An Efficient Parallel FPGA-based Architecture to Implement AES in Image-based IoT Applications

by

Nada Qasim Mohammed
(1740212496)

A thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy

Faculty of Electronic Engineering & Technology
UNIVERSITI MALAYSIA PERLIS

2023

ACKNOWLEDGEMENT

First and foremost, praise and thanks to God, the Almighty, for His showers of blessings throughout my thesis work to complete the research successfully. I want to express my sincere gratitude to my supervisor, Assoc. Prof. Dr. Amiza Amir, for the continuous support of my Ph.D. study and research and for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my Ph.D. study.

I would like to express my sincere thanks to my co-supervisor, Prof Ir Ts Dr R Badlishah Ahmad for giving me the opportunity to do research and providing invaluable guidance throughout this research.My sincere thanks also go to the rest of my thesis committee: (Dr.Muataz Hameed Salih)for insightful comments and hard questions. I am extremely grateful to my parents, my husband, and my two lovely boys for their love, prayers, care, and sacrifices for educating me and continuing to support me in completing this research work. I am very thankful to my sister and brothers for their love.

Finally, my thanks go to all the people who have supported me in completing the research work, either directly or indirectly.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	Advance Encryption Standard
ASIC	Application Specific Integrated Circuits
CA	Cryptographic Algorithm
CB	Connection Block
CLB	Configurable logic blocks
CPU	Central Processing Unit
CUI	User Interface
SPI	Serial Peripheral Interface
DE	Development and Education
DES	Data Encryption Standard
DLL	Delay-Locked Loop
DSP	Digital Signal Processing
DT_M	Data Transfer in Megabits.
DT_G	Data Transfer in Gigabits
FPGA	Field Programming Gate Array
F_{Max}	Frequency Maximum.
GRM	General Routing Matrix
I2C	Inter-Integrated Circuit
MIMD	Multiple Instruction Stream Multiple Data Stream
MISD	Multiple Instruction Stream Single Data Stream
SIMD	Single Instruction Stream Multiple Data Stream
SISD	Single Instruction Stream Single Data Stream
HDL	Hardware Description Language
IDB	Input Data Buffer
IOB	Input / Output Logic Blocks
IoT	Internet of Thing
LCD	Liquid-Crystal Display
LUT	Look-Up Table
MUX	Multiplexer
NCD	Native Circuit Description
NIST	National Institute of Standards and Technology
NEEK	Nios II Embedded Evaluation Kit

N_{CE}	No of the Computing Engine
N_{BPS}	No of the bits per Second.
ODB	Output Data Buffer
PLD	Programmable Logic Devices
PLL	Phase-Locked Loop
RAM	Random-Access Memory
RFID	Radio Frequency Identification
ROM	Read-Only Memory
RSA	Rivest-Shamir-Adleman
RTL	Register Transfer Level
Rx	Receiver
SB	Switch Block
SOC	System on Chip
SRAM	Static Random Access Memory
T	Time in Second
TLD	Top Level Design
TTM	Time to Market
Tx	Transmitter
Thr_G	Throughput in Gigabits per Second.
Thr_M	Throughput in Megabits per Second.
Thrs	Throughput of the System
UART	Universal Asynchronous Receiver/Transmitter
VHSIC	Very High Speed Integrated Circuit

.

Seni Bina Berasaskan FPGA Selari Yang Cekap Untuk Melaksanakan AES Dalam Aplikasi IoT Berasaskan Imej

