ENHANCE IMPLEMENTATION OF EMBEDDED CONCURRENT DES FUNCTIONAL UNITS USING SPATIAL PARALLELISM APPROACH ON FPGA FOR BETTER THROUGHPUT

RANA KHAZAAL KHUDHAIR

UNIVERSITI MALAYSIA PERLIS
2015

ENHANCE IMPLEMENTATION OF EMBEDDED CONCURRENT DES FUNCTIONAL UNITS USING SPATIAL PARALLELISM APPROACH ON FPGA FOR BETTER THROUGHPUT

by

RANA KHAZAAL KHUDHAIR
(1432321196)

A dissertation submitted in partial fulfilment of the requirements for the degree of Master of Science (Embedded System Design Engineering)

School of Computer and Communication Engineering
UNIVERSITI MALAYSIA PERLIS
2015

UNIVERSITI MALAYSIA PERLIS

DECLARATION OF THESIS

Author's full name : …………………………………………………………………………………..........................

Date of birth : ……………………………………

Title : …………………………………………………………………………………..........................

…………………………………………………………………………………..........................

…………………………………………………………………………………..........................

Academic Session : ……………………………………

I hereby declare that the thesis becomes the property of Universiti Malaysia Perlis (UniMAP) and to be placed at the library of UniMAP. This thesis is classified as :

□ **CONFIDENTIAL** (Contains confidential information under the Official Secret Act 1972)*

□ **RESTRICTED** (Contains restricted information as specified by the organization where research was done)*

□ **OPEN ACCESS** I agree that my thesis is to be made immediately available as hard copy or on-line open access (full text)

I, the author, give permission to the UniMAP to reproduce this thesis in whole or in part for the purpose of research or academic exchange only (except during a period of _____ years, if so requested above).

Certified by:

SIGNATURE **SIGNATURE OF SUPERVISOR**

(NEW IC NO. / PASSPORT NO.) **NAME OF SUPERVISOR**

Date :________________ Date : ________________

ACKNOWLEDGMENT

This work would not have been possible without the encouragement and support of so many. This is my time to say thank you to you all.

I wish to express my deepest gratitude and appreciation to my supervisors ***Dr. Muataz S. Hameed*** for his guidance, suggestions, continuous support, and encouragement through the research work.

I also would like to thank the Dean of the School of Computer and Communication Engineering, ***Prof. Dr. R. Badlishah Ahmad*** and **Programme Chairman of Postgraduate Studies *Dr. Phaklen Ehkan*** and all lecturers of the school for their support**.**

Many thanks and appreciations are expressed to many people for their support during this work, some of whom I feel deserve a special mention, particularly my husband ***Dr. Ahmed Azeez Ahmed*** for his invaluable support, encouragement and love. My grateful to my parents dears (***Dr. Khazaal Al-Janabi & Madam. Wedad Muhammed***), also to my sisters and brothers for their support and encouragement. My special thanks to my lovely daughters (***Husna & Asma***) for their patience and encouragement through my study time. I wish for all good luck and happiness in their life.

Finally, I would like to thank our second country ***Malaysia*** for giving us safety; peace and the chance for completing this study.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABREVIATIONS

AES	Advanced Encryption Standard
ANSI	American National Standard Institute
ASIC	Application Specific Integrated Circuit
ATM	Automated Teller Machine
CPU	Central Processing Unit
DES	Data Encryption Standard
DSP	Digital Signal Processing Chip
EFF	Electronic Frontier Foundation
ENIAC	Electronic Numerical Integrator And Computer
ep	expansion permutation
fp	final permutation
FPGA	Field Programmable Gate Array
GPU	Graphic Processing Unit
IBM	International Business Machines
IDB	Input Data Buffer
IDEA	International Data Encryption Algorithm
ip	initial permutation
JTAG	Joint Test Action Group
keysched	key scheduling
MIMD	Multiple Instruction, Multiple Data
MISD	Multiple Instruction, Single Data
NCD	Network Computer Devices
NGD	Native Generic Database
NGU	Native Circuit Unit

NIST	National Institute of Standard and Technology
NSA	National Security Agency
ODB	Output Data Buffer
PAR	Place & Route program
PC-1	Permuted Choice 1
PC-2	Permuted Choice 2
PCB	Printed Circuit Board
PLL	Phase Loop Lock
pp	p-permutation
RAM	Random-Access Memory
roundfunc	round function
RSA	Rivest-Shamir-Adleman
RTL	Register Transfer Level
S-Box	Substitution Box
SD	Secure Digital card
SOC	System On Chip
SIMD	Single Instruction, Multiple Data
SISD	Single Instruction, Single Data
UCF	User Constraint File
VHDL	VHSIC Hardware Description Language
VLSI	Very Large Scale Integrated circuits
WAN	A Wide Area Network

