SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V10I8P105

Volume 10 Issue 8, 48-58, August 2023
© 2023 Seventh Sense Research Group®

Original Article

Performance Evaluation of Light Weight Cryptographic CLEFIA Algorithm

Atul H. Karode[1], Shekhar R. Suralkar[2], Vaishali B. Patil[3]

[1,2]*Department of E&TC, SSBT College of Engineering and Technology, KBC NMU Jalgaon, India.*
[3]*Department of Business Management, RCPET's Institute of Management Research and Development Shirpur, India.*

[1]*Corresponding Author : atulkarode@gmail.com*

Received: 07 June 2023 Revised: 11 July 2023 Accepted: 06 August 2023 Published: 31 August 2023

Abstract *- We have become more cognizant of communication since the 19th century. However, we have known how important communication is for daily life for the last three or four decades. It is merely a method of transmitting data from one end to the other. A transmitter and a receiver are the two ends. Both of these components must be present for communication to succeed. As the application of this process continues to grow, new techniques or tactics have been developed. The human being then learned that communication is crucial, but so is keeping that communication safe. Claimed to be a trustworthy cipher is CLEFIA. The CLEFIA specs and algorithm design can be assessed for performance and security by cryptographers and the general public. For ISO/IEC lightweight cryptography, the CLEFIA cipher is a popular choice. It is a generalised Feistel network with four nodes. This architecture requires little room, both physically and virtually. The Diffusion Switching Mechanism in CLEFIA shields the system from serious assaults. Additionally, the primary scheduling and data processing components of CLEFIA perform comparable tasks, which decreases the gate size. In this study, the execution times of the Low Weight Cryptographic CLEFIA old and modified algorithms are discussed. This calls for using a product from Texas Instruments (TI), the MSP-EXP430FR5994 LaunchPad Development Kit from the MSP430 family. The CLEFIA supports 128-bit blocks and offers 192-bit and 256-bit key sizes.*

Keywords *- Lightweight cryptography, Design, Embedded systems, Hardware, CLEFIA block cipher, IT security, Feistel network structure, Power and energy consumption.*

1. Introduction

In recent decades, the market for embedded systems has expanded significantly. At this time, the utilization of embedded and mobile systems has surpassed that of personal computer systems. The requirement for protection and security administrations has additionally expanded. This must be accomplished with minimal and productive executions of cryptographic natives. One example of a rudimentary cipher is SONY's own CLEFIA symmetric block cipher [1]. In order to ensure resistance to differential and linear assaults, this method supports 128, 192, and 256-bit keys. It offers increased cryptographic security by using, among other things, Diffusion Switch Mechanisms and whitening keys [1].

The efficiency of CLEFIA has recently been shown, especially in ASIC and FPGA hardware implementations. Many of these methods aim to have compact, high-performance architectures that maximise available computing resources and use all opportunities for parallelism in the underlying operations. Unfortunately, most state-of-the-art structures only allow critical expansion up to 128 bits in length when using a 4-branch Feistel network. This is the case since a Feistel network with eight branches is needed to compute the critical enlargement for keys with 128 bits, 192 bits, and 256 bits [2, 3].

1.1. Lightweight Cryptographic Algorithms

The restricted resources of the devices utilised in IoT applications should be considered while designing and implementing cryptographic algorithm solutions. Because of this need, lightweight cryptography was made so gadgets with restricted assets (for example, RFID labels, sensors, and contactless savvy cards) might better use cryptographic protections. Since it is a reliable and safe standard, AES [4] is widely implemented in data transport. While AES is an excellent security protocol, it is unsuitable for computers with lower processing power.

The limitations of AES, especially in low-power contexts, are widely known. Since AES was adopted 16 years ago, numerous technological advancements have occurred. However, as stated in [5], integrated circuits for RFID and similar devices should be produced in the 2000

 This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

GE zone. AES implementations have a 2400 GE space under optimal conditions [6]. Lightweight cryptography means to furnish calculations that give data security little asset use. To do this, numerous lightweight algorithms have been developed. Block encryption techniques make up the vast bulk of established algorithms. The lightweight cryptographic algorithms CLEFIA Block cipher were examined in this research study. The following justifies the decision to use these algorithms.

1.1.1. CLEFIA

CLEFIA is a highly secure block cipher that was first developed in 2007. You might pick a critical length between 128 pieces and 256 pieces. The size of each block is 128 pieces. To make CLEFIA more reliable, its algorithm specification has been made available to the public. This will enable cryptographers all around the world to conduct public assessments. The cipher used in lightweight cryptography specified by ISO/IEC 29192 is called CLEFIA [7].

High Performance

Sony's CLEFIA block cipher, based on a cutting-edge cipher design technique, achieves a thing that has historically been difficult to accomplish: maintains a high degree of security while offering world-leading hardware and software implementation capabilities. The highest hardware gate efficiency in the world is attained when it is implemented in hardware. It can accomplish high-velocity execution on a scope of processors when utilized in programming [8].

Advanced Design

Based on cutting-edge cipher design principles, Sony's CLEFIA block cipher offers unparalleled hardware and software implementation capabilities in addition to a high level of security. If you implement it in hardware, you will have the most outstanding gate efficiency possible. Using it in software provides top-notch performance across several CPU types [8].

Cutting-Edge Design

CLEFIA is made possible by combining tried-and-true design methods with cutting-edge best practices. The 4-branch generalized Feistel structure allows efficient hardware and software implementation of these F-functions. CLEFIA's Diffusion Switching Mechanism can fend off serious dangers. In addition, expenses are reduced [9] due to the smaller gate size that results from the shared functions between the central scheduling component and the data processing component.

For a critical length of 128 bits, the Feistel-based method needs 18 rounds, 22 rounds, and 26 rounds, respectively. Each iteration consists of two 32-bit F functions and four buses. Figure 1 depicts the circular layout of the CLEFIA. P = plain text, C = scrambled text in the encryption cycle; P = 0, C = 128. Besides, C = C0|C1|C2|C3 is a C encoded text obtained by handling four sections as P = P0|P1|P2|P3, with Pi, Ci 0, 132 (0 I 4). In the first, second, and third rounds, essential whitening is performed using WK0, WK1, WK2, WK3, and 132, respectively. The notation RKi 0, 132 (0 i 2r), If r is the total number of iterations, indicates keys generated in rounds.

