J. Sustain. Wireless Syst.
Vol.01/ No. 04
Pages: 215-224
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2019.4.002

# Design of Lightweight Cryptographic Model for End-to-End Encryption in IoT Domain

**Runa Chatterjee,**
Assistant Professor,
Department of Computer Sc. &Engineering,
Netaji Subhash Engineering College,
Kolkata-152, West Bengal, India
Emails:runaseth2006@gmail.com

**Rajdeep Chakraborty,**
Assistant Professor ,Department of Computer Sc. &Engineering,
Netaji Subhash Engineering College,
Kolkata-152, West Bengal, India
rajdeep_chak@yahoo.co.in

**J.K. Mondal,**
Professor, Department of CSE, University of Kalyani,
Kalyani, West Bengal, India
Email: Jkm.cse@gmail.com

## Abstract

Digitalization rapidly connected the entire world. Everyday an enormous volumes of digital data produced by billions of intelligent devices which requires safe transmission over internet. If we look into embedded environment, handling massive volume of data is impractical for low power and low memory devices which leads to lightweight concept. The proposed lightweight model includes many symmetric key sequentially. The model follows fiestel network structure where 64 bits input block divided by two 32 bits blocks. Then every half undergoes through various symmetric key algorithms like TE (Triangular Encryption), RPPT (Recursive Pared Parity Technique), RPSPNC( Recursive Positional Substitution on Prime-Nonprime of Cluster), TB(Transformation of Bits) and bits rotation process. A triangular bit sequence generated by TE and from there various encryption as well as decryption techniques[1] have generated by reading bits in a certain order. RPPT encrypts bits by executing logical OR of successive bits. Bit swapping technique is used by TB for encryption and decryption. RPSPNC interchanges bits on the basis of prime-non prime bit position and considers any in between bit sequence as a cipher text. Lastly two resultant sub-blocks are merged to produce cipher text of 64 bits. To check the acceptance of the proposed model, comparisons take place with popular symmetric key algorithm AES and one embedded algorithm RPPT+TB. Software parameters like entropy, n-gram(4-gram), non-homogeneity, histogram are analysed. Hardware analysis of the model ensures us that it falls into lightweight domain by comparing the GE (Gate equivalent) with the ISO /IEC standard value ranges between 1000-2000GE.



ISSN: 2582-3167 (online)

J. Sustain. Wireless Syst.
Vol.01/ No. 04
Pages: 215-224
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2019.4.002

**Keywords:** Cryptosystem, CBC, End–to-End encryption, lightweight, IoT.

## 1.Introduction

The computer system which involves cryptography is termed as "Cryptographic System" or in shorthand Cryptosystem[5,10]. Various cryptographic techniques and infrastructures are implemented by Cryptosystem to provide security. On the basis of encryption and decryption technique, cryptosystems are categorized by two types- Symmetric or [1,5,6,10] public key and asymmetric or private key cryptosystem. One can differentiate from another only for their encryption and the decryption key. Public key cryptosystem is much quicker than private key cryptosystem. Very small power consumption and small area requirement for installation makes cryptosystem superior than software system. Internet of Things (IoT) domain requires such type of cryptosystem to share and communicate information of wearable devices, home appliances over internet. A large volume of sharable data contains confidential information which leads to security preservation.

Here a new lightweight public key cryptographic model has formed in CBC mode [10] using some of the existing techniques and finally it is claimed as lightweight. Here the software implementation of cryptosystem has done in Cryptool for software analysis and for hardware analysis Spartan 3E FPGA simulator is used. This model is compared with AES algorithm [10] and RPPT+TB, an embedded algorithm, for checking its superiority.

Section 2 illustrates related previous works; Section 3 includes the model structure details, the implementation part and the results survey portion. Section 4 includes the conclusion part.

## 2. Related Works

This section shows various encryption techniques applied in the model. The model incorporated different symmetric key encryption techniques.

### A. Recursive Pared Parity Technique(RPPT)

RPPT is a simplest encryption technique [5,6,10] where binary source sub-stream B=($X_{k-1}$, …… , $X_0$) (where $X_{k-1}$ is MSB and X0 is LSB) are converted to cipher stream using below mentioned transformation formulas 1&2.

$O_{k-1} = X_{k-1}$……(1), $O_i = X_i$ or $O_{i-1}$, where 1<= i <= (K-2)……(2)

### B. Transformation of Bits (TB)

In this method [2,7] firstly the whole message divided into a set of blocks of 64 bits each. Then bit swapping method applies to each block separately. After 31st swapping the original block is returned.

