FPGA IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD ALGORITHM

Aparna Ambule[1], Dr. Y. V. Chavan[2]

[1,2] *Padmabhooshan Vasantdada Patil Institute of Technology, Pune, MS (India)*

ABSTRACT

In this paper The Advanced Encryption Standard was implemented with pure Hardware. However Field Programmable Gate Arrays (FPGAs) offer a more speed than existing implementations. This research investigates the AES algorithm with regard to 256 bits message length and 192 bits key length. In Spartan3 EDK we implemented the AES algorithm through pipelined architecture through the soft core processor Micro Blaze which in deed used for developing a Hardware structure which is configured using System C coding.

Keywords: Advanced Encryption Standard, FPGA, VHDL.

I. INTRODUCTION

AES is the Advanced Encryption Standard, a United States government standard algorithm for encrypting and decrypting data. The standard is described in FederalInformation Processing Standard (FIPS) 197.

1. On January 2, 1997, The National Institute of Standards and Technology (NIST)published a request for comments for the "Development of a Federal InformationProcessing Standard for Advanced Encryption Standard."

2. NIST sought to "considerealternatives that offer a higher level of security" 3. Than that offered by the Data EncryptionStandard (DES), which grew vulnerable to brute-force attacks due to its 56-bit effectivekey length.AES candidates were required to support a symmetric block cipher that supported multiple key lengths. The algorithm had to be publicly defined, free to use, and able to run efficiently in both hardware and software.4. Fifteen AES candidate algorithms were announced in August, 1998. Five finalists were chosen on August 9, 1999.

II. AES ALGORITHM

AES is a symmetric block cipher with a block size of 128 bits. Key lengths can be 128 bits, 192 bits, or 256 bits;8 called AES-128, AES-192, and AES-256, respectively. AES- 128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds.

The main loop of AES9 performs the following functions:

- **SubBytes ()**
- **ShiftRows ()**
- **MixColumns ()**
- **AddRound Key()**

The first three functions of an AES round are designed to thwart cryptanalysis via the methods of "confusion" and "diffusion." The fourth function actually encrypts the data. Claude Shannon described the concepts of confusion and diffusion in his seminal 1949 paper, "Communication Theory of Secrecy Systems:"

"Two methods suggest themselves for frustrating a statistical analysis. These we may call the methods of *diffusion* and *confusion*."10.

Diffusion means patterns in the plaintext are dispersed in the cipher text. Confusion means the relationship between the plaintext and the cipher text is obscured.

A simpler way to view the AES function order is:

1. Scramble each byte (SubBytes).
2. Scramble each row (Shift Rows).
3. Scramble each column (Mix Columns).
4. Encrypt (Add Round Key).

A term associated with AES is "the State," an 'intermediate cipher,'11 or the cipher text

Before the final round has been applied.

AES formats plaintext into 16 byte (128-bit) blocks, and treats each block as a 4x4 State array. It then performs four operations in each round. The arrays contains row and column information used in the operations, especially Mix Columns() and Shift rows ().

2.1 Sub Bytes ()

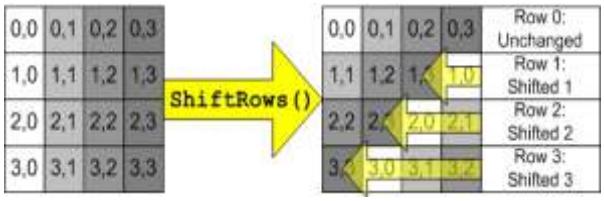
Sub Bytes () adds confusion by processing each byte through an S-Box. An S-Box is a substitution table, where one byte is substituted for another, based on a substitution algorithm. Here is the AES Substitution is

| 0 1 2 3 4 5 6 7 8 9 a b c d e f

To complete an S-Box operation on an example string of "ABC," take the hexadecimal value of each byte. ASCII "A" == hex 0x42, "B" == 0x43 and "C" == 0x44. Look up the first (left) hex digit in the S-Box column and the second in the S-Box row. 0x42 becomes 0x2c; 0x43 becomes 0x1a, and 0x44 becomes 0x1b.

