International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

High Performance Hardware Realization of Advanced Encryption Standard

Kamal Prakash Pandey[1], Rakesh Kumar Singh[2]

[1,2]Associate Professor, Shambhunath Institute of Engineering and Technology, Jhalwa Allahabad, Uttar Pradesh, India

Abstract: ***Advanced Encryption Standard (AES) is a cryptographic algorithm which has wide range of applications. Each application has different power, speed, and resource utilization requirement. This paper thoroughly analyses implementation strategies of Advanced Encryption Standard (AES) algorithm and proposes four different architectures for AES implementation, each of these architectures targeting different applications. Each operation in AES is mathematically analyzed and implemented separately. Based on implementation results best suited strategy of hardware implementation can be chosen for each of four architectures. For this architecture 1 has been proposed and analyzed One of the main contributions of this work is reordering and merging different operation of AES encryption so as to achieve higher speed and lesser device utilization for encryption hardware. Merging techniques have increased the hardware efficiency by 36% compared to previous implementation. This work also suggests pyramid buffer hardware implementation approach to achieve higher throughput for decryption module. This work suggests very low power solution for AES encryption by merging and rolling the encryption architecture.***

Keywords: Cryptography, AES module, Virtex 5 LX110T device, Xilinx Synthesis technology

1. Introduction

Cryptography is referred to the translation of data in to a secret code (Encryption), and secret code back to data (Decryption) for security purpose. Cryptography is used not only for military applications but also many civilian applications like E-commerce, Mobile network, Automatic Teller Machine (ATM) etc. There are two (Software and hardware approach) approaches for the implementation of cryptographic algorithms. Since latter is preferred in terms speed and reliability. This work is analyzing the hardware design strategies of Advance Encryption Standard-cryptographic algorithm .This section is meant to describe previous work in this domain, Motivation and problem definition of the efficient hardware implementation of AES.

Our work include the study of mathematical model of AES algorithm, Implementation and analysis of different implementation strategies of AES architecture and there by formulation of a novel architecture for AES for higher throughput and lesser hardware utilization targeting Field Programmable Gate Array. The existing hardware architecture of AES can be mainly classified as three groups,

1. The first one is an iterative core for AES algorithm which is meant for lesser hardware utilization. Since it use a common hardware for all ten rounds of AES algorithm output of present round is looped back as input to next round. Iterative core also demands a controller design to control looping and selection and skip of different operation which is specific for each round of AES algorithm. Iterative architecture is shown in Figure 1.1.

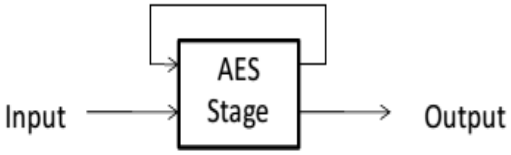

Figure 1.1: Iterative Architecture

2. Second hardware architecture is focused to get higher throughput by pipelining called fully unrolled pipelined architecture of AES. Different round have separate hardware in series with pipeline registers in between. Hence the throughput is increased but there will be hardware overhead of separate hardware for each round and that of pipeline registers. Second hardware implementation strategy is given in Figure 1.2.

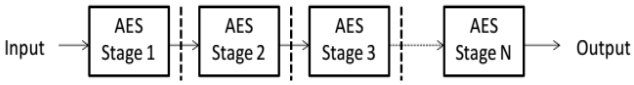

Figure 1.2: Loop unrolled architecture with pipelining

3. Third common implementation strategy is fully unrolled sub pipelined AES architecture targeting even higher throughput by sub paneling inside the hardware each operations in AES such as Substitution and Mix Column. Hardware utilization is highest for this type of architecture. Third architecture is given in Figure 1.3.

