International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

Implementation of cryptography technique using AES algorithm

M. Sony[1]; P. Vijetha[2] & Dr. B. R. Vikram[3]
[1]M.Tech(VLSI_SD) Dept ECE Mallareddy,Hyderabad
[2]M.Tech,LMISTE Internal Guide Mallareddy,Hyderabad
[3]M.E,Ph.d,MIEEE,LMISTE Principal Mallareddy,Hyderabad

Abstract-

All of the cryptographic algorithms we have looked at so far have some problem. The earlier ciphers can be broken with ease on modern computation systems. As a result of technology scaling and higher integration densities there may be variations in parameters and noise levels which will lead to larger error rates at various levels of the computations. As far as memory applications are concerned the soft errors and single event upsets are always a matter of problem. As a result of technology scaling and higher integration densities there may be variations in parameters and noise levels which will lead to larger error rates at various levels of the computations. As far as memory applications are concerned the soft errors and single event upsets are always a matter of problem. In this project we add the key and shuffle the data it is very hard for the unknown person to find out the original data. Since for each key there will be a change in the cipher text and so the person has to know the key in order to find out the original data. The AES algorithm involves the process of giving the data and key as input to the encryption block and then implementing several blocks such as key schedule block, control block, round function block, etc. In this project, we aim at designing a high speed and high performance but cost-effective FPGA based processor which encrypts and /or decrypts the data that has to be transferred from one PC to the other, based on the Advanced Encryption Standard (AES) algorithm.

Keywords: Euclidean geometry low-density parity check (EGLDPC); memory; control logic; Cryptography; AES; FPGA

I. INTRODUCTION

Cryptography

The branch of cryptology dealing with the design of algorithms for encryption and decryption, intended to ensure the secrecy and/or authenticity of messages. An original message is known as the plain text, while the coded message is called the cipher text. The process of converting the plain text to cipher text is known as enciphering or encryption; restoring the plain text from the cipher text is deciphering or decryption. The many schemes used for enciphering constitute the area of study known as cryptography. Such a scheme is known as a cryptographic system or a cipher. Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis. The cryptanalysis are what the lay persons calls —breaking the code. The areas of cryptography and cryptanalysis together are called cryptology. Figure 1 - Simplified model of conventional encryption.

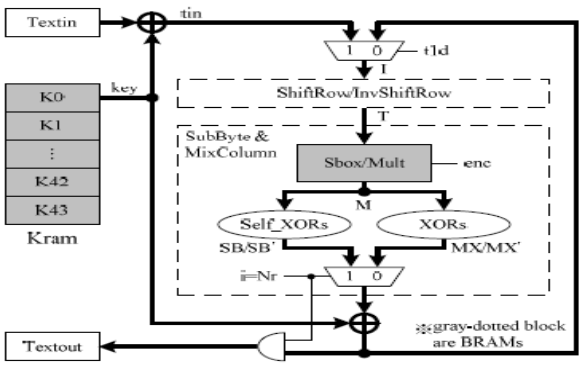


Fig1-AES Block Diagram

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

Encryption

The original intelligible message or data that is fed into the algorithm is the input. Encryption algorithm performs varies substitutions and transformations on the plain text. Secret key is also given as input to encryption algorithm. The key is a value independent of the plain text. The algorithm reproduces the different output depending on the specific key being used at the time. The exact substitutions and transformation performed by the algorithm depend on the key.The output depends on the plain text and the secret key. For a given message, two different keys will produce two different cipher texts. The cipher text is an apparently random stream of data, as it stands, is unintelligible.

Decryption

This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plain text.

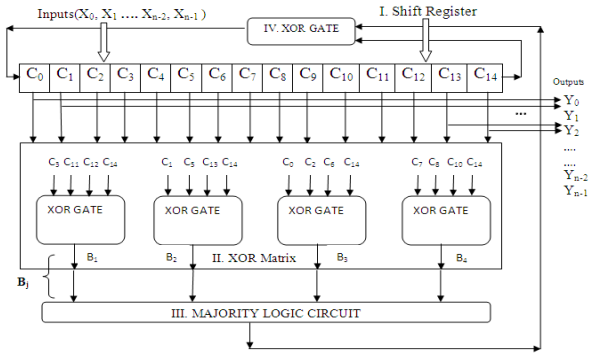


Fig2: AES Internal Diagram

II. PROBLEM STATEMENT

A. Data Encryption Standard (AES)

The AES block cipher algorithm was developed by researchers at IBM and was fine-tuned by government agencies, the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST). The American National Standards Institute (ANSI) adopted AES as the federal standard for encryption of commercial and sensitive data. This is defined in Federal Information Processing Standards (FIPS 46, 1977) published by NIST [1], [2].The AES algorithm has a regular structure that lends itself to pipelining and simple data manipulations to permit fast operations. AES is a symmetric encryption algorithm where the same key is used for both encryption and decryption. AES takes a 64- bit key and a 64-bit block of data as inputs, and outputs 64-bits of encrypted data. The actual key is only 56-bits and the remaining bits, i.e., the least significant bit (LSB) in every byte can be used as parity. The same basic AESing can be used for both encryption and decryption. The Data Encryption Standard (AES) shall consist of the following Advanced Encryption Algorithm (AES) and Triple Advanced Encryption Algorithm (TDEA, as AEScribed in ANSI X9.52). These devices shall be AESigned in such a way that they may be used in a computer system or network to provide cryptographic protection to binary coded data. The method of implementation will depend on the application and environment. The devices shall be implemented in such a way that they may be tested and validated as accurately performing the transformations specified in the following algorithms.

