International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 06
May 2017

An Efficient A.E.S Technique for High Security Applications

B. VENKATESWARA RAO
M.Tech – D.E.C.S
Dept. of E. C.E
VIKAS GROUP OF INSTITUTIONS
NUNNA, KRISHNA DISTRICT

Y. UMA MAHESWARI, M.Tech
Associate professor
Dept. of E. C.E
VIKAS GROUP OF INSTITUTIONS
NUNNA, KRISHNA DISTRICT

ABSTRACT: In this paper, a novel architecture of A.E.S algorithm using high security technique for the VLSI implementation for AES algorithm. The pre-defined keys are required for each input for both encryption and decryption of the AES algorithm that are generated in real-time by the key-scheduler module by expanding the initial secret key and thus used for reducing the amount of storage for buffering. S-boxes are used for the implementation of the S.R, M.C and inverses S.R & M.C shared between encryption and decryption. The round keys needed for each round of the implementation are generated in real-time. The forward and reverse key scheduling is implemented on the same device, thus allowing efficient area minimization. The pipelining is used after each standard round makes fast of operation to enhance the throughput and shift row mix column technique gives high security.

Keyterms: A.E.S, A.D.S, S.R, M.C, S- BOX.

INTRODUCTION

Several techniques such as cryptography, watermarking and scrambling have been developed to keep data secure, private, and copyright protected [1]. Cryptography is an essential tool underlying virtually all networking and computer protection traditionally used for military. However, the need for secure transactions in e-commerce, private networks, and secure message has moved encryption into the commercial way.

Communication / transfer of data in the present days invariably necessitate the use of encryption. It is also used in Military and Government's communication, Encryption is also used for protecting many kinds of civilian services such as Internet e-commerce, Mobile networks, copy protection (especially protection against Software piracy), and many more.

Data encryption is achieved by a systematic algorithm called encryption. An encryption algorithm provides Confidentiality and Authentication. Confidentiality is the requirement that information is kept secret from people who are not permit to access it. Authentication is the process that the message indeed originates from the sender.

Integrity is also used to require that information is unaltered and that information "is modified only by those users who have the right to do so." Nonrepudiation means that the sender or receiver of a message cannot permit to having sent or received the message.

Advanced encryption standard (AES) was issued at Federal Information Processing Standards (FIPS) by National Institute of Standards and Technology (NIST) as a successor to data encryption standard (DES) algorithms. In recent literature, a number of various architectures for the VLSI implementation of AES Rijndael algorithm are reported [6], [7], [8]. It can be observed that some of these architectures are low performance and some provide high area. Further, many of the architectures are not area efficient but it having higher cost when implemented in silicon.

In this paper, a novel architecture of A.E.S algorithm using high security technique that is suitable for optimized for high throughput in terms of the encryption and decryption data rates using pipelining.

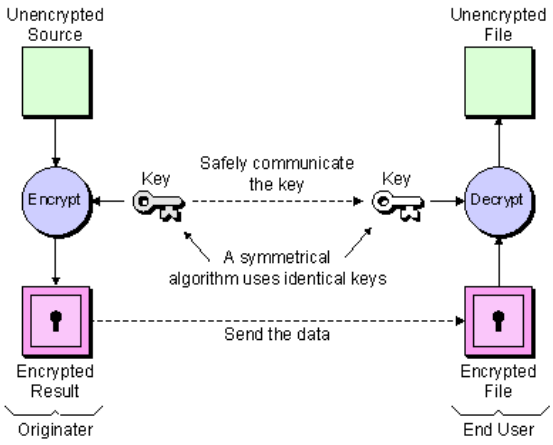

FIG. 1 Algorithm of Encryption and Decryption

We used the tower field approach for the S-box and we adapted the number of shares for each function in the S-box computation to minimize the overall gate count of the S-box. We used only two shares for most of the linear operations and hence had two sets of registers for state update and key schedule. All functions were uniformly shared and the number of shares went up to five in the S-box. We used remasking to satisfy the uniformity in the whole circuit when the uniformly shared functions are combined. Our practical security evaluation confirmed the expected first-order DPA resistance and identified the linear part in two shares as the most vulnerable part of the implementation.

The nonlinearity of the cryptographic algorithms is higher and the confusion of the cipher algorithms is stronger. In fact, the bigger S box , which is used in the hardware structure the calculation, check list and storage are also required more time and space. In this case the algorithm becomes very low efficient. So how to choose a good S box we need to consider the security of algorithm and the work efficiency of implementation. The traditional method generates the S box, which has a good index of cryptography. However it is different to use pure logic hardware implementation consuming a large number of logic units.

The existing system gives the high speed realize about AES and FPGA but it having less security compared with proposed system. To provide high security we are proposing a new algorithm.

