Sādhanā (2022)47:213
https://doi.org/10.1007/s12046-022-01994-0

Hardware-software co-design framework of lightweight CLEFIA cipher for IoT image encryption

PULKIT SINGH[1], K ABHIMANYU KUMAR PATRO[2], RAHUL KUMAR CHAURASIYA[3] and BIBHUDENDRA ACHARYA[1,*]

[1]Department of Electronics and Communication Engineering, National Institute of Technology Raipur, G. E. Road, Raipur, Chhattisgarh 492010, India
[2]Department of Mechatronics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Karnataka 576104, India
[3]Department of Electronics and Communication Engineering, Maulana Azad National Institute of Technology, Bhopal, Madhya Pradesh 462003, India
e-mail: pksingh.phd2015.elx@nitrr.ac.in; abhimanyu.patro@gmail.com; rkchaurasiya@manit.ac.in; bacharya.etc@nitrr.ac.in

MS received 23 May 2022; revised 28 August 2022; accepted 5 September 2022

Abstract. Internet of things (IoT) connects a huge number of small devices across a network. End-to-end security is becoming highly crucial as IoT deploys these devices. In this paper, two hardware architectures for CLEFIA cipher are proposed that are capable of providing robust security to encrypt image input under resource-constrained IoT applications. The proposed round-based and pipelined implementations yield better throughput for high-speed applications. In addition, the proposed round-based and pipelined architectures improve maximum operating frequency by 52.95% and 117.22% for Artix-7 FPGA family. The ASIC implementation results show a 39.22% and 51.92% improvement in hardware efficiency over state-of-the-art design, respectively. Moreover, these proposed architectures have been utilized to encrypt images by selecting variable tile sizes along with the control unit. This paper also explores the security of images encrypted by the proposed hardware architecture of the CLEFIA cipher. The existing solutions were compared to correlation coefficients, NPCR, UACI, MSE, PSNR and entropy values.

Keywords. IoT; lightweight cryptography; low resource devices (LRDs); hardware implementation; CLEFIA.

1. Introduction

Now a days, IoT technology is advancing fast and allowing a huge number of resource-constrained devices to connect each other through internet. In order to meet at specific application requirements of IoT and cyber physical systems (CPS) many of constrained devices are deployed as the most challenging issues in privacy and security. Such devices are not designed with security features. In addition, these devices have a number of challenges, including power and area limitations, as well as higher speed and performance at a reduced cost. As data security requirements become more stringent, there is a growing demand for cipher solutions for LRDs. Given these LRDs' constraints, an optimal encryption implementation is required in terms of area, power, and speed [1].

Traditional crypto, such as AES block cipher, and others, have been widely used mostly for securing remote distributed communication. These ciphers do not meet the requirements for low-power devices, emphasizing the significance of lightweight crypto primitives. The majority of well-known lightweight ciphers lack the security level required for post-quantum applications, as well as adequate green information technology) (Green IT) features.

The various block ciphers such as PRESENT and CLEFIA are well known for their security and implementations. These ciphers have been specified in ISO/IES 29192-2 and can be used in real-world applications [2]. CLEFIA has sufficient crypto primitives like key length and block size, and can fulfill the requirements for power consumption and hardware area for secured limited resources [3]. Even through, hardware implementations of various lightweight block ciphers have been designed comprehensively on FPGA and/or ASIC platforms. The future direction of this work is that the modification and resource optimization are still an interesting challenge for these lightweight ciphers.

*For correspondence
Published online: 26 October 2022

The following are the main contributions made by this paper:

- To develop two hardware architectures of CLEFIA cipher for the encryption of images.
- To implement these proposed architectures on Xilinx FPGA & Design Compiler ASIC platforms and compare the implementation results with existing designs.
- To perform encryption of input images by selecting different tile sizes which are controlled by a controller in the top-level module.
- To analyze security of encrypted images by analyzing different statistical and differential attacks and compare these analyses with existing works.

The rest of the paper is divided into the following sections. Section 2 presents the proposed hardware architectures of the CLEFIA cipher. Section 3 discusses the outcomes of hardware implementation and compares the performance with existing designs. Security analysis is evaluated in section 4. Finally, concluding remarks are given in section 5.

