UNIVERSITI PUTRA MALAYSIA

HARDWARE IMPLEMENTATION OF RC4A STREAM CIPHER ALGORITHM

ABDULLAH AL NOMAN

HARDWARE IMPLEMENTATION OF RC4A STREAM CIPHER ALGORITHM

By

ABDULLAH AL NOMAN

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, In Fulfillment of the Requirement for the Degree of Masters of Science

January 2007

DEDICATION

The Thesis is dedicated
To

My Parents
Dr. Abdullah Al Mamun and Late Amatun Nur Salina

My grandparents
Late Amanat Ullah and Hiron Nesa

My Wife
Dr. Teyeba Begum

&

My Son
Labib Ahmad

Abstract of the thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirements for the degree of Master of Science

HARDWARE IMPLEMENTATION OF RC4A STREAM CIPHER ALGORITHM

By

ABDULLAH AL NOMAN

January 2007

Chairman: Roslina Mohd Sidek, PhD.

Faculty: Engineering

The security of sensitive information against ‘prying eyes’ has been of prime concern throughout the centuries. Therefore, a mechanism is required to guarantee the security and privacy of information. Under the existing circumstances cryptography is the only convenient method for protecting information transmitted through communication networks. The hardware implementation of cryptographic algorithms plays an important role because of growing requirements of high speed and high level secure communications.

Accordingly, in this research attempt is taken to develop a faster and reliable cryptographic hardware by implementing one of the stream ciphers, RC4A in hardware. Verilog Hardware Description Language (HDL) and top down design methodology has been used to design the hardware implemented in this thesis. For hardware implementation of the design, an Altera Field Programmable Gate Array (FPGA) device, EP20K200EFC484-2X from APEX family, APEX 20KE, has been used. The designed hardware consumed 480 logic elements, 146 I/Os, and 10,240 bits memory. The hardware implementation achieved the data transfer rate of 22.28 MB/S in a clock frequency of 33.33 MHz. The implementation is able to support variable key lengths from 8 bits up to 512 bits. Unlike other stream ciphers, the proposed implementation generates two output streams at a time, whereas others generate only one output stream. So, user may use any of keystream which increase the unpredictability of the key as well as security.

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

PELAKSANAAN PERKAKASAN BAGI ALGORITMA ALIRAN KOD RAHSIA RC4A

Oleh

ABDULLAH AL NOMAN

Januari 2007

Pengerusi: **Roslina Mohd Sidek, PhD.**

Fakulti: **Kejuruteran**

Keselamatan terhadap kebocoran maklumat yang sensetif daripada pengetahuan pihak yang tidak dibenarkan menjadi suatu kebimbangan sejak berkurun lamanya. Justeru itu, suatu mekanisma diperlukan untuk memastikan keselamatan dan kerahsiaan maklumat. Kriptografi merupakan satu-satunya cara yang paling mudah untuk melindungi maklumat yang dihantar melalui jaringan komunikasi. Implementasi perkakasan dalam algoritma kriptografi memainkan peranan yang sangat penting disebabkan oleh peningkatan keperluan terhadap komunikasi yang berkelajuan tinggi dan tinggi jaminan keselamatannya.

Melalui kajian ini, usaha diambil untuk membangunkan cip kriptografi yang lebih laju dan mempunyai kebolehkepercayaan yang tinggi melalui implementasi salah satu daripada aliran kod rahsia, RC4A di dalam perkakasan. Implementasi perkakasan yang dicadangkan di dalam tesis ini menggunakan bahasa perihalan perkakasan dan metodologi rekabentuk atas bawah. Bagi rekabentuk implementasi perkakasan, *Altera Field Programmable Gate Array (FPGA)*, *EP20K200EFC484-2X* daripada keluarga *APEX*, *APEX 20KE* telah digunakan. Rekabentuk perkasakan ini mengandungi 480 elemen logik, 146 masukan/keluaran dan ingatan sebanyak 10,240 bits. Implementasi perkakasan ini telah mencapai kadar penghantaran data sebanyak 22.28 MB/S dalam frekuensi jam sebanyak 33.33 MHz. Implementasi ini mampu menyokong pelbagai jenis panjang kunci dari 8 bits hingga 512 bits. Tidak seperti aliran kod rahsia yang lain yang hanya boleh menjana satu keluaran aliran, aliran kod rahsia ini boleh menjana dua keluaran stream pada masa yang sama. Dengan ini, pengguna boleh menggunakan mana-mana kekunci yang dapat meningkatkan ketidaktentuan kekunci disamping meningkatkan juga keselamatan.

