URN etd-0407109-183703-192
Author Yu-Jen Pan
Author's Email Address No Public.
Statistics This thesis had been viewed 65 times. Download 0 times.
Department
Year 2005
Semester 1
Degree Master
Type of Document Master's Thesis
Language zh-TW.Big5 Chinese
Title The implementation of RSA cryptosystem
Date of Defense 0000-00-00
Page Count 51

Keyword
public key cryptography
RSA
serial-parallel multiplier

Abstract
With the fast development in internet networks and the increasing needs of communication products, the question of information safety is more and more important. To provide such security services, most systems use public key cryptography. Among the various public key cryptography algorithms, the RSA proposed by Rivest, Shamir, and Adleman is one of the most popular and reliable method that has been widely used today to provide secure data transmission. In this thesis, we focus on the hardware implementation of the RSA cryptosystem. For area consideration, we have proposed a new logic implementation method for the serial-parallel multiplier to reduce the area of RSA system. By using our new multiplier the area of the RSA system can be efficiently reduced as comparing to the previous methods. Finally, we realize the RSA cryptosystem on a Altera FPGA.
Advisory Committee Tzu-Kun Tien - advisor

Files No Any Full Text File.
Date of Submission 2006-08-10