Design OF Advanced Encryption Standard Algorithm Using Xilinx Project Navigator, ISE 13.1

Shubhangi V. Funde[1], Dr.D.V.Padole [2]

[1]PG Scholar ,Dept. of electronics Engineering ,G.H.Raisoni College of engineering, Nagpur (M.S),India.
sshubhangis90@gmail.com
[2]Professor,Dept. of Electronics Engineering, G.H.Raisoni College of Engineering, Nagpur(M.S.),India

Abstract- Security is the weighty part in wireless communication system, where more randomization in secret keys increases the security as well as complexity of the cryptography algorithms. The AES is used to protect data in cryptography. It is a symmetric block cipher in which encryption and decryption is takes place. For the performance AES algorithm is discussion from its starting publication. The propose method is to design AES algorithm by using Xilinx ISE 13.1. The simulated result shows the different parameters such as power and time of AES algorithm.

Keywords: Substitution, Encryption, Decryption, Plain text, cipher text, VHDL.

1. Introduction

The hardware implementation of the AES algorithm is created for external data storage unit in application. Rijndael is a symmetric block cipher which can process data blocks of 128 bits (4 words), AES is dived into three types , namely AES - 128, AES - 192, and AES-256, In this algorithm 128, 192 and 256 is a key length for the above three types and 10,12 and 14 rounds respectively are takes place. In cryptography, the AES is also known as Rijndael which is a block cipher decide as an encryption standard. It is capable to protect sensitive information. This algorithm is a symmetric block cipher, which encrypt and decrypt information. Encryption converts data in to cipher-text. Decryption of the cipher-text converts into its original form that is plaintext. AES generally allows a 128 bit data length that can be divided into four basic operation blocks. These blocks are Substitute Bytes, Shift rows, Mix columns, Add round key. The algorithm starts with the Add round key stage for both encryption and decryption algorithm.

2. AES Algorithm

AES algorithm encryption and decryption process is shown in Fig.1, in which Inversed its encryption process will be able to decrypt the cipher text.

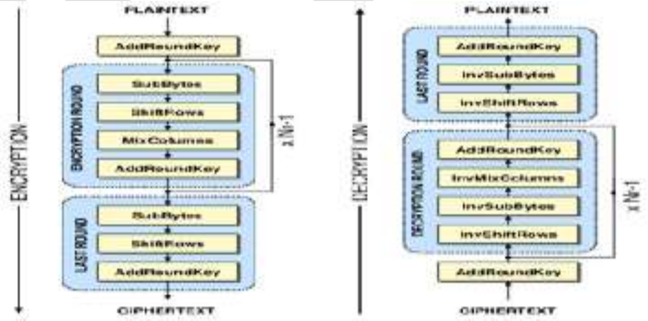


Fig 1. AES algorithm

1. Sub Bytes: During the forward process substitution takes place this substitution depends on bytes. 16x16 lookup table used in the sub bytes.
2. Shift Rows: Shift rows are a cipher result. It contains four rows; the first line of State remains the same, the second, third and fourth shifted by one, two and three respectively.
3. Mix Columns: In the Mix Columns transformation, every column work independently and a new value represents by every byte. In this transformation Matrix multiplication is take place.
4. Add-Round Key: Here add-round key is added in the previous output. XOR operation is used to combine the state byte with the expanded key.

3. The Encryption Key and Its Expansion

The key is arranged in the form of a matrix of 4 × 4 bytes. Here length of key is 128-bit is used, first word is saved in column. These words are arranged in 44 words. They are represented as W0, W1..........W43.

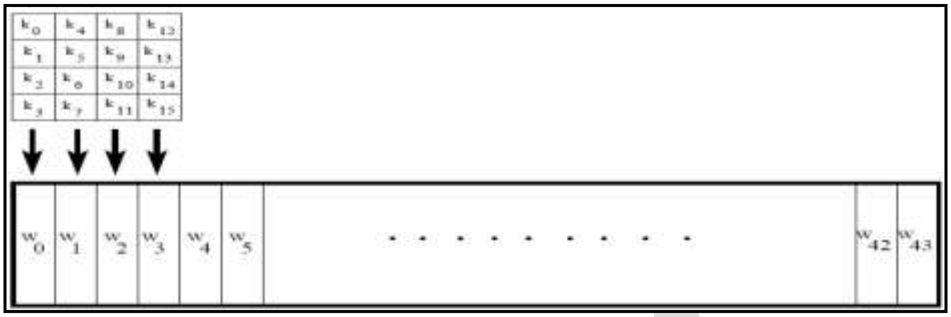


Fig.2 Expanded key schedule

4. Proposed System

For the power consumption the hardware implementation is takes place because it is better than software implementation. The hardware / software partitioning is the process in which application divided between software which is executed on a microprocessor and hardware implemented on an FPGA. The Xilinx Platform Studio (XPS) is used for design the hardware portion of embedded processor system.

