Implementation of Secured Embedded Web server on FPGA

Mrs.K.Sasikala M.E., Mrs.S.Kalaivani M.Tech

yDepartment of ECE , Thangavelu engineering college, Karapakkam, Chennai-97

Abstract- The implementation of web server using Altera Nios II embedded IP core makes best solution for conventional heavy weight web server can be replaced by substituting FPGA based web server providing high speed, Low power consumption, reduced cost. The web server hosts the pages, scripts, programs, and multimedia files and serves them using TCP/HTTP designed to send files to web browsers. In Nios II soft processor approach, designers can make a perfect fit in terms of processors, peripherals, memory interfaces, performance characteristics and cost. ECC (Elliptic Curve Cryptography) is integrated with in the source code of web server to achieve secure communication. ECC is particularly useful in applications where memory, bandwidth and/or computational power is limited.

Index Terms- HTTP/TCP, NIOS II , FPGA, ECC

I. INTRODUCTION

A web server is a computer that delivers web pages to other computers in the network. Every web server has a unique IP address and possibly a domain name. Any computer can work as web server by installing server software. Web server can communicate with the web browser through TCP/HTTP. The web server accepts requests from web browsers and returns the appropriate documents. The web server hosts the web pages and serves them using Hyper-Text Transfer Protocol (HTTP), designed to send files to web browsers protocols.

World Wide Web (WWW) is the user-friendly interface, in which that image, formatted text, video, and audio are available. Users can access their equipment from any browsers. One of the most popular protocol suites is TCP/IP[13] which is the heart of Internetworking communications. The Internet Protocol [13] is responsible for addressing hosts and routing datagram's (packets) from a source host to the destination host across one or more IP networks. TCP/IP is responsible for breaking data down into IP packets before they are sent, and for assembling the packets when they arrive. The IP, the Internet Protocol, is responsible for exchanging information between routers so that the routers can select the proper path for network traffic, while TCP/IP is responsible to ensure the data packets are transmitted across the network reliably and error free.

A microcontroller with an embedded TCP/IP stack called an "Embedded Web Server" [9] sends pages over a physical layer connection to a remote computer with a browser. The browser reads the Hyper-Text Markup language (HTML) formatting and displays a page in the browser window. The user can send data to the Server stack through a form on the web page, the form data is sent over the physical connection and is received by the TCP/IP stack in the remote microcontroller.

Field Programmable Gate Array (FPGA) is the only solution for satisfying all the requirements from user side in (a) Speed (b) Stability (c) Economic (d) Flexibility. If the FPGA is chosen according to its high performance, the web server becomes more effective. By considering this a newly evolving FPGA platform Nios II processor[1] kit supports of 25000 logic elements from the ALTERA vendor is prescribed in this research to achieve maximum reliability using soft core processors. A soft core processor is a microprocessor fully described in software, usually in HDL, which can be synthesized in programmable hardware, such as FPGA.

II. NIOS II SYSTEM

The proposed web server is implemented on NIOS II embedded processor. The Nios II processor is a general-purpose RISC processor with embedded peripheral architecture.The Nios II processor system is equivalent to a microcontroller or "computer on a chip" that includes a processor and a combination of peripherals and memory on a single chip. A Nios II processor system consists of a Nios II processor core, a set of on-chip peripherals, on-chip memory, and interfaces to off-chip memory, all implemented on a single Altera device. The Quartus II software and is available to all Altera customers. It automates the task of integrating hardware components into a larger system. It can specify the system components in a graphical user interface (GUI), and generates the interconnect logic automatically

The Nios II processor and the interfaces needed to connect to other chips on the DE2 board are implemented in the Cyclone II FPGA chip. These components are interconnected by means of the interconnection network called the Avalon Switch Fabric. Avalon Interface: It simplifies system design by allowing easily connection for several components in an FPGA. The Avalon switch fabric enables multiple, simultaneous data transactions for unmatched system Throughput.

