湖南科技大学学术著作出版基金资助项目

数字芯核电路版权保护技术与应用

梁 伟◎著

东南大学出版社
SOUTHEAST UNIVERSITY PRESS

数字芯核电路版权保护技术与应用

梁 伟 著

东南大学出版社
SOUTHEAST UNIVERSITY PRESS
·南京·

图书在版编目(CIP)数据

数字芯核电路版权保护技术与应用/ 梁伟著. —南京:东南大学出版社,2015.4

ISBN 978-7-5641-5585-8

Ⅰ.①数… Ⅱ.①梁… Ⅲ.①计算机网络—安全技术—版权—保护—研究 Ⅳ.①D913.04

中国版本图书馆 CIP 数据核字(2015)第 053209 号

数字芯核电路版权保护技术与应用

出版发行	东南大学出版社
出 版 人	江建中
社　　址	南京市四牌楼 2 号
邮　　编	210096
经　　销	全国各地新华书店
印　　刷	江苏凤凰数码印务有限公司
开　　本	880 mm×1230 mm　1/32
印　　张	7
字　　数	205 千字
书　　号	ISBN 978-7-5641-5585-8
版　　次	2015 年 4 月第 1 版
印　　次	2015 年 4 月第 1 次印刷
印　　数	1～1 501 册
定　　价	32.00 元

(本社图书若有印装质量问题,请直接与营销部联系,电话:025—83791830)

前　言

随着 IC(Integrated Circuit)半导体集成电路技术的快速发展，数字电子产品的应用已经渗透到人们日常生活中的方方面面，人们对于其安全性的关注度也与日俱增[1-2]。伪造、克隆、逆向工程以及在产品中加入恶意元器件等行为已经成为信息时代所面临的最严峻的挑战之一，电路复用、抄板等电子处理技术与软件在给 IC 设计企业带来极大便利并降低生产周期的同时，也给非法企业窃取 IC 机密版权信息提供了可能。如果 IC 版权信息保护不当，那么半导体 IC 制造行业通常会在电子产品的知识产权 IP(Intellectual Property)保护上遭受到巨大的损失。如何对集成电子产品进行有效的知识产权的保护一直是计算机科学研究中的基本问题。

数字水印是一种用来鉴定文件版权信息的传统技术。其名称来源于纸质上的半透明标记的原始技术。近年来，为了保护其他格式文件的版权，类似技术的应用引起了人们极大的兴趣，特别是数字水印技术在数字 IP(Intellectual Property)电路产品所有权保护上的应用[3-4]。顾名思义，数字芯核水印技术就是将数字信息嵌入到 IP 中并使之难以检测和移除。隐藏的信息能够唯一标识作者或者 IP 所有者，并且难以被人察觉。数字水印在必要时能作为证据提交法庭，以证明 IP 的所有权。通常，数字水印的存在能够防止 IP 的非法使用，从而避免了法律诉讼问题。

数字芯核水印技术通常也称为 IP 水印技术，它是一门应用芯核电路载体的冗余信息来隐藏秘密信息的新技术。它的概念起源于 Foundry 提供的安全标准单元库，现指在可重复使用的集成电路模块中隐藏特定的数字标记信息的方法。在数字芯核水印系统设计中，对数字芯核水印的兴趣源于能够使可复用 IP 技术得到健康的发

展，合法 IP 模块的复用设计可以保证 IP 设计更高的研发效率和减少上市周期[5-6]。本书重点关注数字 IP 设计中的 IP 知识产权保护问题。IP 核可以通过多种形式进行描述。从硬件描述语言中的行为描述到实际布局，防止 IP 被不正当使用问题与 IP 提供者和开发集成软件的计算机辅助设计公司都密切相关。芯核水印技术是最直接的解决方法，它能从电子产品中有效地提取出电路的原始版权信息。数字芯核水印技术在电子信息技术领域有着非常广泛的应用前景。因此，研究芯核电路知识产权保护的关键技术不仅在实际应用中具有深远的意义，而且该技术也为电路安全技术的发展带来了新的挑战，如电路空间消耗过大、水印安全性较低、水印嵌入速度较慢等新问题。因此，如何来提高国家信息安全环境下的电路产品的版权保护与安全认证问题是我国信息安全技术快速发展的重要保障之一。

