I. J. Computer Network and Information Security, 2019, 12, 10-16
Published Online December 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.12.02

Design and Implementation of Runtime Reconfigurable Encryption Algorithms using Custom ICAP Processor

Jamuna S
DayanandaSagar College of Engineering, Bengaluru, India
E-mail:jamuna-ece@dayanandasagar.edu

Dinesha P
DayanandaSagar College of Engineering, Bengaluru, India
E-mail:drdinesh-ece@dayanandasagar.edu

K PShashikala
DayanandaSagar College of Engineering, Bengaluru, India
E-mail:shashikala-ece@dayanandasagar.edu

Kishore Kumar K
DayanandaSagar College of Engineering, Bengaluru, India
E-mail:kishorekalluri8@gmail.com

Received: 27 August 2019; Accepted: 16 October 2019; Published: 08 December 2019

***Abstract*—**Field programmable gate arrays (FPGAs) are the reconfigurable logic devices which are widely used in many applications like space missions, automotive electronics, complex computing systems and system prototyping. Run time reconfigurability feature supported in high end FPGAs allows the designer to optimize design with respect to resource utilization and power consumption. Using partial reconfiguration a specific part of the FPGA can be reconfigured at run time without altering the original design. In data communication, safety and confidentiality of data is achieved through a suitable encryption algorithm. Encryption is most important aspect when it comes to security. Design flexibility can be increased by providing an option to the user to select a particular algorithm as per the requirement. Instead of using a single algorithm to encrypt data, multiple algorithms can be used with an option to switch between the algorithms. Thus optimizing the resource utilization and also can avoid security breach. Through this work, an attempt is made to include reconfiguration of the design at run-time. This design implements different encryption algorithms at different instance of time. In this paper two encryption algorithms i.e. Advance Encryption Standard (AES) and TwoFish both of 128-bit are chosen to reconfigure at runtime using a custom ICAP (Internal Configuration Access Port) controller IP provided by Xilinx and is implemented on Zedboard. Main advantage of this implementation is that the user have an option to switch between two algorithms, thus helping in overall resource optimization.

***Index Terms*—**Encryption, *FPGA, ICAP Processor*, Partial Reconfiguration.

I. Introduction

Field Programmable Gate Arrays (FPGAs) are gaining importance because of the advantages they offer. They are flexible to implement any type of design.IP based design helps in reducing the design time and also feature like partial reconfiguration have added extra benefit to the FPGA. Reconfiguration at runtime reduces resource utilization and power consumption. During implementation partial bit files can be generated and used for reconfiguring a specific part in FPGA at runtime without altering the design. This can be carried out with the help of Internal Configuration Access Port (ICAP) [1]. It is a hard wired primitive, which allows user to access configuration memory. The partial bit files can be stored in either internal or external memory and during reconfiguration; they are transferred toconfiguration memory through ICAP. Run time reconfiguration is also called as dynamic partial reconfiguration (DPR) [2]. It is been widely used in a wide range of applications like mission critical applications and self-adaptive systems.

Now a day's data security is becoming a tough task since various attacks are making it difficult to communicate data without breach. Encryption plays a vital role in data management. Ensuring security of data pertaining to basic emails and to the most important bank data is a biggest challenge. Normally, in encryption

process, the secret data is combined with a specific key and a cipher text is generated which is then communicated. These encryption algorithms are classified into two types: Symmetric key and Asymmetric key encryption. If same key is used for encryption and decryption of data then it is called symmetric otherwise it is asymmetric. AES, Twofish, 3DES,Blowfish, RC5 algorithms are the important symmetric type algorithms[3].

