Vol 05, Article 08400, September 2014 International Journal o
http://ijves.com ISSN: 2249 – 6556

A VHDL implementation in FPGA on Advance Encryption Standard (AES) by using Rijndael Algorithm

LAL BAHADUR,
M.TECH SCHOLAR, ECE, TIETECH, RGPV, BHOPAL (M.P), INDIA
klammds@gmail.com

ABSTRACT

Cryptography was and still is one of the hot research areas. The growing demand for cryptography arises from the desire to secure networks and data against potential intruders. This paper presents the VHDL implementation in FPGA on Advance Encryption Standard (AES) in Cryptography is the science of secret codes, enabling the confidentiality of communication through an insecure channel. It protects against unauthorized parties by preventing unauthorized alteration of use. Generally speaking, it uses a cryptographic system to transform a plaintext into a cipher text, using most of the time a key. To increase the computational speed parallelism and pipelining architecture have been implemented. The Advanced Encryption Standard can be programmed in software or built with pure hardware. However Field Programmable Gate Arrays (FPGAs) [1] offer a quicker, more customizable solution. The simulation is done using Xilinx 8.1 version.

Keywords *– AES, FPGA, encryption, decryption, Rijndael, block cipher.*

[1].INTRODUCTION

Cryptography provides a method for securing and authenticating the transmission of information over insecure channels. The expanding use of digital communications, sensitive electronic financial transactions taking place over the Internet, and digital signature applications has emphasized the need for fast and secure communication networks to fulfil the requirements for secrecy, integrity, and non-repudiability of exchanged information. The need for privacy has become a high priority for both governments and civilians desiring protection from signal and data interception. Widespread use of personal communications devices has only increased demand for a level of security on previously insecure communications. However, the applications of cryptography go far beyond simple confidentiality. Sensitive information sent over an open network may be scrambled into a form that cannot be understood by a hacker [3]. This is done using a mathematical formula, known as an encryption algorithm, which transforms the bits of the message into an unintelligible form. The intended recipient has a decryption algorithm for extracting the original message. Advanced Encryption standard (AES)/ Rijndael on the other hand is the new encryption standard. The RSA is the most popular form of public-key algorithm. Elliptic curve cryptosystems (ECCs) are cryptographic algorithms based on mathematical objects known as elliptic curves. Elliptic curve cryptography has been gaining in popularity recently.

[2]. DEFINITIONS

[2.1] Cryptography-Cryptography [6] is the art and science of achieving security by encoding message to make them non-readable.

[2.2] Cryptanalysis- Cryptanalysis [6] is the technique of decoding message from a non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format. It is like a breaking a code.

Cryptology is a combination of cryptography and cryptanalysis. Cryptosystems can provide confidentiality, authenticity, integrity, and non-repudiation services. It does not provide availability of data or systems Confidentiality means that unauthorized parties cannot access information [3].

Authenticity refers to validating the source of the message to ensure the sender is properly identified. Integrity provides assurance that the message was not modified during transmission, accidentally or intentionally. Non repudiation means that a sender cannot deny sending the message at a later date, and the receiver cannot deny receiving it.

When a plain text message is codified using any suitable scheme, the resulting message is called as cipher text. Cipher [2] is any method of encrypting text. It is also sometimes used to refer to the encrypted text message itself. A block cipher is one that breaks a message up into chunks and combines a key with each chunk (for example, 64-bits of text). A stream cipher is one that applies a key to each bit, one at a time. Most modern ciphers are block ciphers.

[3]. ENCRYPTION CLASSES

There are two classes of algorithm in encryption, an asymmetric key and symmetric key.

[3.1].ASYMMETRIC KEY Cryptographic technique were a key pair is used for encryption and decryption operations. RSA is widely used for asymmetric key algorithm for decades and ECC as an alternative to RSA which offers highest security with small bit length of key [6].

Vol 05, Article 08400, September 2014 International Journal o
http://ijves.com ISSN: 2249 – 6556

[3.2]. SYMMETRIC KEY

Cryptographic technique where the same key is used for encryption and decryption operation [6].