2. Methodology and proposed hardware architectures

SHA-256 algorithm is used to generate 128-bits key for CLEFIA key scheduling algorithm firstly. After input key generation, input data (image) and generated key are passed through proposed hardware architectures of CLEFIA cipher. For smooth operation of the proposed designs, a control unit provides important signals to select different tile sizes of input image such as 32x32, 64x64, 128x128, and 256x256. Table 1 shows the control signal used for the selection of different tile sizes during the encryption algorithm. The output control signal of the controller writes output ciphertext at different locations in the memory as shown in figure 1. After the encryption of the image, encrypted image generated from RTL has transformed into MATLAB platform for security analysis.

2.1 *Proposed round-based architecture (D1)*

The two sections in the proposed CLEFIA architecture are namely, round transformation section and the round key generation section. Initially, twelve of the thirty locations are used to generate the intermediate key *L_out* from

Table 1. Control signal for selection of image size.

2-bit control	00	01	10	11
Pixel values	32 × 32	64 × 64	128 × 128	256 × 256

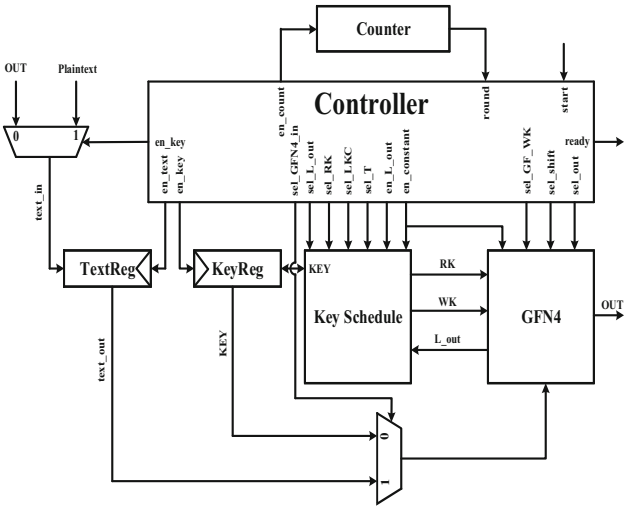

Figure 1. Top module of CLEFIA encryption algorithm.

128-bit master key *K* generated from SHA-256 algorithm as shown in figure 2. The round transformation block handles the input key and constants by passing via multiplexers M_3 and M_4 and taking them as inputs. At the end of twelve clock cycles, the multiplexer M_9 transmits the intermediate key *L_out*. To extract constants from memory, a 5-bits round counter counts the number of clock pulses for eighteen-round encryption, and generates the control signals needed for intermediate key and subkey generation. By using 5-bits round counter, it is possible to synchronize the key constant values and the encryption rounds by using remaining eighteen 64-bit constant values in encryption rounds. The double swap block shifts intermediate key *L_out* in key scheduling algorithm.

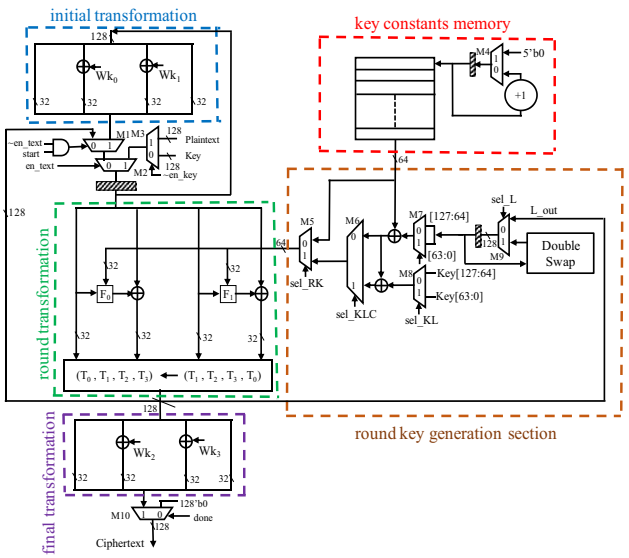

Figure 2. Proposed round-based architecture of CLEFIA cipher.

