



International Journal of Engineering, Business and Enterprise Applications (IJEBA)

www.iasir.net

DESIGN & IMPLEMENTATION OF AES ALGORITHM OVER FPGA USING VHDL

Pallavi Atha
Electronics & Communication
Suresh Gyan Vihar University
Mahal Jagatpura Jaipur, Rajasthan
India

Abstract: Security is an important parameter to be considered with the growth of electronic communication. A key is used in algorithms for cryptography in which the same key value is used in both the encryption and decryption. Secret key cryptography follows an algorithm that is Advanced Encryption Standard (AES) algorithm. The AES algorithm uses cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data. This methodology uses VHDL implementation over FPGA. We have programmed in Xilinx – 10.1 xst software and implemented on FPGA families which are Spartan2, Spartan3 and Virtex2.

Keywords: : AES, FPGA, Encryption, Decryption, Cryptography.

I. Introduction

Nowadays cryptography has a main role in embedded systems design. In many applications, the data requires a secured connection which is usually achieved by cryptography.

Advanced Encryption Standard (AES), is an approved cryptographic algorithm that can be used to protect electronic data. This paper presents the AES algorithm with regard to FPGA and VHDL this proposes a method to integrate the AES encrypter and the AES decrypter. This method can make it a very low-complexity architecture, especially in saving the hardware resource in implementing the AES (Inv) Sub Bytes module and (Inv) Mix columns module etc. Most designed modules can be used for both AES encryption and decryption. Besides, the architecture can still deliver a high data rate in both encryption/decryption operations. The proposed architecture is suited for hardware-critical applications, such as smart card, PDA, and mobile phone, etc.

Objective of the dissertation is to perform an efficient method of implementing a AES algorithm having high performance in terms of delay while maintaining the proper functionality of the system. The software used for the implementation of the algorithm is Xilinx 10.1 – xst and language used is VHDL. Simulation of encryption process of the AES algorithm has been done using the Xilinx software. Inputs will be converted into binary form and given as input to the "Model-Sim Simulator" of Xilinx 6.1. The organization of paper includes, First of all the description of all the steps of algorithms with appropriate diagram then the waveform of results has been shown.

II. Steps Of Aes Algorithm

The AES consists of mainly two units which are Data processing unit and the other one is Key Expansion unit. The Data processing unit have four main modules or transformations in which sub byte transform, shift rows, mix column and add round key are involved and the Key Expansion unit generate the round key for the next round.

2.1 Sub Byte Transformaion

A substitution process in byte-by-byte during the forward process. The substitution step used to decrypt AES is known as Inv Sub Bytes. This process refers a 16×16 lookup table to find replacement of byte for a given byte in the input state array. The lookup table are formed by using t multiplicative inverses in $GF(2^8)$ and bit scrambling to destroy the bit-level correlations inside each byte.

4 transformations:



Figure. 1 Steps Used In Data Processing Unit Of AES

2.2 Shift Row Transformation

Shifts the rows in State cyclically in different offsets. Transformation is almost the same in the decryption process except that the shifting offsets have different values. The goal of this transformation is to scramble and correlate the byte order inside each 128-bit block.

2.3 Mix Column Transformation

This Transformation is for mixing up of the bytes in each column separately during the forward process. The corresponding transformation during decryption is denoted Inv Mix Columns and stands for inverse mix column transformation. The goal is here is to further scramble up the 128-bit input block.

2.4 Add Round Key and Key Expansion

In this operation, the round key is applied to the State by simple bit by bit XOR. Key Expansion unit generates the next round key as for three different key size, AES consist of 10, 12 or 14 rounds. After every round a new round key is produced.. This process utilizes the concept of shifting the bytes and substitution of bytes which were used in Data processing unit. The whole encryption unit is shown in Figure 2.

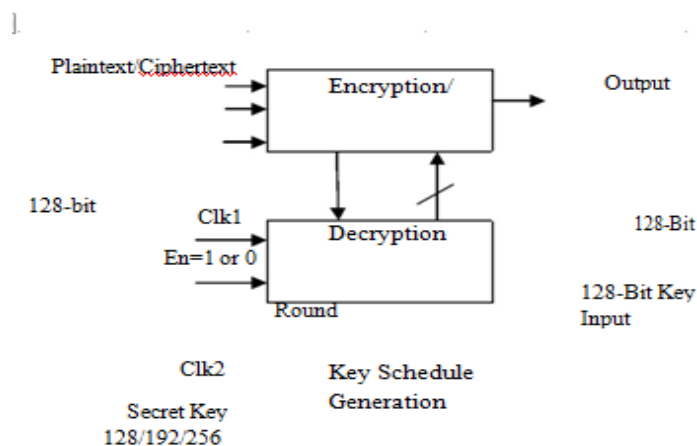


Figure 2: RTL diagram of AES

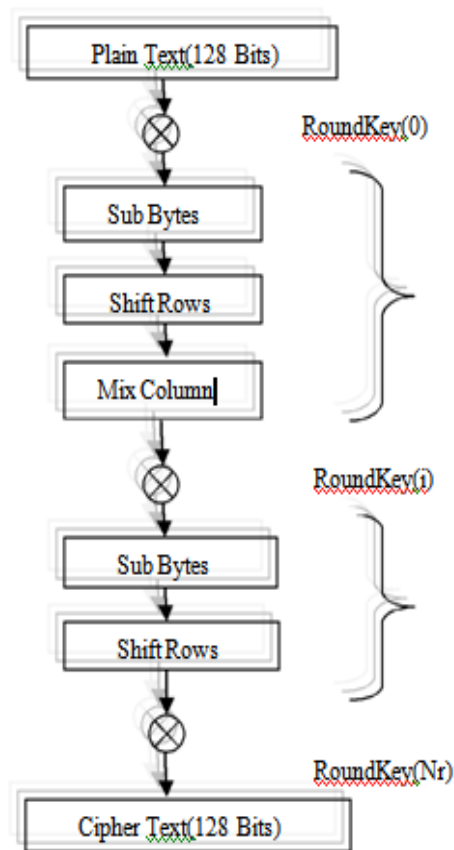


Figure 3: The AES algorithm Encryption structure

III. Results

Calculations are done with Virtex 2E and Device used is XC2S200 and output result has been written down for the further reference.

