Hardware and Software Co-Design of AES Algorithm on the basis of NIOS II Processor

Ganesh G. Sarmokaddam[1], Ms. S.I. Parihar[2], Dr. Mrs. S.A. Chaturvedi[3]

[1]Ganesh G. Sarmokaddam, Mtech IVth Sem, Dept. of ECE, PIET college of Eng.,Maharashtra,India.
[2]Ms.S.I.Parihar,Professor,Dept. of ECE,PIET collage of Eng.,Maharashtra,India
[3]Dr.Mrs.S.A.Chaturvedi,HOD,Dept.of ECE,PIET collage of Eng.,Maharashtra,India

---***---

Abstract - *The Digital Technology is not limited to only computers but has extended its application to a wide range of consumer electronics such as mobile phones, wireless communications, digital cameras, camcorders and many more, in the 21st century. The field of Cryptography deals with such methods which aim at securing or protecting digital/electronic data. Advanced Encryption Standard is a NIST approved Cryptographic Algorithm that converts a 128 bit plaintext into an unintelligible 128 bit ciphertext using a secret key of 128, 192 or 256 bits. For the implementation of AES on FPGA, a Hardware-Software Co-design methodology is proposed. For this embedded approach a Nios II soft-core processor designed for Altera (Now Intel) FPGAs will be explored. For the implementation process, Quartus II EDA tool and NIOS II Integrated Development Environment (IDE) will be required.*

Keywords— AES, FPGA, VHDL,* Quartus II Platform Studio*, Encryption, Dcryption, Plain text, Cipher text.

1.Introduction

In the 21st century, the Digital Technology is not limited to only computers but has extended its application to a wide range of consumer electronics that handle digital data such as mobile phones, wireless communications, digital cameras, camcorders and many more. Due to this, digital data travels to and fro between computers and digital devices. With the advent of Digital technology, methods for providing Digital Information Security have surfaced. The field of Cryptography deals with such methods which aim at securing or protecting digital/electronic data. Cryptography can reformat and transform digital data, making it secure on its trip between computers and digital devices. The world of Cryptography aims at constructing and analyzing algorithms or protocols that provide secure communication of digital information. The general process is to convert an ordinary plain text into an unintelligible ciphertext and vice-versa. So it becomes a method of storing and transmitting data in a particular form so that only those can read and process it for which it is intended. A basic block diagram of Cryptography is described in Fig1.1.

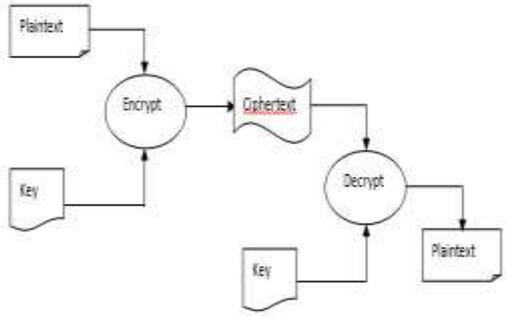


Fig 1.1: Basic block diagram of Cryptography

In 2000 the National Institute of Standards and Technology (NIST) of the United States announced AES as the successor of DES because of its robust security characteristics. This algorithm was developed by two professional cryptographers Joan Daemen and Vincent Rijmen. AES is an acronym for Advanced Encryption Standard. It is a cryptographic algorithm is capable of encrypting and decrypting data of a block size of 128 bits using cipher keys of lengths 128, 196 or 256 bits. For both its Cipher (Encryption) and Inverse Cipher (Decryption) process, the AES algorithm uses an iterative round function that is composed of four different byte-oriented transformations. There are 10, 12 and 14 number of rounds required to be completed for encryption/decryption with cipher key lengths of 128 bit, 192 bits and 256 bits respectively. AES is a widely accepted cryptographic algorithm due to its robust transformations and it can be easily implemented in Hardware as well as Software.Field Programmable Gate Arrays (FPGAs) are modern semiconductor devices which are prominent for their reconfigurable feature. A processor modeled on Hardware Description Languages (HDLs) and implemented completely on a FPGA fabric is known as a Soft Core Processor. As the behavior and architecture of a soft core processor is described at a higher abstraction level using an HDL, the overall design can be understood with relative ease. This kind of processor yields a substantial amount of flexibility to an application through the configurable feature of the FPGA. Using a soft-core processor alleviates many of the issues encountered due to the changing requirements, which can be detrimental to a project if using a discrete microprocessor solution. Also, there are a number of various peripherals available and adding or subtracting a peripheral can be achieved with relative ease. A soft-core processor also offers the flexibility of tailoring the core itself for the application. Hardware implementations provide reliable performance whereas Software implementations have benefits of configurability and flexibility. The present day applications are manifold. These applications have diverse requirements which can be met by adapting Hardware-Software co-design technology. The NIOS II soft core processor is Altera's second generation soft embedded processor design. NIOS II processor is a general-purpose RISC processor core providing Full 32-bit instruction set, data path, and address space. NIOS II soft-core development is based on the NIOS II Integrated Development Environment (IDE). In this project, a methodology of Hardware Software co-design is implemented on Altera's NIOS II processor where AES is selected as an application. AES is a well-known encryption algorithm that has advantages in data ciphering, security, simplicity of implementation and low memory requirements

