International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Design an Aes Using Inexact Floating-Point Adders

[1]G. Raghavendra Rao, [2]G. Laksmi Prasanti, [3]M. Sneha Latha, [4]M. Kamakshi, [5]M. Ram Sai Pradeep, [6] P. Pratyusha

[1,2,3,4,5]B.Tech-Scholar, Dept of ECE, ST. Ann's College of Engineering and Technology, Chirala, India.
[6]Assistant Professor, Dept of ECE, ST. Ann's College of Engineering and Technology, Chirala, India.

ABSTRACT: *In present days it is more efficient to reduce the area and increase the cost in VLSI applications. In this paper we are going to implement the AES algorithm. By using cryptography concept the AES algorithm is implemented. The main intent of this algorithm is to secure the information. Generally, Advanced encryption standard is an algorithm which performs various operations in sequential steps. This algorithm involves the both encryption and decryption process to protect the data and it is the most efficient public key encryption system. This system depends on the Rijndael algorithm which produces faster and efficient cryptography keys. At last we can conclude that compared to existed system, the proposed system will protect the data in very efficient way.*

Key words: **AES algorithm, encryption and decryption.**

I.INTRODUCTION

As we know that Internet plays important role in our day to day life. The people can transfer important data through internet such as Emails, banking, transaction and online purchases. Now, to secure all these transaction security plays major role and it is more efficient. But the network security is obtained only by cryptography. Here cryptography means the art and science of transforming the message to provide them with secure and immune attacks. Coming to the cryptography strength, it is measured in time and the result of cryptography is in cipher text and it is very difficult to decipher. Cryptography algorithm works in the combination of words, numbers and phrases. The security of encrypted data depends on two things mainly one is strength of cryptographic algorithm and second one is the secrecy of key. According to science, cryptography means writing the secret code. Cryptography not only protects the data but also used for user authentication.

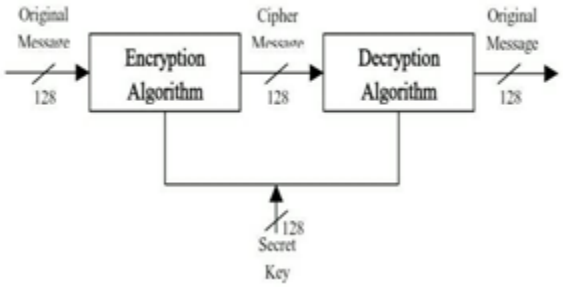

Fig. 1. Representation of encryption and decryption

In this paper we are implementing AES algorithm. Generally AES is an cryptographic algorithm which is used for security purpose. The AES algorithm will protect the electronic data. It is an symmetric block cipher which encrypts and decrypts the information. Here encryption will convert the data to an cipher text and decryption will converts the cipher text to an original form which is called as plain text. From below figure (1) we can observe the

representation of encryption and decryption. At last we can say that by using the proposed system the entire information is secured.

II. EXISTEDSYSTEM

The below figure (2) shows the existed system. Generally, an FP adder architecture consists of hardware blocks. For the purpose of exponent comparison, mantissa alignment, mantissa addition. Now two operands are unpacked from the FP format and each mantissa is added to hidden bit 1. Here the addition of FP numbers involves comparison of two exponents and adding the two mantissas. To find the largest number, exponents are first evaluated and then depend upon the comparison of exponent the mantissa is swapped.

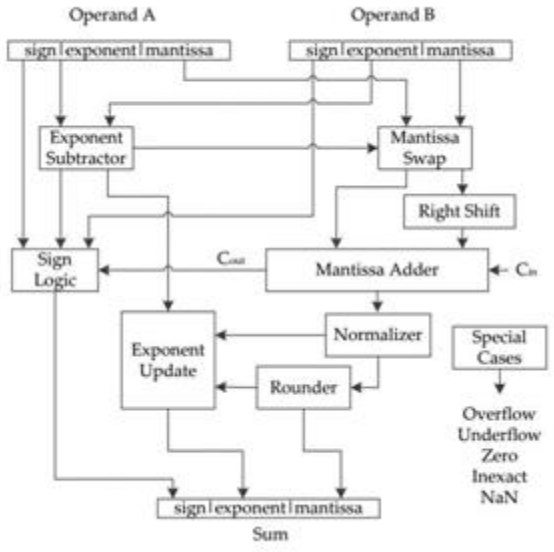

Fig. 2. Existed system

Now we use the lead zero detection process which is an key step for normalization. The normalization process is completed by left shifting the number of leading zeros. At least before storing back the result, rounding process is done. This is applied to the normalized result and it is represented by flags.