B. Advanced Encryption Algorithm

The algorithm is AESigned to encipher and decipher blocks of data consisting of 64 bits under control of a 64- bit key1. Deciphering must be accomplished by using the same key as for enciphering, but with the schedule of addressing the key bits altered so that the deciphering process is the reverse of the enciphering process. A block to be enciphered is subjected to an initial permutation *IP*, then to a complex key-dependent computation and finally to a permutation which is the inverse of the initial permutation *IP*-1. The key-dependent

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

computation can be simply defined in terms of a function *f*, called the cipher function, and a function *KS*, called the key schedule. A AEScription of the computation is given first, along with details as to how the algorithm is used for encipherment. Next, the use of the algorithm for decipherment is AEScribed. Finally, a definition of the cipher function *f* is given in terms of primitive functions that are called the selection functions Si and the permutation function *P*. The following notation is convenient: Given two blocks *L* and *R* of bits, *L R* denotes the block consisting of the bits of *L* followed by the bits of *R*. Since concatenation is associative, *B1B2...B8*, for example, denotes the block consisting of the bits of *B1* followed by the bits of *B2*... followed by the bits of *B8*.

C. Enciphering

The 64 bits of the input block to be enciphered are first subjected to the following permutation, called the initial permutation *IP*:

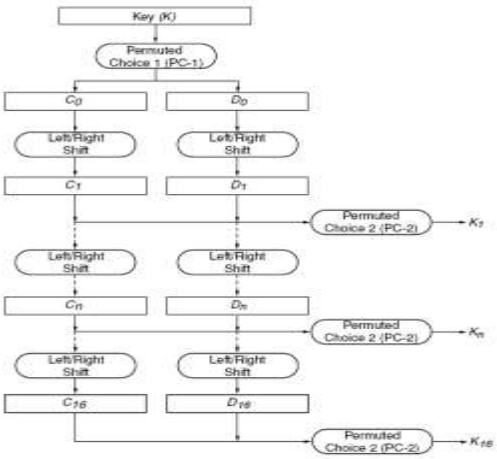


Fig3: Enciphering

III. REVERSIBLE LOGIC GATES

A reversible logic gate is an n-input n-output logic device with one-to-one mapping. This helps to determine the outputs from the inputs and also the inputs can be uniquely recovered from the outputs. Also in the synthesis of reversible circuits direct fan-Out is not allowed as one–to-many concept is not reversible. However fan-out in reversible circuits is achieved using additional gates. A reversible circuit should be designed using minimum number of reversible logic gates. From the point of view of reversible circuit design, there are many parameters for determining the complexity and performance of circuits.

The number of Reversible gates (N): The number of reversible gates used in circuit. The number of constant inputs (CI): This refers to the number of inputs that are to be maintained constant at either 0 or 1 in order to synthesize the given logical function. The number of garbage outputs (GO): This refers to the number of unused outputs present in a reversible logic circuit. One cannot avoid the garbage outputs as these are very essential to achieve reversibility. Quantum cost (QC): This refers to the cost of the circuit in terms of the cost of a primitive gate. It is calculated knowing the number of primitive reversible logic gates (1*1 or 2*2) required to realize the circuit.

Basic Reversible Logic Gates:

Feynman Gate

Feynman gate is a 2*2 one through reversible gate as shown in figure 1. The input vector is I(A, B) and the output vector is O(P, Q). The outputs are defined by P=A, Q=A ⊕ B. Quantum cost of a Feynman gate is 1. Feynman Gate (FG) can be used as a copying gate. Since a fan-out is not allowed in reversible logic, this gate is useful for duplication of the required outputs.

