SYNTHESIZED REPORT ON THE COMPARISON OF LUT AND SPLITTING METHOD FOR DECRYPTION UNIT FOR AES

Puneeth S B[1], Tejaswini M L[2]

[1]*PG Scholar, Department of Electronics and Communication, Don Bosco Institute of Technology, Benagaluru, India*
[2]*Assistant Professor, Department of Electronics and Communication, Don Bosco Institute of Technology, Benagaluru, India*

Abstract

Any encryption or decryption method will have certain key based on which the encoding and decoding will be performed. This is done to avoid access of data by unauthorized personal. Without the decoding key, encoded data is junk. Similarly, Federal Information Processing Standard (FIPS) developed Advanced Encryption Standard, which was used for saving digital data especially in magnetic tape like debit cards and credit cards, so that it provides security for the details and also this can be used in security of PDA's which need to work very efficiently with high speed encoding and decoding and also need to consume less area as possible. It can be built using purely hardware or purely software i.e. using programming language such as Verilog. Decryption and Encryption has main part, Mix Columns and Inverse Mix columns, on which the whole AES operation depends. Here synthesis is performed for the decryption unit of the AES, which can be performed in two methods i.e. Look-up Table and Splitting method. Comparison of two methods is done by synthesizing the program in Spartan -3E of Xilinx ISE 14.1 Suite.

Keywords: *Encryption, Decryption, FIPS, Mix Columns, Inverse Mix Columns.*

----------***----------

1. INTRODUCTION

Cryptography is used for saving a data which the user doesn't wish to be accessed by unauthorized authority. AES is used for safe guarding the electronic data which has entirely replaced the analog data in a past decade. Because this method is not only used in storing data but it is also used in files transactions such as data related to e-commerce, legal files, reports regarding any work will be transferred from one point to other using internet or through phone calls which will be created or exchanged needs security. Many works have been done in this field to make the program to work fast, but it can be still advanced using other methods and working on optimization. To achieve fast performing hardware for this, it will be costly since it has to be replaced with hard disk, high speed bus, etc. This can be easily achieved in software. Hence always reduction in usage of hardware is preferred for optimizing and the same is in increasing demand. In Cryptography there are two parts Encryption and Decryption. Decryption, it is for decoding the data which is Encrypted using certain cryptographic rules[7].

AES is symmetric block cipher designed for 128 bits with 128,192, 256 bit size key, which will be implemented for the byte data block of size 4*4, where an image can be taken and reduced for that size. Every round of AES for encryption will perform four steps which is common for all they are, S-Box/Sub bytes, Shift row, Mix columns and Add round key. Each round will have its own reverse operation block wise.

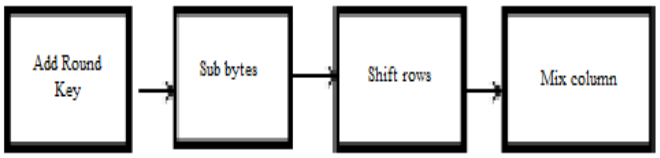

Fig-1: Encryption Block diagram.

For decryption there are four steps which is similar to the encryption they are, Inverse add round key, Inverse sub bytes, Inverse sub bytes, Inverse Mix columns[1]. These four steps make one round of the AES for both encryption and decryption. Based on the given key size the number of rounds of AES will be performed. Here the code written for the decryption block which is encrypted using certain key. This is done in matrix form. The key used for encryption is [2 3 1 1]. With this key any particular 4*4 data will be subjected to matrix multiplication by shifting right for each time of multiplication, which results in 4 values which is encrypted, these values need to be feed to the decryption unit which uses another key for decrypting the data which is [E B D 9] whose values will multiplied by shifting right. This multiplication is part of inverse mix columns and mix columns, after multiplication in inverse mix columns it need to be sent to Galios field multiplier, which will have a value with which the product will be xored. This multiplication can be performed in two different methods i.e., LUT and Splitting method. Each method has its own advantage and disadvantage. Galois field multiplication is operated based on power of 2 whose explanation is beyond this concept[5], [6].

