International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 17
July 2018

HIGH SPEED AES S-BOX/INV S-BOX DESIGN WITH S.R AND M.C TECHNIQUE

[1]KODAVALI BHARGAV KUMAR, [2] K.RADHA[Ph.D]
[1]M.Tech student, Dept of ECE, Sir.C.R.Reddy College of Engineering, Vatluru, A.P
[2]Assistant professor, Dept of ECE, Sir.C.R.Reddy College of Engineering, Vatluru, A.P

ABSTRACT: In this paper we discuss about the cryptographic performance of Rijndael Algorithm. This algorithm is evaluated from the terms of diffusion, confusion, and space-time complexity of them. The diffusion and confusion of them are quantitatively measured by using the avalanche effect and runs test. The time performance metrics are encryption and decryption speeds while space performance metric is memory utilization. The experimental results show that Rijndael Algorithm have good avalanche properties for the plaintext and key. The cipher texts of Rijndael algorithm have good randomness and unpredictability from the results. The encryption and decryption speed of Rijndael are asymmetric although Rijndael algorithm is a symmetric block cipher. Rijndael algorithm requires less number of CPU and memory resources. Rijndael algorithm is beneficial where memory resource is key concern. At last it gives efficient results compared to existed system.

KEY WORDS: Rijndael algorithm, avalanche effect, resource utilization, AES

I.INTRODUCTION

Cryptography is the study of Mathematical techniques for secured communication in the presence of adversaries and also it deals with the aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication. With some wonderful features, such as fast encryption speed, good safety and easy implementation, the block ciphers such as Rijndael algorithms have received increasing attention recently. Since the communication theory of secrecy systems was published.

Confusion and diffusion have been two essential properties of the operation of a secure cipher. They can be quantitatively evaluated by using the avalanche effect and the distribution of cipher text substring. H. Feistel firstly introduced the avalanche effect to cryptography. R. Forré proposed the extended definition and the corresponding spectral characterization. J.C. H. Castro et al. used the strict avalanche criterion to measure the strengths. The avalanche effects in cryptography are divided into two types, i.e.,Plaintext avalanche and key avalanche. The below figure (1) shows the representation of encryption and decryption system.

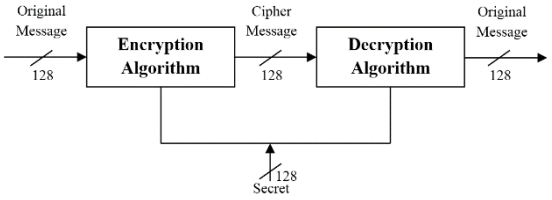

FIG. 1. REPRESENTATION OF ENCRYPTION AND DECRYPTION

The statistical performances of Rijndael algorithm have been drawn so much attention since they were Proposed. H. K. Verma compared the performance of RC6, Twofish and Rijndael block cipher algorithms for various digital media on the basis of execution time and resource utilization. IN our days, the need for secure transport protocols seems to be one

of the most important issues in the communication standards. Of course, many encryption algorithms support the defence of private communications. However, the implementation of these algorithms is a complicated and difficult process and sometimes results in intolerant performance and allocated resources inhardware terms. The explanation for this fact is because these encryption algorithms were designed some years ago and for general cryptography reasons. In recent years, new flexible algorithms specially designed for the new protocols and applications have been introduced to face the increasing demand for cryptography.

The main purpose of these works was the evaluation of the AES finalist algorithms in terms of hardware implementation performance. In order to achieve this, allthe authors used general purpose architectures and not specialized designs for each algorithm implementation. This is a fair methodology for comparison of different algorithms. On the other hand, this way is not well-suited to the implementation of each algorithm separately. In addition, in two of these works, only the encryption mode of operation was implemented and not the decryption. References do not support the on chip- generation of the necessary for the algorithm encryption/ decryption keys. In other words, the proposed designs do not support the completed operation of the algorithms and perform inefficiently in terms of both the encryption and decryption mode of data transformation.

II. BACKGROUND

As cryptography plays a crucial role in the security of data transmission, AES based on Rijndael algorithm was selected as a data encryption standard by the National Institute of Standards and Technology (NIST) in 1997 based on the primary criteria of security, performance, efficiency in software and hardware implementation, and flexibility. AES is one of the most common symmetric encryption algorithms and is widely adopted for a variety of encryption needs, such as wireless networks and secure transactions via the Internet.