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

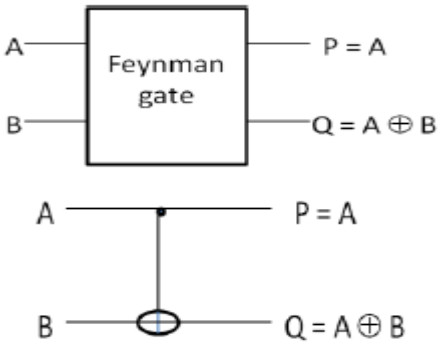


Fig 4:Feynman Gate

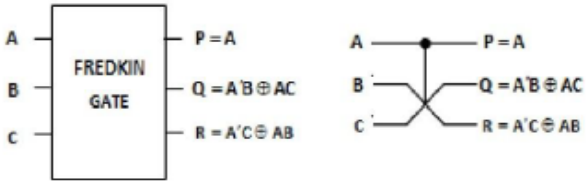
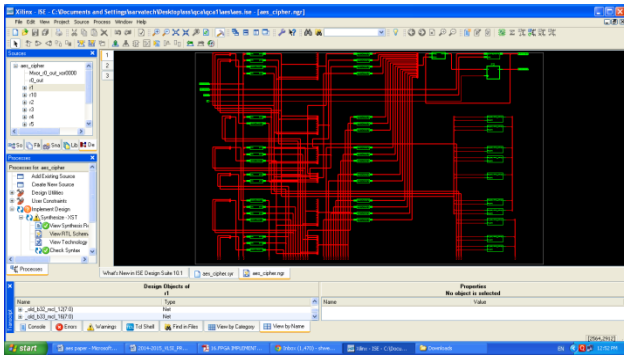
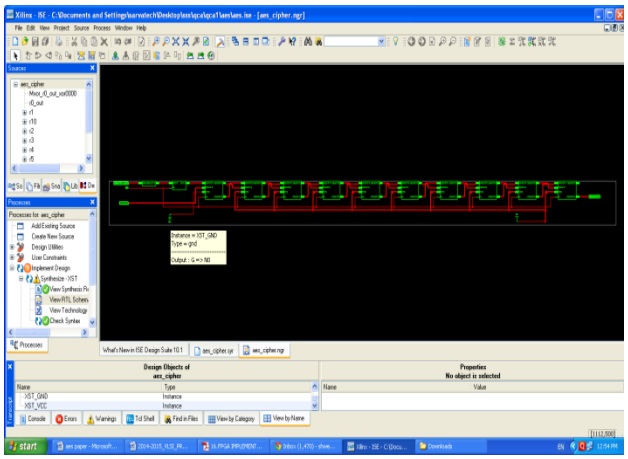


Fig 5:Fredkin Gate

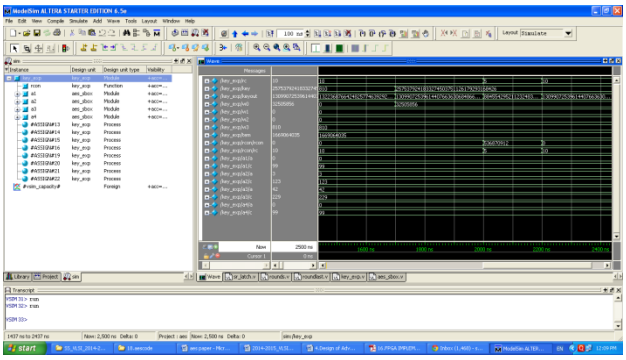
IV RESULTS

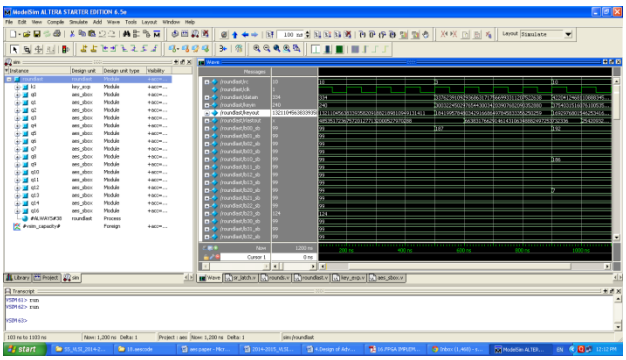
Synthesis Result from Xilinx tool:





Simulation Result from Modelsim tool:





References :

[1] J. Guajardo, S. Kumar, G. Schrijen, and P. Tuyls.—FPGA Intrinsic PUF and Their Use for IP Protection. Cryptographic Hardware and Embedded System, CHES 2007, pp.63–80, Oct 2007.

[2] P.Tuyls, G.-J. Schrijen, B.Skoric, J. van Geloven, Verhaegh, and R.Wolters.Coatings Cryptographic Hardware and Embedded Systems CHES2006, pages 369–383, Oct 2006.

[3] R. S. Pappu. —Physical one-way functions PhD thesis. Massachusetts Institute of Technology. Mar 2001.

[4] J. ZAMBRENO , D. NGUYEN AND A. CHOUDHARY , "Exploring area/delay trade-offs in AES FPGA implementation", Proc. Int. Colif, Field Programmable Logic and Its Applications (FPL), Lecture Notes in Computer Science, Vol. [2] R. Torrance, D. James, —The State-of-the-Art in IC ReverseEngineering, Cryptographic Hardware and Embedded Systems —CHES 2009, pp. 363–381,Oct 2009.

[5] R. Gennaro, A. Lysyanskaya, T. Malkin, S.Micali and T. Rabin, ―Algorithmic Tamper-Proof Security: Tampering,Theory of Cryptography Conference (TCC), pp. 258-277, Feb2004.

[6] J.W. Lee, D. Lim, B. Gassend, G. E. Suh, M.vanDijk, And S. Devadas.―A technique to build a secret key in integrated circuits with identification and Authentication application , Proceedings of the IEEE VLSI Circuits Symposium, June 2004.433203 (Springer-Verlag 2004), pp. 575-585.