Scholars' Press

Dhuha Basheer Abdullah
Riyadh Zaghlool Mahmood

FPGA-Based High Performance Parallel Computing

Dhuha Basheer Abdullah
Riyadh Zaghlool Mahmood

FPGA-Based High Performance Parallel Computing

Scholar's Press

Impressum / Imprint
Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Bibliographic information published by the Deutsche Nationalbibliothek: The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Coverbild / Cover image: www.ingimage.com

Verlag / Publisher:
Scholar's Press
ist ein Imprint der / is a trademark of
OmniScriptum GmbH & Co. KG
Heinrich-Böcking-Str. 6-8, 66121 Saarbrücken, Deutschland / Germany
Email: info@scholars-press.com

Herstellung: siehe letzte Seite /
Printed at: see last page
ISBN: 978-3-639-70858-5

Zugl. / Approved by: Mosul, University of Mosul, 2013

Dhuha Basheer Abdullah
Riyadh Zaghlool Mahmood

FPGA-Based High Performance Parallel Computing

Acknowledgement

I would like to express my deepest gratitude and thankfulness to my supervisor, Dr. Dhuha Basheer Abdullah, for her judicious guidance and valuable conduct, a special respect and esteem for her.

I would also like to thank the Dean of the college of computer sciences and mathematics, the venerable Dr. Dhafir Ramadhan Matar, and the honorable manager of the department of computer sciences, Dr. Manal Ali, and all of my honorable professors and lecturers for their great efforts exerted to accomplish this thesis.

Preface

This book is based on dissertation submitted for the fulfillment of the requirements of the Ph.D. in computer sciences/college of Mathematics and computer Sciences / university of Mosul by the second author and supervised, converted to a book by the first author. The dissertation earned the excellence degree after comprehensive discussion; an advice was given by the discussion committee to convert it to a book.

This book deals with parallel computing applications by using the Field Programmable Gate Array (FPGA) device which is characterized by high speed and flexibility. This device has the capability of re-organization of designed system requirements much easier in comparison with the Application Specific Integrated Circuit (ASIC) by the use of special programming language which is called Very high integrated circuit Hardware Description Language (VHDL).

The high performance of the FPGA device is due to its capability of implementing parallel computing by building parallel processing elements called virtual processors. So implementing any system based on this device will give faster and more precise results than these PCs, even if they use parallelism.

In this work, two systems based on FPGA device have been built for high performance computing (HPC). Code breaking for DES algorithm was chosen as case study. The first system was a parallel system consisting of 256 FPGA devices implemented in parallel manner. Each FPGA device contains 32 PEs (Processing Elements) operated also in a parallel fashion. Each PE represents one round from 16 of DES algorithm rounds. DES code-breaking needs 16.289 days by implementing this system. The second system was parallel-pipeline system consisting of 256 FPGA devices operated in a parallel way. Each FPGA device contains 4 PEs operated in parallel fashion. Each PE represents one DES algorithm with all 16 complete rounds.

List of Contents

Subject	Page
Chapter 1: Overview	
1.1 Overview	14
1.2 Related works	18
1.3 Thesis statement	25
1.4 Contribution	25
1.5 Thesis composition	25
Chapter 2: Parallel Processing	
2.1 Introduction	27
2.2 Parallel Processing Concept	27
2.2.1 The benefit of using Parallel Processing	27
2.2.2 Major applications of Parallel Processing	28
2.2.3 Parallel Processing in computers	29
2.3 Flynn's taxonomy of computer architecture	30
2.3.1 SIMD Architecture	32
2.3.2 MIMD Architecture	33
2.3.2.1 Shared memory organization	36
2.3.2.2 Message passing organization	39
2.4 Parallel computing	41
2.5 Dependencies	42
2.6 The PRAM model and its variations	43
2.7 Hardware and Software Parallelism	46
2.7.1 Hardware Parallelism	46
2.7.2 Software Parallelism	46
2.8 Levels of parallelism in program execution on modern computer	48
2.8.1 Instruction Level	49
2.8.2 Loop Level	49
2.8.3 Procedural Level	50
2.8.4 Subprogram Level	51