The first step is to XOR WK0 and WK1 from the open text with P1 and P3. After that, the (RK0, P0) operation is carried out, and the function F0 is accessed with the RK0 key. The P1WK0 operation's result is then XOR'd onto the output. Likewise, the P2 block is shipped off the F1 capability utilizing the RK1 key, and the F1 (RK1, P2) activity is XORed with the P3WK1 result. The accompanying round is passed by exchanging the P0 | P1 | P2 | P3 block created at the finish of the round to P0 P3, P1 P0, P2 P1, and P3 P2. The P1 and P3 functions of the previous round's function outputs are XORed with WK2 and WK3 [5, 6].

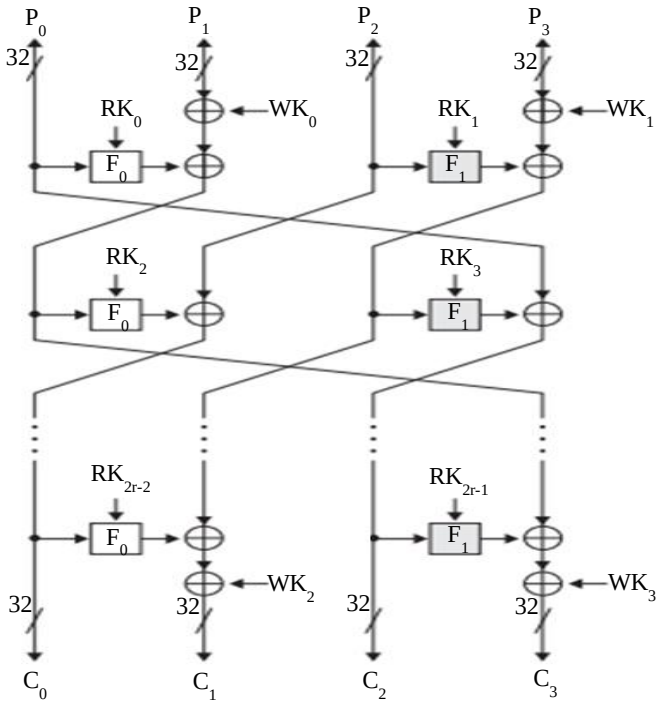

Fig. 1 CLEFIA encryption round structure [4]

CLEFIA's designers believe that no attack threatens the entire game. They tried the linear cryptanalysis, the differential attack, the square attack, the linear attack, and the impossible differential attack.

1.2. Description of Block Cipher

Block and critical sizes in block ciphers are fixed. Block ciphers use the operations of confusion and diffusion to encrypt data. There is much ambiguity about the connection between the encryption key and the cipher text. The

influence of each crucial part on the rest of the cipher text is assumed. Diffusion makes cipher text very sensitive to statistical assaults [10] because it multiplies the effects of each plain text item from a block across more pieces in the code text.

1.2.1. Block Cipher Varieties

There are two significant categories of block ciphers: those based on Feistel networks and those based on Substitution Permutation Networks (SPN). Classical Feistel Networks and Generalised Feistel Networks are two subcategories of Feistel Networks.

Feistel Structures

Feistel structures typically require more rounds than SPNs since they operate on just half of the data every round. Unscrambling capabilities in Feistel type structures do not have enormous execution costs since a similar programming code is utilized for both encryption and decoding tasks to save memory needs. CLEFIA [1], SIMON [11], PICCOLO [12], TWINE [13], Spot, and XTEA [14] are some well-known Feistel organizations. There are two types of Feistel networks: CFSs (Classical Feistel Structures) and GFSs (Generalized Feistel Structures). More rounds are needed for GFS to give the highest level of security.

Substitution Permutation Networks (SPN)

A collection of related mathematical operations is known as SPN. A single SPN round comprises three layers: replacement, permutation, and essential mixing layers. The replacement or confusion function contributes to the confusion in a substitution/confusion layer.

Non-linear operations such as bit-slice implementation or S-boxes (based on look-up tables) are provided at this layer. Each of the two layers-diffusion and permutation-involves P-boxes. The change layer comprises invertible direct changes or primary fixed stages (word or touch-wise). It necessitates the invertibility of the S-box and has an abundance of parallelism built in for chaos and spread. Some of the newest and most popular SPN block ciphers include AES [15], PRESENT [16, 17], KLEIN, LED, and mCrypton [18].

The details of the performance analysis of the lightweight algorithm CLEFIA Block cipher algorithm are described in this paper. The CLEFIA supports 128-bit block sizes and three key sizes: 128-bit, 192-bit, and 256-bits. Cryptographic algorithms can be used more effectively for small, low-energy, and small devices such as RFID tags, sensors, and contactless smart cards. Our primary objective is to study and assess new and current lightweight algorithms.

The reduction in execution time is the primary objective of this study. This study compares the times of existing lightweight algorithms and new/modified lightweight algorithms. After the improvement in execution time, we calculated power and energy consumption by using an enhanced CLEFIA block cipher lightweight algorithm.

The structure of the present research work is as follows: Section 1 presents a detailed introduction to the topic, including Lightweight Cryptographic Algorithm, CLEFIA and Block Cipher information. Section 2 presents a literature survey of the present research work. Section 3 includes a performance analysis of the Clefia algorithm model and the result obtained by the algorithm model. Section 4 presents the conclusions of the research work. The last section includes references to research work.

2. Literature Survey

In [19], the author discusses compact CLEFIA hardware implementations. The cornerstone of his research is contemporary serialised designs in the data processing block. We develop and synthesise three unique hardware architectures using a typical cell library of 0.13 m in width.

According to our estimates, the tiny implementation, which is far smaller than the previous most minor version, only requires 2,488 GE. Additionally, only 116 GE can enable decryption.

