Dynamic Partial Reconfiguration Implementation of AES Algorithm

Snehal Wankhade
PG Student [VLSI & Embedded system],
Dept. of ECE,
Dr.D.Y.P.S.O.E. Lohegaon,
Pune, India

Prof. Rashmi Mahajan
Assistant professor,
Dept. of ECE,
Dr.D.Y.P.S.O.E. Lohegaon,
Pune, India

ABSTRACT
This work reports Partial Reconfiguration (PR) by which selected areas of an FPGA can be reconfigured during runtime. Today cryptographic algorithms are not safe also embedded cryptographic hardware is costly. Hence to make it cost effective and to provide more secureness reconfigurable hardware such as FPGA is used with the concept of partial reconfiguration. This work gives briefings about the method of hardware implementation for AES encryption algorithm with Dynamic reconfigurable keys. Our implementation reaches very good efficiencies than the compared one as we have adopted our own methodology for key expansion. With the combination of adopted methodology & used FPGA this paper shows better agreement as compared to previous work. This implementation could be a good solution to preserve confidentiality and convenience to the information in the numeric communication.

Keywords
Partial Reconfiguration, Embedded system, Reconfigurable computing, cryptography, FPGA

1. INTRODUCTION
Today, security becomes perplexing and grave issue especially for real time applications. Considering for cryptography algorithms full software implementation is very hefty and slows down the speed of the information exchange. From another side, full hardware implementation is very expensive in terms of area, power and can also worsen speed of information transitions. But the effective implementation of cryptographic algorithm can be done by using Dynamic Partial Reconfiguration (DPR), called as Dynamically PR implementation of a Cryptosystem. Partial Reconfiguration (PR) is the process of changing a portion of reconfigurable hardware circuitry while the other part is still operating [1]. Static Partial reconfiguration and Dynamic Partial reconfiguration are different approaches for reconfiguration. Dynamic partial reconfiguration, also known as active partial reconfiguration, allows changing a part of the device while the rest of an FPGA is still running. Partial Reconfiguration uses three different design flows like Module based, difference based, JBits [2][3][4][5].

With the reference of importance of partial reconfiguration and as this topic is related to recent trend in VLSI Domain the proposed work present an optimal implementation of the AES (Advanced Encryption Standard) cryptography algorithm. By using Partial Reconfiguration (PR) FPGA can dynamically reconfigure itself. PR facility could help to reduce area requirements and increase systems versatility. The reconfigurable aspect adapts the key length which will be given like AES128, AES192, AES256 and the size of the provided information i.e. the fixed data of 128 bits, and makes all the AES blocks reconfigurable. This work is organized as follows: Section 2 describes the AES algorithm which is followed by the next section of Dynamic PR of AES and AES implementation is presented in section 4. Section 5 gives results and last section finally concludes this paper.

2. AES ALGORITHM
Advanced Encryption Standard called as AES is a United States encryption standard defined in Federal Information Processing Standard (FIPS) 192, published in November 2001[6][7]. It was consented in May 2002 as a federal standard. It is the most recent of the four current algorithms approved for federal in the United States called as symmetric encryption algorithm processing data in block of 128 bits. Under the effect of a key, a 128-bit block is encrypted by altering it in a unique way into a new block of the same size. As same key is used for encryption and the reverse transformation, decryption AES is symmetric algorithm. The only secret needed to keep for security is the key. AES may design to use different key-lengths, AES-128, AES-192 and AES-256. Each bonus bit in the key effectively doubles the strength of the algorithm. For the AES algorithm, 128 bits represents the length of the input block, the state and the output block which is denoted as Nb = 4, reflects the number of 32-bit words i.e. number of columns in the State. The key length is represented by Nk = 4, 6, or 8, for 128,192 & 256 bit key which reflects the number of 32-bit words i.e. number of columns in the Cipher Key. The number of rounds which is represented as Nr to be performed during the execution of the algorithm is dependent on the key size i.e. Nr = 10 when Nk = 4, Nr = 12 when Nk = 6, and Nr = 14 when Nk = 8[8]. This algorithm uses a round function for both its Cipher and Inverse Cipher that is composed of four different byte-oriented transformations: 1) byte substitution using a substitution table (S-box), 2) shifting rows transformation, 3) mixing the data within each column of the State array, and last one adding a Round Key to the State.

The Sub_Bytes_transformation is a non-linear byte substitution that operates independently on each byte of the State using a substitution table. In the Shift_Rows_transformation, last three rows bytes of the State are cyclically shifted over different numbers of bytes (offsets). The Mix_Columns_transformation works on the State column-by-column, considering each column as a four-term polynomial. By matrix form it is $s'(x) = a(x) \otimes s(x)$. In the Add_RoundKey_transformation, by a simple bitwise XOR

operation a Round Key is added to the State. Each Round Key contains Nb words from the key schedule [9][10].

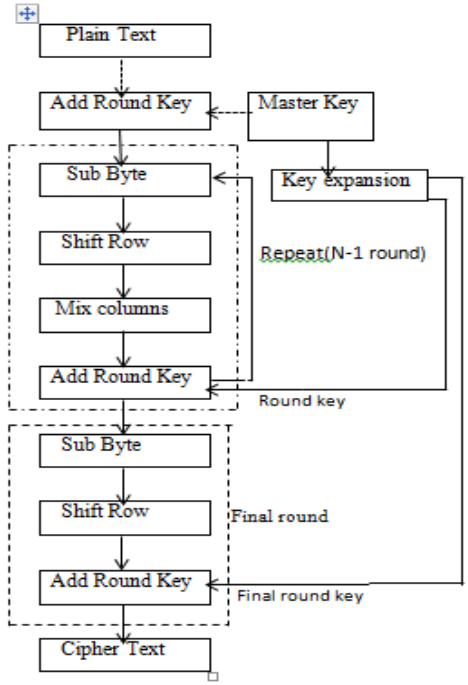

Fig 1: AES Algorithm (Encryption)

3. DYNAMIC PARTIAL RECONFIGURATION OF AES

Dynamic partial reconfiguration is active partial reconfiguration, allows changing a part of the device while the rest of an FPGA is still running. FPGA can reconfigure itself under the control of embedded microprocessor which provides intelligent control of device reconfiguration run-time [11][12][13]. The complexities during the runtime can be simplified by a tool called PlanAhead which was introduced by Xilinx that is able to implement run time reconfigurable systems for all Virtex FPGAs. PlanAhead is the first graphical environment for Partial Reconfiguration. With all FPGA capacities AES Algorithm is implemented as shown in block diagram given below. Here we have used three different AES Types as reconfigurable modules.

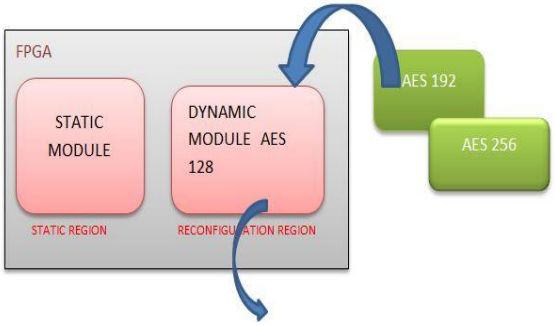

Fig 2: Block Diagram of AES Algorithm with PR

4. PR IMPLEMENTATION OF AES

Design flow of proposed work is shown below in figure 3 in which all AES Types, also called as keys are PR modules. In each AES Type encryption and Decryption is included separately. Figure 4 is global architecture for AES implementation. Manager controller controls and computes the reconfiguration parameters with the help of available embedded processor using the available input and the key size as well as computes the best parameters under input constraints, and writes these parameters in the configuration register for managing the reconfiguration process. Again it supports to reconfigurable AES core i.e. three different types of AES- AES 128, AES 192, AES 256. To increase the performance of the implemented circuit, especially cost, power and inaccessibility, all of the AES blocs may be reconfigurable [14][15][16]. In this way we can change the AES type without stopping normal operation of the system and hence security/performance of AES Algorithm gets enhanced.

Fig 3: Design flow of proposed work

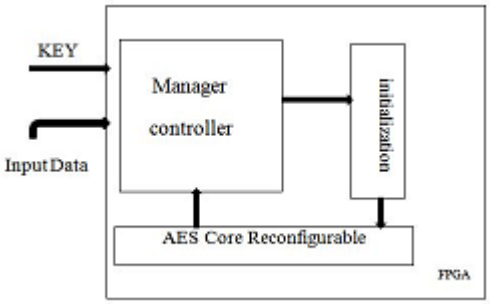

Fig 4: Global architecture for implementation the AES

5. RESULT

In this section, we are going to analyse the obtained results of all AES cryptographic algorithms on Virtex V (XC5VLX110T), comparing them with the results reached by other authors [17]. XilinxISE14.2 was used for the synthesis, place-and-route, and timing analysis. After obtaining the BIT files, our implementation reaches to the results as shown in table 1, achieving very good efficiencies of 2.09Mb/s for AES 128, 1.83Mb/s for AES 192 and 1.81Mb/s for AES 256 than the compared efficiencies. So our result is comparable and better than the [17] implementation. Again we have successfully displayed running AES type on LCD. The table 1 describes the comparison in deeply. Figures 5 & 6 shows simulation of AES Encryption and Decryption which are followed by AES 192 implementation shown in figure 7.

Table 1. Device Utilization History

AES TYPES & FPGA RESOURCES & PARAMETERS			DEVICE XC2V500	DEVICE XC5VLX110T
AES 128	Resources	Slices	192/3072	726/69120
		LUTs	342/6144	2332/69120
		BRAMs	6/32	4/148
	Parameters	Minimum period (ns)	13.674	3.521
		Maximum frequency (MHz)	78.59	284.22
		Clock cycle used	250	748
AES 192	Resources	slices	241/3072	776/69120
		LUTs	341/6144	2322/69120
		BRAMs	6/32	4/148
	Parameters	Minimum period	13.863	3.710
		Maximum frequency	71.78	276.42
		Clock cycle used	300	778
AES 256	Resources	slices	207/3072	742/69120
		LUTs	381/6144	2362/69120
		BRAMs	6/32	4/148
	Parameters	Minimum period	15.045	4.410
		Maximum frequency	70.975	275.45
		Clock cycle used	350	820

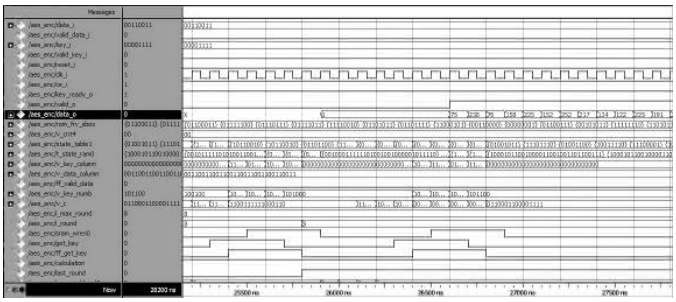

Fig 5: Simulated result of the AES Encryption

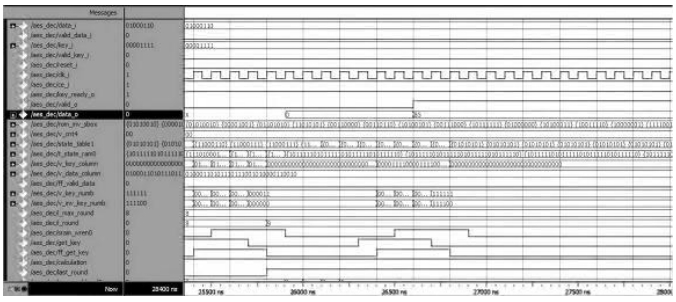

Fig 6: Simulated result of the AES Encryption

Fig 7: AES 192 implementation

6. CONCLUSION & FUTURE SCOPE

Through this work concept of partial reconfiguration is tried to cover. It has been observed that the idea of dynamic reconfiguration can be adapted to reduce the resources. It also reflects that PR is beneficial for reducing device count, reducing power consumption, provide more secure aspect in case of encryption methodology etc. As a part of encryption methodology, in this work, we have presented an implementation of the AES cryptographic algorithm using dynamic partial reconfiguration. The main advantage of this work is the facility to modify the size of the key without stopping the normal operation of the system and hence increases the security of AES algorithm. Implementation of the AES crypto-processor with this new configuration illustrates the ability of this architecture to optimize the reconfiguration time. When we compare our result with other AES implementations (developed by other authors), we obtain the best efficiency (throughput/area) parameter which is most reliable one for purposes of comparison. This implementation could be a good solution to preserve confidentiality and accessibility to the information in the numeric communication.

As this topic could give good contribution in encryption and decryption domain, we would like to extend our ideas by using this algorithm in real communication systems. We would also try to develop the project in more secure aspect.

7. REFERENCES

[1] M. Huebner, C. Schuck, M. Kuhnle, J. Becker, "New 2-Dimensional Partial Dynamic Reconfiguration Techniques for Real-time Adaptive Microelectronic Circuits," Proc. Of Emerging VLSI Technologies and Architectures, Karlsruhe,Germany, Mars 2006.

[2] Matthew G.Parris. Optimizing Dynamic Logic Realizations For Partial Reconfiguration Of Field Programmable Gate Arrays. B.S.University of Louisville. 2008.

[3] K. Bondalapati and V. Prasanna. "Reconfigurable Computing systems," in *Proc. IEEE*, vol. 90, no7, pp.1201-1217,July 2002.

[4] Katherine Compton and Scott Hauck, "Reconfigurable Computing: A Survey of Systems and Software," *ACM Computing Surveys*, vol. 34, no. 2, pp.171-210, June 2002..

[5] Eric Lechner and Steven A. Guccione, "The Java Environment for Reconfigurable Computing", in Proceedings of the 7th International Workshop on Field-Programmable Logic and Applications, FPL 1997. Lecture Notes in Computer Science 1304", Wayne Luk and Peter Y. K. Cheung, eds., Springer-Verlag, Berlin, September 1997, pp. 284-293.

[6] Jose´ M. Granado, Miguel A. Vega-Rodrı´guez, Juan M.Sa´nchez-Pe´ rez, JuanA. Go´ mez-Pulido, "IDEA and AES, two cryptographic algorithms implemented using partial and dynamic reconfiguration" in Microelectronics Journal 40 (2009) .

[7] J. Daemen, V. Rijmen,"AES Proposal : Rijndael, The Rijndael Block Cipher", AES Proposal, 1999.

[8] Z. A. Alaoui, A. Moussa, A. Elmourabit & K. Amechnoue "Flexible Hardware Architecture for AES Cryptography Algorithm" IEEE Conference on Multimedia Computing and Systems, ouarzazate, morocco, April 2009.

[9] Zine El Abidine ALAOUI ISMAILI and Ahmed MOUSSA, "Self-Partial and Dynamic Reconfiguration Implementation for AES using FPGA" , Innovative Technologies Laboratory, National School of Applied Sciences, Tangier,Morocco in IJCSI International Journal of Computer Science Issues, Vol. 2, 2009

[10] J.DaemenandV.RijmenRijndael"Rijndael:AlgorithmSpecification,http://csrc.nist.gov/encryption/aes/rijndael,(2001)

[11] Jose M. Granado-Criado, Miguel A. Vega-Rodrıguez, Juan M. S anchez-Perez, Juan A. Gomez-Pulido, "A new methodology to implement the AES algorithm using partial and dynamic reconfiguration" in INTEGRATION, the VLSI journal43(2010)

[12] Samir El Adib and Naoufal Raissouni, "AES Encryption Algorithm Hardware Implementation Architecture: Resource and Execution Time Optimization" in International Journal of Information & Network Security (IJINS) Vol.1, No.2, June 2012, National School for Applied Sciences of Tetuan, University Abdelmalek Essaadi Innovation & Telecoms Engineering Research Group. Remote Sensing & Mobile GIS Unit. Mhannech II, B.P 2121 Tetuan, Morocco.

[13] A Jelbirt, I Nyip, B Chetwynd, C Paar. "An FPGA Implementation & Performance Evaluation Of The Aes Block Cipher Candidate Algorithm Finalists"

[14] J. Daemen, V. Rijmen, "AES Proposal: Rijndael , The Rijndael Block Cipher",AES Proposal, 1999.

[15] K Vu, D Zier. "FPGA Implementation Aes For Ccm Mode Encryption Using Xilinx Spartan-Ii", Ece-679 (2003)

[16] B. Schneier , "Applied Cryptography", John Wiley & Sons Inc., New York, USA,1996.

[17] Zine El Abidine ALAOUI ISMAILI and Ahmed MOUSSA, "Self-Partial and Dynamic Reconfiguration Implementation for AES using FPGA" , Innovative Technologies Laboratory, National School of Applied Sciences, Tangier,Morocco in IJCSI International Journal of Computer Science Issues, Vol. 2, 2009