Meningkatkan Pelaksanaan Selaras Dengan DES Unit Rephrase Menggunakan Pendekatan Spatial Parallelisme di FPGA Untuk Dikendalikan Lebih Baik

ABSTRAK

Secara umum, keselamatan adalah berkenaan semua jenis maklumat dan data sistem. Kebanyakan piawaian keselamatan adalah terdiri daripada keterteraan hingga perdagangan dan komunikasi persendirian. Salah satu aspek penting untuk komunikasi yang selamat adalah kunci peribadi kriptografi. Baru-baru ini kebanyakan aplikasi dan piawaian keselamatan ditakrifkan kepada algoritma bebas, iaitu, membolehkan pilihan daripada satu set algoritma kriptografi untuk tujuan yang sama. Semenjak Piawaian Penyulitan Data (DES) adalah sistem kunci peribadi algoritma yang paling banyak digunakan, DES mempunyai peranan penting dalam aplikasi keselamatan. "*Field Programmable Gate Arrays*" (FPGA) adalah peranti perkakasan pembentukan semula juga fenomena menarik dalam pembangunan pembenaman. Dalam kajian ini, pelaksanaan DES dalam pengoptimuman algoritma yang telah dicapai melalui DES komponen unit replikasi hingga rephrase serentak DES unit berfungsi. Operasi ini telah dijalankan dengan menggunakan pendekatan keselarian spatial. Data input / output telah disimpan dalam RAM yang dipisahkan kepada dua komponen simpanan yang menyokong proses baca dan tulis serentak. Pendekatan ini adalah bagi mempercepatkan pemprosesan data. Tambahan pula, kekerapan yang disokong oleh lembaga telah disalin dari 50 sehingga 200 MHz dengan menggunakan "*Phase Locked Loop"* (PLL) untuk mengelakkan sebarang kelewatan pelaksanaan DES unit untuk berfungsi. Semua ini telah membawa kepada meningkatkan dan kepantasan pelaksanaan DES algoritma dan peningkatan daya pemprosesan. Reka bentuk dan pelaksanaan dilakukan pada papan siklon III FPGA NEEK.

Enhance Implementation of Embedded Concurrent DES Functional Units using Spatial Parallelism Approach on FPGA for Better Throughput

ABSTRACT

In general, the security is concerned of all types of information and data systems. Many standards to security are ranging from military to commerce and private communications. One essential aspect for secure communications is the private key cryptography. Recently most security applications and standards are defined to independent algorithm, which is allowing a choice from a set of cryptographic algorithms for the same purpose. Since Data Encryption Standard (DES) is still the most widely used private-key encryption algorithm, DES has a significant role in security applications. Field Programmable Gate Arrays (FPGA) is reconfigurable hardware devices and interesting phenomenon in embedded development. In the present work, DES algorithm implementation optimization has been achieved through the DES unit components replication to four concurrent DES functional units. This operation has been performed by using a spatial parallelism approach. The input/output data has been stored in the separated RAMs which it is dual port memories that supports the read and write processes concurrently. This approach is speedup the processing of data. Furthermore, the frequency which is supported by the board has been duplicated from 50 up to 200 MHz by utilizing the Phase Locked Loop (PLL) to avoid any delay of DES functional unit implementation. All of this has led to enhance and speedup the implementation of DES algorithm and increase throughput as well. The design and implementation is performed on Altera Nios II Embedded Evaluation Kit (NEEK) board.

CHAPTER 1

INTRODUCTION

1.1 Overview

In general, the security is concerned of all types of information and data systems. Through the past years, national security and military matters lead to the requirement of the protected communications. Nowadays, business and private sectors are needed also security requirements. Safety internet communications have an important role in electronic commerce. Many companies have firewalls to secure internal information for businesses from competitors. In the particular sector, many products are obtainable to compete both telephone communications and email (Gaurav, 2012). One of providing security means in information and data systems are Cryptography which is the fundamental technique to protect the digital information data. It is a mechanism that is used to avoid an unsecured access of system of data which it assists to provide responsibility vastness, preciseness and also provide privacy. There are two main operations of Cryptography which are called as encryption and decryption. By using encryption, data is transferred in a way which made it unreadable. These data is recovered by using decryption. In principle, decryption process is achieved rightly by the meant receiver(s). The "strength" or "security" of the encryption form is determined by depending on the validity of this predication (Gaurav, 2012; Amandeep, 2010).