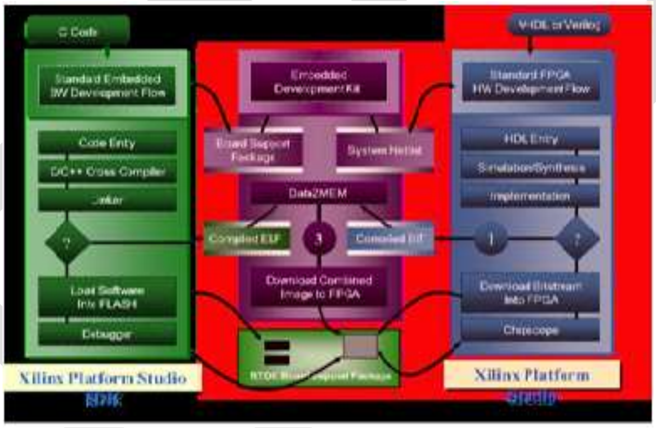


Fig.3 Design Flow of EDK

EDK consist the hardware and software system which are the important part of the embedded processor system.

Xilinx Platform Studio (XPS): It is used for designing the hardware portion of embedded system. This h/w then implemented on the FPGA with the help of microblez.

Software Development Kit (SDK): It is used to design the software portion of the embedded system which is then implemented on the FPGA.

5. AES with Hardware for Encryption and Decryption (VHDL)

In figure 4, 128 bit length key is used in the plain text. With the help of 2:1 MUX, encryption of AES is controlled.

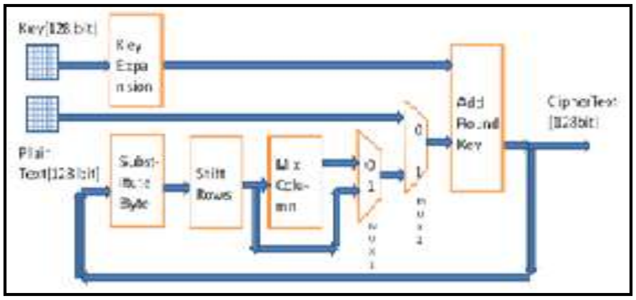


Fig.4- AES with hardware for encryption

With the help of two 2:1 MUX Flow of Decryption is controlled .These muxes is used to decide the path of execution. Because of the flexibility VHDL is used as the hardware description language.

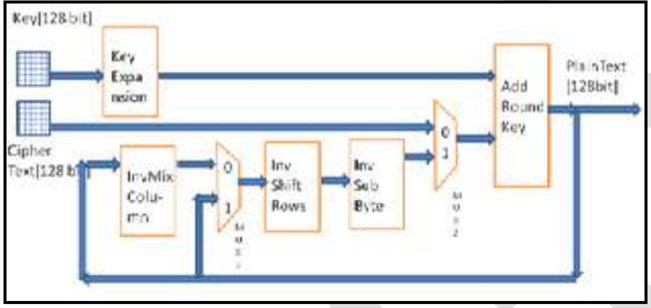


Fig.5 AES with hardware for decryption

The software used for this work is Xilinx ISE 13.1 suite. This software is used for writing, debugging and optimizing efforts, and also for fitting, simulating and checking the performance results using the simulation tools.

6. Simulation Result

Fig 5 shows the simulated result of encryption and decryption on ISE13.1.

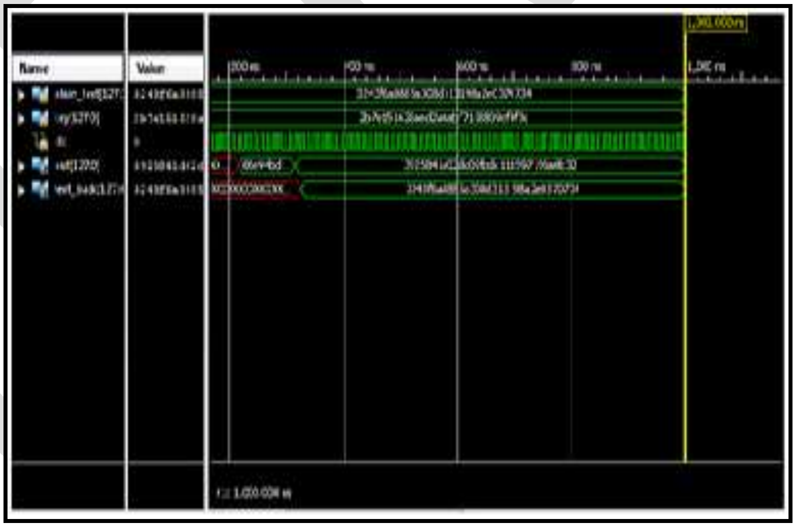


Fig.6 Simulation Result

Simulation Test Vectors For Encryption and Decryption process:
PlainText:128'h3243f6a8_885a308d_313198a2_e03704;
Key: 128'h2b7e1516_28aed2a6_abf71588_09cf4f3c;
Cipher Text: 3925841d02dc09fbdc118597196a0b32
Text back: 128'h3243f6a8_885a308d_313198a2_e03704;

