A Novel Architecture of S-Box Design for AES Algorithm

Mounica Machunoori, MAIL ID: mounica432@gmail.com, Jagruti Institute of Engineering and Technology
Mr.R.Ramesh Babu, Email: ID:ram4dhani@gmail.com, Associate Professor

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 higherintegration densities there may be variations in parameters andnoise levels which will lead to larger error rates at various levelsof 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 addthe key and shuffle the data it is very hard for the unknownperson to find out the original data. Since for each key therewill 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 AESalgorithm involves the process of giving the data and key asinput to the encryption block and then implementing several blocks such as key schedule block, control block, roundfunction block, etc.In this project, we aim at designing ahigh speed and high performance but cost-effective FPGAbased processor which encrypts and /or decrypts the datathat has to be transferred from one PC to the other, basedon the Advanced Encryption Standard (AES) algorithm.

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

I. INTRODUCTION

A. 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 fromthe cipher text is deciphering or decryption. The manyschemes used for enciphering constitute the area of studyknown as cryptography. Such a scheme is known as acryptographic system or a cipher.Techniques used fordeciphering a message without any knowledge of theenciphering details fall into the area of cryptanalysis. Thecryptanalysis are what the lay persons calls ―breaking thecode. The areas of cryptography and

cryptanalysistogether are called cryptology.Figure 1 - Simplified model of conventional encryption.
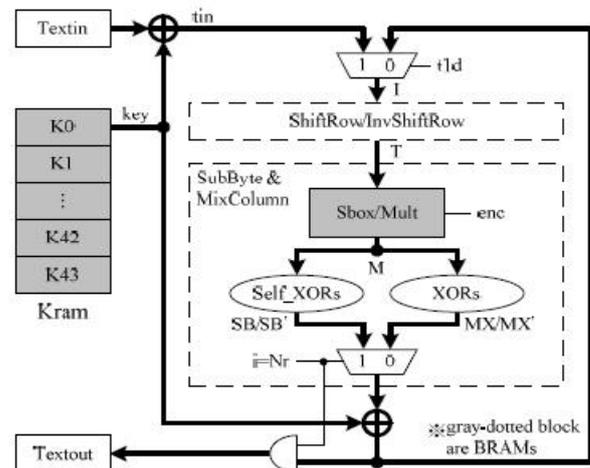
A. Encryption

The original intelligible message or data that is fed intothe 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. Thealgorithm reproduces the different output depending onthe specific key being used at the time. The exactsubstitutions and transformation performed by thealgorithm depend on the key.The output depends on theplain text and the secret key. For a given message, twodifferent keys will produce two different cipher texts. Thecipher text is an apparently random stream of data, as itstands, is unintelligible.

B. 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.
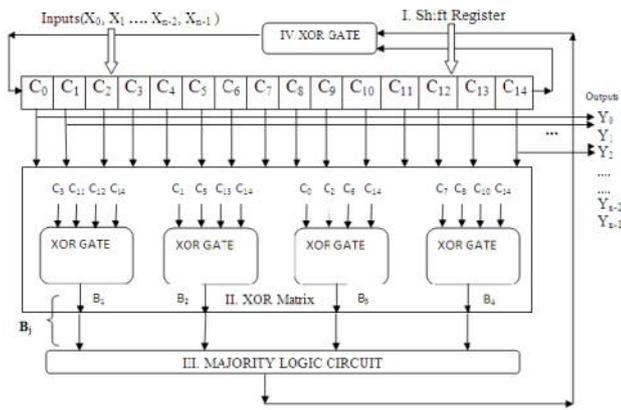
A. Data Encryption Standard (AES)

The AES block cipher algorithm was developed byresearchers at IBM and was fine-tuned by governmentagencies, the National Security Agency (NSA) and theNational Institute of Standards and Technology (NIST).The American National Standards Institute (ANSI)adopted AES as the federal standard for encryption ofcommercial and sensitive data. This is defined in Federal Information Processing Standards (FIPS 46, 1977)published by NIST [1], [2].The AES algorithm has aregular structure that lends itself to pipelining and simpledata manipulations to permit fast operations. AES is asymmetric encryption algorithm where the same key isused for both encryption and decryption. AES takes a 64-bit key and a 64-bit block of data as inputs, and outputs64-bits of encrypted data. The actual key is only 56-bitsand the remaining bits, i.e., the least significant bit (LSB)in every byte can be used as parity. The same basicAESing can be used for both encryption and decryption.The Data Encryption Standard (AES) shall consist of thefollowing Advanced Encryption Algorithm (AES) andTriple Advanced Encryption Algorithm (TDEA, asAEScribed in ANSI X9.52). These devices shall beAESigned in such a way that they may be used in acomputer system or network to provide cryptographicprotection to binary coded data. The method ofimplementation will depend on the application andenvironment. The devices shall be implemented in such a

way that they may be tested and validated as accuratelyperforming the transformations specified in the followingalgorithms.