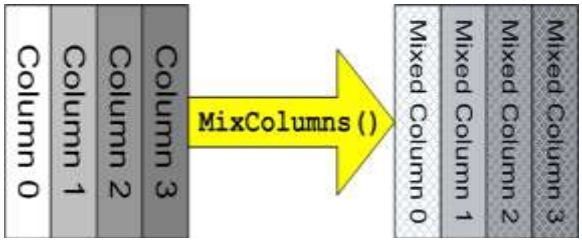
2.2 Shift Rows ()

Shift Rows () provides diffusion by mixing data within rows. Row zero of the State is not shifted, row 1 is shifted 1 byte, row 2 is shifted 2 bytes, and row 3 is shifted 3 bytes, as shown in the *FIPS* illustration that follows:



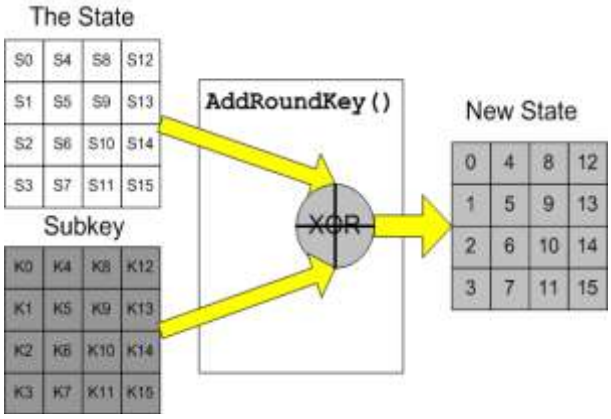
2.3 Mix Columns ()

Mix Columns () also provides diffusion by mixing data within columns. The 4 bytes of each column in the State are treated as a 4-byte number and transformed to another 4-byte number via finite field mathematics, as shown in the FIPS illustration that follows:



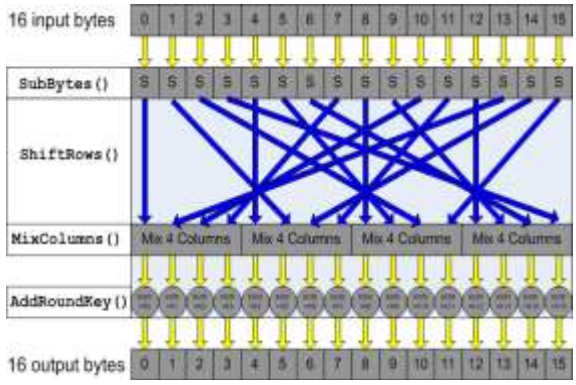
2.3 AddRound Key ()

The actual 'encryption' is performed in the AddRoundKey () function, when each byte in the State is XORed with the subkey. The subkey is derived from the key according to a key expansion schedule, as shown in the *FIPS* illustration that follows:



2.4 One Round of AES

Here is one round of AES encryption, shown in the FIPS publication two dimensionally:



III. AES DECRYPTION

Decryption occurs through the function AddRoundKey (), plus the inverse AES functions InvShiftRows(), InvSubBytes(), and InvMixColumns(). AddRoundKey() does not require an inverse function, as it simply XORs the state with the sub key (XOR encrypts when applied once, and decrypts when applied again).

IV IMPLEMENTATION

The Field Programmable Gate Array is majorly used for generation ASIC IC's to the computations. They offer more speed in execution process. SO, for generation ASIC IC's FPGA's are majorly used. The 64 FFT with radix 4 is simulated and synthesized as well as implemented on the FPGA of below configuration.

Table3.1: Configuration of FPGA

Property Name	Value
Family	Spartan 3
Device	XC3S200
Package	TQG144
Speed Grade	-4

4.1 Xilinx Platform Studio

The Xilinx Platform Studio (XPS) is that the development atmosphere or user interface used for planning the hardware portion of your embedded processor system. B. Embedded Development Kit Xilinx Embedded Development Kit (EDK) is associate integrated software system tool suite for developing embedded systems with Xilinx MicroBlaze and PowerPC CPUs. EDK includes a spread of tools associated applications to help the designer to develop associate embedded system right from the hardware creation to final implementation of the system on an FPGA. System style consists of the creation of the hardware and software system parts of the embedded processor system and also the creation of a verification element is elective. A typical embedded system style project involves: hardware platform creation, hardware platform verification (simulation), software system platform creation, software system application creation, and software system verification. Base System Builder is that the wizard that's wont to mechanically generate a hardware platform in keeping with the user specifications that's defmed by the MHS (Microprocessor Hardware Specification) file. The MHS file defines the system design, peripherals and embedded processors]. The Platform Generation tool creates the hardware platform mistreatment the MHS file as input. The software system platform is defmed by MSS (Microprocessor software system Specification) file that defines driver and library customization parameters for peripherals, processor customization parameters, customary one hundred ten devices, interrupt handler routines, and different software system connected routines. The MSS file is associate input to the Library Generator tool for personalisation of drivers, libraries and interrupts handlers.