### C. Triangular Encryption (TE)

In the TE[5,9] process, the plaintext or input message to be transmitted is grouped into blocks .Let consider a input block, $SB_K$ = $S^0$0 $S^0$1 $S^0$2 $S^0$3 $S^0$4 …$S^0$n $S^0$n-1. Here Figure 1 displays the



ISSN: 2582-3167 (online)

J. Sustain. Wireless Syst.
Vol.01/ No. 04
Pages: 215-224
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2019.4.002

formation of triangle by performing XOR operation between two successive bits MSB ($S^0 0$) the start bit and next to MSB ($S^0 1$) and creates the first (n-1)bits. This logical operation executes 'n-1' times to ultimately generate $Sn^{-1}\,0$.

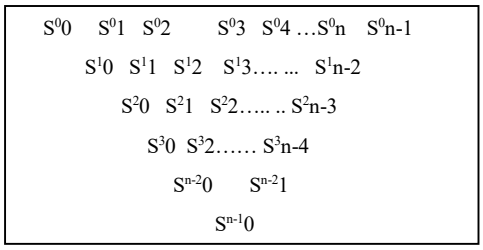


Figure 1. Triangle Formation

Now based on the sequence of reading bits order encryption method is decided. Option 1 reads the MSB bits from $S^0 0$ to $S^{n-1}\,0$, option 2 follows a series of MSB bits from $S^{n-1}\,0$ to $S^0 0$, option 3 follows a series of LSB bits $S^0 n\text{-}1$ to $S^{n-1} 0$ and option 4 includes entire LSB bits from $S^{n-1} 0$ to $S^0 n\text{-}1$. For option 1 and 4 encryption, decryption is same. For option 2 & 3 encryption, decryption option is 3 & 2 independently.

### D. Recursive Positional Substitution on Prime-Nonprime of Cluster (RPSPNC)

Generating function based block cipher technique RPSPNC [8] operates on block of n bit length which generates an equal length different intermediate blocks. The following algorithm describes the way of generating target intermediate block t or target stream:

1. when (n-i) is a nonprime integer [5,6].then i th bit of block s will copied to (n-i)th bit of block t.
2. The value of i th bit in block s will be placed in j th bit in block t, where j is the immediate previous prime integer [5,6] (if any) of a prime integer (n-i).
3. Otherwise, for the block s and t nth bit is same.
4. After checking all conditions 1, 2 and 3, the remaining vacant position of any bit in the block t is now filled by (n-2)th position bit in the block s.

### E. Cipher Block Chaining (CBC)

CBC based on feedback technique applied on a block. Here before encryption each plaintext block is XOR with prior level cipher text block. Thus, every cipher text block at a particular point depends on prior processed plaintext blocks. During decryption XOR operation is performed between each decrypted cipher text block and previous cipher text block. For both cases, initialization vector (IV) fed into the first block as an external input. The length of initialization vector is equal to input block length.

## 3.Proposed work

### 3.1 The Technique



ISSN: 2582-3167 (online)

J. Sustain. Wireless Syst.
Vol.01/ No. 04
Pages: 215-224
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2019.4.002

This part describes a short idea on design structure and implementation process of the proposed model. The model has a non-feistel structure and implemented in CBC mode. Schematic block diagram in Figure 2 and 3 show details steps of encryption and decryption process separately. Here plaintext [5,6,10] and cipher text are considered as 64 bits binary data block.

First the input plaintext is divided into n-numbers of blocks $P_1$, $P_2$, $P_3$,..Pn. Each block size is 64 bits. During encryption each plaintext block is dividing into two 32 bits sub-blocks. Then TE algorithm is applied to each sub-block. Now a series of encryption algorithms fed into both halve. Left half includes 8 bits left direction circular rotation follows by the RPSPNC technique which finally produces 32 bits left cipher text .The TE encrypted right half again encrypted by RPPT and TB sequentially which ultimately generates 32 bits right cipher text. Finally sub-blocks are merge to produce 64 bits cipher text.

The decryption technique follows the reverse order of the encryption process. First, the output cipher text grouped into two 32 bits left and right sub-blocks. For left sub-block the algorithms which applied sequentially but in reverse order of encryption process are RPSPNC, 8 bits right rotation (opposite of 8 bits left rotation during encryption) and TE .For right sub-block the sequence is TB, RPPT and TE. Thereafter combines both halves resultant plaintext to achieve the original ones.