In [2], the author discusses and evaluates high-performance hardware designs for the CLEFIA 128-bit block cipher. The author created five different CLEFIA hardware structure types by fusing three F-functions with two loop structures. These designs were created using a library of 90-nm CMOS standard cells, and their speed and size were assessed. At 400.96 Kbps/gates, the output efficiency was 1.5 times greater than prior levels.

In [1], the author describes the 128-bit CLEFIA structure, which accommodates various key lengths. Keys of 128, 192, and 256 bits are accepted. The clefia has also met the AES standard. The new Clefia framework effectively handles immunity to well-known assaults. Additionally, with the aid of design methodologies, It can be efficiently modified for a hardware and software structure. In terms of how well it runs on hardware and software, CLEFIA achieves an excellent profile. CLEFIA is an efficient framework, especially for hardware.

In [20], according to the author, specific structures are currently more effective for cryptographic procedures. These structures only allow for the processing of one algorithm. For the multi-algorithm processors that are now available, expensive and inefficient structures are needed. We are utilising reconfigurable technology results in increased expenses for both efficiency and configuration. The recommended approach allows several algorithms to use shared elements, resulting in a typical result.

In [21], the author discusses a brand-new Differential Fault Analysis (DFA) using a 128-bit key CLEFIA. Two pairs of fault-free and flawed cipher texts are used in the same assault. Additionally, the 128-bit secret key is found. The attacker need not be aware of the original data. Fault induction during the fifteenth encryption cycle is required for the more potent CLEFIA-discovered fault attack. It can be done using a brute-force search of about 20 bits and two sets of flawless and flawed cipher messages. The simulation results supported the accuracy of the assault mentioned above. The simulation results show that the assault may succeed in obtaining the 128-bit secret key after around a minute of operation. Given the complexity and input requirements, the attack is the most successful.

In [22], according to the author, L Block is a brand-new, lightweight cipher. Routine assaults on encryption plans are frustrated by L Block, including related-key assaults, differential cryptanalysis, straight cryptanalysis, and unimaginable differential cryptanalysis. 8-bit microcontrollers are one example of a hardware and software environment where the L Block may be successfully implemented.

In [23], the author subjected the 128-bit block cipher CLEFIA to impossible differential cryptanalysis. A 9-round unthinkable differential and the consequences of an unimaginable differential assault utilizing it were distributed in 2007 alongside the idea of CLEFIA. The creator guarantees that a 128-bit key might be utilized to send off an unimaginable differential assault against 12 rounds of CLEFIA. For key sizes of 192 bits and 256 bits, this attack is vulnerable to the 13-round and 14-round CLEFIA, respectively.

In [24], the author suggests that CLEFIA is a powerful yet lightweight cipher that offers sophisticated copyright protection and network authentication. Additionally, it is used in SSL and TLS-based secure communication protocols. Safeguarding it against differential shortcoming examination, which decreases the number of flaws and builds the fleeting intricacy of an assault, has been the subject of many reviews since its most memorable show in 2007. If one error is input during the last few rounds of the CLEFIA, this assault, which is quite adequate, enables the recovery of the whole secret key. The research presents an approach to finding vulnerabilities in the CLEFIA block cipher. When flaws were introduced as late as the last four rounds, their findings could still identify them at a low cost.

3. Performance Analysis and Results

This study presents an improved cryptographic algorithm with a reduced execution period. Improvements in execution speed are made in coding to achieve better results. The CLEFIA cipher is used for this purpose on an online c Compiler. The performance study of Enhanced Lightweight Cryptographic Algorithms based on energy consumption is described; for this purpose, MSP-EXP430FR5994 LaunchPad development kit [25] from Texas Instruments (TI) company is chosen.

3.1. Enhanced Execution Time

One of the crucial measures used to assess the effectiveness of CLEFIA block ciphers is the speed of the operation or execution time [26]. Results from a run on a laptop using Microsoft Visual Studio are presented in the seventh report. The execution took two milliseconds for a CLEFIA key size of 128 bits with 512 bytes of plain text.

3.1.1. Old CLEFIA Algorithm Execution Time

Table 1 shows the Execution time values obtained from the old CLEFIA Algorithm of research work, and that Figure 2 shows the variation in Execution time for different experiment trials.

Table 1. Execution time values obtained from the old CLEFIA algorithm

Experiment Trails	Value (sec)
1	0.000255
2	0.000306
3	0.000305
4	0.000317
5	0.000355
6	0.000343
7	0.000399
8	0.000341
9	0.000278
10	0.000257
Average	0.000316

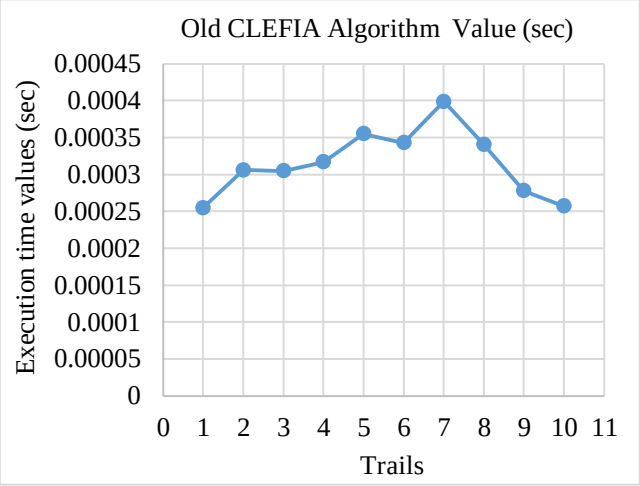

Fig. 2 Variation in execution time values for different trails

3.1.2. Enhanced CLEFIA Algorithm Execution Time Values

Table 2. Execution time values obtained from enhanced CLEFIA algorithm

Experiment Trails	Value (sec)
1	0.000151
2	0.000201
3	0.000183
4	0.000152
5	0.000144
6	0.000147
7	0.00017
8	0.000139
9	0.000217
10	0.000136
Average	0.000164

