AN EFFICIENT VLSI ARCHITECTURE FOR AES AND its FPGA IMPLEMENTATION

Siddesh G K, Shruthi J

Professor, and Guide, Dept of ECE, JSSATE, Bengaluru, Karnataka, India
M. Tech, (VLSI Design, and Embedded Systems), JSSATE, Bengaluru, Karnataka, India

---***---

Abstract - *Security is the most vital element in information communication system, where greater randomization in secret keys increases the safety as well as the complexity of the cryptography algorithms. The algorithms corresponding to DES, Triple DES are compensating with enormous memory spaces and cannot be executed on the hardware platform. By using Field programmable gate arrays(FPGA'S) we can implement hardware platform situation owing to its reconfiguration nature, low charge and advertising space. The main objective of this paper is to reduce the delay in order to speed up the process by using pipelining. The RIJNDAEL cryptography algorithmic rule may be a block cipher used to encrypt/decrypt digital information and is capable of using cryptographical keys of 128, 192 and 256 bits. A unique characteristic of the proposed pipelined layout is that the round keys, that are consumed during distinct iterations of encryption, are generated in parallel with the encryption method. The overall delay related to each round key of coding delay of a plaintext block is reduced. This approach can by experimentation simulate the usage of Xilinx programming with Verilog hardware Description Language and hardware implementation on FPGA Spartan 3E.*

Key Words: **AES, Cipher text, Cryptography, FPGA, Pipelining, Rijndael(Encryption, Decryption).**

1. INTRODUCTION

Information needs to be secured from an unauthorized party. Cryptography is one in all of the secured mechanisms to protect data from public access. Cryptography is a Greek origin word this means that "secret writing" to make the records at ease and proof against attacks. Traditional cryptography was used for top-secret communications between humans. These days it's changed into the algorithmic program based mostly cryptography keep with demand through the users. It consists of 2 methods encryption and decryption, inside the primary method encryption; the plain text (original message) might be converted into secured textual content or Ciphertext (Encrypted message) using a specific algorithm. Besides, decoding here ciphertext might be changed into the plain content the utilization of all the reverse process connected for encryption. AES encryption is based on a personal key (additionally referred to as a symmetric key) and public key algorithm. personal Key algorithms contain only one key, each for encryption as well as decryption whereas; public key algorithms involve a pair of keys, one for encryption and other for decryption. Advanced encryption standard is based on a public key algorithm.

2. ADVANCED (AES) ENCRYPTION STANDARD/RIJNDAEL

The AES is a subset of a much larger encryption algorithm known as Rijndael, which become one among many proposals to the NIST competing for becoming a widespread encryption algorithm. On October of 2000, the NIST introduced the Rijndael algorithm as the winner due to high-quality normal routing in security, overall performance, efficiency, implementation capability, and ease.

The AES algorithm is a symmetric cipher. In Symmetric ciphers, a single secret key is used for both the encryption and decryption, whereas in asymmetric ciphers, there are two sets of keys referred to as a private key and public keys. The plaintext has encrypted the usage of the public key and can only be decrypted using the private key.
Further, the AES algorithm is a block cipher because it operates on fixed-length groups of bits(blocks), whereas in stream ciphers, the plaintext bits are encrypted one by one, and the set of transformations carried out to successive bits may also vary throughout the encryption technique.

The AES algorithm operates on blocks of 128 bits, with the aid of the usage of cipher keys with lengths of 128, 192 or 256 bits for the encryption process. The input and output for the AES algorithms are blocks of 128 bits. The cipher key input is a series of 128, 192 or 256 bits. In different words, the length of the cipher key, $N_{K,}$ is either 4,6 or 8 words which represent the number of columns in the cipher key. The AES algorithm is classified into three versions based totally on cipher key length.

