VERILOG HDL BASED DESIGN AND VERIFICATION OF AREA OPTIMIZED AES BASED ON FPGA

[1] Dr. Mr. ARVIND KUNDU, [2]Mr. M.KARTHIK , [3] Mr.M.SURESH KUMAR
[1]Associate Professor, [2]PG Student, [3]Assistant Professor
[1]Department of ECE
[1]SCIENT INSTITUTE OF TECHNOLOGY, HYDERABAD

ABSTRACT: In this paper, design and verification of area optimized aes based on fpga using verilog hdl is proposed. Advanced Encryption Standard (AES), has received significant interest over the past decade due to its performance and security level. In most of the previous works subbytes and inverse subbytes are implemented in Separate Modules using lookup table method. In this paper we used combinational logic which helps for making inner round pipelining in an efficient manner. Furthermore, composite field arithmetic helped in obtaining lesser area. Using proposed architecture, a fully sub pipelined encryptor/ decryptor with 3 substage pipelining in each round can achieve a throughput of 25.89Gbps on Xilinx xc5vlx110t-1 device which is faster. This AES design was implemented using Verilog HDL and synthesized with Xilinx ISE using Spartran3 Xilinx Family , Simulation and Verification was done using Mentor-Graphics ModelSim-6.5e and achieved the maximum through put.

Keywords: AES,Encrytion,Decryption,Pipelining,Key expansion.

I. INTRODUCTION

AES is short for Advanced Encryption Standard and is a United States encryption standard defined in Federal Information Processing Standard (FIPS) 192, published in November 2001. It was ratified as a federal standard in May 2002. AES is the most recent of the four current algorithms approved for federal us in the United States. One should not compare AES with RSA, another standard algorithm, as RSA is a different category of algorithm. Bulk encryption of information itself is seldom performed with RSA.RSA is used to transfer other encryption keys for use by AES for example, and for digital signatures. AES is a symmetric encryption algorithm processing data in block of 128 bits. A bit can take the values zero and one, in effect a binary digit with two possible values as opposed to decimal digits, which can take one of 10 values. Under the influence of a key, a 128-bit block is encrypted by transforming it in a unique way into a new block of the same size. AES is symmetric since the same key is used for encryption and the reverse transformation, decryption. The only secret necessary to keep for security is the key. AES may configured to use different key-lengths, the standard defines 3 lengths and the resulting algorithms are named AES-128, AES-192 and AES-256 respectively to indicate the length in bits of the key. Each additional bit in the key effectively doubles the strength of the algorithm, when defined as the time necessary for an attacker to stage a brute force attack, i.e. an exhaustive search of all possible key combinations in order to find the right one .

1.2 Some background on AES:

In 1997 the US National Institute of Standards and Technology put out a call for candidates for a replacement for the ageing Data Encryption Standard, DES. 15 candidates were accepted for further consideration, and after a fully public process and three open international conferences, the number of candidates was reduced to five. In February 2001, the final candidate was announced and comments were solicited. 21 organizations and individuals submitted comments. None had any reservations about the suggested algorithm. AES is founded on solid and well-published mathematical ground, and appears to resist all known attacks well. There's a strong indication that in fact no back-door or known weakness exists since it has been published for a long time, has been the subject of intense scrutiny by researchers all over the world, and such enormous amounts of economic value and information is already successfully protected by AES. There are no unknown factors in its design, and it was developed by Belgian researchers in Belgium therefore voiding the conspiracy theories sometimes voiced concerning an encryption standard developed by a United States government agency. A strong encryption algorithm need only meet only single main criteria:

- There must be no way to find the unencrypted clear text if the key is unknown, except brute force, i.e. to try all possible keys until the right one is found.

A secondary criterion must also be met:

- The number of possible keys must be so large that it is computationally infeasible to actually stage a successful brute force attack in short enough a time.

The older standard, DES or Data Encryption Standard, meets the first criterion, but no longer the secondary one – computer speeds have caught up with it, or soon will. AES meets both criteria in all of its variants: AES-128, AES-192 and AES-256.

II. ADVANCED ENCRYPTION STANDARD :

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. It has been adopted by the U.S. government and is now used worldwide. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

In the United States, AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001 after a five-year standardization process in which fifteen competing designs were presented and evaluated before it was selected as the most suitable (see Advanced Encryption Standard process for more details). It became effective as a Federal government standard on May 26, 2002 after approval by the Secretary of Commerce. It is available in many different encryption packages. AES is the first publicly accessible and open cipher approved by the National Security Agency (NSA) for top secret information (see Security of AES, below).

Originally called **Rijndael**, the cipher was developed bytwo Belgian cryptographers, Joan Daemen and Vincent Rijmen, and submitted by them to the AES selection processtwo Belgian cryptographers, Joan Daemen and Vincent Rijmen, and submitted by them to the AES selection process. The name *Rijndael* (Dutch pronunciation: ['rɛindaːl][5]) is a play on the names of the two inventors.