2.Literature Review

An older cryptography algorithm was the Data Encryption Standard (DES) [01]. Previously, for security products, DES algorithm was widely used. Such that from the year 1977, the Data Encryption Standard has been used as the standard algorithm however, just because of the very small key size of only 56 bits, it can be easily hacked and cracked. Because of this reason, in September 1997 an institute known as the National Institute of Standards and Technology (NIST) announced for new different algorithms. After that in August 1998, fifteen AES candidate algorithms were declared as security algorithm. A group of five algorithms are selected by NIST in August 2000 that are: RC6, Rijndael, Mars, Twofish and Serpent as the finalist. In these algorithms more analysis was performed which was based on the priority that which algorithm will be the best AES algorithm. At last, on 2 October, 2000, the Rijndael algorithm was selected, that was announced by the NIST. In November 2001, the NIST declared the Advanced Encryption Standard (AES) [02] algorithm as the perfect security algorithm and it replaces the DES algorithm. The AES algorithm was created by two scientists Dr. Joan Daemen and Dr. Vincent Rijmen, which is a symmetric block cipher. AES clarifies as an encryption algorithm which can encrypt and decrypt information/data given to its input. The block size of AES is always fixed to 128 bits and the key size may vary to three different keys length of 128, 192, and 256 bits and the name for it is given as AES-128, AES-192 and AES-256 respectively. In cryptography, security of data is very important such that the two developers Joan Daemen and Vincent Rijmen developed an algorithm that was Advanced Encryption Standard (AES), also famous as Rijndael [3], as this name of algorithm is based on the combination of their names Previously used cryptography algorithm was DES, but it has a small key size of just 56 bits, it can be easily hacked by hackers and it had a feistel structure. AES is similar to DES but in these ways AES is little bit different from DES and has an upgraded version of it. Different AES specifications is shown in the given Table I below, where Nk represents no. of columns, Nr represents no. of rounds, Nb represents no. of bits in the data block and specifications of Input and Output is shown in Table II below.

2.1.AES Encryption

AES works on an array of bytes of a 4x4 matrix, which is known as state. All transformations of encryption process are performed only on a state. After each transformation values are stored in a state, this state is the input for the next transformation. In encryption four transformations in each round is performed which are based on the methods of permutation and substitution:

Substitute bytes: A substitution of the byte from S-box.

ShiftRows: A cyclic shifting is an example of simple permutation.

MixColumns: A substitution of an arithmetic values over GF (2^8).

AddRoundKey: An XOR operation performs between the input state and a small part of 16 bytes of the expanded key.

2.2.AES Decryption

Decryption is the reverse process of Encryption. In AES decryption data will again convert into its original message and it gets at the output of the decryption block. Both cipher of AES, Encryption and Decryption are not identical to each other but the key scheduling is same for both. Such that the four stages of transformation is different for decryption. They are:

proposed that hardware implementation has better speed in comparison to software implementation. In the proposed work, AES as implemented on FPGA as it provides reconfigurable hardware to verify the real-time implementation. The proposed design uses repetitive looping

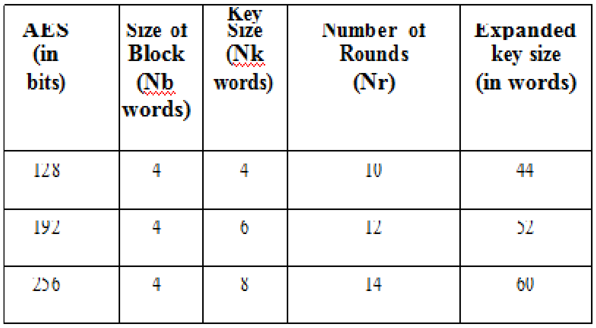
InvSubBytes:-- A substitution of the byte value from an inverse S-box.