2. LOOK-UP TABLE

It is pre-stored values for all the possible combination of multiplier and multiplicand, whose products are unique for the given combination at any point of time. The table can be created using code book generation which will generate to code tables out of which one is called L-Table and the other is named as E-Table. The values for these tables can be given in number system which is comfortable for the user, whose values do not repeat and the values are of 8bit. This table helps in reducing multiplication operation every time, which consumes much of the time.

The encoding of the data is done by the help of same L table and E table. For encoding, the given data the following steps need to be followed.

For example, [34 56 78 A1] are the inputs which are given to the encoding block, As explained above the key for encoding is [2 3 1 1] then, if the input is multiplied with key 1 then it's value will not be taken from LUT, it will be just multiplied.

The key will be operated by shifting right for every row,

2 3 1 1
1 2 3 1
1 1 2 3
3 1 1 2

This will be the key, with which the inputs will be multiplied

Output[0]=34*2 xor 56*3 xor 78*1 xor A1*1.
=E(L(34)+L(2)) xor E(L(56)+L(3)) xor 78 xor A1.
=E(21+19) xor E(8B+01) xor 78 xor A1.
=E(3A) xor E(8C) xor 78 xor A1.
=68 xor FA xor 78 xor A1.
=4B

Output[1]=34*1 xor 56*2 xor 78*3 xor A1*1
=34 xor E(L(56)+L(2)) xor E(L(78)+L(3)) xor A1.
=34 xor E(8B+19) xor E(4E+01) xor A1
=34 xor E(A4) xor E(4F) xor A1
=34 xor AC xor 88 xor A1
=B1

Similarly it is performed for the other two outputs which will be 61 and 29. While adding the numbers it has to be checked whether the sum is more than FF, if it is then mod(FF) has to be performed.

For decoding, the key used is [E B D 9]. Similar to the encoding method the keys are performed shift right and multiplied with the data which need to be decoded.

E B D 9
9 E B D
D 9 E B
B D 9 E

Input= 4B, B1, 61, 29

O[0]=4B*E xor B1*B xor 6A*D xor 59*9
=E(L(4B)+L(E)) xor E(L(B1)+L(B)) xor E(L(61)+L(D)) xor E(L(29)+L(9))
=E(F1+DF) xor E(BB+68) xor E(28+EE) xor E(25+C7)
=E(1D0) xor E(123) xor E(116) xor E(EC)
=E(D1) xor E(24) xor E(17) xor E(EC)
=CF xor 37 xor A4 xor A7
=34

Similarly we get other remaining answers in the same method which are 56, 78, A1

The product of multiplication is given by the L lookup table and adding the results of multiplicands and finding the E lookup table value for product.

Either in Encryption or in decryption the key must be expanded, which will be used in Add Round key function. Each time add round key is used, the results will be XORed. During the AES performance Add round will be called for each time and one extra time during the beginning of AES.

3. SPLITTING METHOD

One of the easy methods of obtaining product of 2 numbers being multiplied is Splitting method; multiplication being a basic mathematical operation to find the product of big numbers which is difficult to find the product using normal method is complicated. As the name indicates both the numbers which need to multiplied are split in such a way that one number is multiple of 10 and remaining will be written with it. After the multiplication of all combinations it will be added up to give final answer.

Example: 42*56,
It is split into 40+2 and 50+6.

Now, all the combinations of multiplication will be performed 40*50,2*50,40*6,2*6.
=2000, 100, 240, 12

If we add all these terms, we get 2000+100+240+12=2352, which is the product of 42*56.

Galios field multiplier is a part of this splitting method in AES. It is a part of operation in Inverse mix columns. The data which is encoded need to be decoded, for example if 10001101 then it is given as $x^7+x^3+x^2+1$. In this, to get the sum of two numbers it needs to be xor bitwise. Polynomial algebraic multiplication is performed by multiplying each term with rest of the terms in the other polynomial, which results in a polynomial product. In the product if the power of the polynomial is more than 7, then it needs to be reduced so modulo of $x^8+x^4+x^3+x+1$need to be applied. This is done by x^{i-8}, 'i' is the degree of polynomial that has to be reduced. This is done by xoring the product with 11B where it has to be seen that MSB bit of the polynomial should match with the MSB of 11B and bitwise xor operation need to be performed.

