STUDY OF DIFFERENT FPGA SYSTEMS IMPLEMENTED AES ALGORITHM: A REVIEW

[1]Sharayu Sharad Karwade, [2]Dr. Kalyani Akant

[1]PG Scholar,[2]Associate Professor

[1,2]Department of Electronics & Telecommunication Engineering,

[1,2]G H Raisoni College of Engineering, Nagpur, Maharashtra, India.

Absarct: With the rapid growth of multimedia technologies cryptograpghy is considered as one of the most secured way for transmitting and receiving data. Now a days AES algorithm is not only limited to transmit video data but also for image and text transmission. In this paper we have reviewed four FPGA boards on which AES algorithm has been implemented.

Keywords-FPGA, AES, Xilinx, DSP.

I. INTRODUCTION

Cryptography is technique of preserving data from unwanted objects by transforming in the pattern that is unrecognizable by hackers while transmission. Encryption is the process where maximum part of informtion is scrambled like text-data, images, audio, and video so to make the data undcipherable, unseen untillthe proces is donef. The primary objective of cryptography is to protect information from non authoritzed hackers. The data decryption decryption is nothing but the receving of encrypted data which recreates the original information. At present cryptography is not limited to secure military document but known as one important method for policy of security cosidering any organization and recognized as standard for industry for giving secure data, access control, and financial agreement through electronic medium. The primary information that will be send or saved is known as plaintext, the which either a person or machine can read. Whereas the hidden information called cipher text, which is not readable, neither by a person nor by any device can accurately processed until it is decrypted. The implementation is done by either softare or hardware. For analyzing cryptography algorithms on hardware the most efficient solution is provided by Field Programmable Gate Arrays (FPGAs) [18]. Xilinx ISE suit provides easy medium between software and hardware. There are different kits for performing operations though. FPGA is the most advance platform for performing various applications.This paper decribes different FPGA boards in which the AES algorithm has been performed successfully.

In section II the crptography procedure and brief information about AES algorithm is decribed. Section III is decribes about FPGA working and how AES algorithm is used on FPGA. In section IV diferent FPGA systems and results on that particular kit are described. Conclusion is given in senction V.

II. CRYPTOGRAPHY

Cryptosystem is a system that gives encryption and decryption. When a cryptosystem uses algorithms for encryption that decides how easy or complicated the encryption algorithm will be, neccessary software components, and the key, that works with the algorithm to encrypt or decrypt the original data [1][2]. Length of key space measured security level of encryption algorithm [2]. If the key size is large it will take more time for the attacker to be searched thus there is higher the security. In encryption process, when transformation is done from plaintext to cyphertext the key is main content that defines the specific transformation. Key of the encryption is depended on how much the keys space is, it is that perticular value which can be used to make key. When the keys space is large causing more possible keys can be formed for e.g. key sizes are 128, 192, or 256 bits are uses commonly today, so that key size of 256 can give a 2256 keys pace[2][3]. Some parameters such as secrecy of key, key length and the vector of initialization are depending on the strength of the encryption algorithm how they all work together. Based on the algorithm and size of the key, the strength of encryption can be considered. Cryptography algorithms are divided as either symmetric algorithm that use symmetric keys also known as secret keys or asymmetric algorithm, which use asymmetric keys also called as public and private keys.

2.1 Advance Encryption Standard (AES)

In 1997, the national bureau of standards asked for a fresh standard which will replace the data encryption standard. The contest ends in November 2001 as they chose the Rijndael crypto-system as the Advanced Encryption Standard (AES) [3][7]. The Rijndael system oprates on blocks of 128 bits, every 8 bit inputsarrange as 4 × 4 matrices. The technique uses variable block length and a key length, any combination of keys lengths is allowed latest specification.

