FPGA Implementation of Modified Secured Web Server

Dr.K.V.Karthikeyan[#1], K.Gomathy [#2]
[#1] Professor, Sathyabama University,
Chennai, Tamilnadu, India-600119
kandvas@yahoo.com
[#2] Assistant Professor, Velammal Institute of Technology,
Chennai, Tamilnadu, India-601 204
gomathykannan@yahoo.com

***Abstract*-- Demand for High speed portable networks impels compulsory optimization in various aspects. A common web server is to act as a central control point which responds to the user request, and employing a high sophisticated computer for this purpose is not obligatory. This Paper focuses on a portable low power automated web server in a FPGA platform by accomplish the Network on chip concept. This web server has the capability to adapt multipurpose operation, a client can share the web content not only the HTML files but also can control a device operated in a remote place through this web server. In accession a modified Elliptic curve cryptographic architecture is implemented to fortify the communication of server to client system. The ECC is coalition with Montgomery multiplication for certain advantage like minimum register usage.**

Keyword - Montgomery Multiplication, Reconfigurable, Elliptic Curve Cryptography

I. INTRODUCTION

The hackneyed purpose of the web server is to share the suitable complete information among the users in secured manner. The secured information sharing is corroborating with the use of Elliptic curve cryptography (ECC)[9]. The ECC is chosen because the high security obtained with less key length.

The FPGA web server is endow in secured manner using ECC and embrace Montgomery arithmetic method in ECC to reduce the no of logical elements, worse case time and power consumption.

The HTML web pages are collected in external Static Dynamic (SD) card in encrypted format using ECC security method. A web browser interface will be developed either .NET or JAVA script. An Ethernet interface will be developed using VHDL language for the interaction of Altera NIOS II trainer FPGA kit and client computer. The clients may be increased by implementing a proper router design. The router actually works on shortest path implementation and finding a correct end client. Web browser designs entangle suitable login name and password. If password is authentic the elliptic curve cryptography will decrypt the HTML pages and approbation the display in viewable form. The HTML pages are formed with link for reference with other related documents by using a HTML language. Bus arbiter, buffer, Elliptic curve cryptography and Ethernet module are created using VHDL language. A system on chip builder (SOPC builder) is used to create the Ethernet controller, bus arbiter and NIOS CPU instruction etc variable clock frequency generator will be supplied using PLL module using IP mega core.

The active modules are as follows

- Buffer
- Memory
- Key generation
- Encryption
- Decryption
- Montgomery multiplication

Buffer is used as a cache for speed matching between transmitter and receiver. If the intermediate storage is not there suppose the data coming from transmitter is ready but at all the case the receiver may not be available. So at that time the probability of data loss is high. The Memory is used to store data pages, software program and instruction set. The SRAM cell is designed. It is set in different options. One option is as inactive. Other is getting the data and another one is loading a data. The key generation, encryption and decryption in ECC are entangling for secured communication of web pages and the third person should not embezzle information. The most important in ECC security method is key pair generation which actually invigorates the security.

The Montgomery multiplication is utilized in ECC for modular multiplication that makes the exponent multiplication operations into simple one, thereby reducing the huge register usage. It is especially advantage

when exponent and the modulus number are too high. It may not be very advantages if the exponent number is too small. The main part of the Montgomery multiplication is it uses limited no of registers. If the register size is reduced that entice reduction in area and power consumption.

II. DESCRIPTION

A. Block Diagram

The FPGA inbuilt with NIOS II processor act as a web server for serving the information to web users [1]. The information is stored using SD card in the HTML format. The information is encrypted using Encryption formulas followed in ECC.

B. System Client

A client is nothing but a computer which needs service from server in form of displaying the particular related all information. A request is raised from client side by entering a keyword of the information need to be displayed.

C. Central HUB

The purpose of the central HUB is used to serve for more than one client shown in Fig.1