InvShiftRows:-- This is just the inverse process of transformation of ShiftRows in which a cyclic shifting operation is performs.

For InvAddRoundKey, the same function of AddRoundKey is use as the inverse of it is same.

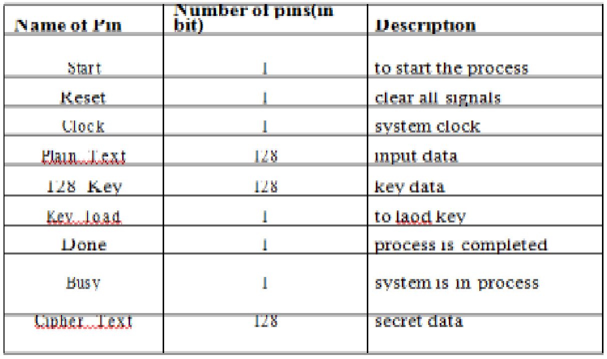
InvMixColumns:--This transformation is also just the inverse process of the MixColumns stage.

TABLE 1. AES SPECIFICATIONS



AES (in bits)	Size of Block (Nb words)	Key Size (Nk words)	Number of Rounds (Nr)	Expanded key size (in words)
128	4	4	10	44
192	4	6	12	52
256	4	8	14	60

TABLE 2. SPECIFICATION OF INPUT OUTPUT PINS



Name of Pin	Number of pins(in bit)	Description
Start	1	to start the process
Reset	1	clear all signals
Clock	1	system clock
Plain_Text	128	input data
128 Key	128	key data
Key_load	1	to laod key
Done	1	process is completed
Busy	1	system is in process
Cipher_Text	128	secret data

2.3. **Related Work**

Preeti Dixit *et al*., studied the effect of Hardware-Software co-design by implementing Advanced Encryption Standard Algorithm on FPGA. AES is implemented in C language on Microblaze soft core processor and the time required for the plain text to convert to cipher text is measured with the Software Profiling. MicroBlaze is a soft-core RISC processor. It is developed and maintained by Xilinx and is therefore optimized for Xilinx FPGA. To improve the timing results , Hardware Software Codesign is incorporated with putting the most time consuming block i.e. Mix Column in hardware by forming a customized IP and connecting it to the Microblaze processor with the help of Processor Local Bus(PLB) [1]. Zabina Kouser *et al*., method with 128 bits block size and key size. The language used was VHDL and tool Xilinx ISE 14.4. Applications of AES are smart cards, Wireless communication, Electronic financial transactions, ATM machines, WWW servers, cell phones and e-mails, and digital video recorders [10]. Meghana A. Hasamnis *et al*., investigated the hardware / software co-design methodology to implement one of the functional modules of AES Algorithm in hardware and subsequent remaining modules in software. The module in hardware was implemented on FPGA and added as hardware accelerator to the processor. The proposed hardware/software implementation was done on Altera NIOS II processor platform. An implementation result shows a considerable improvement in speed as compared to software only approach. On the other hand, the significant reduction in area was also notable as compared to hardware only approach [9]. Kuan Jen Lin *et al*.,achieved the balance between the cost and efficiency of software and hardware design by implementing AES encryption algorithm with hardware in combination with part of software using the custom instruction mechanism provided by the ALTERA Nios II platform. The advantages of custom instructions include the reduction of instruction sequence and the speed acceleration by hardware [8]. Disha Yadav *et al*., discussed some architectures for AES-128 implementation. The basic AES core has been developed for encryption and decryption using Look-up Table and Composite Field Arithmetic. The conclusion leads to the following statement that though AES implementation using LUT gives greater speed than implementation using CFA (Composite Field Arithmetic) without inner pipeline, area occupied by it is very large. All these implementations were synthesized, mapped, placed, routed and simulated using Xilinx 9.2 on Spartan and Virtex series of devices.