ABSTRAK

Internet of Things (IoT) ialah rangkaian yang membolehkan peranti mengumpul dan memproses maklumat, tanpa campur tangan manusia, dari tempat terpencil. Peranti IoT berurusan dengan sejumlah besar data yang dihantar, diproses dan disimpan. Ini disertai dengan peningkatan ancaman untuk mengakses, mencuri, merosakkan atau menukar maklumat semasa penyimpanan atau penghantaran melalui saluran tidak selamat. Algoritma kriptografi keselamatan tinggi seperti AES memerlukan keupayaan pengiraan yang tinggi untuk mencapai keselamatan maklumat. Tetapi kebanyakan peranti IoT mempunyai kuasa pemprosesan yang terhad. Oleh itu, adalah perlu untuk menggunakan seni bina pengkomputeran selari yang mengeksploitasi teknologi moden dalam kedua-dua selari spatial dan temporal untuk mendapatkan kuasa pengiraan yang paling boleh difikirkan. Pelbagai kaedah telah diperkenalkan untuk mencapai pemprosesan selari. Salah satu daripadanya ialah tatasusunan gerbang boleh diprogramkan medan (FPGA), yang mempunyai ciri-ciri yang baik sesuai untuk melaksanakan seni bina selari dengan penggunaan kuasa yang lebih rendah. Tesis ini bertujuan untuk mereka bentuk dan melaksanakan alat pancar-terima seni bina enjin pemprosesan berbilang pengkomputeran tertanam dengan prestasi tinggi, untuk mendapatkan daya pemprosesan yang lebih baik menggunakan kedua-dua selari ruang dan temporal pada teknologi FPGA untuk menyulitkan dan menyahsulit imej. Dalam reka bentuk ini, dua papan digunakan, "papan DE1_Soc dan NEEK" dengan peranti Altera Quartus prime 18.1, cyclone v 5CSEMA5F31C6 FPGA untuk sintesis dan simulasi. Setiap enjin beroperasi pada frekuensi maksimum 600 MHz dalam satu enjin dan 412 MHz dalam enjin empat. Dalam proses penyulitan dan penyahsulitan, setiap imej dibahagikan kepada bahagian bersaiz sama, dan satu enjin memproses setiap bahagian secara serentak untuk mencapai keselarian ruang. Secara dalaman, enjin mengendalikan bahagian imej dalam keselarian temporal menggunakan saluran paip dalam untuk melaksanakan tugas yang berbeza secara serentak. Semua data yang diproses dalam enjin disulitkan melalui algoritma AES, dilaksanakan sebagai bahagian penting dalam seni bina enjin. Keputusan yang diperoleh meningkatkan daya pemprosesan sebanyak 210.9 Gbps dalam enjin quad dan 76.8Gbps dalam enjin tunggal. Ini menjadikan seni bina pengkomputeran ini cekap dan sesuai untuk aplikasi pantas seperti IoT.

An Efficient Parallel FPGA-based Architecture to Implement AES in Image-based IoT Applications

ABSTRACT

Internet of Things (IoT) is a network that enables devices to collect and process information, without human intervention, from remote places. IoT devices deal with a massive amount of transmitted, processed, and stored data. This is accompanied by increased threats to access, steal, damage, or change the information during storage or transmission over unsecured channels. High-security cryptography algorithms like AES require high computational capabilities to achieve information security. But most IoT devices have limited resource. Therefore, it is necessary to use parallel computing architectures that exploit modern technologies in both spatial and temporal parallelisms to obtain the most conceivable computational power. Various methods have been introduced to achieve parallel processing. One of them is field-programmable gate arrays (FPGAs), which have good characteristics suitable for implementing parallel architectures with lower power consumption. This research aims to design and implement an embedded multiple computing processing engine architecture transceivers with effective performance, to obtain better throughput using both spatial and temporal parallelism on FPGA technology to encrypt and decrypt images. In this design, two boards are used, "DE1_Soc and NEEK board" with Altera Quartus prime 18.1, cyclone v 5CSEMA5F31C6 FPGA device for synthesis and simulation. Each engine operates at a 600 MHz maximum frequency in a single engine and 412 MHz in a quad engine. In encryption and decryption processes, each image is divided into equal-sized parts, and a single-engine processes each part concurrently to achieve spatial parallelism. Internally, the engine handles the image's part in temporal parallelism using deep pipelining to execute different tasks concurrently. All data processed in engines is encrypted via the AES algorithm, implemented as a significant part of the engine architecture. The obtained results increased throughput by 210.9 Gbps in the quad engine and 76.8Gbps in the single-engine. This makes this computing architecture efficient and suitable for fast applications such as IoT.