Subject	Page
2.8.5 Job (Program) Level	51
2.9 Speedup	52
2.9.1 Linear Speedup	52
2.9.2 Speedup Extreme	52
2.9.3 Super-Linear Speedup	53
2.10 Efficiency	53
2.11 Pipeline Computing	54
2.11.1 Concept and Motivation	54
2.11.2 Costs and Drawbacks	55
2.11.3 Linear Pipeline Processor	55
2.11.3.1 Asynchronous and Synchronous Models	55
2.11.3.2 Clocking and Timing Control	58
2.11.3.3 Speedup, Efficiency and Throughput	59
2.11.4 Nonlinear Pipeline Processors	60
2.11.5 Superscalar and Superpipeline Design	60
2.11.5.1 Super Pipeline Design	61
2.11.5.2 Superpipeline Design	65
Chapter 3: FPGA (Field Programmable Gate Array)	
3.1 Introduction	68
3.2 History	69
3.3 Applications	70
3.3.1 Applications in High Performance Computing	71
3.3.2 Application performance Measurement	72
3.3.3 CPU and FPGA Application Time	72
3.3.4 Relative Application Performance	73
3.4 Programming an FPGA	74
3.5 FPGA technologies	74
3.6 Types of FPGAs	75
3.6.1 Virtex-2 FPGAs	76
3.6.2 Spartan-3 FPGAs	76

Subject	Page
3.7 Configuration cells	78
3.7.1 CLBs and LABs	79
3.7.1.1 A Xilinx CLB slice	81
3.7.1.2 A Xilinx Spartan-3 Multipurpose LUT	82
3.7.1.3 A Xilinx Logic Cell	83
3.7.2 Input/output Blocks (IOBs)	84
3.7.3 Other Components of Spartan 3 FPGAs	85
3.7.3.1 RAM Blocks and Multipliers in Xilinx FPGAs	85
3.7.3.2 Embedded RAMs	86
3.7.3.3 Digital Clock Manager (DCM)	87
Chapter 4: VHDL	
4.1 Introduction	88
4.2 Design Flow	89
4.3 Translation of VHDL Code into a Circuit	90
4.4 Fundamental VHDL Units	92
4.4.1 Library Declarations	93
4.4.2 ENTITY	95
4.4.3 ARCHITECTURE	96
4.5 Creating a Test Circuit	97
4.6 Programming the FPGA	100
Chapter 5: FPGA parallel & pipeline system design	
5.1 Introduction	106
5.2 Breaking Encryption Algorithms	106
5.3 Brute Force Attack	107
5.4 Case Study	107
5.5 The Concept of Breaking the DES Code Algorithm	107
5.6 Selecting FPGA Device-Type Spartan 3	108
5.7 Components both system design	108
5.8 First System Architecture	108
5.8.1 The Number of DES Algorithms Built within a	110

Subject	Page
Single FPGA Device	
5.8.2 The System Model	111
5.8.3 Partitioning PC1 Key for Each FPGA Device	112
5.8.3.1 A 43-Bit Counter	112
5.8.3.2 A 5-bit PE	113
5.8.3.3 An 8-Bit FPGA	113
5.8.4 Main Control Unit	114
5.8.4.1 Input Signals	115
5.8.4.2 Output Signals	117
5.8.4.3 "Main Control Unit" Processes	120
5.8.5 Processing Elements (PEs)	125
5.8.5.1 Input Signals	125
5.8.5.2 Output Signal	128
5.8.5.3 PE's Processes	128
5.9 Dependency principle for FPGA parallelism	130
5.10 Dependency principle for DES Algorithms (PEs)	132
5.11 Second System Architecture	134
5.11.1 The number of DES algorithms Built in a Single FPGA	134
5.11.2 System Design Principle	135
5.11.3 Partitioning the PCI key of each FPGA	139
5.11.4 Main Control Unit	139
5.11.5 Process Elements (PEs)	140
Chapter 6: FPGA parallel & pipeline system implementation	
6.1 Introduction	142
6.2 First System Testing	142
6.3 Execution Steps	142
6.3.1 First Experiment for the 1st Key Breaking	144
6.3.1.1 Key Generation	144
6.3.1.2 Encryption	146
6.3.1.3 Code Breaking	147

