UNIVERSITI PUTRA MALAYSIA

DEVELOPMENT OF AN 8-BIT FPGA-BASED ASYNCHRONOUS RISC PIPELINED PROCESSOR FOR DATA ENCRYPTION

PANG WAI LEONG

DEVELOPMENT OF AN 8-BIT FPGA-BASED ASYNCHRONOUS RISC PIPELINED PROCESSOR FOR DATA ENCRYPTION

By

PANG WAI LEONG

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, In Fulfilment of the Requirements for the Degree of Master of Science

September 2003

Abstract of thesis presented to the Senate of University Putra Malaysia in fulfilment of the requirements for the degree of Master of Science

DEVELOPMENT OF AN 8-BIT FPGA-BASED ASYNCHRONOUS RISC PIPELINED PROCESSOR FOR DATA ENCRYPTION

By

PANG WAI LEONG

September 2003

Chairman: Roslina Mohd. Sidek, Ph.D.

Faculty: Engineering

Microprocessors are widely used in various applications. One of the application is in the area of data security where data are encrypted and decrypted before and after transfer via communication channel. The microprocessor design can be categorized into two types, which are synchronous and asynchronous processors. The asynchronous processor may offer better speed improvement because it is self-timed where a control circuit will generate enable signals for all instruction executions based on the request and acknowledgement signals. Unlike the asynchronous design, synchronous design requires global clock. The clock must be long enough to accommodate the worst-case delay.

In this work, an 8-bit asynchronous processor is designed based on a synchronous RISC pipelined processor architecture. The synchronous processor consists of three stages. They are instruction fetch stage, instruction decode stage and execution stage. The reduce instruction set computer (RISC) architecture is used to minimize the instruction and to perform specific operation. To design the

asynchronous processor, an asynchronous control circuit is added to synchronous design. The asynchronous control circuit is designed based on handshake protocol.

Both the synchronous and asynchronous designs are applied fully using VHDL. The MAX+PLUS II is used as the simulation tools to design and for design verification. The UP1 education board that contains the FLEX10K chip is used to observe the hardware operation.

The asynchronous processor was successfully designed with higher million instructions per second (MIPS) and higher operation frequency as compared to synchronous processor. The asynchronous processor has 10.772 MIPS and operated under frequency of 11.16MHz. The asynchronous processor design consumed 63% of the total logic cells in FLEX10K chip. The processor fits in FLEX10K and provides extra spaces for future expansion.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

PEMBANGUNAN PEMPROSES TAK SEGERAK RISC BERSALUR MENGGUNAKAN FPGA BAGI PENGENKRIPTAN DATA

Oleh

PANG WAI LEONG

September 2003

Pengerusi: **Roslina Mohd. Sidek, Ph.D.**

Fakulti: **Kejuruteraan**

Pemproses banyak digunakan dalam pelbagai kegunaan. Salah satu kegunaan pemproses adalah mengenkript dan mendekript sebelum dan selepas penghantaran maklumat melalui saluran komunikasi untuk keselamatan maklumat. Rekaan pemproses bolek dibahagikan kepada dua jenis, iaitu jenis pemproses segerak dan tak-segerak. Pemproses tak-segerak boleh mempertingkatkan kepantasan operasi. Pemproses tak-segerak adalah pemasa sendiri, dimana litar kawalan tak-segerak akan menjanakan isyarat pemboleh untuk melaksanakan semua arahan bergantung kepada isyarat permintaan dan perakuan. Berbeza dengan rekaan tak-segerak, rekaan segerak memerlukan jam global. Jam yang digunakan perlu cukup lama untuk memuatkan lambatan kes paling buruk.

Satu pemproses tak-segerak direka bergantung kepada pemproses segerak RISC bersalur. Pemproses segerak mempunyai tiga peringkat, iaitu tahap menghantar arahan, tahap membahagi arahan dan tahap pengendalian. Set arahan RISC digunakan untuk mengurangkan bilangan arahan dan menjalankan operasi

tertentu sahaja. Untuk merekabentuk pemproses tak segerak, satu litar pengawal tak-segerak ditambahkan kepada rekaan segerak. Litar pengawal tak-segerak direkakan menggunakan protokol jabat-tangan.

VHDL digunakan sepenuhnya dalam kedua-dua rekaan segerak dan tak-segerak. Program MAX+PLUS II digunakan merekabentuk dan juga untuk mengesahkan rekabentuk. Peralatan UP1 yang mengandungi chip FLEX10K digunakan untuk meneliti operasi perkakasan tersebut.