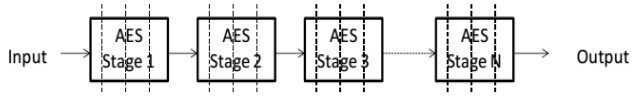

Figure 1.3: Loop unrolled sub pipeline architecture

2. AES Encryption

Each encryption round has 4 main steps, Shift Rows, Byte Substitution using the Substitution Box (S-BOX), Mix Columns, and Add Round Key. Encryption takes data to be encrypted and key used for encryption. First step is addition of input data and initial round key, after this key addition step, encryption follows three iterative steps respectively, Shift Rows, Byte Substitution using the Substitution Box (S-BOX), Mix Columns and Round Key Addition. Iteration performed "N-1" times if total number of rounds are „N".For the last time Shift Rows, Byte Substitution using the Substitution Box (S-BOX) is performed and Mix Column operation is skipped. In the case of AES 128 bit tenth round

operation will skip the mix column operation. AES Algorithm starts by a key addition operation and then follows the four major operations till the last round. Figure 2.1 gives the flow of encryption algorithm.

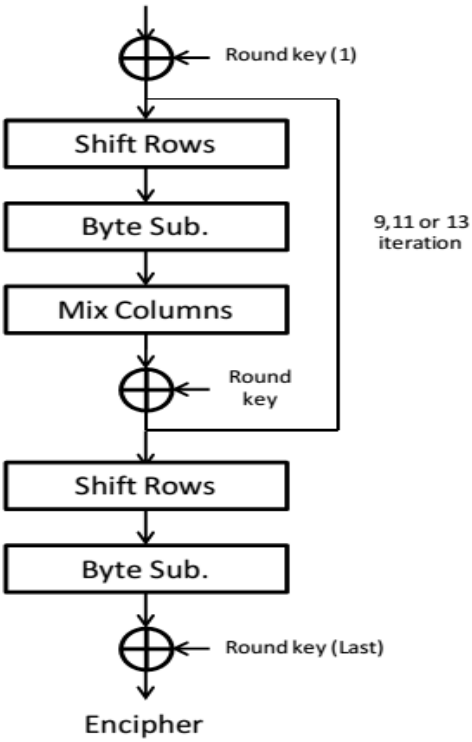

Figure 2.1: Encryption Algorithm

3. Results and Discussion

Architecture 1 consists of key generation module and encryption unit with common control unit. It is a looping AES architecture. The design uses only LUTs, ROMs for all the operations of AES encryption and decryption. This approach reduces device utilization and significantly improves the speed compared to other implementation. Delay report of AES encryption with common 4-bit counter controller is given in table 1

Table 1: Delay Report of Architecture 1

Total delay	3.420ns (1.115ns logic, 2.305ns route)
Frequency	292.403MHz

In this proposed design, the encryption unit takes 10 clock cycles to complete the operation. The maximum path delay of the design is 3.420ns resulting in a maximum frequency of operation as 292.403MHz. The throughput of the proposed encryption module is 3.74Gbps.

$$Throughput = \frac{Number\ of\ bits \times clock\ freaquency}{number\ of\ output\ per\ cycle}$$

Hardware utilization report of AES encryption with common 4bit counter controller is given in table 2

Table 2: Hardware Utilization of architecture 1

Slices	1106
register	128
Utilization	LUT2: 242 LUT3: 128 LUT5 : 96 LUT6 : 640 MUXF7: 256 MUXF8: 128
Input output buffers	IBUF : 260 OBUF : 128

The proposed architecture achieves a throughput of 3.74 Gbps and thereby utilizing only 1% of slices in the targeted FPGA. Since the speed is higher than the already reported systems of same kind, the proposed design serves as the best high speed encryption algorithm and is thus suitable for various applications. Moreover with less area utilization, the proposed design can be embedded with other larger designs as well. Figure 3.1 represents the simulation result of Encryption unit of architecture 1.