For example: $(x^3+x)*(x^6+x^2)=x^9+x^7+x^5+x^3$.

$$x^9+x^7+x^5+x^3$$
$$+\ x^9+x^5+x^4+x^2+x$$
$$x^7+x^4+x^3+x^2+x$$
$$+\ x^8+x^4+x^3+x+1$$
$$x^8+x^7+x^2+1$$
$$+\ x^8+x^4+x^3+x+1$$
$$x^7+x^4+x^3+x^2+x$$

For the inverse operation in matrix multiplication, we take E, B, D, 9, in splitting method these numbers will be split to:

E=2+C;
B=3+8;
D=1+C;
9=1+8;

Distributive law holds good for addition, hence E B D 9 will be split into the 2 matrices as shown above. Data encoded will be multiplied with both the matrices. The key used for decoding, which will be split into 2 matrix will be performed shift right and matrix multiplication will be performed and results are added up.

4. RESULTS

To simulate and synthesis the program which is written in Verilog in Xilinx Spartan-3E. The summary report for the written program gives the information about the number of slices consumed and number of 4 input LUTs consumed.
For the LUT method, 426% of slices are consumed and 849% of 4 input LUT consumed out of the available in Spartan-3E package. This results in over mapping since it's requirements cross Spartan 3E specifications. This also leads to the consumption of large area.

The summary of Splitting method will give same information and even is implemented for same specification as mentioned above, the number of 4 input LUT consumed during the execution is around 5% and number of slices consumed is around 6%. Number of bonded IOB's is 96%.

5. FUTURE SCOPE AND CONCLUSION

Number of gates used in above mentioned two methods is more even after optimization. Hence alternative method is required or the existing methods need to be modified so that the results are made better. Vedic multiplier is used in splitting method which replaces the normal multiplier in mixed columns and inverse mixed columns and also in Galios field multiplier[3], [4].

REFERENCES

[1] J. Daemen and V. Rijmen, *AES Proposal: Rijndael*, AES Algorithm Submission, September 3, 1999.

[2] Advanced Encryption System (AES), Nov. 26, 2001.

[3] Huddar, S.R.; Rupanagudi, S.R.; Kalpana, M.; Mohan, S., "Novel high speed vedic mathematics multiplier using compressors," Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on , vol., no., pp.465,469, 22-23 March 2013

[4] Sushma R. Huddar, Sudhir Rao Rupanagudi, Venkatesh Janardhan, Surabhi Mohan, and S. Sandya, "Area and Speed Efficient Arithmetic Logic Unit Design Using Ancient Vedic Mathematics on FPGA," in Advances in Computing, Communication, and Control, pp. 475-483, Springer, Berlin Heidelberg, 2013.

[5] Hua Li and Zac Friggstad, Department of Mathematics, University of Lethbridge. An efficient architecture for the AES Mix columns operation. IEEE 2005.

[6] Dr.R.V.Kshirsagar, M.V.Vyawahare, "FPGA Implementation of High speed VLSI Architectures for AES Algorithm", 2012 Fifth International Conference on Emerging Trends in Engineering and Technology.

[7] "ABI Software development" written by Adam Bernet.

[8] Ashwini M. Deshpande, Mangesh S. deshpande and Devendra N. Kayatanavar, "FPGA Implementation of AES Enryption and Decrytion", International Conference On "Control, Automation, Communication And Energy Conservation -2009.

[9] AES page available via http://www.nist.gov/CryptoToolkit

BIOGRAPHIES

Puneeth S B, He has obtained Bachelor of Engineering degree in Electronics and Communication from Visveswarya Technical University, Belguam in 2013. Currently presuing Master's of Technolgy in Digital Electronics from Visveswarya Technical University, Belguam.

Tejaswini M L, She has obtained Bachelor of Engineering degree in Electronics and Communication from Visveswarya Technical University, Belguam in 2004. Master's of Technolgy in Dayanad Sagar College of Engineering, Bengaluru in 2008. She is currently Assistant Professor in Don Bosco Institute of Technology, Bengaluru.