AES can be implemented on a wide range of platforms under different constraints. In portable applications computing resources are usually limited and dedicated hardware implementation of the security process is essential. Implementation using Field Programmable Gate Array (FPGA) is not suitable for such applications mainly due to size and power constraints. FPGA being a general purpose logic array usually there is some residual (unused) logic and I/O blocks, and consequently, highly compact implementation is difficult to achieve. In addition, FPGA implementation is prone to switching noise induced power analysis attack.

A compact small foot- print full-custom chip is more suitable in such a case. In additionsuch a dedicated hardwired AES implementation can provide higher data rate for fast handling of ciphered network data packets in applications such as routers compared to software packages. The hardwired implementation is also physically secure since tempering by an attacker is more difficult. The overall efficiency of AES hardware implementation in terms of size, speed, security and power dissipation depends largely on the AES architecture. For high throughput, loop-unrolled pipelined structure is used, but on the other hand, to save power and area, iterative single round with resource sharing is implemented.

The S-Box is at the core of any AES implementation and is considered a full

complexity design consuming the major portion of the power and energy budget of the AES hardware. This paper is focused on area-efficient low-voltage and low-power CMOS implementation of the S-Box/Inv S-Box. There are various reported techniques to implement the S-Box to satisfy the varying criteria such as power, speed and delay for different applications. Among them there are two main streams: (a) Implementation using look up tables (LUTs) which stores all predefined 256 8-bit values of S-Box in a Read-Only-Memory (ROM). The advantage of using LUT is that it offers a shorter critical path. However, it has a drawback of the unbreakable delay path in pipelined designs, and hence it is not suitable for high speed applications. This delay prohibits each round unit from being divided into more than two sub-stages to achieve any further increase in processing speed. It also requires a large area to implement both AES encryption and decryption as a different table is used in each case.

III. EXISTED SYSTEM

The below figure (2) shows the block formation of existed system. The existed systemoperates on individual bytes by using a sub- situation table. There are various reported techniques to implement the S-Box to satisfy the varying criteria such as power, speed and delay for different applications. To designsub-situation tablemultiplicative inversion is used.

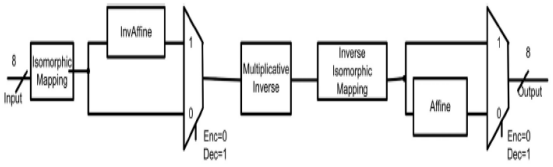

FIG. 2. EXISTED SYSTEM

It is implemented using XOR circuits, multiplexers and AND gates. The Optimization of the low voltage and low power composite field S-Box implementation has been further enhanced. In addition, it employs a low-power design methodology such as minimizing the circuit size by efficient logic implementation as well as reduced supply voltage using an advanced CMOS technology.

Thisarchitectureperforms both SubBytes and Inv-SubBytes simply by switching combinatorial logic blocks using multiplexers.The composite field inversion is used to create compact AES implementations. This approach has been chosen to achieve small area design.An affine transformation is carried out to create the cipher data. This can be represented by the elementary transformations. The Inverse Sub-Bytes involves first an isomorphic transformation followed by an inverse affine transformation. Then inversion in composite field is carried out followed by inverse isomorphic mapping. This can be represented by the elementary transformations. But this system does not gives effective results in terms of power, area, and delay. So a new system is proposed as discussed in below section.

IV. PROPOSED SYSTEM

The below figure (3) shows the architecture of RIJNDAEL. Rijndael algorithm is an iterated block cipher supportinga variable data block and a variable key length of 128, 192 or256 bits.The initial key is expanded to generate the round keys, eachof size equal to block length.Each standard round includes four fundamental algebraicfunction transformations on arrays of bytes. The final round of the algorithm is similar tothe standard round, except that it does not have MixColumnoperation. Decryption is performed by the application of theinverse

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 17
July 2018

transformations of the round functions. The sequenceof operations for the standard round function differs fromencryption. The computational performance differs betweenencryption and decryption because the inverse transformationsin the round function is more complex than the correspondingtransformation for encryption. The order of operation of the Rijndael architecture is discussed below.