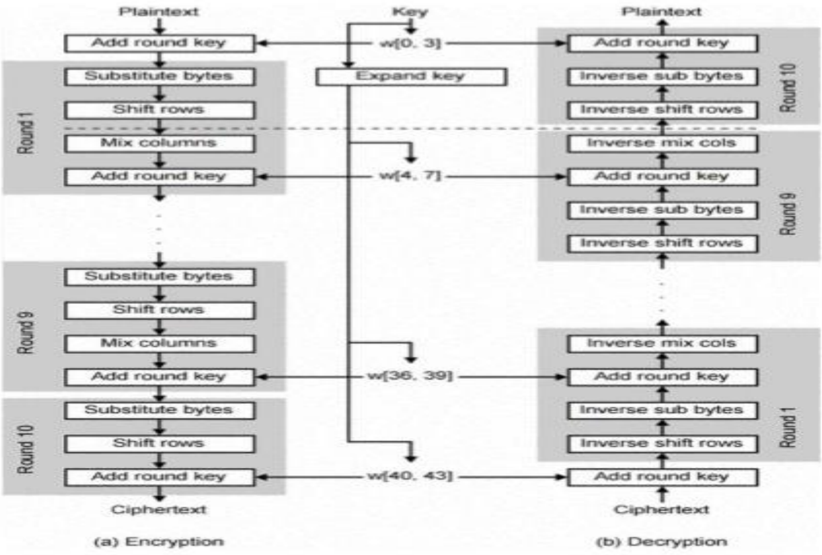

Fig. 1: The AES encryption and decryption flow [5]

Figure 1 Flow of shows the AES encryption as well as decryption [5].Other than 128 bits key length AES also uses 192 and 256 bits of key size blocks callled AES-192 and AES-256 respectively.The AES-128 uses 10 rounds,AES-192 uses 12 rounds and AES-256 uses 14 rounds.

III. FPGA

It is a semiconductor device having programmable logic blocks and interconnection system.At its core, FPGA is an array of interconnected digital sub circuits that performed regular functions while also offering very high levels of flexibility.Even after the product released in the market FPGA can implement any logical function as an ASIC can and we can re-program it [5].

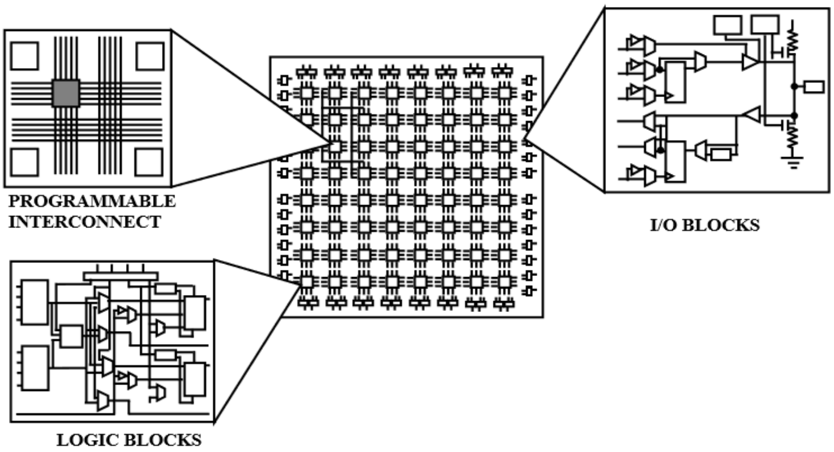

Fig. 2: Internal structure of FPGA [6]

Figure 2 shows the internal sturcture of FPGA in which it is divided into three major parts programmable interconnect, input/output blocks, logic blocks.

3.1 Implementation of AES algorithm in FPGA

In FPGA 128 bits key length AES algorithm is used. As Aes-128 has 10 rounds and divided into 4 stages. These stages are as follows:

1) Subbyte tranformation: In this it splits the subbytes into phaes and then pass each one through a box called substition box.Substitution informaion is provided from look up table [7].
2) Shiftrow tranformation: In this the rows of the state array are shifted cyclically to generate diffusion.
3) Column-Mix Transformation: Columns are oprated individually; it mixes every four byte of each coloumn to form a new value.According to Galois Field (GF) rulethe operation is performed dot wise [8].
4) Add-round Transformation: The Ex-ORing is performed around round key and state having each key length sized 128 bits. This is a column wise opration takes one word from round key and state columnsfour bytes.

There are different ways to implement this algorithm in field programming gate array some of the FPGA systems on which AES algorithm are being performed are deceibes as follow.