The round transformation operation is accomplished by raising the *start* signal high for one clock pulse and directly storing the initial transformed data into the register. Once the round transformation operation is completed, the intermediate values are stored in the same register. The *done* signal becomes high at the end of number of encryption clock cycles. Then, the final transformed data, known as ciphertext, is passed by multiplexer M_{10}.

2.2 *Proposed pipelined architecture (D2)*

Some RFID readers prefer high speed in order to read a large number of devices. A pipelined architecture is a technique for implementing the design for high-speed applications with the highest possible throughput. When registers are used in the critical path delay, the maximum operational clock frequency of the device can be achieved. As a result, parallel systems with pipelined architecture achieve high throughput rates that are helpful for high-speed RFID tag applications.

The pipelined architecture uses a 64-bit pipeline register (shown as a dotted thick blue rectangular box) to increase the throughput of the proposed design. The round key values are transmitted through pipelined register on next positive edge clock, causing a one-clock cycle delay. An AND gate with two input signals *en_text* and *start*, together with the use of multiplexer M_1 is utilized to synchronize the first transformed data with the round key generating block as shown in figure 3. Therefore, round key values favour the round function. Consequently, the number of flip-flops in the FPGA Virtex-5 LX30 device has been increased from 426 to 491, meaning a 15.26% increase in area over round-based design, and the frequency is increased from 188.50 MHz to 245.60 MHz, implying a 30.29% increase in the maximum operating frequency. The final transformation block is integrated with round transformation block when the counter reaches the last encryption round of cycle.

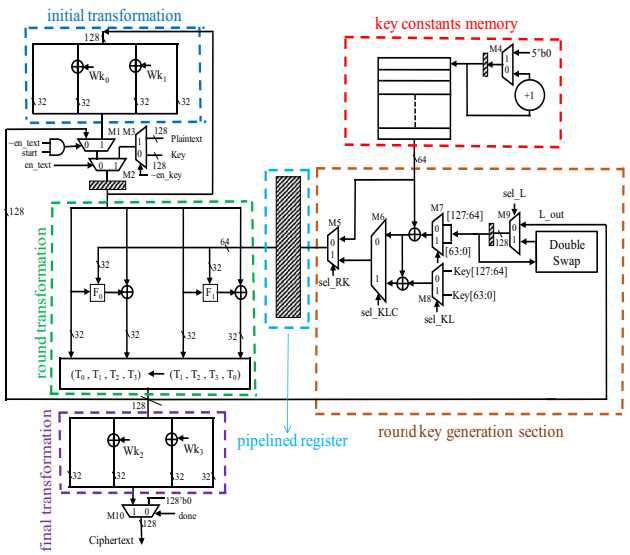

Figure 3. Proposed pipelined architecture of CLEFIA cipher.

3. Hardware implementation results and discussions

This sub-section evaluates the results on FPGA and ASIC hardware platforms. Results of several state-of-the-art and proposed architectures implemented on FPGA platform are tabulated in table 2. Compared to state-of-the-art CLEFIA architectures like [4, 5] and [6], the proposed pipelined implementation achieves better results in terms of maximum operating frequency for Virtex-4 and Artix-7 families. For Spartan-3E and Virtex-5 families, pipelined implementation also provides higher results in terms of maximum frequency than earlier reported CLEFIA architectures like [4, 5, 7]. The throughput parameter is also good, and it is higher for the same FPGA family. However, the number of slices is smaller in comparison with the earlier reported CLEFIA architectures like [4, 6]. The proposed pipelined design is able to generate first ciphertext in eighteen clock cycles. Thus, the high throughput achieved by pipelined architecture increases the processing speed for high-speed applications.

As demonstrated in table 2 for the same FPGA family, the proposed round-based solution exhibits good results with regard to hardware parameters. From table 2, it can be seen that the number of slices for the proposed round-based design is lower than that of the earlier reported CLEFIA architectures like [4, 7] for same FPGA family. Hence, this design achieves a higher throughput per area efficiency than the state-of-the-art designs, which shows the right balance between speed and area footprint consumption.

