Error Detection And Correction Architecture Of A.E.S Algorithm Using High Security Technique

1.PINGILY JYOTHIRMAYEE,2. Mrs.S.SRI BINDU,3. Mr.P.PAVAN KUMAR

1. M.Tech Vlsi, E.C.E Dept., CMR Institute Of Technology,Kandlakoya(V), Medchal(M), Hyderabad.
2. Assistant Professor, E.C.E Dept, CMR Institute Of Technology, Kandlakoya(V), Medchal(M), Hyderabad.
3. Assistant Professor, E.C.E Dept, CMR Institute Of Technology, Kandlakoya(V), Medchal(M), Hyderabad.

ABSTRACT:*In this paper, a novel architecture of A.E.S algorithm using high security techniquefor 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 thusused for reducing the amount of storage for buffering. 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.*
KeyWords: A.E.S, Cryptography, Standarad Round.

I.INTRODUCTION

Several techniquessuch 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 movedencryption into the commercial way.

Communication / transfer of data in the present days invariably necessitatethe use of encryption. It is also usedin 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 systematicalgorithm 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 isalso 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.

II.ADVANCED ENCRYPTION STANDARD

Advanced encryption standard (AES) was issued at FederalInformation Processing Standards (FIPS) by National Instituteof Standards and Technology (NIST) as a successor to dataencryption standard (DES) algorithms. In recent literature,a number ofvarious architectures for the VLSI implementation ofAES Rijndael algorithm are reported[6], [7], [8].It can be observed that some of these architectures are lowperformance and some provide high area. Further, manyof the architectures are not area efficient but it havinghigher cost when implemented in silicon.

In this paper, anarchitecture of A.E.S algorithm using high security techniquethat is suitable for optimized for high throughputin terms of the encryption and decryption data rates usingpipelining.

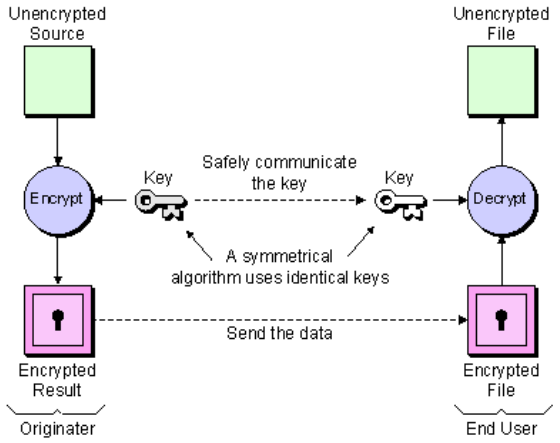

FIG. 1Algorithm of Encryption and Decryption

We used the tower field approach for the S-box and we adapted the number of shares for eachfunction in the S-box computation to minimize the overallgate count of the S-box. We used only two shares for most ofthe linear operations and hence had two sets of registers forstate update and key schedule. All functions were uniformlyshared and the number of shares went up to five in the S-box. We used re-masking to satisfy the uniformity in the whole circuitwhen the uniformly shared functions are combined. Ourpractical security evaluation confirmed the expected first-orderDPA resistance and identified the linear part in two shares asthe most vulnerable part of the implementation.

In this extended version, we investigate the uniformity problemand the need for re-masking in more detail. We prove thatunder certain circumstances; it is enough to re-mask only afraction of the shares. Moreover, we argue that if there isenough re-masking, we do not need to share functions uniformly.This observation helps us to further reduce the areaand randomness requirements. We provide two new implementations.

The first one is similar to the one in, butit uses at least three shares in all the operations, includingthe linear ones. We use it to investigate the increase in security when moving from at least two to at least three shares,and to quantify the associated cost. The second implementationis based on the one in but modified according toour findings regarding uniformity and re-masking. It requires only about 8 BITSwith the library that we use and 32 bitsof additional randomness per S-box calculation. Our threeimplementations need the same number of clock cycles tocomplete the calculation, and allow us therefore to focuson some trade-offs between area and additional randomness.

III.SHIFT ROW MIX COLUMN TECHNIQUE

We use a serial implementation for round operations and key schedule which requires only one S-box instance and loads the plaintext and key byte-wisein row-wise order. We also use one Mix Columns instance that operates on the whole column and provides an output.