CHAPTER 1 : INTRODUCTION

1.1 Overview

Digital image processing has evolved through various approaches due to networking and communication. A digital image consists of a finite number of elements and pixels, each having a particular place or position and a value. In recent years, the rapid development of technologies has given rise to the processing of digital image data in various applications. One of these applications is the Internet of Things (IoT), which allows a direct connection between intelligent electronic devices and sensors through the network in the real world. IoT devices gather a massive number of digital images data, with different types and sizes, from the physical environment in the real world and then may share them images via unsecured communication technologies to be used for various purposes. Most images may include sensitive personal information. (Mohialden et al., 2021), (Shahid, 2021), (Iqbal et al, 2017).

The Internet of Things (IoT) provides innovative solutions to various challenges and issues related to our lives such as smart homes, health care, smart cities, smart farming, industrial production, etc. The number of IoT devices is increasing, and they are used in all areas of everyday life practices. The total number of IoT devices is expected to reach 75 billion by 2030. In an IoT environment, the devices communicate without human intervention and are accessible globally, which means that at any time and anywhere, they can be accessed by anyone. Furthermore, in IoT, entities with significant heterogeneity are located in different areas and exchange information between each other via unsecured channels, with interoperable and scalable environments. Therefore, there are several opportunities available to intruders and hackers to gain control, usurp the object's functionality, and

access or modify IoT data, which becomes an attractive target for them. So, achieving security and privacy for the image data collected by IoT devices is gaining more and more importance. Securing such IoT device data raises many challenges, particularly in environments with limited resources and heterogeneous platforms. (Fadhil et al., 2021), (Shahid, 2021).

There is a need to use a suitable mechanism to achieve security and privacy for data collected by IoT devices that are appropriate to the nature of the internet of things environments to protect the transmitted or stored image data. One of the solutions is to use an appropriate cryptographic algorithm. There are many symmetrical and asymmetrical cryptographic systems used to provide security services. However, most of the traditional cryptosystems cannot be used for secure IoT environments because most devices within IoT work with resources constrained such as processing speed, power, and storage capacity. Hence, the adaption of efficient techniques became a challenge to guarantee the security and privacy of data collected by the IoT network devices with efficient computation power, as well as provide trused security with cost and performance trade-offs. One efficient solution is to use cryptography, an effective tool to secure data delivered over IoT devices and networks or stored data. (Habeeba & Hussien, 2021), (Jumaa, 2017), (Tausif et al., 2017), (Staddon et al., 2021).

The Advanced Encryption Standard (AES) is one of the cryptographic data systems that has not yet been cracked. AES is a symmetric-key technique, meaning only duplicate keys for encrypting and decrypting processes are used. Three AES versions are adapted from the United States National Institute of Standards and Technology (NIST); the block size is 128.bit, but they differ in key length sizes: 128, 192, or 256 bits and number of round that depend on the key length. The AES system is referred to as the Rijndael algorithm, which

was developed by Joan Daemen and Vincent Rijmen. In this algorithm there are nine rounds, four operations are performed on the data in each of these nine rounds. In the case of encryption, the operations that are performed are: byte substitution (S-box), shift rows, mixcolumns, and add round key. In the tenth (last) round, the same operations are performed except for the Mix Columns transformation. In the case of decryption, the previous operations Are performed in reverse, the reverse operations are more complex compared to the same operations in the encryption. The number of rounds in this algorithm depends on the length of the key. (Mohialden et al., 2021), (Nabil et al., 2020), (Hussein et al.,2019), (William, 2017), (Jallouli, 2017).