B. Advanced Encryption Algorithm

The algorithm is AESigned to encipher and decipherblocks of data consisting of 64 bits under control of a 64-bit key1. Deciphering must be accomplished by using thesame key as for enciphering, but with the schedule ofaddressing the key bits altered so that the decipheringprocess is the reverse of the enciphering process. A blockto be enciphered is subjected to an initial permutation IP,then to a complex key-dependent computation and finallyto a permutation which is the inverse of the initialpermutation IP-1. The key-dependent computation can besimply defined in terms of a function f, called the cipherfunction, and a function KS, called the key schedule.AAEScription of the computation is given first, along withdetails as to how the algorithm is used for encipherment.Next, the use of the algorithm for
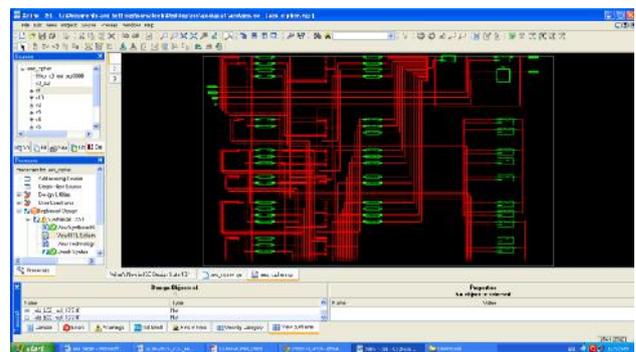
decipherment isAEScribed. Finally, a definition of the cipherfunction$f$isgiven in terms of primitive functions that are called theselection functions Si and the permutation function P. Thefollowing notation is convenient: Given two blocks $L$and$R$of bits, LRdenotes the block consisting of the bits of$L$followed by the bits of R. Since concatenation isassociative, $B1B2...B8$, for example, denotes the blockconsisting of the bits of $B1$followed by the bits of$B2$...followed by the bits of $B8$.
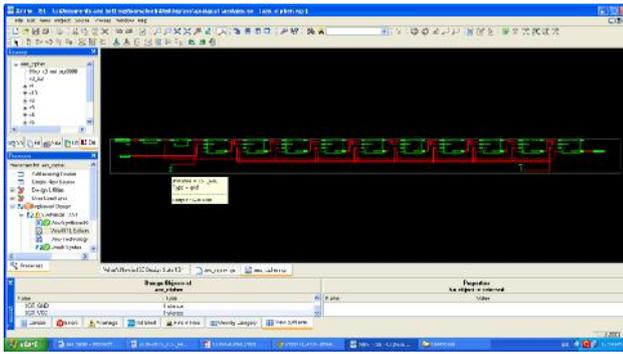
C. Enciphering

The 64 bits of the input block to be encipheredare first subjectedto the following permutation, called theinitial permutation IP:
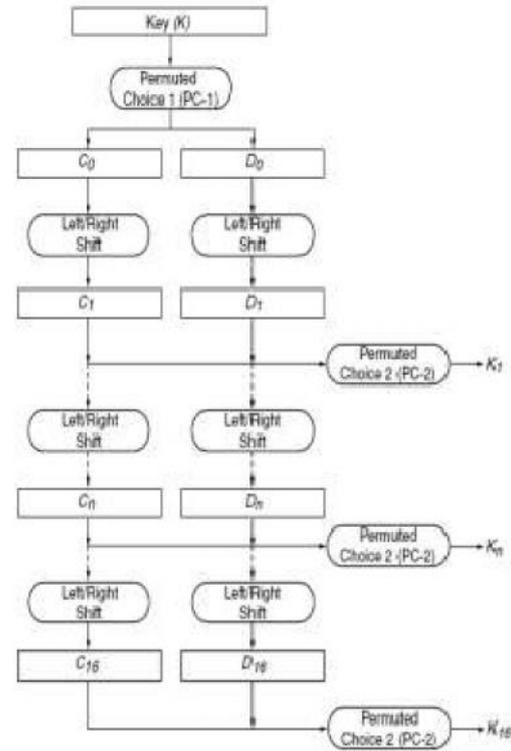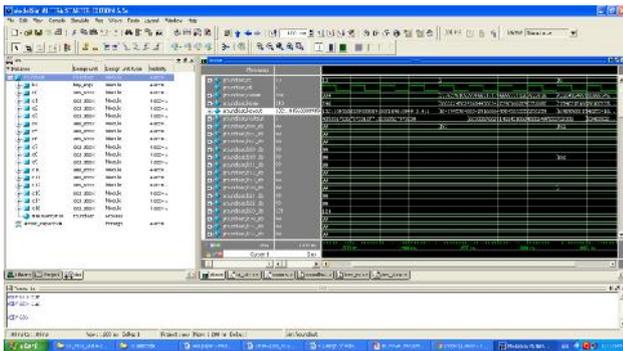

Synthesis Result from Xilinx tool:

Simulation Result from Modelsim tool:
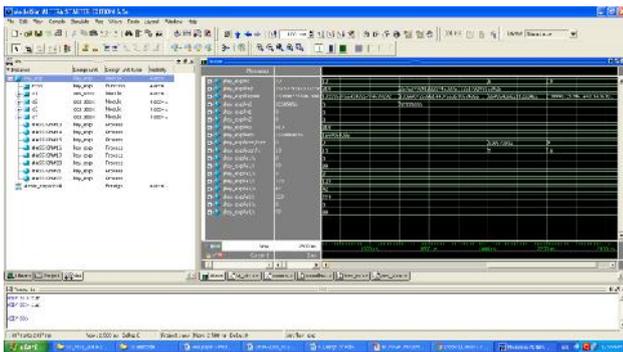
References :

[1]   J. Guajardo, S. Kumar, G. Schrijen, and P.Tuyls.—FPGA IntrinsicPUF and Their Use forIPProtection.Cryptographic Hardware andEmbeddedSystem, CHES 2007, pp.63–80, Oct 2007.

[2]   P.Tuyls, G.-J. Schrijen, B.Skoric, J. van Geloven,Verhaegh, and R.Wolters.CoatingsCryptographicHardware and Embedded SystemsCHES2006, 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 inAES 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.