國 立 交 通 大 學

電 信 工 程 學 系

碩 士 論 文

橢圓曲線密碼系統於有限場 $GF(p)$和 $GF(2^m)$ 之硬體實現

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

研 究 生： 盧冠州

指導教授： 李程輝 教授

中華民國九十三年六月

橢圓曲線密碼系統於有限場 $GF(p)$和 $GF(2^m)$之硬體實現

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

研 究 生： 盧冠州　　Student: Guan-Zhou Lu

指導教授： 李程輝 教授　　Advisor: Prof. Tsern-Huei Lee

國 立 交 通 大 學

電 信 工 程 學 系

碩 士 論 文

A Thesis

Submitted to Department of Communication Engineering

College of Electrical Engineering and Computer Science

National Chiao Tung University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in

Electrical Engineering

June 2004

Hsinchu, Taiwan, Republic of China.

中華民國 九十三 年 六 月