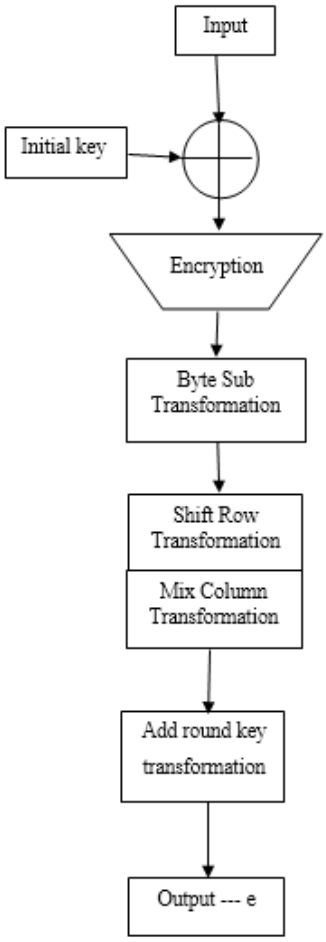

Fig.2 A.E.S Block Diagram

The fig: 2 shows the A.E.S. block diagram with high security implementation. The initial stage having input and initial key to under goes encryption with changing of binary bits into a matrix representation. This conversion of binary data to a matrix is totally carried out by byte sub transformation. Now the total matrix consisting of roce and columns by using these us implementation the security by the technique.

Shift Row transformation is one of the technique for security i.e. the total roce is matrix is shifted to another roce and with vice and versa. The second technique is mix column transformation it gives two columns into a single column to reduce the size. In another way we can make as comparison of two columns into a single column.

The add round key transformation is used rounding the nearest value of matrix. This represents the rounded output taken as 'e' for A.E.S. block. The total A.E.S. block is used in the transmitter side.The output of A.E.S. block given to input to A.D.S. block.

Similarly A.D.S. block consisting of sub blocks as A.E.S. with small inversion. So the input 'e' taken as input for decryption the input 'e' and final key goes under decryption and the output of the decryption given to input as for inverse byte sub transformation. The inverse byte sub transformation divide the matrix representation into binary representation.

The inverse shift row transformation and inverse mix column transformation operate as inversion of shift row transformation and mix column transformation. The inverse add round key is used to take the value accurate and give an output 'e' for A.D.S. block.

If this technique is used to protect cascaded functions, then extra measures like the binary data discussed in the previous section need to be taken, such that the input for the following nonlinear operation is again a uniform masking. A similar situation occurs when the technique is used to protect several functional blocks acting in parallel on (partially) the same inputs. This occurs for example in implementations of the AES S-box using the tower field approach. If no special care is taken, then "local uniformity" of the distributions of the outputs of the individual blocks will not lead to "global uniformity" for the joint distributions of the outputs of all blocks.

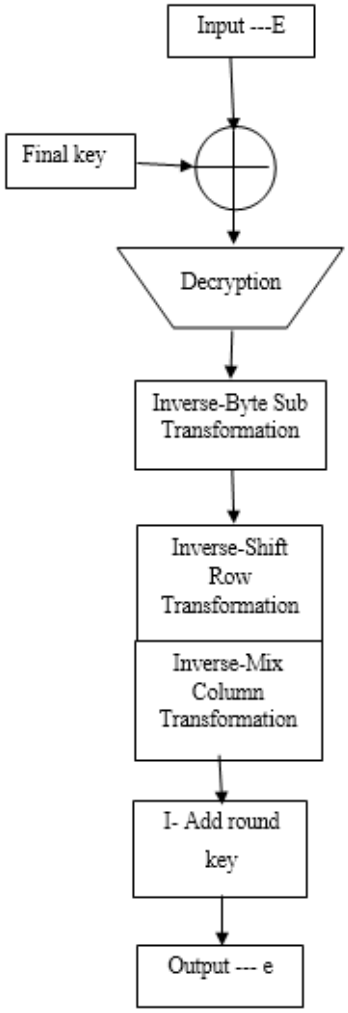

FIG. 3 A.D.S Block Diagram

The R.T.L schematic diagram shows in below Figure 4

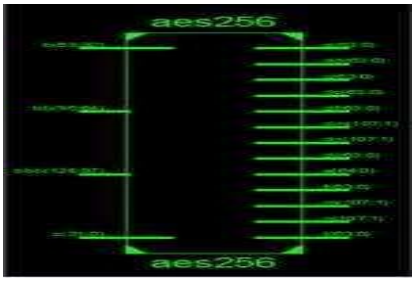

FIG. 4 R.T.L Schematic

The technology schematic shows in figure 5.

