JCST Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7766127

PERFORMANCE ANALYSIS OF LIGHT WEIGHT CRYPTOGRAPHIC ALGORITHM CLEFIA 128

Atul H. Karode[1], Dr. Shekhar R Suralkar[2]
[1]Ph D Research Scholar,
[1] Department of E&TC, SSBT's College of Engineering and Technology, Bambhori Jalgaon
Jalgaon 425001 (India), [1]atulkarode@gmail.com
[2]Professor
[2] Department of Computer Engg., SSBT's College of Engineering and Technology,
Bambhori Jalgaon, Jalgaon 425001 (India)
[2]shekhar_srs@rediffmail.com

Abstract: The important benefit of light weight algorithm are tiny block sizes, tiny key sizes, Simpler rounds, Simpler key schedule as we know Complex key size increase the memory usage , execution delay and the power consumption of implementations; therefore, for many applications like Wireless sensor network lightweight block ciphers use simple key structure that can generate sub-keys.

In this paper the performance analysis of Light Weight Cryptographic CLEFIA based on energy consumption is discussed, so for this purpose MSP-EXP430FR5994 Launch Pad Development Kit [25] is used which belongs to MSP430 family, It is the product of Texas Instruments (TI) Company. The CLEFIA algorithm supports 128-bit block size having three different key sizes 128-bit, 192-bit, 256-bits respectively.

Key words- Lightweight cryptography, Clelia, key size.

1. Introduction

This paper describes the details of performance analysis of light weight algorithm CLEFIA 128. The CLEFIA cipher operates on 128-bit block size with three different key sizes 128-bit, 192-bit, 256-bits. Cryptographic algorithm can be used more effectively for very small size, low energy consumption and small devices such as RFID tags, sensors, and smart cards which are contactless. As my first objective is to Study and analysis of existing light weight algorithm. So, in this paper I am going for analysis of the parameters such as energy consumption, power consumption, voltage, current and battery life.

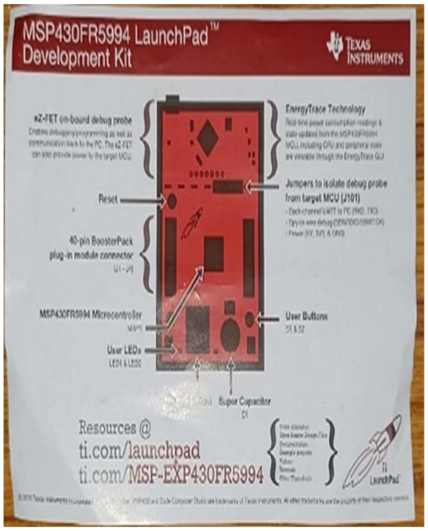
2. CLEFIA 128 algorithm-

CLEFIA is a 128-bit block cipher with its key length being 128, 192 and 256 bits, which is consistent with Advanced encryption standard (AES). CLEFIA consists of two parts the first part is a data processing part and second is a key scheduling part. CLEFIA uses a generalized Feistel structure which is a symmetric structure with four data lines, and the width of each data line is 32 bits.

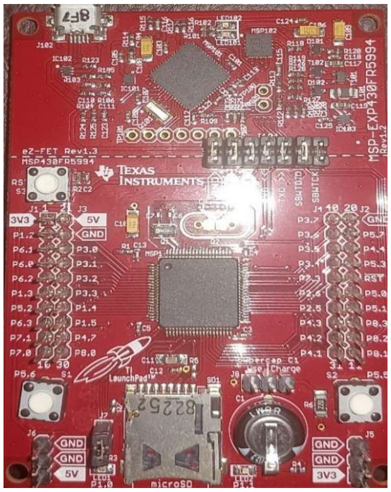
2.1 Performance analysis and Results

In this analysis, MSP-EXP430FR5994 Launch Pad Development Kit [25] is used from MSP430 family, the product of Texas Instruments (TI). For performance analysis parameter