In the past years concerning of volume of information and data which widely increased, fast and secure cryptographic algorithms were evolved to face security threats and measures which became fundamental through performing of digital data and information transactions. The security applications faced an additional challenge because the elevated diversity. Since the cryptography demands not only highly secure algorithms but actually for some applications require a high performance and for others less space (Srinivas, 2007). The most public example through the different cryptographic algorithms in the symmetric ciphers scope is the Data Encryption Standard (DES) algorithm (O'Melia & Adam, 2010; Liu, 2007). Since 1972, the National Institute of Standard and Technology (NIST), was conscious of the possible thread of computer and communications data. The NIST produced a programme for developing a consolidated encryption algorithm. In 1976, the DES was already released which it is presently the most excessively used private-key algorithm and it was became also important portion of many standards e.g., the Secure Socket Layer, Automated Teller Machine (ATM) cell, and for different American National Standard Institute (ANSI) banking standards. The DES algorithm stills significant and will have a mainly role in several more years, though it is not reapproved.

The new security applications and standards are defined to be independent algorithm. Therefore, for a determined security service like privacy, a number of various algorithms are used alternatively. This specified to public-key based applications in addition to private-key applications. It is quite simple to turn cryptography algorithms in software platforms, but it is uneasy on traditional hardware. On the other hand, the solutions of hardware give a good speed and better security. The better solution of this problem is reconfigurable hardware. On reconfigurable hardware, performing cryptographic algorithms gives main benefits over Very Large Scale Integrated circuits (VLSI). Furthermore, implementations of VLSI are speedy and must be designed from the behavioural characterization to the physical layout. They are required a costly and time consuming production operation. Where the time is the important and vital factor of implementation process the software platforms implementation has been offered highly flexibility but also they do not have enough speed for the applications. While the cost and time of VLSI fabrication and design process was reduced through reconfigurable devices and for that they are become attractive. Furthermore, the reconfigurable devices offer a high ability to reprogram and experiment on multiple architectures.

One of the modern reconfigurable hardware is based on Field Programmable Gate Array (FPGA) devices which implement algorithms. Thus, FPGA devices are used for building graceful algorithm applications. Therefore, the same device may be used for various algorithms that it is independent on the algorithms nature. In cryptographic aspect, many various encryption algorithms are realized using FPGA. However, the public-key and private-key algorithms are performed using the same FPGA. The DES algorithm is organized in iterated rounds formed of many bit-level operations like "shift operations, substitutions, permutations, logical operations, etc."(Saqib et al. 2004). DES algorithms were implemented on many platforms though FPGA has characteristics are suited for active implementations. From those platforms: software (O'Melia, & Adam, 2010; Liu, 2007), VLSI (Arich, & Eleuldj, 2002; Tiri, & Verbauwhede, 2005; Weiwei et al. 2009) and reconfigurable hardware using FPGA devices (Mulani & Mane, 2014; Saqib et al. 2004; Raed et al. 2014).

In the present work, the optimization of DES algorithm implementation has been performed through the replicated DES unit components in order to become 4 concurrent DES functional units. This process has been accomplished by utilizing a spatial parallelism approach. The input/output data has been stored in the input/output buffers which it is dual port memories that supports the read and write processes simultaneously. This process helps to speed up the processing of data.

Moreover, the frequency that supported by the board has been duplicated from 50 up to 200 MHz by using the Phase Locked Loop (PLL) for avoiding any delaying in implementation of the DES functional unit. All of that has led to enhance and speedup the implementation of DES algorithm for better throughput.

1.2 Problem Statement

Since the beginning of the 80th of the previous century, it was a huge growing in communication and information systems, e.g. wireless communications, electronic payment systems and the other areas of communications. At the same time, the security aspects of communication and information are growing also. The mobile conversations, credit card number and bank transection are few examples of threats imposed by unprotected communication infrastructure. Therefore, the main tool for achieving the require security is cryptography. DES algorithm is one of the important private key algorithms that most widely used and it is also part of many other standards, e.g. ATM cell encryption and various banking standards.

Currently, most of researchers are successfully implemented and analysed the DES algorithm using many embedded platforms, e.g. Digital Signal Processing chip (DSP), smart card, Graphic Processing Unit (GPU) and FPGA technology. However, DES algorithm has been implemented to process one block of plaintext for one time.

Researchers have been directed to use parallel scenario to improve the throughput of DES algorithm by utilizing off-chip approach. Whereas, off-chip is effective and increases the throughput, this approach also increase design size, power consumption and cost as well. Therefore to avoid off-chip parallelism, a platform that utilizing spatial parallelism on-chip for DES algorithm is needed to increase throughput without any extra size, power and cost.