III. PROPOSED SYSTEM

Advanced encryption standard is an symmetric block cipher used by the u.s.government to protect the classified information and it is implemented in software and hardware for sensitive data encryption. Each round in encryption process consists of some steps. Each round posses again four rounds. They are 1. Sub bytes, 2. Shift rows, 3. Mix column and 4. Add round key. Coming to the substitution, in this sub bytes are substituted as byte by byte during the forward encryption process.

Coming to this shift rows, in this during forward process the rows are shifted at state array. Next one is to mix up the bytes in each column separately during forward process. At last during forward process a round key is added to the output of previous step. Now this step differs from others because of size difference. In the proposed system involves two operations one is encryption and decryption. Let us discuss about the encryption process in detail manner. From below figure (3) we can observe the AES encryption algorithm.

The implementation process of AES encryption algorithm is same as the process involved in key expansions. Here the shift rows function iterates all the rows and then

call shift row with the correct offset. Now around key is generated during iteration process. In XOR gate the each byte of key is respective to the byte of state. As before shift row process is performed in the same way the mix columns process is implemented. Here mix column is implemented by first one which generates a column and then call mix column. At last this is applied to matrix multiplication. Entirely in one AES round it consists of all four operations on the state.

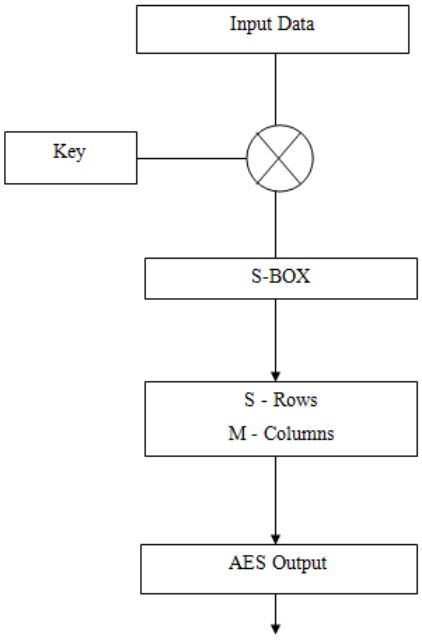

Fig.3. Encryption

This is about the AES encryption algorithm now let us discuss about the decryption process. In decryption process, the key schedule remains same. Here we need to implement the following operations they are inversed sub bytes, shift rows and mix columns. Coming to add round key it remains same as before. In this we use inversed s box for substitution and multiplication matrix is different for inversed mix column operation.

Now all these are kept together in one inversed main algorithm. So from this proposed system we can observe that it secures high information and it is more efficient. From below figure (4) we can observe the AES decryption algorithm.

