橢圓曲線密碼系統於有限場 $GF(p)$和 $GF(2^m)$之硬體實現

學生： 盧冠州　　　　　　　　　指導教授： 李程輝 教授

國立交通大學電信工程學系碩士班

中文摘要

近年來廣為使用的 RSA 密碼系統，為了保持一定的安全性，其金鑰位元長度不斷的增加，進而加重了 RSA 的運算複雜度。相對於 RSA，橢圓曲線密碼系統（ECC）逐漸被重視。在西元 1985 年，Koblitz 與 Miller 提出橢圓曲線密碼系統，其安全性是建立在橢圓曲線離散對數問題（ECDLP）。目前已經被廣泛地制定於國際標準如 ISO 11770-3、ANSI X9.62、IEEE P1363、FIPS 186-2 等。

橢圓曲線密碼系統的優點是，在相同的安全性下，其所使用的金鑰長度比 RSA 密碼系統短（1024 位元 RSA 密碼系統的安全強度等於 155 位元的 ECC）。這個好處可以應用在智慧卡或行動電話這種記憶體跟運算能力有限的系統上面。

本論文在實作方面是利用 Verilog 硬體描述語言來撰寫橢圓曲線密碼系統。我們採用 A.F. Tenca 和 C.K. Koc 所提出的用於蒙哥馬利乘法的可擴充性架構[32]，並改良使之可以支援有限場 $GF(p)$和 $GF(2^m)$的運算。另外我們採用 Projective 座標系統，將除法運算轉變為乘法運算，進而降低運算結果的時間。我們利用 Synopsys 的合成軟體來將 Verilog codes 合成成電路，並加以模擬驗證。

Hardware Implementation of Elliptic Curve Cryptosystem over Finite Fields *GF*(*p*) and *GF*(2^m)

Student: Guan-Zhou Lu Advisor: Prof. Tsern-Huei Lee

Department of Communication Engineering

National Chiao-Tung University

Abstract

The RSA cryptosystem used widely in recent years, for keeping the certain security degree, continuous to increase the length of public key, and aggravated the RSA to operate the complicacy. Opposite to RSA, the Elliptic Curve Cryptosystem (ECC) attracts more and more attention. In 1985, Koblitz and Miller proposed a higher security public key cryptosystem, based on ECDLP, called ECC. At present, there are several international standards proposed in ISO 11770-3, ANSI X9.62, IEEE P1363, FIPS 186-2.

The advantages of ECC are that its key sizes are smaller than RSA with equivalent levels of security (1024 bits RSA is equal to 155 bits ECC) so that it can be implemented in smart card or mobile phone.

In this thesis, we developed the hardware implementation of ECC by using Verilog HDL. We adopted the scalable architecture for Montgomery multiplication proposed by F.A. Tenca and C.K. Koc [32], and modified it to support the operations

over dual-field *GF*(*p*) and *GF*(2^m). Also, the inversion is designed in the projective coordinates that will save much computation time. We synthesize our verilog codes by software of Synopsys, and confirm by simulation.

誌 謝

研究所兩年的時間，過程辛苦但也很充實。其中我最感謝的是我的指導教授李程輝教授，在我的論文研究上不厭其煩的給予我指導。不論在研究的方向或者是架構的設計等等，都給了我相當中肯且實用的建議；並且讓我在論文研究的過程中瞭解到如何去發現問題、思考問題最後解決問題，著實讓我獲益良多。其次，我要感謝網路技術實驗室的同學－程翔、思儒、克偉、柏成、柏均以及麗雲。他們在我的研究過程中給予了我相當的幫助，在我程式寫不出來的時候為我加油打氣，讓我得以順利的完成此篇論文。另外我也要感謝網路技術實驗室的學弟、妹們，陪我一起度過了許多歡笑以及難過的時光。最後，我要感謝我的父母親以及我的女朋友，不斷的給我支持與鼓勵，使得我有力量完成這篇論文。謹以此篇論文獻給我的家人以及所有曾經關心過我、陪我一起歡笑一起難過的朋友們。

Contents

List of Tables

List of Figures