Acknowledgement

In the name of Allah (God), The Merciful, the Compassionate.

Indeed Allah (God) is with those who fear Him and those who do good. [Qur'an16:128]

Glory be unto You! We have no knowledge save that which You have taught us; You are All-Knowing All Wise. [Qur'an 2:32.]

Bismillah, "In the name of Allah (God)," is the start of all things good. Me too shall start with it.

First of all I bear in mind the Greatness of Allah (God) The Merciful, the Compassionate, from Him do we seek help, allow me to complete this work successfully. All praise be to Allah (God), the Sustainer of All the Worlds, and blessings and peace be upon our Prophet Muhammad (SA) and on all his Family and Companions.

Credit for much of the work described in this thesis belongs to my Supervisor, Dr Roslina Mohd Sidek, for her insight, guidance, and patience. She provided an excellent research environment, left me enough freedom to do things the way I thought they should be done, and was always available to discuss ideas and problems. I would also like to thank my committee member Assoc. Professor Dr. Abdul Rahman b. Ramli. Their doors were always open for me to get help and suggestions whenever needed. It is beyond doubt that without their assistance, it was impossible for me to complete this thesis work.

I also would like to say that I should never forget Dr. Liakat Ali, for me previous supervisor. During his short stay he helped me a lot to streamline this thesis.

Appreciation also to my parents, who provided the item of greatest worth - opportunity. Thank you for standing by me through the many trials and decisions of my educational career. I would like to thank my parents in law, uncles, aunties, grandparents, cousins. Special thanks go out to my younger brother Abdullah Al Makin for his unconditional help throughout my life.

I owe a lot to my friend Rafizi Affandi for his contributions in the proposed research. Our conversations and work together have greatly influenced this thesis.

My appreciation and thanks to all around my surrounding especially Mehdi & his family, Oliullah vi, Dr. Ekram & his family, Dr. Rowsan & his family, Dr. Awal & his family, Eyakub vi, Sadat vi, Lotus vi, Zia vi, Asad vi, all my school, college and university friends.

At the end, my sincere gratitude goes to my wife Dr. Teyeba for her constant encouragement and supports. Her sacrifice for me is beyond description. Thanks also to my son, Labib Ahmad, who was a great joy and motivation for me.

I certify that an Examination Committee has met on date of viva to conduct the final examination of Abdullah Al Noman on his Master of Science thesis entitled “Hardware implementation of RC4A Stream Cipher Algorithm" 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:

Sudhanshu Sheker Jamuar, PhD
Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Syed Javaid Iqbal, PhD
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Mohd Nizar Hamidon, PhD
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Mohd Alauddin Mohd Ali, PhD
Professor
Faculty of Engineering
Universiti Kebangsaan Malaysia
(External Examiner)

HASANAH MOHD. GHAZALI, PhD
Professor/Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 9 August 2007

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

Roslina Mohd Sidek, PhD
Lecturer
Faculty of Engineering,
Universiti Putra Malaysia
(Chairman)

Abdul Rahman B. Ramli, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

AINI IDERIS, PhD
Professor/Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 9 August 2007

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.

ABDULLAH AL NOMAN

Date: 2 August 2007

TABLE OF CONTENTS

Page

APPENDICES

LIST OF TABLES

LIST OF FIGURES

Figures **Pages**

Figures **Pages**

LIST OF ABBREVIATIONS

CPLD	Complex Programmable Logic Device
CLB	Configurable Logic Blocks
ESB	Embedded System Block
EDA	Electronic Design Automation
ECB	Electronic Codebook
FPGA	Field Programmable Gate Array
GUI	Graphical User Interface
GSM	Global System for Mobile communication
HDL	Hardware Description Language
IC	Integrated Circuit
I/O	Input/Output
KSA	Key Scheduling Algorithm
LPM	Linear Parameterized Module
LUT	Look up tables
LAB	Logic Array Block
LFSR	Linear Feedback Shift Registers
OFB	Output Feedback
OVI	Open Verilog international
PRGA	Pseudo Random number Generation Algorithm
PRNG	Pseudorandom Number Generator
RAM	Random Access Memory