Pemproses tak-segerak berjaya dicipta dengan lebih banyak arahan dapat dikendalikan sesaat dan lebih tinggi kelajuan pemprosesan dibandingkan dengan pemproses segerak. Pemproses tak-segerak dapat mengendalikan 10.772 MIPS dan berfungsi dibawah kelajuan 11.16MHz. Pemproses tak-segerak menggunakan 63% jumlah logik dalam FLEX10K. Pemproses dapat dimuatkan dalam FLEX10K dan terdapat ruang lebihan untuk perubahan di masa depan.

ACKNOWLEDGEMENTS

A sincere appreciation is delivered to my project supervisors, Dr. Roslina Mohd. Sidek, Mr. Wan Zuha and Mr. Rahman Wagiran for their invaluable guidance, constructive suggestions and encouragement throughout the duration of this project.

I also wish to extend my deepest personal thanks to my dearly coursemates to whom I owe my sincere appreciation. They are Mr. Yeong Tak Nging and Mr. Kenny Gan, who have help to accomplish this project.

Lastly, I would like to express my sincere appreciation to my family especially my parents for their undying love and support. I also would like to thank my friend, Miss Ivy Ling for her care and love. All of that have enabled me to complete the project successfully.

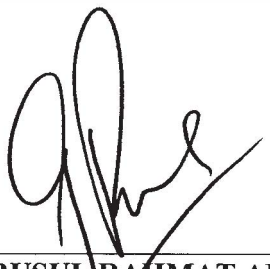
I certify that an Examination Committee met on 5th September 2003 to conduct the final examination of Pang Wai Leong on his Master of Science thesis entitled "Development of an 8-bit FPGA-Based Asynchronous RISC Pipelined Processor for Data Encryption" in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulations 1981. The Committee recommends that the candidate be awarded the relevant degree. Members of the Examination Committee are as follows:

S.S. Jamuar, Ph.D.
Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Roslina Mohd Sidek, Ph.D.
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Rahman Wagiran
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Wan Zuha Wan Hasan
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)



GULAM RUSUL RAHMAT ALI, Ph.D.
Professor/Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 08 DEC 2003

This thesis submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirements for the degree of Master of Science. The members of the Supervisory Committee are as follows:

Roslina Mohd Sidek, Ph.D.
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Rahman Wagiran
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

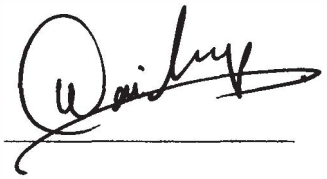
Wan Zuha Wan Hasan
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

AINI IDERIS, Ph.D.
Professor/Dean
School of Graduate studies
Universiti Putra Malaysia

Date: 8 JAN 2004

DECLARATION

I hereby declare that the thesis is based on my original work except for quotations and citations, which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UPM or other institutions.



(PANG WAI LEONG)

Date: 1/12/03

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ADDR	Input address
ADDRA	Address A
ADDRB	Address B
ADDRT	Destination address
ALU	Arithmetic Logic Unit
ALUOP	Arithmetic Logic Unit operation code
ARC	Asynchronous register control
ARCB	Basic module of the ARC design
ARCO	Optimised asynchronous register control
AUP	Asynchronous processor
AUPO	Optimised asynchronous processor
BEQ	Branch if equal
BNE	Branch if not equal
BRANCH	Branch address generator
BRANCHAD	Branch address
BRANCHM	Branch module
C	CARRY/BORROW
CC	Condition code
CI	Carry inputs port
CLK	Clock
CNF	Compile Netlist Files
CO	Carry output port
COND	Condition
CRYPT	Cryptography
CTR	Control signal
CTRLUNIT	Control unit
DATAA	Data A
DATAB	Data A
DATAI	Data input
DEC	Decrypt
DES	Data Encryption Standard
DECODE7	7-output decoder
DIN	Data input
DMEM	Data memory
DOUT	Data output
DSA	Digital Signature Algorithm
EAB	Embedded Array Block
EDIF	Design Interchange Format
EN	Enable
EN1, EN2, EN3	Enable 1, 2 and 3
ENC	Encrypt
ENCODE2	2-input encoder
ENCODE3	3-input encoder
ENCODE7	7-input encoder
FIFO	First-in first-out