3. AES ALGORITHM

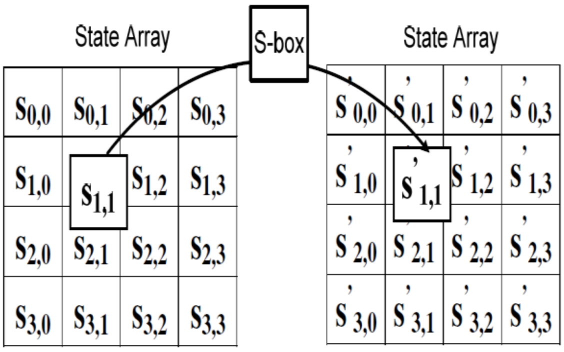
All operations are performed on a two- dimensional 4x4 array of bytes which is called the state, and any individual byte within the state is referred to as $S_{r,c}$, where 'r' represent the row and 'c' denotes the column. At the beginning of the encryption process, the state is populated with the plaintext. Then the cipher key performs a set of substitutions and permutations in the state. After the cipher operations are

conducted in the state, the final value of the state is copied to the ciphertext output.
The AES cipher operates on state or an entire row/column. Then, an initial Round Key addition is performed in the state. Round keys are derived from the cipher key using the Key expansion routine. The key expansion routine generates a sequence of round keys for every round of transformations that are performed on the state.

The transformations performed in each state array are different and each round depends on cipher key. Each round of AES cipher(except the last one) consists of all the following transformations. SubBytes(s-box), ShiftRows, MixColumns, AddRoundKey.

3.1 Bytes substitution

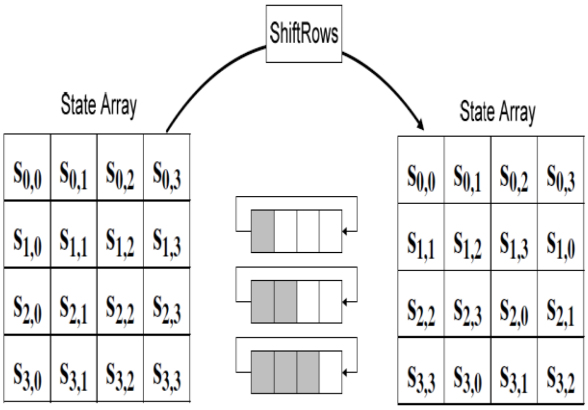
This transformation operates on each byte of the state using substitution table which is a non-linear byte. Substitution table consists of ff rows/columns.


State Array
S-box
State Array
S0,0 S0,1 S0,2 S0,3
S1,0 S1,1 S1,2 S1,3
S2,0 S2,1 S2,2 S2,3
S3,0 S3,1 S3,2 S3,3
S' 0,0 S' 0,1 S' 0,2 S' 0,3
S' 1,0 S' 1,1 S' 1,2 S' 1,3
S' 2,0 S' 2,1 S' 2,2 S' 2,3
S' 3,0 S' 3,1 S' 3,2 S' 3,3

Fig(1a)

3.2 Shift rows

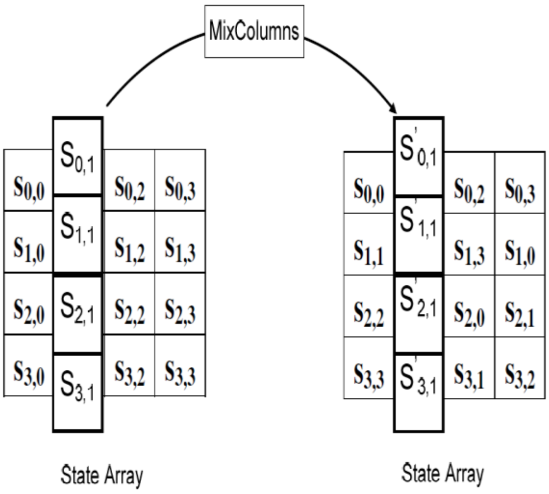
With the Shift Row, transformation first row is not shifted and the remaining three rows are shifted circularly. In the second row, one byte is left shifted circularly. For the three row, a 2-byte round left shift is done. For the fourth row, a three-byte round left shift is accomplished. And for the decryption technique, it will be shifting towards right circularly.



