國立交通大學

資訊工程學系

碩 士 論 文

替換排列網路之線性攻擊策略

Attack Strategies of Linear Cryptanalysis on SPN

研 究 生：陳政愷

指導教授：陳榮傑　教授

中 華 民 國 九 十 四 年 六 月

替換排列網路之線性攻擊策略
Attack Strategies of Linear Cryptanalysis on SPN

研 究 生：陳政愷　　Student：Cheng-Kai Chen

指導教授：陳榮傑　　Advisor：Dr. Rong-Jaye Chen

國 立 交 通 大 學

資 訊 科 學 系

碩 士 論 文

A Thesis

Submitted to Department of Computer Science and Information Engineering

College of Electrical Engineering and Computer Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Computer Science and Information Engineering

June 2005

Hsinchu, Taiwan, Republic of China

中華民國九十四年六月