International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 6 (July 2014) http://ijirae.com

Design of advanced encryption standard using Vedic Mathematics

Soumya Sadanandan
Dept. of ECE, MG University, Kerala
Mangalam College of Engineering

Anjali.V
Dept. of ECE, MG University, Kerala
Mangalam College of Engineering

Abstract— This work describes about the designing of Advanced Encryption System suitable for areas requiring maximal area minimization such as that for mobile phones. As the demand for secure transactions in banking and such related areas is increasing, encryption and decryption using cryptography plays a very important role. Nowadays, as majority of secure transactions occurs on smart phones and other handheld devices, an algorithm that consumes less area and that without compromising with overall performance becomes a necessity. In order to meet this requirement, several algorithms have been designed and implemented in the past, but each of these algorithms possess their own shortcomings with respect to an ASIC or an FPGA implementation. The design is done using Verilog hardware description language which provides an immediate hardware implementation possibility. The hardware implementation of the system is faster when compared to the conventional designs. We utilize the techniques involved in Vedic mathematics to realize the same. Comparisons are carried out with the conventional designs to state the advantages of the proposed design.

Keywords— AES, Urdhwa Tiryakbhyam Sutra, Galois field multiplication.

I . INTRODUCTION

The encryption of data that is to be transmitted is always of major concern in wireless communication systems. cryptographic algorithms have been proposed to encrypt and decrypt data to ensure security. It is useful to transmit and store data through insecure networks in 2001,national institute of standard and technology (nist) replaced previous encryption standards like des and triple des with advanced encryption standard because of its efficiency, implementation and flexibility. The advanced encryption standard is a subset of much larger encryption algorithm known as rijndael. The cryptographic algorithms involves encrypting the data to be transmitted or shared by means of unique keys, for encryption and decryption, which are known only to the authorized parties, thereby ensuring data security. This serves as a great boon to common man as well as for military applications. Several cryptographic algorithms have been discovered and researched upon in the recent times ,giving importance to the problem of vulnerability of the algorithms especially in applications which demand high security i.e. for smart cards, ATMs,WWW servers etc. Among these,the Advanced Encryption Standard (AES) algorithm is one of the highly preferred algorithms as it has higher immunity towards attacks.

However, when considering the hardware implementation of the design, the AES is losing, since it involves several complex operations implemented in the Galois Field .Also, these complex operations are iterative in nature which in turn disturbs the speed of the encryption system and therefore increases the vulnerability. In this paper, an area efficient architecture for performing the various operations involved in the Advanced Encryption Standard(AES) method of cryptography is introduced. Here we make use of techniques used in ancient Vedic mathematics. Vedic mathematics is an archaic style of mathematics which subsisted in India in 1500 B.C,and was later on brought to limelight by a famous scholar Sri Bharathi Krishna Tirthaji between 1911 and 1918.He systemized it into 16 simple sutras, which are used by most of the researchers and mathematicians due to its ease of use.Out of the 16 formulae available in Vedic Mathematics, the Urdhwa Tiryakbhyam Sutra was utilized in order to address the flaws observed in the conventional mix columns architecture utilized in AES.

II . OVERVIEW OF AES ALGORITHM

AES is a symmetric encryption block cipher which encrypts and decrypts 128 bits of electronic data in several rounds. It was originally called Rijndael algorithm which was developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. It was later adopted by National Institute of Standards and Technology(NIST), USA in November 2001. The key size required to encrypt the data is the sender's choice i.e. the key size can either be 128 bits or 192 bits or 256 bits keeping the data/plain-text fixed i.e. 128 bits. A copy of the 128 bit plain text is stored in a 4*4 matrix called the state array, with each location supporting 1byte of the plain text. Example: if the plain text is a1 a2 a3 a4 a5 a6 a7 a8 a9 a10 a11 a12 a13 a14 a15 a16, it is arranged in a matrix format as shown in Fig. 1.