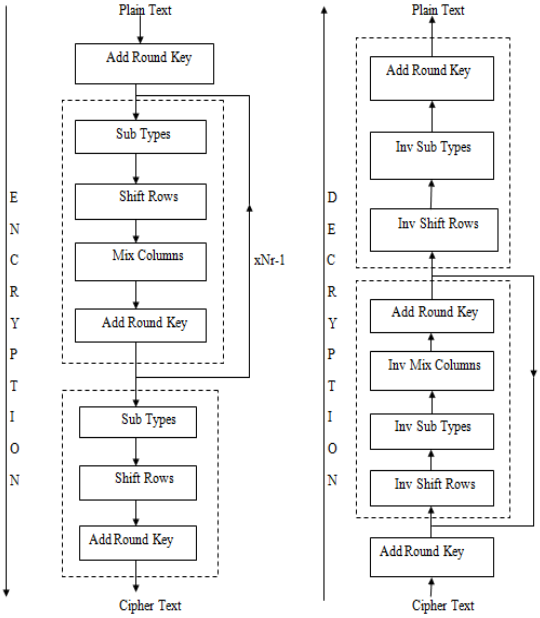

FIG. 3. PROPOSED SYSTEM

a) **Architecture of the Data Unit:** The data unit consists of: the initial round of key addition,*Nr*1 standard rounds, and a final round. The architecturefor a standard round composed of four basic blocks is shownin Figure (3). For each block, both the transformation and theinverse transformation needed for encryption and decryption,respectively are performed using the same hardware resources.This implementation generates one set of subkey and reusesit for calculating all other subkeys in real-time.

b) **Shift Row:** In this transformation the rows of the blockstate are shifted over different offsets. The amount of shiftsis determined by the block length. The proposed architectureimplements the shift row operation using combinational logicconsidering the offset by which a row should be shifted.

c) **Mix Column:** In this transformation each column of theblock state is considered as a polynomial over *GF*(28). Itis multiplied with a constant polynomial $C(x)$ or $D(x)$ overa finite field in encryption or decryption, respectively. Inhardware, the multiplication by the corresponding polynomialis done by XOR operations and multiplication of a block byX. This is implemented using a multiplexer, the control beingthe MSB is 1 or 0.

d) **Add Round Key:** In this transformation the round key obtained from the key scheduler is XORed with the block state obtained from the *Mix Column* transformation or Shift Rowtransformation based on the type of round being implemented. In the standard round, the round key is XORed with the output obtained from the *Mix Column* transformation. In the final round the round key is XORed with the output obtained from the Shift Row transformation. In the initial round, bitwise XOR operation is performed between the initial round key and the initial state block.

From this we can observe that the proposed system gives better results in terms of power, area and delay. The proposed architecture is optimized for high throughputin terms of the encryption and decryption data rates usingpipelining. At last in the proposed architecture both theencryption and decryption modes use common hardware resources,thus making the design area efficient.