3.Theme And Methodology

Many systems are complex and pose various design challenges such as, large specifications, short time-to-market, high performance, multiple designers, interface to manufacturing etc. A Proper design methodology helps to manage the design process and improves quality, performance and design cost. Co-design is an interdisciplinary activity that combines concepts and ideas from diverse disciplines, e.g. system-level modeling, hardware design and software design. Embedded systems employ both Hardware and Software techniques to reduce complexity and increase speed of the design. In this thesis, a hardware software co-design methodology is used to design a system for Advanced Encryption Standard. components can satisfy the specifications. Hardware components include processor, memory, interface, peripherals etc. Programs and their operations can be described as software components.

3.1.A Simplified Design Flow of Co- design Methodology[2,3]

A simplified design flow of Co-design methodology is time depicted in Fig 3.1.

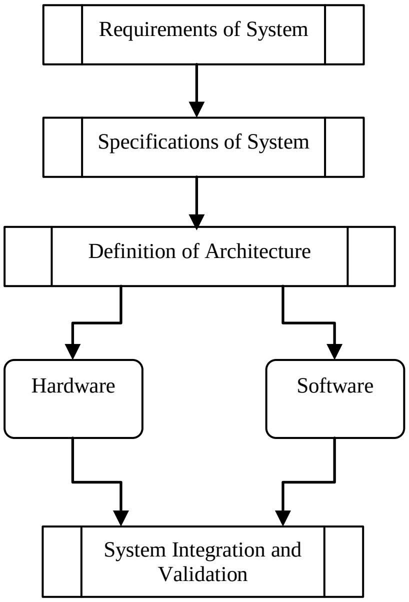


Fig 3.1: Simplified Design Flow of Co- design

3.1.1.Requirements of System:

This part includes having a formal description of the system and its application using a plain language. Functional and Non-Functional requirements of the system are chalked out. Non-Functional requirements include performance, reliability, power consumption, size etc.

3.1.2.Specifications of System

This part provides a proper and precise description of the behavior of the system. At this step, the target architecture is not specified but the relation of inputs to the architecture of the system is provided. It may include functional or non-functional requirements. The description of the specification can be put into a mathematical form for formal verification.

3.1.3.Definition of Architecture

In this part, the specifications of the system are distributed to Hardware and Software approaches. This basically tells how the hardware and software

3.1.4.System Integration and Validation

This part puts together the hardware and software components. The system integration phase is crucial to validate the interaction among the different system components. Many system level bugs can be indentified at this stage so that the system can take a step closer towards validation.

3.2.AES: Software Approach[2,3]

The Nios II is a soft core processor based on 32-bit RISC architecture from Altera for use in their FPGAs. The system designer can define a custom Nios II core based on the requirements of the application to be developed. Altera's Quartus II and NIOS II Integrated Development Environment are the design tools used for building, debugging and running a Nios II system. SOPC builder is a powerful system development tool included in the Quartus II for creating systems including processors, peripherals, and memories. It enables us to define and generate a complete system-on-a-programmable-chip (SOPC) in much less time than using traditional, manual integration methods. For AES as a software component, its complete functionality is described in a higher level language i.e. C-language. The SOPC system for AES as software is depicted in Fig 3.2. The Nios II processor executes the C- code through the NIOS II IDE which is a software development tool. Performance of the system in terms of speed is calculated by a Performance counter core. This core can accurately measure execution time taken by multiple sections/modules of code.

Realized in hardware. Fig 3.3 depicts the SOPC system for AES as Hardware-Software.