a_1	a_5	a_9	a_{13}
a_2	a_6	a_{10}	a_{14}
a_3	a_7	a_{11}	a_{15}
a_4	a_8	a_{12}	a_{16}

Fig. 1. Arrangement of 128 bit plain text in a state array in a 4*4 fashion

Based on the key size, 10, 12, or 14 rounds of transformations are performed on the state matrix for key sizes of 128, 192 or 256 bits respectively, in order to encrypt it.These transformations, for a single round, include several steps such as addition of round key, Sub-byte transformation, Shift Rows and Mix Columns. Decrypting the cipher involves inverse transformations on the cipher but in the reverse order. The inverse transformations comprise of addition of round key, inverse sub-byte transformation, inverse shift rows and inverse mix columns which once again constitute a single round. The mix column operation is skipped in the last round i.e. 10th round during encryption as well as decryption. The various steps involved , depicted in Fig. 2.

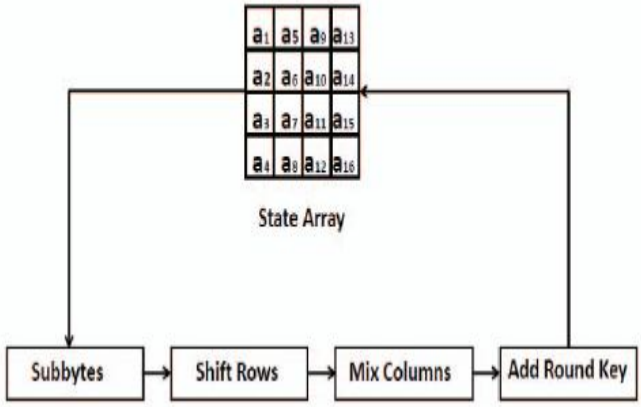


Fig. 2. Single round of AES encryption. Decryption is performed in the reverse order.

A. *Add Round Key*

The Add round key step involves logically XORing a round key with the state array which is in turn generated using a main key. This is performed using a unique key expansion algorithm.

B. *Subbyte transformation & inverse subbyte transformation*

The data obtained after the add-round key operation is further transmogrified by means of a Subbyte transformation.Traditionally, Subbyte transformation and Inverse Subbyte transformation is accomplished by computing the Multiplicative Inverse of the input byte procured from the previous stage, followed by an affine transformation. In order to reduce complexity, these steps are usually performed by simply looking up an “S-box” table which contain pre-computed values for the multiplicative inverse and the transformation.

C. *Shift rows and inverse shift rows*

The Shift Rows and Inverse Shift Rows Stage mainly focus on cyclically shifting all the elements of a particular row of the matrix obtained after Subbyte transformation and Inverse Subbyte transformation respectively, keeping the elements of the 1st row of the state matrix unoperated.

D. *Mix columns and inverse mix columns*

Mix columns (MC) and inverse mix columns (IMC) are implemented by performing matrix multiplication over Galois field i.e. GF(28) using the irreducible polynomial x^8 + x^4 + x^3+ x+ 1. The constant matrices used for mix columns and inverse mixcolumns are unique and are defined by the FIPS.

E. Mix column using vedic mathematics

One of the crucial mathematical operation performed during the mix column step in AES,is the Galois field multiplication.Multiplication,being a tedious and a power hungry operation,causes the computation of mix columns and its inverse to be an even more difficult task.This is due to the fact that,it involves matrix multiplication.Therefore,there arises a necessity to ease the entire process of mix columns.In order to achieve the same,the Urdhwa Tiryakbhyam Sutra of Vedic Mathematics,is utilized in our proposed architecture for mix columns and its inverse due to its excellence in terms of speed and area.