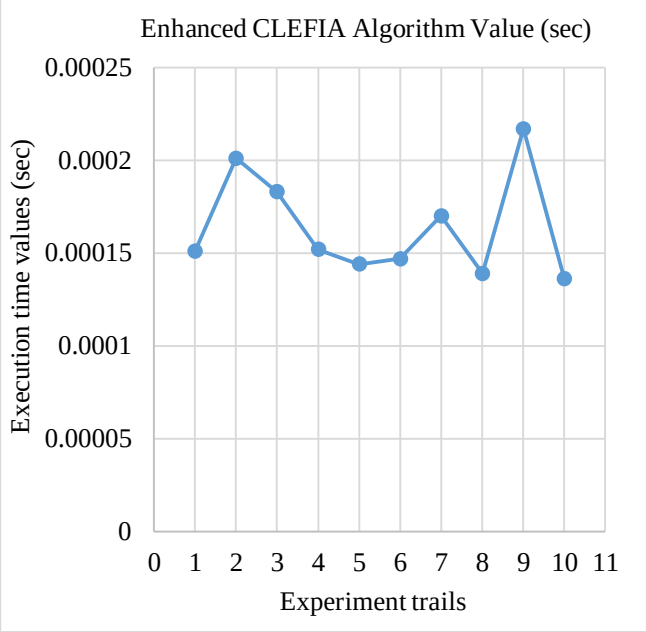

Fig. 3 Variation in execution time values for different trials by enhanced CLEFIA algorithm

3.1.3. Comparison of Old CLEFIA Algorithm and Enhanced CLEFIA Algorithm Execution Time Values

Table 3 shows the comparative time values for the execution of data by the Old CLEFIA algorithm and the enhanced CLEFIA algorithm. We take 10 experiment trials to test time Execution using the Old CLEFIA and enhanced CLEFIA algorithms.

Table 3. Comparison of old CLEFIA algorithm and modified CLEFIA algorithm execution time values

Experiment Trails	Enhanced CLEFIA Algorithm Values (sec)	Old CLEFIA Algorithm Values (sec)
1	0.000151	0.000255
2	0.000201	0.000306
3	0.000183	0.000305
4	0.000152	0.000317
5	0.000144	0.000355
6	0.000147	0.000343
7	0.00017	0.000399
8	0.000139	0.000341
9	0.000217	0.000278
10	0.000136	0.000257
Average	0.000164	0.000316

It is observed from Table 3 and Figure 3 that the Old CLEFIA algorithm takes more time for the execution of data as compared to the enhanced CLEFIA algorithm for enhanced time. Figure 4 represents the difference between the time Execution of the Old CLEFIA and the enhanced CLEFIA algorithm. The average time value of the Old CLEFIA algorithm is 0.000316 sec, and for the enhanced CLEFIA algorithm, it is only 0.000164 sec, almost 50 % less than the Old CLEFIA algorithm.

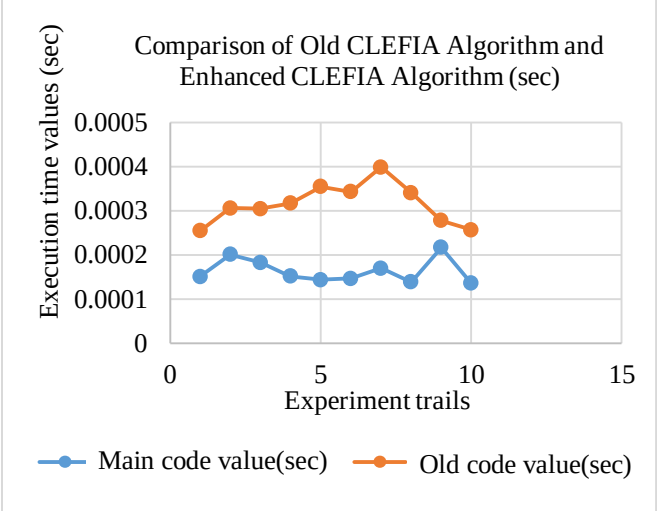

Fig. 4 Variation in execution time values for different experiment trials by the old CLEFIA algorithm and modified CLEFIA algorithm

The enhanced algorithm is executed on online c Complier "Programiz" with the same parameter and enhanced time with 0.158 milliseconds. (0.000158 seconds) as also shown in Table 3 and below Figure 5.

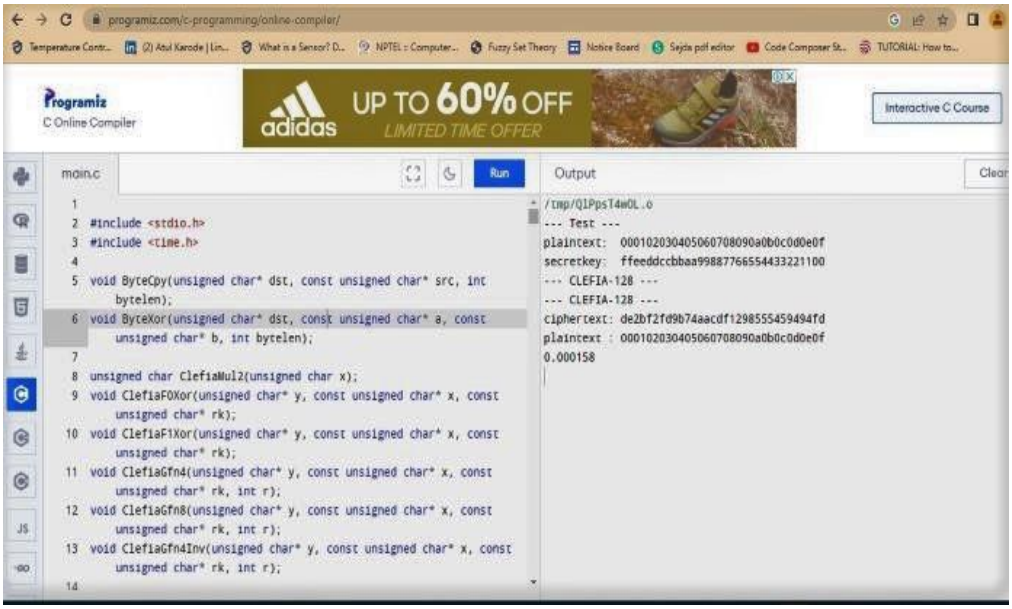

Fig. 5 Execution time for CLEFIA 128-bit key size with plain text 512 byte

3.2. Performance Analysis and Results on Enhanced CLEFIA Algorithm

CLEFIA is an AES-viable 128-bit block figure that additionally upholds 192-piece and 256-digit keys. CLEFIA comprises an information handling part and an essential booking part. CLEFIA utilizes a nonexclusive Block figure fabricated utilizing the Feistel structure, a symmetric structure with four data lines and a 32-bit width per data line.

