Implementation of Advanced Encryption Standard in Vivado Design Suite

[1] Divya M, [2] Dinesha P, [3] Jamuna S
[1,2,3] Department of electronica and communication, Dayananda Sagar college of Engineering, Bangalore

Abstract: System On Chip (SoC) are devices which have a FPGA fabric and a processor in its architecture. SoC are used in remote applications where human intervention is not possible. In such circumstances reconfiguration of the devices are required which can be done on the FPGA fabric. One application where this technique can be used is Advanced encryption standard (AES) is a cryptographic technique where the plain text is of 128 bit. The key used for encryption are of different lengths like 128 bit, 192 bit and 256 bit. The keys are chosen according to the kind of encryption needed. This paper describes the implementation of AES in Vivado with the key length of 128 bits. The implementation of the design is placing the design on the FPGA fabric and the wiring connections. The proposed design is realised using XILINX Vivado 2017.1.

Index Terms **- System on chip, reconfigurable logic, partial reconfiguration, FPGA, key length, Intellectual property.**

I. INTRODUCTION

Field programmable gate arrays (FPGA) are preferred for most applications due to their flexibility of reprogramming. The FPGA fabric along with a processor allows implementation of a System on chip applications on FPGA. Recent FPGAs like ZynqUltrascale+MPSoC CG devices, ZynqUltrascale+MPSoC EV devices, Zynqultrascale+RFSoC with data convertors [1].These have a processor to perform a particular function. They are hardened processors to perform a particular functionality. Whereas the FPGA fabric is reconfigurable. The processor is called the processing system (PS) and the FPGA fabric is called the programmable logic (PL).

Proposed design can be targeted on Zynq 7000 FPGA. A Zynq 7000 SoC has ARM cortex A9 processor which is the processing system (PS) and the FPGA fabric forms the programmable logic. The processing system works with custom software. While the programmable logic enables the implementation of custom logic. The ARM cortex A9 processor is a dual core system which enables using complete operating system like Linux. The FPGA fabric is of Xilinx 7 series. The communication between these two systems is by AXI interfaces which provide high bandwidth, low latency connection between the two regions.

The design process in Vivado involves simulating the design to verify the functionality. Once the design is verified for functionality. It is followed by synthesis and implementation of the design. Once the design is implemented and package pins are assigned. The design is ready for bit streams to be generated.

Advanced encryption Standard (AES) is encryption standards where the plain test is of 128 bits and the keys used are of different lengths. The keys used are of 128 bit, 192 bit and 256 bit. There are number of rounds for each of the keys usually 10 rounds. And encryption is performed by generating new keys in each round [3].

II. BACKGROUND

The programmable logic (PL) and processing system (PS) include different components to realise a particular function. The processor is Zynq 7000 SoC with dual core capable of running an operating system like Linux in one core and another like FreeRtos in another core. The programmable logic(PL) include combinational logic blocks(CLBs), slice, look up tables(LUT),flip flop(FF), switch matrix, input output blocks(IOBs). Combinational logic blocks are regular grouping of logic elements in a two dimensional array on programmable. Slices are a sub unit within the CLB contains resources for implementing combinational and sequential logic circuits. LUT is a flexible resource capable of implementing a logic function of up to six inputs, a ROM, RAM, shift register. Flip flop is a sequential circuit implementing a 1bit register with reset functionality. Switch matrix is placed next to each CLB, provides a flexible routing facility for making connection between elements with CLB and from CLB to resources on the PL. Input /Output Blocks provide interfacing between PL logic resources and physical device pads to connect to external circuit. Zynq is equipped with these capabilities to realize the appropriate functionality using the required peripherals as and when required [4].

The plain text of 128 bits is divided into blocks of 32 bits such that they appear as rectangular rows and columns which can be denoted by letter Nb [6]. The different operations performed are shift rows, mix columns, key generation, add round key and generate the cipher text. Ten rounds of the iteration are performed and finally the cipher text is generated [3].

The process of encryption in AES is done by adding round keys to each round of encryption. The number of rounds is chosen according the length of the key like 128 bit \, 192 bit and 256 bit. The next step is substitution of the bytes by elements of the S-box. Followed by mixing rows of the column where the bytes are shifted. Once the bytes are shifted. The next step is mixing columns, where the bytes are multiplied by elements of Galois field. The last step of the design is adding the round key. And the same step is repeated for a number of rounds. The same process is repeated for decryption. But the substitution is done by using inverse S-box.[3] The implementation of the design is done in Vivado. Intellectual property (IP) for AES is created using the tool. The created IP is synthesized and implemented.

III. PROPOSED WORK

This paper describes the implementation of AES on vivado. The tool invoking is done using the Vivado project flow. The code is written, debugged and simulated to verify the functionality. The simulation results are shown in Fig 1.