SOPC	System-On-a-Programmable-Chip
SOC	System On a Chip
SDRAM	Static Dynamic RAM
UART	Universal Asynchronous Receiver and Transmitter
VHDL	Very High Speed Hardware Description Language
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network

TITLE

HARDWARE IMPLEMENTATION OF RC4A STREAM CIPHER ALGORITHM

ABSTRACT

The security of sensitive information against ‘prying eyes’ has been of prime concern throughout the centuries. Therefore, a mechanism is required to guarantee the security and privacy of information. Under the existing circumstances cryptography is the only convenient method for protecting information transmitted through communication networks. The hardware implementation of cryptographic algorithms plays an important role because of growing requirements of high speed and high level secure communications.

Accordingly, in this research attempt is taken to develop a faster and reliable cryptographic hardware by implementing one of the stream ciphers, RC4A in hardware. Verilog Hardware Description Language (HDL) and top down design methodology has been used to design the hardware implemented in this thesis. For hardware implementation of the design, an Altera Field Programmable Gate Array (FPGA) device, EP20K200EFC484-2X from APEX family, APEX 20KE, has been used. The designed hardware consumed 480 logic elements, 146 I/Os, and 10,240 bits memory. The hardware implementation achieved the data transfer rate of 22.28 MB/S in a clock

frequency of 33.33 MHz. The implementation is able to support variable key lengths from 8 bits up to 512 bits. Unlike other stream ciphers, the proposed implementation generates two output streams at a time, whereas others generate only one output stream. So, user may use any of keystream which increase the unpredictability of the key as well as security.

Chapter 1

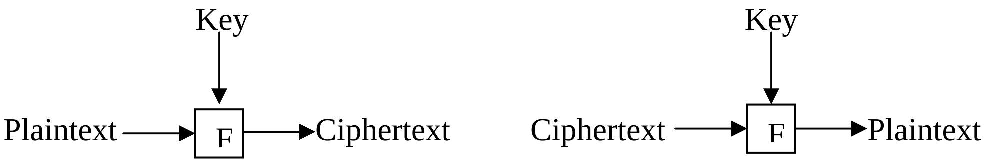
INTRODUCTION

1.1 Introduction to Cryptography

The term "cryptography"("secret writing") derived from the Greek word *kryptós*, "hidden" and *gráphein*, "to write" is often used to refer to the field as a whole, as is "cryptology" ("the study of secret writing"). The study of how to circumvent the use of cryptography is called "cryptanalysis" or, loosely, "code breaking." The term "cryptology" originally designated for the "study of secret writing" for purposes of maintaining and/or breaching the security of "cryptography" ("secret writing").

Cryptography or cryptology is a field of mathematics and computer science concerned with information security and related issues, particularly encryption. Technically, "cryptography" refers to the use and practice of cryptographic techniques and "cryptology" to refer to the subject as a field of study; despite this, the term "cryptography" is often used to refer to the entire field. Cryptography is an interdisciplinary subject, drawing from several fields. Older forms of cryptography were chiefly concerned with patterns in language. More recently, the emphasis has shifted, and cryptography makes extensive use of mathematics, particularly discrete mathematics, including topics from number theory, information theory, computational complexity, statistics and combinatories. Cryptography is also considered a branch of engineering, but it is considered to be an unusual one as it deals with active, intelligent and malevolent opposition. Cryptography is a tool used within computer and network security [10, 11, 19, and 24].

Until modern times, cryptography referred almost exclusively to encryption, the process of disguising a message in such a way as to hide its substance. The message or the original information is known as plain text. The encrypted message is known as cipher text. Decryption is the reverse, turning cipher text back into plaintext. A cipher is a pair of algorithms which perform this encryption and the reversing decryption. A key is a piece of information that controls the operation of a cryptography algorithm. In encryption, a key specifies the particular transformation of plaintext into cipher text, or vice versa during decryption. For encryption, $c=e_k(m)$, where m is the plaintext, e is the encryption function, k is the secret key, c is the cipher text. For decryption, $m=d_k(c)$, where m is the plaintext, d is the decryption function, k is the secret key, c is the cipher text. Encryption and decryption is presented in Figure 1.1.



(a) Encryption **(b) Decryption**

Figure 1.1: Encryption and Decryption.

Historically, cryptography was concerned solely with encryption; that is, means of converting information from its normal, comprehensible form into an incomprehensible