From the MSP430 family, we chose the MSP-EXP430FR5994 LaunchPad Development Kit [28] for our investigation. Operating System: Windows 10 v.10.0 x86_64 / win32 Code Composer Studio Version: 11.0.0.00012Version 11.0.11 of Java

The MSP430FR5994 microcontroller runs C code developed in CCS to implement the compact improved CLEFIA algorithms. The energy, power, and current of the improved CLEFIA algorithms for 128-bit, 192-bit, and 256-bit key sizes were measured using Energy Trace software provided in CCS [23].

The Energy Trace technology, which measures and displays the energy needed for the application, is based on energy code analysis. Additionally, this technology aids in power consumption optimization. Code Composer Studio (CCS) incorporates the energy trace programme into its functionality. Figure 6 depicts the actual setup for Enhanced measurement [21].

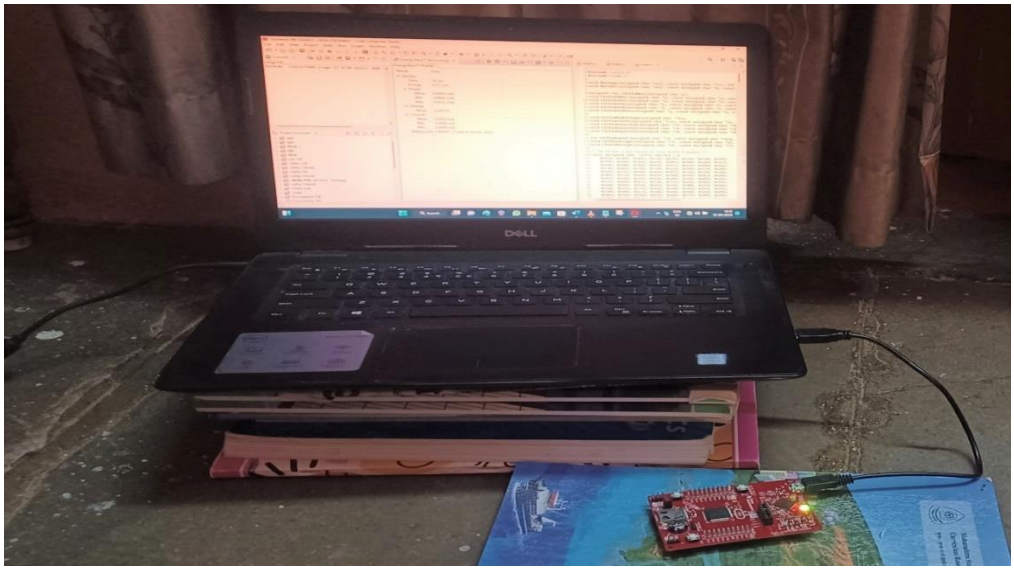

Fig. 6 Experiment set up for enhanced measurement

With the Energy-Trace mode and CCS, fundamental energy measurements are possible. The CPU routinely samples the input voltage to get a read on power consumption and energy use.

This mode allows you to test the application's power consumption without using the debugger. After monitoring the gadget for 10 seconds to record energy, power, and current statistics.

3.3. Measurement of Various Parameter of Enhanced CLEFIA 128 Block Cipher

The energy profile of the improved CLEFIA lightweight algorithm is assessed and shown using Energy Trace technology. This software aids in power consumption optimization as well. This programme operates in integrated mode within Code Composer Studio.

3.3.1. Energy Consumption

The energy trace technology simulation windows that display power and energy use are created. The device may display the mean power value and fluctuation in minimum and maximum modes.

This software also generates the electric parameters current and voltage, their mean values and maximum and minimum variation ranges.

Energy Consumption for Key Length 128

Energy consumption for improved CLEFIA 128 at 10 seconds of operation is 0.010mj (mill joule). Figure 7 is an actual measurement example.

Energy Consumption for Key Length 192

The energy consumed for enhanced CLEFIA 192 is 0.009 mj (mill joule) using it for a full 10 seconds before stopping.

Energy Consumption for Key Length 256

The energy consumed for enhanced CLEFIA 256 is 0.0011mj (mill joule) operating the device for 10 seconds.