Although the AES algorithm provides good security, but it needs high computing power to perform its operations within several used rounds, that needs more time for the encryption and decryption of the data. So, using the AES encryption system takes a long to perform its operations, making it unsuitable for devices with limited resources. At the same time, IoT processing devices have limited resources and are not able to perform operations in a fast manner in real time. The growth of image data gathering and processing needs to explore modern technologies that speed up processing, achieve high throughput, and lower power consumption in real-time. So, it is necessary to use suitable approaches to speed up its operations to meet these requirements using the AES algorithm by implementing it in a parallel manner. One of the solutions to increase processing speed is parallel processing. For every abstraction level, there are two basic methods for creating parallel computing structures spatial parallelism and temporal parallelism. Therefore, the researchers update architecture techniques to make the processing faster than before without changing the techniques themselves (Habeeba & Hussien, 2021), (Nabil et al., 2020), (Phadikar et al., 2020), (Hameed et al., 2018).

Spatial parallelism consists of several simultaneously executed tasks, computing n cells at a time with n duplicated pipelines. While in temporal parallelism, cascading *m* stream processing elements are based on coarse-grained pipelining of *m* successive iterations. Research and academics propose many devices and techniques in hardware and software implementations that use parallel processing to achieve this goal. One of the suitable candidates' approaches to implementing parallel processing is field-programmable gate arrays (FPGAs), which have features that meet parallel processing requirements for IoT environments (Kamalakkannan et al., 2021), (Phadikar et al., 2020), (Purkayastha et al., 2018), (Nagasu et al., 2016).

FPGAs provide the System on Chip (SoC) technique, in which the designer uses this to design and implement a large number of hardware clocks via a single chip only. FPGA can reconfigurable and process signals, manipulate them, and produce output pins efficiently, which helps to deem them as a special purpose reprogrammable processor. Embedded systems are most often the core of IoT devices as a result of their low power consumption and low price. (Zodpe & Sapkal, 2020), (Yazdeen et al., 2021).

The Field Programmable Gate Arrays (FPGAs), which are semiconductor devices, are based around a matrix of configurable logic blocks (CLBs) and constitute the main logic resource for implementing synchronous as well as combinatorial circuits, which are connected via programmable interconnects. Each CLB contains four slices, each containing two Look-Up Tables (LUTs) to implement logic and two dedicated storage elements that can be used as flip-flops or latches. Due to FPGAs, programmable nature is an ideal fit for many markets. One can be used FPGAs to implement any logical function that an Application Specific Integrated Circuit (ASIC) could perform. FPGAs have the ability to update the functionality, partially re-configuration a portion of the design, and the low costs

relative to an ASIC design, which offer many advantages for many applications implementation that need high processing power. The FPGA series produced by Altera is one of the most advanced FPGA families used in industry and education. The configurability of FPGA is generally specified using an HDL (Hardware Description Language) that is needed and important for describing the structure and functions of architectures to be designed. The proposed, designed architectures are implemented in this thesis using two boards the Altera FPGA devices. (Jasim Shaban, 2020), (Neelima, & Brindha, 2018).

This work presents a high-performance Quad-engines architecture aimed at overcoming the security and trust problems surrounding the Internet of Things using the Advanced Encryption Standard (AES) algorithm. It applies an FPGA-based embedded system to keep hardware costs as low as possible by employing them to perform independent computational tasks to process data in real-time. The proposed design uses two boards with different capabilities the Development and Education Kit (DE1) and the Nios II Embedded Evaluation Kit(NEEK), makes them compatible, allowing communication via Wi-Fi. Two approaches to architecture use spatial and temporal parallelism by using single or quad engines for secure data, which are suitable and convenient for IoT environments. The architecture works by partitioning each image into several parts and distributing these parts to four engines, where each image part is processed by one engine using concurrent spatial and temporal parallelism.

1.2 Problem Statements and Motivations

IoT applications have expanded into many aspects of our contemporary lives. This expansion was accompanied by significant growth in data gathering, transmitting,

processing, and storage, which included sensitive information. Most transmitted or stored data has become a target for intruders, hackers, and unauthorized access. Therefore, these IoT data challenges need mechanisms to protect them, which act as a gatekeeper of security within the whole life from all kinds of data corruption or unauthorized use. One of the most effective methods to protect them is to use powerful and trusted cryptographic security algorithms. These algorithms must meet the requirements of maintaining data security in an IoT environment without a standard encryption system that faces these security challenges and is commensurate with the capabilities of the devices. (Jeyanthi & Thandeeswaran, 2019), (Yazdeen et al., 2021), (Mohialden et al., 2020).

