URN etd-0407109-183719-1566
Author Chaol-Lung Hsu
Author's Email Address No Public.
Statistics This thesis had been viewed 53 times. Download 0 times.
Department
Year 2007
Semester 2
Degree Master
Type of Document Master's Thesis
Language zh-TW.Big5 Chinese
Title The Implementation of RSA System on an Embedded System
Date of Defense 0000-00-00
Page Count 51
Keyword
Public key cryptography
RSA
Embedded system

Abstract
Along with the progress of computer science and technology, the development of internet brings humanity the convenience accompanying with the data security problem. In order to guarantee the security of data transmitting, the cryptography system is used to encrypt the original data before it has been transmitted. Most crypto 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. Because the RSA cryptographic system needs the massive multiplication operation, the implementation of RSA system usually uses the specific hardware circuit to make the encryption and the decipher work. In this thesis, we use soft/hardware co-design method to realize the RSA cryptography system on an embedded system. The circuit of RSA system is implemented on the FGPA to speed up the encryption procedure and decryption procedure. The experimental result shows that the operation frequency of the RSA system can reach 48.78 MHz.
Advisory Committee Tzyy-Kuen Tien - advisor

Files No Any Full Text File.
Date of Submission 2008-07-30