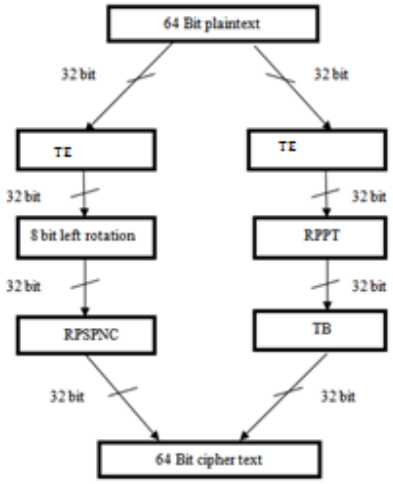


Figure 2. Encryption process block diagram

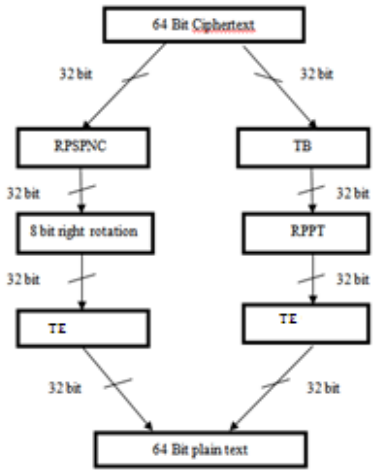


Figure 3. Decryption process block diagram

### 3.2 Implementation

The model includes FPGA [1] based hardware implementation which has done in VHDL on Xilinx ISE 14.7 [5] software. To do this it reads input from a file. Then encryption is performed over the input and the generated cipher text is written in another file. In Dev C++ platform C programming has been written to implement the model and Cryptool has used to compare software parameters efficiency.

### 3.3 The Result and Analysis



ISSN: 2582-3167 (online)

J. Sustain. Wireless Syst.
Vol.01/ No. 04
Pages: 215-224
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2019.4.002

The proposed lightweight model has been compared with RPPT+TB and AES. There are some parameters have been considered for software analysis like entropy, non-homogeneity, N-gram test and histogram which are described in Sec 3.3.1, Sec 3.3.2, Sec 3.3.3 and Sec 3.3.4 respectively. Hardware analysis executed in Xilinx simulator which is shows in sec 3.3.5.

### 3.3.1. Entropy Test

In a thermodynamic system Entropy measures the randomness of data. In 1948 Shannon adapted in measuring the unpredictability of information content. According to him it is defined as $H(X)=-\sum Prob[xi]\cdot log2(Prob[xi])$.....(3) where Prob[xi] denotes probability and a random variable x takes on the values.x1,x2,x3,…,xn.

| **Serial no** | **Name of the file** | **Size of file(in kb)** | **Entropy** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Proposed Model** | | | **AES** | | | **RPPT+TB** | | |
| | | | Actual | Max | % | Actual | Max | % | Actual | Max | % |
| 1 | 07.jpg | 81 | 8.00 | 7.89 | 98.62 | 8.00 | 7.99 | 99.87 | 8.00 | 7.90 | 98.75 |
| 2 | sqmapi.dll | 131 | 8.00 | 7.59 | 94.87 | 8.00 | 7.99 | 99.87 | 8.00 | 7.97 | 99.62 |
| 3 | Jview.exe | 151 | 8.00 | 7.12 | 89 | 8.00 | 7.99 | 99.87 | 8.00 | 6.60 | 82.5 |
| 4 | Gender.txt | 207 | 6.61 | 5.60 | 84.72 | 8.00 | 7.99 | 99.87 | 4.70 | 4.31 | 53.87 |
| 5 | Pod.exe | 245 | 8.00 | 4.77 | 59.62 | 8.00 | 7.99 | 99.87 | 8.00 | 2.54 | 54.04 |
| 6 | Devices.txt | 303 | 8.00 | 4.92 | 61.5 | 8.00 | 7.99 | 99.87 | 4.70 | 4.28 | 53.5 |
| 7 | Names.txt | 473 | 6.61 | 5.72 | 86.53 | 8.00 | 7.99 | 99.87 | 4.70 | 2.92 | 62.12 |
| 8 | Uninst.exe | 567 | 8.00 | 7.30 | 91.25 | 8.00 | 7.99 | 99.87 | 8.00 | 7.4 | 92.5 |
| 9 | Cordic.pdf | 679 | 8.00 | 7.89 | 98.62 | 8.00 | 7.99 | 99.87 | 8.00 | 7.33 | 91.62 |
| 10 | Setuolog.txt | 817 | 6.61 | 5.57 | 84.26 | 8.00 | 7.99 | 99.87 | 4.70 | 4.21 | 89.57 |