Table 3 shows the implementation results of CLEFIA cipher and proposed CLEFIA architectures on an ASIC platform. The results of the proposed architectures have been compared with those of earlier reported architectures such as CLEFIA [3], CLEFIA [4]. The comparison is based on several hardware metrics, such as area in GE and speed in throughput. Figure 4 illustrates the throughput/area comparison of earlier reported CLEFIA architectures with the proposed architectures. In terms of hardware efficiency, the proposed architectures provide good throughput/area. In addition, the round-based and pipelined implementations enhance hardware efficiency by 39.22% and 51.92%, respectively, compared to the state-of-the-art CLEFIA cipher [3].

4. Security analysis

In this paper, the encrypted images are used for security analysis in MATLAB platform. All the images are taken from the "USC-SIPI Image" [10] and "Cancer Imaging Archive (TCIA)" [11] databases. To validate the security

Table 2. Comparison of FPGA implementation results.

Algorithms	Devices	Slices	Max freq. [MHz]	Thr* [Mbps]
CLEFIA [4]	Virtex 4	14069	146.00	1038.22
CLEFIA [4]	Virtex 5	2845	167.00	1187.56
CLEFIA [5]	Spartan 3E	624	108.00	768.00
CLEFIA [5]	Virtex 4	625	179.00	1273.00
CLEFIA [5]	Virtex 5	170	240.00	1707.00
CLEFIA [7]	Virtex-5	267	267.00	742.96
CLEFIA [6]	Artix-7	506	147.00	990.00
This work(D1)	Virtex 4	1222	122.59	871.75
This work (D1)	Virtex 5	538	188.50	1340.44
This work(D1)	Spartan 3E	1086	65.51	465.85
This work(D1)	Artix-7	427	224.84	1598.86
This work(D2)	Virtex 4	1274	187.48	1333.19
This work(D2)	Virtex 5	667	245.60	1746.49
This work(D2)	Spartan 3E	1154	108.11	768.78
This work(D2)	Artix-7	489	319.32	2270.72

Thr* = Throughput

Table 3. Comparison of ASIC implementations results.

Algorithms	Area [Kgates]	Max freq. [MHz]	Throughput [Mbps]
CLEFIA [4]	–	746.27	663.35
CLEFIA [8]	10.38	362.32	2576.49
CLEFIA [3]	5.98	225.83	1605.94
CLEFIA [3]	4.95	201.28	715.69
CLEFIA [9]	2.68	–	73 Kbps*
This work(D1)	5.88	309.14	2198.33
This work(D2)	6.93	397.87	2829.31

*Throughput@100KHz

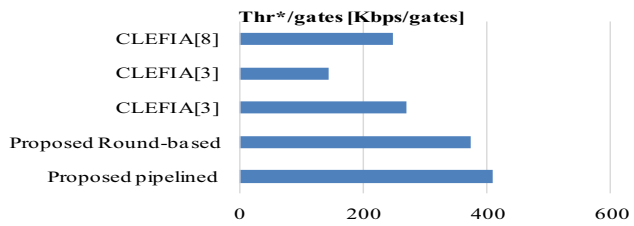

Figure 4. Throughput/ area comparison for proposed implementations of CLEFIA cipher on ASIC platform.

against attacks, key space, adjacent pixel correlation, differential attack, MSE and PSNR, and information entropy analyses are evaluated and analyzed.

4.1 *Key space analysis*

The following are the keys utilized in the proposed architecture of CLEFIA cipher algorithm:

- 128-bits key in CLEFIA encryption algorithm
- Hash values of SHA-256 hash algorithm

In the proposed architecture, CLEFIA cipher has used the key length of 128-bits, so the key space is 2^{128}. For SHA-256 hash algorithm, the key space is 2^{128}. As a result, the proposed architecture's total key space is $2^{128} \times 2^{128} = 2^{256}$, which is larger than 2^{128} to successfully secure against brute-force attack. Table 4 compares the proposed architectures with the architectures of other referred algorithms in terms of total key space results [12–14].

4.2 *Adjacent pixel correlation analysis*

Table 5 demonstrates comparison of correlation results between the algorithm in References [12, 14] for gray-level and colour images. The following observations are found:

Table 4. Comparison of key space results.