本书主要内容为芯核电路知识产权保护的关键技术，主要包括基于混沌映射的芯核水印、基于 FSM 时间约束的芯核水印、现场可测试的芯核水印、分散隐藏策略的高容量芯核水印、零知识芯核水印盲检测以及隐秘信息自恢复双重芯核水印等方案内容。全书内容共四篇，总计九章。第一篇内容共两章，主要介绍了本书相关研究的意义、当前相关研究的背景知识以及芯核电路保护的基础知识等。第二篇内容共四章，主要介绍了芯核水印的相关技术方法，提出了一种基于混沌映射的芯核水印结构，提出了一种基于 FSM 冗余属性特征的时间约束芯核水印方法，提出了一种适用于可测试环境下的多扫描链芯核水印算法，提出了一个支持高容量嵌入的 FPGA 芯核水印方法等。第三篇内容共两章，主要介绍了基于零知识证明协议的芯核水印盲检测方法，以及一种基于隐秘信息自恢复机制的双重芯核水印认证算法。第四篇内容共一章，主要介绍了一种自主开发的集成电路知识产权保护原型系统，本章重点介绍了原型系统中各种方法的水印嵌入、提取、检测以及认证等工作。

本书的主要内容是作者多年从事芯核水印技术研究的一点成果，本书的建议读者对象为从事芯核电路设计及其应用等相关领域

的研究人员。

本书由湖南科技大学梁伟博士执笔，徐建波教授统稿，李雄博士校稿。感谢湖南大学张大方教授和哈尔滨工业大学深圳研究生院崔爱娇博士对本书的相关内容提出了许多宝贵的意见，另外还感谢为本书校稿的博士生彭理、龙静，硕士生盛勇、钱鑫等同学。

本书的出版得到湖南科技大学学术著作出版基金资助，同时还要感谢国家自然科学基金项目(61202462)、湖南省教育厅科学研究重点项目(14A047)、湖南省自然科学基金项目(13JJ3091)、湖南省自然科学基金湘潭联合基金(11JJ9014)项目等的资助！

本书针对芯核电路知识产权保护的关键技术进行了浅显的研究，由于学识浅陋，见闻不广，必有许多不足之处，望同行指正。

梁　伟

2015 年 4 月

目　录

第一篇　芯核水印技术基础

数字水印技术在多媒体数据版权保护中的应用已经发展到了成熟阶段，而在嵌入式系统与集成电路设计等方面的应用仍然起步不久[7]。一些大学与研究机构的学者开始探索将数字水印技术引入到FPGA集成电路设计中，以解决其版权的保护问题。由于集成电路这种特殊载体对功能要求十分严格，因而多媒体数字水印方案直接应用到集成电路完全行不通。考虑到集成电路的自身特点及其所依赖的相关技术，可以从集成电路的特征为出发点，设计集成电路芯核的水印算法。本篇的内容共两章，各章节内容概括如下：

第1章为绪论，主要介绍了本书相关研究的意义，然后简要介绍了当前相关研究的背景，最后给出了全书的结构及主要工作。

第2章介绍了IP水印技术的定义以及发展历程、IP版权保护技术的分类、FPGA的结构组成、IP设计流程、FPGA开发工具以及IP水印技术目前的国内外研究现状等，全面归纳了芯核水印在FPGA设计领域的缺陷和面临的安全挑战，最后对本文的相关基础进行分析并做出总结。

1 绪论

本章首先介绍了本书相关研究的意义，然后简要介绍了当前相关研究的背景知识，最后给出了全书的结构及主要工作。

1.1 研究意义

超大规模集成电路(Very Large Scale Integration，VLSI)单个芯片上晶体管的数量增长能力到2015年可达到百亿数量级[8]。然而，每过12个月芯片制造能力的提高约为58%，设计能力却只能提高21%，在这种情况下，芯片制造能力与设计能力的差距将变得越来越大，原有的垂直型芯片设计模式已无法满足当今芯片设计的需求[9]。因此，为了能在VLSI设计过程中解决芯核(IP)产品的诸多问题，譬如完善设计结构、降低产品成本、缩短设计周期和降低市场风等，建立一种新型高效安全的芯核可复用技术(Reused IP)已势在必行。