Fig(1b)

3.3 Mix Columns Transformation

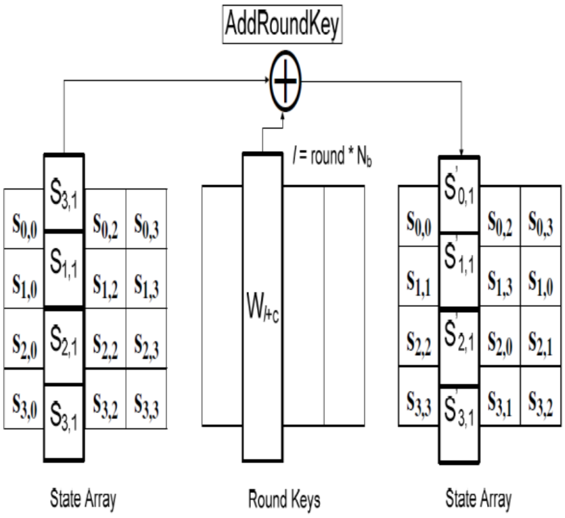
This transformation is based on Galois field multiplication. Each byte of a column is changed with the different value that may be a feature of all 4 bytes in the given column. The transformation operates on the state column, treating each column as a polynomial. The columns are considered as polynomials over GF (28).



Fig(1c)

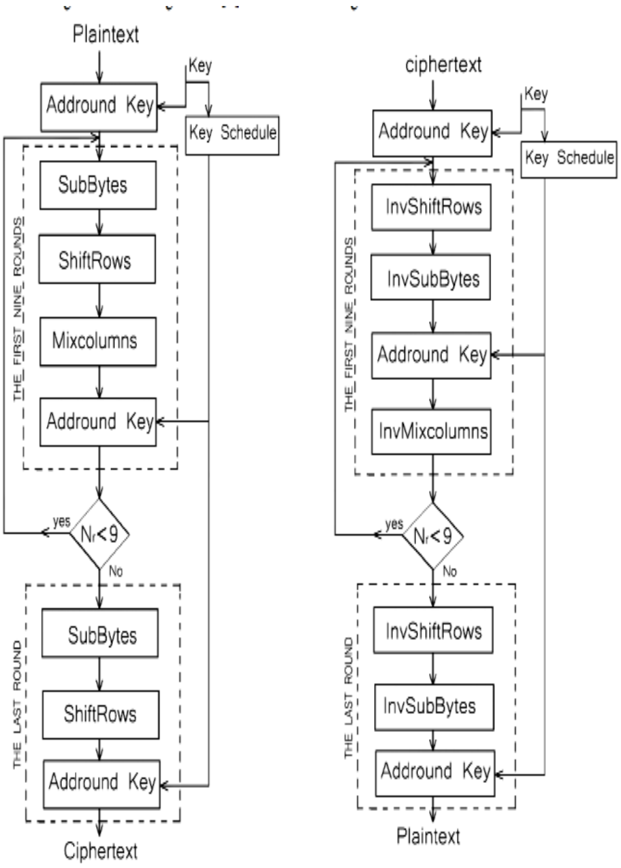
3.4 AddRoundKey

The AddRoundKey operation is meant as a cipher; all the 128 bits of the state unit of activity XORed with four, 32-bit words of the extended key on account of key enlargement. AddRoundKey is the most effective operation that entails using the key to making sure safety. The AES key expansion set takes a four-word (16-byte) as input and produces a linear array of 44 words.



Fig(1d)

Below figure shows block diagram of RIJNDAEL encryption/decryption.



