Ain Shams University
Faculty of Engineering
Computer and Systems Engineering Department

Efficient Techniques for Cryptographic Algorithms Implementation

A Thesis
Submitted in partial fulfillment for the requirements of
Master of Science degree in Electrical Engineering

Submitted by:

Ahmad Mohammad Abdel-Fattah Ahmad

B.Sc. of Electrical Engineering
(Computer and Systems Engineering Department)
Ain Shams University, 2006

Supervised by:

Prof. Dr. Hossam Mahmoud Ahmed Fahmy

Dr. Ayman Mohammad Bahaa Eldin

April 2010
Cairo

Statement

This dissertation is submitted to Ain Shams University for the degree of Master of Science in Electrical Engineering (Computer and Systems Engineering).

The work included in this thesis was carried out by the author at the Computer and Systems Engineering Department, Faculty of Engineering, Ain Shams University, Cairo, Egypt.

No part of this thesis was submitted for a degree or a qualification at any other university or institution.

Name: Ahmad Mohammad Abdel-Fattah Ahmad
Date: July 13, 2010

Acknowledgements

All praise is due to Allah, Most Merciful, the Lord of the Worlds, Who taught man what he knew not. I would like to thank God Almighty for bestowing upon me the chance, strength and ability to complete this work.

I wish to express my gratitude to my supervisors, Professor. Hossam Mahmoud Fahmy and Dr. Ayman Mohammad Bahaa Eldin for their exceptional guidance, encouragement, insightful thoughts and useful discussions. It was my great pleasure to work with them.

I am in no way capable of appropriately thanking my parents for their unconditional love and unlimited support.

Ahmad Mohammad Abdel-Fattah
Computer and Systems Engineering Department
Faculty of Engineering
Ain Shams University
Cairo, Egypt
2010

Abstract

The aim of this thesis is to develop a cryptographic accelerator module, focusing on public-key cryptographic algorithms.

Most public key cryptographic algorithms require heavy computational effort. This is due to the reliance on modular arithmetic over very large operands. Typical bit length of operands in public key ciphers is 1024 bits or even higher. Examples of such ciphers are RSA and Elliptic Curve Cryptography (ECC). Almost all public key algorithms involve modular multiplication and modular exponentiation. Such operations become very time-consuming when operating on large operands. Modular multiplication is the core of modular exponentiation.

Many algorithms have been developed to accelerate modular multiplication on general purpose processors. The common target of any accelerating algorithm is to avoid the ordinary pencil-and-paper steps. Many researchers managed to reduce both time and space complexities of modular multiplication.

However, considering embedded security devices such as smart cards and cryptographic tokens, the limited processing power of embedded microprocessor forces the need for more research to accelerate cryptographic algorithms on embedded platforms. The fast evolution of VLSI designs using Field Programmable Gate Arrays (FPGAs) and Application Specific Integrated Circuits (ASICs) has introduced further level of enhancement. The enhancement would be on the hardware level in the form of a cryptographic co-processor.

A cryptographic co-processor is a hardware accelerator that is specifically designed to perform complex cryptographic operations. The integration of such co-processor to a general purpose embedded CPU introduces an excellent platform for portable security devices.

In this thesis, a new hardware architecture for a modular multiplier is introduced. The design can be used to enhance the performance of all public key cryptosystems. The proposed architecture is based on the interleaved modular multiplication algorithm. It scores better timings (considering both operating frequency and total operation time)than the latest known designs to the author's knowledge. Further enhancements have been proposed to support parallel processing and different operand sizes. The proposed designs have been developed using a Hard-

ware Description Language (HDL). They have also been integrated to a soft processor core so that a complete platform is produced.

Contents

List of Figures

List of Tables

List of Symbols

AES	Advanced Encryption Standard
ALU	Arithmetic and Logic Unit
ASIC	Application Specific Integrated Circuit
CLA	Carry Lookahead Adder
CMM	Chained Modular Multiplier
CPU	Central Processing Unit
CRT	Chinese Remainder Theorem
CSA	Carry Save Adder
DES	Data Encryption Standard
DH	Diffie-Hellman
DMIPS	Dhrystone Million Instruction per Second
DPU	Data Processing Unit
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
FSM	Finite State Machine
GCD	Greatest Common Divisor
HDL	Hardware Description Language
IMM	Interleaved Modular Multiplication
KDC	Key Distribution Center

LHS	Left Hand Side
MIMM	Modified Interleaved Modular Multiplication
MSB	Most Significant Bit
NIST	National Institute of Standrads and Technology
PCB	Printed Circuit Board
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastrcture
RHS	Right Hand Side
RCA	Ripple Carry Adder
RNS	Residue Number System
RSA	Rivest-Shamir-Adelman
SHA	Secure Hash Algorithm
UUT	Unit Under Test

Chapter 1

Introduction to Cryptology and Public Key Cryptography

This chapter discusses the basic principles of public key cryptography, and the difference between symmetric and asymmetric (public key) cryptographic algorithms. It also points out the appearing challenges when implementing a public key cryptosystem. The chapter also clarifies the objective of this thesis. It then presents the methodology followed during the research. The chapter ends with an illustration of the thesis structure.

1.1 Overview

Cryptology is defined as the study of techniques for ensuring the secrecy and authenticity of information [1]. The study of cryptology is divided into two main categories: Cryptography and Cryptanalysis. Cryptography involves methods and techniques to achieve the secrecy of data. Such secrecy should be accomplished using an encryption/decryption algorithm (cipher). Cryptanalysis is the study of different ways to attack a cryptographic algorithm in order to break the security of information. Cryptanalysis provides methodologies for measuring how strong a cipher is. In this work, a focus is made on cryptography.