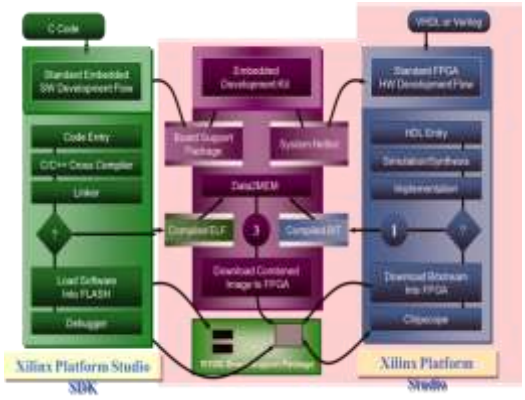


Figure4.1: Embedded Development Kit Design Flow

The creation of the verification platform is facultative and is predicated on the hardware platform. The MHS file is taken as Associate in Nursing input by the Siegen tool to make simulation files for a particular machine. 3varieties of simulation models will be generated by the Siegen tool: behavioral, structural and temporal arrangement models. Another helpful tools on the market in EDK ar Platform Studio that provides the GUI for

making the MHS and MSS files. Produce / Import IP Wizard thatpermits the creation of the designer's own peripheral and import them into EDK comes. Platform Generator customizes and generates the processor system within thesort of hardware net lists. Library Generator tool configures libraries, device drivers, file systems and interrupt handlers for embedded processor system. Bit stream Initializer tool initializes the instruction memory of processors on the FPGA shown in figure2. antelope Compiler tools are used for collection and linking application executable for every processor within the system [6]. There are2choiceson the market for debugging the appliance created victimization EDK namely: Xilinx microchipcorrect (XMD) for debugging the appliance package employing a microchip correct Module (MDM) within the embedded processor system, and package programmer that invokes the package programmer appreciate the compiler getting used for the processor. C. package Development Kit Xilinx Platform Studio package Development Kit (SDK) is Associate in Nursing integrated development atmosphere, complimentary to XPS, that's used for C/C++ embedded package application creation and verification. SDK is made on the Eclipse open source framework. Soft Development Kit (SDK) may be a suite of tools that allows you to style a package application for elite Soft IP Cores within the Xilinx Embedded Development Kit (EDK).The package application will be written during a "C or C++" then the entire embedded processor system for user application are completed, else correct&download the bit file into FPGA. Then FPGA behaves like processor implemented on it in a Xilinx Field Programmable Gate Array (FPGA) device.

Hardware implementation was through system C coding and its results are as follows

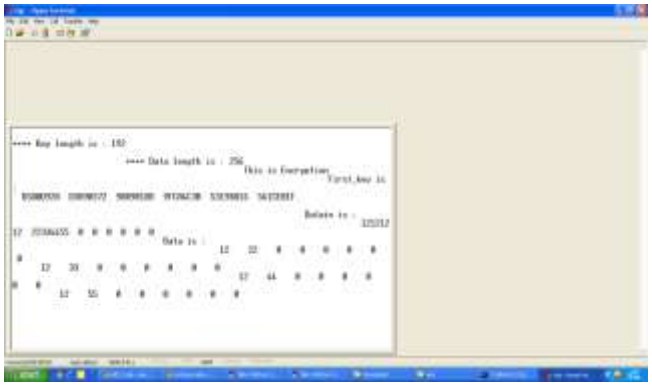


Fig: FPGA Sent Data was Seen in Pc Through Hyperterminal

Fig: Synthesis Report

V. CONCLUSION

In this work Advanced Encryption algorithm was implemented using FPGA. This system works on a period pipelined flow on the Micro Blaze architecture of Spartan3 EDK. On the opposite hand, synthesis results show

that space consumption is low, using simply 100 percent of logic components of FPGA forAES, permitting the implementation of this method over inexpensive FPGAs.

REFERENCES

[1] FIPS FIPS-197, Federal Information Processing Standards Publication FIPS-197, Advanced Encryption Standard (AES), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 1999.

[2] DAEMEN, J. AND RIJMEN, V., The design of Rijndael: AES — The Advanced Encryption Standard. Springer-Verlag, 2002.

[3] SCHNEIER, B., Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley & Sons, Inc. 2nd Ed, 1996.

[4] GOMES, O. S. M.; PIMENTA, T. C.; MORENO, R. L., "A Highly Efficient FPGA Implementation", 2nd Latin America Symposium on Circuits and Systems (LASCAS-2011), February 2011.

[5] DAEMEN, J. AND RIJMEN, V. A Specification for The AES Algorithm. NIST (National Institute of Standards and Technology).http://csrc.nist.gov/archive/aes/rijndael/wsdindex.html , 2010.

[6] Ahmad, N.; Hasan, R.; Jubadi, W.M; “Design of AES S-Box using combinational logic optimization”, IEEE Symposium on Industrial Electronics & Applications (ISIEA), pp. 696-699, 2010.

[7] Alex Panato, Marcelo Barcelos, Ricardo Reis, “An IP of an Advanced Encryption Standard for Altera Sevices”, SBCCI 2002, pp. 197-202, Porto Alegre, Brazil, 9 and 14 September 2002.