FPGA	Field Programmable Gate Array
GPR	General-purpose register
GPRFILE	General-purpose register
HEX	Hexadecimal
HIF	Hierarchy Interconnect File
IC	Integrated circuit
ID	Instruction decode module
IDATA	Data input
IE	Execution module
IFE	Instruction fetch module
IMEM	Instruction Memory
IMM	Immediate
INC1	Increase one
INSTDEC	Instruction decoder
INSTR	16-bit instruction code
INSTRIN	16-bit instruction
JUMP, JUMPA	Jump address
LATCON	Latch controller
LC	Logic cell
LCELL	Buffer
LDB	Load
LED	Light emitting diodes
LPM	Library of Parameterised Modules
LSB	Less significant bit
LUT	Look-up table
MC	Muller-C
MEC	Mutual exclusive circuit
MEMAD	Memory address
MEMWR	Memory write
MSB	Most significant bit
MUX2	2-input multiplexer
MUX2SEL	Multiplexer select signal generate module
MUX3I	3-input multiplexer
MUX4	4-input multiplexer
MUX8	8-inputs multiplexer
N	NEGATIVE
NPC	Next program counter
OFF	Jump address
OP	Operation code
OPCODE	Operation code
PC	Program counter
PCADD1	PC value added by one
PLD	Programmable Logic Device
POF	Programmer Object Files
RA	Register A data
RB	Register B data
RAM	Random Access Memory
RAOUT	Register A content
RBOUT	Register B content

REG1	Single-bit register
REG10	10-bit register
REG16	16-bit register
REG4	4-bit register
REG8	8-bit register
REGWR	Register write
RESET	Reset signal
RISC	Reduced Instruction Set Computer
ROM	Read Only Memory
RSA	Riverst, Shamir and Adleman
RT	Register destination address
RTADDR	Register destination address
SEGDEC	Seven segment display decoder
SEL	Select Signal Generate
SNF	Simulator Netlist File
SOF	SRAM Object Files
SRAM	Static Random Access Memory
SUP	Synchronous processor
TTF	Tabular Text Files
V	OVERFLOW
VHDL	Very High Speed Hardware Description Language
VITAL	VHDL Initiative Toward ASIC Libraries
WR	Write enable
XOR	Exclusive OR
Z	ZERO
ZE	Zero

CHAPTER 1

INTRODUCTION

Processor is invented in early 1970s, the first 4-bit processor is developed at 1971. The processor gives deep impact to the industrial electronics revolution and also many other fields. The development of the processor is very fast in the past 30 years. The same computation ability and faster response available in a small hand-held calculator compare to the first electronic computer that consists of 18,000 vacuum tube and large space consumed, plus require a good cooling system. The modern processors become smaller and the capability is increased comparing the conventional processor.

The processor is designed for multiple usages and suitable for all kind of digital or analog operation. The processor is capable to do the complex computation or controlling operation. Processor is widely used in a variety of applications that require complex and advance operations for process or control purposes, or some simple application. The processor gives a high accuracy, shorter operation period and complex calculation to various applications.

The computer architecture increases the complexity of processors to complex instruction set computer (CISC) architectures. CISC aims to supply more support for high-level languages and operating system, as the fabrication technology is capable to fabricate more complex integrated circuit (IC). It has to become more complex as the technology advances enable it to include more complex operation on VLSI

devices. The CISC become more complex because it requires longer design cycle and hard to be fully tested.

The processor may not be fully utilized during the instruction execution. Since only part of the processor is used for the instruction execution. The processor can be utilized by braking the instruction cycle to a sequence steps that each separation will take a fraction of time to complete the entire instruction. This can be achieved by separating the processor to few stages and each stage performing different operation.

In this age of universal electronic connectivity that full of viruses, hackers, electronic eavesdropping and electronic fraud, data security becomes important and highly demanded. The growth in computer system and the networking highly depends on the information stored and communication of both organizations and individuals using the computer networking. This causes higher demand to protect the data and resources from disclosure. A way should be figured out to guarantee the authenticity of data and messages, and to protect systems from network-based attacks. Cryptography ability should be added for the data security purposes. The processor must provide the data encryption and decryption to protect the privacy of the information. There are various types of cryptographic algorithms. The three of the most common algorithms are Data Encryption Standard (DES), Rivest, Shamir, and Adleman (RSA), and Digital Signature Algorithm (DSA).

Programmable Logic Device (PLD) is used for the design application to reduce the design cycle time and for the system verification purposes. PLD can be

reprogrammed for the system modification or programmed for other system. This reduces the design cost and simplicity the design modification. The PLD can be categorized to two types, which are the conventional and modern PLD. The conventional PLD are programmable logic array (PLA) and programmable array logic (PAL). The modern PLD are Complex Programmable Logic Device (CPLD) and Field Programmable Gate Array (FPGA). The modern PLD are reprogrammable and have larger storage spaces as compared to the conventional PLD.