Objective of the proposed work is to validate runtime reconfiguration feature through Encryption algorithms. Two encryption algorithms namely AES and Twofish are designed using Verilog. Partial reconfiguration concept is applied for selecting any one algorithm at a time. This is performed using custom ICAP processor IP available in the Xilinx Vivado IDE. This processor requires basically three input signals i.e. ICAP_go, bitstreamlength and reconfiguration done signals. Initially partial bit streamfiles are stored in SD card and when partial reconfiguration is initiated, the appropriate partial bit files are then stored in DDR, and from there to ICAP processor. The proposed design has one reconfigurable partition (RP) with two functional reconfigurable modules. The ICAP signals are monitored using integrated logic analyzer (ILA) and the inputs and outputs are provided using virtual input-output IP (VIO). The entire design is implemented on Zed board.

The paper is organized as: section 2,outlines previous related work; section 3, briefly describes the encryption algorithms; section 4, describes the proposed design implementation; section 5 shows the simulation results; finally, the conclusion and future work are followed in section 6.

II. Previous Related Work

In this section, most relevant works of encryption algorithms and partial reconfiguration are detailed.

Yuwen Zhu et al [7] have implemented AES for 128, 192 and 256 bits on Virtex- V kit. They have tried to select any one key length at a time as per the requirement. They claim that hardware efficiency is better compared to other similar works. Only one type of algorithm is considered.

Ye Yuan et al [8] have proposed a high performance AES system which works for all three key lengths. As they implemented the design based on pipelining concept, area and throughput are improved. ShuchishmanBurman et al [9] have proposed AES design considering different key sizes like 128-bit, 192-bit and 256-bit and used reconfiguration concept. They also implemented high speed and low area AES and on Zed board. Madhumita Panda [10] compared symmetric i.e. AES, Blowfish and DES design with asymmetric i.e. RSA cryptographic algorithms by taking text, binary and image files. Three parameters decryption time, encryption time and throughput are considered for comparison. Rashmi Mahajan et al [11] proposed a method to implement AES encryption with reconfigurable keys and it stands a good solution for preserving secrecy and also convenient in the numeric communication. Ramesh Yegireddi et al. [12] surveyed different commonly used encryption algorithms and reported their vulnerabilities so that they can be implemented correctly. This survey intended to design a new secure conventional encryption algorithm in Cryptography. Rizvi et al [13] performed analysis between security and performance of Twofish and AES algorithms. Initially they considered safety factor and encryption speed for both the algorithms by encrypting image, text and audio. They also analyzed performance of these algorithms in terms of throughput. Pil-Joong Kang et al. [14] proposed MDS-M2 Twofish algorithm that can be used for wireless communication. MDS-M2 block, modified version of MDS block is developed. The comparison proved improved speed, decreased complexity and power. A total of 11% improvement is achieved with MDS-M2 block and it also proved to be suitable for wireless data communication.

III. Encryption Algorithms and Run-Time Reconfigurability

A. AES Encryption

AES is developed by Rijmen and JhonDeamen hence also known as Rijndeal. It is an alternative for Data Encryption Standard (DES). It stands good with both software and hardware. It is established for digital data encryption which is specified by National Institute of Standards and Technology (NIST), U.S. in 2001.[2,4, 15-18] AES can be used with 128-bit block size and it has three variants in which key length changes i.e. 128, 192 and 256 bits wide as shown in Figure 1.