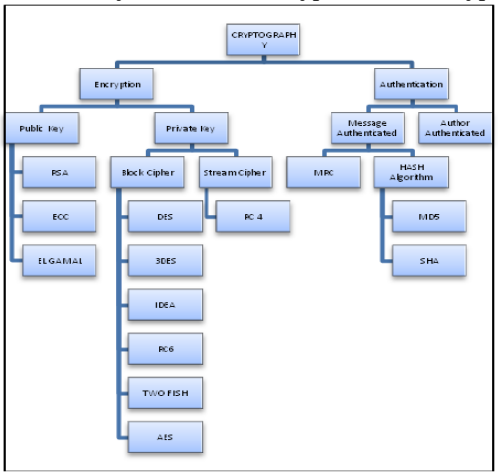

Fig [2.1]. Basic Block Diagram of Cryptography

[4]. AES ALGORITHM

In AES input to the encryption and decryption algorithms is a single 128-bit block. This block of input is depicted as a square matrix of bytes. This block is copied into the state array, which is modified at each stage of encryption or decryption. After the final stage, state is copied to an output matrix. These operations are depicted in Fig.2. Similarly, the 128-bit key is depicted as a square matrix of bytes. This key is then expanded into an array of key schedule words; each word is four bytes and total key schedule is 44 words for the 128-bit key. The ordering of bytes within a matrix is by column. It was basically designed to have the following characteristics:

I. Resistance against all known attacks.

II. Speed and code compactness on a wide range of platforms.

III. Design Simplicity.

[4.1].AES algorithm Process

The encryption and decryption process consist of a number of different transformation applied consecutively over the data block bits, in affixed number of iteration, called rounds. The number of rounds depends on the length of the key used for the encryption process. For key length of 128 bits, the number of iteration required are 10 that is Nr= 10.Each of the first Nr-1 rounds consists of 4 transformations: SubBytes(), ShiftRows(), MixColumns() &AddRoundKey(). The four different transformations are given in detail below.

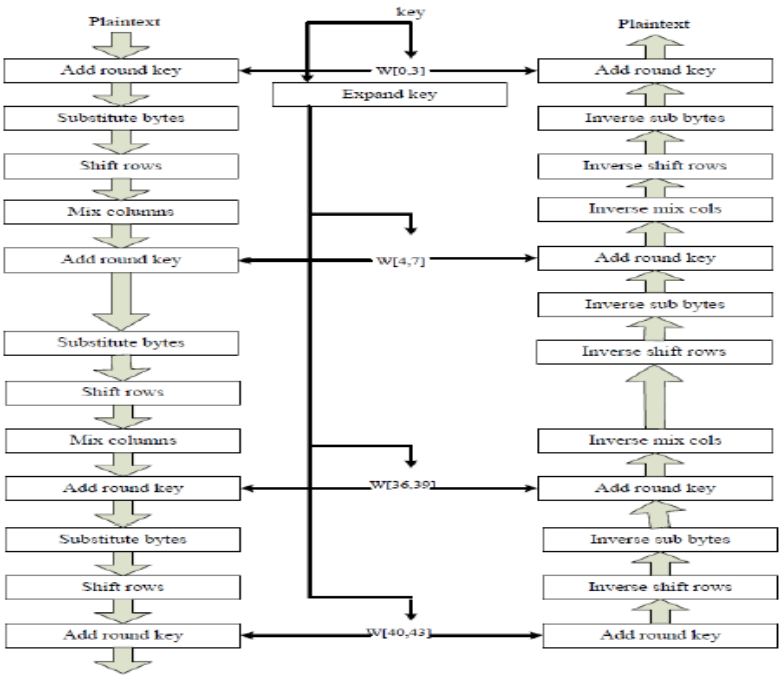

Fig [4.1].AES Encryption and Decryption

Vol 05, Article 08400, September 2014 International Journal o
http://ijves.com ISSN: 2249 – 6556

[4.1.1]. Sub Bytes Transformation

It is a non-linear replacement of bytes that operates autonomously on each byte of the State employing a substitution table (S box). This S-box which is invertible is constructed by first taking the multiplicative inverse in the finite field GF (28) with irreducible polynomial m(x) = x8 + x4+ x3 + x + 1. The element {00} is mapped to itself. Then affine transformation is applied (over GF (2)).