IV. FPGA SYSTEMS

4.1 SPARTAN 3 FPGA

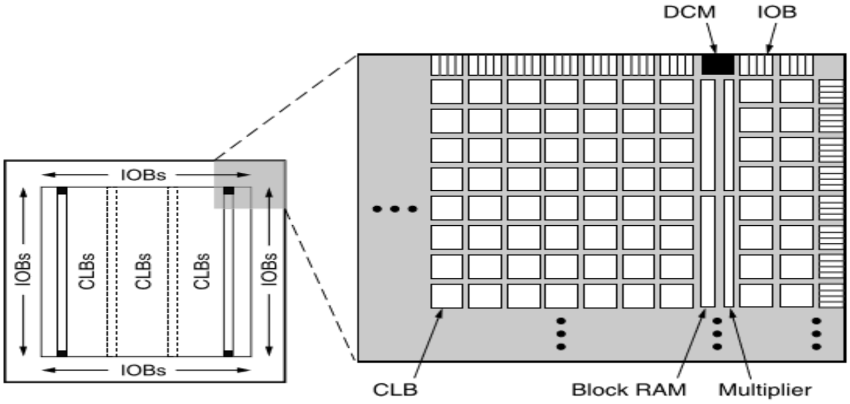

Fig. 3: Spartan-3 family architecture [9]

Figure 3 shows the spartan-3 family architechture which contain cofigurable logic blocks and block RAM for implementation of logic and storing purposes that can be use as flip-flop or latches. Block RAM can provide the storage up to 18KB duel port block. It has upto 633 I/O pins. Two 18bit binary numbers is accepted as input and calculate the result by multiplier. Digital clock manager (DCM) blocks give entire digital solutions for distribution, delay, multiplication, division, and phase shifted clock signals [9].

4.2 Implemented Results

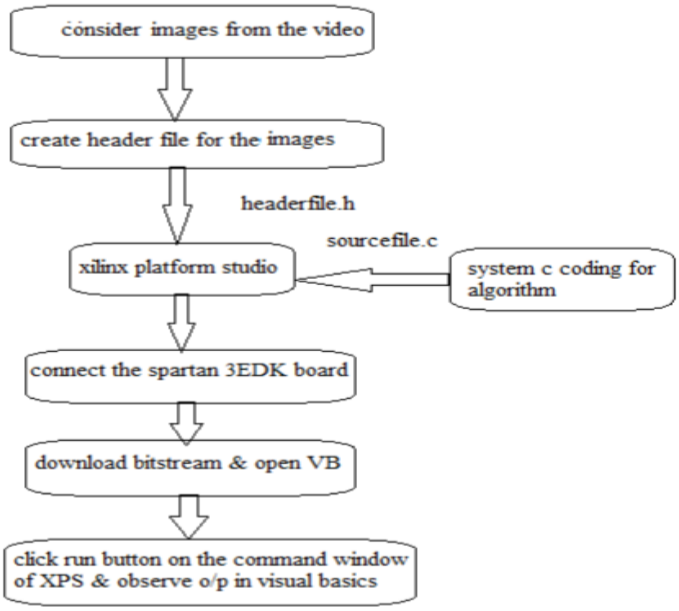
consider images from the video
create header file for the images
headerfile.h
sourcefile.c
xilinx platform studio
system c coding for algorithm
connect the spartan 3EDK board
download bitstream & open VB
click run button on the command window of XPS & observe o/p in visual basics

Fig. 4: Proposed block digram for AES algorithm using spartan-3[10]

In above configuration spartan 3 EDK, device-XC3S200, package-TQG144, speed grade of -4 is been used. The advance AES algorithm is implemented. On the opposite hand, synthesis results show that area consumption is low, using simply 100 percent of logic circuits of FPGA for AES, allowing the implementation of this method over affordable FPGA's [10].