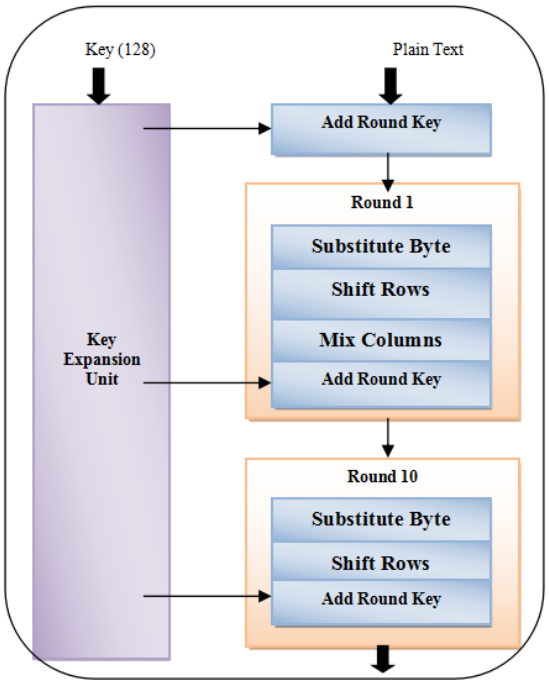

Fig.1. Block diagram of AES

AES has N rounds which changes with the key width (128 bit: 10 rounds, 192 bit: 12 rounds, 256 bit: 14

rounds). Table 1 shoes the size of parameters for AES encryption. Four transformations named sub bytes, shift rows, mix columns and add round key are considered for AES encryption. Initially, before first round i.e. round 0, only add around key transformation is done for plain text. From 1 to N-2 round all the four transformations are performed but for N-1 round mix column is excluded. There are three functions in key expansion unit, rotate word, substitute word and reconfiguration unit. In rotate word 1-bit circular left shift is performed. Substitute word transforms 32-bit key word and reconfiguration unit does XOR with round constant.

Table 1. AES parameters [2, 12, 15]

Key Size	128	192	256
Plaintext Block Size	128	128	128
Number of rounds	10	12	14
Round Key Size	128	128	128
Expanded Key Size	176	208	240

B. Twofish Encryption

Twofish belongs to the symmetric key cipher similar to the AES. It is derives from Blowfish, Square and SAFER. It has a block size of 128-bits and a key size extendable up to 256-bits. It has a total of 16 rounds**[5,6].** Similar to DES, Twofish also has a feistel structure and works on a maximum distance separable matrix. Figure 2 shows the block diagram for Twofish encryption. Initially for twofish, input whitening is performed by dividing 128-bit plain text into four parts each of 32-bits wide and performing exclusive-or with sub-keys. [2, 9]These 32-bit sub-keys are generated using sub-key generators. F-function contains two g-functions which comprises of S-box and MDS matrix multiplier. The outputs from two g-functions are combined to perform Pseudo Hadamard Transform (PHT). For the next round, two F-functions exchange their positions. After the final round (16^{th} round), swapping is done and the result is passed through output whitening to get cipher text.

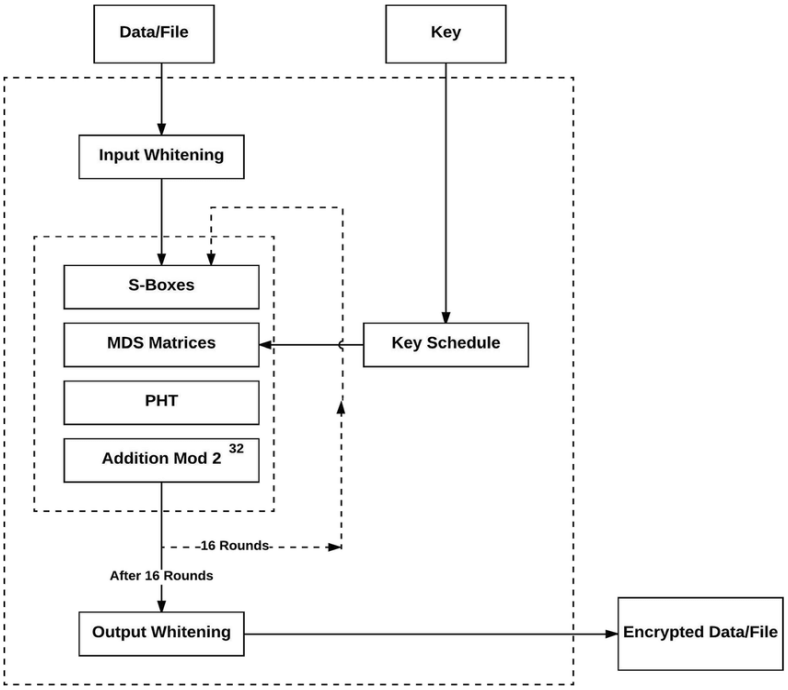

Fig.2. Block diagram for Twofish algorithm

C. Run-time Reconfigurability

One of the most important features of high-end FPGA devices is partial reconfiguration. It allows user to change the functionality of a specified area in FPGA without the need to alter the overall design. The main advantages of partial reconfiguration are reduction in power, size and cost of the design as compared to the normal design techniques [1].