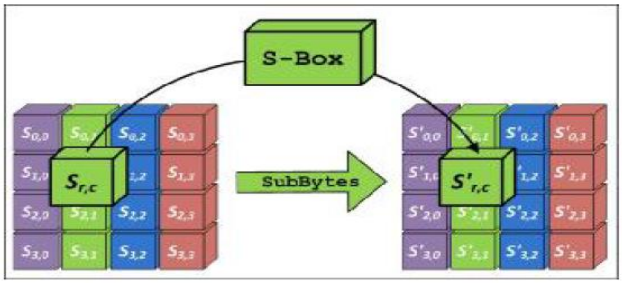

Fig [4.1.1]. Sub Byte Block

[4.1.2].Shift Rows Transformation

Cyclically move the rows of the State over unlike offsets. The operation is equally the similar in the decryption process except at the point that the shifting offsets have dissimilar values.

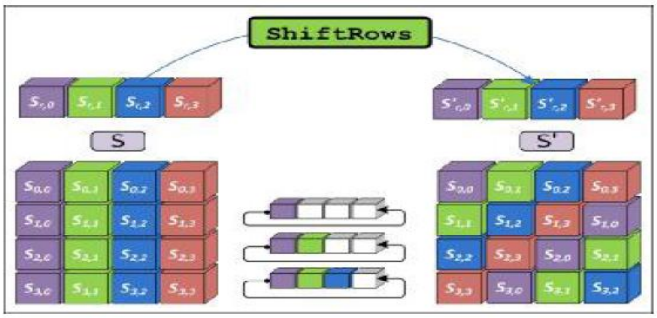

Fig [4.1.2]. Shift Rows Block

[4.1.3].Mix Columns Transformation

This transformation operates on the State column-by-column, considering each column as a four-term polynomial. The columns are taken as polynomials over GF (28) and multiplied by modulo x4 + 1 with a fixed polynomial a(x) = {03} x3+ {01} x2+ {02} x.

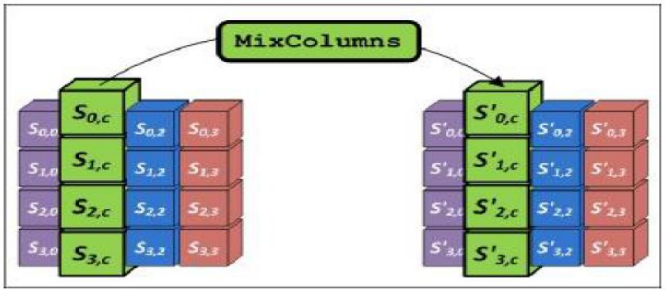

Fig [4.1.3]. Mix columns Block

[4.1.4].Add Round Key Transformation

In this transformation is having Round Key which is added to the State by a simply XORing operation. Every Round Key contain of Nb words from the key expansion. Those Nb words are added into the columns of the State. Key Addition is the same for the decryption process.

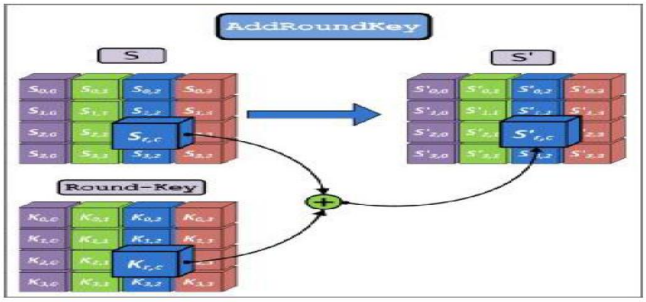

Fig [4.1.4]. Add Round key Block

Vol 05, Article 08400, September 2014 International Journal o
http://ijves.com ISSN: 2249 – 6556