III. MULTIPLER ARCHITECTURE

The Multiplier Architecture is based on the Vertical and Crosswise algorithm of ancient Indian Vedic Mathematics. In the overlay architecture, grouping of 4 bits at a time is done for both multiplier and multiplicand and thereafter vertical and crosswise algorithm is applied to decompose the whole of the multiplication operation into 4x4 multiply modules. The algorithm is explained in Table-1 for 16x16 bit number. After getting the sub-product bits in parallel from the 4x4 multiply modules, we can employ an efficient method of addition to generate the final 32 bit product. This method can be generalized for NXN bit multiplication where N is a multiple of 4 such as 8,12,16,20,24,....4n. Thus instead of implementing the entire multiplication through a single NXN bit multiplier, we can get the same product efficiently by using the proposed overlay architecture. The advantage of this is that the multiply operation of large number of bits can now be performed by using smaller and efficient 4x4 multiplier.

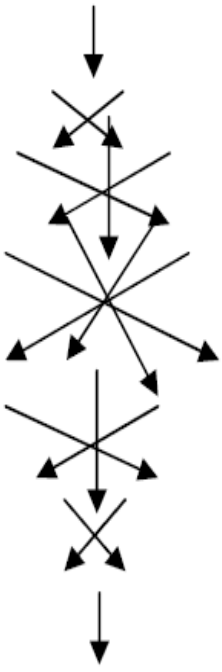
TABLE 1- 8 x 8 bit Vedic multiplier Using Urdhva Tiryakbhyam.
CP- Cross Product (Vertically and Crosswise)

A= A7 A6 A5 A4 | A3 A2 A1 A0
X1 | X0
B= B7 B6 B5 B4 | B3 B2 B1 B0
Y1 | Y0

X1 X0 Multiplicand [8 bits]
Y1 Y0 Multiplier [8 bits]

F E D C
P3 P2 P1 P0 Product [16 bits]

Where X1, X0,Y1 and Y0 are each of 4 bits.



Note: Each Multiplication operation is an embedded parallel 4x4 multiply module

IV. SIMULATION RESULTS

The algorithm for the Advanced Encryption Standard using Vedic Mathematics technique was designed and simulated in Verilog HDL using Xilinx ISE.The design of the conventional implementation of the AES was also carried out in order to compare with the proposed design.The designing was carried out so as to be implemented and synthesized for a Spartan 3e series XC3s1600e Xilinx FPGA.The table below shows the results of the simulation proposed design,after comparison with the conventional counterpart.

Algorithm	Area occupancy(%)	No.of gates	Timing(ns)
Conventional AES	7.35	1210	11.816
Proposed AES using Vedic Technique	5.11	731	12.33

We can find that the proposed design provides savings in overall area required for implementation when compared with the conventional design,with only a small increase in the timing requirement.

V. CONCLUSION

In this paper,an area efficient design of 128 bit advanced encryption standard that is suitable for carrying out cryptographic applications is done.The architecture of design performs well when compared with the conventional designs.The design provided good savings in the overall area with only neglectable increment in the timing requirement that proves its applicability in mobile devices.The optimizations can be extended towards the design of Sub byte operation in the future.

VI. ACKNOWLEDGEMENT

My sincere thanks to Peiyi Zhao,Member IEEE.

VII. REFERENCE

[1] Huang, Xu, Shirantha Wijesekera, and Dharmendra Sharma. "Quantum cryptography for wireless network communications." Wireless Pervasive Computing, 2009. ISWPC 2009. 4th International Symposium on. IEEE,2009.
[2] Himanshu Thapliyal and M.B Srinivas,VLSI Implementation of RSA Encryption System Using Ancient Indian Vedic Mathematics,Center for VLSI and Embedded System Technologies,International Institute of Information Technology
[3] H Thapliyal,and H R Arabnia,A time area-power efficient multiplier and square architecture based on Ancient Indian Vedic Mathematics, Proceedings of the 2004 International Conference on VLSI,June 2004,pp. 434-9.
[4] M C Hanumantharaju,H Jayalaxmi,R K Renuka,and M Ravishankar,A high speed block convolution using Anciet Indian Vedic Mathematics,International Conference on Computational Intelligence and Multimedia.