集成电路(Integrated Circuit，IC)产业作为国民经济中具有先导型、战略性的基础工业，其技术水平和产业规模已成为一个国家经济发展、科技进步和工业实力的重要标志，它的发展将给信息产业、装备制造业以及信息化的发展带来重大变化。近年来，在国家产业政策引导和市场需求带动下，我国集成电路产业快速发展，产业规模迅速扩大，技术水平显著提升。2011年国内集成电路产业销售额达到1 572.21亿元，销售额同比增长9.2%。其中，IC设计业销售额473.74亿元，芯片制造业销售额486.91亿元，封装测试销售额611.56亿元。国内企业(和个人)累计的授权发明总数达到18 297件。国内企业(和个人)集成电路布图设计登记达到4 262件，占总量的87.09%[10]。

随着集成电路技术的迅猛发展，人们可以方便地利用芯核可复

用技术设计和制造各种电子产品[11]。与此同时，而在数字电路时代，大规模集成电路抄板的工艺已经到达了一个很高的水平，集成电路技术发展使得电路版权信息的复用和传输变得更加简单和方便。一些非法厂商和个人为了达到缩短产品开发周期的目的，通过可复用 IP 技术对一些芯核在非授权的情况下进行盗用，这样导致每年的芯核知识产权纠纷问题急速上升。从图 1.1 中可以看出：单一芯片上晶体管的数量平均每年将增长 58%(Complexity Growth Rate)，而系统设计人员每人每月能够设计的晶体管数量平均每年增长 21%(Productivity Growth Rate)。不难看出，随着时间的推移，芯片制造能力与设计能力之间的差距将进一步拉大，从而造成设计危机[12]。

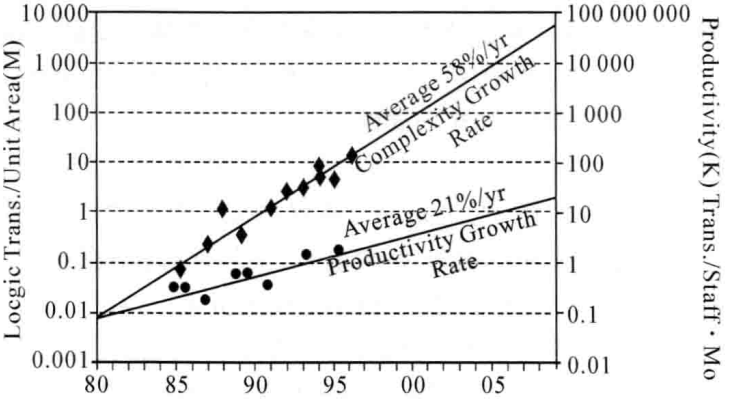

图 1.1　芯核产品年增长率比较图

我们通过复用方法将这些预先设计好并验证成功的电路模块引入待开发的系统，这样可以成为 IP 产品开发中降低成本和减少产品上市时间最有效的方法之一。这些已经成功验证、可以重复利用且具有某种确定功能的集成电路模块就是 IP 核，本文称之为芯核。芯核可以用于专用集成电路(ASIC)或者可编程逻辑器件(FPGA)。在集成电路设计中，可以将一些比较复杂且常用的功能块，如常用密码算法、FIR 滤波器及 USB 控制器等设计成可以修改参数的模块。其他用户可以直接调用这些模块完成复杂系统设计。重复使用这些芯