Table 1. Entropy Analysis

| **Sr No** | **Name of the file** | **File size(in kb)** | **Proposed lightweight model** | | **AES** | | **RPPT+TB** | |
|---|---|---|---|---|---|---|---|---|
| | | | **Chi value** | **Degree of** | **Chi value** | **Degree of** | **Chi value** | **Degree of** |

Table 2. Non homogeneity test Analysis



ISSN: 2582-3167 (online)

J. Sustain. Wireless Syst.
Vol.01/ No. 04
Pages: 215-224
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2019.4.002

| | | | | freedom | | freedom | | freedom |
|---|---|---|---|---|---|---|---|---|
| 1 | 07.jpg | 81 | 2930 | 255 | 2901 | 255 | 4196 | 255 |
| 2 | sqmapi.dll | 131 | 911570 | 255 | 405038 | 255 | 453939 | 255 |
| 3 | Jview.exe | 151 | 2179748 | 255 | 1524732 | 255 | 3577211 | 255 |
| 4 | Gender.txt | 207 | 108038272 | 255 | 3400779 | 255 | 132754464 | 84 |
| 5 | Pod.exe | 245 | 3688778 | 255 | 2738725 | 255 | 4223144 | 255 |
| 6 | Devices.txt | 303 | 29360786 | 163 | 2701723 | 255 | 257540 | 65 |
| 7 | Names.txt | 473 | 149186800 | 214 | 3914536 | 255 | 61141140 | 89 |
| 8 | Uninst.exe | 567 | 1354812 | 255 | 320837 | 255 | 1170567 | 235 |
| 9 | Cordic.pdf | 679 | 992144 | 255 | 701673 | 255 | 1054675 | 225 |
| 10 | Setuplog.txt | 817 | 497023744 | 215 | 5788855 | 255 | 3907850 | 90 |

Figure 4. Entropy Test analysis

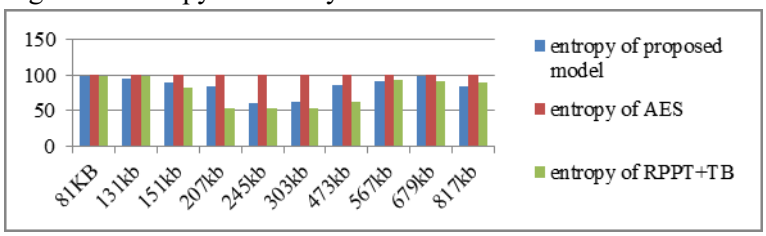


Table 1 displays the entropy parameter value of different files encrypted by different algorithms and Figure 4 is the respective graphical representation. Here ten sample source files have been encrypted by AES, RPPT+TB and by proposed model and finally calculates entropy from each cipher text. It is noticeable that the model has acquired quite high entropy w.r.t. others.

### 3.3.2. Non-Homogeneity Test

This test measures the similarity of two categorical probability distributions. Pearson ‘s Chi-Square statistic as follows:

$$X^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i} \quad \text{.....(4)}$$

O stands for Observed frequency or plaintext and E for Expected frequency or cipher text. Table 2 shows chi-value of all ten files and bar chart in Figure 5 illustrates the logarithmic base 10 Chi-values of the three algorithms taken into consideration. It is clearly shows that for all ten files Chi-values of proposed model are quite higher than AES and for 80% better than RPPT+TB. It has been decided that proposed model is superior to others.



ISSN: 2582-3167 (online)

J. Sustain. Wireless Syst.
Vol.01/ No. 04
Pages: 215-224
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2019.4.002

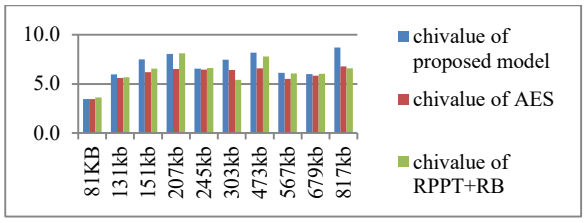


Figure 5. Non-homogeneity test

### 3.3.3. N-gram analysis

The n bit strings of distinct characters are named as N-gram. The input text is divided into words based on specified characters list, and finally produces N-grams of each word of the specified length. Figure 6.displays the bar charts of N-gram analysis.

