Design and Implementation of Parallel Model Embedded FPGA-based Computing Architecture for DES Algorithm

by

Husham Ibrahim Mahdi AL-Salman
(1730212480)

A thesis submitted in fulfillment of the requirements for the degree of
Master of Science in Computer Engineering

Faculty of Electronic Engineering Technology
UNIVERSITI MALAYSIA PERLIS

2021

ACKNOWLEDGEMENT

In the name of ALLAH, the most merciful. For blessing and giving me strength and ability to complete this thesis.

(وَلَوْلاَ فَضْلُ اللهِ عَلَيْكَ وَرَحْمَتُهُ لَهَمَّت طَّآئِفَةٌ مِّنْهُمْ أَن يُضِلُّوكَ وَمَا يُضِلُّونَ إِلاَّ أَنفُسَهُمْ وَمَا يَضُرُّونَكَ مِن شَيْءٍ وَأَنزَلَ اللهُ عَلَيْكَ الْكِتَابَ وَالْحِكْمَةَ وَعَلَّمَكَ مَا لَمْ تَكُنْ تَعْلَمُ وَكَانَ فَضْلُ اللهِ عَلَيْكَ عَظِيماً)

[النساء 113]

I am very grateful and thankful to many individuals who in various ways in the completion of this final year project. First and foremost, thanks to ALLAH, for the blessings. Thanks to my supervisors Associate Professor Ts. Dr. Phaklen Ehkan and Dr. Muataz Hamed AL-Doori for their guidance throughout this thesis. Their willingness to share the knowledge, advises, point of view regarding any issues about the study without any hesitation has been a great opportunity for me. Not forgotten.

I am grateful to all my family members especially, my father and my mother for their continuous support and concern at anytime, anywhere and everything I need during completing. Thank to my beloved friends for their tolerance of my absences, physically and emotionally. I am blessed and strengthened by their unconditional support and love.

Finally, special thanks to my housemates and other friends who are always with me to share and give me a moral support, excitements and opinions throughout this project. Unfortunately, there are too many of them to be listed in this limited space.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AADL	Architecture Amylase and Design Language
ASIC	Application-Specific Integrated Circuit
CAD	Computer Aided Design
CERT	Cyber Emergency Response Team
CPS	Cypher Physical System
CPU	Central Processing Unit
3D	Three Dimension
DNS	Domain Name System
DES	Data Encryption Standard
DoS	Denial of Service
DSL	Digital Subscriber Line
DSP	Digital Signal Processing
FPGA	Field Programmable Gate Array
FIPS	Federal Information Processing Standard
4G/3G	Fourth/Third Generation
GSM	Global System for Mobile communications
HDL	Hardware Description Language
IBM	International Business Machines
ICT	Information and Communications Technology
ICS	Industrial Control Systems
IOS	Internet of Services
IoT	Internet of Thing
ip	Initial Permutation
IP	Internet Protocol
M2M	Machine to Machine
MMC	Modular Multilevel Converters
NISI	Network Information Service Infrastructure
NSA	National Security Agency
PC	Personal Computer
PCB	Printed Circuit Board
PLL	Phased-Locked Loop
RFID	Radio Frequency Identification
RTL	Register Transfer Level

SBC	Single-Board Computer
SCI	Small Computer Interface
SoC	System on Chip
SRAM	Static Random-Access Memory
SDK	Software Development Kit
SQA	Simulated Quantum Annealing
SPE	Stream Processing Engine
TCP	Transmission Control Protocol
UART	Universal Asynchronous Receive\Transmitter
UML	Unified Modeling Language
USB	Universal Serial Bus
VHDL	Very High Speed Integrated Circuit Hardware Description Language
WI-FI	Wireless Fidelity
WSN	Wireless Sensor Network
OS	Operating system

LIST OF SYMBOLS

n	Megabits per second
f	Frequency
$\boldsymbol{D}$	Data per clock
ns	Nanosecond

Rekabentuk dan Pelaksanaan Sistem FPGA Terbenam Model Selari berasaskan Senibina Pengkomputeran untuk Algoritma DES