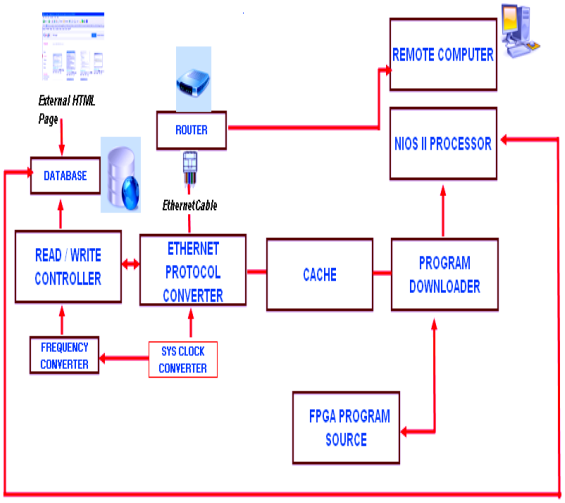


Figure 1: System Circuit diagram

The memory blocks in the Cyclone II device can be used to provide an on-chip memory for the Nios II processor. The SRAM, SDRAM and Flash memory chips on the DE2 board are accessed through the appropriate interfaces. Parallel and serial input/output interfaces provide typical I/O ports used in computer systems. A special JTAG UART interface is used to connect to the circuitry that provides a Universal Serial Bus (USB) link to the host computer to which the DE2 board is connected. This circuitry and the associated software are called the USB-Blaster. Another module, called the JTAG Debug module, is provided to allow the host computer to control the Nios II system.

It makes it possible to perform operations such as downloading programs into memory, starting and stopping execution, setting breakpoints, and collecting real-time execution trace data. Since all parts of the Nios II system implemented on the FPGA chip are defined by using a hardware description language (HLD).

III. CRYPTOGRAPHY AND ALGORITHM

The Cryptography is the science of using mathematics to hide or protect information from unauthorized users, which aims to provide all of the services known as confidentiality, integrity and authentication, access control, non- repudiation.

Encryption and Decryption

The process of making the information unreadable is called encryption or enciphering. The result of encryption is a cipher text or cryptogram. Reversing this process and retrieving the original readable information is called decryption or deciphering. To encrypt or decrypt information, an algorithm or so-called cipher is used.

A Cryptographic algorithm is controlled by a secret key, sometimes called password. Only those who are authorized to read the information know the key. Without knowing the key, it should be impossible to reverse the encryption process, or the time to attempt to reverse the process should required take so much time that the information would become useless.

Elliptic Curve Cryptography (ECC)

For the purpose of cryptography, an elliptic curve can be thought of as being given by an affine equation of the form y2 = x3 + ax + b, where a and b are elements of a finite field with pn elements, where p is a prime larger than 3.(The equation over binary and ternary fields looks slightly different.) The set of points on the curve is the collection of ordered pairs (x, y) with coordinates in the field and such that x and y satisfy the relation given by the equation defining the curve, plus an extra point that is said to be at infinity. The set of points on an elliptic curve with coordinates in a finite field.

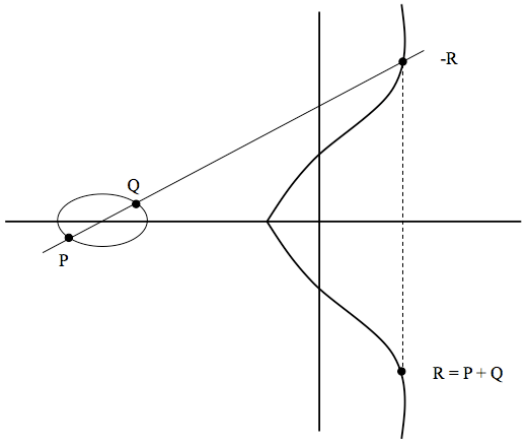


Figure.2.Group law on an Elliptic Curve

Elliptic Curve Cryptography (ECC) has been regarded mature to provide robustness for secure data transaction. Compared with RSA, ECC can supply equivalent level of security with a much smaller key length. Therefore, ECC has become an attractive alternative cryptosystem and many designs have been proposed in recent years among them, there are dual-field ECC implementations that support both binary field GF(2m).

The primary advantage is that ECC is based on either integer factorization or the discrete log problem in the multiplicative group of a finite field in the absence of a sub exponential-time algorithm.

- ECC uses smaller key size as compared to RSA. As a result it achieves greater speed and less storage.
- Key pair generation is much faster than other algorithm.
- Greater flexibility.