V. RESULTS

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 17
July 2018

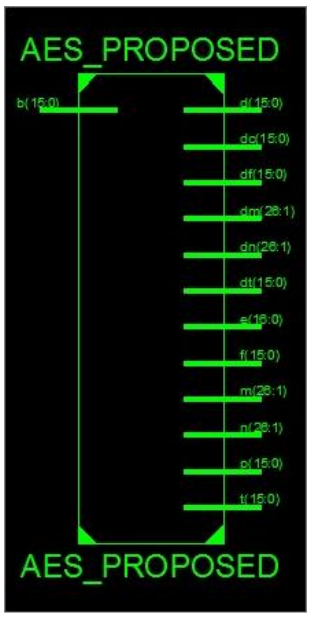

FIG. 4. RTL SCHEMATIC

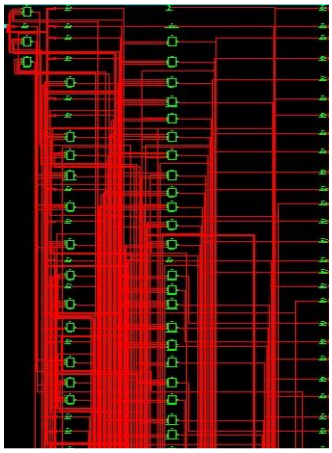

FIG. 5. TECHNOLOGY

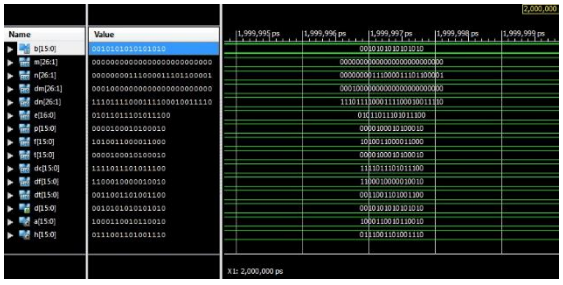

FIG. 6. OUTPUT

VI. CONCLUSION

The cryptographic performance of Rijndael hasbeen analysed with a set of input files. The experimental results conclude that Rijndael have good plaintext avalanche and key avalanche properties. The encryption or decryption speed of Rijndael algorithm is faster than that of other algorithms. Result also concludes that the encryption and decryption speed of Rijndael are asymmetric. With the increase ofdata to be encrypted or decrypted, the encryption or decryption speed ofRijndael algorithm shows a slight down trend. From the user point of view,Rijndael algorithm is faster and simpler.

VII. REFERENCES

[1] J. S. Park, K. S. Bae, C. Y. Choi, D. H. Choi, and J. C. Ha, "A fault resistant implementation of AES using differential bytes between input and output," Journal of Supercomputing, vol. 67, no. 3, pp. 615-634, Mar. 2014.

[2] S. S. Liu, Z. Gong and L. B. Wang, " Cryptanalysis of Reduced-Round DASH," Journal of Computer Science and Technology, vol.28, no.1, pp. 159-164, Jan. 2013.

[3] C. E. Shannon, "Communication theory of secrecy systems," Bell System Technical Journal, vol. 28, no. 4, pp. 656–715, Oct.1949.

[4] I. Muniraj, C. Guo, R. Malallah, et al, " Choice of optical system is critical for the security of double random phase encryption systems," Optical Engineering, vol. 56, no. 6, pp. 1-14(063103), Jun. 2017.

[5] H. Feistel, "Cryptography and Computer Privacy," Scientific American, vol. 228, no. 5, pp. 15-23, May 1973.

[6] R. Forré, "The strict avalanche criterion: spectral properties of Boolean functions and an extended definition," Proceeding CRYPTO '88 Proceedings on Advances in cryptology, Lecture Notes in Computer Science, Springer-Verlag, Berlin, vol. 403, pp. 450-468, 1990.

[7] J. C. H. Castro, J. M. Sierra, A. Seznec, A. Izquierdo, A. Ribagorda, "The strict

avalanche criterion randomness test," Mathematics and Computers in Simulation, vol. 68, no.1, pp. 1-7, Feb. 2005.
[8] L. Q. Min, and G. R. Chen, "A novel stream encryption scheme with avalanche effect," The European Physical Journal B, vol.86, no. 459, pp. 1-13, Nov. 2013.
[9] A. Dandalis, V. K. Prasanna, J. D. P. Rolim, "A comparative study of performance of AES final candidates using FPGAs," Lecture Notes in Computer Science, vol.1965, pp. 125-140, 2000.
[10] A. J. Elbert, E. Yip, B. Chetwynd, and C. Paar: "An FPGA implementation and performance evaluation of the AES block cipher candidate algorithm finalists", IEEE Transactions on Very Large Scale Integration Systems, vol. 9, no. 4, pp. 545-557, Aug. 2001.

KODAVALI BHARGAV KUMAR received the B.Tech. (JTNUK) degree from Ramachandra College of engineering, vatluru. Present pursuing M.TECH from SIR C.R. Reddy College of engineering,vatluru. It is affiliated to Andhra University. His M.Tech specialization is VLSI.

K.RADHA received the M.Tech. (JTNUH) degree from Gudlavalleru Engineering College, Gudlavalleru. She had completed her AMIE in Electronics and Communication Engineering. She is having 10 years of experience in teaching, presently working as an Assistant Professor in the Department of Electronics & Communication Engineering at Sir.C.R.Reddy College of Engineering, vatluru. Her current research interests include Low power VLSI Design, Design of digital circuits.