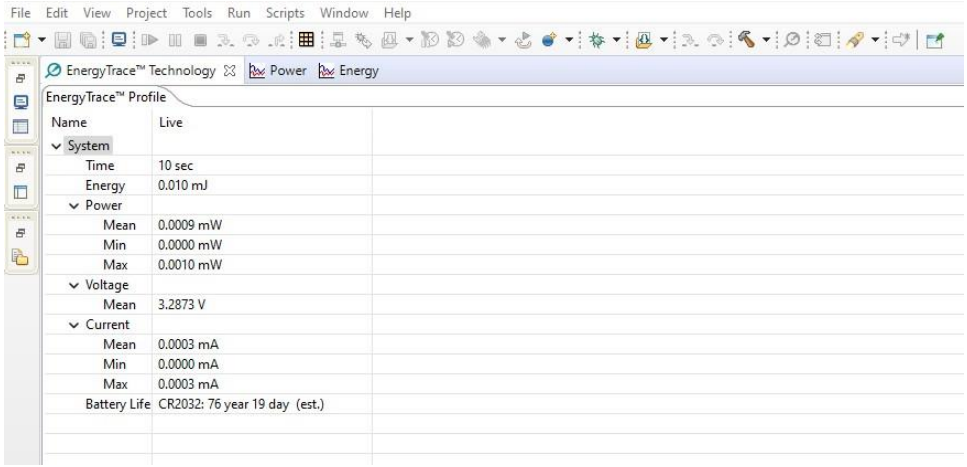

Fig. 7 Actual measurement for enhanced CLEFIA 128 using energy trace software

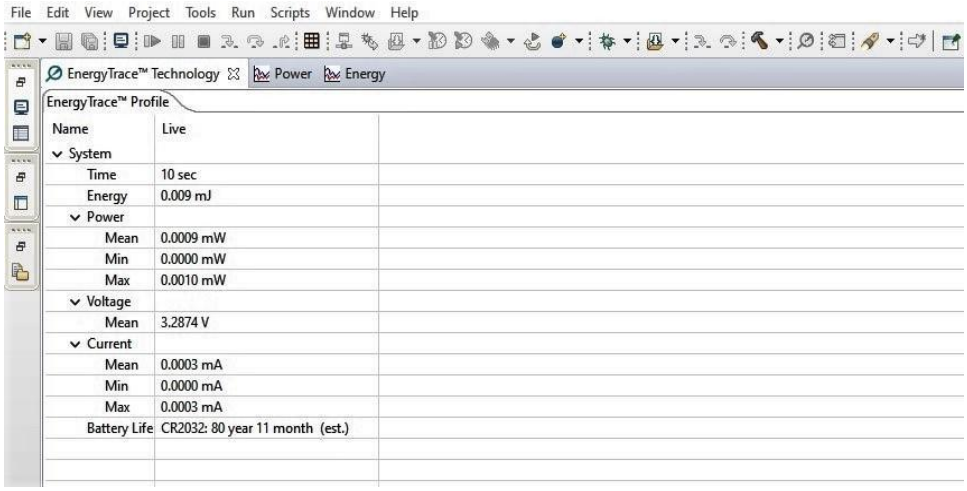

Fig. 8 Actual measurement for enhanced CLEFIA 192 using energy trace software

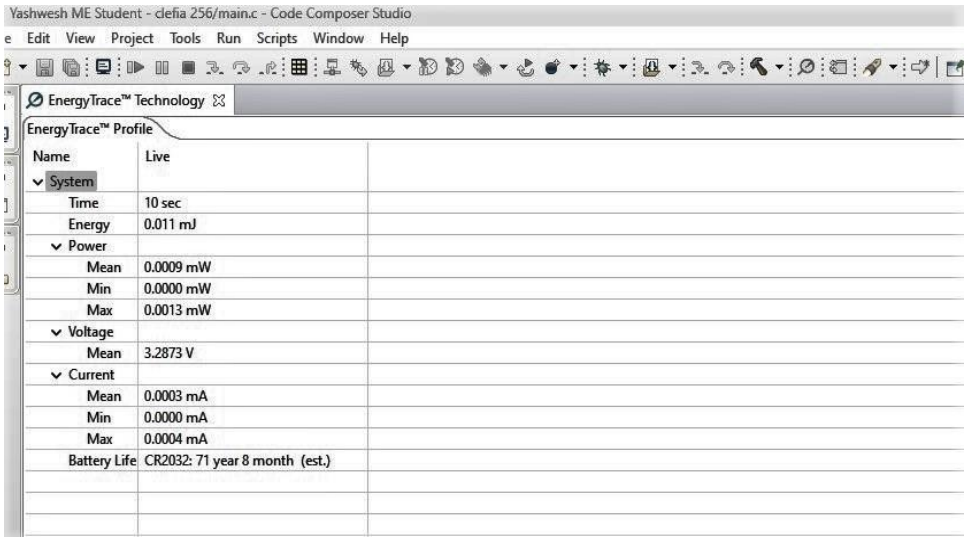

Fig. 9 Actual measurement for enhanced CLEFIA 256 using energy trace software

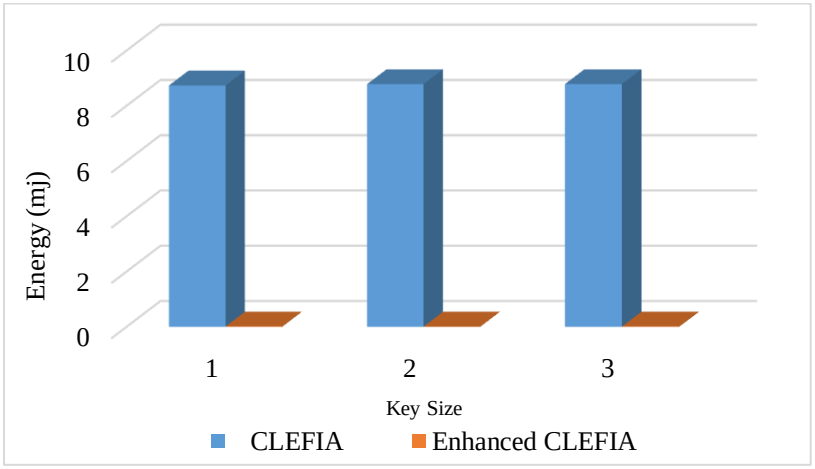

Fig. 10 Comparative analysis of energy consumption

Table 4 displays the results of a comparison between the energy usage of Enhanced CLEFIA 128 and that of CLEFIA 128.

3.4. Power Consumption

3.4.1. Power Consumption for Key Length 128

In Figure 7, the power consumed for Enhanced CLEFIA 128 is 0.0009 mw (milliwatt), operating the device for 10 seconds.

3.4.2. Power Consumption for Key Length 192

Referring to Figure 8, the power consumed for CLEFIA 192 is 0.0009 mw (milliwatt), operating the device for 10 seconds.

3.4.3. Power Consumption for Key Length 256

Referring to Figure 9, the power consumed for CLEFIA 256 is 0.0009 mw (milliwatt), operating the device for 10 seconds. Table 4 shows the results of a comparison of enhanced CLEFIA 128's power consumption.