Time and speed analysis

Time taken by aes 128 = 4.356 sec

Memory used = 524 MB

Speed = 62.352 MB/SEC

POWER IN SPARTAN 2E KIT-

MIX COL = 28.20 MW

SHIFT = 28.20 MW

Subyte = 26.36 MW

Netlist of the AES system is shown in figure 3

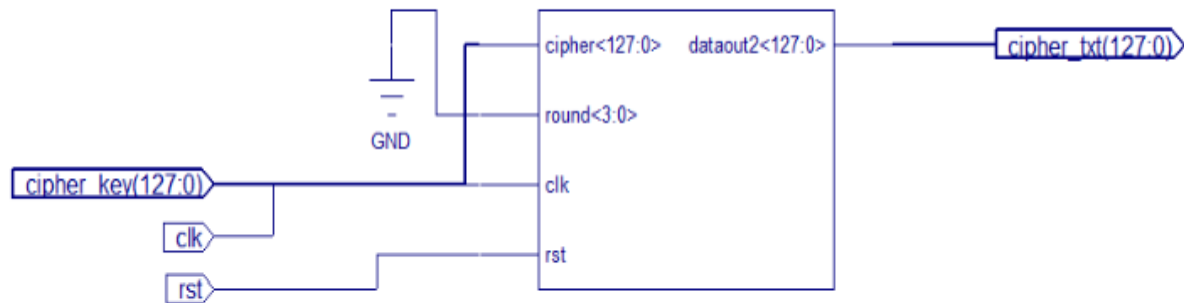


Figure 3: The netlist of AES algorithm

The output which has been framed in the software Xilinx 10.1 is shown in figure 4

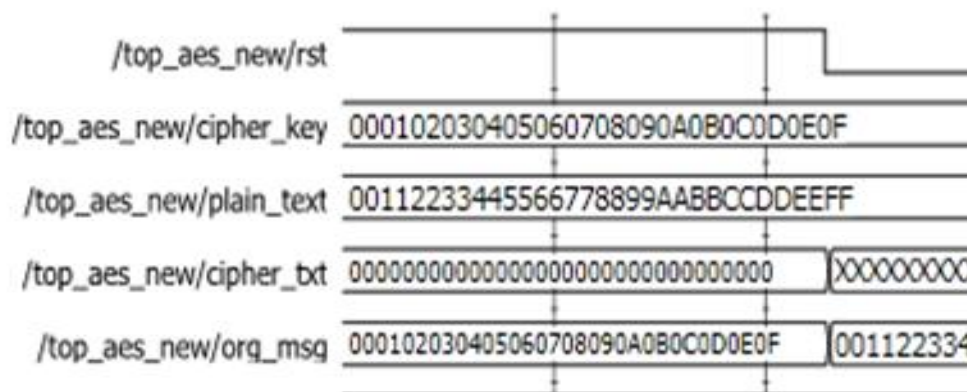


Figure 4: Output graph

IV. Conclusion

In this paper, I have briefly explained about the basics of AES algorithm and the implementation of its modules by using VHDL. The simulations are performed with different device families. The software we have used is Xilinx6.1i and the waveforms are simulated with model sim simulator. The calculations of Time, Speed & power have been done for appropriate output.

V. Future scope

For future work,

- This AES algorithm may be implemented by selection of cipher key bits (128,192 or 256).
- For higher throughput, 16 S-Box can be used completing whole processes around 44-50 cycles(at the same time, compromising the silicon area)
- Graphical User Interface (GUI) can also be made which may be interactive with the user.

VI. References

- [1] Chih-Peng Fanand and Jun-Kui Hwang “FPGA Implementations Of High Throughput Sequential And Fully Pipelined AES Algorithm” *International journal of Electrical Engineering*, vol.15, no.6, pp. 447-455, 2008.
- [2] Mehran Mozaffari-Kermani and Arash Reyhani-Masoleh Efficient and High Performance Parallel Hardware Architecture for the AES-GCM” *IEEE Transactions On Computers*, vol.61, no. 8, August 2012.
- [3] Saambhavi Baskaran and Pachamuthu Rajalakshmi “Hardware Software Co-Design of AES on FPGA” *ICACCI '12,ACM* August 2012.
- [4] Ashwini M. Deshpande, Mangesh S. Deshpande and Devendra N. Kayatanavar “FPGA Implementation of AES Encryption and Decryption” *International Conference on Control, Automation, Communication and Energy conservation* -2009

VII. Acknowledgements

I hereby take the opportunity to express deep sense of gratitude to Tevatron Technologies Pvt. Ltd. for the motivation, guidance and supervision. They help us in all respects for finishing this project and hence gave a good working environment for doing the project.