Strictly speaking, AES is the name of the standard, and the algorithm described is a (restricted) variant of Rijndael. However, in practice the algorithm is also referred to as "AES" (a case of totum pro parte).

III.AREA-OPTIMIZED AES-128

3.1 Brief Description of Rijndael Algorithm:

Rijndael algorithm consists of encryption, decryption and key schedule algorithm. The main operations of the encryption algorithm among the three parts of Rijndael algorithm include: bytes substitution (SubBytes), the row shift (ShiftRows), column mixing (MixColumns), and the round key adding (AddRoundKey). It is shown as Fig. 1

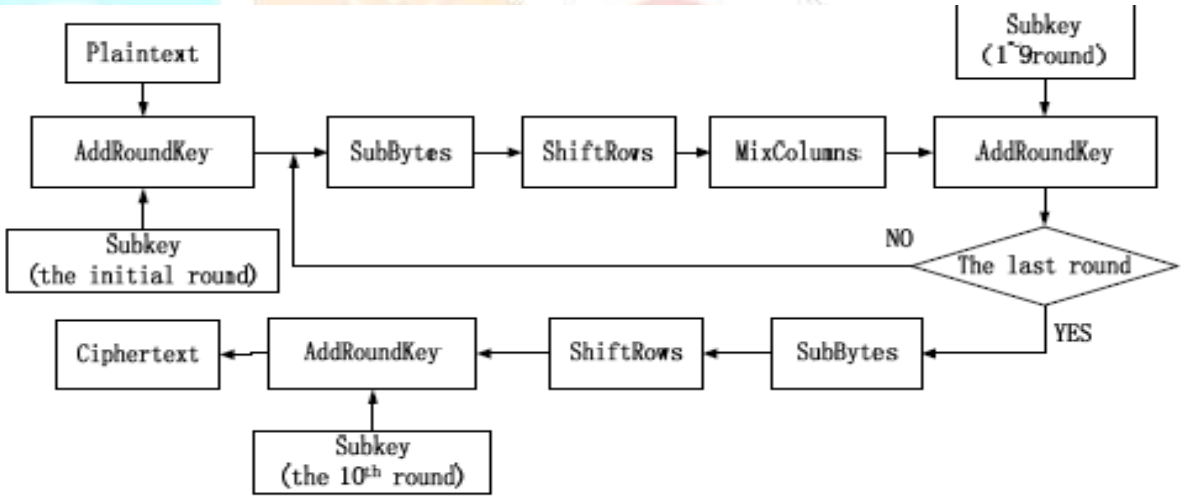


Figure1. The structure of Rijndael encryption algorithm

Encryption algorithm processes Nr+1 rounds of transformation of the plaintext for the ciphertext. The value of Nr in AES algorithm whose packet length is 128 bits should be 10, 12, or 14 respectively, corresponding to the key length of 128,192,256 bits. In this paper, only the (AES-128) encryption scheme with 128-bit keys is considered.

3.2 The Design of Improved AES-128 Encryption Algorithm:

1) Two main processes of AES encryption algorithm:

The AES encryption algorithm can be divided into two parts, the key schedule and round transformation. Key schedule consists of two modules: key expansion and round key selection. Key expansion means mapping Nk bits initial key to the so-called expanded key, while the round key selection selectes Nb bits of round key from the expanded key module.

Round Transformation involves four modules by ByteSubstitution, ByteRotation, MixColumn and AddRoundKey.

2) Key points for the design:

In the AES-128, the data in the main process mentioned above is mapped to a 4×4 two-dimensional matrix. The matrix is also called state matrix, which is shown as Fig.2.

a_{00}	a_{01}	a_{02}	a_{03}
a_{10}	a_{11}	a_{12}	a_{13}
a_{20}	a_{21}	a_{22}	a_{23}
a_{30}	a_{31}	a_{32}	a_{33}

Figure 2. The state matrix

In the four transformation modules of round transformation, the ByteRotation, MixColumn and AddRoundKey are all linear transformations except the ByteSub.

A. Take analysis of the AES algorithm principle and we can find:

ByteSubstitution operation simply replaces the element of 128-bit input plaintext with the inverse element corresponding to the Galois field GF (28), whose smallest unit of operation is 8 bits/ group.

ByteRotation operation takes cyclic shift of the 128-bit state matrix, in which one row (32 bits) is taken as the smallest operand.

MixColumns operation takes multiplication and addition operations of the results of ByteRotation with the corresponding irreducible polynomial x8 + x4 + x3 + x + 1 in GF(28), whose minimum operating unit is 32 bits.

Addroundkey operation takes a simple XOR operation with 8-bit units.

The inputs of plaintext and initial key, intermediate inputs and outputs of round transformation, as well as the output of ciphertext in the AES algorithm are all stored in the state matrixes, which are processed in one byte or one word. Thus, in order to take operations at least bits, the original 128-bit data should be segmented. We design some external controllers in the new algorithm, so that the data transmission and processing can be implemented on each column of the state matrix (32bit).