Table 4. Comparative analysis of power consumption for enhanced CLEFIA 128

Block Length	Key Length	Number of Rounds	CLEFIA Power (mW)	Enhanced CLEFIA Power (mW)	Saved Power in mw
128	128	18	0.8653	0.0009	0.8644
128	192	22	0.8698	0.0009	0.8689
128	256	26	0.8703	0.0009	0.8694

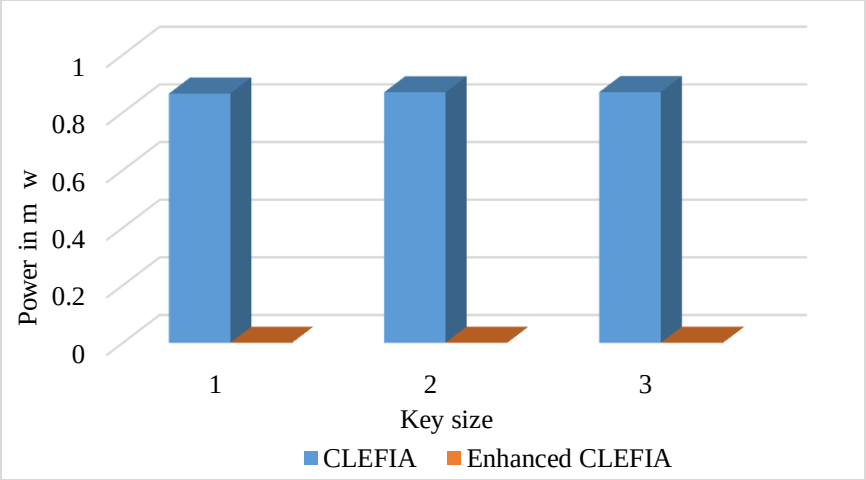

Fig. 11 Comparative analysis of power consumption

3.5. Voltage and Current Measurement

Various key sizes require various voltage and current measurements. Table 5 contains a comparative table for measuring voltage for different key sizes using figures 7, 8, and 9.

Table 5 shows no more effect on the voltage the device consumes while executing various key sizes in enhanced mode. Similarly, the Comparative measurement of current is shown in Table 6 for various key sizes. Referring to figures 7, 8, and 9.

Table 5. Comparison of measurement of voltage

Block Length	Key Length	Number of Rounds	Voltage (Mean)
128	128	18	3.2873
128	192	22	3.2873
128	256	26	3.2873

Table 6. Comparative analysis for measurement of current

Block Length	Key Length	Number of Rounds	CLEFIA Current (mA)	Enhanced CLEFIA	Saved Current (mA)
128	128	18	0.2633	0.0003	0.2630
128	192	22	0.2647	0.0003	0.2644
128	256	26	0.2648	0.0003	0.2645

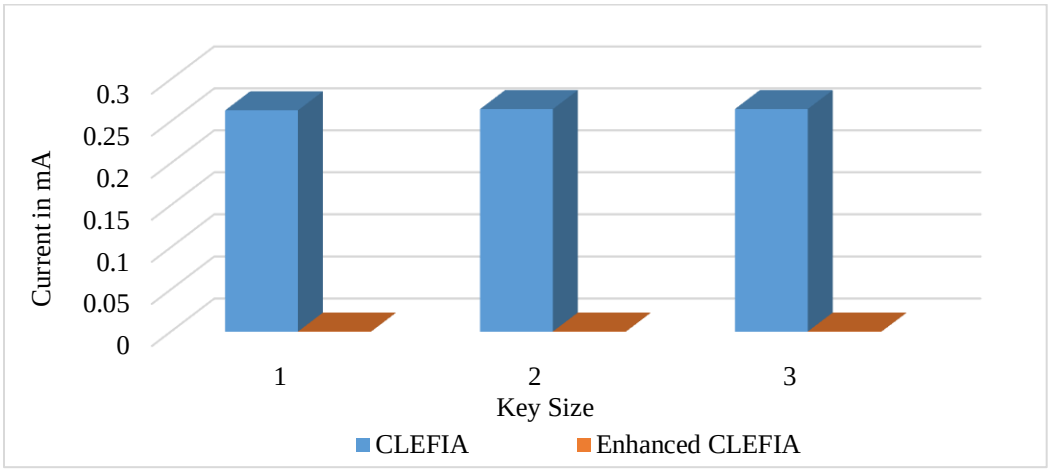

Fig 12. Comparative analysis for measurement of current

3.6. Estimated Battery Life

Table 7 lists the device's operating capacity and expected battery life for the CR 2032 battery. A CR 2032 battery is a primary lithium coin or button cell that is 20mm in diameter and 3.2mm thick. It is not rechargeable. It features a 3-volt voltage and a 240 mAh capacity. Regarding Figures 7, 8, and 9, the Comparative table for estimated Battery Life for different key size is provided in Table 7.

Table 7. Comparative analysis of energy consumption for CLEFIA 128 with enhanced CLEFIA

Block Length	Key Length	Number of Rounds	CLEFIA Battery Life (CR 2032) Estimated Lithium Coin or Button Cell Battery	Enhanced CLEFIA Battery Life (CR 2032) Estimated Lithium Coin or Button Cell Battery
128	128	18	1 month 1 day	76 Years 19 Months
128	192	22	1 month 21 hours	80 Years 11 Months
128	256	26	1 month 20 hours	71 Years 8 Months

Thus, a CR 2032 lithium coin or button cell battery may power the gadget. Batteries 76 Years 19 Months for the key length of 128, 80 Years 11 Months for the key length of 192 and 71 Years 8 Months for 256, respectively.

4. Conclusion

This paper proposes a small hardware architecture for computing the CLEFIA block cipher algorithm that can conduct essential expansion for all key sizes as well as data time execution is proposed. This study shows how the abilities of the FPGA innovation, for example, addressable shift registers and Slam blocks, might be utilized in developing the different branches of the Feistel organization.

According to experimental findings, the updated CLEFIA algorithm executes data in around 50% less time than the original CLEFIA algorithm. According to Table 3, the enhanced algorithm executes time on average in 0.000154 mini seconds, less time than the old CLEFIA Algorithm. In contrast, the old code executes time on average in 0.000316 mini seconds. Based on the obtained improved findings, it can be said that the suggested CLEFIA algorithm's parameters, such as energy consumption, power consumption, voltage, current, and anticipated battery life, have been greatly enhanced.