(a) Encryption (b)Decryption

fig(2a) Rijndael encryption/decryption

4. AES KEY EXPANSION

The AES algorithm requires 4 words of round keys for each encryption round. That can be a typical of four*(Nr+1) round keys thinking about the initial set of keys required for the number one upload round Key transformation. All of the round keys are derived from the cipher key itself.

The AES key expansion algorithm takes as input a four-word key and produces a linear array of 44 words. The Key is copied into the primary 4 words of the expanded key. Then the rest of the key is filled in 4 words at a time. Each added word w[i] relies upon on the straight away preceding word, w[i– 1],and the word four positions returned w[i – 4]. In three out of four instances, a simple XOR is used.

Every round uses four of these words as shown in fig 2(b). Each word incorporates 32 bytes which suggest each subkey is 128 bits long.

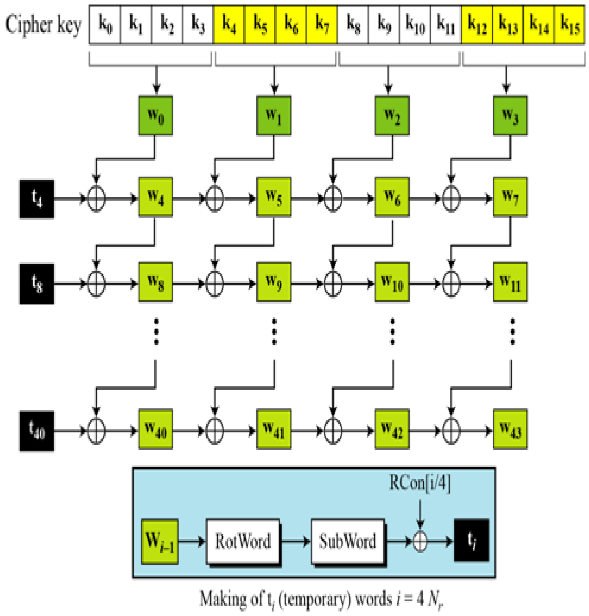

Cipher key
k_0 k_1 k_2 k_3 k_4 k_5 k_6 k_7 k_8 k_9 k_{10} k_{11} k_{12} k_{13} k_{14} k_{15}
w_0 w_1 w_2 w_3
t_4 w_4 w_5 w_6 w_7
t_8 w_8 w_9 w_{10} w_{11}
t_{40} w_{40} w_{41} w_{42} w_{43}
RCon[i/4]
w_{i-1}
RotWord
SubWord
t_i
Making of t_i (temporary) words $i = 4\ N_r$

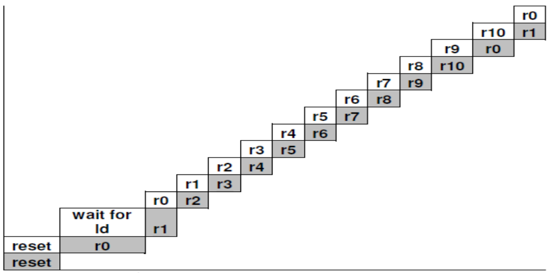
Fig (2b) AES key expansion

5. METHODOLOGY

As discussed above the round key generation in the proposed design is pipelined with the encryption rounds. The pipelined operation of round key expansion and the cipher is shown in fig 2(c). Each AES encryption round 'n' is pipelined with the key generation for round 'n+1'.

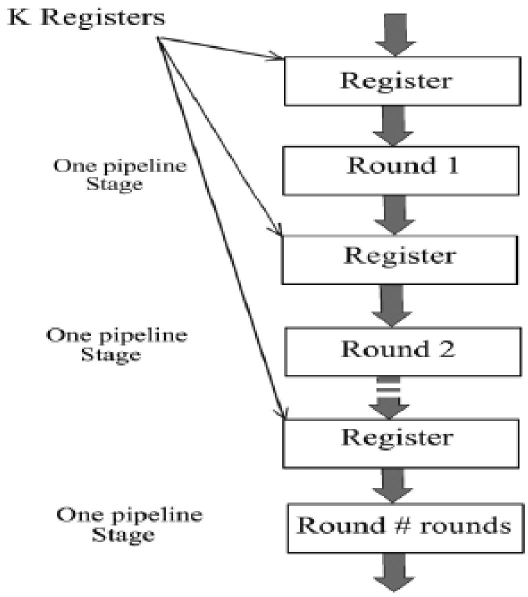
Pipelining techniques offer improvement in speed with the cost in terms of area. By using pipelining methodology very high throughput and efficiency are achieved.