4.3 Virtex 5 FPGA

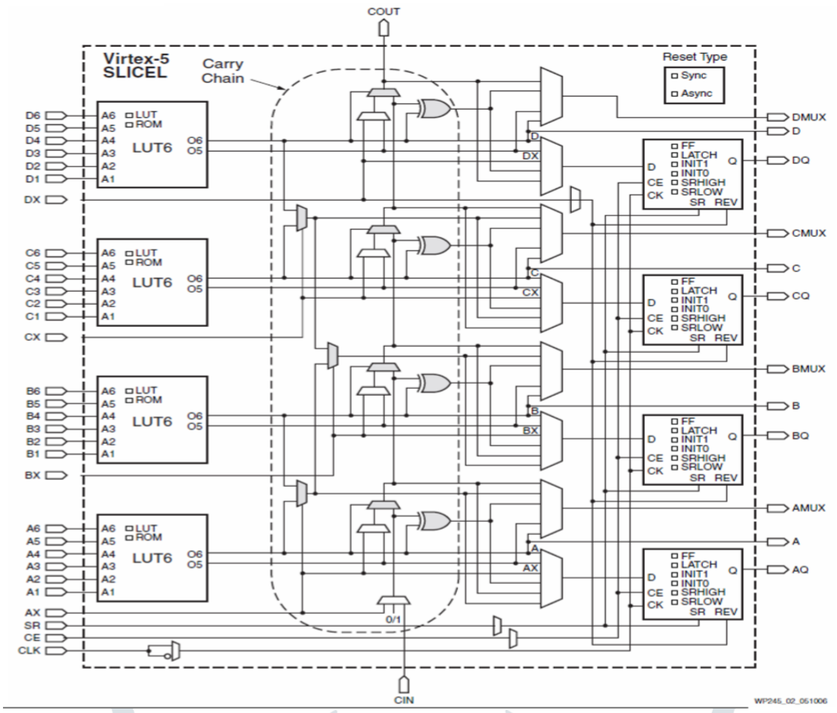

Fig. 5: Slice element structure in Virtex-5[11]

Figure 5 shows Slice element structure in Virtex-5. It utilized the second generation Advanced Silicon Modular Block (ASMB) column wise family of vertex 5 includes five different sub systems, the maximum assortments provides by no other FPGA system. It has most developed high performable fabriccable logic. Virtex 5 FPGA has various system level blocks of hard IP, 36-Kbit block RAM/FIFOs are also inclueded, 25 x 18 DSP slices of second generation, built-in digitally-controlled impedance is with SelectIO technology, interface blocks of chip sync sourcesynchronous, functionality system monitor, advance tiles clock management with integrated managers with digital clock and phase locked loop, and latest configurating choices [12].

4.4 Implemented Results

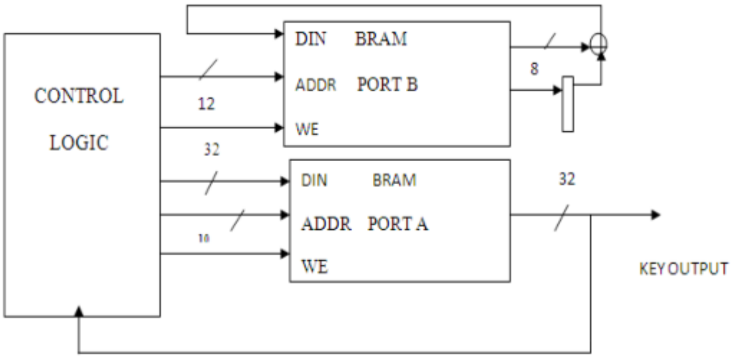

Fig. 6:Pipelined AES module [13]

In the above module the pielined structure of AES algorithm and parallel processing has been focused. Virtex-5FPGA board had been used with software Xilinx ISE 8.1i. New methods for performing AES operations at high throughput using on chip BRAM and DSP blocks with comparatively less use of traditional user logic such as flipflops, look up charts is been presented. This perticuler design methodology is to be supported by encryption and decryption standard [13].

4.5 Altera Cyclone-II FPGA

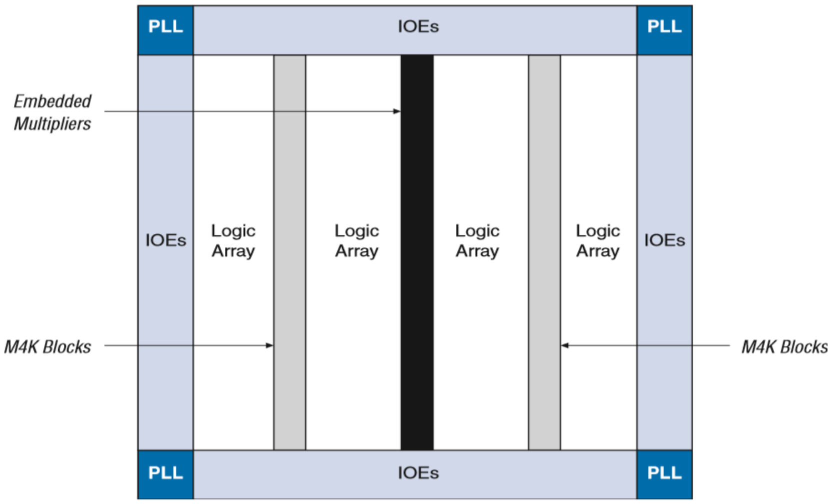

Fig. 7: Cyclone-II block diagram [14]

Above figure shows the block diagram of cyclone II. Cyclone is low cost production of Altera Corporation. It is a two diamentional row and column based architechture. It consists of 16 logic elements in each logic array block. M4K memory block has 4K bits of memory. Multipiler can be implemented upto two 9*9 bit multiplier. It has four PLL devices.