1.3 Objectives

The objectives of the work are to:

i) To Implement Embedded Concurrent DES Functional units with following specifications:

a) Lower level of design complexity; achieve high operating frequency and consume minimal chip resources.

b) Increase throughput by applying spatial parallelism approach.

ii) To verify and evaluate the design performance of the system by using FPGA CAD tool and on board testing.

1.4 Scope

The scopes of this project are:

1. A new implementation of embedded DES functional units on FPGA by applying spatial parallelism.
2. Achieving lower level of implementation complexity; high operating frequency, less chip resources and scalable throughput.

1.5 Thesis Outlines

This thesis comprises of five chapters including the overview. **Chapter 2** demonstrates two important concepts which have been used in the third chapter. It includes too the description of DES algorithm in details and the importance of embedded platforms and their challenges in comparison with other classic hardware. In **chapter 3** was demonstrated the methodology of work in addition to the tools that helped to achieve the project. **Chapter 4** describes and discusses the results obtained by the implementation of the algorithm on board. **Chapter 5** shows the conclusion and the future work.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Parallel computing is a form of computation in which many calculations are carried out simultaneously, operating on the principle that large problems are often be divided into smaller ones, which are then solved concurrently ("in parallel") (Almasi & Gottlieb, 1989). There are several different forms of parallel computing: bit-level, instruction level, data, and task parallelism. Parallelism has been employed for many years, mainly in high-performance computing, but interest in it has grown lately due to the physical constraints preventing frequency scaling (Adve et al. 2008). The consumption of power by PCs became a very important in the last few years. The parallel computing became the controlling sample in the architecture of computers basically, in the shape of multi processer's core (Asanovic et al. 2006; Cristobal et al. 2014).

2.2 Parallel Computing Design

Traditionally, computer software has been written for serial computation. To solve a problem, an algorithm is constructed and implemented as a serial stream of instructions. These instructions are executed on a Central Processing Unit (CPU) on one computer. Only one instruction may execute at a time after that instruction is finished, the next is executed (Blaise, 2007).

Parallel computing, on the other hand, uses multiple processing elements simultaneously to solve a problem. This is accomplished by breaking the problem into independent parts so that each processing element may execute its part of the algorithm simultaneously with the others. The processing elements are diverse and include resources such as a single computer with multiple processors, several networked computers, specialized hardware, or any combination of the above (Blaise, 2007). The parallelism’s role in increasing the speed of computing has been noticed for many decades. Its role in supplying pluralism in data paths and increasing the storage access has been important in commercial purposes. The scalable execution and minimal cost of the parallel platforms is reflected in an extensive assortment of applications. The development of parallel software and hardware has been intensive effort and time. If one wants to observe this in the context of quickly improving uniprocessor acceleration, one is attempted to ask the requirement for parallel computing. In the future, there are some clear directions in the design of hardware, that refer to that the architectures uniprocessor might not be eligible to keep the rate of increasable performance. As a result of the limitation in the physical and computational number therefore, the emanation of combined parallel computing hardware, libraries and environments has basically decreased the time to parallel solution (Ananth et al., 2005).

The major significant for using the parallel computing design is to save time or money, solve more complex problems, provide concurrency, take advantage of non-local resources and make better use of underlying parallel. During the past twenty years, the trends indicated by ever faster networks, distributed systems, and multi-processor computer architectures clearly show that parallelism is the future of computing. In this same time period, there has been a greater than 500,000x increase in supercomputer performance, with no end currently in sight as displayed in Fig. 2.1 (Blaise, 2007).

