ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 4, April 2014**

# Performance Enhancement of AES Algorithm Using Dynamic Partial Reconfiguration

**Ms.Snehal Wankhade[1], Prof. Rashmi Mahajan[2]**

PG Student [VLSI & Embedded system],Dept. of ECE, Dr.D.Y.P.S.O.E. Lohegaon,Pune, India[1]

Assistant professor,Dept. of ECE, Dr.D.Y.P.S.O.E. Lohegaon,Pune, India[2]

**ABSTRACT**: This work reports Partial Reconfiguration (PR) by which FPGA can dynamically reconfigure. The concept of self-reconfiguration is tried to explain under the control of embedded microprocessor like microblaze. Here PR could be useful to reduce area requirements and upsurge systems versatility. Partial Reconfiguration is supported on high end FPGAs like Sparten III, Virtex series.
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 can be used. In this project AES (Advanced Encryption Standard) algorithm has been selected for PR implementation to achieve the goal of secureness in cryptography. This work gives briefings about the method of hardware implementation for AES encryption algorithm with Dynamic Partial Reconfigurable keys. 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

## I.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]. Field programmable gate arrays are frequently used as a provision to PR. Partial reconfiguration allows for critical parts of the design to continue operating while a controller will load a partial design into a reconfigurable module. Xilinx has supported partial reconfiguration for many generations of devices like high end FPGAs, Xilinx Virtex series, Spartan-II.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.

This work uses Partial Reconfiguration (PR) by which FPGA can dynamically reconfigure itself under the control of embedded microprocessor like Microblaze. PR facility could help to reduce area requirements and increase systems versatility, and it could also present an optimal implementation of the AES (Advanced Encryption Standard) cryptography algorithm. 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 blocs reconfigurable.
This work is organized as follows: Related work is tried to cover in section II. Section III describes the AES algorithm which is followed by the Algorithm specification in section IV which will elaborate CIPHER. Dynamic PR of AES and AES implementation is presented in section V and VI. Section VII gives results. The last section finally concludes this paper.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 4, April 2014**

## II.RELATED WORK

Wang Lie et al. has introduced in 2009 about a simple reconfigurable system and focused on the advantages of the newest dynamic partial reconfiguration design flow [2] Different researcher has mentioned about three design flows. A short paper on Module Based Implementation of Partial Reconfiguration Using VHDL on Xilinx FPGA is presented by Solomon Raju Kota et al [3, 4]. Guccione and Delon Levi explains about JBitsie. a Java-Based Interface to FPGA Hardware. How Difference-based partial reconfiguration is useful for making small on-the-fly changes to design parameters such as logic equations, filter parameters, and I/O standards and again how increases in speed and functionality of FPGA based system is presented in IJAET [5].

An innovative implementation for real time audio and video processing using run time internal partial reconfiguration. System is implemented on Virtex-4 FPGA. Internal reconfiguration is handled using internal configuration access port (ICAP) driven by soft processor core. The considerable savings in device resources, bit stream size and configuration time is observed.[6]

Taking an optimal implementation of the AES (Advanced Encryption Standard) cryptography algorithm, many researchers have been devoted the efforts to implement cryptographic algorithm. In the implementation of the AES crypto-processor with partial reconfiguration, it modify the size of the key without stopping the normal operation of the system and hence increases the security of AES algorithm.

The widespread adoption of IEEE 802.11 wireless networks has brought its security paradigm under active research. One of the important research areas in this field is the realization of fast and secure implementations of cryptographic algorithms. Under this work, such an implementation has been done for Advanced Encryption Standard (AES) onfast, efficient and low power Field Programmable Gate Arrays (FPGAs) whereby computationalintensive cryptographic processes are offloaded from the main processor thus results in achieving high speed secure wireless connectivity. The dedicated resources of Spartan-3 FPGAs have been effectively utilized to develop wider logic function which minimizes the critical paths by confining logic to single Configurable Logic Block (CLB), thus improving the performance, density and power consumption of the design. The resultant design consumes only 4 Block RAMs and 487 Slices to fit both AES cores and its key scheduling.[7]

This work, present an experience in implementing two different cryptographic algorithms in anFPGA: IDEA and AES. Both implementations have been done by means of mixing Handel-Cand VHDLand using partial and dynamic reconfiguration in order to reach a very high performance. In both cases,obtained very satisfactory results, achieving27.948Gb/s in the IDE Algorithm and 24.922Gb/sin the AES algorithm.[8]

## III.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. 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 designed 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.

## IV.ALGORITHM SPECIFICATION

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

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 4, April 2014**

dependent on the key size i.e. Nr = 10 when Nk = 4, Nr = 12 when Nk = 6, and Nr = 14 when Nk = 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.

A. CIPHER

At the start of the Cipher, the input is copied to the State array and after an addition of initial Round Key, the State array is transformed by implementing a round function 10, 12, or 14 times (depending on the key length), with the last i.e. final round contrary from the first Nr -1 rounds. The final State is then copied to the output. Key schedule that consists of a one-dimensional array of four-byte words derived using the Key Expansion routine, parameterized the round function. The encryption and decryption process runs as follows in fig 1.

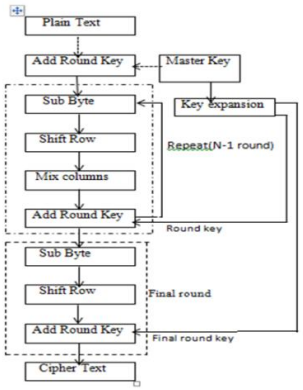



Fig. 1 AES Algorithm (Encryption)

Sub_Bytes_Transformation

The Sub_Bytes_transformation is a non-linear byte substitution that operates independently on each byte of the State using a substitution table (S-box). The S-box used in the Sub_Bytes_transformation is presented in hexadecimal form in Fig. 3. For example, if s(1,1)={53}, then the substitution value would be determined by the intersection of the row with index '5' and the column with index '3' in Fig. 3[9]. This would result in s'(1,1) having a value of {ed}.

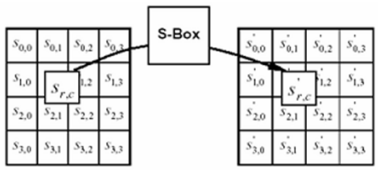


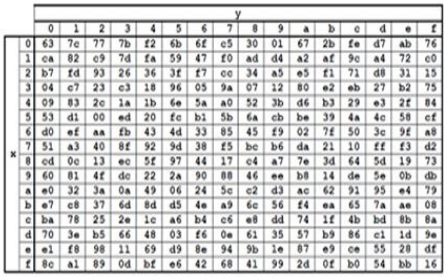

Fig. 2SubBytes() applies the S-box to each byte of the State.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 4, April 2014**



| x \ y | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 63 | 7c | 77 | 7b | f2 | 6b | 6f | c5 | 30 | 01 | 67 | 2b | fe | d7 | ab | 76 |
| 1 | ca | 82 | c9 | 7d | fa | 59 | 47 | f0 | ad | d4 | a2 | af | 9c | a4 | 72 | c0 |
| 2 | b7 | fd | 93 | 26 | 36 | 3f | f7 | cc | 34 | a5 | e5 | f1 | 71 | d8 | 31 | 15 |
| 3 | 04 | c7 | 23 | c3 | 18 | 96 | 05 | 9a | 07 | 12 | 80 | e2 | eb | 27 | b2 | 75 |
| 4 | 09 | 83 | 2c | 1a | 1b | 6e | 5a | a0 | 52 | 3b | d6 | b3 | 29 | e3 | 2f | 84 |
| 5 | 53 | d1 | 00 | ed | 20 | fc | b1 | 5b | 6a | cb | be | 39 | 4a | 4c | 58 | cf |
| 6 | d0 | ef | aa | fb | 43 | 4d | 33 | 85 | 45 | f9 | 02 | 7f | 50 | 3c | 9f | a8 |
| 7 | 51 | a3 | 40 | 8f | 92 | 9d | 38 | f5 | bc | b6 | da | 21 | 10 | ff | f3 | d2 |
| 8 | cd | 0c | 13 | ec | 5f | 97 | 44 | 17 | c4 | a7 | 7e | 3d | 64 | 5d | 19 | 73 |
| 9 | 60 | 81 | 4f | dc | 22 | 2a | 90 | 88 | 46 | ee | b8 | 14 | de | 5e | 0b | db |
| a | e0 | 32 | 3a | 0a | 49 | 06 | 24 | 5c | c2 | d3 | ac | 62 | 91 | 95 | e4 | 79 |
| b | e7 | c8 | 37 | 6d | 8d | d5 | 4e | a9 | 6c | 56 | f4 | ea | 65 | 7a | ae | 08 |
| c | ba | 78 | 25 | 2e | 1c | a6 | b4 | c6 | e8 | dd | 74 | 1f | 4b | bd | 8b | 8a |
| d | 70 | 3e | b5 | 66 | 48 | 03 | f6 | 0e | 61 | 35 | 57 | b9 | 86 | c1 | 1d | 9e |
| e | e1 | f8 | 98 | 11 | 69 | d9 | 8e | 94 | 9b | 1e | 87 | e9 | ce | 55 | 28 | df |
| f | 8c | a1 | 89 | 0d | bf | e6 | 42 | 68 | 41 | 99 | 2d | 0f | b0 | 54 | bb | 16 |

Fig. 3 Intersection of row and column

Shift_Rows_Transformation

In the Shift_Rows_transformation, last three rows bytes of the State are cyclically shifted over different numbers of bytes (offsets). The first row, r = 0, is not shifted. Specifically, the Shift_Rows_transformation proceeds as follows:
This has the effect of moving bytes to "lower" positions in the row (i.e., lower values of c in a given row), while the "lowest" bytes wrap around into the "top" of the row (i.e., higher values of c in a given row).Figure below illustrates the Shift_Rows_transformation.[9]

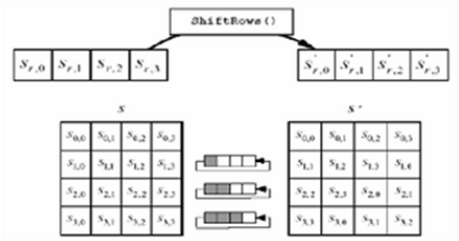



Fig. 4Shift_Rows cyclically shifts the last three rows in the State.

Mix_Columns_Transformation

The Mix_Columns_transformation works on the State column-by-column, considering each column as a four-term polynomial. The columns are reflected as polynomials overGF($2^8$) and multiplied modulo $x^4 + 1$ with a fixed polynomial a(x) which is given by $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$.This can be written as a matrix multiplication. Let $s'(x) = a(x) \otimes s(x)$:

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \quad \text{for } 0 \le c < Nb.$$

Figure below illustrates the Mix_Columns_transformation.[9]

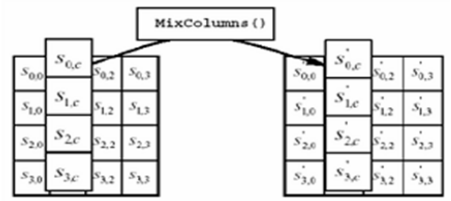



Fig. 5Mix_Columns operates on the State column-by-column.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 4, April 2014**

Add_RoundKey_Transformation

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.The action of this transformation is illustrated in Fig. below, where l = round * Nb.[9]

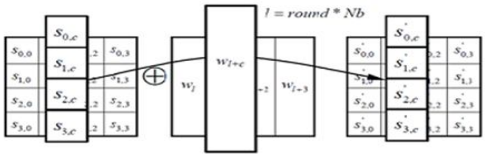



Fig. 6Add_RoundKey XORs each column of the State with a word from the key schedule.

## V.DYNAMIC PARTIAL RECONFIGURATION OF AES

Partial Reconfiguration (PR) is the process of changing a portion of reconfigurable hardware circuitry while the other part is still operating [10]. 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. FPGA can reconfigure itself under the control of embedded microprocessor. This embedded processor provides intelligent control of device reconfiguration run-time. And this reconfiguration can be done with the help of internal configuration access port, control logic, a small configuration cache and an embedded processor. The embedded processor can be Xilinx Microblaze, which is a 32-bit RISC soft processor core [11].Another embedded processor named as hard-core Power PC on virtexII pro can also be used. Internal configuration access port application program interface (ICAP API) and Xilinx partial reconfiguration toolkit (XPART) provide methods for reading and modifying selected FPGA resources and support for relocatable partial bitstreams. With all these FPGA capacities AES Algorithm can be implemented as shown in block diagram given below.

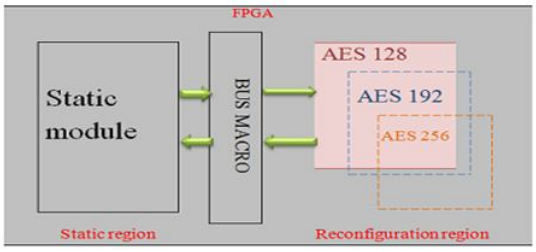



Fig. 7Block Diagram of AES Algorithm with PR

## VI.PR IMPLEMENTATION OF AES

To increase the performance of the implemented circuit, especially cost, power and inaccessibility, all of the AES blocs may be reconfigurable [12].Following figure shows the global architecture for AES implementation. Microblaze processor computes the reconfiguration parameters 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. Internal configuration access port application program interface provide methods for reading and modifying selected FPGA resources. Again it supports to reconfigurable AES core.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 4, April 2014**

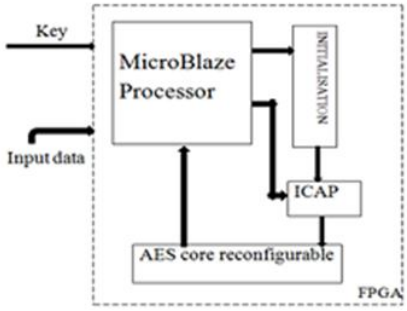



Fig. 8Global architecture for implementation the AES

## VII.RESULT

AES algorithm is implemented with Virtex II (XC2V500) [13] & theresults are summarized as follows:

TABLE I
DEVICE UTILIZATION SUMMARY

| | FPGA Resource | Resource Used/Total Resource (XC2V500) |
|---|---|---|
| AES-128 | Slices | 192/072 |
| | Slice Flip-Flops | 78/6144 |
| | 4-input LUTs | 342/6144 |
| | BRAMs | 6/32 |
| AES-192 | Slices | 241/3072 |
| | Slice Flip-Flops | 76/6144 |
| | 4-input LUTs | 341/6144 |
| | BRAMs | 6/32 |
| AES-256 | Slices | 207/3072 |
| | Slice Flip-Flops | 81/6144 |
| | 4-input LUTs | 381/6144 |
| | BRAMs | 6/32 |

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 4, April 2014**

TABLE II
PERFORMANCE PARAMETERS

| | Parameter | Device (XC2V500) |
|---|---|---|
| AES-128 | Minimum Period (ns) | 13.674 |
| | Maximum Frequency | 78.59 |
| | Clock Cycle Used | 250 |
| | Thtoughput (Mbps) | 40.57 |
| | TPS (kbps/slice) | 232 |
| AES-192 | Minimum Period (ns) | 13.863 |
| | Maximum Frequency | 71.78 |
| | Clock Cycle Used | 300 |
| | Thtoughput (Mbps) | 31.72 |
| | TPS (kbps/slice) | 135 |
| AES-256 | Minimum Period (ns) | 15.043 |
| | Maximum Frequency | 70.975 |
| | Clock Cycle Used | 350 |
| | Thtoughput (Mbps) | 26.734 |

TABLE III
DEVICE UTILIZATION SUMMARY FOR MicroBlaze system and AES

| | | FPGA Slices | LUTs | FF/Latches | BRAM |
|---|---|---|---|---|---|
| | MicroBlaze System | 4083 | 3383 | 3228 | 25 |
| AES coprocessor | AES 128 | 3565 | 3086 | 3042 | 4 |
| | AES-192 | 3764 | 3259 | 3149 | 4 |
| | AES-256 | 3632 | 3127 | 3205 | 4 |

With this, paper results are tried to optimize with VirtexV(XC5VLX110T).AES Encryption & Decryption work is reported in the paper. Simulated results of AES encryption and decryption are as follows:

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 4, April 2014**

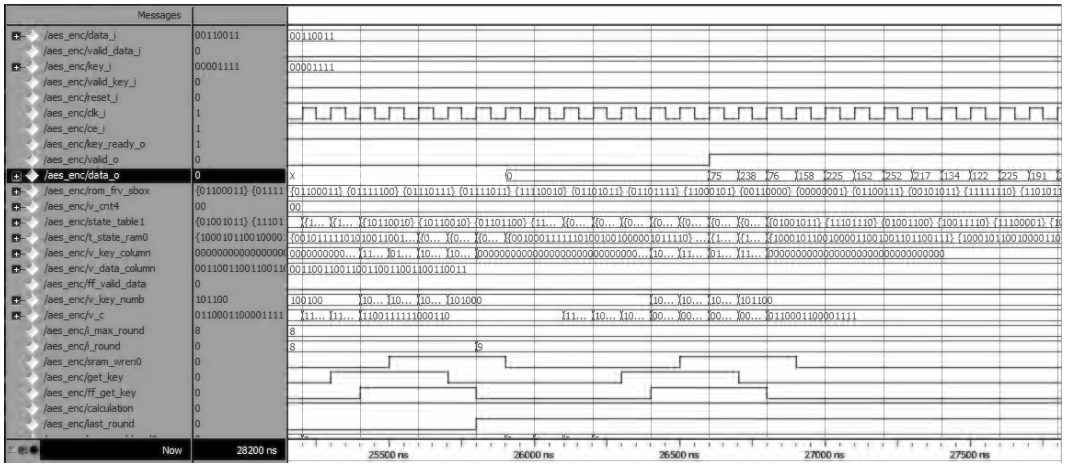



Fig. 9 Simulated result of the AES Encryption

]

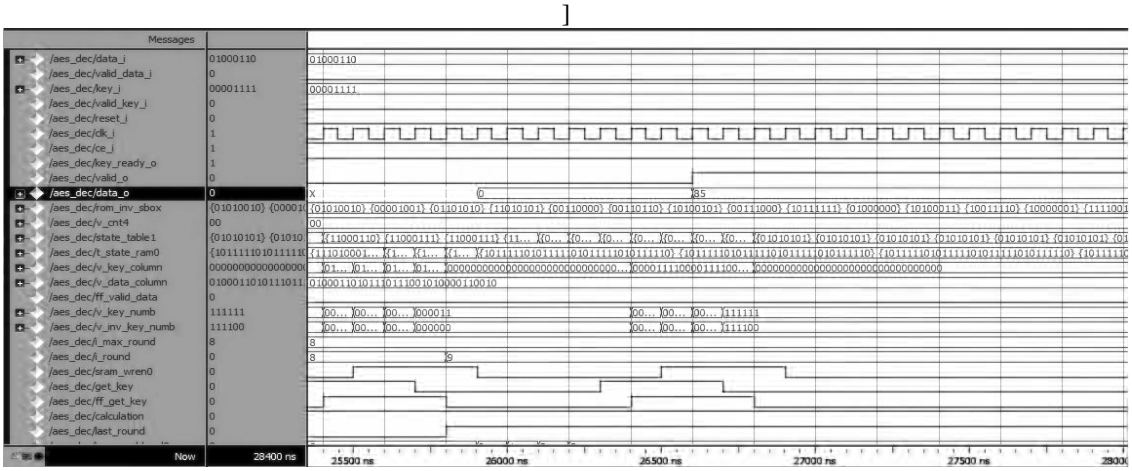



Fig. 10 Simulated result of the AES Decryption

## VI.CONCLUSION

Through this paper 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 AES can indeed be implemented with reasonable efficiency on an FPGA. 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 processor occupation and the reconfiguration time. This implementation is a good solution to preserve confidentiality and accessibility to the information in the numeric communication.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 4, April 2014**

## 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] Sheetal U. Bhandari, ShailaSubbaraman, ShashankPujari and RashmiMahajan"Internal dynamic partial reconfiguration for real time signal processing on FPGA" in Indian Journal of Science and Technology Vol. 3 No. 4 (Apr. 2010).
[7] "FPGA Implementation Aes For Ccm Mode Encryption Using Xilinx Spartan-Ii", Ece-679 (2003) by K Vu, D Zier.
[8] 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) .
[9] J. Daemen, V. Rijmen,"AES Proposal : Rijndael, The Rijndael Block Cipher", AES Proposal, 1999.
[10] Matthew G.Parris, "Optimizing Dynamic Logic Realizations For Partial Reconfiguration Of Field Programmable Gate Arrays." B.S.University of Louisville .2008.
[11] Xilinx, Inc., "The Programmable Logic Data Book", 1996.
[12] 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.
[13] 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
[14] A Jelbirt, I Nyip, B Chetwynd, C Paar. "An FPGA Implementation & Performance Evaluation Of The Aes Block Cipher Candidate Algorithm Finalists"
[15] K Vu, D Zier. "FPGA Implementation Aes For Ccm Mode Encryption Using Xilinx Spartan-Ii", Ece-679 (2003)
[16] J.DaemenandV.RijmenRijndael"Rijndael:AlgorithmSpecification,http://csrc.nist.gov/encryption/aes/rijndael,(2001)
[17] 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) .
[18] 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)
[19] Samir El Adib and NaoufalRaissouni, "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 AbdelmalekEssaadi Innovation & Telecoms Engineering Research Group. Remote Sensing & Mobile GIS Unit. Mhannech II, B.P 2121 Tetuan, Morocco.
[20] B. Schneier , "Applied Cryptography", John Wiley & Sons Inc., New York, USA,1996.
[21] M. Kandemir, W. Zhang, & M. Karakoy, "Runtime code parallelization for onchip multiprocessors", In Proceedings of the 6th Design Automation and Test in Europe Conference, Munich, Germany, March, 2003.
[22] J. Daemen, V. Rijmen, "AES Proposal: Rijndael , The Rijndael Block Cipher",AES Proposal, 1999.
[23] M. Huebner, C. Schuck, M. Kuhnle, and 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.