The most important advantage of the pipelined design is the lower delay for each encryption iteration.
since the round keys for every encryption, iteration is present at the beginning of the iteration cycle. The lower delay in every encryption, iteration means that quicker completion of every round of encryption. This reduces the overall encryption delay and allows the design to control at higher clock frequencies. The higher clock frequency will increase the message encryption rate making its design suitable for time critical encryption applications.



Fig(2c) pipelined Round key generation and cipher rounds

Fig 2(d) below shows complete pipelined structure which consists of k registers. One pipeline stage consists of one round and each round consists of different transformation. The key output of the first transformation is fed as input to the second transformation through registers and so on till it completes last round.



Fig(2d) pipelined structure

6. RESULTS AND OUTCOME

In this project, a hardware accelerator for the AES128 encryption algorithm was designed, modeled and verified using the System Verilog hardware description language. The pipelined design of the AES encryption algorithm reduces the delay related to every round of encryption, that allows the hardware to control at a way higher clock frequencies, compared to a non-pipelined design. This will increase the message encryption throughput and makes the hardware model appropriate for time essential encryption applications. Additionally, the hardware implementation of AES encryption algorithm provides final secrecy of the encryption key, with much faster speed compared to software implementation, and higher throughput by means of inherent hardware concurrency.

ACKNOWLEDGEMENT

I express my sincere gratitude to Dr.Siddesh G K Dept of ECE JSSATE, Bengaluru, for his stimulating guidance, & constructive suggestions to improve the quality of this paper.

REFERENCES

[1]Joan Daemen and Vincent Rijmen, The design of Rijndael, AES, Springer-Verlag 2002.

[2]International Journal of Advances in Engineering & Technology, May 2012. AN EFFICIENT FPGA IMPLEMENTATION OF AES ALGORITHM Shylashree.N, Nagarjun Bhat and V. Shridhar Research Scholar (R.N.S.I.T), in E.C.E, at PESCE, Mandya, Karnataka, India.

[3]ARPN Journal of Engineering and Applied Sciences. VLSI Implementation of Enhanced AES Cryptography Lakavath Srinivas, Zuber M. Patel, B Chandra Sekhar Naik Electronics Department, SVNIT, Surat, Gujarat, India, 2 Assistant Professor, Electronics Department, SVNIT, Surat, Gujarat, India.

[4]International Journal Of Advanced Research and Innovation -Vol.7, Issue. FPGA Based Implementation of AES Encryption and Decryption with Verilog HDL Y.Aruna1, Prof.S.N.Shelke2 M.Tech (Electronics), JDCOE, Nagpur. Algorithm in FPGA Device," in IEEE, 2007.

[5]Shylashree. N, Nagarjun Bhat, and V Sridhar, "FPGA implementations of advanced encryption standard": a survey," in ijaet, 2012.

[6]Mr. Atul M. Borkar, Dr. R. V. Kshirsagar and Mrs. M. V. Vyawahare "FPGA Implementation of AES Algorithm" 2011 IEEE

[7]William Stalling (2006), Network Security Essential Applications and Standards(chapter 4.6 Finite Fields of the Form GF(2^n)) , New Jersey Pearson, Education, 2000.

[8]L.Thulasimani, "A Single Chip Design and Implementation of AES-128/192/256 Encryption Algorithms"-International Journal of Engineering Science and Technology, Vol.2(5),2010,1052-1059.