B. That means the data should be packed and put into further operations.

Take the independent and reversible bytes substitution operation of S-box as example. Firstly, the state matrix is divided into four columns. And then byte replacement is achieved by the operation of look-up table shown as Fig. 3.

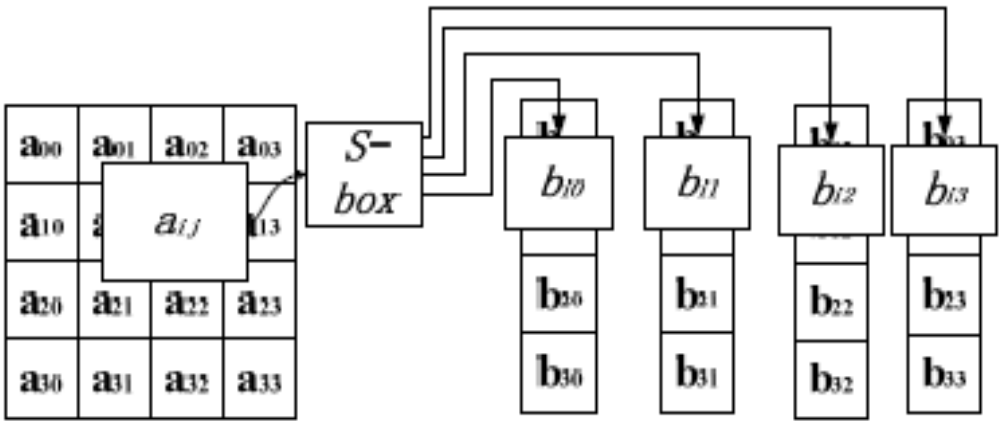


Figure 3. Bytes segmentation and replacement processing

Therefore, the original 128-bit input of plaintext and key will be replaced with four consecutive 32-bit input sequences respectively. In order to decrease the output ports, four continuous 32-bit ciphertext sequences have taken place of the original 128-bit output by adding a clock controller. The 128- bit data in the round transformation is also split into four groups of 32-bit data before the operation of pipelining.

C. The Process of New algorithms

From the above analysis, we can find that the process of AES encryption can be mainly divided into two parts: key schedule and round transformation. The improved structure is also divided into these two major processes. The initial key will be sent to the two modules: Keyexpansion and Keyselection, while the plaintext is to be sent to the round transformation after the roundkey is selected. But the operand of data transmission is turned into a 32-bit unit. The process of new algorithm is shown as Fig. 4.

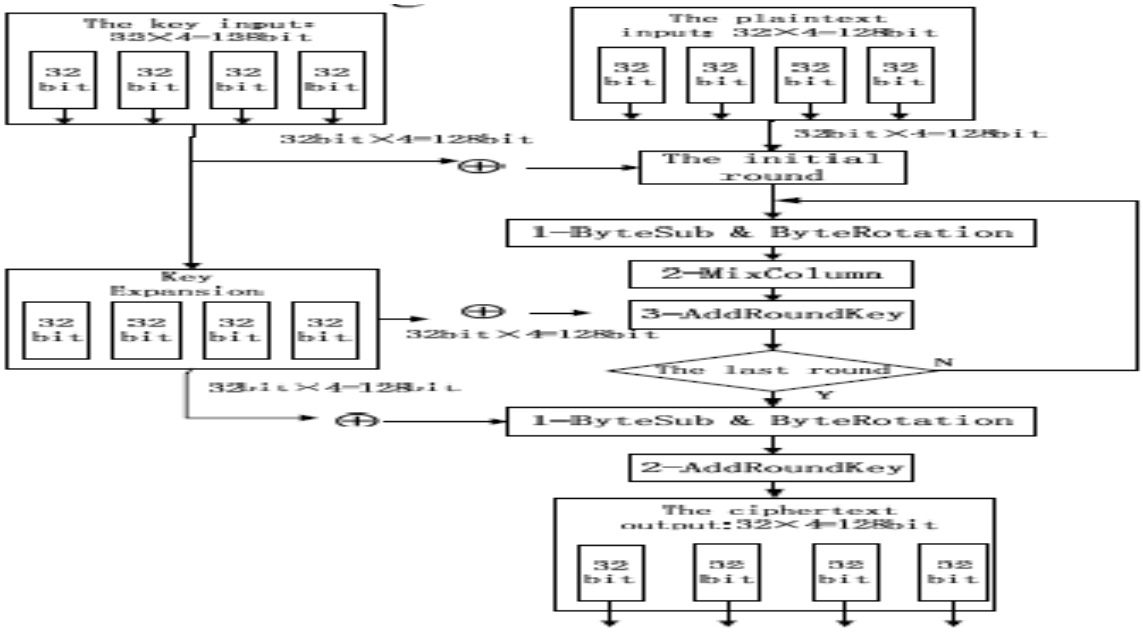


Figure 4. The new improved structure of AES algorithm

The functions of various parts of the structure shown above are described as follow:

- The initial round of encryption:

The four packets of consecutive 32-bit plaintext (128 bits) have been put into the corresponding registers. Meanwhile, another four packets of consecutive 32-bit initial key (128 bits) have been put into other registers by the control of the enable clock signal. Furthermore, this module should combine the plaintext and initial key by using the XOR operators.

