ISSN 2278 - 3091

International Journal on Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 No.1, Pages : 28 – 30 (2015)
Special Issue of ICACE 2015 - Held on March 02, 2015,Mysore, India
http://warse.org/pdfs/2015/icace2015sp06.pdf

NoC Implementation of AES Algorithm: A Survey

[1]Harish Babu L, [2]Savitha C, [3]Dr. M Z Kurian
[1] 4th sem, M.Tech (VLSI and Embedded Systems), SSIT, Tumkur (harishbabumay2@gmail.com)
[2] Asst.Prof, Dept.of ECE, SSIT, Tumkur
[3] HOD, Dept.of ECE, SSIT, Tumkur

ABSTRACT

Network on chip (NoC) is the scalable platform where billion transistors have been integrated on to a single chip. NoC architecture is a m×n mesh of processing elements where resources are placed on the slots formed by the switches. Each switch is connected to one resource and four neighboring switches, and each resource is connected to one switch. A resource can be a processor core, memory, or any other intellectual property (IP) block, which fits into the available slot and complies with the interface of the NoC. The NoC architecture is an on-chip communication infrastructure which comply OSI protocol stack.

Existing Algorithm has a deadlock issue and head of line blocking problem which reduces the efficiency of system. Here a modified routing logic has been proposed and the same will be developed for NoC architecture to overcome drawbacks of algorithm. Here an Advanced Encryption Standard (AES) blocks will be used for the designing of the Network-on-Chip architecture. And the survey of the related researches has been carried out to support the design.

Key words: *Network on chip (NoC), Advanced Encryption Standard (AES), Open System Interconnect (OSI).*

INTRODUCTION

Network on chip is an emerging paradigm for communications within the large VLSI systems implemented on a single silicon chip. As the size of the transistor shrinks and for instance if the large amount of IP block functions are to be added on to the chip the physical infrastructure that carries data on the chip and guarantees the quality of service begins to crumble.

The numbers of processing cores on the single chip have been increasing, which is the key factor for the evolution of the concept of network on chip architecture. NoC had been replacing the traditional bus architecture in order to provide high performance and on chip communication. The Importance of Network on Chip are listed as follows:

- Reduce wire rooting Congestion
- Ease of timing closure
- Higher operating Frequency
- Change IPs easily

The two standard cryptographic algorithms are Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are been compared, The Advanced Encryption Standard is symmetric key algorithm. AES algorithm supports a key length of 56,192 and 256 bits. Given that a block of encrypted and decrypted data is known, if the 56 bit DES algorithm could be broken in one second simply by trying every single key, the same method using 128 bit AES algorithm approximately will take 1.5x1014 years to break.

The AES algorithm has been selected for many reasons, few such reasons are given to be as the Encryption core will need to support a wide range of applications and can be used to encrypt large amount of data. The core will go into a library that other designers can use a black box design.

LITERATURE SURVEY

In the paper “Overview of Network on Chip Architecture”, authorized by Bharathi B.Sayankar and S S Limaye., Network-on-Chip (NoCs) are the key components of emerging System-on-Chip (SoCs). As SoCs grows in area, complexity and functionality, their communication requirements in terms of performance and number of interconnected components will increase.

Reducing NoC latency is crucial for SoC performance. Also its mentioned that the function of Network-on-Chip is to deliver message from source node to destination node, and there are many alternatives to accomplish this job. Topology Development states that topology defines how nodes are placed and connected, affecting the bandwidth and latency of a network. Routing is the mechanism responsible for determining the path that a packet

ISSN 2278 - 3091

International Journal on Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 No.1, Pages : 28 – 30 (2015)
Special Issue of ICACE 2015 - Held on March 02, 2015,Mysore, India
http://warse.org/pdfs/2015/icace2015sp06.pdf

traverse from source node to destination. Routing algorithm such as *Adaptive* and *Deterministi*c ones have been proposed. Some of the architectures designed here for network design are Circuit Switched Router Design, Virtual Channel router Design and Wormhole Router Design [1].

In the paper "Implementation and Evolution of On-Chip Network Architecture", authored by Paul Gratz, Chngkyu Kim and Robert McDonald,. Systems are driven by the higher bandwidth and the complexity reduction, off-chip interconnect has evolved from proprietary busses to network architectures. A similar evolution is occurring on the on-chip interconnect too. The research presented the design, implementation and evolution of one such on-chip network, the TRIPS OCN. Trade-off s made in the design of the OCN, in particular why area and complexities were trade off against the latency were also discussed. And finally the effect of link bandwidth and router FIFO depth on overall performance[2].

In the paper "A Comparative Study of Different Topologies for Network-on-Chip Architecture", authored by Sonal S Bhople and M A Gaikwad,. Presents the idea of different network topologies that have been developed on On-Chip networking.The network topology refers to the shape of the network, How the different nodes in the network are connected to each other and how they communicate is determined by the network's topology[3].

In the paper "3D Topologies for Networks-on-Chip", authored by Vasilis F. Palvidis and G. Freidman,. The idea of 3D topologies have been put forth in this paper, and explained that several interesting topologies emerge by incorporating the third dimension in networks-on-chip (NoC). The speed and power consumption of 3-D NoC are compared to that of 2-D NoC. Physical constraints, such as the maximum number of planes that can be vertically stacked and the asymmetry between the horizontal and vertical communication channels of the network, are included in speed and power consumption models of these novel 3-D structures. Tradeoffs between the number of nodes utilized in the third dimension, which reduces the average number of hops traversed by a packet, and the number of physical planes used to integrate the functional blocks of the network, which decreases the length of the communication channel, is evaluated for both the latency and power consumption of a network. A performance improvement of 40% and 36% and a decrease of 62% and 58% in power consumption is demonstrated for 3-D NoC as compared to a traditional 2-D NoC topology for a network size of N = 128 and N = 256 nodes, respectively.