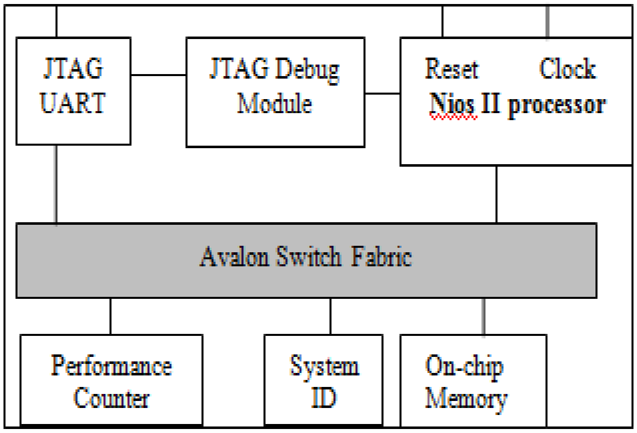


Fig 3.2: SOPC System for AES as Software

3.3.AES: Hardware-Software Approach

The Nios II processor has features or concepts that are unique or different from other discrete microcontrollers. Creating custom components and integrating them into Nios II processor system is one of the unique concepts. For performance-critical systems that spend most CPU cycles executing a specific section of code, it is a common technique to create a custom peripheral that implements the same function in hardware. This approach offers a double performance benefit: the hardware implementation is faster than software; and the processor is free to perform other functions in parallel while the custom peripheral operates on data. AES works on an array of bytes of a 4x4 matrix, which is known as state. All transformations of encryption process are performed only on a state. After each transformation values are stored in a state, this state is the input for the next transformation. AES algorithm has an iterative pattern called round which performs substitution and permutation on the digital data. The round has a module known as SubBytes transformation. The SubBytes transformation is carried out using an already calculated substitution table called S-box. That S-box table contains 256 numbers (from 0 to 255) and their corresponding resulting values. The Key Schedule of AES takes the Cipher Key, K, as input and performs a key expansion routine to generate expanded keys for use by the AddRounKey transformation at the end of every round. The developers of this algorithm included the SubBytes transformation in the key expansion routine to make it more robust. Therefore, taking this extensive use of SubBytes transformation, this project selects it as the module to be realized by hardware i.e. a custom component for the Nios II processor. The decryption process has InvSubBytes transformation; therefore, a custom component for InvSubBytes is also

4. Simulation Environment

In the presented work, AES is implemented using Hardware-Software Co-design methodology. Nios II soft core processor has been selected which is implemented on Altera's Cyclone II FPGA. Quartus II design software is a comprehensive environment for system-on-a-programmable-chip (SOPC) design. The Nios II IDE ia a graphical user interface that is used to build C Applications written for Software part as well as Hardware-Software part and run those applications on the FPGA to get the result in terms of speed i.e. clock cycles. VHDL is used as the Hardware Description language for the design of Hardware Components.

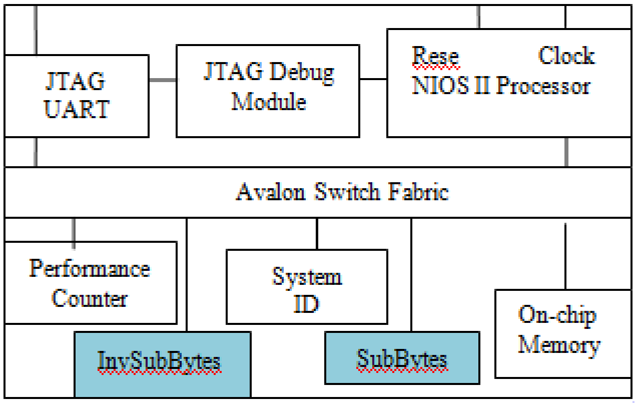


Fig 3.3: SOPC System for AES as Hardware-Software

3.4.SOPC Builder[14,16]:

SOPC Builder automates the task of integrating hardware components. Using traditional design methods, the designer must manually write HDL modules to wire together the pieces of the system. Using SOPC Builder, the designer can specify the system components in a GUI and SOPC Builder then generates the interconnect logic automatically. In addition to that, SOPC Builder generates HDL files that define all components of the system, and a top-level HDL file that connects all the components together. It generates a system interconnect fabric that contains logic to manage the connectivity of all modules in the system.

Decryption Result on Nios II IDE Console: Hardware Software Approach

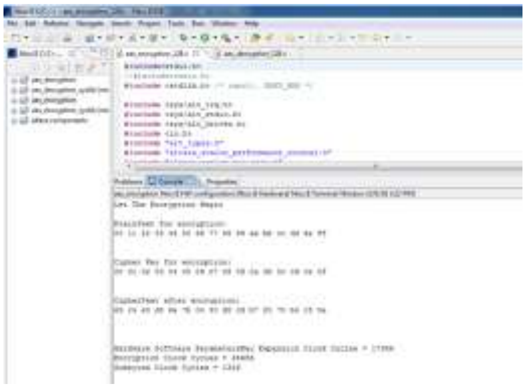
CPU Clock Cycles Comparison

Process	Software Approach	Hardware Software Approach
Key Expansion	469325	17956
Encryption	1857016	48686
Decryption	1944191	134940

Simulation Parameters for the presented work

Parameter	Value
Soft Core Processor	Nios II
FPGA	Cyclone II
FPGA Design Software	Quartus II 8.1
Software Development Tool	Nios II IDE
HDL	VHDL
Design Methodology	HW-SW Co-Design