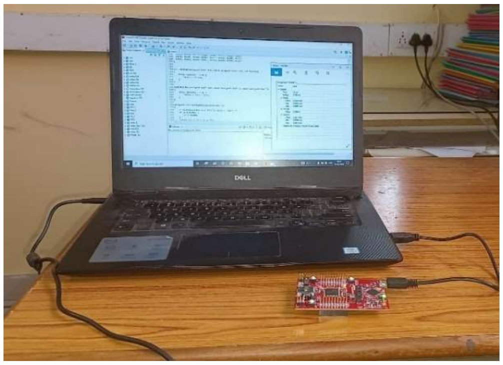
related to energy and power consumption is used. The kit used is a development platform consist of MSP430FR5994 microcontroller. This microcontroller operates with 16 MHz clock frequency and it has 256 kB ultra-low power consumption Ferroelectric Random-Access Memory (FRAM) which is permanent memory. Also, MSP430FR5994 has low power consumption and is very effective as consist with Low-Energy Accelerator (LEA) technique which uses minimum power for execution. This microcontroller process analog data in real time mode. The built-in
e Z-FET debugging feature gives better performance and so with this feature, the performance of the encryption code can be tested and analyzed. The Code Composer Studio (CCS) used in devices manufactured by Texas Instruments TI, has been used as a software development tool used to write, build, test, and debug a program [25]. The Code Composer Studio Version: 11.0.0.00012 with OS: Windows 10, v.10.0, x86_64 / win 32Java version: 11.0.11 is used.


MSP430FR5994 LaunchPad™
Development Kit
Texas Instruments
eZ-FET on-board debug probe
Enables debugging/programming as well as communication back to the PC. The eZ-FET can also provide power to the target MCU.
EnergyTrace Technology
Real-time power consumption readings & state updates from the MSP430FR5994 MCU including CPU and peripheral state are viewable through the EnergyTrace GUI
Jumpers to isolate debug probe from target MCU (J101)
- Back-channel UART to PC (RXD, TXD)
- Spy-bi-wire debug (SBWTDIO/SBWTCK)
- Power (5V, 3V3, & GND)
Reset
40-pin BoosterPack plug-in module connector
(J1 - J4)
MSP430FR5994 Microcontroller
MSP1
User LEDs
LED1 & LED2
User Buttons
S1 & S2
Super Capacitor
C1
Resources @
ti.com/launchpad
ti.com/MSP-EXP430FR5994
TI LaunchPad

Photograph1 overview of MSP-EXP430FR5994 Launch Pad Development Kit.
The photograph 1 shows overview of MSP-EXP430FR5994 Launch Pad Development Kit.



Photograph 2 MSP-EXP430FR5994 Launch Pad Development Kit.



Photograph 3 Practical set up for measurement

The lightweight CLEFIA algorithms was executed and complied with C code in CCS and codes were transferred to MSP430FR5994 device. The energy, power, and current measurements of the CLEFIA algorithms for three different key sizes 128-bit, 192-bit, 256-bits was carried out with help of Energy Trace software available in CCS [25]. The Energy Trace technology is based on energy code analysis that measures and displays the energy required for the algorithm execution. This technology also helps for enhancement which reduces power consumption. The energy trace software works in unified mode within Code Composer Studio (CCS). The practical set up for measurement is shown in photograph 3.

The basic energy measurements can be made with the Energy-Trace mode using CCS. The supply voltage in the microcontroller is species continuously to measure energy and power. This mode can be used to verify the application’s energy consumption Without accessing the debugger.

With operating of energy trace software, the MSP430FR5994 will work into active mode (AM). The mode (AM) in every second, it will perform the encryption or decryption process, and then it will go into the power saving mode LPM (Low Power Mode. [25]. The device is operating for 10 seconds and hence Energy, power, and current data of algorithms were measured.

3. Measurement of various Parameter of CLEFIA 128 Block Cipher

Using Energy Trace technology, the energy consumption of CLEFIA light weight algorithm is measured and displayed. This software also helps for enhancement in ultra-low power Consumption. This software works within Code Composer Studio in unified mode.

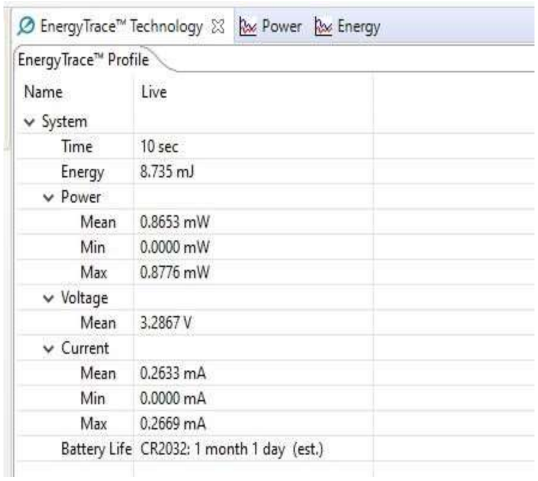
3.1 Energy consumption

The simulation windows of energy trace technology are generated showing Energy consumption, Power Consumption. The device is capable of showing mean value of power as well as variation in power with minimum and maximum mode.