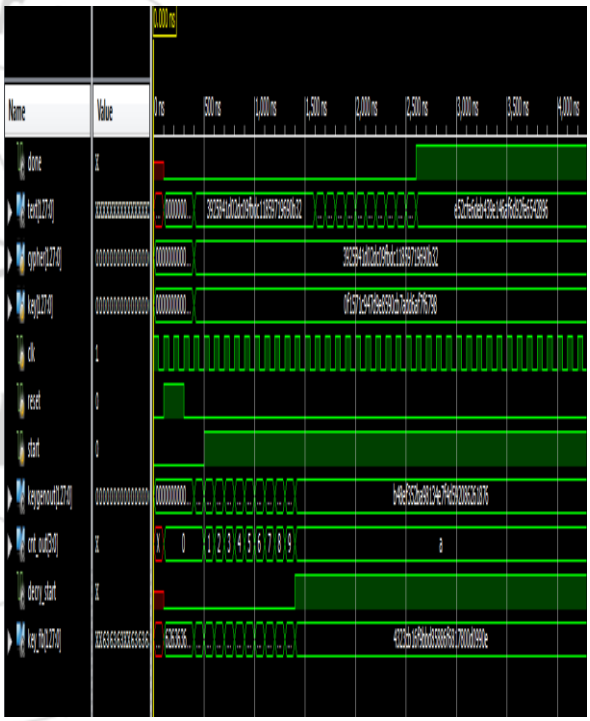

Figure 3.1: Simulation result of Encryption unit of architecture 1

Figure 3.2 represents simulation result of AES decryption unit of architecture 1.

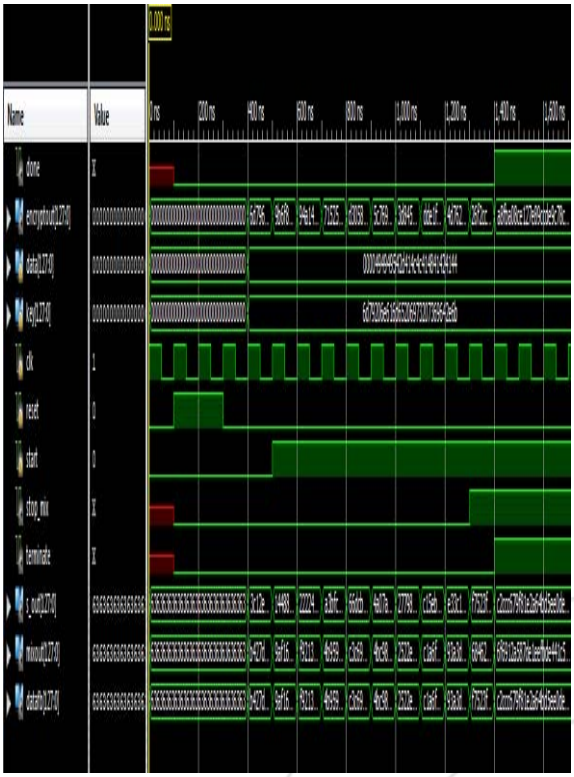

Figure 3.2: Simulation result of AES decryption unit of architecture 1

Key generation module is very important part of AES architecture 1. It limits the speed of AES encryption and decryption. Delay report of AES key generation with common 4 bit counter controller is given below table 5.7

Table 3: Delay Report of Architecture 1-Decryption

Total delay	2.255ns (0.943ns logic, 1.312ns route)
Frequency	443.465MHz

As long as delay of key generation is lesser than delay of encryption and decryption then delay of the whole unit depend on delay of encryption and decryption. In architecture 1 controller is common to key generation and encryption/Decryption, Hence there will be a slight hardware overhead on key generation unit. All the control signal is output from key generation unit hence have more output ports. Hardware utilization report of AES key generation with common 4 bit counter controller is given below table 4

Table 4: Hardware utilization report of AES key generation

Slices	347
register	132
Utilization	LUT2: 57 LUT3: 7 LUT4: 9 LUT5 : 6 LUT6 : 640 MUXF7: 64 MUXF8: 32 FDCE:132
Input output buffers	IBUF : 130 OBUF : 130

Table 5: Compares Architecture 1 with previous relevant implementations

Design	*Delay (ns)*	*Max. frequency (MHz)*	*Throughput (Gbps)*	*LUTs*	*Registers*
Proposed design	3.42	292.40	3.74	1%	1%
M. Goswami &S. kannujiya[19]	4.25	235.29	2.73	.7%	1%
W.Wei, C.jie, X.Fei[20]	4.97	201.20	2.57	Not Available	
Kampen *	5.291	189	.016	73%	39%
J.Castillo *	6.711	149	.0375	94%	57%
Four sbox AES *	6.493	154	.241	93%	22%
H. Satyanarayan*	3.690	271	2.166	81%	33%

