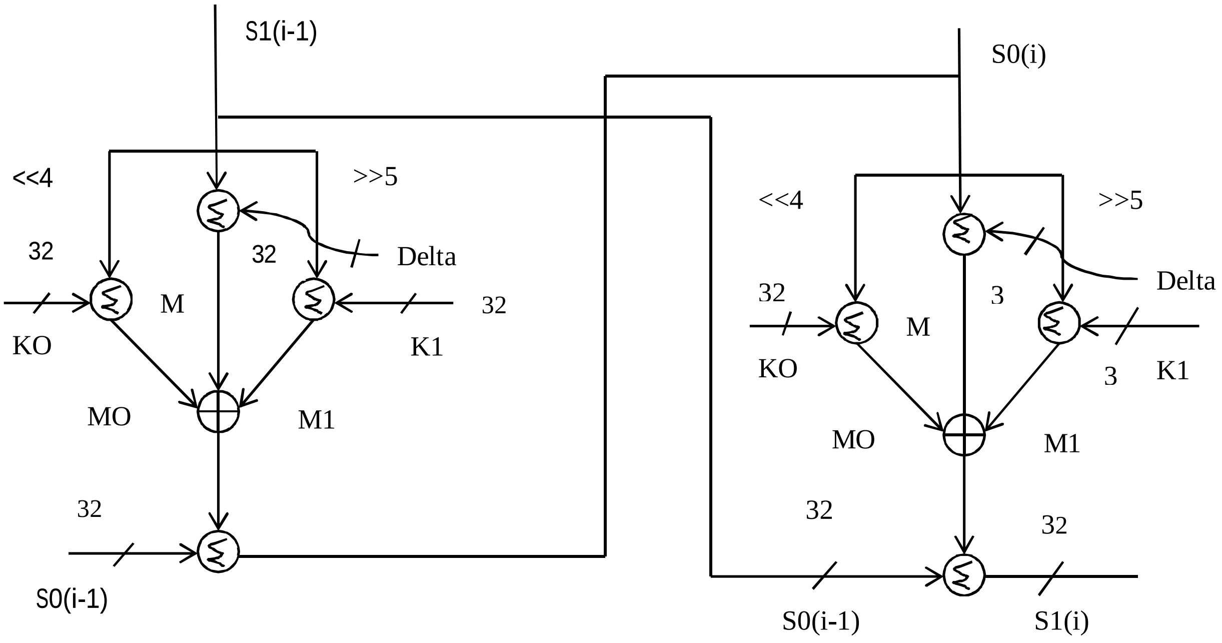


Fig.4. Block diagram TEA Algorithm

E. KATAN

KATAN is a block cipher KATAN32, KATAN48, and KATAN64.All the ciphers use 80-bit keys. KTANTAN is more compact in hardware – it assumes that the key is burnt into the target device and cannot be changed.

Algorithm is used is same as trivium. Each of KATAN algorithm loads a data block into two internal shift registers at top and bottom as shown in figure 6. it performs 254 rounds and it uses nonlinear function which obtained by feedback register. It uses Irregular value(IR) addition to several bits of register. The value depends on number of rounds

The function of KATAN48 and KATAN64 is similar to that of KATAN32, wherein KATAN48 and KATAN64 uses different bits of IR to provide a feedback.KATAN48 and KATAN64 make use of register which are large in size. For key schedule processing of KATAN linear feedback shift register been used. Nonlinear feedback shift register is used for counting rounds as well as terminate the encryption process.