The 3-D IC–3-D NoC topology provides the optimum choice in terms of minimizing the zero-load network latency, as with this topology both the delay and power consumption components can be efficiently reduced. For the case where the impedance characteristics of the buss and crossbar switch within the network are of similar magnitude, the 2-D IC–3-D NoC offers the minimum latency and power consumption, while for large networks, the impedance of the buss determines the delay and power characteristics of the network and, therefore, a 3-D IC–2-D NoC topology yields the best results. For medium sized networks, a 3-D IC–3-D NoC topology is preferable, since in these network sizes both the number of hops and the length of the buss can be decreased to produce the minimum zero-load latency and power consumption [4].

In the paper "Advanced Encryption Standard: Cryptanalysis Search" authorized by Daniyal M.Alghazzawi and Syed Hasan,. The Advanced Encryption Standard (AES) has been the focus of Cryptanalysis since it was released. And the later stage the AES was also declared as the Type-1 Suit-B Encryption Algorithm by the NSA in 2003. Which makes it deemed suitable for being utilized for encryption of the both Classified & Unclassified security documents and systems. Some of the attacks on the AES:

Pre-existing Attack: Here the relationship difference between the input & output of the function block are exploited by differential cryptanalysis.

Algebraic Attack: This technique treats the AES as combination of multivariable polynomial equation across a single Galois field, with the aim of recovering the key variable by solving these equations.

SAT-Solver: This is done by setting the cipher-text and plain-text variable in the expression to their corresponding known plain-text and cipher-text, the key can be recovered.

Side Channel Attack: This attack utilizes the information that is leaked out of the cryptosystem because of the loopholes in the system's physical implementation, instead of cryptographic weakness in the algorithm [5].

In the paper "AES-512: 512-Bit Advanced Encryption Standard Algorithm Design and Evolution" presented by Abidalrahman Moh'd and

International Journal on Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 No.1, Pages : 28 – 30 (2015)
Special Issue of ICACE 2015 - Held on March 02, 2015,Mysore, India
http://warse.org/pdfs/2015/icace2015sp06.pdf

Yaser Jararweh,. The FPGA architecture for a new version of the Advanced Encryption Standard Algorithm and efficient hardware implementation is done. The new Algorithm (AES-512) uses input block size and key size of 512-bits which makes more resistant to cryptanalysis with tolerated area increase. AES-512 will be suitable for applications with high security and throughput requirement and less area constrains such as multimedia and satellite communications. This system is developed in VHDL and observed the throughput increase of 230% when compared with the AES-128.

This algorithm has four main different byte-based transformations. First is the byte substitution which substitute the value of 512 bits and this is achieved using the parallel S-boxes. The second transformation is the Shifting Rows, which shifts the rows of the output from the previous step by an offset equal to the row number. Third is the mixing column, where each column of the previous step is multiplied by different value. And final is the adding the Round Key to the final result of this round [6].

In the paper "Parallel AES Encryption Engine for Many-Core Processor Arrays", authored by Bin Liu and Bevan M. Baas,. It is explained that by exploring different granularities in data level and task level parallelism, they have mapped 16 implementations of Advanced Encryption Standards(AES) cipher with both online and offline key expansion on a fine-grained many-core system. The smallest design utilized only six cores for offline key expansion and eight cores for online key expansion, while the largest took 107 and 137 respectively. Comparing the research with the AES cipher implementation on to general purpose processors, their design had 3.5 to 15.6 times higher throughput per unit of chip area and 8.2 to 18.1 times higher efficiency.

An overview of cryptanalysis research for the advanced encryption standard is explained in the case of a block Cipher, linear combinations of plaintext patterns and linear combinations of Cipher text patterns are compared to linear combinations of key bits. The advantages of a software implementation include ease of use, ease of upgrade, portability, and flexibility [7].

CONCLUSION

The main aim is to implement the Network-on-Chip (NoC) architecture for the Advanced Encryption Standard (AES). In the literature survey which is made prior to designing of the system is been observed that there are many innovative solutions and ideas put forth by many researchers which includes the architectural topologies, some properties of the network topologies, 2D and 3D architectures of On-Chip topologies, types of attacks in encryption standards, advancement in operating number of bits in AES so as to improve the throughput

So observing all these, it can be concluded that the *Network-on-Chip* would be the best approach to speed up the parallel operation of multisystem provided the IP cores modules incorporating on single board.

REFERENCES

[1] Bharathi B.Sayankar and S S Limaye, *"Overview of Network on Chip Architecture"*, national conference on information and communication technology 2011

[2] Paul Gratz, Chngkyu Kim and Robert McDonald. *"Implementation and Evolution of On-Chip-Network Architecture"*, IEEE transactions 2006

[3] Sonal S Bhople and M A Gaikwad, *"A Comparative Study of Different Topologies for Network-on-Chip Architecture"* , IEEE transaction 2013

[4] Vasilis F. Palvidis and G. Freidman *"3D Topologies for Networks-on-Chip*", IEEE transactions on Very Large Scale Integration (VLSI) systems, vol. 15, no. 10, October 2007

[5] Daniyal M. Alghazzawi, and Syed Hamid Hasan, *"Advanced Encryption Standard: Cryptanalysis Research"*,IEEE Transaction 2014.

[6] Abidalrahman Moh'd and Yaser Jararweh, *"AES-512: 512-Bit Advanced Encryption Standard Algorithm Design and Evolution"*, IEEE Transaction 2011.

[7] Bin Liu and Beven M. Baas, *"Parallel AES Encryption Engines for Many-Core Processor Arrays"*, IEEE Transaction on computers, vol. 62, no.3, March 2013