The electric parameter Voltage with its mean value and current with its mean including maximum and minimum variation is also generated by this software

3.1.1 Energy consumption for key length 128

The energy consumed for CLEFIA 128 is 8.735mj (millijoule) operating the device for 10 seconds. The screen shot of actual measurement is as shown in Figure 1

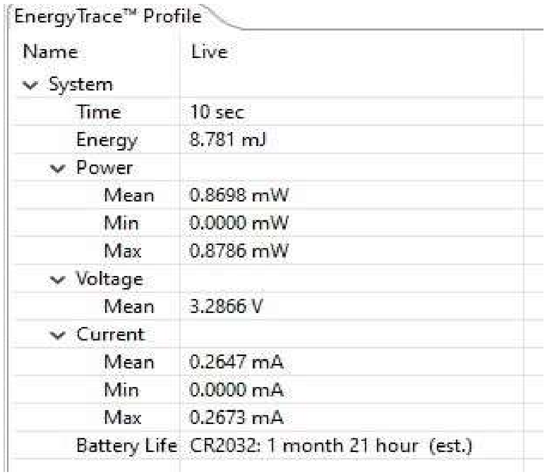


Name	Live
System	
Time	10 sec
Energy	8.735 mJ
Power	
Mean	0.8653 mW
Min	0.0000 mW
Max	0.8776 mW
Voltage	
Mean	3.2867 V
Current	
Mean	0.2633 mA
Min	0.0000 mA
Max	0.2669 mA
Battery Life	CR2032: 1 month 1 day (est.)

Figure 1 Screen shot of actual measurement for CLEFIA 128 using energy trace software

3.1.2 Energy consumption for key length 192

The energy consumed for CLEFIA 192 is 8.781mj (millijoule) operating the device for 10 seconds.

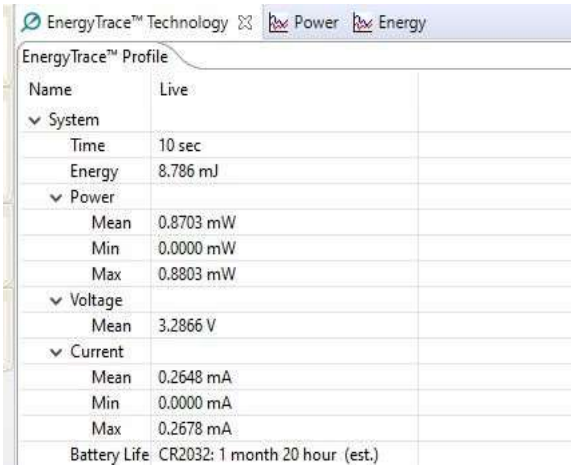


Name	Live
System	
Time	10 sec
Energy	8.781 mJ
Power	
Mean	0.8698 mW
Min	0.0000 mW
Max	0.8786 mW
Voltage	
Mean	3.2866 V
Current	
Mean	0.2647 mA
Min	0.0000 mA
Max	0.2673 mA
Battery Life	CR2032: 1 month 21 hour (est.)

Figure 2 Screen shot of actual measurement for CLEFIA 192 using energy trace software

3.1.3 Energy consumption for key length 256

The energy consumed for CLEFIA 256 is 8.786 mj (millijoule) operating the device for 10 seconds.



Name	Live
System	
Time	10 sec
Energy	8.786 mJ
Power	
Mean	0.8703 mW
Min	0.0000 mW
Max	0.8803 mW
Voltage	
Mean	3.2866 V
Current	
Mean	0.2648 mA
Min	0.0000 mA
Max	0.2678 mA
Battery Life	CR2032: 1 month 20 hour (est.)

