Design and Implementation of NOC based Parallel AES Computation

Bharati.S. Kerakalamatti
MTech student, UTL Technologies
VTU Extension Centre, Bangalore-22, India

Nagaraj. P
Asst.Professor , UTL TechnologiesVTU
Extension Centre, Bangalore-22, India

ABSTRACT
In today's SOC, the number of processing cores is increasing with growth of VLSI technology. The on chip communication among multiple cores using NOC based architecture is effective than conventional bus based architecture, Since NOC has many advantages than bus based architecture mainly in terms of scalability (increase in number of nodes) and flexibility. Hence in this paper, Mesh based NOC architecture with packet switching is adopted for cryptography without virtual channel and pipelining techniques. The deterministic X-Y routing algorithm is used for routing a packet within the NOC. This paper presents a 10 -20% less area consumption NOC with AES as processing element , over previous work.

Keywords
SOC (System On Chip), NOC (Network On Chip), AES(Advanced Encryption Standard), X-Y routing algorithm.

1. INTRODUCTION
In the past recent years, the rapid evolution in Very Large Scale Integration (VLSI) results into a single silicon chip which is fabricated with millions of transistors. In the existing CMOS technology, a design can be put into effect with approximately a single chip with one billion transistors. This improvement in the micro-electronics influence to the integration of various elements of a computing system or any other electronic system on a single Integrated Circuit (IC) to implement a complete system on a chip. Thus a standard called System on Chip (SoC) came into reality that refers to the system made up of interconnected cores or Intellectual Property (IP) block on a single chip [1].

Crossbars, rings, buses, and NoCs are the different types of interconnection Patterns, which are currently used for communication among cores within SOC. Among these interconnection patterns, bus and NOC have been leading in the research area. The bus based communication in SOC leads to remarkable decrease in the performance of SOC as the number of processing elements increases, since buses are affected from poor scalability [2]. Thus buses are not considered suitable communication scheme for systems, which have more number of cores. This drawback of bus based communication is beated by on-chip communication networks, known as Networks-on-Chip (NoC). As the number of nodes increases in SOC, scalability is still very efficient in case of NOC based communication. Because of NOCs good scalability, they are considered the most feasible communication scheme for multi-core chips [3].

If all the cores (PE) are performing same task in a NOC, then they are homogeneous cores. Driving homogeneous cores in a NOC improves the performance of a Specific task [4]. Thus in this paper , all processing elements do AES computation to improve the performance of specific task such as cryptography .Cryptography is the science of writing in secret code and is an ancient art. Data can be protected from theft or modification using Cryptography. In Cryptography, the plaintext is referred as original unencrypted data. The process of converting plaintext into cipher text is called encryption. Whereas process of returning to plaintext from cipher text is called decryption [5]. Cryptography is essential while communicating over any untrusted medium, which include just about any network.The research [6] has realized a NOC for parallel DES computation. The ciphers, which are earlier to AES such as DES, Triple DES, can be broken with ease on modern computation systems. The features such as resistance against known attacks, code compactness on many CPUs and design simplicity make the AES more secured and popular than DES[7].

MicroBlaze or Networked Processor Array (NePA) are the soft core processors. In Some papers [8][9][10], processing element in NOC are MicroBlaze or Networked Processor Array (NePA). These are used for DES implementation. But these cores have much more complicated functions than traditional DES needs. Thus adding soft cores becomes more expensive because of the remarkable increase of complexity. This restricts the performance enhancement .From the above discussion, the problem statement is NOC with Soft core DES as processing element will effectively increases the area and even DES is less secured than AES. The solution for this problem is discussed in Section II of this paper.Data encryption/decryption is essential in now a days for data protection .Hence paper presents a high performance NOC specific to cryptography. This paper demonstrates 4 X 4 Mesh based [11] NOC architecture with Deterministic X-Y routing algorithm [12] and Round Robin algorithm for arbitration. Here Processing Element (PE) does Advanced Encryption Standard (AES) computation.The flow of this paper is as follows: Section 2 illustrates the solution. Section 3 illustrates architecture of NOC. Section 4 illustrates experimental results. Last section concludes this paper.

2. SOLUTION
Since AES is more secured than DES, this paper presents a NOC for parallel AES computation as module without complicated deigns of pipeline and virtual channel technique. Hence proposed NOC is of low area consumption NOC.

3. ARCHITECTURE OF NOC
A typical NOC architecture consist of Routers, processing elements, network interface (NI) and links are the major components of a NoC architecture. The key component of

NOC architecture is router, which does the vital task of routing information from a source to its destination. The processing elements are computation part of network such as different or similar CPU/cores. The network interface detaches the computation part from the communication part and operates as a mediator between the processing element and the router. A link makes connection among routers in the NOC according to the selected topology. Network Topologies are chosen based on application requirements. The main factors of NOC design are discussed below.