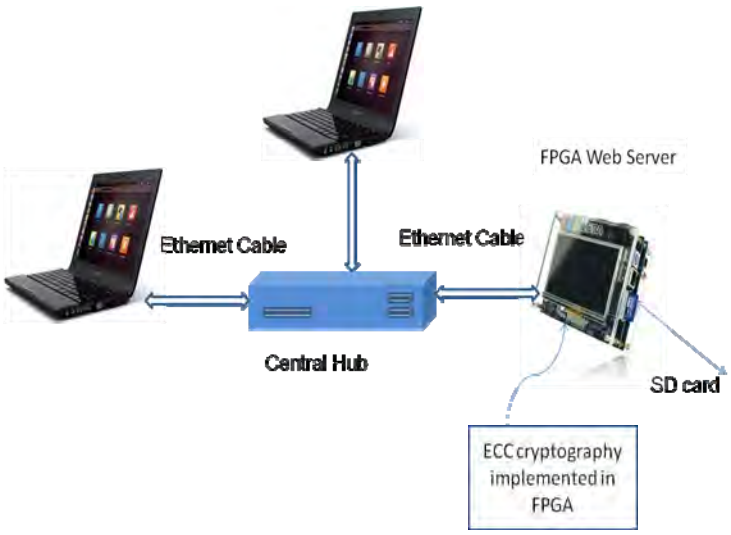

Fig. 1: General Diagram

III. SYSTEM DESIGN

This design example shows a HTTP server using the sockets interface of the NicheStack™ TCP/IP Stack Nios II Edition on MicroC/OS-II to serve web content from the DE2-115 board[2,3,4]. The server can process basic requests to serve HTML, JPEG, GIF, PNG, JS, CSS, SWF, ICO files from the Altera read-only .zip file system.

The following describes the related SOPC system. The SOPC system used in this demo contains Nios II processor, On-Chip memory, JTAG UART, timer, Triple-Speed Ethernet, Scatter-Gather DMA controller and other peripherals etc. In the configuration page of the Altera Triple-Speed Ethernet Controller, users can either set the MAC interface as MII or RGMII.

Once the Triple-Speed Ethernet IP configuration has been set and necessary hardware connections have been made as shown in Fig. 2, FPGA web server is implemented using ALTERA NIOS II board.

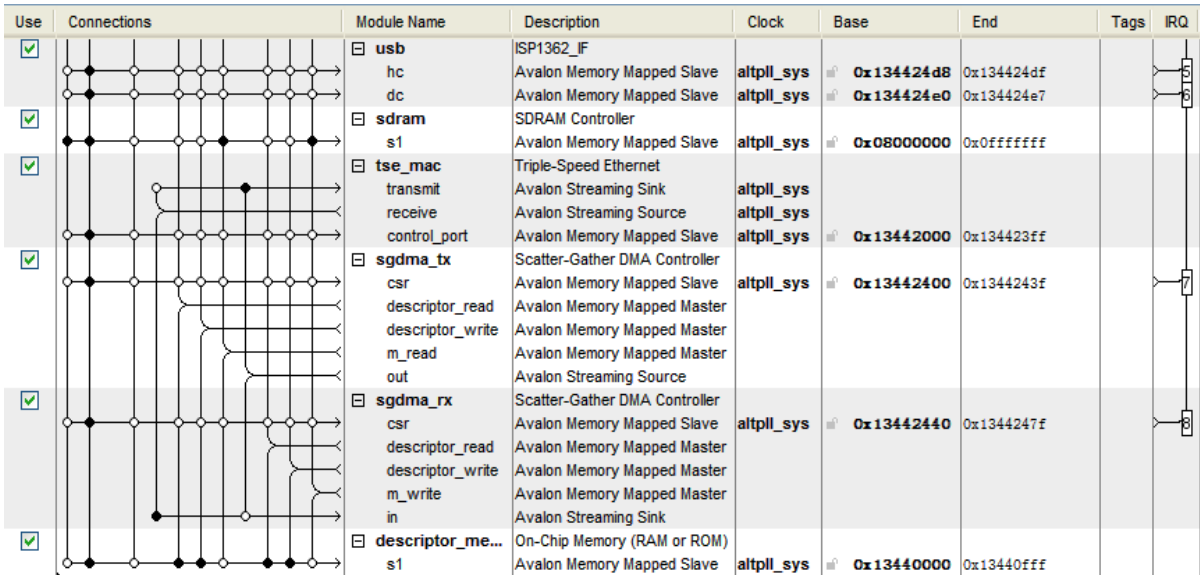

Fig . 2: SOPC builder connections

A. NIOS processor

A Nios II processor [15] includes a processor, some peripherals and memory on a single chip as shown in Fig. 3. A Nios II processor system has its own instruction set and programming model.