核可以避免重复劳动，大大降低了设计者的负担与风险，加快了系统设计的进度[13]。

据统计，每年的芯核复用技术中由于版权侵害而造成的业界损失高达500亿美元[14]。典型的案例包括：2005年初，日立环球存储科技公司宣布对中国南方汇通微硬盘科技股份有限公司及其联营研究机构Riospring Inc提出诉讼，控告该公司侵犯日立GST硬盘机的多项芯核知识产品专利权[15]；2009年11月5日，南京源之峰公司侵犯上海华润矽威科技有限公司集成电路布图设计专有权纠纷一案，被告被要求停止侵害原告PT4115芯片布图设计专有权，销毁侵权产品，并赔偿原告的经济损失[16]。这些知识产权纠纷案例的出现，不仅给企业带来了巨大的经济损失，更对企业品牌的国际声誉和相关客户的合作关系造成严重破坏。面对如此众多的版权纷争，芯核可复用保护技术这一重要技术研究课题在全世界各地受到了普遍的关注。其中，如何防止数字芯核产品被侵权、盗版和随意篡改，已经成为世界各国亟待解决的热门课题。

因此，目前该技术已经受到国际学术界和企业界的高度关注[17]。芯核水印技术同时也是一门新兴的交叉应用学科，它涉及了不同学科领域的思想和理论，如微电子、信号处理、图像处理、信息论、编码理论、密码学、检测理论、概率论和随机理论、数字通信、对策论、计算机科学及网络技术、算法设计等技术，还包括许多公共策略和法律相关的问题，不但具有重要的学术意义，还有极为重要的经济应用价值。

1.2 研究背景

集成电路产业作为我国战略性新型产业之一，是国民经济和社会信息化的重要基础。近年来，在国家一系列政策措施的扶持下，我国集成电路产业得到了快速发展。《国务院关于印发进一步鼓励软件产业和集成电路产业发展若干政策的通知》（国发[2011]4号）进一步加大了对集成电路产业的扶持力度，扩大了扶持范围，优惠政策

覆盖了产业链各个环节，产业发展环境将进一步得到优化。目前，以集成电路为核心的电子信息产业已经超过了以石油、钢铁、汽车为代表的传统工业，成为带动传统产业迈向信息化时代的强大引擎和雄厚基石。过去五年我国集成电路市场规模年均增速14%，2011年已经超过8 000亿元。预计到2015年，国内集成电路市场规模将超过1万亿元。发达国家国民经济总产值增长部分约70%与集成电路有关[10]。

集成电路产业的发展中，低功耗和高集成度依然是技术竞争的焦点。芯片集成度仍将不断提高，并且将沿摩尔定律继续前进。片上系统(System on Chip，SoC)设计技术发展成为集成电路设计主导方向。在高度复杂的SoC系统中，设计能力和工艺水平之间的矛盾是制约SoC发展的突出障碍。如果一切从头开始设计，不但增加了设计的难度和复杂度，而且无法保证设计产品的上市时间。为了解决这个问题，业内提出一种复用技术，也就是将经过预先设计、实现并验证成功的集成电路模块重用于SoC设计。复用技术的提出，不仅降低了设计层次及复杂性，而且大大缩短了产品的设计周期。目前，这项技术已成为当今超大规模集成电路的主流技术[11-16]。复用技术的发展创造了一个繁荣高效的市场，但是，这种快速设计技术的使用也带来了极大的版权盗用风险。集成电路模块的设计需要半导体企业或机构花费大量的财力和物力。若侵权者可以轻而易举地对集成电路进行盗用并仿制，将严重损害开发者的利益并且极大挫伤半导体公司或机构的开发积极性。据集成电路行业巨头英特尔公司统计，通过盗用集成电路可以节省90%以上的开发成本和一年半左右的开发时间[17-18]。近年来，集成电路的版权盗用在亚洲尤其是在我国呈现泛滥的趋势，严重制约了集成电路产业的发展，阻碍了我国国民经济发展和社会进步。据统计，每年因为版权侵害而造成的业界损失高达5亿美元[19]。针对集成电路发展中版权盗用问题，工业和信息化部门制定的《集成电路产业“十二五”发展规划》中也反复强调实施知识产权战略，加大知识产权的保护力度，以促进市场公平有序的健康发展。本文将研究集成电路知识产权的保护方法。