3.1 Topology

The topology of a network is defined as an arrangement of components within a network, where it is related with the mapping of routing nodes and interconnecting links. Topologies used for on-chip networks are adopted from large-scale networks and parallel computing. Two-dimensional topologies can easily be mapped to the planar nature of a chip. Due to the regularity and linear area growth with the number of nodes, two dimensional mesh is most preferred topology in NOC[11]. Hence 2-D Mesh topology is used in proposed on-chip network is shown in Fig 1.

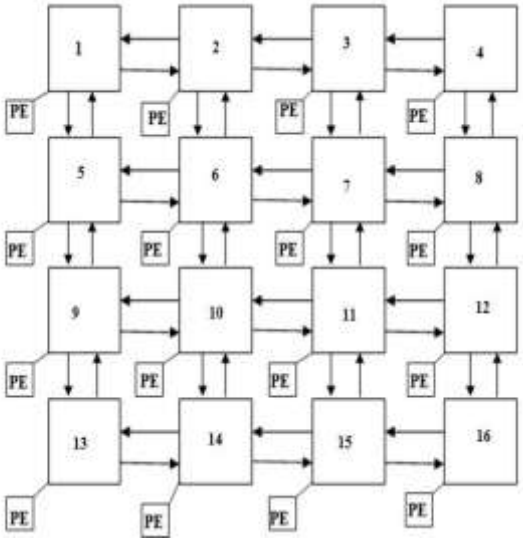

Fig 1: 4X4 Mesh Topology

3.2 Router

In NOC, router is the main part which routes an incoming packet based on routing algorithm to destination node .In order to keep implementation cost as low as possible, the router design should be simple .Hence the router which has been designed in this paper is not using pipelining and virtual channel techniques.The Fig 2 shows router operation. The packet arrived at each port will be stored into the respective port buffer to avoid the congestion. If more than one packet arrived simultaneously from different ports, then arbiter (Round –Robin arbiter) decides which packet has to be routed based on routing algorithm. X-Y routing algorithm is used in this paper for routing the packets within the network. A node where destination address matches with current node (source) address, then that node is the destination for the packet else routing will continue Based on X-Y routing algorithm till packet reaches its destination node.

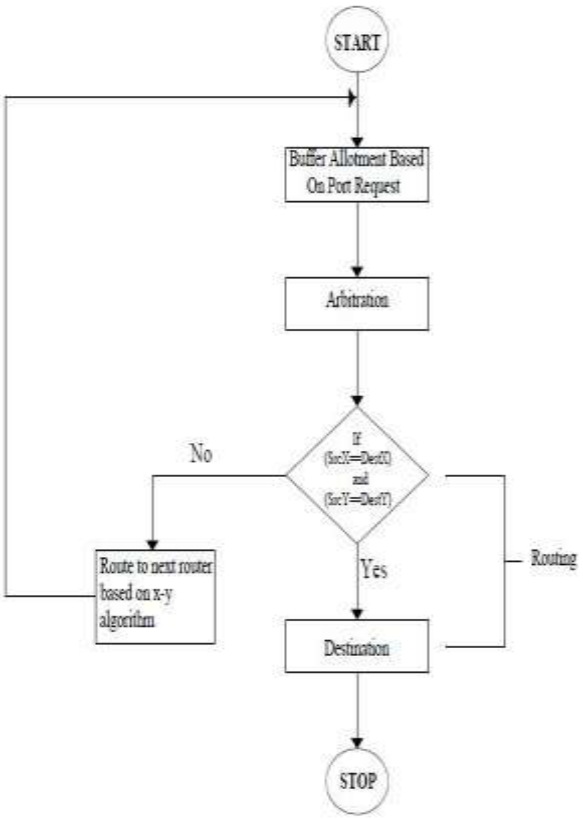

Fig 2: Flowchart of Router operation

3.2.1 Arbitration

The function which performs the allocation of a shared resource among multiple agents is called as arbitration. The control logic which performs the arbitration in router is called arbiter. The Fig 3 shows round robin arbitration.

Basically round robin arbitration is a simple time slice scheduling algorithm. In this paper, RR arbiter allots equal amount of time for each port request to access output port in a ring manner. Local, west, south, east and north, this is the sequence of output port allotment to different port request in the proposed RR arbiter.