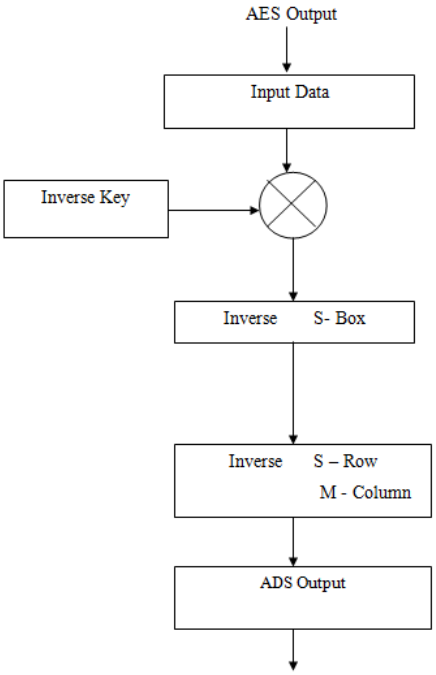

Fig 4. Decryption

IV. RESULTS

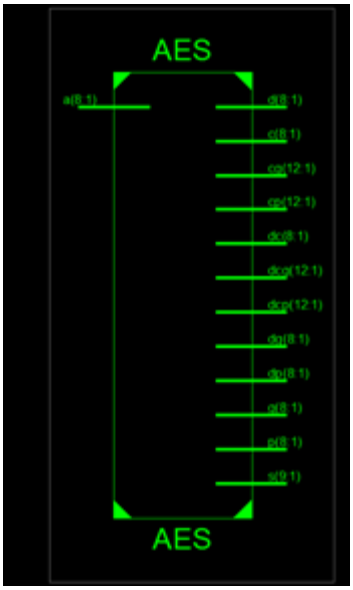

Fig 5. RTL Schematic

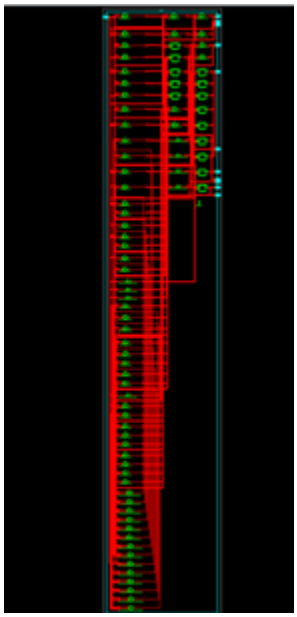

Fig 6. Technology Schematic

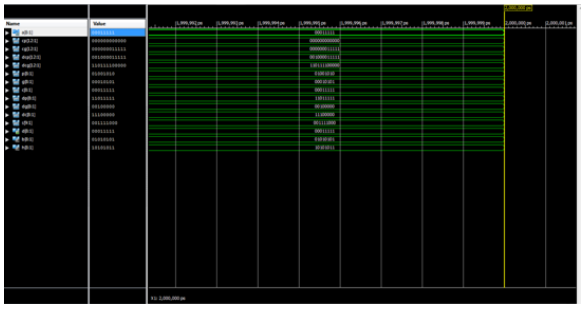

Fig 7. Output Waveform

V. CONCLUSION

To perform the both encryption and decryption process in VLSI architecture we use Rijndael AES algorithm. For the implementation of multiplicative inverses we use s boxes and this shares the information between encryption and decryption. Now round keys are used in each round for the implementation in real time. The main intent of encryption is to hide the data from unauthorized users and coming to decryption is used to get the original data. In this paper we propose a method to employ the crypto processor that run in integration way with general purpose processor. At last to encrypt the data in AES algorithm we have presented pipeline version. From this proposed system we can observe that it protects the data in an efficient way.

VI. REFERENCES

[1] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli, “A DCT Domain Visible Watermarking Technique for Images,” in

Proc of the IEEE International Conf on Multimedia and Expo, 2000, pp. 1029–1032.

[2] M. S. Kankanhalli and T. T. Guan, "Compressed-Domain Scrambler Descrambler for Digital Video," IEEE Transactions on Consumer Electronics, vol. 48, no. 2, pp. 356–365, May 2002.

[3] B. M. Macq and J. J. Quisquater, "Cryptography for Digital TV Broadcasting," Proceedings of the IEEE, vol. 83, no. 6, pp. 944–957, Jun 1995.

[4] H. Kuo and I. Verbauwhede, "Architectural Optimization for a 1.82 Gbits/sec VLSI Implementation of the AES Rijndael Algorithm," in Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems, 2001, vol. 2162, pp. 51–64.

[5] M. McLoone and J. V. McCanny, "Rijndael FPGA Implementation Utilizing Look-up Tables," in Proceedings of the IEEE Workshop on Signal Processing Systems, 2001, pp. 349–360.

[6] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A Compact Rijndael Hardware Architecture with S-Box Optimization," in Proceedings of Advances in Cryptology - ASIACRYPT 2001, 2001, pp. 171–184.

[7] S. Mangard, M. Aigner, and S. Dominikus, "A Highly Regular and Scalable AES Hardware Architecture," IEEE Transactions on Computers, vol. 52, no. 4, pp. 483–491, April 2003.

[8] T. Sodon O. J. Hernandez and M. Adel, "Low-Cost Advanced Encryption Standard (AES) VLSI Architecture: A Minimalist Bit-Serial Approach," in Proc of IEEE Southeast Conference, 2005, pp. 121–125.

GATTUPALLI.RAGHAVENDRA RAO Pursuing B.tech in St. Ann's College of engineering and technology, Chirala. His area of interest is VLSI.

GUDIPATI. LAKSHMI PRASANTI Pursuing B.Tech in St. Ann's College of engineering and technology, Chirala. Her area of interest is VLSI.

MADUGULA. SNEHA LATHA Pursuing B.Tech in St. Ann's College of engineering and technology, Chirala. Her area of interest is VLSI.

MAMIDIPAKA.KAMAKSHI Pursuing B.Tech in St. Ann's College of engineering and technology, Chirala. Her area of interest is VLSI.

MOGILI. RAM SAI PRADEEP Pursuing B.tech in St. Ann's College of engineering and technology, Chirala. His area of interest is VLSI.

PUSHADAPU. PRATYUSHA, she received her B.Tech degree in Electronics and Communication Engineering in 2008 from the JNTU Hyderabad and M. Tech degree in VLSI system Design from JNTUH in 2012. At present, she is working as Assistant Professor at SACET, Chirala. Her areas of interest include VLSI, Antennas.