ABSTRAK

Sejak beberapa tahun kebelakangan ini, ada pertumbuhan secara eksponensial dalam bidang pengkomputeran awan *(cloud)* disebabkan keperluan untuk perkhidmatan dalam kemajuan platform mudah alih telah menyaksikan peningkatan permintaan yang pantas. Perubahan ini telah mendorong keperluan langkah keselamatan berlipat ganda untuk pengkomputeran awan. Isu keselamatan adalah masalah utama untuk *cloud* dan juga perkhidmatan internet yang lain. Sebab utama pencegahan penggunaan pengkomputaran awan sepenuhnya adalah sebilangan besar masalah keselamatan yang dihadapinya, walaupun ia berguna. Dua masalah utama telah dihadapi dengan platform ini; pertama, kelewatan dalam pemprosesan data dan kedua, bahaya keselamatan untuk kemungkinan ancaman. Kesimpulan dari platform ini tidak dapat memenuhi keseluruhan cabaran keselamatan untuk proses cepat dan pengurangan tahap bahaya. Kedua-dua masalah ini diselesaikan melalui rekabentuk semula algoritma DES dalam tiga rekabentuk iaitu tunggal, berganda, dan *quad* untuk mengenkripsi/mendekripsi komponen untuk dijalankan sebagai rekabentuk pantas. Jadi, untuk memaksimumkan keluaran *(throughput)*, senibina ini dapat menyediakan satu blok cipher untuk setiap kitaran blok. Selanjutnya, untuk melakukan keluaran maksimum, laluan kritikal yang merupakan jalan terpanjang antara dua register dikurangkan menjadi satu tahap. Ini dilakukan dengan menggunakan dua register 32 bit/s pada setiap akhir pusingan untuk menahan cipher separa dan mencapai keluaran tertinggi. Model ini diduplikasi dan berganda (quad) dengan teknik selari *spatial*. Perbandingan di antara mereka dibuat untuk mencari rekabentuk terbaik, dan kemudian rekabentuk yang dipilih dibandingkan dengan kajian luaran untuk mencari kaedah terbaik. Analisis ini telah memperkuat algoritma DES pada masa yang diperlukan untuk mengenkripsi data dan menyampaikan kekunci. Sebaliknya, enkripsi lebih dari satu blok dicapai pada satu masa dan jumlah rekabentuk untuk mencari aplikasi yang paling sesuai untuk pemprosesan data. Kajian ini menerapkan kecekapan berasaskan algoritma DES untuk rekabentuk mesin selari berganda 16 pusingan bagi penyelesaian enkripsi kos rendah, berskala, dan kuat untuk pelaksanaan perkakasan dimana percapaian frekuensi tertinggi 227 MHz, dan keluaran 58,288.64 Mbps diperolehi.

Design and Implementation of Parallel Model Embedded FPGA System-based on Computing Architecture for DES Algorithm

ABSTRACT

Over the past few years, there has been exponential growth within the field of cloud computing because the need for services on the go for mobile platforms has seen a speedy increase in demand. This success has spurred the requirement for multiplied security measures for cloud computing. Security is the primary issue for the cloud as well as other internet services. The primary reason preventative of the complete adoption of cloud computing is in truth the various security problems it comes with, despite how useful it is going to be. Two major problems have been confronting these platforms; firstly, delay in data processing, and secondly, security hazards for potential threats. The conclusion from these platforms is unable to fulfill the whole security challenge for fast processing and hazard reduction. These two problems had been solved through a DES algorithmic redesign in three designs namely, single, dual, and multiple (quad) engines to encrypt/decrypt components to be carried out as the fast design. So, for maximizing the throughput, this architecture can provide one block of cipher for each block cycle. Furthermore, in order to perform maximum throughput, the critical path which is the longest path between two registers is reduced to one stage. This was performed by using two 32 bit/s registers at the end of every round in order to hold the partial cipher and reach the highest throughput. This model is duplicated and multiple (quads) by means of the spatial parallelism technique. A comparison between them was made to find the best design, and then the selected design was compared with external studies for finding the best method of it. This analysis has strengthened the hand, the encryption of more than one block was achieved at a time and over the number of designs to find the most suitable application for data processing. This study implemented a DES algorithm-based efficient for the design of 16-round multiple parallel engines for low-cost, scalable, and powerful encryption solution for hardware implementation which has a high frequency of 227 MHz and achieved a throughput of 58,288.64 Mbps.