To implement reconfiguration, special bitstreams called partial bitstreams are generated which are then used in later stages to reconfigure the functionality at runtime. This is done through a configuration interface called ICAP which allows user to access (writing or reading) the configuration data. Fig. 3 depicts features of the ICAP module.

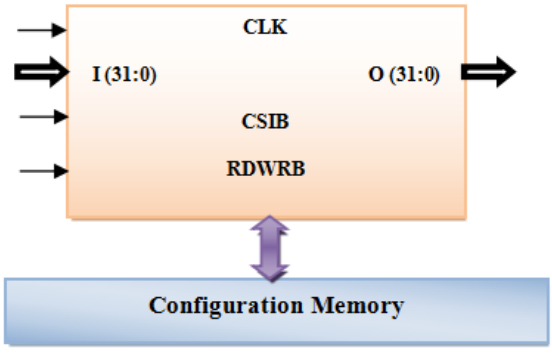

Fig.3. ICAP Primitive

IV. Design Methodology

In the proposed design switching between AES and Twofish algorithms are implemented using ICAP processor and UART port available on zed board. Initially individual algorithms are designed, synthesized and implemented to obtain respective partial bit files. This processor assists in realizing dynamic reconfiguration**. Fig 4 shows the internal block details of the FPGA present on the ZED board. It mainly consists of processor section (PS) and programmable logic section (PL).**Initially in the device floor-plan, a single partition (reconfigurable partition-RP) is created to accommodate partial reconfigurable blocks of encryption algorithms.

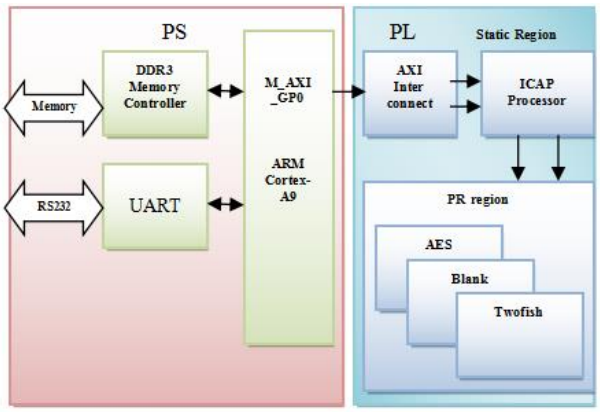

Fig.4. Block diagram of the proposed design

This pre-defined partition region gets mapped with any one of the module at a time depending on the control signal. During the implementation process, AES and Twofish algorithms are defined individually as reconfigurable modules. Later, AES and Twofish are added in the RP since both AES and Twofish modules to be reconfigured. After implementation and bitstream generation, three partial (AES, Twofish and Blank) and one full bitstream are generated. Initially partial bitstreamfiles are stored in SD card and when partial reconfiguration is initiated, appropriate partial bit files are then stored in DDR, and from there to ICAP processor as shown in Figure 4. Reconfiguration is carried out through UART port. Three control inputs are included for specifying a particular encryption module to be executed. They are A, T and B for the blank module. Three partial bitstrams are reconfigured with a specific name each i.e. pressing A reconfigures AES; T reconfigures Twofish and B for Blank. The ICAP signals are monitored using integrated logic analyzer (ILA) and the inputs and outputs are provided using virtual input/ output (VIO). The complete design implementation is done on zedboard. The proposed design is simulated and then synthesized before implementing on the hardware ZED board. Fig 5 shows the outcome of synthesis process. The synthesis tool generated module level schematic of the proposed design overview is as in fig 5. Block design named system_i and reconfigurable encoder is highlighted and the overall design is shown in the right down corner as world view.