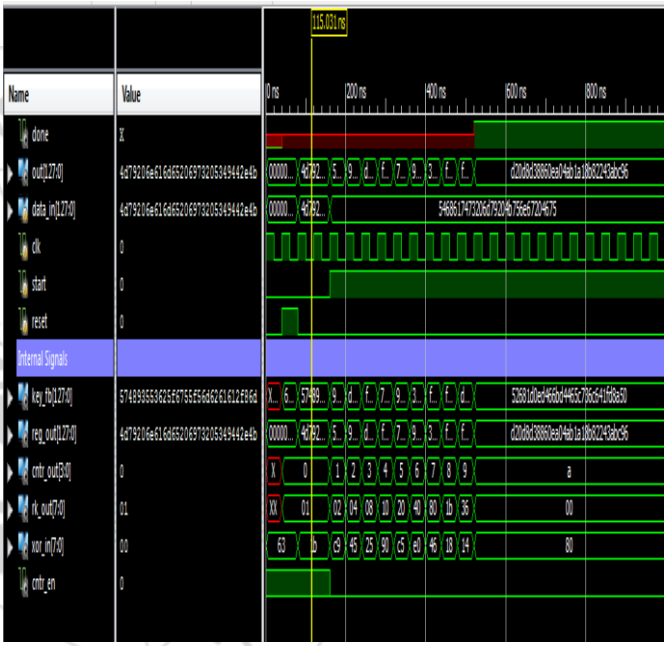

Figure 3.3: Shows the Simulation of key generation module

4. Conclusion

Four architectures have been discussed and Advanced Encryption Standard including very high throughput AES encryption, Very high throughput decryption, Hardware efficient design of AES encryption unit and looping architecture for encryption and decryption with common control unit. All the architecture are implemented on board and thoroughly verified on simulator and hardware.

Thorough analysis of AES algorithm leads to a novel technique of hardware reduction by relocating and merging different operation in AES algorithm. New hardware implementation strategy achieved an efficiency increase of 36% as compared to previous implementation. This new encryption module is best suited for e-commerce server which must have higher throughput and also in RFID module which require lesser area of implementation.

References

[1] W. Stallings, "Cryptography and network security principles and practice," Pearson edition 2009, pp. 135-160.
[2] FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce,November2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[3] K. Gaj and P. Chodowiec. Very Compact FPGA Implementation of the AES Algorithm. In the proceedings of CHES 2003, Lecture Notes in Computer Science, vol 2779, pp. 319-333, Springer-Verlag
[4] T.Good and M.Benaissa, "Very Small FPGA Application-Specific Instruction Processor for AES", IEEE Transactions on Circuit and Systems-I, Vol. 53, No. 7, July 2006.
[5] G. Rouvroy, F.-X. Standaert, J.-J. Quisquater and J.-D. Legat, "Compact and efficient encryption/decryption module for FPGA implementation of the AES Rijndael very well suited for small embedded applications", Information Technology Coding and Computing 2004.
[6] J. M. Granado-Criado, M. A. Vega-Rodriguez, J. M. Sanchez-Perez, and J. A. G"omez-Pulido, "A new methodology to implement the AES algorithm using partial and dynamic reconfiguration,"Integr. VLSI J., vol. 43, pp. 72–80, 2010.
[7] K.Jarvinen, M Tommiska, and Skytta, "A Fully Pipelined Memory less 17.8 Gbps AES-128 Encryptor". Proc. ACM/SIGDA 11th ACM Int. Symposium on Field-Programmable Gate Arrays, FPGA 2003, Monterey, CA, USA, February 2003, pp. 207–215.
[8] X. Zhang and K. K Parhi, "High-speed VLSI Architecture for the AES Algorithm", *IEEE Transactions on Very Large Scale Integration (VLSI) System.*, vol.12, no. 9, pp. 957–967, Sep. 2004.
[9] I. Hammad, K. El-Sankary and E. El-Masry, "High Speed AES Encryptor with Efficient Merging Techniques," IEEE Embedded Systems letters, vol. 2, no. 3, pp. 67-71, Sept. 2010