4.6 Implemented Results

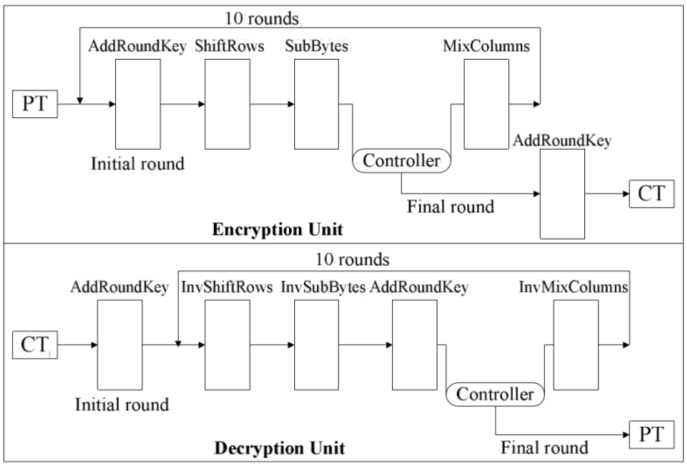

Fig. 8: Structure for AES encryption and encryption systems [14]

Entire structure shown in above designed decreases AES encryption and decryption system which is shown in Fig. 2, encryption unit is the upper half part, the second part is decryption unit [14]. In this FPGA Altera Cyclone EP2C35F672C6 is been used and tested for AES algorithm, it provides less hardware compare to pipeline AES algorithm. Throuputs for encryption and decryption within total 760 logic elements are 593.45Mbps 267.63Mbps respectively. These results make this system more secure, dependable and cost efficient.

4.7 Atrix 7 FPGA

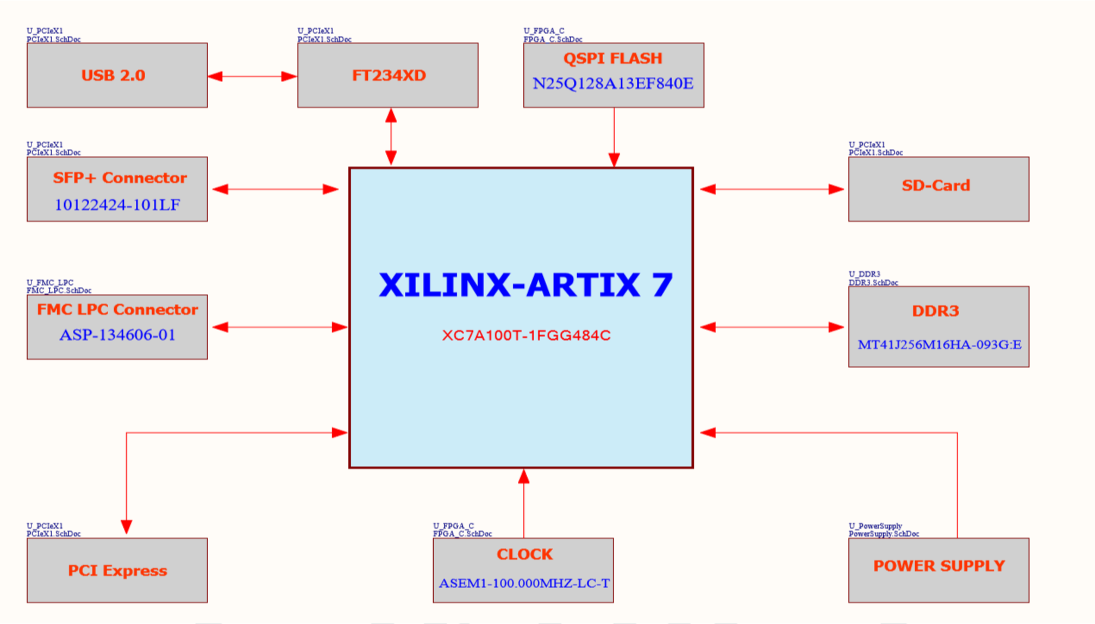

Fig. 9: Block Diagram of Artix-7 FPGA [16]

Artix 7 FPGAs are optimized for the lowest in prize and power with large volume automotive applications and small form factor packaging [17]. It has 36 Kb dual-ports block RAM accompnied by built-in FIFO logic for on chip data buffer. It has also advance speed of serial connectivity added with in-build serial transceivers starts from 500 Mb/s upto 6.25 GB/s of maximum rates. It has large variety of configuration options; with HMAC/SHA-256 authentication it supports upto 256-bit AES encryption.