CHAPTER 1 : INTRODUCTION

1.1 Overview

There is a great change in the modification for industry sectors. The fourth revolution as an example performed by Internet of Things (IoT), is a point of establishing connection of things to the internet of isolation. IoT helps the organisation to execute a particular business application and objectives. For example, the maintainance activity to decrease the asset of downtime and operational expenditures, deployed products and assets were referred to as being of the network, and improved the corporate systems to enhance their production at a larger rate (Ranjbar, Sedehi, Rashidi, & Suratgar, 2019; Roy & Roy, 2018). IoT platform helps to provide a linkage between the sensors and hardware at the edge of the network within the major information technology (IT) systems and infrastructure. Role of IoT platform is to translate more premitive data content, structure and format that are required to the edge of network. It is used to prepare into an enterprise ready system regarding the integration of business applications and systems.

The IoT platform has a wonderful part, but it does not dealt with the business context. It is totally associated with the flow of data from the edge of the network. It needs to be another piece of the puzzle to bridge that gap. The IoT engagement engine take a huge amount of stream for producing the data by the IoT platform and integrates with contextual business information. For example, it could be used in the service history of the applications to identify the actual business needs and then telling the business applications to perform some activities such as an increase in customer services.

The IoT is used to generate intelligent networks for connecting different machines, work as well as systems which could automatically trigger the information. It was observed that 85% of companies applied Industry 4.0 for all important solutions of business activities in five years time frame (Geissbauer, Schrauf, Koch, & Kuge, 2014). Industry 4.0 is also defined as a series of differentiating features which tried to integrate other intelligent infrastructures such as mobile or logic infrastructures, smart buildings and enhancing technological modifications. Proper research work helps to perform proper monitoring most of the cases and also stopped with various solutions that had been highlighted by using various studies with different views.

The techniques are providing advantages to the business process including technology used by FPGA which can be applied in the security systems of many important corporate companies. It helps to manage a large amount of information within the company and outside environment. It also helped to improve the production activities in a particular company (Lasi, Fettke, Kemper, Feld, & Hoffmann, 2014).

Industry 4.0 was completely associated with cyberspace which emphasized the production system. The sensors were entirely installed in physical objects for connecting the physical world with a lot of the models (AL-Salman & Salih, 2019). Due to this revolution, the use of sensors and network-related gadgets was growing rapidly and working on solving the issues associated with big data (Lee, Bagheri, & Kao, 2015). The common concept associated with the industry was based on the communication which highlighted most of the hazards of these industries. It had gone through one of the most common issues that were elaborated in various scientific engineering and search for solutions to resolve those gaps that are considered as the

most important requirements of today's work. The use of multiple technologies provides high speed and a large amount of security.

1.2 Problem Statement

Real-time networking needs a computational architecture that is robust, efficient, and accurate in order to provide fast data forwarding and secure data transmission with lower complexity. In addition, the architecture should be flexible and scalable. Currently, the computing infrastructure depends on traditional processing platforms such as personal computers (PCs), single-board computers (SBC), and microcontroller-based systems (Benias & Markopoulos, 2017&Teitel & Teitel, 2015). All these platforms performed well and achieving acceptable throughput. Two major problems confront with these platforms are the delay in data processing and security hazard for potential threats (Huang, 2015). Issues such as synchronization signals, processing unit architecture, and computational power in the platforms cause a delay in data processing. It is also a high possibility of system infection and penetration because of its operating system-based approach. These platforms are unable to fulfill the whole Industry requirements for fast processing and hazard reduction (Cavanini et al., 2018 & Dang & Merieux, 2018).

The option of researchers use multiple platforms to improve processing power and implement security algorithms to minimize threats. These improvements are effective, and this scenario has a drawback of processing power that perhaps impacted by complex security algorithms and an extra hardware which is included due to platform capacity limitation. Therefore, to avoid this approach, a platform that has an efficient concurrent architecture and high processing power is needed to fulfill the requirement of industry with comprehension secure architectural resources.

1.3 Objectives

The main objective of this research work is to enhance data flow for data encryption standard (DES) using embedded field programmable gate array (FPGA) system-based computing architecture. The sub-objectives of this research include

i. To design an embedded-based FPGA computing architecture for DES using parallel behavior .

ii. To design a new routing approach for control and data planes on FPGA technology using parallel behavior for reducing the data flow time.

iii. To evaluate and verify architectural performance in terms of maximum frequency, and efficient throughput by using the FPGA CAD tool and onboard testing.