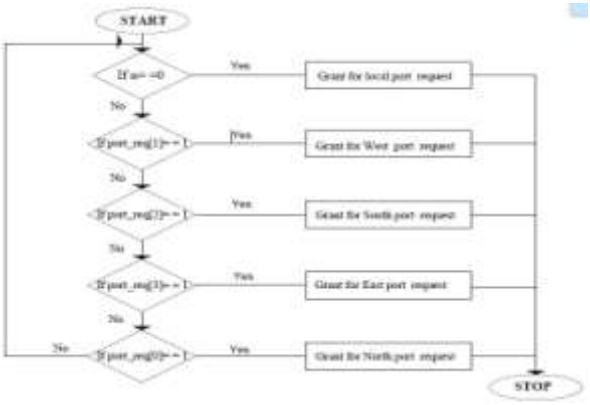

Fig 3: Flowchart of RR Arbitration.

3.2.2 X-Y Routing algorithm

The algorithm, which determines the path for a packet from source to the destination node is referred as routing algorithm. Deterministic and adaptive schemes are two main routing schemes in NOC. In Deterministic routing scheme, the path

between a Source and destination node is predefined by source and destination addresses. In an adaptive routing scheme, there are many paths from source to destination node, so paths are not fixed .Path selection are made on a per-hop basis at each routing node. As a result, adaptive routing is more difficult for implementation in order to provide flexibility in load balancing. In this paper, a popular deterministic routing scheme named as X-Y routing which is better for mesh and tori based NOC, is used [12] . In XY routing, a packet traverses along a row first, then traverses along the proper column to the destination. The Fig 4 shows flowchart of X-Y routing algorithm.

3.3 Processing Element

In this paper, processing element of NOC performs AES (Advanced Encryption Standard) computation. The key size as well as data size in AES is 128 bits. The number of iterations required to complete one AES operation is 10.

Address of each node is represented with coordinate(X, Y) for X-Y routing algorithm implementation. Source node address is referred as (srcx, srcy), whereas (destx, desty) as destination node address. The X-Y routing algorithm compares source node address (srcx, srcy) with the destination address (destx, desty) of the packet to be route. As per X-Y routing algorithm packet has to be routed along row(X-coordinate) first, then along the column. Therefore, first srcx is compared with destx. If srcx is less than destx then the packet will be routed to the west, else packet will be routed to East if srcx is greater than destx .

On which node, srcx is equals to destx, is the final node for horizontal routing of a packet. Now the srcy of a node, where srcx = destx ,is compared with desy. If srcy is less than desy then packet will be routed to North else packet will be routed to South. While routing vertically if srcy = desy in any node , then that is the destination node of a packet. In destination node srcx = desx and srcy = desy.This is how proposed paper presents implementation of X-Y routing algorithm.

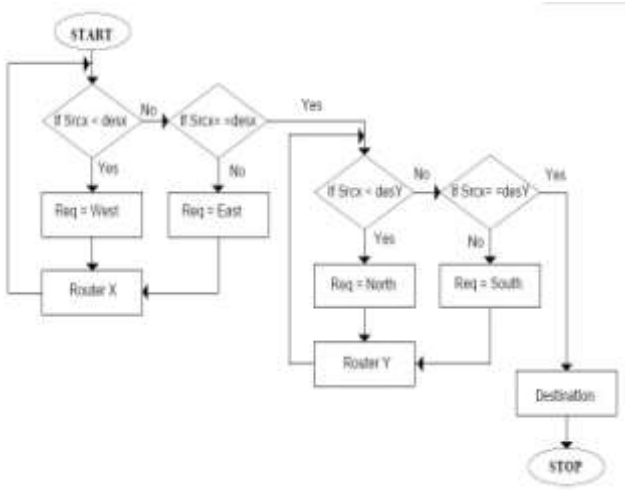

Fig 4: Flowchart of X – Y Routing Algorithm

4. EXPERIMENTAL RESULTS

4.1 Experimental Setup

The complete NOC design has done in Xilinx ISE 13.2 targeting on XC5VLX220-2FF1760 device. All simulations done in Modelsim - 6.3C.