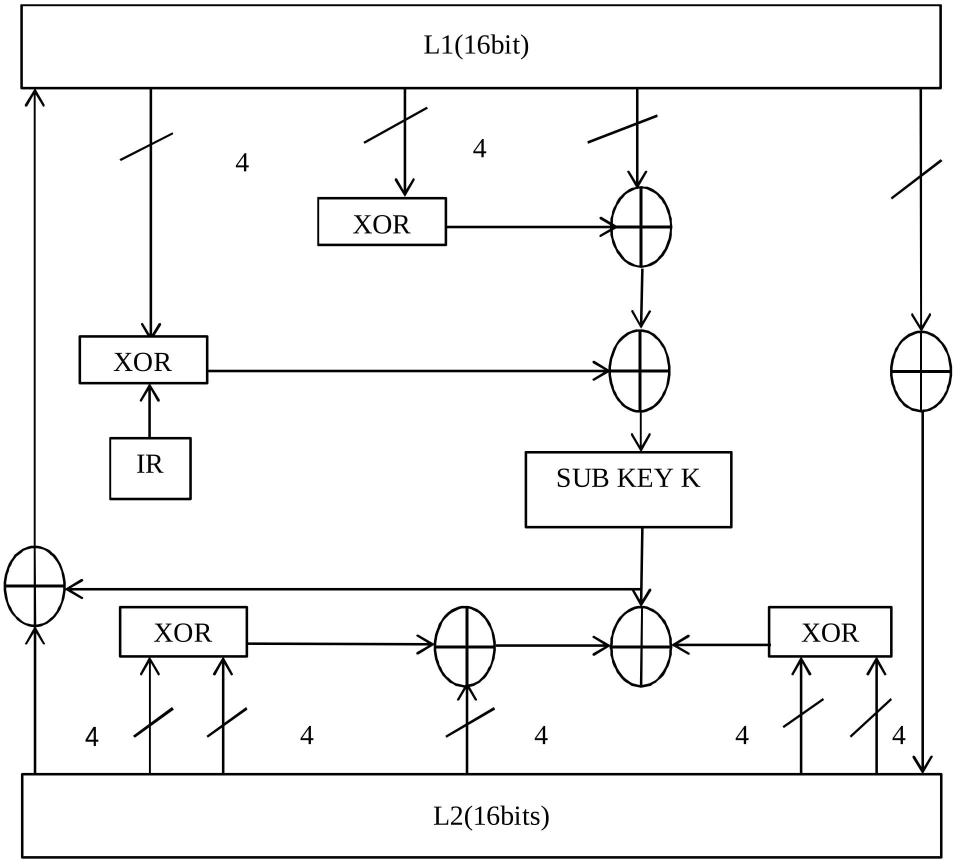


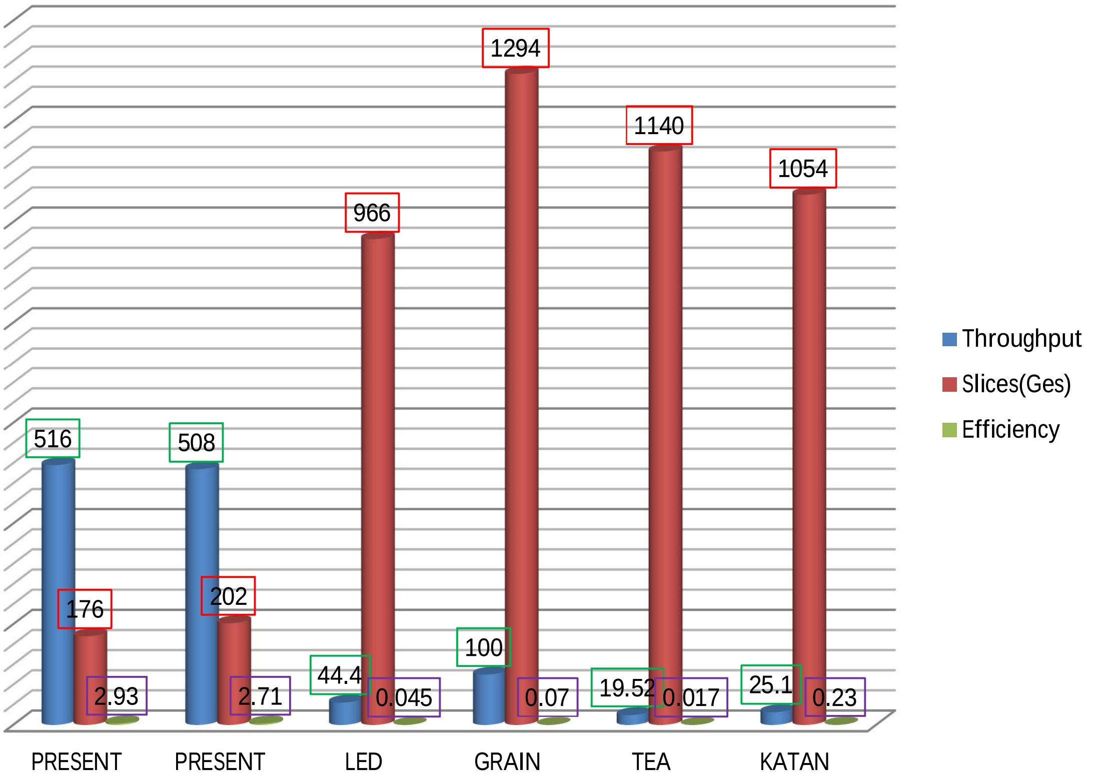
Fig.5. Block diagram of KATAN

III. TABLE AND GRAPH

Cipher	Key Size	FPGA Device	Throughput	Slices(GEs)	Efficiency
PRESENT	80	Spartan3XC35400	516	176	2.93
PRESENT	128	Spartan3XC35400	508	202	2.51
LED	128	Spartan3XC35200	44.4	966	0.045
GRAIN	128	Spartan3XC35200	100	1294	0.07
TEA	128	Spartan3XC35200	19.52	1140	0.017
KATAN	80	Spartan3XC35200	25.1	1054	0.23

Table 1. Comparisons Between Different Types Of Light Weight Cryptographic Algorithms

From the above mentioned table 1, PRESENT cipher with the key size 80 has the highest throughput and KATAN with key size 80 has least throughput. As the efficiency increases the performance of the design becomes more effective. If the slice is more the system becomes ineffective to be used.FPGA device used is Spartan3XC5XXX series.and the graph of these comapared algorithms is shown in graph 1.



Graph. 1. Comparisons Between Different Types Of Light Weight Cryptographic Algorithms

IV. CONCLUSION

By comparing the several algorithms that is LED, PRESENT, GRAIN,TEA, KATAN we can conclude the efficiency for present cipher is the best. As the efficiency of the cipher increases it reduces the power consumed and there by the area and cost. It is found from security analysis that the algorithms provide adequate security. But the power consumption of PRESENT is comparatively