Architectures		Total key space 2^{256}
Proposed	CLEFIA cipher	
Mishra *et al* [12]	LEA cipher	2^{128} or 2^{192} or 2^{256}
Mishra and Acharya [13]	SIT cipher	2^{64}
Jangir and Pandey [14]	GIFT cipher	2^{128}

- Using the proposed approach, the correlation values of encrypted gray-level and colour images are nearly equal to 0 in all three directions. In encrypted images, this illustrates the weak correlation between adjacent pixels.
- In comparison to the algorithm of References [12, 14] in gray-level images and Reference [14] in colour images, the correlation values of the encrypted images utilizing by the proposed approach are close to 0. It shows that the proposed approach performs weak correlation of neighboring encrypted.

4.3 *Information entropy analysis*

The entropy results of the proposed approach are compared with the algorithm of References [12–14] and Reference [14] in table 6 and 7, respectively. All of the algorithms have entropies close to the ideal value of 8. This means that the proposed approach, as well as those in References [12–14], effectively withstand the entropy attack.

4.4 *Differential attack analysis- NPCR and UACI*

Tables 8 and 9 compare the average NPCR and UACI results of gray-level and colour images, respectively using the proposed technique to the algorithm of References [13, 14]. The NPCR and UACI of the gray-level images and red (R), green (G), blue (B) components of the colour images using the proposed approach are almost equal than the algorithms of References [13, 14].

Table 6. Comparison of information entropy for gray-level images.

Architectures		Images	encrypted images
Proposed	CLEFIA cipher	Moon surface	7.99
		Clock	7.99
		Pelvic	≅8.00
		Kidney	≅8.00
[12]	LEA	Moon surface	≅8.00
		Clock	≅8.00
[13]	SIT	Pelvic	7.99
		Kidney	7.99
[14]	GIFT	Moon surface	8.00
		Clock	8.00

Table 7. Comparison of information entropy for colour images.

Images	Proposed algorithm	GIFT [14]
Tree	7.99	8.00
Female	7.99	8.00

Table 8. Comparison of NPCR and UACI for gray-level images.

Architectures		Images	NPCR (%)	UACI (%)
Proposed	CLEFIA cipher	Moon surface	99.6123	33.8559
		Clock	99.6142	33.9209
		Pelvic	99.6096	34.1754
		Kidney	99.6122	33.4732
[13]	SIT	Pelvic	99.6110	37.2240
		Kidney	99.6450	38.6800
[14]	GIFT	Moon surface	98.7900	39.9900
		Clock	99.6700	36.4800

4.5 *MSE and PSNR analysis*

Tables 10 and 11 compare the PSNR and MSE results of gray-level and colour images, respectively using the

Table 5. Comparative results of correlation coefficient for gray-level images.

	Gray-level images				Colour images			
	Proposed scheme		LEA [12]	GIFT [14]	Proposed scheme		GIFT [14]	
Components	Leena	Clock	Leena	Clock	Tree	Female	Tree	Female
Horz.	0.0055	0.0004	− 0.0055	0.003	− 0.0011	0.0033	0.002	0.002
Vert.	− 0.0010	0.0020	− 0.0021	0.002	− 0.0012	− 0.0020	0.002	0.002
Diag.	0.0018	− 0.0018	0.0091	0.002	0.0024	0.0007	− 0.002	0.022

Table 9. Comparison of NPCR and UACI for colour images.

	Proposed algorithm		GIFT [14]	
Images	NPCR (%)	UACI (%)	NPCR (%)	UACI (%)
Tree	99.62	33.83	99.89	38.96
Female	99.62	33.83	99.85	38.90

Table 10. Comparison of MSE and PSNR for gray-level images.

Architectures		Images	MSE	PSNR
Proposed	CLEFIA cipher	Moon surface	6235.90	10.18
		Clock	12321.00	7.22
[14]	GIFT	Moon surface	6233.29	10.18
		Clock	12195.95	7.26

Table 11. Comparison of MSE and PSNR for colour images.

	Proposed algorithm		GIFT [14]	
Images	Avg. PSNR	Avg. MSE	PSNR	MSE
Tree	8.16	9999.53	8.70	5928.30
Female	8.89	8544.40	8.82	6012.32

proposed technique to the algorithm of Reference [14]. The PSNR and MSE of the gray-level and *R*, *G*, *B* components of the colour images using the proposed approach are better than the algorithm of Reference [14].