Many algorithms are proposed to encrypt/decrypt the data, each one has its pros and cons, but some of them are not suitable for the requirements of resource-constrained IoT devices since they need high computing power. Therefore, there is a need to use cryptographic algorithms that are appropriate to the nature of the IoT environments and match the capabilities of IoT devices by exploring modern technologies by speeding up the processing to achieve high throughput and lower power consumption within real-time processing. One of the most powerful and trusted cryptographic algorithms is the AES algorithm, which has immunity against comprehensive key search attacks and has not been known to be cracked until now. But the AES algorithm requires high computing capabilities, which are not available in some IoT devices due to the limited resources of those devices, which become less useful when used with sequential processing. So, there is a necessity to use parallel processing to speed up the processing while implementing the AES algorithm to save time and cost. This requires designing processing architectures using modern technology to conduct parallel processing. (Nabil et al.,2020), (Arul Murugan et al., 2020), (Rajasekar & Mangalam, 2020), (Rao & Sharma, 2017).

Many techniques can be used for parallel processing in hardware and software for implementing parallel processing. One of the suitable candidates' approaches to achieving this goal is field-programmable gate arrays (FPGAs), which have good features such as reliability, flexibility, low cost, and long-term maintenance that meet processing requirements suitable for IoT environments. (Boutros & Betz, 2021), (Jasim Shaban, 2020) (Behera et al., 2019), (Shiddibhavi, 2019).

1.3 Research Objective

This research aims to design and optimize an end-to-end architecture implementing an AES algorithm on FPGA to optimize power, increase processing speed, and evaluate its effectiveness. Specifically, to study the following.

1. To design an end-to-end architecture suitable for implementing the AES algorithm in an IoT environment.
2. To improve data processing speed and gain high throughput by implementing temporal and spatial parallelism.
3. To evaluate the design performance of the proposed architecture in term of its performance efficiency.

1.4 Research Scope

In the Internet of Things environment, huge amounts of data, especially images, are transmitted. The processing of these images requires high computing power. Thus, in order to obtain high throughput, the design and implementation of a processing architecture capable of performing the required processors~~;~~ such as image encryption and decryption quickly. The dissertation focuses on speeding up the image processing transmitted through

IoT environments due to some resource constraints to obtain higher throughput. The processing speed depends on designing a parallel processing architecture that makes use of modern FPGA techniques. The FPGA technique provides a reconfigured integrated circuit containing Configurable Logic Blocks (CLBs) arrays. In addition, the application of the spatial and temporal parallelism method in behavior design leads to a high-performance power processor with high throughput, called "processed quad computing engines." To secure the transmitted image within IoT applications, a secure cryptographic 128-bit AES algorithm is used to encrypt images while transferring in an IoT environment to ensure security by coding it in VHDL and simulating it on board an FPGA.

The proposed architecture takes into consideration using a heterogeneous device, different devices at the sender and receiver. The DE1-SoC and NEEK board's hardware implementation is a Cyclone V (5CSEMA5F31C6) FPGA device running at 50 MHz However, the FPGA chip's processing handles all data and directive operations to manipulate the area and the engine's throughput and F(max) to achieve a low-area, high-performance implementation of the process.

1.5 Thesis Organization

The thesis organization contains five chapters as follows: Chapter 2 introduces the FPGA-IoT. This chapter introduces a briefly related work that was accomplished in this area of FPGA architectures and the system advantages, and introduction of various aspects of FPGA applications with IoT. Chapter 3 describes the implementation of the AES algorithm with a new architecture to achieve the project's goal. The chapter provides a highlighted overview of the Parallelism design, its modules, and their functionality. Chapter 4 presents the results obtained, a discussion, and a detailed explanation of the investigation and

implementation phases. Chapter 5 conclude the entire implementation of the system and future work is also discussed.