1.4 Scope of study

The main focus of this study is the design and implementation of an efficient embedded computing architecture for multi-model by using FPGA. The design was done in two directions; first, working on the algorithm responsible for the encryption and decryption process, and second, designing several models using parallel technology (single, dual, multi-quad) for the purpose of finding the most suitable one. The system utilizes the parallelism approach-spatial to reduce the potential delay that can happen during processing and transferring data. The proposed system is limited only in reducing all unauthorized access to and data penetration. The virus infection will not be considered because the design applying fully digital circuits as FPGA does not use any operating system. The study can be used in all existing industrial plants. Some

calculations, assumptions, and selections are made as a consideration of a proper and realistic design.

1.5 Thesis Outline

Chapter 1 provides brief prologue and introduction to the topic and the current issues. It also discusses the project's objective and scope of the study as well as the desired result. Chapter 2 describes the research of literature and some hypotheses concerning the topic. Some related works done previously also being reviewed and studied in this chapter. The algorithms and techniques used from other journals, conferences, and websites are briefly discussed in this chapter too.

Chapter 3 explains the research methodology for this project. Some architecture design, algorithm design, and techniques used are briefly discussed in this chapter. The procedural and methodology to make this study complete have been considered in this chapter. Chapter 4 describes the final result of the study and the discussion regarding the result. It also comments on the result obtained, interpreting the meaning of results, Chapter 5 provides a conclusion regarding the objectives of the project. It also comments on how closely the achievement of measurements and calculations, and summaries the prior reason for any discrepancies.

CHAPTER 2 : LITERATURE REVIEW

2.1 Introduction

This chapter reviews the relevant literature and research related to embedded system design challenge, field programmable gate array (FPGA) and presents background of the design and security challenges, their capabilities and benefits, and different parallel systems architectures (temporal parallelism and spatial parallelism). It also covers various tools of communication service such as internet of things (IoT), discussion about universal asynchronous receiver/transmitter (UART) protocol, and then followed by overview of data encryption standard (DES) algorithms including the core features of an architecture of DES algorithm that being used in this work.

The assembling industry is experiencing incredible changes. The fourth uprising, driven by the IoT is occurring. It made smart systems associating with the machines, work, and frameworks that can self-sufficiently trade data trigger activities, and control each other freely (Rüßmann et al., 2015). Likewise, Industry 4.0, is described into one stage in a progression of different highlights, which are expected for coordination other intelligent infrastructures, such as smartphones and logistics, and clever-turned houses (Ray & Bhadra, 2017).

The reconstruct capacity of FPGA secures the client's board applications as well as ensures against theft that could change the system's behavior conduct. These highlights likewise help with distant system refreshes (Pang & Membrey, 2016). FPGA offers this usefulness so a planner can refresh their systems by reconstructing the FPGA

without disturbing the segments around it. The planned security could be a piece of the structure procedure, not a bit of hindsight. It is basically the planned to be ensured against altering, whichever strategies are picked regardless of whether it is oblivious or unlawful (Adhikari, Morris, & Pan, 2017).

There exists a nearly to greatly decision of network choices for hardware designers and application engineers taking a shot at items and systems for the IoT (Yogita Pundir, Sharma, & Singh, 2016). Many connectivity technologies, such as wireless fidelity (Wi-Fi), Bluetooth, ZigBee, and 2G/3G/4G mobile, are notable, but there are also a few new growing networking options, such as string as an option for smart home apps and whitespace TV (Pereira, 2016). The IoT together use the cases depending on application, considerations such as information requirements, protection and future requests and battery life shall guide the decision of one or some other kind of blend of advanced technologies. This technology executed in major urban communities in the wider area (Li, Dai, & Zhao, 2014).

2.2 Embedded System Design Challenge

The computing system is very common to build for the very different purpose, for example, desktop computer, workstation, mainframes and servers. Precise definitions of an embedded system can be defined as closely any computing system beside than desktop, laptop or processor computer (Benveniste et al., 2018). Embedded systems usually found in a different of electronic gadgets, for instance, customer hardwares (mobile phones, advanced cameras, camcorders, versatile computer games, calculators, as well as personal digital assistants), home apparatuses (microwaves, indoor regulator, home security, clothes washers, and lighting frameworks), office computerization (fax machines, copiers, printers, and scanner), business devises (cash registers, alarm systems, card reader, scanners, and robotized teller machines), and vehicles (transmission control, journey control, fuel infusion, antilock brakes devices, and dynamic suspension) (Brzoza-Woch & Nawrocki, 2015).