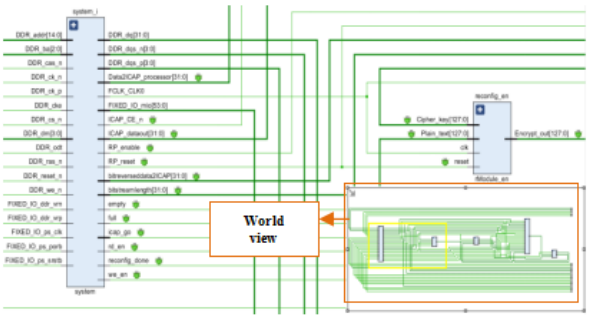

Fig.5. RTL schematic of the proposed design

A. Power Estimation

Power consumed for implemented design is estimated from the tool generated report. The static and dynamic power report is shown in Table 2. It is the report as generated by the Vivado tool. The total power is 1.769W.

Table 2. Power consumption of overall design

On-Chip Power	Power in Watts
Dynamic Power	1.625W
Device Static Power	0.143W
Total Power	1.769W

B. Resource Utilization Report

The final design is mapped on the FPGA device LUTs, registers etc. Table 3 shows the resource utilization summary for each internal block in the proposed design. It is been compiled based on the Vivado tool generated report after synthesizing the design.

Table 3. Utilization summary

Name	Slice LUTs	Slice Registers	F7 Muxes	F8 Muxes	Slice	LUT as Logic
Top	15820	9980	3331	1326	5581	14113
vio	579	1465	80	0	416	579
system	718	1138	1	0	336	655
Reconfigurable encryption	9391	128	3032	1304	2405	9391
ila	4656	6515	218	22	2255	3036
dbg_hub	476	734	0	0	232	452

V. Simulation Results

As per the proposed methodology, design has been coded using Verlog-HDL. It is verified through simulation using ISIM simulator present in the Vivado IDE. Different combinations of input keys are considered as inputs and the outputs are checked. Fig 6 depicts both input and output values as a timing diagram.

For AES encryption following are considered:
Plain text: 0x0f0ffff,
Cipher key: 0x0ff,
Cipher key: 4cb227245c89afa8e431bd0098b5a846.

Other details are mentioned in simulation outputs for AES and Twofish separately as shown in figure 6 and 7 respectively.

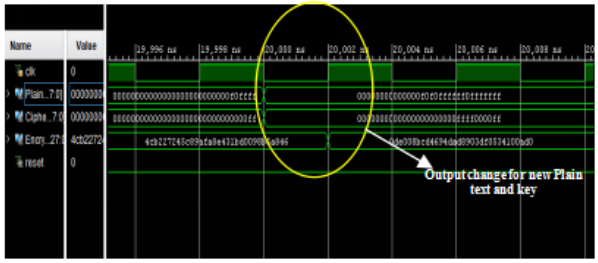

Fig.6. Output for AES encryption

Different combinations of input keys are applied as inputs for the Twofish algorithm and the outputs are checked. Fig. 7 depicts both input and output values as a timing diagram.

For Twofish encryption following are considered:
Plain text: 0x0ffff0000ffff,
Cipher key: 0x0ff00,
Cipher key: c562b3685bcc5a1df489180ef5eb2198.