Subject	Page
6.3.1.4 Decryption	154
6.3.2 completing 1st System test	154
6.4 Second System Testing	154
6.5 Discussion of Results	156
6.5.1 First System Results	156
6.5.2 Second System Results	161
6.6 Two system design comparison	165
6.7 Comparison of DES Code-Breaker systems	165
6.8 Minimizing time required to break DES key	166
6.9 Speed Up for both systems design	167
6.10 Efficiency for both systems design	169
Chapter 7: Conclusions and future works	
7.1 Conclusions	170
7.2 Future works	172
References	173
Appendices	
Appendix-A	183
Appendix-B	201
Appendix-C	203

List of Figures

Figure Name	Page
Figure (2-1): SISD Architecture	31
Figure (2-2): SIMD Architecture	31
Figure (2-3): MIMD Architecture	31
Figure (2-4): SIMD Architecture model	32
Figure (2-5): Two SIMD schemes	33
Figure (2-6): Shared memory versus message passing architecture	35
Figure (2-7): UMA(SMP) shared memory system	37
Figure (2-8): Two NUMA shared memory system	38
Figure (2-9): COMA shared memory system	39
Figure (2-10): Generic model of message –passing multicomputer	41
Figure (2-11): PRAM model for parallel computations	45
Figure (2-12): Executing an example program by two issue super scalar processor	48
Figure (2-13): Levels of parallelism in program execution on modern computers	50
Figure (2-14): Two models of linear pipeline units and the corresponding reservation table	57
Figure (2-15): A two-issue superscalar processor and a sample program for parallel execution	63
Figure (2-16): Superpipelined processor architectures without and multiple instruction issues, respectively	67
Figure (3-1): CPU based Application Time	72
Figure (3-2): FPGA Based Application Time	73
Figure (3-3): Spartan-3 FPGA XC3S1000	77
Figure (3-4): Top-down view of simple FPGA architecture	78
Figure (3-5): A CLB containing four slices(the number of slices depends on the FPGA family)	80
Figure (3-6): A slice containing two logic cells	81
Figure (3-7): CLB slice structure	82
Figure (3-8): Multipurpose LUT	83
Figure (3-9): Simplified view of a Xilinx Logic Cell	84
Figure (3-10): Basic I/O Block Structure	64

Figure Name	Page
Figure (3-11): RAM Blocks and Multipliers in Xilinx FPGAs	85
Figure (3-12): The functions forming a MAC	86
Figure (3-13): embedded RAM blocks	87
Figure (3-14): A clock manager generates daughter clocks	87
Figure (4-1): Summary of VHDL design flow	89
Figure (4-2): Full-adder diagram and truth table	90
Figure (4-3): Example of VHDL code for the full-adder unit of Figure (4-2)	90
Figure (4-4): Examples of physical circuits obtained from the full-adder code of Figure (4-3)	91
Figure (4-5): Simulation results from the VHDL design of Figure (4-3)	92
Figure (4-6): Fundamental section of a basic VHDL code	93
Figure (4-7): Fundamental part of a LIBRARY	94
Figure (4-8): Signal mode	96
Figure (4-9): NAND gate	96
Figure (4-10): Project setup	98
Figure (4-11): 4-input NAND gate	98
Figure (4-12): Edit Constrain	99
Figure (4-13): Constraints file	99
Figure (4-14): Generate Programming File	100
Figure (4-15): JTAG cable	101
Figure (4-16): Generate Programming File	101
Figure (4-17): Configure Devices	101
Figure (4-18): Automatic connection to cable	102
Figure (4-19): Auto detect the FPGA	102
Figure (4-20): Selecting .bit file	102
Figure (4-21): Warning about the "JTagClk" being changed	103
Figure (4-22): Programming Flash-Rom	103
Figure (4-23): Program	103
Figure (4-24): Verifying	104
Figure (4-25): Programming	104