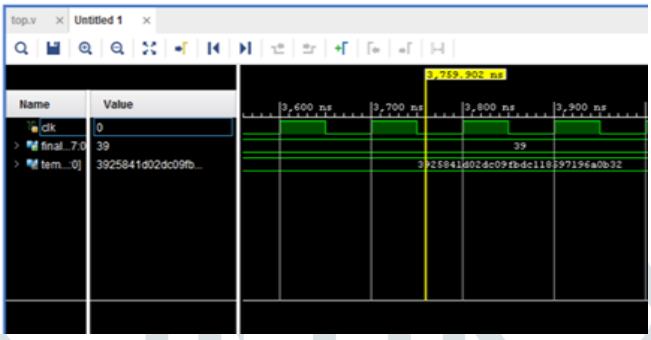

Fig 1: Simulation of AES encryption

The code for AES is simulated to verify the functionality of the design. Once the design is simulated. Synthesis of the design is performed to generate the check point files for the design. These files act as constraints for the design to define regions on the FPGA fabric. The Intellectual property (IP) for the design is created with the Zynq processing system and reset system with the Advanced Extensible Interconnect (AXI). This standard is used for communication with the Zynq processing system and the created custom IP. The results obtained are described in the next section.

IV. RESULTS AND DISCUSSION

The technique of implementation in Vivado is described. After the simulation is performed and the functionality is verified. In order to implement the design .Intellectual property (IP) can be used. In this method the different modules of the design like Zynq processing system, the reset system and the AXI interconnect are created. And the created IP for AES will communicate with this block through this interface of AXI. After this process the synthesis, implementation of the design is performed. Once the synthesis and implementation is performed the bit streams are generated. The tool can be enabled for partial reconfiguration. The IP can also be added to a reconfigurable partition as a reconfigurable module. And the technique of partial reconfiguration can also be applied. The created IP with the Zynq processor and the reset system is shown in Fig 3. The Advanced eXtensible Interface (AXI) peripheral communicates with the Zynq processor, the reset system and the created IP for AES. Once the IP is created the top level wrapper code for the design is generated. This top level wrapper includes all the registers, the clocks and the reset system used for the design. It also includes option to add user logic.

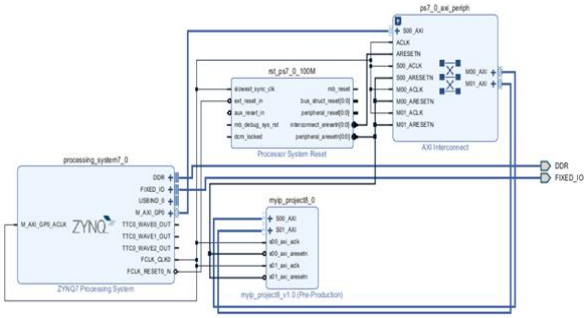

Fig.2 IP creation for AES

The logic of AES is included in the wrapper code for the IP where the input and output ports are to be defined. Once this step is done the synthesis is done in global context mode and added as a reconfigurable module in a partially reconfigurable design. The implemented of design is done followed by bit stream generation. The final implemented design with all the wiring connections is shown in Fig 3.

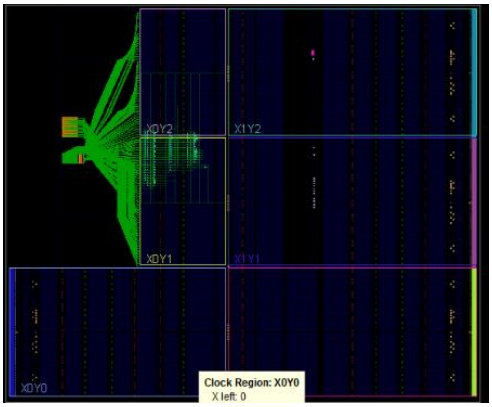

Fig 3: The implementation of AES in vivado

V. CONCLUSION AND FUTURE SCOPE

This paper explained the implementation of Advanced Encryption Standard in Vivado. The paper describes the method of IP creation to synthesize and implement the design. Once the IP for the design is created it can be implemented on Zedboard. The IP can also be added as a reconfigurable module in a reconfigurable partition to enable partial reconfiguration of the design.

ACKNOWLEDGEMENT

This work is been carried out as a part of DRDO sponsored research work on fault tolerant computing in the Department of ECE. We thank DRDO for the support provided.

REFERENCES

[1] https://www.xilinx.com/products/silicon-devices/soc.html

[2] Xilinx UG909 User guide for partial reconfiguration

[3]William Stallings, “Crytography and Network security”

[4] The Zynq book

[5]Aaron Stoddard,Ammon Gruwell,Peter Zabriskie,”High-speed PCAP configuration scrubbing on Zynq-7000 All Programmable SoCs”,Field Programmable Logic and Applications (FPL) 26th International Conference,2016

[6] Ashwini M Deshpande, Mngesh S Deshpande, Devendra N. Kayatanavar ,”FPGA Implementation of AES Encryption and Decryption”, International conference on control, automation, communication and energy conservation, 2009

[7] Xilinx UG585 Zynq 7000 Technical reference manual

[8] Xilinx UG1165 Zynq 7000 all programmable SoC:Embedded design tutorial

[9]. Vivado user guide on partial reconfiguration- UG 947

[10]. Technical reference manual for Zynq devices- UG 585

[11].Vivado user guide Creating, Packaging Custom IP tutorial- UG 1119

[12].ZC702 Evaluation Board for the Zynq-7000 XC7Z020 All Programmable SoC- UG 850

[13].Zynq-7000 All Programmable SoC Data Sheet - DS190

[14].Vivado User guide Implementation - UG904

[15].Vivado user guide Synthesis – UG901