less in hardware implementation. The throughput of present is higher than other algorithms. So it is found from the analysis that present is more suitable as cryptographic algorithm for resource constrained devices.

REFERENCES

[1] Jian Guo, Thomas Peyrin, Axel Poschmann and Matt Robshaw ,“ The LED Block Cipher “.

[2] 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”.

[3] Prabhat Kumar Kushwaha ,M. P. Singh Prabhat Kumar ,“A Survey on Lightweight Block Ciphers” International Journal of Computer Applications (0975 8887) Volume 96 - No. 17, June 2014.

[4] Thomas Eisenbarth, Sandeep Kumar,Christof Paar and Axel Poschmann and Leif Uhsadel “ A Survey of Lightweight-Cryptography Implementations” IEEE Design & Test of Computers-November–December 2007.

[5] Mohammad Ubaidullah Bokhari and Shadab Alam “A Detailed Analysis of Grain family of Stream Ciphers” I.J. Computer Network and Information Security, 2014, 6, 34-40 Published Online May 2014 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2014.06.05

[6] Kiran Kumar.V.G, Sudesh Jeevan Mascarenhas, and Sanath Kumar published article “Design And Implementation Of Tiny Encryption Algorithm” et al. Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622,Vol. 5, Issue 6, (Part -2) June 2015, pp.94-97

[7] Rahul Ranjan and I. Poonguzhali, “VLSI Implementation of IDEA Encryption Algorithm”- Mobile and Pervasive Computing (CoMPC–2008)