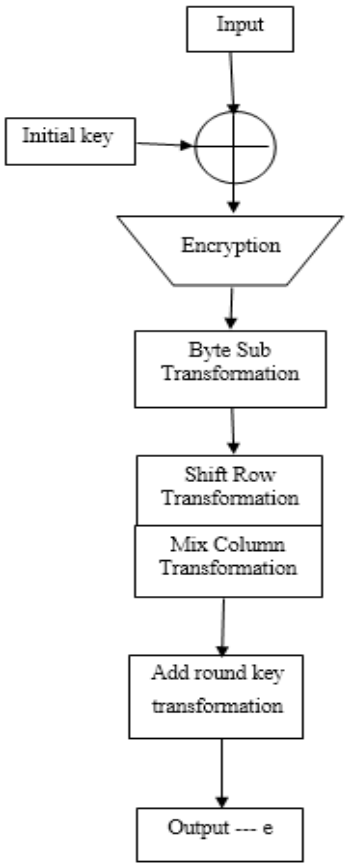

Fig.2 A.E.S Block Diagram

The data unit consists of: the initial round of key addition and a final round. The architectureof a standard round composed of 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 reusesfor calculating all other subkeys in real-time.

1. **Byte Sub:**In this architecture each block is replaced by the substitution in S-Box table consisting of the byte of the block.
2. **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.
3. **Mix Column:** The mix column in encryption and decryption done the columns to be mix and inverse of column mixing respectively.

In the Advance decryption process is shown in figure 3 and the total operations in the A.E.S is inverse the operations like inverse byte sub transformation, inverse shift row, inverse mix column. The output of A.E.S is "E" it is given to input for A.D.S and the output of A.D.S is equal to the input of A.E.S.

If this technique is used to protect cascaded functions,then extra measures like thebinary data discussed in the previoussection need to be taken, such that the input for the following onlinear operation is again a uniform masking. A similarsituation occurs when the technique is used to protect functional blocks acting in parallel on (partially) the sameinputs. This occurs for example in implementations of theAES S-box using the tower field approach. If no special careis 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.

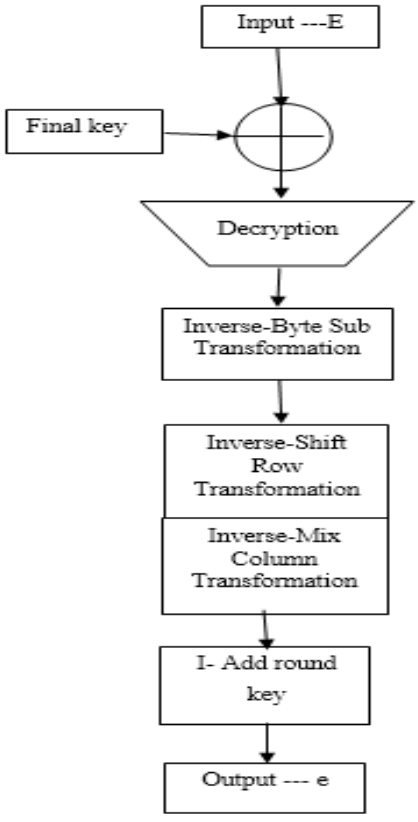

FIG. 3 A.D.S Block Diagram

IV.SIMULATION RESULTS

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

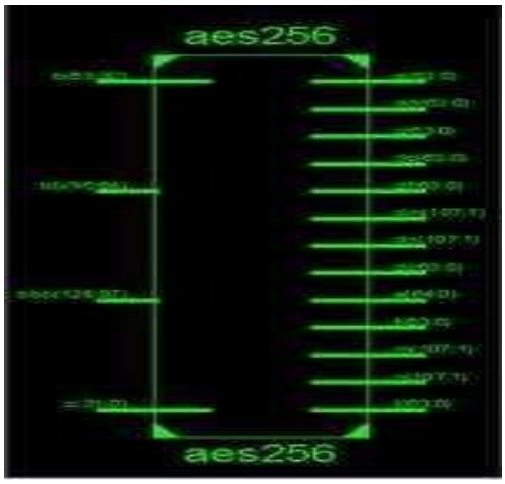

FIG. 4 R.T.L Schematic

The technology schematic shows in figure 5.