- Round Transformation in the intermediate steps:

A round transformation mainly realizes the function of SubBytes and MixColumns with 32-bit columns. Four packets of round transformation are processed independently. Then the results of MixColumns and the 32-bit keys sourced from Keyexpansion are combined by using XOR operators. Here, the round transformation is a module with 64 input ports (32- bit plaintext+32-bit key) and 32 output ports.

The function of SubByte is realized by Look-Up Table (LUT). It means that the operation is completed by the Find and Replace after all replacement units are stored in a memory (256×8bit = 1024 bit).

The implementation of MixColumn is mainly based on the mathematical analysis in the Galois field GF(28). Only the multiplication module and the 32-bit XOR module of each processing unit(one column) are needed to design, because the elements of the multiplication and addition in Galois field are commutative and associative. Then the function of MixColumn can be achieved. Fig.5 is a block diagram for the introduction of pipelining technology used in the round transformation.

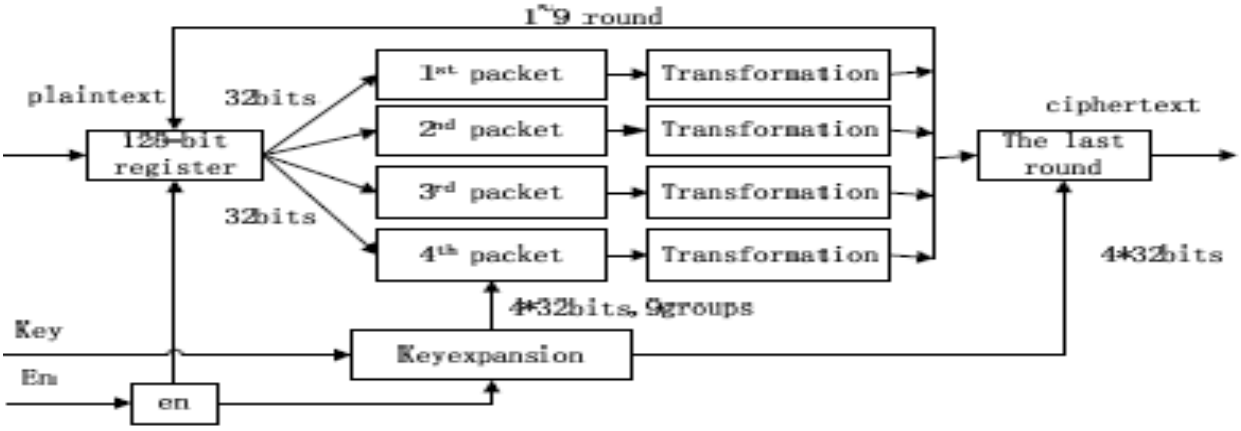


Figure 5. The round processing with pipeline technology

In the process of pipelining, the 128-bit data is divided into four consecutive 32-bit packets that take round transformation independently.

The operation of the above four groups of data can be realized in pipelining technology. In brief, it can be described as follow: store the unprocessed data in the 128-bit register, and
control the clock for re-starting the 128-bit register to read the new data when the four groups' operations have been overcome. Thus the 128-bit round-operating unit has been transformed into four 32-bit round-operating elements. The internal pipelining processing should be implemented during the whole nine intermediate Round Transformations of the four packets before achieving the 128-bit ciphertext.