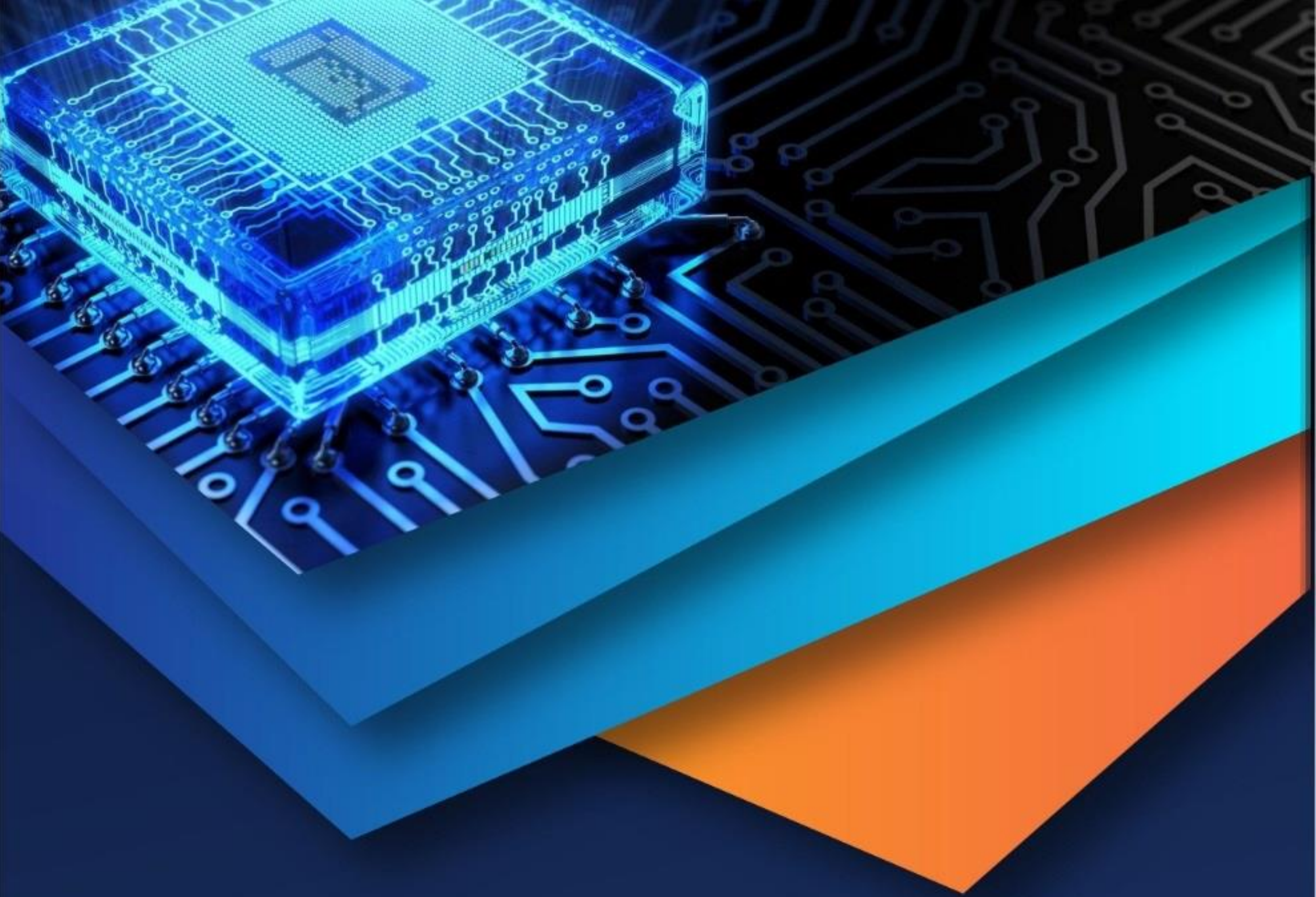
[8] T. Blesslin Sheeba1 and P.Rangarajan [5] “Novel NOC Architecture for SoC based Ultra Lightweight Crypto- Processor Using Present and Katan Algorithm”

[9] Jacob John,“Performance Analysis of New Light Weight Cryptographic Algorithms” IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume 5, Issue 5 (Sep-Oct. 2012), PP 01-04

[10] Thomas Eisenbarth Sandeep Kumar Christof Paar and Axel Poschmann Leif Uhsadel, “A Survey of   Lightweight-Cryptography Implementation

[11] P.Felsis Raja Sofia , Dr T.Blesslin Sheeba,“Efficient Hardware Implementation Of Led Block Cipher”.

[12] Sandeep Sadanandan, Rajyalakshmi Mahalingam," Light Weight Cryptography and Applications".



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY