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. 2, Issue 10, October 2013

HIGH SPEED PARALLEL CONCURRENT ERROR DETECTION SCHEME FOR ROBUST AES HARDWARE

Amandeep Kamboj[1], R. K Bansal[2], Savina Bansal[3]

P.G. Student, Dept. of E.C.E, PTU GZS Campus, Bathinda, Punjab, India[1]

Professor, Dept. of E.C.E, PTU GZS Campus, Bathinda, Punjab, India[2]

Professor, Dept. of E.C.E, PTU GZS Campus, Bathinda, Punjab, India [3]

Abstract: This paper proposes the high speed parallel concurrent error detection scheme for robust AES hardware. Very large scale integration devices are very susceptible to transient errors. Due to the efficiency and flexibility of the advanced encryption standard (AES) algorithm, it becomes the popular choice in different applications like embedded systems; satellites etc. AES is the current standard for the secret key encryption. The FIPS 197 used a standardized version of the algorithm called as Rijndael for AES. This paper basically shows the detection of soft error in the AES cipher output during the hardware implementations.The hardware design of this AES block with single bit error correction was accomplished using VHDL and implemented on Xilinx Virtex 6 FPGA. The modelling process utilized in this project is the bottom-up approach. All the modules in the design hierarchy were modelled in behavioural style, but the root module consisted of data flow modelling. This process yields better results as hardware is developed in such a fashion that it supports parallelism in it.

Keywords: AES, soft error, cipher output anderror detection

I. INTRODUCTION

In recent times due to technological advancements, the performance of integrated circuits has increased a lot also lower device sizes, low power consumption have also helped to improve the performance of the devices. But on the other hand, modern devices have become more susceptible to transient faults and when these faults are executed, it creates soft errors. So soft errors are errors which are not consistent rather they are random. Although Soft errors cannot damage the physical hardware of the chip however they can corrupt the value stored in the chip. Hard errors are related to the system hardware. So the difference between soft errors and hard errors is that, soft errors can be corrected by applying different techniques where as to rectify hard errors physical changes has to be done on hardware.

Soft errors can occur due to environmental conditions such as radiation flux, alpha particles, cosmic rays, power supply fluctuations, temperature, pressure, humidity and electromagnetic interference. Causes of soft errors are alpha particles from package decay and cosmic rays emissions and thermal neutrons. Alpha particles are released from radioactive atoms, they contain positive charge and kinetic energy and when it travels through the semiconductor it can disturb the electron hole pair distribution. By this the digital signal can change from 0 to 1 or vice versa.Cosmic rays can also cause soft errors. Large part of the earth's surface contains energetic neutrons. The flux of these energetic neutrons is called cosmic rays. Cosmic rays flux depends on altitude. So at higher altitudes a system can suffer more soft errors compared to sea level.

Temperature changes, electromagnetic fields and stress affect electronic devices causing their abnormal operation and erroneous output. Until 1996, it had not been known that the erroneous output of the cryptographic algorithm could be used to perform an attack. Boneh et al first showed that the algorithms that are used for security can be broken by inducting errors during encryption process. These fault attacks may be the reason of transient faults and can take advantage of it that will cause bit flip error in the registers of the device. Advanced encryption standard replaced the 64 bit data encryption standard as the AES algorithm is a symmetric cipher that is it uses a single secret key for encryption and decryption.

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. 2, Issue 10, October 2013

II. AES ALGORITHM

The AES is a subset of a much larger encryption algorithm known as *Rijndael*, which was one of many proposals to the NIST competing for becoming a standard encryption algorithm. On October of 2000, the NIST announced the *Rijndael* algorithm as the winner due to the best overall score in security, performance, efficiency, implementation capability and simplicity. The AES algorithm is a symmetriccipher. In symmetric ciphers, a single secret key is used for both the encryption and decryption, whereas in asymmetric ciphers, there are two sets of keys known as private and public keys. The plaintext is encrypted using the public key and can only be decrypted using the private key. In addition, the AES algorithm is a block cipher as it operates on fixed-length groups of bits (blocks), whereas in stream ciphers, the plaintext bits are encrypted one at a time, and the set of transformations applied to successive bits may vary during the encryption process. Each round of AES cipher (except the last one) consists of all the following transformation:

1) *Block and key*: The AES algorithm operates on blocks of 128 bits, by using cipher keys with lengths of 128, 192 or 256 bits for the encryption process. The block size is commonly denoted as N_b and the key size is commonly denoted as N_k, .The plaintext input and cipher text output for the AES algorithms are blocks of 128 bits. The cipher key input is a sequence of 128, 192 or 256 bits. In other words the length of the cipher key, N_k, is 4, 6 or 8 words which represent the number of columns in the cipher key.
2) *Rounds*:The number of rounds of encryption for AES depends on the cipher key size. Algorithm uses a number of rounds to transform the data for each block. The number of rounds used is maximum of N_b andN_k. In the AES algorithm, the number of rounds is represented by N_r, where $N_r = 10$ when $N_k = 4$, $N_r = 12$ when $N_k = 6$, and $N_r = 14$ when $N_k = 8$. The following table illustrated the variations of the AES algorithm. For the AES algorithm the block size (N_b), which represents the number of columns comprising the *State* is $N_b = 4$.
3) *Key Expansion*: The original cipher key needs to be expanded from 16 bytes to 16(rounds + 1) bytes. Round key will be of 16 bytes similar to the block size. A rounded key is needed after each round and before the first round. The expanded key is then broken up into round keys. Round keys are added to the current state after each round and before the first round.
4) *S Box*: It is used to change the original plain text to cipher text. The values can be represented as hexadecimal notation.
5) *Shift Rows*: In this the rows are shifted x number of the bytes to the left where x is the row number. This means row 0 will not be shifted, row 1 will be shifted 1 byte to the left and so on.
6) *Mix Column*: The mix column table takes a byte and transforms it into four bytes.

All the AES algorithm operations are performed on a two dimensional 4x4 array of bytes which is called the State, and any individual byte within the State is referred to as $s_{r,c}$, where letter '*r*' represent the row and letter '*c*' denotes the column. At the beginning of the encryption process, the State is populated with the plaintext. Then the cipher performs a set of substitutions and permutations on the State. After the cipher operations are conducted on the State, the final value of the state is copied to the cipher text output. The AES cipher either operates on individual bytes of the State or an entire row/column. At the start of the cipher, the input is copied into the State as described. Then, an initial RoundKey addition is performed on the State. Round keys are derived from the cipher key using the Key Expansion routine. The key expansion routine generates a series of round keys for each round of transformations that are performed on the State.

III. PROPOSED APPROACH

Although normal AES hardware designs which exist today are highly reliable, chances of soft error occurrence cannot be ruled out. This no doubt forms a major hurdle in the design of microelectronic circuits and systems. Designing a microelectronic chip is a very expensive task and excessive design costs are the greatest threat to continuation of the semiconductor industry's growth. In order to contain this threat, the increasing gap between the complexity of new systems and the productivity of system design methods must be mitigated by developing new and more efficient design

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. 2, Issue 10, October 2013

methods and tools. Functional correctness of systems is becoming ever more difficult to attain and it is becoming the main bottleneck in the systems' development process.

In this paper we have attempted to formulate a design procedure which can always guarantee the functional correctness of the AES hardware that is designed. In this method error detection is done by validating the output block cipher during the hardware implementations.The hardware design of this AES block with single bit error correction was accomplished using VHDL and implemented on Xilinx Virtex 6 FPGA. The modelling process utilized in this project is the bottom-up approach. This means that the leaf components in the design hierarchy were developed first and the higher-level modules were constructed by instantiating their subcomponents and connecting them with the internal signals. All the modules in the design hierarchy were modelled in behavioural style, but the root module consisted of data flow modelling as well to implement the four major cipher transformations.
The inputs to the design are:-

- Plaintext
- Key block
- Clock
- Reset

The output is soft error hardened cipher text. This has been accomplished via two steps: **I)** according to a built-in reliability functions library, the designer specifies the coding techniques to be incorporated into the circuit; II) then, by using a specific fault injection technique, the designer estimates the circuit reliability. Both steps are performed in VHDL high-level description language.The first step of the approach is based on the incorporation of coding techniques into the original VHDL circuit description. The coding approaches considered are in the form of: **(a)** Hamming code plus one parity bit per storage element (single registers) to correct single errors and to detect double errors (SEC/DED); and **(b)** Two-dimensional parity code to be applied to the columns and lines of embedded memory arrays.

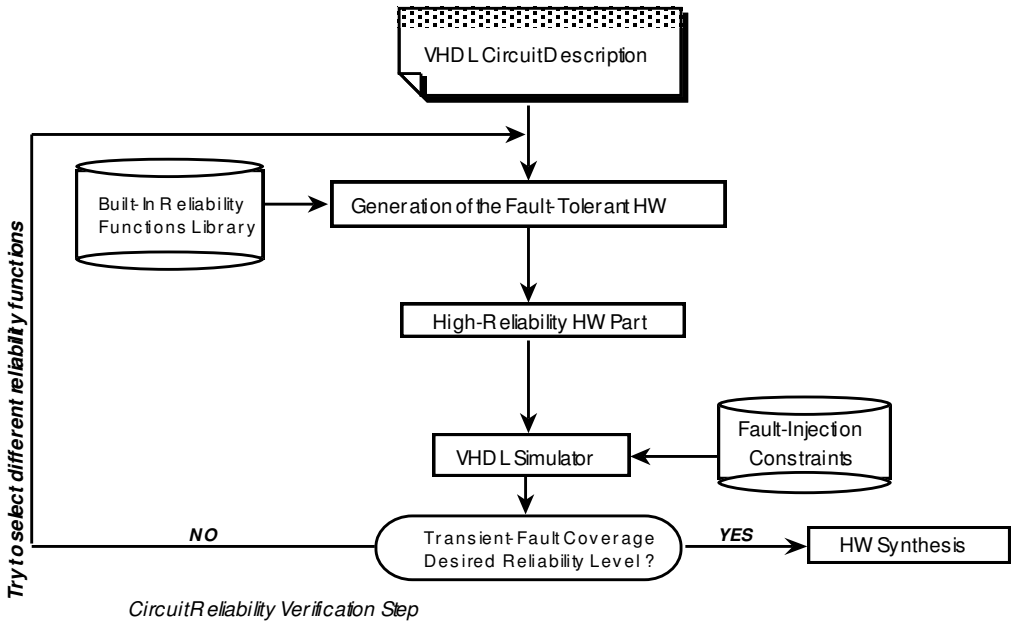

Fig 1: Detection and Correction of soft errors

The above design approach is also consistent with the thought that hardware fault tolerance requires multiple modules in order to tolerate module failures. Hence all the individual modules have been designed with SEU self checking capability. The complete hardware with this soft error detection capability has been implemented in Xilinx ISE design

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. 2, Issue 10, October 2013

suite. There were basically two things to be considered, one was to have a hardware implementation that had a low area footprint for efficiency and second was to have a high speed system that was capable of performing multiple encryption cycles within a very less time while still maintaining high accuracy bounds as far as soft errors are concerned.

IV. RESULTS

Complete RTL view of the design is shown below (Opened within XILINX ISE GUI):-

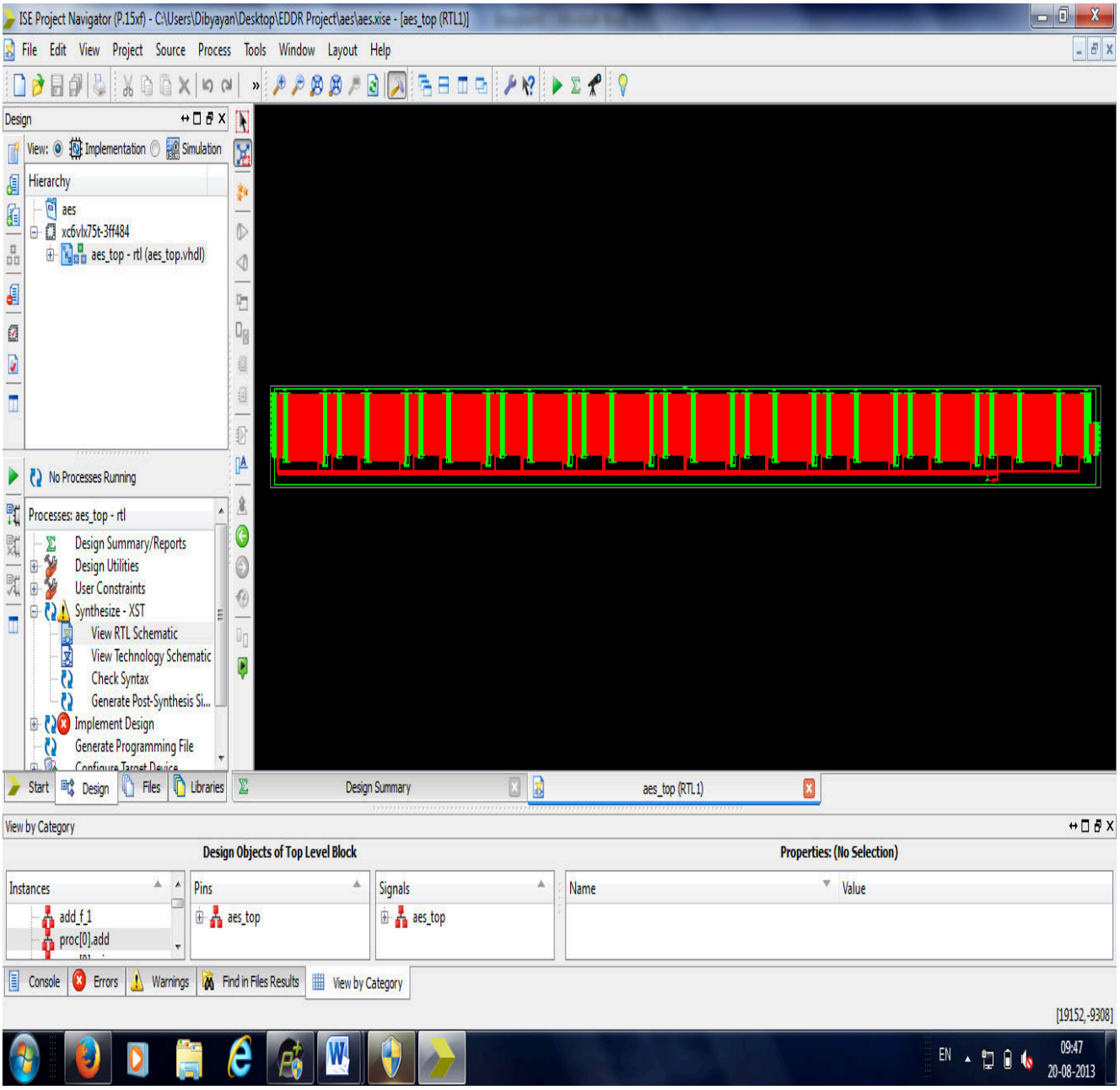

Fig 2: The complete RTL view of the design

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. 2, Issue 10, October 2013

The individual RTL blocks are shown below:-

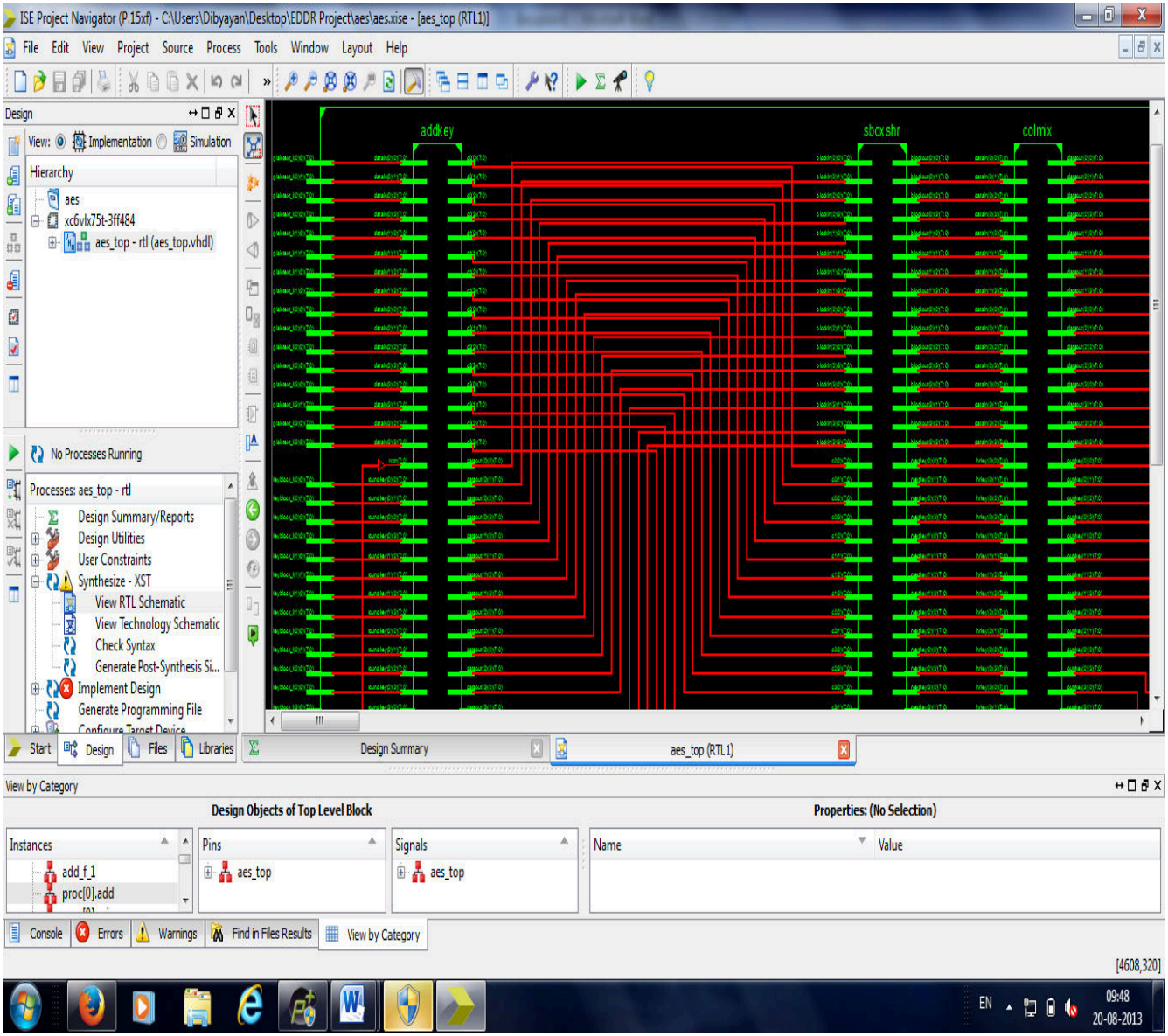

Fig 3: The individual RTL blocks

From these RTL blocks one can clearly see the level of parallelism introduced for obtaining high throughput for better performance.

The complete VLSI hardware of the system (technology view) is shown below:

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. 2, Issue 10, October 2013

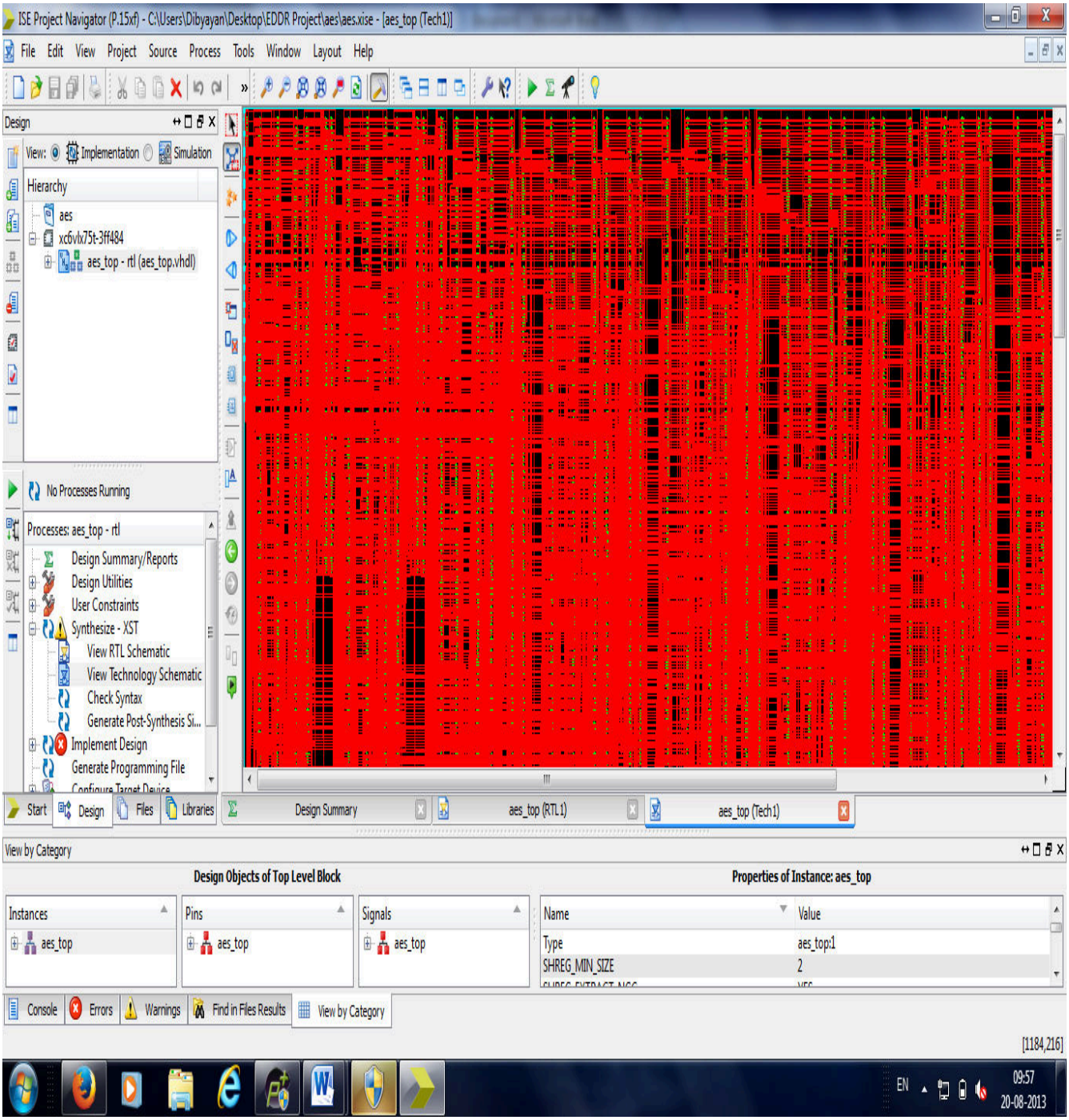

Fig 4: The complete VLSI hardware of the system

The dense matrix of interconnects and components can be seen above. The net hardware efficiency (area/logic gates) achieved is around 92% (approximately).

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. 2, Issue 10, October 2013

V. COMPARISON TABLE

Parameters	This project	Existing Best
Clock cycles	12	24
Max. Frequency	739 MHz	340 MHz
Latency	60 ns	92.5 ns
Hardware efficiency	92% (approx)	90%

VI. CONCLUSIONS

As Advanced encryption standard (AES) algorithm is popular choice among different applications so it is necessary to detect errors. So some techniques are required which can reduce these soft errors and increase the performance as well as reliability of a system. In proposed method error is detected by validating output cipher block during hardware implementations. The hardware design of this AES block is accomplished using VHDL and implemented on the Xilinx Virtex 6 FPGA. We showed the level of parallelism to get high throughput. This is time consuming method and provides better efficiency.

ACKNOWLEDGMENT

My sincere thanks toco-authors; Dr. R.K Bansal and Dr. Savina Bansal, for their guidance and support. I also want to acknowledge all the researchers whose works have been used as reference in preparing this paper.

REFERENCES

[1] Kalaiarasi et.al, *"A hybrid fault detection and correction AES for space applications"*, International journal for electronics and communication engineering ISSN 0974-2166 vol 6, No. 2 , pp. 187-197, 2013

[2] Akashi Satoh et al , *"*High performance current error detection scheme for AES hardware*"*, E Oswald and P. Rohatgl (Eds): CHES 2008, LNCS 5154, pp. 100-112,2008

[3] N. MiskovZivanov and D. Marculescu, *"*Modelling and reduction of soft errors in combinational circuits," Piscataway, NJ, USA, pp.767-72, 2006.

[4] Norbert Seifert, Xiaowei Zhu and Lloyd W.Massengill, "Impact of scaling on soft error rates in commercial microprocessors*,"* IEEE transactions on nuclear science, vol.49, No.6, December 2002.

[5] Timothy.C.May*, "*Alpha particle-induced soft errors in dynamic memories," IEEE transactions, vol ED 26, No.1, January 1979.

[6] AtulMaheshwari, "Trading off transient fault tolerance and power consumption in deep submicron (DSM) VLSI circuits*"*, IEEE transactions on very large scale integration systems, vol 12, No.3, March 2008.

[7] P. Chodowiec, K. Gaj, "Comparison of the hardware performance of the AES candidates using reconfigurable hardware,"AES3 candidate conference, April 2000.

[8] P. Chodowiec, K. Gaj, "Very compact FPGA implementation of the AES algorithm*"*, In the proceedings of CHESS 2013, vol 2799,pp. 319-333,Springer-Verlag,2013.

[9] Yen, C.H. & Wu, B.F. "Simple error detection methodsfor hardware implementation of Advanced Encryption Standard*"*, IEEE transactions on computers, vol. 55, No. 6, pp 720-731, June 2006.

[10] G. Bertoni, L. Breveglieri, "Error analysis and detection procedures for a hardware implementation of the Advanced EncryptionStandard*"*, IEEE transactions on computers, vol 52, No. 4, pp 492-505, April 2003.

BIOGRAPHY

1. AMANDEEP KAMBOJ is a Post Graduate Student in Electronics and Communication Department at Punjab Technical University Giani Zail Singh Campus, Bathinda, Punjab. She received B.Tech degree in Electronics and Communication from Global Institute of Technology & Management, Jaipur in the year 2009. Her interests include Digital Signal Processing and Digital Electronics.

2. Dr. R. K Bansal, Professor in the ECE department of PTUGZS Campus, Bathinda.

3. Dr. Savina Bansal, Professor in the ECE department of PTUGZS Campus, Bathinda.