5.Result and Conclusion



Encryption Result on Nios II IDE Console: Hardware Software Approach

Hardware approach can deal with real-time data feedbacks and software approach can handle complex decision making. The Hardware Software co-design approach offers the substantial flexibility to practically implement and realize the complex systems. The Hardware Software co-design methodology can be easily extended to any application. The application under consideration in the present work is NIST approved Advanced Encryption Standard. By incorporating custom components, the number of clock cycles required get reduced drastically when compared to software only approach and the rise in area due to the inclusion of the custom components is also nominal. Thus, we conclude that Hardware Software Co-Design methodology is capable of enhancing the speed of a system by providing dedicated hardware for selected modules of the system which result in reduction of the number the clock cycles.

SubBytes	182244	1326
InvSubBytes	182244	1326

Synthesis Report Comparison

Items	Total Count	Software Approach	Hardware Software Approach
Total Logic Elements	**33216**	**3131(9%)**	**3687 (11%)**
Total Combinational Functions	**33216**	**2984 (9%)**	**3540 (11%)**
Dedicated Logic Registers	**33216**	**1865 (5.6%)**	**1941 (5.8%)**
Total Memory Bits	**483840**	**342016 (71%)**	**342016 (71%)**
Embedded Multipliers 9-bit elements	**70**	**4 (6%)**	**4 (6%)**

Time to market is a pivotal constraint in deciding the design approach of an application.

REFERENCES

[1] Preeti Dixit, Jitendra Zalke, Sharmik Admane, "Speed optimization of AES algorithm with Hardware-Software Co-design," 2nd International Conference for Convergence in Technology (I2CT), 2017.

Computing, Control and Industrial Engineering, 2010.

[6] P. Moore, M. McLoone and S. Sezer, "Reconfigurable Instruction Interface Architecture for Private-Key Cryptography on the Altera Nios-II Processor," Proceedings of the Advanced Industrial Conference on Telecommunications/Service Assurance with Partial and Intermittent Resources Conference/ELearning on Telecommunications Workshop, 2005.

[7] Prashant G. Salunke, Akbarali M. Sayyed, "Design of Embedded Web Server Based on NIOS-II Soft Core Processor," International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016 Kuan Jen Lin, Chin-Mu Hsiao and Ching Hung Jhan, "Exploring HW/SW Codesign of AES Algorithm Using Custom Instructions", The 13th IEEE International Symposium on Consumer Electronics (ISCE2009).

[8] Meghana A. Hasamnis, S. S. Limaye, "Design and Implementation of Rijindael's Encryption Algorithm with Hardware / Software Co-design Using NIOS II Processor," 7th IEEE Conference on Industrial Electronics and Applications (ICIEA), 2012.

[9]Zabina Kouser, Manish Singhal, Amit M. Joshi, "FPGA Implementation of Advanced Encryption Standard Algorithm," IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2016), December 23-25, 2016.

[2]Onkar S. Dhede, S.K. Shah, “A Review: Hardware Implementation of AES Using Minimal resources on FPGA,” International Conference on Pervasive Computing (ICPC), 2015.

[3] Mohini Mohurlel, Vishal V. Panchbhai, “Review on Realization of AES Encryption and Decryption with Power and Area Optimization,” IEEE International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES-2016).

[4]Amal Hafsa, Anissa Sghaier, Wajih Elhadj Yousef, Mohsen Machhout,Jihene Malek, “Image Encryption/Decryption Design Using NIOSII Soft Core Processor,” ICEMIS2017, Monastir, Tunisia 2017.

[5] Wang Wei, Zhong Guidong, “The Design and Implementation of High-Speed Data Acuisition System Based on NIOS II,” International Conference on

[10] Disha Yadav, Arvind Rajawat, “Area and Throughput Analysis of Different AES Architectures for FPGA Implementations,” IEEE International Symposium on Nanoelectronic and Information Systems, 2016.

[11] N. S. SAI SRINIVAS, MD. AKRAMUDDIN, “FPGA Based Hardware Implementation of AES Rijndael Algorithm for Encryption and Decryption,” International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016.

[12] NIST, “Advanced Encryption Standard(AES),” FIPS PUBS 197, Nov. 2001.

[13] Nios II Processor Reference Handbook by Altera.

[14] Quartus Introduction using Schematic designs by Altera.