Figure 3 Screen shot of actual measurement for CLEFIA 256 using energy trace software

The Comparative analysis of energy consumption **CLEFIA 128** with Feistel Architecture is as shown in table 1

Table 1 Comparative analysis of Energy Consumption for CLEFIA 128

Block length	Key length	Number of rounds	Energy (mJ)	Energy Difference in mJ
128	128	18	8.735	--
128	192	22	8.781	0.046
128	256	26	8.786	0.051

3.1.4 Energy plot for CLEFIA

Energy plot for CLEFIA 128 is as shown Figure 4

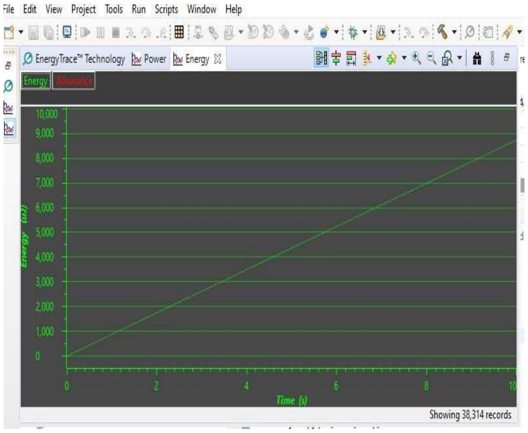


Figure 4 Energy plot for CLEFIA 128

3.2 Power consumption

3.2.1 Power consumption for key length 128

Referring Figure 1 The Power consumed for CLEFIA 128 is 0.8653mw (milliwatt) operating the device for 10 seconds.

3.2.2 Power consumption for key length 128

Referring Figure 2 The Power consumed for CLEFIA 192 is 0.8698mw (milliwatt) operating the device for 10 seconds.

3.2.3 Power consumption for key length 256

Referring Figure 3 The Power consumed for CLEFIA 256 is 0.8703mw (milliwatt) operating the device for 10 seconds

The Comparative analysis of Power consumption CLEFIA 128 with Feistel Architecture is as shown in table 2

Table 2 Comparative analysis of Power Consumption for CLEFIA 128

Block length	Key length	Number of rounds	Power (mW)	Power Difference in mW	Max and Min Power in mW
128	128	18	0.8653	--	Max 0.8776
					Min 0.0000
128	192	22	0.8698	0.0045	Max 0.8786
					Min 0.0000
128	256	26	0.8703	0.0050	Max 0.8803
					Min 0.0000

3.2.4 Power plot for CLEFIA

Power plot for CLEFIA 128 is as shown Figure 5

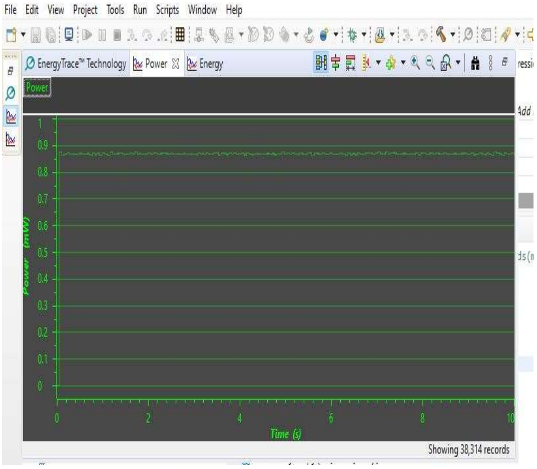


Figure 5 Power plot for CLEFIA 128

3.3 Voltage and Current Measurement

The voltage and Current measurement are made for different key size

The Comparative table for measurement of voltage shown in table 3 for various key size.

Referring to Figure 1,2 and 3

Table 3 Comparison for measurement of voltage

Block length	Key length	Number of rounds	Voltage (Mean)
128	128	18	3.2867
128	192	22	3.2866
128	256	26	3.2866

From the table 3 we can see that their no much more effect on voltage consumed by device while executing on various key size.

Similarly, the Comparative measurement of current shown in table 4 for various key size.

Table 4 Comparative measurement of current

Block length	Key length	Number of rounds	Current (mA)	Difference in Current mA	Max and Min Current in mA
128	128	18	0.2633	--	Max 0.2669
					Min 0.0000
128	192	22	0.2647	0.0014	Max 0.2673
					Min 0.0000
128	256	26	0.2648	0,0015	Max 0.2678
					Min 0.0000

3.4 Estimated battery life

The working capacity of the device with battery CR 2032 estimated battery life is tabulated in table 5.