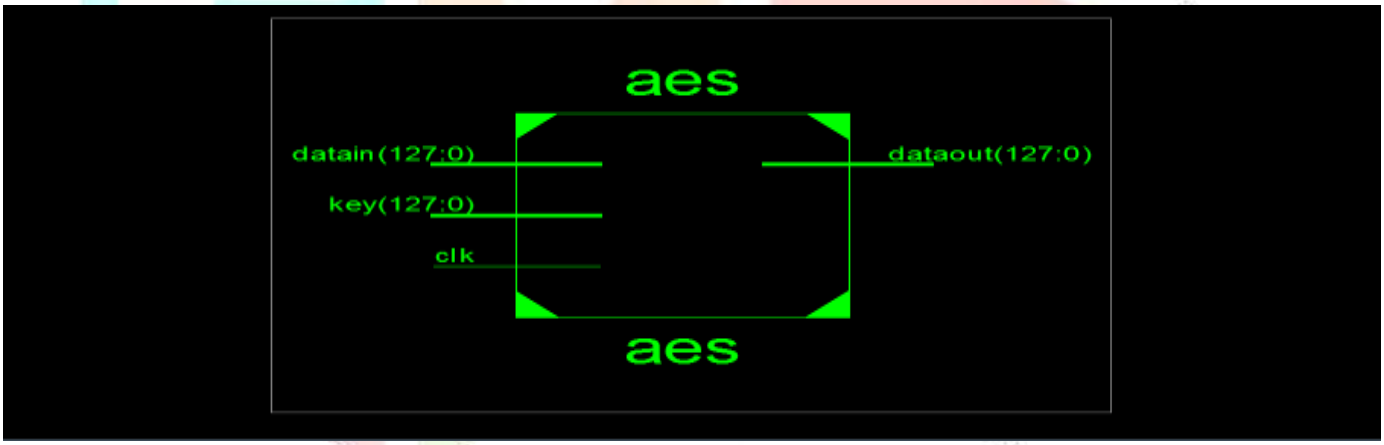
- The process of the last round

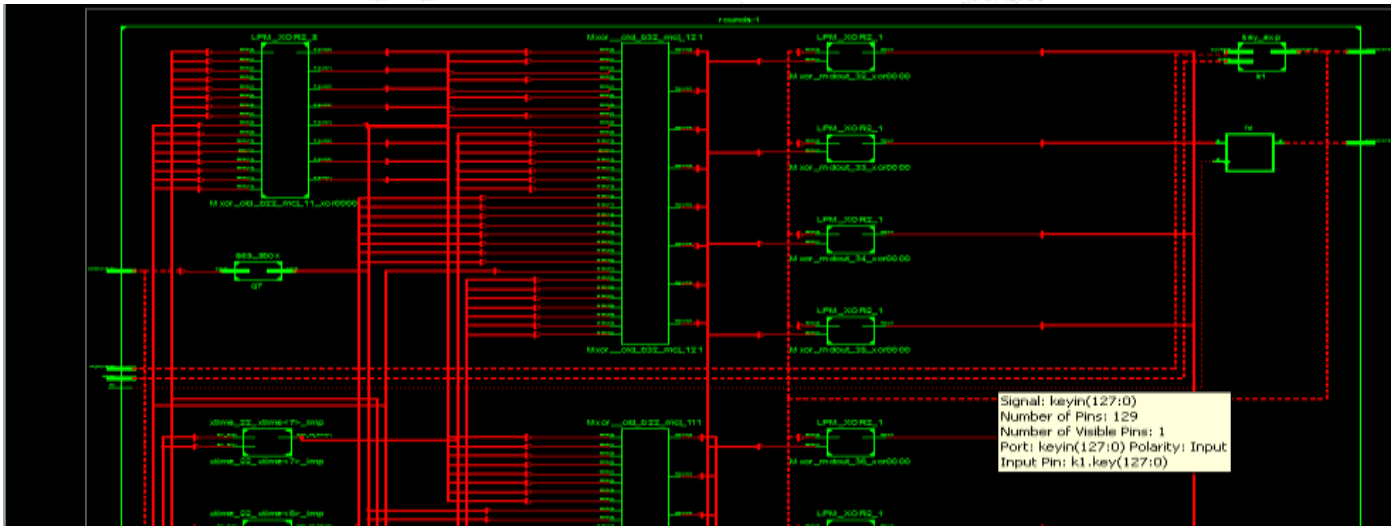
The final round is a 128-bit processor. After nine rounds of operations included Shiftrows, SubByte and Mixclumns, the 128-bit intermediate encrypted data will be used in XOR
operation with the final expanded key(4*32bit), which is provided by the key expansion module. The output of final round in the processor is the desired 128-bit ciphertext. Similarly, the ciphertext is divided into four packets of 32- bit data by an external enable signal.