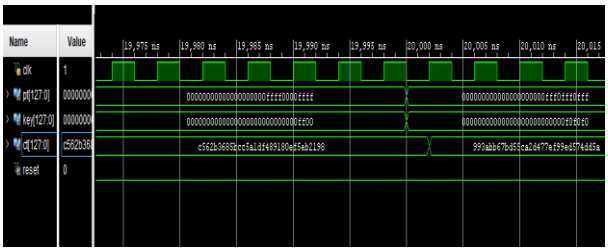

Fig.7. Output for Twofish encryption

Fig 8 shows the floorplan of the implemented design. The highlighted areas shows different modules placed on the zedboardZynq Evaluation and Development Kit (xc7z020clg484-1) after placement and routing. Partial reconfiguration region in the floorplan is dedicated only for reconfiguration; no static design can be placed in this region.

Fig 9 shows the terminal window after connecting to the UART. Different reconfigurations can be observed by sending A (AES), B (Blank), T (twofish) and Q (quit). These commands are transferred to the processor though UART i.e. RS232 from PC.

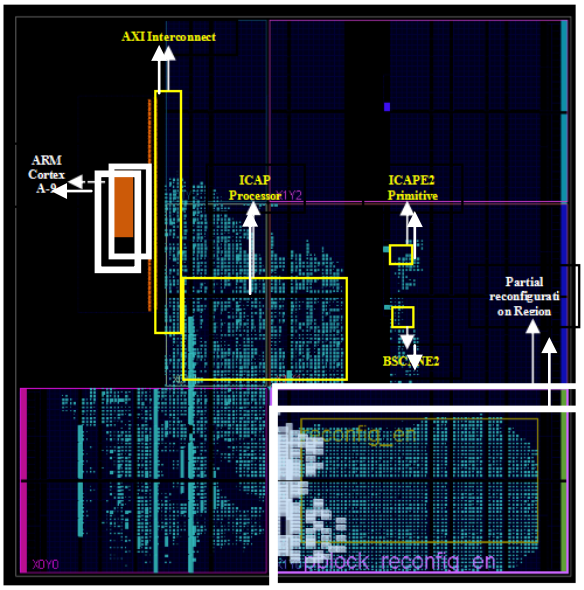

Fig.8. Implemented layout of proposed design on Zedboard

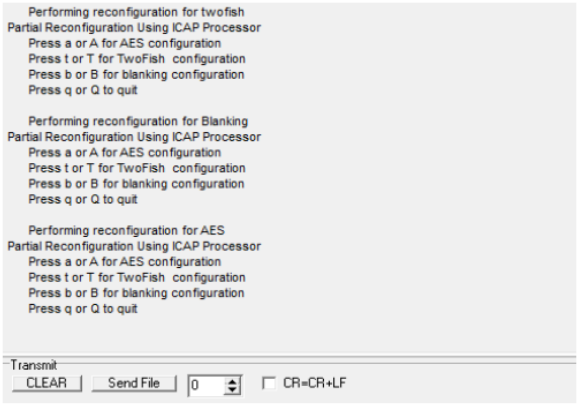

Fig.9. Terminal window

Fig. 10 shows the ILA window; here various ICAP signals are monitored during reconfiguration.

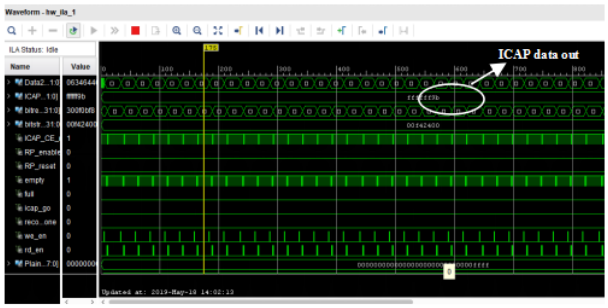

Fig.10. ILA window

The ICAP_data_out signal (fffff9b) shows that partial reconfiguration is successfully done. Figure 11 shows the VIO window where inputs can be forced and output can be monitored. This window shows the encrypted output after AES reconfiguration. Similarly results were obtained for twofish algorithm on VIO after two fish reconfiguration.

