擴充式字元基礎蒙哥馬利乘法演算法之改進

學生：楊程翔　　指導教授：李程輝 教授

國立交通大學電信工程研究所

中 文 摘 要

隨著有線、無線通訊的發展，安全性的考量也日益重要。許多網路上的應用如電子商務、網路銀行…等，都需要一個完整的安全機制來保證其安全性；其基本上的安全需求，包含有隱密性，可認證性，資料的完整性和不可否認性。為了提供上述的安全服務，大多的網路系統使用公開金鑰密碼系統。而在各種公開金鑰密碼系統的演算法中，現今最著名的是RSA 密碼系統，且由於其多功能性，所以被公開金鑰密碼系統廣泛使用。在公開金鑰密碼系統演算法中，其最主要的運算是模數的乘法，它是被利用來計算模數的指數運算。然而，模數的指數運算，當模數的位元數高達512 位元以上，將使得RSA 密碼系統，很難有較快速運算的處理能力。因此擁有較高的資料處理能力是RSA 密碼系統最主要改善的地方。另外，隨著破密學的發展以及硬體製程的進步，破解RSA密碼系統所需要的時間愈來愈短；因此，增加RSA金鑰位元數來達成更佳的安全性也是未來的趨勢之一

在RSA加密演算法中，長整數模數指數運算是主要的運算，模數指數運算是由連續的模數乘法所組成，所以一個快速的模數乘法演算法是非常重要的。因此我們提出一個改進的字元基礎蒙哥馬利乘法演算法(Modified Word based Montgomery Multiplication Algorithm)來加速RSA加密演算法的運算。字元基礎的架構同時可以提供硬體的可擴充性；若是想加強系統安全性而增加金鑰位元數，僅需要調整舊有的硬體即可，並不需要重新換一套新的硬體，而其所需付出的代價是時間的增加。這對於目前的企業來說是相當的有吸引力的，若是因為想增加系統安全性而必須另外買一套硬體，對企業或是使用者而言都是極重的負擔。而我們提出的硬體架構，不但延續了"可擴充性"這個優點，其速度及效能更較之前所提出的方法佳。在TSMC 0.25μm的製程以及Synopsys Design Analyzer軟體的模擬環境下，我們8位元單一元件的設計總共只需要784個邏輯閘，並且系統整體能達到588.23Mbps的高速資料處理量。

A Modified Word Based Montgomery Multiplication Algorithm

Student: Cheng-Xiang Yang Advisor: Dr. Tsern-Huei Lee

Institute of Communication Engineering
National Chiao Tung University

Abstract

With the rapid growth of Internet applications and various information devices, security of our data becomes an important issue. RSA algorithm is the most popular public key system in the world. The main computation of RSA algorithm is modular exponentiation. Therefore, how to make the computation of modular exponentiation faster is the major problem.

In this thesis, we present a Modified Word-Based Montgomery Multiplication Algorithm. The proposed multiplier is able to work with any precision of the input operands, limited only by memory or control constraints. Its architecture gives enough freedom to select the word size and the degree of parallelism to be used, according to the available area and/or desired performance. We use the ASIC design flow to implement this modified architecture. Using TSMC 0.25 μm CMOS process technology and Synopsis Design Analyzer, the 8 bits single processing element of our design costs 784 gate counts , and our system can achieve a high throughput of 588.23Mbps.

誌 謝

首先我要對我的指導教授李程輝教授致上最由衷、最誠摯的感謝。感謝他在我研究所這兩年的時間內不厭其煩的指導我研究的方向和架構的設計，並給我相當中肯且實用的建議，讓我在論文研究的過程中瞭解到如何去思考一個問題、如何去解決問題，著實讓我獲益良多。另外，我也要感謝網路技術實驗室的成員們能夠在我遇到困難的時候，提供給我適當的協助，並且也度過了許多歡笑的時光。最後，我要感謝我的父母以及我的哥哥，特別是敏綺，是他們不斷的給我支持與鼓勵，使得我有力量完成這篇論文。謹以此論文獻給他們，還有許許多多幫助我，鼓勵我的人。