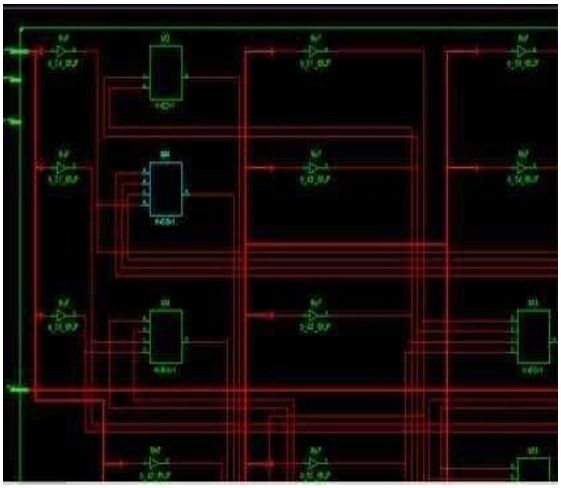

FIG. 5 Technology schematic

It is evident that the Rijndael's S-Boxes are the dominantelement of the round function in terms of required logic. Each Rijndael round requires sixteen copies ofthe S-Boxes, each of which is an 8-bit look-up-table,requiring less hardware resources. However, the remainingcomponents of the Rijndael round function – byte swappingwere found to be simpler structure, resulting inthese elements of the round function requiring fewer hardwareresources. It was found that the synthesis toolsbe minimize the overall size of a Rijndael roundto allow for a fully unrolled or fully pipelined implementation.

As compared to a one-stage with no sub pipelining,the addition of a sub-pipeline stagesynthesis tool greater flexibility optimizations, resultingin a more area efficient implementation. The 2-stage loopunrolling was found to yield the highest throughput whenoperating 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.

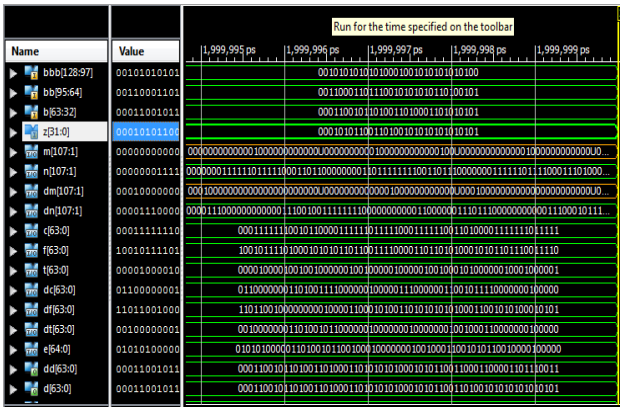

FIG. 6 Output Waveform

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

V.CONCLUSION

We have presented a VLSI architecture for the Rijndael AESalgorithm that performs both the encryption and decryption.The S-boxes are used for the implementation of the S.R, M.C and inverses S.R & M.C shared between encryption and decryption. Theround keys needed for each round of the implementation aregenerated in real-time. The initial and final key schedulingis implemented on the same device, thus allowing efficientarea minimization. The implementation of the key unit in the proposed architecture, can be scaledfor the keys of length 256 bits. The total delay to implement this architecture is 20.742 ns and memory used is 210912kb.

REFERENCES

[1] K. Fu and J. Blum, "Controlling for cybersecurity risks of medicaldevice 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 PervasiveComput.*, vol. 7, no. 1, pp. 30–39, Jan./Mar. 2008.

[3] M. Rostami, W. Burleson, A. Jules, and F. Koushanfar, "Balancingsecurity and utility in medical devices?" in *Proc. 50th ACM/EDAC/IEEEInt. Conf. Design Autom.*, May/Jun. 2013, pp. 1–6.

[4] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medicaldevices 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 securityissues," *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. VLSIDesign*, 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 highperformanceconcurrent fault detection approach for the compositefield S-box and inverse S-box," *IEEE Trans. Comput.*, vol. 60, no. 9,pp. 1327–1340, Sep. 2011.