An embedded system consisting of desired functionality is easy to course construct but is difficult for the implementation that simultaneously optimizes the design metric (Möller, 2016). Embedded system can be subjected to a physical constraint which can perform computation with the physical world in two ways. Reaction constraint normally consists of the deadlines, throughput, and jitter and originates from the behavioural needs and reaction constraint will deal with the control theory. Computer engineering will deal with originating from the implementation selections, while execution constraint guaranteed accessible power, processor speed, and hardware failure rates. Both of this constraint will interplay with the computation to meet the goal for the implementation platform (Tripakis, 2016).

There are three generations of the embedded system. The liberation of both design and implementation was shown when design practices have transformed from the adjacent connection between these two. Language and synthesis-based origins were the first generations of strategies that traced their roots to one of both sources. The language-based method lies in the software approach and synthesis-based approach which is based on hardware. The language-based approach focuses on a particular programming language with a specific runtime system. The most recent early example of Ada is RT-Java. Synthesis-based is another approach which evolved from circuit design techniques and the Hardware description language (HDL) such as Very High Speed Integrated Circuit Hardware Description Language (VHDL) and Verilog was the present implementation method (Pang & Membrey, 2016).

The second generations of the technique introduced are the implementation of the platform independence. This technique has presented the separation of the design and implementation level which to achieve the maximum independence of the specific platform. There is various example use for this generation and the most common are System C combines asynchronous execution mechanisms and synchronous hardware semantics from software (C++), common dataflow languages such as Matlab's, generally implement an asynchronous semantics (Di Paolo Emilio, 2015).

The third generation is Unified Modelling Language (UML), execution semiconductor independence depends on modelling languages including the Architecture Analysis and Design Language (AADL). This results in the release from a particular programming language, system design and resource constraints (Hidayat & Utomo, 2016 & Nakajima, Talpin, Toyoshima, & Yu, 2016).

2.2.1 FPGA Design and Security Challenge

Field Programmable Gate Array (FPGA), a present technology which is widely used in education, research, industrial field. FPGA provides flexible structure and greater functionality but still have some limitations (Anton & Sklyar, 2015). In the late of 1980s, FPGA was introduced for building system prototypes of application-specific integrated circuit (ASIC) and system on chip (SoC) design (Alwzan, Khidhir, & Thabit, 2020) It contains a huge amount of the configurable logic grew rapidly and these useful components are the requirement to build and test the latest design which grew in both complexity and size. In the earlier stage of FPGA generation need a large array of devices to fully accommodate a logic design.

FPGA board as shown in Figure 2.1 allows hardware designer to test and develop the systems, and software developer can early access to a fully functioning hardware platform (Di Paolo Emilio, 2015).

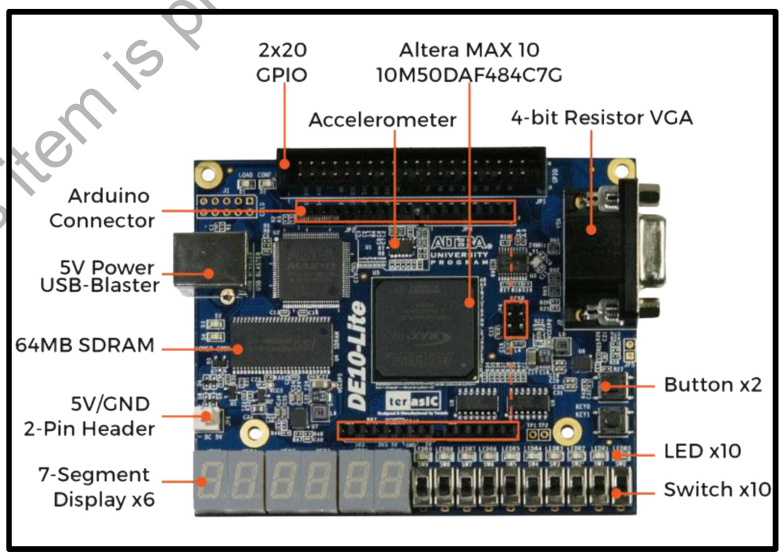

Figure 2.1 FPGA Board (Terasic Inc, 2017)