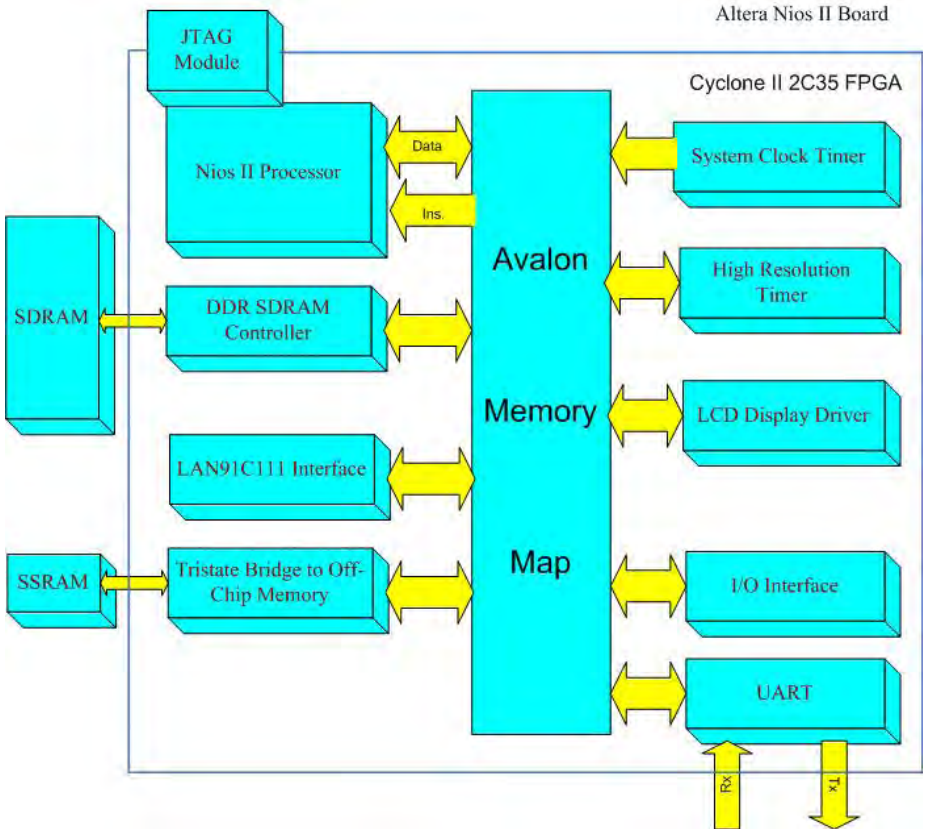

Fig. 3: ALTERA Nios II Board

B. *ECC Cryptography*

The ECC cryptography is the most secured method that is achieved with less key size [9, 13].

The encryption formula:

Cipher text=message data^ public key mod N

The decryption formula:

Message data= cipher text^ private key mod N

The public and private keys are formed based on certain rules mentioned in ECC.

SD card:

The SD card is storage unit of non-volatile type. It is available in different physical size. The information is secured by setting a password in card.

C. HTML page

The data is available in HTML format, which propagate from one link to another link.

IV. PROPOSED METHOD

A. Montgomery Arithmetic

Several modular multiplications are involved in ECC. The encryption formula is $y=b^{\wedge a} \bmod m$

The multiplication come modular operation is done at each single level and the immediate results are stored in temporary registers and the same steps are repeated till the exponent or index value exceeds [10, 14]. For example consider a number 2 with exponent value 5 and the final result is stored in the output register y.

E.g. 2^5 mod 3

A= (2x2) mod 3

A= (Ax2) mod 3

A= (Ax2) mod 3

A= (Ax2) mod 3

output Y= A mod n the simulation output of implementing Montgomery multiplication for the example is obtained as below. By viewing the simulation output as in Fig. 4, flow summary as in Fig. 5, power analyzer as in Fig. 6 and timing analyzer as in Fig. 7 using Quartus II software. The parameters like area, power and time have been improved.