4.8 Implemented Results

AES 128 bit key algorithm implemented on artix 7 Nexys 4 kit proposed a platform using AES algorithm for encryption and decryption without having a personal computer. Including feedback loops all the complexities of the algorithm is being handled by artix 7 systems efficiently [18]. This result provides the encryption by using 128 bits key on Artix 7 FPGA board successfully which can be expanding for further use of 192 bits & 256 bits key [18].

V. CONCLUSION

In this paper, we have surveyed the AES algorithm implemented FPGA systems. We have given brief information about different FPGA kits and then implemnted results have been provied. The analysis gave us interesting results about how the advancement in FPGA systems is done. What changes have been done in AES algorithm according to application has been described in this paper. We can conclude that FPGA is a good platform for implementing AES algorithm. There are various ways to use AES algorithm and FPGA boards depending upon the application.

REFERENCES

[1] Kessler, Gary C., (1998). An Overview of Cryptography, available from http://www.garykessler.net/library/crypto.html.
[2] B. White, Gregory, 2003. Cisco Security+ Certification: Exam Guide, McGraw-Hill.
[3] Shon Harris, 2007. SICCP Exam Guide, fourth edition, McGraw-Hall
[4] Jean-Yves chouinard. Design of secure computer systems CSI4138/CEG4394 notes on the advanced encryprion standard (AES), available from http://www.site.uottawa.ca/~chouinar/Handout_CSI4138_AES_200 .pdf.
[5] Anupama Gopalan, Janani Ganesh and Swathi.M, "FPGA-based Message Encryption and Decryption", International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE).Volume 4, Issue 5, May 2015.
[6] Module 4, Design of Embedded Processors, Lesson 20 Field Programmable Gate Arrays and Applications, Version 2 EE IIT, Kharagpur, avilable from https://nptel.ac.in/content/storage2/courses/108105057/Pdf/Lesson-20.pdf.
[7] Ahmad N., Hasan R. and Jubadi W.M., "Design of AES S-Box using comnbitional logic optimization",IEEE Symposium on Industrial Electronics & Applications (ISIEA), pp. 696-699, 2010
[8] Prof. Venkateswarlu S., Deepa G.M. and Sriteja G.,"Implementation of Cryptographic Algorithm on FPGA", IJCSMC, Vol.2, Issue. 4, April 2013, Pg. 604-609.
[9] Spartan-3 FPGA Family Data Sheet, DS099 June 27, 2013 Product Specification avilable from, www.xilinx.com
[10] K Jyothi, S.V.R. Manimala, "FPGA Implementation of Short Duration Video Encryption & Decryption",

IJESC July 2015 Issue, DOI: 10.4010/2015.386
[11] Petar Borisov Minev and Valentina Stoianova Kukenska "The Virtex-5 Routing and Logic Architecture", avilable from http://kst.tugab.bg/staff/vally/4.pdf .
[12] Virtex-5 Family Overview, DS100 (v5.1) August 21, 2015 00 Product Specification avilable from, www.xilinx.com
[13] J. Senthil Kumar, C.Mahalakshmi "Implementation of Pipelined Hardware Architecture for AES Algorithm using FPGA", 2014 International Conference on Communication and Network Technologies (ICCNT), DOI:10.1109/CNT.2014.7062766
[14] Altera Corporation Cyclone II Device Handbook, Volume 1 February 2007 avilable from https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/hb/cyc2/cyc2_cii51002.pdf
[15] Yang Jun, Ding Jun, Li Na, Guo Yixiong "FPGA-based design and implementation of reduced AES algorithm", 2010 International Conference on Challenges in Environmental Science and Computer Engineering, DOI:10.1109/CESCE.2010.123
[16] Numato Systems Pvt Ltd, Tagus V2.0, Block Diagram.SchDoc, and Title: Tagus, Size: Project: Tagus.PrjPcb,
avliable from https://numato.com/help/wp-content/uploads/2018/05/TagusSchematic.pdf
[17] XA Artix-7 FPGAs Data Sheet: Overview DS197 (v1.3) November 15, 2017 Product Specification avilable from, www.xilinx.com
[18] Sheetal U. Jonwal, Pratibha P. Shingare "Advanced Encryption Standard (AES) implementation on FPGA with hardware in loop", International Conference on Trends in Electronics and InformaticsICEI 2017, DOI:10.1109/ICOEI.2017.8300776