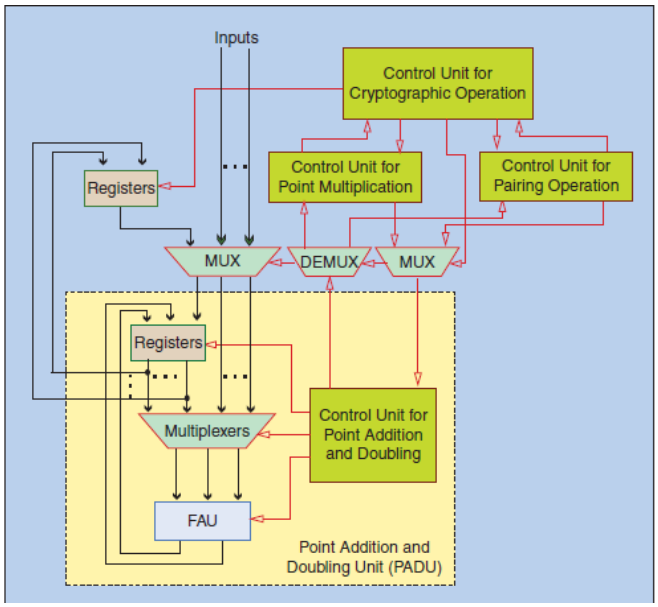


Figure 3.Bock diagram of ECC

The following table to demonstrate the key size relationship between ECC and RSA

Table 1.ECC VS RSA Comparision

ECC Key Size	RSA Key Size	Key-Size Ratio
163	1,024	1:6
256	3,072	1:12
384	7,680	1:20
512	15,360	1:30

Since the ECC key sizes are so much shorter than comparable RSA keys, the length of the public key and private key is much shorter in elliptic curve cryptosystems. This results into faster processing times, and lower demands on memory and bandwidth. ECC[12] is faster than RSA for signing and decryption, but slower for signature verification and encryption. ECC is particularly useful in applications where memory, bandwidth and/or computational power is limited (e.g., a smartcard) and it is in this area that ECC use is expected to grow.

ALGORITHM

Input: A point P = (x, y), an l-bit integer k = (kl−1, . . . , k1, k0).
Output: Q = kP.
1: $X_1 = x$, $Z_1 = 1$, $X_2 = x4 + \beta$, $Z_2 = x_2$.
2: for i = l−2 to 0 by −1 do
3: if ki = 1 then
4: $(X_1,Z_1) = Madd(X_1,Z_1,X_2,Z_2)$, $(X_2,Z_2) = Mdouble(X_2,Z_2)$
5: else
6: $(X_2,Z_2) = Madd(X_1,Z_1,X_2,Z_2)$, $(X_1,Z_1) = Mdouble(X_1,Z_1)$
7: end if
8: end for
9: $Q = Mxy(X_1,Z_1,X_2,Z_2)$
10: $Madd(X_1,Z_1,X_2,Z_2)$ // Point Addition
11: $Z3 = (X_1 \times Z_2 + X_2 \times Z_1)2$, $X_3 = x \times Z_3 + (X_1 \times Z_2) \times (X_2 \times Z_1)$
12: $return(X_3,Z_3)$
13: $Mdouble(X_1,Z_1)$ // Point Double
14: $Z_12 = Z_12 \times X_12$,$X_12 = X_14 + b \times Z4$
15: $return(X_2,Z_2)$
16: $Mxy(X_1,Z_1,X_2,Z_2)$ // Coordinate Conversion
17: $X = X_1/Z_1$, $Y = (x+X) \times (y+x2 + (X_2/Z_2 + x) \times (X1/Z1 + x))/x+y$
18: return(X,Y)

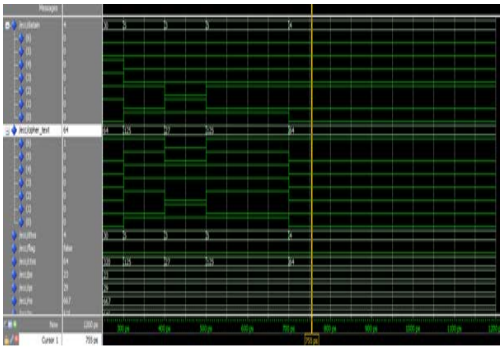
HARDWARE AND SOFTWARE TOOLS

- Modelsim
- Altera's Quartus II software and SOPC Builder
- Nios II IDE
- The Nios Development Board, Cyclone II