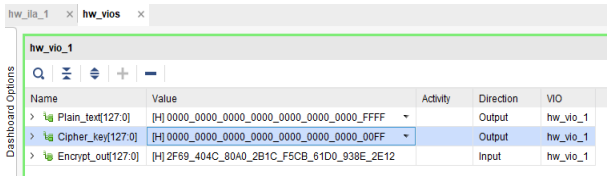

Fig.11. VIO window

Proposed design is been compared with the similar works as given in table 4. It does not give an exhaustive comparison, since very few papers were found in the available literature and also most of them have concentrated on only one algorithm. These works have not targeted on resource optimization. In the proposed design two different encryption algorithms were considered with a set of limited hardware resources, thus achieving area optimization.

Table 4. Comparison with the existing techniques

	Encryption Algorithm	FPGA Kit	Static/DPR design	Area Optimization
Shuchishman et al [6]	Only AES-128/192/256	Zedboard	DPR	yes
Rashmi Mahajan et al [8]	Only AES-128/192/256 bits	Virtex-V	DPR	no
Zine et al [12]	Only AES-128/192/256 bits	Virtex-II	DPR	no
Proposed design	Both AES and Twofish 128 bits	Zedboard	DPR	yes

VI. Conclusion

This paper explained about the implementation of reconfigurable encryption algorithms. A design methodology is illustrated which helps the user to select the type of algorithm depending on the requirement. ICAP processor was used for realizing run-time reconfiguration. Any digital application can be designed as a flexible design through runtime reconfiguration with less number of hardware resources. Resource utilization and power consumption are tabulated. It is been planned to implement three encryption algorithms based on the same methodology. In addition to resource optimization, ,reliability aspect for the design will be introduced in future. Since fault tolerance is a very important aspect for any system-on chip designs, it is been planned to implement encryption algorithm as fault tolerant design through single event upset management.

Acknowledgement

This work is been carried out as a part of DRDO-ERIP/ER/DG-Med&CoS/990916502/M/01/1659sponsored research work in the Department. We are grateful for the financial support provided.

References

[1] Xilinx “Partial Reconfiguration User Guide” UG 702.
[2] “Practical cryptography”, Text book Ferguson N. Schneier B. Wiley, 2003 ISBN-0471223573, 9780471223573.
[3] Xilinx “7 Series FPGAs Configuration User Guide” UG470.
[4] Divya, Dinesha P, Jamuna S, “ Implementation of Advanced Encryption standard in Vivado Design suite” JEITR, volume 5, August 2018
[5] Aparna. K, Jyothy Solomon, Harini . M, Indhumathi “A Study of Twofish Algorithm” 2016 IJEDR | Volume 4, Issue 2 | ISSN: 2321-9939
[6] Sanjay Kumar, Shashi Bhushan Thakur, Yogesh, Sanjeeth and Dr. Jamuna S, " Design and Implementation of Two Fish Encryption algorithm on ZED board", IJSRR, Volume 8, Issue 5, May 2019
[7] Yuwen Zhu, Hongqi Zhang, YibaoBao “Study of the AES Realization Method on the Reconfigurable Hardware,” 2013 International Conference on Computer Sciences and Applications. **DOI:** 10.1109/CSA.2013.23
[8] Ye Yuan, Yijun Yang, Liji Wu, Xiangmin Zhang , “A High Performance Encryption System Based on AES Algorithm with Novel Hardware Implementation,” IEEE conference. DOI: 10.1109/EDSSC.2018.8487056
[9] S. Burman, P. Rangababu and K. Datta, "Development of dynamic reconfiguration implementation of AES on FPGA platform," *2017 Devices for Integrated Circuit (DevIC)*, Kalyani, 2017, pp. 247-251. DOI: 10.1109/DEVIC. 2017. 8073945.
[10] SnehalWankhade and Rashmi Mahajan. “Dynamic partial reconfiguration implementation of AES algorithm,” International Journal of Computer Applications, 97(3), 2014. DOI: 10.5120/16986-7084
[11] R. Yegireddi and R. K. Kumar, "A survey on conventional encryption algorithms of Cryptography," *2016 International Conference on ICT in Business Industry & Government (ICTBIG)*, Indore, 2016, pp.1-4. DOI: 10.1109/ ICTBIG. 2016.7892684.
[12] S. A. M. Rizvi, S. Z. Hussain and N. Wadhwa, "Performance Analysis of AES and TwoFish Encryption Schemes," *2011 International Conference on Communication Systems and Network Technologies*,Katra, Jammu, 2011, pp. 76-79. DOI: 10.1109/CSNT.2011.160.
[13] M. Panda, "Performance analysis of encryption algorithms for security," *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, Paralakhemundi, 2016, pp. 278-284. DOI: 10.1109/SCOPES.2016.7955835.
[14] Pil-Joong Kang, Seon-Keun Lee and Hwan-Yong Kim, "Study on the design of MDS-M2 Twofish cryptographic algorithm adapted to wireless communication," *2006 8th International Conference Advanced Communication Technology*, Phoenix Park, 2006, pp. 4 pp.-695. DOI: 10.1109/ICACT.2006.206060.
[15] Zine El AbidineAlaouiIsmaili and Ahmed Moussa. Self-partial and dynamic reconfiguration implementation for aes using fpga. ArXiv preprint arXiv:0909.2369, 2009.
[16] PUB FIPS. 197, advanced encryption standard (aes), national institute of standards and technology, us department of commerce (November 2001). Link in: http://csrc. nist. gov/publications/fips/fips197/fips-197, 2009.
[17] PawelChodowiec, Po Khuon, and Kris Gaj. Fast implementations of secret-key block ciphers using mixed