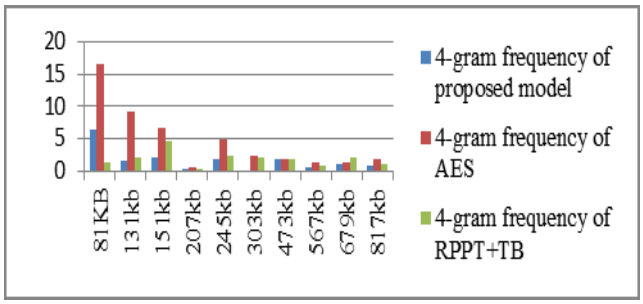


Figure 6. 4 gram value analysis

| Sr. No | Name of the file | File Size (in kb) | 4gram analysis frequency in%) | | |
|---|---|---|---|---|---|
| | | | Proposed lightweight model | AES | RPPT+TB |
| 1 | 07.jpg | 81 | 6.25 | 16.66 | 1.33 |
| 2 | sqmapi.dll | 131 | 1.50 | 9.09 | 2.00 |
| 3 | Jview.exe | 151 | 2.02 | 6.66 | 4.5 |
| 4 | Gender.txt | 207 | 0.12 | 0.45 | 0.31 |
| 5 | Pod.exe | 245 | 1.78 | 4.76 | 2.28 |
| 6 | Devices.txt | 303 | Null | 2.38 | 2.18 |
| 7 | Names.txt | 473 | 1.75 | 1.92 | 1.91 |
| 8 | Uninst.exe | 567 | 0.63 | 1.26 | 0.85 |
| 9 | Cordic.pdf | 679 | 1.11 | 1.33 | 2.1 |
| 10 | Setuplog.txt | 817 | 0.75 | 1.72 | 0.98 |

Table 3 shows the 4-gram analysis of three algorithms, RPPT+TB, the proposed model and AES. Graphical view displays in Figure. 6 which prove that repetition of tokens is less in the proposed model w.r.t. others.

### 3.3.4. Frequency distribution graph (Histogram)



ISSN: 2582-3167 (online)

J. Sustain. Wireless Syst.
Vol.01/ No. 04
Pages: 215-224
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2019.4.002

Histogram of a plaintext generates a graphical bar chart view of frequency distribution of characters from input within a certain window (plot type). The x-axis defines set of all characters presents in the character set: Here 'Gender.txt' file has been chosen for comparisons with others. Comparing Figure.8, 9, 10 w.r.t. Figure. 7, it is seen that histogram of the proposed model includes all 256 characters where AES, RPPT+TB includes % of characters.