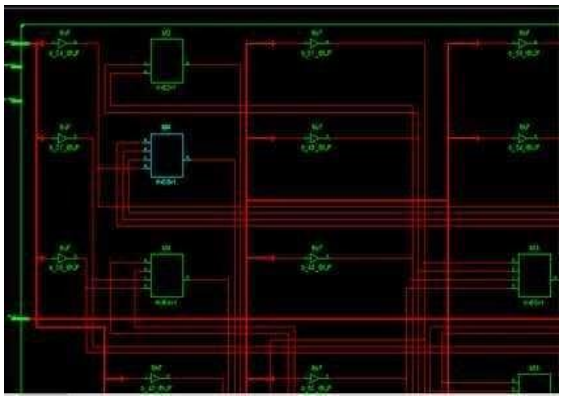

FIG. 5 Technology schematic

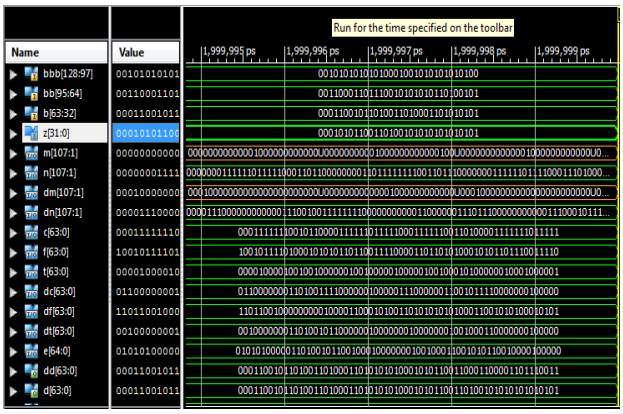

FIG. 6 Output Waveform

It is evident that the Rijndael's S-Boxes are the dominant element of the round function in terms of required logic resources. Each Rijndael round requires sixteen copies of the S-Boxes, each of which is an 8-bit look-up-table, requiring more hardware resources. However, the remaining components of the Rijndael round function – byte swapping were found to be simpler in structure, resulting in these elements of the round function requiring fewer hardware resources. Additionally, it was found that the synthesis tools could not minimize the overall size of a Rijndael round sufficiently to allow for a fully unrolled or fully pipelined implementation.

As compared to a one-stage implementation with no sub pipelining, the addition of a sub-pipeline stage afforded the synthesis tool greater flexibility in its optimizations, resulting in a more area efficient implementation. The 2-stage loop unrolling was found to yield the highest throughput when operating in Feedback (FB) mode.

The output wave forms is shown in figure 6. In this figure we shows the encryption and decryption with error detection and correction. The errors in the decryption is overcome by using this architecture.

The no. of slices , L.U.T's and IOB'S shows in below tabular form 1

Logic Utilization	Used	Available	Utilization
Number of Slices	306	960	31%
Number of 4 input LUTs	572	1920	29%
Number of bonded IOBs	1063	66	1610%

Table 1

CONCLUSION

We have presented a VLSI architecture for the Rijndael AES algorithm that performs both the encryption and decryption. S-boxes are used for the implementation of the S.R, M.C and inverses S.R & M.C shared between encryption and decryption. The round keys needed for each round of the implementation are generated in real-time. The forward and reverse key scheduling is implemented on the same device, thus allowing efficient area minimization. The implementation of the key unit in the proposed architecture, can be scaled for the keys.

REFERENCES

[1] K. Fu and J. Blum, "Controlling for cybersecurity risks of medical device software," *Commun. ACM*, vol. 56, no. 10, pp. 35–37, Oct. 2013.

[2] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 30–39, Jan./Mar. 2008.

[3] M. Rostami, W. Burleson, A. Jules, and F. Koushanfar, "Balancing security

and utility in medical devices?" in *Proc. 50th ACM/EDAC/IEEE Int. Conf. Design Autom.*, May/Jun. 2013, pp. 1–6.
[4] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," *Proc. IEEE*, vol. 102, no. 8, pp. 1174–1188, Aug. 2014.
[5] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, Jan./Feb. 2010.
[6] M. Mozaffari-Kermani, M. Zhang, A. Raghunathan, and N. K. Jha, "Emerging frontiers in embedded security," in *Proc. 26th Int. Conf. VLSI Design*, Jan. 2013, pp. 203–208.
[7] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, Sep. 2011.
[8] T. H.-J. Kim, L. Bauer, J. Newsome, A. Perrig, and J. Walker, "Challenges in access right assignment for secure home networks," in *Proc. USENIX Conf. Hot Topics Secur.*, 2010, pp. 1–6.
[9] M. Mozaffari-Kermani and A. Reyhani-Masoleh,"Concurrent structureindependent
fault detection schemes for the Advanced Encryption Standard," *IEEE Trans. Comput.*, vol. 59, no. 5, pp. 608–622, May 2010.
[10] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "A low-power highperformance concurrent fault detection approach for the composite field S-box and inverse S-box," *IEEE Trans. Comput.*, vol. 60, no. 9, pp. 1327–1340, Sep. 2011.

B.Venkateswara Rao studied his B.Tech in lakireddy Balireddy College of engineering, Mylavaram. His area of interest is V.L.S.I.

Y. UMA MAHESWARI studied her B.Tech in Srinivasa Engg College and M.Tech in Nalanda Institute of Engg And Technology. She has 10 years of teaching experience and present working as associate professor in Vikas Group of Institutions, Nunna.