4.6 *Known-plaintext attack (KPA) and chosen-plaintext attack (CPA) analysis*

The proposed algorithm is highly resistant to both attacks i.e., KPA and CPA. The generated keys for proposed architectures are not only related to the specified key values, but also to the plain images using the hash values obtained by the SHA-256 hash algorithm. As a result, for each input of original images, keys are modifying. Consequently, attackers cannot obtain useful information by encrypting some chosen images because the encrypted output is limited to those images.

5. Conclusion

In this paper, two hardware architectures of CLEFIA block cipher are proposed and examined the security analyses for image encryption applications. The proposed round-based architecture showed good trade-off between area and speed whereas pipelined architecture yielded high throughput that improved the processing speed. When compared to other CLEFIA architectures, the proposed architectures maintained higher hardware efficiency and provided high throughput. In order to encrypt images, controller is designed in such a way that can solve the image boundary problem. SHA-256 algorithm is used to generate the input key for the proposed hardware architectures. The proposed architectures are thus effectively protected against KPA and CPA. In addition, this method of key generation gives a high level of security against brute-force attacks. This confirms the strong resistance against various statistical and differential attacks.

References

[1] Kumar V G K and Rai C S 2021 Design and analysis of novel BRISI lightweight cipher for resource constrained devices. *Microprocess. Microsyst.* 84(104267): 1–10

[2] ISO/IEC 29192-2:2012 Information technology—Security techniques—Lightweight cryptography—Part 2: Block ciphers. https://www.iso.org/standard/56552.html

[3] Shirai T, Shibutani K, Akishita T, Moriai S and Iwata T 2007 The 128-bit blockcipher CLEFIA. In: *International Workshop on Fast Software Encryption*, Berlin: Springer, pp. 181–195

[4] Kryjak T and Gorgon M 2009 Pipeline implementation of the 128-bit block cipher CLEFIA in FPGA. In: *2009 International Conference on Field Programmable Logic and Applications*, pp. 373–378

[5] Chaves R 2013 Compact CLEFIA implementation on FPGAs. In: *Embedded Systems Design with FPGAs*, New York: Springer, pp. 225–243

[6] Cheng X, Zhu H, Xu Y, Zhang Y, Xiao H and Zhang Z 2021 A reconfigurable and compact hardware architecture of CLEFIA block cipher with multi-configuration. *Microelectronics J.* 114(105144): 1–8

[7] Hanley N and ONeill M 2012 Hardware comparison of the ISO/IEC 29192-2 block ciphers. In: *2012 IEEE Computer Society Annual Symposium on VLSI,* pp. 57–62

[8] Sugawara T, Homma N, Aoki T and Satoh A 2008 High-performance ASIC implementations of the 128-bit block cipher CLEFIA. In: *2008 IEEE International Symposium on Circuits and Systems*, pp. 2925–2928

[9] Akishita T and Hiwatari H 2012 Very compact hardware implementations of the blockcipher CLEFIA. In: *International Workshop on Selected Areas in Cryptography*, Berlin: Springer, pp. 278–292

[10] USC-SIPI. http://sipi.usc.edu/database/ (1977)

[11] Clark K, Vendt B, Smith K, Freymann J, Kirby J, Koppel P, Moore S, Phillips S, Maffitt D, Pringle M and Tarbox L 2013 The cancer imaging archive (TCIA): maintaining and operating a public information repository. *J. Digit. Imaging.* 26: 1045–1057

[12] Mishra Z, Nath P K and Acharya B 2020 High throughput unified architecture of LEA algorithm for image encryption. *Microprocess. Microsyst.* 78(103214): 1–10

[13] Mishra Z and Acharya B 2020 High throughput and low area architectures of secure IoT algorithm for medical image encryption. *J. Inf. Secur. Appl.* 53(102533): 1–15

[14] Jangir A and Pandey J G 2021 GIFT cipher usage in image data security: hardware implementations, performance and statistical analyses. *J. Real-Time Image Process.* 18: 2551–2567