Research Objective

The main objectives of the research are to design an 8-bit asynchronous pipelined Reduced Instruction Set Computer (RISC) processor with cryptography using Very High Speed Hardware Description Language (VHDL). The self-timed asynchronous system can generate the clock internally when the job occurs to replace the global clock signal used in synchronous system.

The RISC architecture gives simple, fixed length instruction formats that allows fast hardwired decoding and greatly simplify adopting the pipelining architecture. RISC eliminates the microcoded routines and turns the low-level control of the machine over the software.

The pipelining architecture adopted to utilize the processor usage and performance. The instruction execution is split in few steps; each step consumes one

clock cycle and use part of the processor. Up to the number of steps that the instructions can be executed concurrently.

The simple data encryption system (DES) is added to provide cryptography services in the processor. The DES algorithm can no longer be considered computationally secure, but it is still used because it is easy to apply.

The synchronous processor is tested using MAX+PLUS II software and developed using the VHDL. The processor is tested using ALTERA Field Programmable Gate Array (FPGA) chip. UP1 Education Board is used for the hardware verification purposes. Asynchronous register control module, which provides the enable signals for the processor, is designed for the asynchronous processor.

Both synchronous and asynchronous processors are tested using MAX+PLUS II for the processors' simulation, verification and timing analysis. The performances of both processors are compared for the performance comparison purpose.

CHAPTER 2

LITERATURE REVIEW

The literature review is focused on the following scope: the design tools used either full custom design or FPGA design, RISC and CISC, Pipelining and non-pipelined architecture, asynchronous and synchronous systems, module used for asynchronous design, cryptography algorithms, processors, synchronous processor modules and finally the conclusion.

There are many design method and tools available; the best and available software is selected for the simulation analysis. The RISC and CISC reviews are required to emphasize the advantages of RISC over the CISC in the processor design. The pipelining architecture review is used to identify the number of pipelining stages used in the processor invented in the past. The asynchronous and synchronous systems review is required to compare the advantage and drawback between these two systems. The extra components that may be used in the asynchronous design are also as part of this literature review. The knowledge and techniques available for the cryptography process are required to select the simplest technique for the processor application. Review on processors covers those available in market or in research. A synchronous processor that fulfills the requirement will be selected as the module for the asynchronous processor design.

2.1 Design Tools

Various computer aided design (CAD) tools are available in market for efficient, faster and economical digital design. The CAD tools are capable to support the digital design in all phases that are description or specification, and design or synthesis. The CAD tools can perform various optimizations to reduce cost and performance improvement [1,2]. The Altera (MAX+PLUS II) PLD software or the Xilinx (Foundation Series) PLD software can be used for the processor design. The Altera PLD software is the only one available in lab, so it is chosen as the simulation tools and the targeted PLD is Altera UP1 education board.

2.1.1 VHDL

VHDL is an industry-standard hardware description language, which describes the inputs and outputs, function and behavior of the design circuits. Two successive standards are used to define the language:

1. IEEE Std 1076-1987 or called "VHDL 1987".
2. IEEE Std 1076-1993 or called "VHDL 1993".

Both standards are fully integrated into MAX+PLUS II. The VHDL language is used to describe the hardware components or the systems. Therefore, many language features in VHDL are designed to support this desire.

VHDL constructs are powerful and versatile. The entire hierarchical of the system designs can be created with VHDL, or mix VHDL Design Files with other types of design files in a hierarchical design [13].

The VHDL used to document the digital electronic design. VHDL consists of several parts organized as shown below:

1. The actual VHDL language.
2. The additional data type declarations in the Package STANDARD.
3. The utility functions in the Package TEXTIO.
4. The WORK library reserved for the designers design.
5. A STD library that contain Package STANDARD and TEXTIO.
6. A vendor package.
7. Vendor libraries.
8. User libraries and packages.

The VHDL language is used to document the interconnection between the modules or components and the behavior of the digital system design. The VHDL description is used as input for the simulator to run with test cases. The VHDL design used as logic synthesizing tool input to produce tooling. The VHDL design able to be described with several levels of abstraction plus some details and explanation hidden to make it easier to read and understand. The designers are able to design in VHDL from top down with successive refinements and specifying more details of the design architecture [3].