7. Power Analysis and Time Analysis

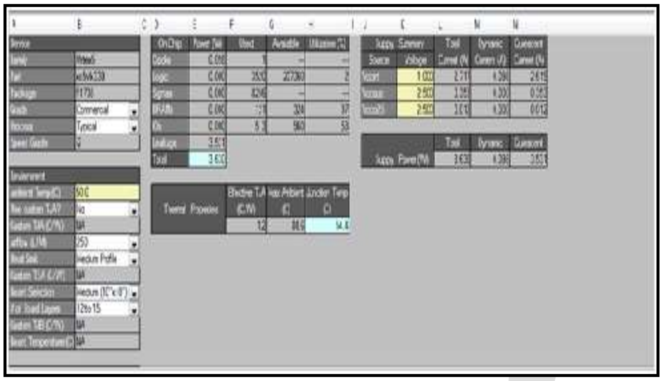
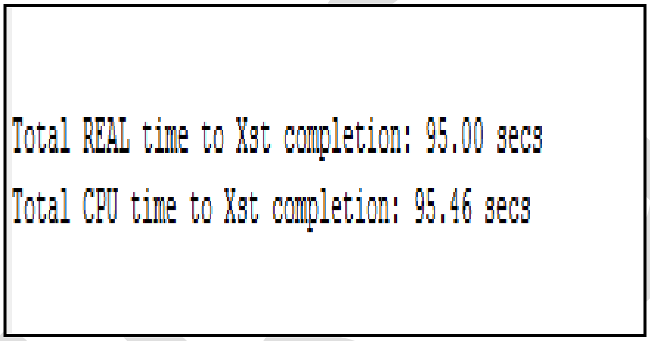


Fig.6 analysed power

X-Power Analyzer is graphical tool. With the help of this tool analyse the power used for the synthesis of AES on Xilinx ISE 13.1. Here total power used for synthesis is 3.630W.



```
Total REAL time to Xst completion: 95.00 secs
Total CPU time to Xst completion: 95.46 secs
```

Fig.7Time analysis

For the synthesis of AES in real time it takes total 95.oo secs and for CPU it takes 95.46 sec.

8. Conclusion and Future Work

This paper introduces a design scheme to implement an AES IP Core based on key lengths. Future work will be Design software and Hw/Sw code-sign and implement on Spartan6. For the Software implementation, C language is used and for the hardware development VHDL is preferred. This co-design is implemented using Xilinx platform studio and evaluates the parameters of AES algorithm for the performance evaluation.

REFERENCES:

1. Yang , Jun Ding ,"FPGA-Based Design And Implementation Of Reduced AES Algorithm", 978-0-7695-3972-0/10 $26.00 © 2010 IEEE
2. AES Overview. Intel® Advanced Encryption Standard (AES) New Instructions Set323641-001 Revision 3.0 May 2010
3. Vilas V Deotare, Dinesh V Padole, Ashok S. Wakode,'' Performance Evaluation of AES using Hardware and Software Codesign'', ISSN: 2321-8169 Volume: 2,june 2014
4. Santhosh Kumar. D, K.Navatha, Dr.Syed mushtak Ahmed,'' Implementation of AES Algorithm on Micro Blaze Processor in FPGA'', International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013
5. Meghana A. Hasamnis, ," Design and Implementation of Rijindael's Encryption Algorithm with Hardware / Software Co-design Using NIOS II Processor†"† 78-1-4577-2119-9/12/$26.00_c 2011 IEEE
6. Hoang Trang, Nguyen Van Loi," An efficient FPGA implementation of the Advanced Encryption Standard algorithm", 978-1-4673-0309-5/12/$31.00 ©2012 IEEE
7. Ciprian Leonard Pițu, Ciprian Leonard Pițu, Radu Câmpeanu.'' Differential Power Analysis: Simulated versus Experimental Attacks'', 978-1-4799-1555-2/13/$31.00 ©2013 IEEE
8. M.Sambasiva Reddy, Mr. Y. Amar Babu,'' Evaluation Of Microblaze and Implementation Of AES Algorithm using Spartan-3E'', international journal of advanced research in electrical, electronics and instrumentation engineering*vol.* 2, issue 7, july 2013
9. MicroBlaze overview.
http://www.xilinx.com/support/documentation/sw_manuals/xilinx14_2/mb_ref_guide.pdf
10. Medhat H. A. Awadalla, Kareem Ezz El-Deen, Kareem Ezz El-Deen, "Real-Time Software Profiler for Embedded Systems"Department of Computer Science, Faculty of Computers and Information / Organization Name,University of Fayoum, Egypt