Table 5 Comparative analysis of estimated Battery life

Block length	Key length	Number of rounds	Battery life (CR 2032) Estimated lithium coin or button cell battery
128	128	18	1 month 1 day
128	192	22	1 month 21 hours
128	256	26	1 month 20 hours

A CR 2032 battery is a non-rechargeable (primary) lithium coin or button cell battery that is 20mm diameter and 3,2mm thickness. It has a voltage of 3 volts and capacity up to 240mAh. Referring to Figure 1, 2 and 3 the Comparative table for estimated battery life shown in table 5 for various key size.

In this way, the device can work with CR 2032 lithium coin or button cell battery. Batteries for 1 months and 1 day for key length of 128, 1 month 21 hours for key length of 192 and 1 month 20 hours for 256 respectively.

When the performance results obtained in the analysis are checked, it can be seen that the number of loops and block size of the CLEFIA algorithms make a slight difference in terms of energy consumption, current measurement, Hence CLEFIA is the encryption algorithm that has the largest block length among the other light weight algorithms examined with 128-bit block length, while, in other algorithms, 64-bit is preferred as block length. This is important for the devices operating in application such as the Internet consisting low-capacity devices [25]. Using the CLEFIA, the encryption time is enhanced due to small size blocks.

4. Conclusion:

From obtained results it is concluded that with increased key size increases the energy consumption and power consumption that degrade the efficiency of system. But it is seen that, the larger the key size is, the better the security is provided. Hence the applications such as IoT where sensors are working in wireless mode for 24*7 that's why the energy consumption, power consumption voltage, current measurement estimated battery life carried out with Energy Trace technology which is based on energy code analysis and it is tool that measures and it shows the energy required for the application. This technology also helps for optimization that reduces power consumption

References

[1] Avinash Kak "Some Basic Vocabulary of Computer and Network Security and a Brief Review of Classical Encryption Techniques Lecture Notes on Computer and Network Security, Purdue University 18 April, 2018.

[2] Sattar B. Sadkhan, Akbal O. Salman "A Survey on Lightweight-Cryptography Status and Future Challenges", International Conference on Advances in Sustainable Engineering and Applications (ICASEA),Wasit University, Kut, Iraq. IEEE Conference proceeding, ISSN 978-1-5386-3540-7/18/31.00$©2018 IEEE, 2018. pp.105-108. June 2018.

[3] Thomas Eisenbarth Sandeep Kumar Christof Paar and Axel Poschmann "A Survey of Lightweight-Cryptography Implementations" IEEE proceeding on IEEE Design & Test of Computers, Co published by the IEEE CS and the IEEE CASS, ISSN 0740-7475/07/$25.00 G 2007 IEEE, pp 1-12,4 October 2017.

[4] Yulong Zou, Jia Zhu, Xianbin Wang and Lajos Hanzo, "A Survey on Wireless Security Technical Challenges, Recent Advances, and Future Trends" Proceedings of the IEEE Volume 104, No. 9, Digital Object Identifier: 10.1109/JPROC.2016.2558521, pp 1727-1765 September 2016.

[5] Gaurav Bansod, Nishchal Raval and Narayan Pisharoty "Implementation of a New Lightweight Encryption Design for Embedded Security" IEEE Transactions On Information Forensics And Security, Vol. 10, No. 1, ISSN 1556-6013 © 2014 IEEE, DOI10.1109/TIFS.2014.2365734 pp,142-151 January 2015.

[6] Pradeep Semwal, Mahesh Kumar Sharma "Comparative Study of Different Cryptographic Algorithms for Data Security in Cloud Computing" ISSN 978-15090-6403-8/17/$31.00 © 2017 IEEE pp.1-7, 2017.

[7] Sarika Y. Bonde, Dr. U. S. Bhadade, "Analysis of Encryption Algorithms (RSA, SRNN and 2 key pair) for Information Security" ISSN 978-1-5386-4008-1/17/$31.00 ©2017 IEEE. pp. 1-7 2017.

[8] Ahmer Khan Jadoon , Licheng Wang , Tong Li , and Muhammad Azam Zia ,"Review Article Lightweight Cryptographic Techniques for Automotive Cybersecurity ", Hindawi Wireless Communications and Mobile Computing Volume 2018, Article ID 1640167, pp 1-15, 26 June 2018.

[9] Shehnaz T. Patel, Nita H. Mistry,"A Survey: Lightweight Cryptography in WSN" IEEE International Conference on Communication Networks (ICCN) 2015, IEEE Proceeding

ISSN 978-I-S090-00S 1-7I 1S/$3 1.00©2015 IEEE, DOl 1O.l 109/ICCN.20IS.3. pp 11-15,2015.