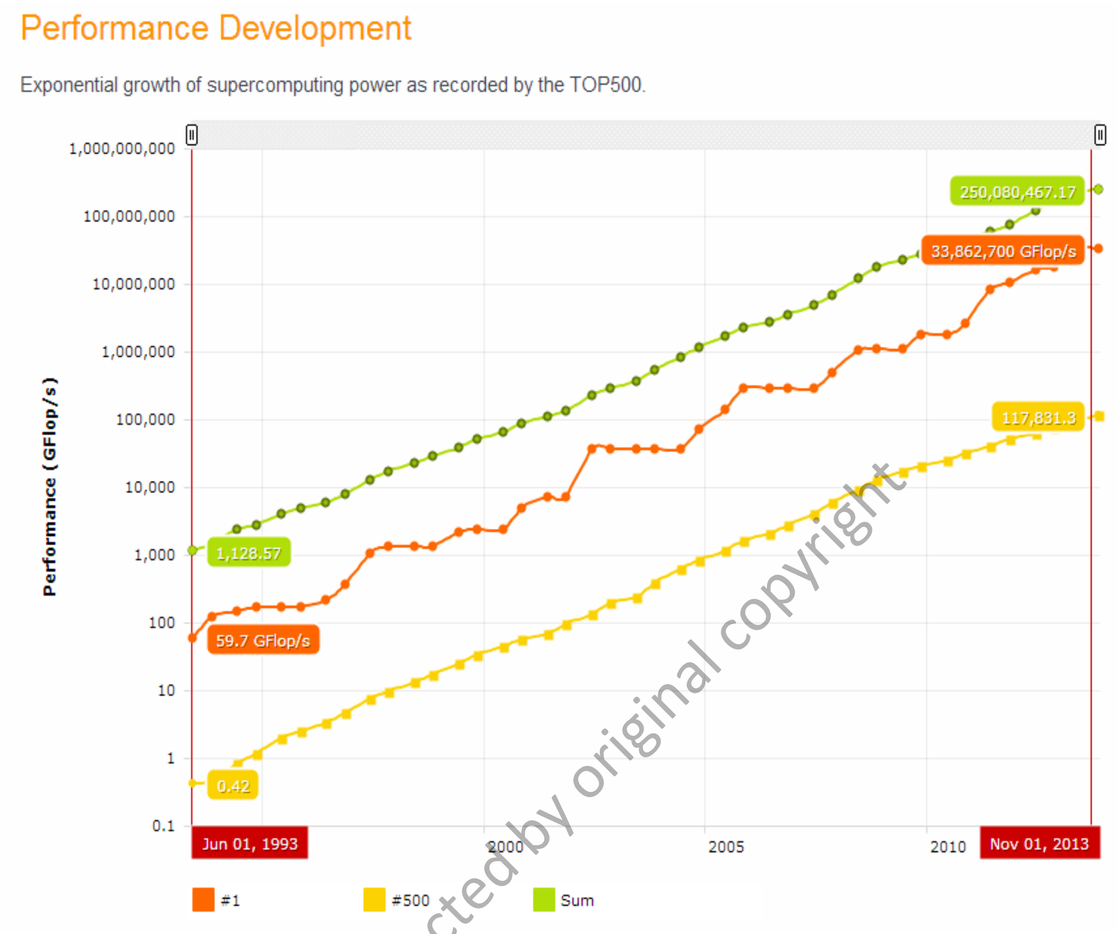

Figure 2.1: Exponential Growth of Supercomputing Power (Blaise, 2007)

2.2.1 Concepts of Parallel Computing

Since 19th Century different parallel computing approaches are started. Thus, the actual beginning of parallel computing is unknown for anyone. Parallel computing was started about the middle of 1980s. During this period of years the parallel computers were began programming as a real parallel mechanism that might contend with the founded super-computers (Womble et al. 1999; Timothy, 2005).

2.2.1.1 Machine Model

The von Neumann model is defined as computer architecture is described since 1945 by the scientist J. von Neumann and others. This architecture was described for electronic digital computer that consisted of parts of CPU that contains a memory to save the instructions and data simultaneously, processor registers and arithmetic logic unit, a control unit that contains register instruction and program counter and I/O mechanisms as displayed in Fig. 2.2 (Godfrey & Hendry, 1993).

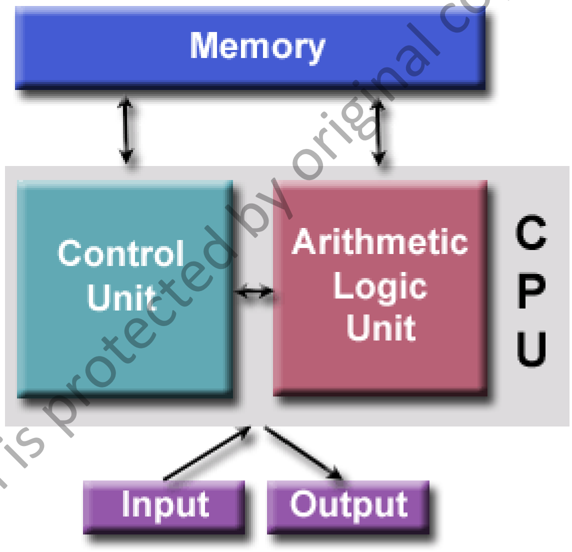

Figure 2.2: von Neumann Architecture (Blaise, 2007)

Actually, all computers have followed this basic design which is comprised of four main components which are memory, control unit, arithmetic logic unit and Input/Output. However, these components are performing all the processing operations such as Read/write, random access memory which is used to store both program instructions and data. Program instructions are coded data which tell the computer to do