Figure Name	Page
Figure (4-26): programming Succeeded	104
Figure (4-27):Testing	105
Figure (5-1): General system structure for DES code breaker	109
Figure (5-2): Block diagram of DES code breaker	110
Figure (5-3): Block diagram of Internal structure of each	112
Figure (5-4): Key Partition	112
Figure (5-5): Block diagram of the "Main Control Unit"	115
Figure (5-6): 16-digit Key Display in scanning mode	120
Figure (5-7): Flow chart of Counter and Round Generator	122
Figure (5-8): Flow chart of the Found Key	123
Figure (5-9): Flow chart of Key Display	124
Figure (5-10): Block diagram of one of (32) PEs	125
Figure (5-11): Flow chart of DES Process	129
Figure (5-12): Flow chart of comparison process	130
Figure (5-13): Second General System Structure for DES Code Breaker	135
Figure (5-14): Block diagram of Internal structure of each FPGA	136
Figure (5-15): Block diagram of Pipeline architecture	138
Figure (5-16): Key Partition	139
Figure (5-17): Block diagram of the Main Control Unit	140
Figure (5-18): Block diagram of one of (4) PEs	141
Figure (6-1): Key with 3-Minute Counter	145
Figure (6-2): Timing Diagram of Key Generation or("000000430E2340" 56-Bit Hex)	146
Figure (6-3): Plaintext Encryption with ("010408010B0E1504" 64-Bit Hex) Key	146
Figure (6-4): Entering Plaintext and Ciphertext into the Main Control Unit related with ("010408010B0E1504" 64-Bit Hex) Key	147
Figure (6-5a): Synthesizing	149
Figure (6-5b): Timing Summary	149
Figure (6-6): Implementation	150

Figure Name	Page
Figure (6-7): Generating Program File	151
Figure (6-8): Programming the FPGA	151
Figure (6-9): ("010408010B0E1504" 64-Bit Hex) Key Search	153
Figure (6-10): Code Breaking for("010408010B0E1504" 64-Bit Hex) key	153
Figure (6-11): Decryption using Key_1	154
Figure (6-12): ("020226231532321C"Hex) Key Search	155
Figure (6-13): Code Breaking for Key ("020226231532321C" Hex)	156
Figure (6-14): Differences in time for different number of PEs related with FPGA	159
Figure (6-15): Differences in time for different number of FPGAs related with PE	160
Figure (6-16): Differences in time for different number of PEs related with FPGA	163
Figure (6-17): Differences in time for different number of FPGAs related with PE	164
Figure (6-18): Speedup of the first system design	168
Figure (6-19): Speedup of the second system design	168

List of Tables

Subject	Page
Table (5-1): Permutation Choice1^{-1}	121
Table (6-1): First system testing values	143
Table (6-2): Design Summary	139
Table (6-3): Second system testing values	155
Table (6-4): DES Code Breaker time comparison based on the differences between FPGA numbers and PE numbers/system 1	158
Table (6-5): DES Code Breaker time comparison based on the differences between FPGA numbers and PE numbers/system 2	162
Table (6-6): Comparison of DES Code-Breaker systems	165

List of Abbreviations

Abbreviation	Definition
ADC	Analog to-Digital Converter
AES	Advanced Encryption Standard
ASIC	Application Specific Integrated Circuit
BRAM	Block RAM
BSP	Burroughs' Scientific Processor
CLB	Configurable Logic Block
Clk	Clock
CMOS	Complementary of Metal Oxide Semiconductor
COMA	Cache-Only Memory
CPLD	Complex Programmable Logic Device
CPU	Central Processing Unit
CR	Concurrent Read
CT	Cipher Text
CW	Concurrent Write
DAC	Digital to-Analog Converter
DCM	Digital Clock Manager
DDR	Double-Data-Rate
DES	Data Encryption Standard
DNA	Deoxyribonucleic Acid
DRAM	Distributed RAM
DSP	Digital Signal Processing
E	Extended Bit Selection
e_RAM	Embedded Random Access Memory
ER	Exclusive Read
EW	Exclusive Write
FFT	Fast Fourier Transform
FIFO	First-In-First-Out
FPAA	Field Programmable Analog Array
FPGA	Field Programmable Gate Array
HDL	Hardware Description Language