[10] Oscar Delgado-Mohatar , Amparo Fúster-Sabater, Jose M. Sierra ,"A light-weight authentication scheme for wireless sensor networks" , Journal of Elsevier B.V, ISSN 1570-8705/$. doi:10.1016/j.adhoc.2010.08.020, pp 727-735, 8 September2010.

[11] Khalid Mahmood, Shehzad Ashraf Chaudhry, Husnain Naqvi Taeshik Shon, Hafiz Farooq Ahmad "A lightweight message authentication scheme for Smart Grid communications in power sector", Journal of Elsevier B. V Computers and Electrical Engineering ,0045-7906/©2016 Elsevier Ltd. pp 1-11,07 March 2016.

[12] Rajani Devi. T, "Importance of Cryptography in Network Security", IEEE Proceeding ISSN 978-0-7695-4958-3/13 $26.00 © 2013 IEEE, IEEE Computer Society, DOI 10.1109/CSNT.2013.102, pp 462-467, 2013.

[13] Masanobu Katagi and Shiho Moriai, "Lightweight Cryptography for the Internet of Things", White paper by Sony Corporation, pp 1-4.

[14] Lara-Ni, Carlos Andres, Morales-Sandoval, Miguel and Dıaz-Perez "An evaluation of AES and PRESENT ciphers for lightweight cryptography on smart phones", IEEE Proceeding ISSN 978-1-5090-0079-1/16/$31.00 ©2016 IEEE, pp 87-93, 2016.

[15] Charalambous Manifavas, George Hatzivasilis, Konstantinos Fysarakis , and Konstantinos Rantos "Lightweight Cryptography for Embedded Systems - A Comparative Analysis" White paper by Dept. of Applied Informatics & Multimedia, Technological Educational Institute of Crete, Heraklion, Crete, Greece, pp 1-10.

[16] Axel York Poschmann Bochum, "LIGHTWEIGHT CRYPTOGRAPHY -Cryptographic Engineering for a Pervasive World "Thesis, Faculty of Electrical Engineering and Information Technology Ruhr University Bochum, Germany.pp 1-5, February 2009.

[17] Kerry A. McKay, LarryBassham, Meltem Sonmez Turan , Nicky Mouha "Report on Lightweight Cryptography" NISTIR 8114,National Institute of Standards and Technology U.S. Department of Commerce, Internal Report 8114 pp-1-14 March 2017.

[18] Tetsu Iwata "The 128-bit Block cipher CLEFIA Design Rationale" Report on development of CLEFIA by Sony Corporation, Konan, Minato-ku, Tokyo 108-0075 Japan June 1, 2007.

[19] Madhumita Panda "Performance Analysis of Encryption Algorithms for Security" International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016 IEEE Proceeding ISSN 978-1-5090-4620-1/16/$31.00 ©2016 IEEE, pp 278-284, 2016.

[20] Chaitra B, Kiran Kumar V.G, Shatharama Rai "A Survey on Various Lightweight Cryptographic Algorithms on FPGA" IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 12, Issue 1, Ver. II (Jan.-Feb. 2017), PP 54-59

[21] Jaber Hossein Zadeh, Abbas Ghaemi Bafghi "Evaluation of Lightweight Block Ciphers in Hardware Implementation: A Comprehensive Survey"2016 1st International Conference on New Research Achievements in Electrical and Computer Engineering.

[22] Levent Ertaul, Sachin Kattepura Rajegowda "Performance Analysis of CLEFIA, PICCOLO, TWINE Lightweight Block Ciphers in IoT Environment" International

Conference on Security and Management SAM'17, ISBN: 1-60132-467-7, CSREA Press ©, Pp 25-31.

[23] Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata "The 128-bit Blockcipher CLEFIA" (Extended Abstract), Sony Corporation, Konan, Minato-ku, Tokyo 108-0075 Japan June 1, 2007.

[24] Tetsu Iwata of Nagoya University, The 128-bit Block cipher CLEFIA Algorithm Speciation, Revision 1.0 June 1, 2007.

[25] Bora Aslan FusunYavuzer Aslan and M. Tolga Sakallı "Energy Consumption Analysis of Lightweight Cryptographic Algorithms That Can Be Used in the Security of Internet of Things Applications" Research Article Hindawi Security and Communication Networks, Volume 2020, Article ID 8837671, 15 pages