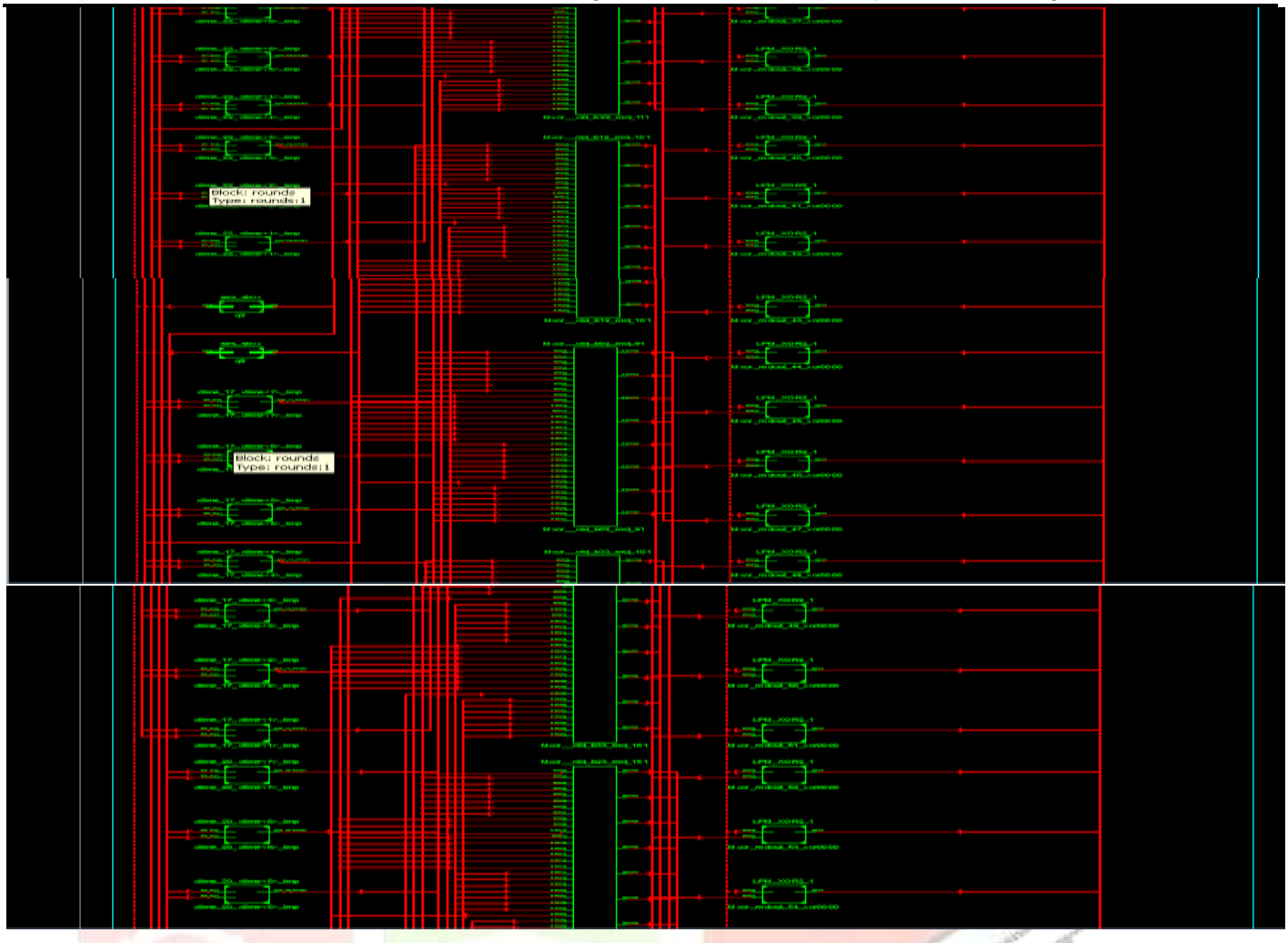
- Key expansion and Key extraction

This module is implemented basically the same with the traditional way as another part of the AES encryption algorithm. The only difference lies on the mode of data transmission. The
initial key and expanded keys are divided into four 32-bit data before being extracted.
All of the above modules can be decomposed into basic operations of seeking and XOR if the AES algorithm is implemented on FPGA. So the basic processing unit (look-uptable)
of FPGA can be used. The operation of AddRoundKey is taken first in each round. When the plaintext and initial key are input, the encryption module starts running, and the expanded
keys are stored into the registers at the same time. This implementation method is independent on a specific FPGA.

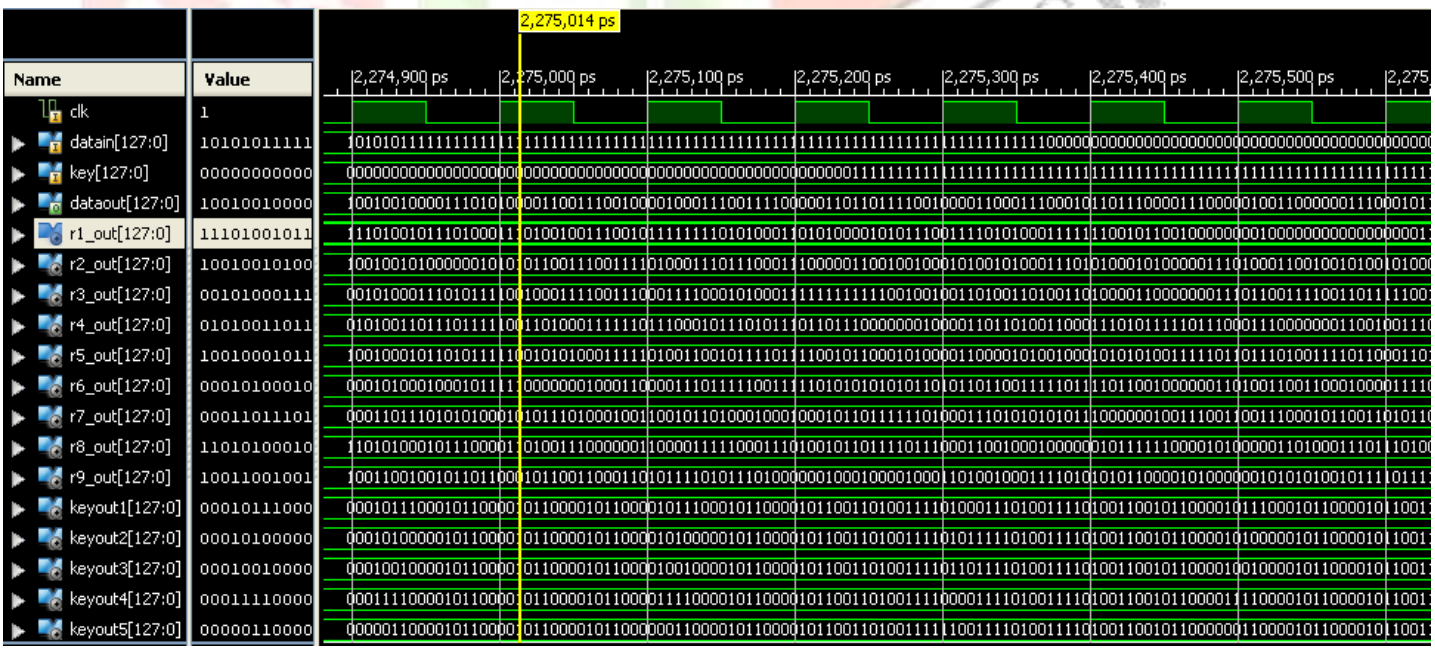
IV.RTL SCHEMATIC:



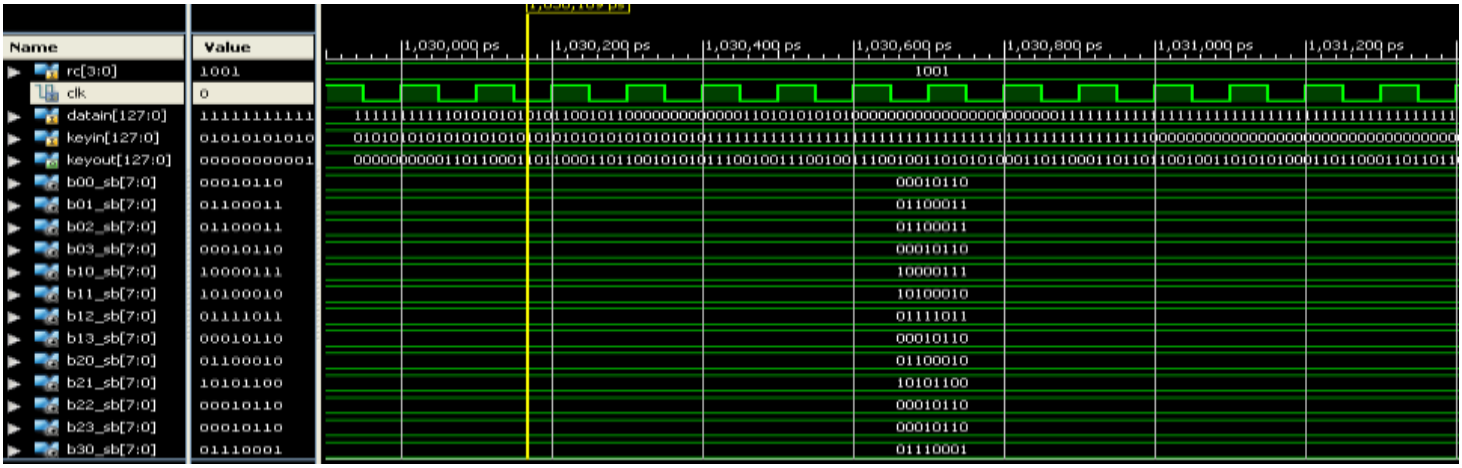




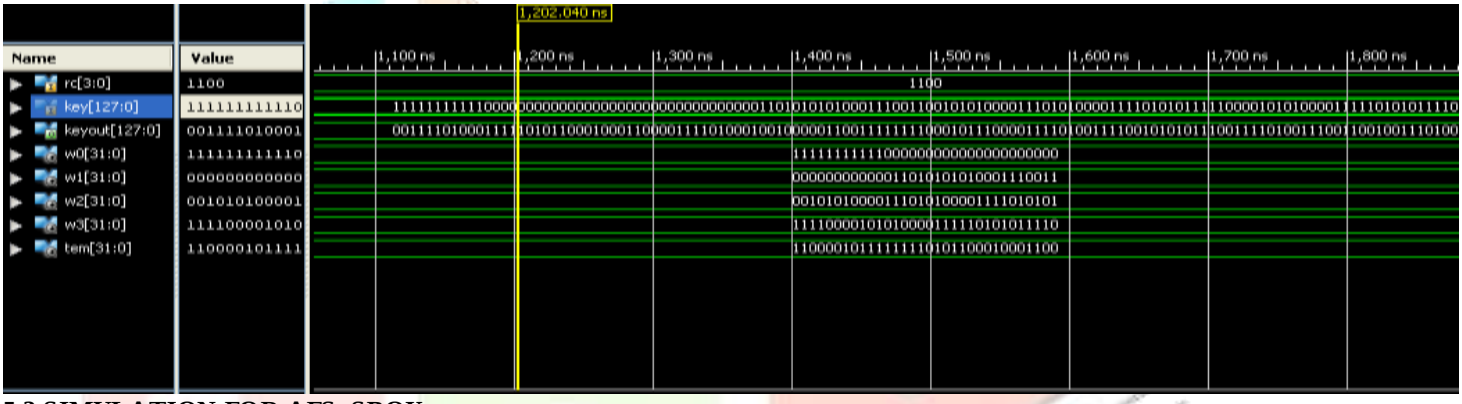
V. SIMULATION FOR AES:



5.1 SIMULATION FOR ROUNDS:



5.2 SIMULATION FOR KEY EXPANSION:



5.3 SIMULATION FOR AES_SBOX:

VI.APPLICATIONS:

- Widely used for computer and communication network.
- Information security has aroused high attention.
- Used in military, political and diplomatic fields
- Also applied to common fields of people's daily lives.

VII. FUTURE SCOPE AND CONCLUSION:

In this paper, we presented a efficient pipeline AES architecture which includes both encryption and decryption. Also sub pipelining architecture helped us to get higher throughput than earlier implementations. The design is modeled using Verilog HDL and simulated with the help of Model sim. Synthesis is done by using Xilinx. As the S-box is implemented by look-up-table in this design, the chip area and power can still be optimized. So the future work should focus on the implementation mode of S-box.

Mathematics in Galois field (28) can accomplish the bytes substitution of the AES algorithm, which could be another idea of further research.

REFERENCES:

[1] J.Yang, J.Ding, N.Li and Y.X.Guo,"FPGA-based design and implementation of reduced AES algorithm" IEEE Inter.Conf. Chal Envir Sci Com Engin(CESCE)., Vol.02, Issue.5-6, pp.67-70, Jun 2010.
[2] A.M.Deshpande, M.S.Deshpande and D.N.Kayatanavar,"FPGA Implementation of AES Encryption and Decryption"IEEE Inter.Conf.Cont,Auto,Com,and Ener., vol.01,issue04, pp.1-6,Jun.2009.
[3] Hiremath.S. and Suma.M.S.,"Advanced Encryption Standard Implemented on FPGA" IEEE Inter.Conf. Comp Elec Engin.(IECEE),vol.02,issue.28,pp.656-660,Dec.2009.
[4] Abdel-hafeez.S.,Sawalmeh.A. and Bataineh.S.,"High Performance AES Design using Pipelining Structure over GF(28)" IEEE Inter Conf.Signal Proc and Com.,vol.24-27, pp.716-719,Nov. 2007.
[5] Rizk.M.R.M. and Morsy, M., "Optimized Area and Optimized Speed Hardware Implementations of AES on FPGA", IEEE Inter Conf. Desig Tes Wor.,vol.1,issue.16,pp.207-217, Dec. 2007.
[6] Liberatori.M.,Otero.F.,Bonadero.J.C. and Castineira.J. "AES-128 Cipher.High Speed, Low Cost FPGA Implementation", IEEE Conf. Southern Programmable Logic(SPL),vol.04,issue.07,pp.195-198,Jun. 2007.
[7] Abdelhalim.M.B., Aslan.H.K. and Farouk.H. "A design for an FPGAbased implementation of Rijndael cipher",ITICT. Ena TechSoc.(ETNKS), vol.5,issue.6,pp.897-912,Dec.2005.

Author's Details:

Dr. ARVIND KUNDU, he did B. Tech from H.P. University (SHIMLA) in Electronics & Communication. He did M. Tech from M.D. University (ROHTAK) in Electronics & Communication Engineering. He did Ph. D from Ranchi University and area of research is ADHOC Networks, EMBEDDED System, Cryptography, Message authentication Protocol, Image Processing, Routing protocol etc. He is working as HOD ECE Department at SCIENT INSTITUTE OF TECHNOLOGY, IBRAHIMPATNAM

Mr. M.KARTHIK , He received B.Tech degree in ECE dept from JNTUH. Presently He is pursuing M.TECH in BRANCH of VLSI&ES at SCIENT INSTITUTE OF TECHNOLOGY, IBRAHIMPATNAM.

Mr.M.SURESH KUMAR He did B. Tech from Geetanjali institite of science and technology (JNTU Hyderabad) in Electronics & Communication. He did M. Tech from sri vidyanikethan engineering college (Autonomous),Tirupathi in Digital Electronics & Communication Systems. He is Currently working as **Assistant Professor** ECE Department at SCIENT INSTITUTE OF TECHNOLOGY, IBRAHIMPATNAM.