4.2 Simulation results

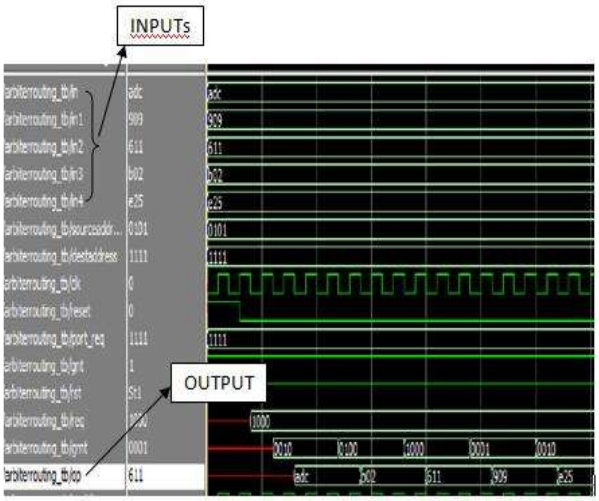

Fig 5: Waveform of R

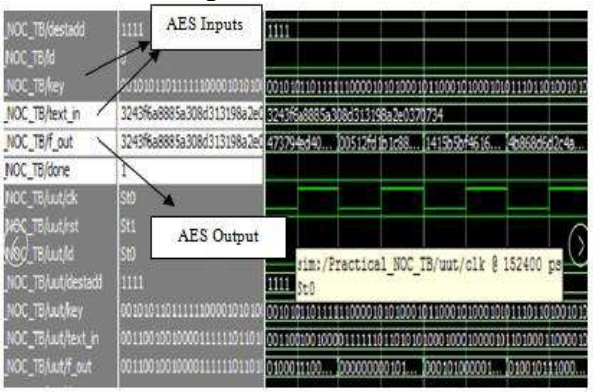

Fig 6: waveform of AES Output

The fig 5 shows wave form of a router. Router inputs are in(Localin),in1(West), in2(South),in3(East) and in4(North) outputs are req and op. The Fig 6 shows waveform of AES computation. In this waveform, key is 128 bit key, text_in is 128 bit data ,these are the inputs. whereas f_out is AES output.

4.3 Synthesis results

4.3.1 Area Utilization Results

The area utilization of proposed NOC and previous work is shown in Table I.

Table I: Area Utilization Result

Work	Slice Usage	
	Register	LUT
Proposed NOC	0.008%	5%
Previous Work[6]	13%	24%

4.3.2 RTL Schematic

Fig 7: RTL Schematic of proposed NOC

5. CONCLUSION

The AES of 128key is implemented with less number of rounds as compared with DES implementation with higher security and opposition against the unauthorized users. Higher throughput AES Computation can be achieved by mesh based NOC without virtual channel and pipeline technique. From Table I, the proposed 4X4 Mesh based NOC having AES as PE consumes comparatively 10% -20% lesser area than previous work [6].

Future work will focus on implementation of Key Manager in AES Computation and modified extended XY routing. This routing algorithm gives possible shortest path for packet to reach its destination. Hence performance of NOC can be further improved.

6. REFERENCES

[1] L. Benini and G. De Micheli, ―Network on Chips: A New SoC Paradigm‖, Proc. IEEE Transactions on Computers, Vol.35 No.1, January 2002, 70-78.

[2] P. Pratim Pande, C. Grecu, M. Jones, A. Ivanov, and R. Saleh, ―Performance evaluation and design trade-offs for network-on-chip interconnect architectures‖, IEEE Transactions on Computers, vol. 54, no. 8, pp. 1025-1040, 2005.

[3] ARTERIS. 2005. *A comparison of network-on-chip and buses*. White paper.

[4] T.T.-O. Kwok and Y.-K. Kwok. ―On the esign,Control, and Use of A Reconfigurable Heterogeneous Multi-core System-on-a-Chip‖. In IPDPS 2008, pages 1–11,Apr.2008.

[5] A. Lee, NIST Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government, National Institute of Standards and Technology, ovember 1999.

[6] R. Yuan,*S.-J. Ruan and J. G¨otz* **"**A Practical NoC Design for Parallel DES Computation‖ In International symposium on VLSI Design, Automation, and Test, April – 2013.

[7] J.Daemen and V. Rijmen, ―The block cipher Rijndael, Smart Card research and Applications‖, LNCS 1820, Springer-Verlag, pp. 288-296.

[8] H.C. Freitas, L.M. Schnorr, M.A.Z. Alves, and P.O.A. Navaux. ―Impact of Parallel Workloads on NoC Architecture Design‖. In Parallel,Distributed and Network-Based Processing (PDP), 2010 18th Euromicro International Conference on, pages 551– 555, Feb. 2010.

[9] X. Li and O. Hammami. ―An Automatic Design Flowfor Data Parallel and Pipelined Signal Processing Applications on Embedded Multiprocessor with NoC: Application to Cryptography‖. Int. J. Reconfig. Comput., 2009, Jan. 2009.

[10] Y.S. Yang, J.H. Bahn, S.E. Lee, and N. Bagherzadeh. ―Parallel and Pipeline Processing for Block Cipher Algorithms on a Network-on-Chip‖. In ITNG 2009, pages 849–854, Apr. 2009.

[11] Sonal S. Bhople and M. A. Gaikwad **"** A Comparative Study of Different Topologies for Network-On-Chip Architecture‖,International Journal of Computer Applications (0975 – 8887) Recent Trends in Engineering Technology-2013

[12] Aline Vieira de Mello, Luciano Copello Ost,Fernando Gehm Moraes, Ney Laert Vilar Calaza ―Evaluation of Routing Algorithms on Mesh Based NoCs*"* Technical report series number 040 may, 2004.