[4.1.5].Key Expansion

Each round key is a 4-word (128-bit) array induced as a product of the previous round key, a constant that changes each round, and a series of S-Box lookups for each 32-bit word of the key. The Key schedule Expansion results in a total of Nb (Nr + 1) words. The decryption process is exact inverse of the encryption process. All the transformations implied in encryption process are opposite to encryption process. That means the last round values of both the data and key are first round inputs for the decryption process and follows in decreasing order.

[5]. FPGA IMPLEMENTATION OF ALGORITHMS

In this section we will discuss about implementation [5] of Advanced Encryption Standard / Rijndael [1] and Elliptic Curve Cryptographic Algorithm on FPGAs. The performance of cryptographic implementation on FPGA is evaluated on the basis of throughput and the amount of hardware resources consumed to achieve this throughput.

[5.1].Advanced Encryption Standard / Rijndael on FPGA

Many implementations of Rijndael[1] the AES, have been presented using both Xilinx and Altera FPGAs. The implementation in achieves a throughput of 6.956 Gbits/sec using a Xilinx. Implementing the Rijndael Byte-Sub operation using ROM resulted in a significant increase in throughput. Rijndael implementations achieved throughputs ranging from 570 Mbits/sec to 964 Mbits/sec depending on theimplementation methodology using Xilinx. The implementation described in achieves a throughput rate of 17.8 Gbits/s for a 128-bit key through pipelining. The work presented in presents a very compact implementation of AES on FPGA. It proposed a new way of implementing the MixColumns and Inv-MixColumns transformations which reduces area. It achieves data streams of 150 Mbits/sec for encryption anddecryption on a low cost Xilinx.

[5.2]. Elliptic Curve Cryptography on FPGA

In a new elliptic curve crypto processor (ECCP) [1] architecture has been proposed for the computation of point multiplication for curves defined over Galois Field (GF).The ECP has a scalable architecture in terms of area and speed specially suited for FPGAs. This processor uses a high-radix Montgomery multiplier that relies on the pre-computation of frequently used values and on the use of multiple processing engines. The ECCP consists of main controller, arithmetic unit controller and the arithmetic unit. The authors developed a prototype that implemented ECCP on a Xilinx FPGA. The ECCP prototype used 11,416 LUTs, 5,735 Flip- Flops, and 35 Block RAMS. The frequency of operation of the prototype was 40 MHz for 192 bit operands and 37.3 MHz for the 521-bit multiplier.

[6]. Conclusions

Optimisation of VHDL code is developed for the implementation of both encryption and decryption process. Each program is tested with some of the sample vectors provided by NIST and output results are perfect with minimal delay. The time varies from chip to chip and the calculated delay time can only be regarded as approximate. Adding data pipelines and some parallel combinational logic in the key scheduler and round calculator can further optimize this design.

[7].REFERENCE

[1] Daemon, J., and Rijmen, V. ―The Design of Rijndael: The Wide Trail Strategy Explained.‖ New York, Springer – Verlag, 2000.
[2] T. Yamaguchi, T. Hashiyama, and Shigeru Okuma, "A Study on Reconfigurable Computing System for Cryptography," in Proceedings of IEEE International Conference on Systems, Man and Cybernetics, vol. 4, pp. 2965-2968, October 2000.
[3] V. K. Prasanna, and A. Dandalis, "FPGA-based Cryptography for Internet Security," Online Symposium for Electronic Engineers, November 2000.
[4] Virtex 2.5 V Field Programmable Gate Arrays, San Jose, CA: Xilinx Inc., 1998
[5] Muhammad H. Rais and Syed M. Qasim "Efficient Hardware Realization of Advanced Encryption Standard Algorithm using FPGA", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.9, September 2009.
[6] Atulkahate– 2nd edition TMH of cryptography and network security page-38, 39 and important abbreviation.