Table 3. N-Gram (4-Gram) Analysis

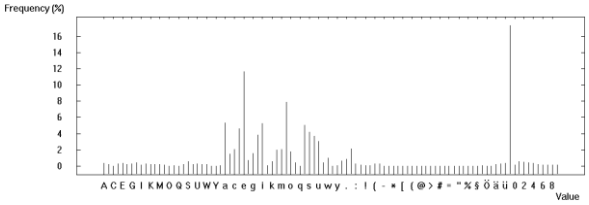


Figure 7. Gender.txt source file

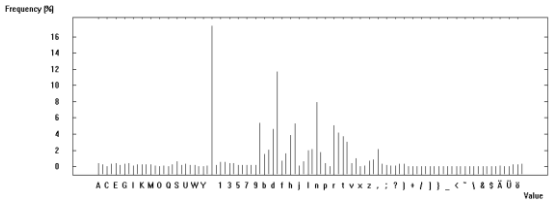


Figure 8. AES encrypted gender.txt

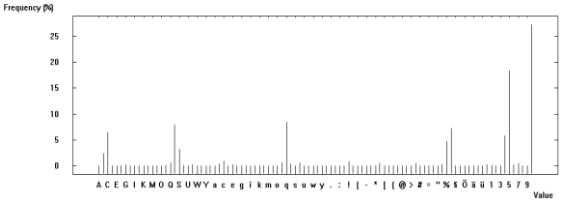


Figure 9. RPPT+TB encrypted gender.txt

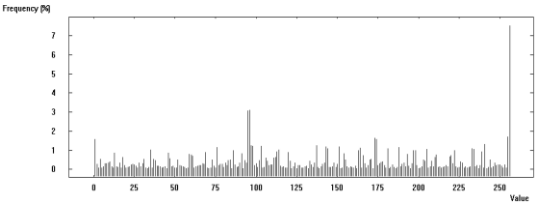


Figure 10. model encrypted gender.txt

### 3.3.5. Hardware/FPGA based analysis

For hardware based implementation and simulation Xilinx 14.7 ISE with Spartan 3E FPGA chip has been used. The comparison among Proposed lightweight model, RPPT+TB and AES have been done w.r.t. timing summary and net-list [3] values. Table-4 shows result of timing parameters analysis. Percentage (%)of hardware resources requirement calculation has done in Table 5.

Table 4. FPGA Timing Summary

| Timing Parameters | Proposed lightweight model | AES | RPPT+TB |
|---|---|---|---|
| Minimum input arrival time before clock | 1.914ns | 6.933ns | 0.489ns |
| Maximum output required time after clock | 0.640ns | 6.611ns | 0.650ns |
| Maximum combinational path delay | 0.354ns | 7.790ns | 0.570ns |

Table 5. FPGA Net-list generation



ISSN: 2582-3167 (online)

J. Sustain. Wireless Syst.
Vol.01/ No. 04
Pages: 215-224
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2019.4.002

**Advanced HDL Synthesis Report (Gate Equivalent count)**

Macro Statistics

| | |
|---|---|
| # **Multiplexers** | : 19 |
| 1 bit 2 X 1 multiplexer | : 16 |
| 64 bits 2 X 1 multiplexer | : 3 |
| # **Xors** | : 1622 |
| 1-bit xor2 | : 1621 |
| 1-bit xor21 | : 1 |
| Total | : 1641 |

Here the proposed lightweight model provides effective result in timing summary and net list generation report. Advance HDL synthesis report shows that Gate Equivalent (GE) of the proposed method is 1641 which is belong to the ISO/IEC standard GE for lightweight cryptographic algorithm. Result shows that the model requires fewer resources than RPPT+TB and AES**.**

## 4. Conclusion

In this paper one lightweight cryptographic model has been proposed which is successfully designed in software as well as hardware platform. The technique is applicable to IoT embedded platform also for its lightweightness. By analysing the efficiency parameters it is decided that the proposed lightweight model is superior to AES and RPPT+TB. 4-Gram analysis test has given the best result while non-homogeneity and frequency distribution test provide better and optimal result respectively. Hardware analysis proved that this model is lightweight w.r.t. GE and so the proposed lightweight model can be implemented in IoT based embedded systems for tiny devices.

## References

[1] Rajdeep Chakraborty, AvishekDatta and JK Mandal “Secure Encryption Technique (SET): A Private Key Crypto System”, published in International Journal of Multidisciplinary in Cryptology and Information Security (IJMCIS) ISSN 2320 –2610, accepted & published in Volume 4, No.1 (January – February 2015) issue, PP 10-13.

| Net-List Parameters | Proposed lightweight model | | AES | | RPPT+TB | |
|---|---|---|---|---|---|---|
| | Amount | % | Amount | % | Amount | % |
| Number of Slices | 117 | 00 | 1051 | 03 | 01 | 00 |
| Number of Slice Flip Flops | 00 | 00 | 1399 | 02 | 15 | 00 |
| Number of 4 input LUTs | 129 | 00 | 1450 | 02 | 00 | 00 |
| Number of bonded IOBs | 133 | 21 | 390 | 57 | 17 | 08 |

[2] Ashwini R. TondeȦ and Akshay P. DhandeȦ, “Implementation of Advanced Encryption Standard (AES) Algorithm Based on FPGA”, International Journal of Current Engineering and Technology, Volume 4 No. 2 (April 2014), pp 1048 – 1050.

[3] Bernhard Schmidt, Daniel Ziener, J¨urgenTeich, and Christian Z¨ollner, “Optimizing Scrubbing by Netlist Analysis for FPGA Configuration Bit Classification and Floorplanning”,VLSI Journal 59C (2017) pp. 98-108, DOI: 10.1016/j.vlsi.2017.06.012

[4] P.Gupta, Pankaj Gulhane,” Design and Implementation of HDLC Controller Using VHDL Code” International Journal of Advance Research, Ideas and Innovations in Technology, ISSN: 2454-132X, (Volume3, Issue3),2017, Page | 1465.