Contents

中文摘要 i

Abstract ii

誌謝 iii

Contents iv

List of Tables vi

List of Figures vii

Chapter 1 Introduction 1

1.1 Introduction 1

1.2 Background 2

1.2.1 Cryptography 2

1.2.2 Secret Key 4

Cryptosystem

1.2.3 Public Key 5

Cryptosystem

Chapter 2 The RSA Cryptosystem 8

2.1 The RSA Algorithm 8

2.1.1 Number Theory 8

2.1.2 The RSA Scheme 9

2.2 Digital Signature 11

2.3 The security of RSA 12

Chapter 3 Scalable Montgomery Multiplication Architecture. 15

3.1 Modular Exponentiation Operation 15
3.1.1 Modular Exponentiation Algorithm 15
3.1.2 Montgomery Modular Multiplication Algorithm 17
3.1.3 Appling Montgomery Algorithm to Modular Exponentiation 18
3.2 Scalable Architecture for Montgomery Multiplication 20
3.2.1 Scalability 20
3.2.2 A Word-Based Radix-2 Montgomery Multiplication Algorithm 21
3.3 Mapping the MWR2MM Algorithm to Hardware 22
3.3.1 Parallel Computation of the MWR2MM 22
3.3.2 Scalable Architecture for Montgomery Multiplication 25
3.3.3 The Final Word Adder and Subtraction 30
3.4 An Improved Scalable Montgomery Multiplication Architecture 32
Chapter 4 Simulation Result 37
4.1 Design Evaluation 38
4.2 Experimental Result 39
4.2.1 A Single Processing Element 40
4.2.2 Synthesis result 41
Chapter 5 Conclusion 43
Reference 44

List of Tables

Table 2.1 Progress in factorization …….. 14

Table 3.1 The difference between the two MWR2MM algorithm …….. 34

Table 3.2 The area and data arrive time between Mux and Full Adder …….. 34

Table 4.1 The clock rate and gate count of different adders …… 39

Table 4.2 A single 8 bits and 16 bits PE's area of Koc's architecture and our architecture 40

Table 4.3 The speed and area of the original design with different PEs …….. 41

Table 4.4 The speed and area of the improved design with different PEs ….. 41

Table 4.5 The speed and area of the original design with different precision of PEs …… 42

Table 4.6 The speed and area of the improved design with different precision of PEs …….. 43

List of Figures

Figure 1.1 Cryptosystem process 3

Figure 1.2 Block diagram of secret-key cryptosystem …… 4

Figure 1.3 Block diagram of public-key cryptosystem ……... 7

Figure 2.1 An example of RSA encryption/decryption ……..... 11

Figure 3.1 Montgomery Modular Exponentiation Algorithm …..... 19

Figure 3.2 The dependency graph for the MWR2MM algorithm …..... 23

Figure 3.3 An example of pipeline computation for 7-bits operands, where w = 1.. 24

Figure 3.4 An example of pipeline computation for 7-bit operands, where w = 1.. 25

Figure 3.5 Pipelined organization for the multiplier …….... 26

Figure 3.6 The block diagram of the processing element (PE) ……... 26

Figure 3.7 PE's data path for w = 3 bits ……... 27

Figure 3.8 The cycle time of different configurations which n = 256 ……. 29

Figure 3.9 The cycle time of different configurations which n = 1024 ……... 30

Figure 3.10 The Word Adder for Final Addition ……... 31

Figure 3.11 Converting the result to final form in the last stage of the pipeline …. 32

Figure 3.12 An example of improved architecture's data path ……. 35

Figure 3.13 The diagram between two multiplications of exponential computation …..... 36

Figure 4.1 The design flow of our Architecture ……..... 38

Figure 4.2 The symbol view of 8 bits PE …… 40

Figure 4.3 The symbol view of the final design ……. 42