As stated in the synopsis, The goal of improving CLEFIA, a lightweight cryptographic algorithm with low power consumption, has been achieved. Every performance parameter, except voltage, has improved compared to the results from the previous execution.

Standard cryptography method's speed, size, and energy consumption can be very high for restricted systems. RFID tags and WSN are frequently cited as instances of lightweight cryptography, which is commonly described as encryption for resource-constrained devices. The suggested upgraded algorithm consumes very little energy and power and requires little time for encryption and decryption, making it an energy-efficient approach for light networks.

References

[1] Taizo Shirai et al., "The 128-Bit Blockcipher CLEFIA (Extended Abstract)," *Fast Software Encryption*, pp. 181-195, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[2] Takeshi Sugawara et al., "High-Performance ASIC Implementations of the 128-Bit Block Cipher CLEFIA," *2008 IEEE International Symposium on Circuits and Systems*, Seattle, WA, USA, pp. 2925-2928, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[3] Paulo Proenca, and Ricardo Chaves, "Compact CLEFIA Implementation on FPGAs," *2011 21st International Conference on Field Programmable Logic and Applications*, Chania, Greece, pp. 512-517, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[4] Simon Heron, "Advanced Encryption Standard (AES)," *Network Security*, vol. 2009, no. 12, pp. 8-12, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[5] Ari Juels, and Stephen A. Weis, "Authenticating Pervasive Devices with Human Protocols," *Advances in Cryptology - CRYPTO*, pp. 293-308, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[6] Amir Moradi et al., "Pushing the Limits: A Very Compact and a Threshold Implementation of AES," *Advances in Cryptology – EUROCRYPT*, pp. 69-88, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[7] Tomasz Kryjak, and Marek Gorgon, "Pipeline Implementation of the 128-Bit Block Cipher CLEFIA in FPGA," *2009 International Conference on Field Programmable Logic and Applications*, Prague, Czech Republic, pp. 373-378, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[8] João Carlos Resende, and Ricardo Chaves, "Dual CLEFIA/AES Cipher Core on FPGA," *Applied Reconfigurable Computing*, Bochum, Germany, pp. 229-240, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[9] Daniel Engels et al., "The Hummingbird-2 Lightweight Authenticated Encryption Algorithm," *RFID. Security and Privacy*, pp. 19-31, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[10] Ahssan Ahmed Mohammed, and Abdulkareem O. Ibad, "A Proposed Non Feistel Block Cipher Algorithm," *Qalaai Zanist Journal*, vol. 2, no. 2, pp. 72-82, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Ray Beaulieu et al., "The SIMON and SPECK Families of Lightweight Block Ciphers," *Cryptology ePrint Archive*, 2013. [Google Scholar] [Publisher Link]

[12] Kyoji Shibutani et al., "Piccolo: An Ultra-Lightweight Blockcipher," *Cryptographic Hardware and Embedded Systems - CHES 2011*, pp. 342-357, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[13] Tomoyasu Suzaki et al., "Twine: A Lightweight, Versatile Block Cipher," *ECRYPT Workshop on Lightweight Cryptography*, 2011. [Google Scholar] [Publisher Link]

[14] Roger M. Needham, and David J. Wheeler, "*Tea Extensions*," Cambridge University, 1997. [Google Scholar] [Publisher Link]

[15] Joan Daemen, and Vincent Rijmen, *AES Proposal: Rijndael*, The Rijndael Block Cipher, pp. 1-45, 1999. [Google Scholar] [Publisher Link]

[16] A. Bogdanov et al., "PRESENT: An Ultra-Lightweight Block Cipher," *Cryptographic Hardware and Embedded Systems - CHES 2007*, pp. 450-466, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[17] B. Akhil et al., "Light Weight Security Coding using PRESENT Algorithm for Cryptography Application," *SSRG International Journal of VLSI & Signal Processing*, vol. 7, no. 2, pp. 1-5, 2020. [CrossRef] [Publisher Link]

[18] Chae Hoon Lim, and Tymur Korkishko, "mCrypton-a Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors," *Information Security Applications*, pp. 243-258, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[19] Toru Akishita, and Harunaga Hiwatari, "Very Compact Hardware Implementations of the Block Cipher CLEFIA," *Selected Areas in Cryptography*, pp. 278-292, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[20] Nicolas Sklavos et al., "Efficiency of Cryptography for Multi-Algorithm Computation on Dedicated Structures," *4th International Conference on Modern Circuits and Systems*, 2015. [Google Scholar] [Publisher Link]

[21] S. K. Subidh Ali, and Debdeep Mukhopadhyay, "Protecting Last Four Rounds of CLEFIA is not Enough against Differential Fault Analysis," *Cryptology ePrint Archive*, 2012. [Google Scholar] [Publisher Link]

[22] Wenling Wu, and Lei Zhang, "LBlock: A Lightweight Block Cipher," *Applied Cryptography and Network Security*, pp. 327-344, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[23] Jongsung Kim et al., "Impossible Differential Cryptanalysis for Block Cipher Structures," *Progress in Cryptology – INDOCRYPT*, pp. 82-96, 2003. [CrossRef] [Google Scholar] [Publisher Link]

[24] Wei Li et al., "Fault Detection on the Software Implementation of CLEFIA Lightweight Cipher," *Journal of Networks*, vol. 7, no. 8, pp. 1288-1294, 2012. [Google Scholar] [Publisher Link]

[25] Bora Aslan, Fusun Yavuzer Aslan, and M. Tolga Sakalli, "Energy Consumption Analysis of Lightweight Cryptographic Algorithms that Can be Used in the Security of Internet of Things Applications," *Security and Communication Networks*, vol. 2020, pp. 1-15, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[26] Mohammad Kamrul Hasan et al., "Lightweight Cryptographic Algorithms for Guessing Attack Protection in Complex Internet of Things Applications," *Complexity*, vol. 2021, pp. 1-13, 2021. [CrossRef] [Google Scholar] [Publisher Link]