B. Output

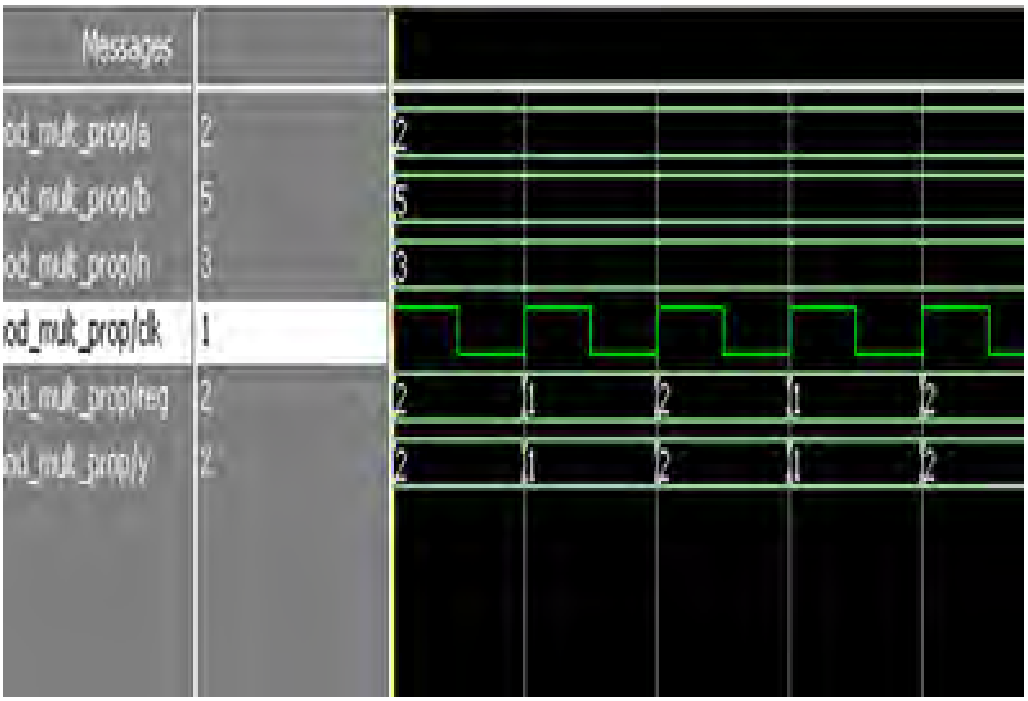

Fig. 4 :Output

Flow summary:

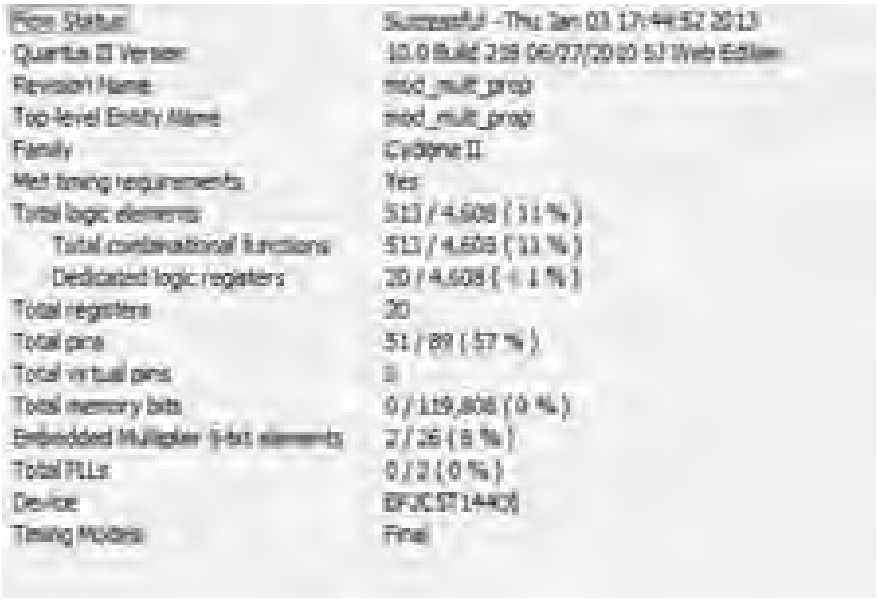

Fig. 5: Flow summary

Power analyzer result:

Fig. 6: Power Analyzer result

Timing analyzer result:

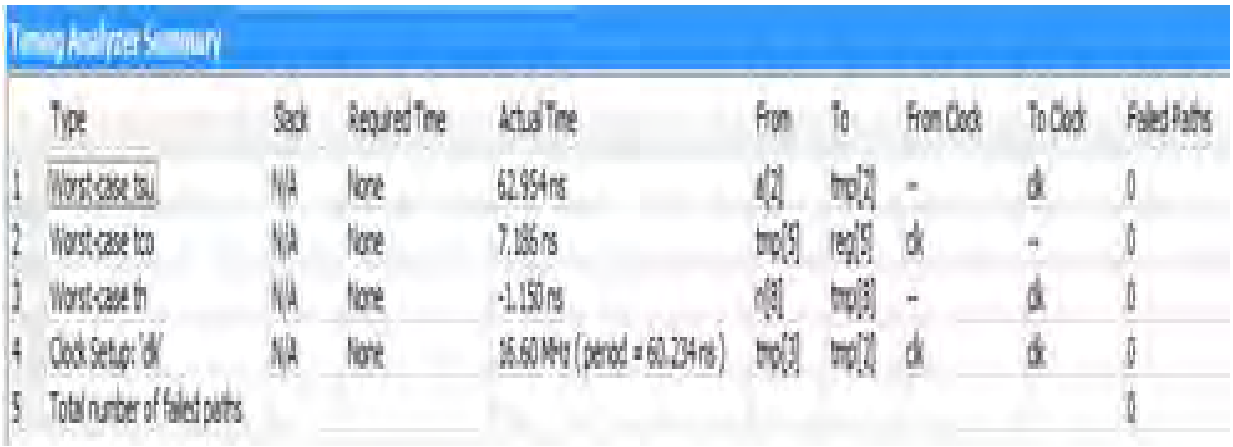

Fig.7 Timing analyzer result

The comparison table reveals that Montgomery Multiplication is efficient.

TABLE I

Comparison parameters	**Existing method**	**Proposed method**
Total logic elements	1523/4608(33%)	513/4608 (11%)
Total combinational functions	1523/4608(33%)	513/4608 (11%)
Dedicated logic registers	64/4608 (1%)	20/4608 (<1%)
Maximum time utilized	150.692ns	62.954ns
Total thermal power dissipation	37.70mw	35.11mw
Total pins	73/158 (46%)	51/89 (57%)

V. SYSTEM IMPLEMENTATION

The FPGA web server is designed with the Quartus II software tool which has a SOPC builder. The SOPC builder software is used to create a chip with custom application.

The steps involved in creating a custom chip are

- Create a new project.
- Click Tools menu in that select SOPC builder.
- Select the Avalon component which is needed for the application.
- Run the program
- The message is displayed as “system generation was successful”. It indicates that the program was successfully created.

A. FPGA web server

The Ethernet controller and TCP/IP protocol are generated with the help of SOPC builder [11, 12]. The ECC cryptography with Montgomery multiplication is integrated with SOPC generated program. The final program is downloaded in the ALTERA kit to design the web server. The results are shown below.

Comparison Table II explains between existing and proposed of FPGA web server obtained using tool Quartus II

TABLE II

Comparison parameters	**Existing method**	**Proposed Method**
Total logic elements	12,703	11,220
Total combinational functions	10,118	8,861
Dedicated logic registers	8,296	7,498
Total thermal power dissipation	1093.40mw	1005.55mw
Total pins	487	487

B. Web server Automation

The file sharing concept of web server can be enhanced with system controlled automation of remote devices. DE2 FPGA web server can be designed to work in dual mode for html file sharing and also for device controlling as shown in Fig.8. An Ethernet cable connected with the FPGA server used to initiate TCP/IP Protocol and a dedicated USB Blaster cable is used as a control interface to control the SERVER connected device[5,6,7]. The tool control module of WEB server is shown in figure 8.

A GUI Interface is developed for user interaction with button controls; the controlling module is designed to process the kit level components like LED, SEVEN SEGMENT and VGA Devices [8].