inner-and outer-round pipelining. In Proceedings of the 2001 ACM/SIGDA ninth international symposium on Field programmable gate arrays, pages 94–102. ACM, 2001.

[18] Jos ́e M Granado-Criado, Miguel A Vega-Rodr ́ıguez, Juan M S ́anchez- P ́erez, and Juan A G ́omez-Pulido. A new methodology to implement the aes algorithm using partial and dynamic reconfiguration. INTEGRATION, the VLSI journal, 43(1):72–80, 2010.

Authors' Profiles

Jamuna S is working asa Professor in the department of ECE, DayanandaSagar College of Engineering, Bangalore, India since 2008. She has done M.Tech in VLSI Design and Embedded Systems from VTU, Belgaum and Ph.D fromJNTU,Hyderabad. Her research domain includes VLSI design, verification and testing. She is currently, executing a funded project as principal investigator in thedepartment. Research funds are sanctioned from DRDO, New Delhi, India.

Dinesha P is a Professor, Department of Electronics and CommunicatingEngineering, Bangalore, India. He received his Ph. D degree from University of Mysore, India, in the year 2014. His research interest is in VLSI Design (Digital Design), Digital System Design and Nanotechnology (Applications of conducting polymer composites).

KPShashikala is an associate professor in DayanandaSagar College of Engineering; Bangalore, India .She did her Bachelors in Electronics from MSRIT, Bangalore.Masters in Digital Communication from BMSCE, Bengaluru, and Doctorate in PalmprintBiometrics from Rayalseema University Kurnool, AP. Her areas of interests include Biometrics, Image processing and Digital Communication.

Kishore Kumar K is working as a Junior Research Fellow in the department of ECE, DayanandaSagar College of Engineering, Bengalru, India. He has done M.Tech in VLSI design and embedded systemsfromBengaluru Institute of Technology, Bengaluru. His research domain includes VLSI design and Verification.

How to cite this paper: Jamuna S, Dinesha P, K PShashikala, Kishore Kumar K, "Design and Implementation of Runtime Reconfigurable Encryption Algorithms using Custom ICAP Processor", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.12, pp.10-16, 2019. DOI: 10.5815/ijcnis.2019.12.02