学校编码：10384　　分类号＿＿＿＿密级＿＿＿
学号：231200811531176　　UDC ＿＿＿＿＿＿＿＿

硕 士 学 位 论 文

可重用可信平台模块 IP 核设计
Design of Reusable Trusted Platform Module IP core

刘智超

指导教师姓名：　王云峰　讲师
专 业 名 称：　电路与系统
论文提交日期：　2011　年　　月
论文答辩日期：　2011　年　　月
学位授予日期：　2011　年　　月

答辩委员会主席：＿＿＿＿＿＿
评　　阅　　人：＿＿＿＿＿＿

2011 年 5 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

由于计算机和通信网络的广泛应用，信息安全得到了广泛的重视，从政治军事到金融业商业，各个领域对敏感信息的保护都提出了迫切要求。为了解决信息安全与保密问题，多种技术被提出；其中，可信计算技术是当前研究热点。有别于传统的安全技术，可信计算技术通过可信平台模块保证网络的信息安全。

随着半导体制造技术的快速发展，芯片集成规模按照摩尔定律飞速提高，集成电路设计已经进入了片上系统时代；但集成电路市场竞争日趋激烈和产品寿命周期的日益缩短要求芯片的设计周期必须缩短。目前，IP 重用技术是解决设计复杂度与设计周期短这一矛盾的有效手段。论文采用了 IP 重用技术进行可信平台模块设计；同时，所设计的可信平台模块满足 IP 重用标准，可被重用于复杂 SoC 芯片设计。

可信平台模块通常由处理器、密码引擎、存储器、IO 等模块构成。存储器设计技术发展快速，通常采用特殊的工艺降低成本，更新换代周期短。因此论文设计的可信平台模块 IP 片上只集成了必要的存储器，通过预留外部接口的方式，扩展存储空间；系统设计时可根据具体应用选择存储器，增加系统设计的灵活度，同时延长了芯片的产品寿命。

论文采用 8051 的指令集，进行可信平台模块 IP 的处理器设计。处理器通过通用 IO、SPI 接口控制单元，可实现与外部 FLAHSH 等存储器的通信。

论文重用了可重构密码引擎模块作为可信平台模块的密码模块单元。该单元包括对称密码算法 AES 模块、非对称密码算法 RSA 模块、伪随机数发生器模块。可重构芯片结合了微处理器的灵活性和专用 ASIC 的高效性，使密码模块可以根据需要改变硬件结构，以适应不同的安全性需求。在完成可信平台模块 IP 的后端设计后，进行了 MPW 流片，并开发了其在金融系统的 U-key 应用方案。芯片的测试结果与应用方案的演示结果表明，该可信平台模块 IP 具有通用性，可以广泛应用于各类信息安全系统。

关键词：可重用 IP；可信平台模块；8051 处理器

Abstract

Because of a wide range of computer and communication network applications, information security shows more and more significance not only in political or military businesses but also in financial and commercial settings. And there are kinds of technology raised to make important information security; among them, trusted computing has become the hotspot. Trusted computing, different from traditional security technology, could keep information security through trusted platform module.

With the rapid development of the semiconductor technology, the scale of integrated circuit (IC) makes wing-footed growth according to the Moore's low, IC design has enter into the age of system on a chip(SoC); while fiercer and fiercer competition of the IC market, shortened age of design technology of the production ask for design cycle shorter. At the moment, IP reusing is the main method to solve the problem. Paper designs trusted platform module based on IP reusing; meanwhile, the module designed meets IP reusing stardard, can be used for complex SoC design.

Trusted platform module is consisted of processor, crption engine, memory, IO and so on. Because of using special craft to reduce design cycle, the design technology of memory develops rapidly, the cycle of replacement is very short. So, the module designed in the paper has contained the most necessary momery, but it can extand momery space by reserving IO ports; user can choose appropriate memory according the Application requirements. In this way, the flexibility of system can be uodated and the age of chip can be lengthened.

8051 processor instruction set is adopted to design the processor of trusted platform module in the paper. The processor can control external memory through general IO or SPI interface.

Cryption engine based on reconfigurable computing is reused in the paper as encryption/decryption unit including AES module, RSA module and PRNG module. Reconfigurable computing possesses the flexibility of microprocessor and high efficiency of ASIC, which make it possible for encryption engine to change the

architecture according to different security needs in all kind of levels. After MPW tape, paper design U-key application in financial system using the chip. Testing result and demonstration effect shows that the trusted platform module designed in the paper with high universal. It can be used in all kinds of information security system widely.

Key words: Reusable IP Core; Trusted Platform Module; 8051 microprocessor

目录

CONTENTS

第一章 绪论

1.1 研究背景与意义

随着计算机与通信技术的高速发展，信息在军事、政治、金融业等领域运用越来越广泛，标志着当今社会已进入信息时代，信息已经成为社会的重要资源，而互联网是信息资源交流的重要渠道，同时，由于互联网的公开性，信息安全变得尤为重要[1]，保护信息安全是信息时代的迫切需要。传统的 X86 计算平台体系由 IBM 在上世纪 80 年代建立，但当时网络还未兴起，未考虑网路安全性，所以由该体系所带来的安全威胁一直存在，面对黑客、病毒的攻击，传统计算机变得难以抵抗。为了应对这一情况，由 IBM、Intel、AMD、HP 和 Microsoft 等公司组成的 TCG(Trusted Computing Group)提出了一个全新可信架构，以保证计算平台的可信性。其中，可信平台模块(TPM：Trusted Platform Module)是可信计算中的关键部分，用来进行整个平台的完整性和可测性检测，保证平台的安全，同时，可信平台模块内部还有受到保护的存储区域，用来存储用户密钥和安全证书。为了达到可信计算要求，可信平台模块芯片不仅要包含处理器，而且要集成密码算法引擎和接口，目前常用的密码算法有非对称加密算法 RSA、对称加密算法 AES 等[2]。

随着半导体工艺技术的发展，芯片设计进入片上系统（SoC：System on a Chip)时代，将整个系统功能集成到一个芯片中。根据摩尔定律，集成电路的集成规模以每年 58%的速度增加，而集成电路设计仅以每年 21%速度增加。集成电路设计水平与半导体工艺水平之间，形成了一定的剪刀差[3]。借鉴和使用已经成熟或完成的设计，可以有效的提高 SoC 芯片设计效率，缩短产品面市时间，降低开发成本，因此以可重用 IP 为基础的 IP 重用技术已经成为 SoC 芯片设计的主要技术方法。IP 模块是经过预先设计、预先验证，具有相对独立的功能，接口符合标准，符合一定都重用准则，具有商业流通能力的电路模块[4]。IP 核标准化是设计可重用 IP 的重要指标。SoC 设计中，集中了不同来源的各种 IP 模块，这些模块若用不同的编码风格和不同的接口结构，会降低 IP 模块的重用性[5]。