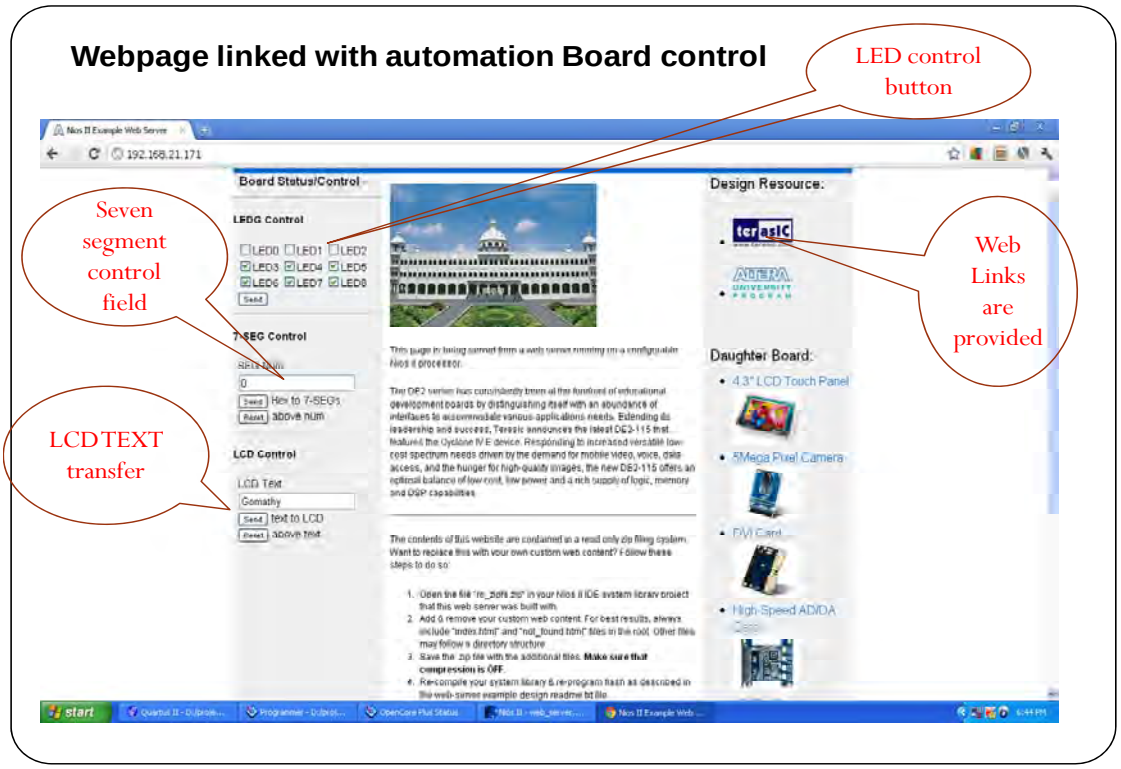

Fig. 8 :Webserver output screen

VI. CONCLUSION

The NOC design of secured web server is successfully designed and implemented using ALTERA CYCLONE IV DE2 FPGA Board. The HTML files with JPEG, bmp images can be served through triple speed reconfigurable Ethernet port between FPGA server and client. The performance comparison existing elliptic cryptography with the modified ECC is tabulated by means of Power, delay time and area. The web server is designed with FPGA inbuilt with Nios II processor allows more flexibility in usage of different peripherals, interfaces and controllers thereby it is apparent to install in different application. The hardware design board of DE2 FPGA is configured using high level VHDL Language with low power elliptic curve cryptography. User authentication logic is developed in C++ language to encrypt and decrypt the HTML contents.

The web server logic for HTML file sharing and device control module is merged into a single entity, from which a client user can select any mode as per requirement.

REFERENCES

[1] Altera Corporation."Ethernet and the NicheStack TCP/IP Stack,"in *Nios II Software Developer's Handbook*. [online] Available at www.altera.com [Nov. 21, 2010].
[2] Interniche technologies, inc. Internet: www.iniche.com/nichestack.php.[Nov. 22, 2010].
[3] AlteraCorporation.Internet: www.altera.com,[Nov.22, 2010].
[4] Altera Corporation,altera *DE2 Development and Education Board User Manual*,2006
[5] Altera Corporation.(2010).*Avalon Interface Specifications* [Online] Available:ww.altera.com[Nov 23,2010].
[6] Altera Corporation.(2009).*Quartus II Handbook Embedded Peripherals* Version 9.1. [Online].Available: www.altera.com [Nov23,2010].
[7] Altera Corporation.(2010).*Embedded Peripherals IP User Guide.*[On-line].Available: www.altera.com[Nov 23,2010].
[8] Altera Corporation.(2009).DDR and DDR2 SDRAM Controller Compiler User Guide.[On-line].Available: www.altera.com [Nov23,2010].
[9] V.Miller, "Uses of elliptic curves in cryptography",Crypto 1985, LNCS 218: *Advances in Cryptology, Springer*-Verlag, 1986.
[10] Montgomery Multiplication Duncan A. Buell , October 11, 2005
[11] E.Mohan and C. Puttamadappa , "VLSI Implementation of TCP/IP Stack", *European Journal of Scientific Research*, Vol.22 Issue 2, pp 296-302, Oct 2008
[12] *Ethernet and the NicheStack TCP/IP Stack* - Nios II Edition
[13] S.V.Sandeep, I.Hameem Shanavas and V.Nallusamy, "Hardware Implementation of Elliptic Curve Cryptography over Binary Field", *International Journal of Computer and Information Security*, Vol.2, pp. 1-7, 2012
[14] Montgomery Multiplication Algorithmic and Hardware Implementations Allen Michalski ,November 6th, 2002
[15] Rami Amiri, Omar Elkeelany, "*An Embedded TCP/IP Hard Core for SmartGrid Information and Communication Networks*", in proceedings of the IEEE Southeast Symposium on System Theory SSST'12, Florida, 2012.