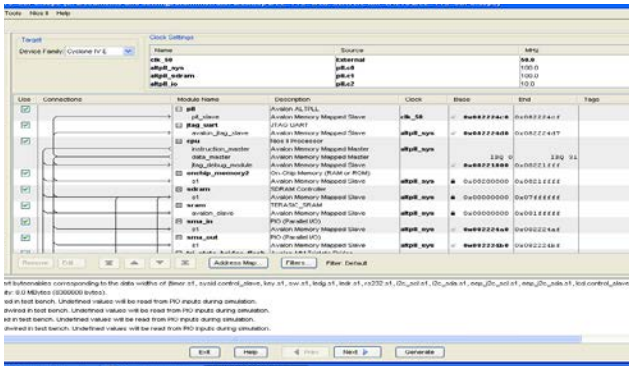
SIMULATION RESULT

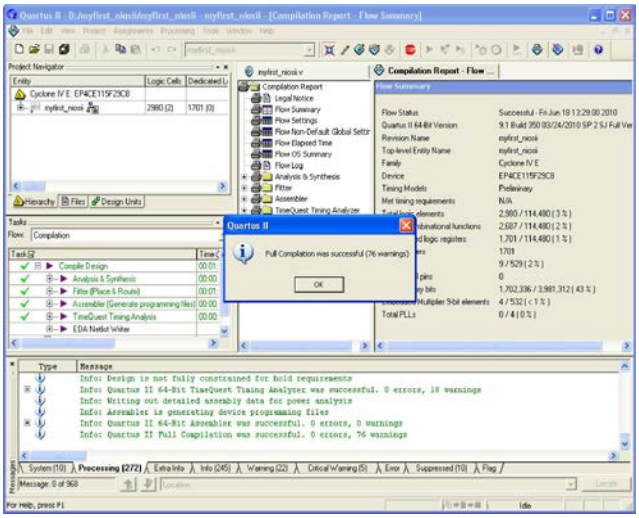
The web server is implemented using NIOS II altera board provides area and power consumption. The web pages can be shared with registered clients also the security achieved through ECC

SIMULATION RESULT FOR THE ENCRYPTION&DECRYPTION

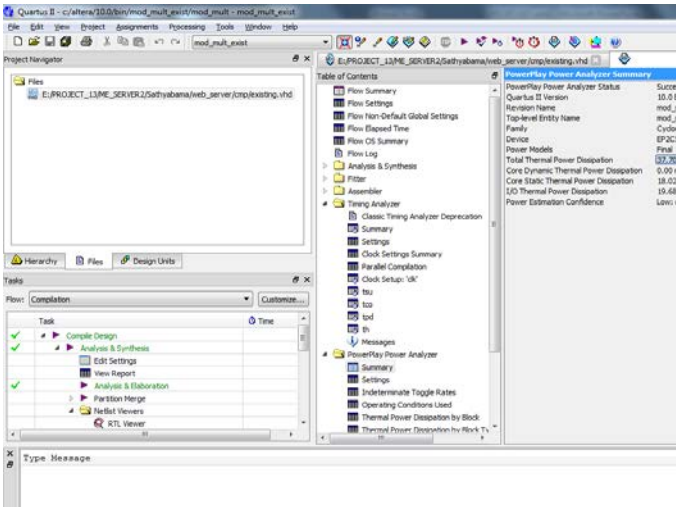


SYNTHESIS REPORT FOR NIOS II PROCESSOR AND PERIPHERIAL GENERATED

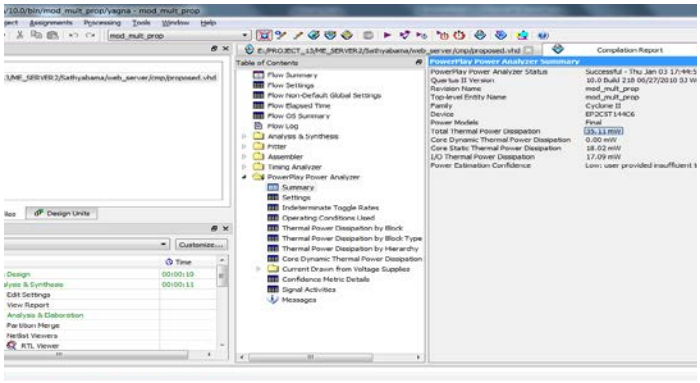




SYNTHESIS REPORT FOR ECC:



SYNTHESIS REPORT FOR MONTGOMERY ECC:



IV. CONCLUSION

Implementing Nios II processor on FPGA allows more flexibility on both hardware and software. ECC provides time as well as power consumption too. This makes it an ideal choice for portable, mobile and low power applications. It can be a very secure and useful replacement of already being used cryptosystems for key exchange, key agreement and mutual authentication After downloading the VHDL software program to the FPGA Hardware the synthesis report from the Kit supporting software is tabulated by means of (a) speed (b) logic elements used (c) power consumption .The web pages can be shared with registered clients via Ethernet cable by issuing a TCP/IP request. The web pages are filtered according to the authorization of the end user.

References

REFERENCES

[1] Altera Corporation, (2010) 'Nios II Software Developer's Handbook' 1. Chapter 11: Ethernet and the Niche Stack TCP/IP Stack - Nios II Edition

[2] Auer (2005) 'Embedded Web Server Technology for Remote Online Labs' IEEE ISIE , Dubrovnik, Croatia

[3] Blum.T and Paar.C (1999) 'Montgomery modular multiplication on reconfigurable hardware'. In Proceedings of the 14th IEEE Symposium on Computer Arithmetic (ARITH-14), pages 70-77

[4] Da Liu, Jian-rong Gong,(2002)'System-programmable Chip (SOPC) Design And Development Strategies' Modern Electronic Technology, Pp.76- 77

[5] Fielding.R, (1996) 'Hypertext Transfer Protocol - HTTP/1.0' RFC

[6] Guajardo.J and Paar.C (1997) 'Efficient Algorithms for Elliptic Curve Cryptosystems' vol. 1294, pringer-Verlag, pp. 342–56.

[7] Hankerson.D (1965) 'Software implementation of elliptic curve cryptography over binary fields. In Cryptographic Hardware and Embedded Systems LNCS, pages 1–24.

[8] Hong-bo Zhang, Zi-shan (2003)'SOPC Applied System Research and Design Based on NIOS Processor' Electron Mass,vol.1pp. 84-86.

[9] Ian Agranat, "Embedded Web Servers in Network Devices," Communication Systems Design, March 1998, pp. 30-36.1999.

[10] Lixia Liu(2010)'Research on Technology of Embedded Web Server Application Information Management and Engineering (ICIME)', 2nd IEEE International Conference

[11] Nivedita N. Joshi, Dakhole P. K, Zode "Embedded Web Server on Nios II Embedded FPGA Platform" Second International Conference on Emerging Trends in Engineering and Technology, ICETET -09

[12] Rosing.M (1999)'Implementing Elliptic Curve Cryptography' Manning Publications Co.Stevens,TCP/IP Illustrate,(1994)Volume 1: The Protocols. Addison-Wesley Professional Conference.

[13] Tenca.A.Koc.C.k: 'A Scalable Architecture for Modular Multiplication Based on Montgomery's Algorithm',(2003) IEEE Transactions on Computers, No 9., (52), pp. 1215-1225

[14] Yang C.C,Chang T.S, and Jen C.W, "A new RSA cryptosystem hardware design based on Montgomery's algorithm", IEEE Trans. Circuits and Systems II: Analog and Digital Signal Processing, vol. 45, pp. 908 –913, July 1998.

[15] www.Altera.com,(2009)'Quartus II Handbook Version 9.1 Volume 5: Embedded Peripherals'

[16] www.Altera.com,(2010)"Embedded Peripherals IP User Guide"

[17] www.Altera.com,(2009)"DDR and DDR2 SDRAM Controller Compiler User Guide".

[18] Zhan mei-qiong (2008)'Research and Implementation of Embedded Web Server',International Conference on Multimedia and Information Technology DOI 10.1109/MMIT.

[19] ZhouChuanShen(2007)'implementation of a General Reduced TCP/IP Protocol Stack for Embedded Web Server for Intelligent Information Hiding and Multimedia Signal Processing', IIHMSP Third International Conference.

AUTHORS

First Author – Mrs.K.Sasikala M.E, Department of ECE , Thangavelu engineering college, Karapakkam, Chennai-97
Second Author – Mrs.S.Kalaivani M.Tech, Department of ECE , Thangavelu engineering college, Karapakkam, Chennai-97