ISSN: 2582-3167 (online)

[5] Miodrag J. Mihaljevic and Hideki Imai, “A Stream Cipher Design Based on Embedding of Random Bits”, International Symposium on Information Theory and its Applications, ISITA2008, Auckland, New Zealand, 7-10, December, 2008, ieeexplore.ieee.org

[6] AvishekDatta, RajdeepChakraborty and J.K. Mandal, “The CRYPSTER: A Private Key Crypto System”, published & presented in 2015 IEEE International Conference on Computer Graphics, Vision and Information Security (IEEE CGVIS 2015) IEEE Conference Record number: #36759, held on November 02-03, 2015, at Bhubaneswar, India, DOI 10.1109/CGVIS.2015.7449882:, pp 06-10.

[7] Rajdeep Chakraborty, Runa Seth and J.K. Mandal, “Design of FPGA Based ECB Cryptosystem: RPPT Embedded with TB”, Published and Presented in 5th International Conference on Computing, Communication and Sensor Network, CCSN 2016, held on 24th-25th,Dec 2016, Kolkata, W.B., India, organized and sponsored by International Association of Science, Technology and Management, IEEE (EDS) Kolkata Chapter, Foundation of Computer Science, ISBN 81-85824-46-0, pp 23 – 27.

[8] Rajdeep Chakraborty, Runa Seth and J.K. Mandal, “An FPGA Based Block Cipher through Recursive Positional Substitution on Prime-Nonprime of Cluster (RPSPNC)”, published & presented in 3rd International Conference on Microelectronics, Circuits and Systems, MICRO 2016, July 09th – 10th, 2016, at Science city, Kolkata, West Bengal, India, organized and sponsored by MaulanaAbulKalam Azad University of Technology (MAKAUT), IEEE, CCSN, EDS, Kolkata, India, ISBN: 978-93-80813-45-5,pp 96-101.

[9] Rajdeep Chakraborty, Runa Seth and J.K. Mandal, "High Entropy and Avalanche Based Non-Feistel Cascaded CFB Block CipherThrough RSBPNDS and TE", CICBA-2017, March, 2017, Kolkata, W.B., India organized and sponsored by Calcutta Business School, IEEE, Computer Society of India, Springer CCIS series, DOI 10.1007/978-981-10-6427-2, indexed in DBLP, Google Scholar, EI-Compendex, Mathematical Reviews, SCImago, Scopus, pp 485 – 494 (part – I).

[10] Behrouz A. Forouzan, “Cryptography and Network Security”, Special Indian Edition 2007, Tata Mc-Graw-Hill, ISBN-13: 978-0-07- 066046- 5, ISBN-10: 0-07-066046-8.

## Authors Biography

**Runa Chatterjee** received B.Tech.dergee in CSE from Maulana Abul Kalam Azad University of Technology(formerly known as West Bengal University of Technology), West Bengal and M.Tech, in CSA from University of Calcutta. She has started her Ph.D. work since 2016.Her current research area mainly in lightweight cryptography and computer security for embedded system. She has four publications in international conferences. She has also guided many UG projects.



ISSN: 2582-3167 (online)

J. Sustain. Wireless Syst.
Vol.01/ No. 04
Pages: 215-224
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2019.4.002

Author did his PhD in CSE from University of Kalyani with M.Tech in IT and BE in CSE. His research experience is of 9 years and academic experience is of 14 years. He has several publications in reputed international journals and conferences. His field of interest is mainly in cryptography and computer security. He has also guided many master's thesis and UG projects.

Author did his PhD in CSE from Jadavpur University with M.Tech in CSE and M.Sc. in Physics. His research experience is of 25 years and academic experience is of 31 years. He has several publications in reputed international journals and conferences. His field of interest is mainly in Coding Theory, Data and Network Security, Remote Sensing & GIS based Applications, Data Compression Error Corrections, Information security, Watermarking, Steganography and Document Authentication, Image Processing, Visual Cryptography, MANET, Wireless and Mobile Computing/security, Unify Computing, Chaos Theory and Applications.. He has also guided many master's thesis and UG projects and supervised 22 PhD scholar.



ISSN: 2582-3167 (online)