装备科技译著出版基金

Integrated Circuit Authentication Hardware Trojans and Counterfeit Detection

集成电路认证

硬件木马与伪芯片检测

[美] Mohammad Tehranipoor Hassan Salmani Xuehui Zhang

李雄伟 陈开颜 张阳 等译

国防工业出版社
National Defense Industry Press

Springer

装备科技译著出版基金

集成电路认证
——硬件木马与伪芯片检测

Integrated Circuit Authentication

Hardware Trojans and Counterfeit Detection

[美] Mohammad Tehranipoor
Hassan Salmani
Xuehui Zhang
著

李雄伟　陈开颜　张　阳
谢方方　李　艳　韩月霞
译

国防工业出版社

·北京·

著作权合同登记　图字:军-2016-054号

图书在版编目（CIP）数据

集成电路认证:硬件木马与伪芯片检测/(美)穆罕默德·特朗普(Mohammad Tehranipoor),(美)哈桑·塞马尼(Hassan Salmani),(美)张雪辉(Xuehui Zhang)著;李雄伟等译.—北京:国防工业出版社,2016.11

书名原文:Integrated Circuit Authentication Hardware Trojans and Counterfeit Detection

ISBN 978-7-118-11116-3

Ⅰ.①集… Ⅱ.①穆… ②哈… ③张… ④李… Ⅲ.①集成电路—认证 Ⅳ.①TN407

中国版本图书馆 CIP 数据核字(2016)第 255381 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路23号　邮政编码100048)

腾飞印务有限公司印刷

新华书店经售

*

开本 710×1000　1/16　印张 12¾　字数 257 千字

2016 年 11 月第 1 版第 1 次印刷　印数 1—2000 册　定价 68.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)88540777　发行邮购:(010)88540776

发行传真:(010)88540755　发行业务:(010)88540717

译者序

随着信息时代的发展，信息安全受到高度关注，信息加密、入侵检测、防火墙等大量信息安全技术用于提高系统的安全性。然而，近年来出现了硬件木马和伪芯片问题，可能使得这些安全措施成为信息时代的“马其诺防线”。

硬件木马是对原始设计的恶意篡改，能够造成芯片失效、自毁、泄密，甚至破坏己方系统，能够轻易绕过现有的安全防护体系。伪芯片则是用赝品芯片充当正品芯片，其形式包括以假充真、以旧充新、以次充好等。如果系统使用了含有硬件木马的芯片或伪芯片，那么这些芯片必将成为整个系统的“阿喀琉斯之踵”。在此情况下，不管对系统使用何等强度的安全防护，系统都难逃毁灭的命运。目前，我国大力发展集成电路等基础产业，集成电路安全作为其中一个重要方面应给予足够重视。硬件木马和伪芯片问题是当前研究中的热点问题，加强该方面研究对于提高我国信息基础设施的安全性具有重大意义。

本书是系统性分析硬件木马和伪芯片的著作，对硬件木马和伪芯片分类、硬件木马检测、可信硬件设计、脆弱性评估等方面均进行了讨论分析，提出了环形振荡器网络、基于轻量级片上传感器的 IC 指纹设计等硬件木马防护手段，是目前该领域较为全面的著作，也是相关技术的代表性著作，对本领域发展具有很好的引领作用。因此，在承担自然科学基金项目的过程中，我们组织项目组主要成员翻译了本书，冀以推动我国硬件木马和伪芯片相关研究的发展，从而促进芯片安全的整体发展。

参加本书翻译的有李雄伟、陈开颜、张阳、谢方方、韩月霞、李艳、王晓晗等，李雄伟对全书进行了统稿和校对。

本书的翻译工作受到国家自然科学基金（编号：61271152、51377170、61602505）、河北省自然科学基金（编号：F2012506008）和装备科技译著出版基金的资助，深表感谢。

需要说明的是，本书涉及内容多，专业性强，且由多人翻译，限于水平和经验，加之有些概念译法上本身就有难度，故而谬误在所难免，敬请读者见谅，并提出宝贵意见。

译 者

2016 年 6 月

原书前言

随着集成电路(IC)设计与制造的大量外包,其安全与可靠性问题备受关注。一方面,硬件木马对IC设计特性进行恶意修改,从而造成系统失效或秘密信息泄露;另一方面,伪芯片问题也日益严重,引起了政府和工业领域的严重担忧。所谓伪芯片是指不符合原始设计规范要求的非授权产品。伪芯片问题不但降低了系统的可靠性,减少了设计公司的研发收益,挫伤了创新的积极性(因知识产权模块IP常被窃取),而且产生大量质量低劣的产品冒充正品。

为了解决这些问题,本书给出了面向实际应用的综合IC认证方案。书中对IC供应链进行了深入分析,并研究了其对于硬件木马和伪芯片的脆弱性。

本书共分为11章。第1章介绍了VLSI系统集成,详细讨论了最具挑战性的两个安全问题:硬件木马与伪芯片。第2章进行案例研究,利用形式化证明和代码覆盖分析对植入第三方IP核的硬件木马进行检测。第3章采用旁路信号分析技术检测非可信IC制造过程中植入的硬件木马。第4、5章描述了两种提高硬件木马检测率的可信硬件设计技术。这些技术能够更有效地激活木马,增强由木马引起的旁路信号,使得测试工程师更容易检测到木马。第6章提出了另外一种可信硬件设计技术——基于环形振荡器网络的片上结构,能够监控由木马引起的电压波动,从工艺扰动引起的噪声信号中区分出硬件木马引起的噪声信号。第7章给出了综合性脆弱分析,对激活木马的难度和各部分电路的可观测性进行量化分析。另外该章将硬件木马可检测性定义为其对电路特性的影响力度量。第8章介绍了内建自认证技术(BISA),能够在非可信生产过程中的GDSII开发和掩模生成阶段防止硬件木马的植入。第9章给出了伪芯片、缺陷品、异常品的详细分类,以及与之相关的伪造类型和可行的检测技术;讨论了检测和预防伪芯片所面临的主要挑战。第10章阐述了轻量级传感器设计,它能够防止伪造者从过时电子系统中回收部件。由于传感器能够提供芯片的使用信息,因此,测试工程师通过传感器可以很容易检测出回收部件。最后,第11章讨论了指纹识别技术,主要描述了基于电路时序分析的伪芯片检测。

美国康涅狄格州斯托尔斯
Mohammad Tehranipoor
Hassan Salmani
Xuehui Zhang

目　录

第1章 引 言

人类社会高度依赖于计算机系统，它为人们的生活提供了高性能、高精度和高安全性的服务。从核电控制到飞机发动机，再到洗碗机、微波炉等家用电器都受益于计算机系统。计算机系统的可靠性决定了其可用范围。一方面，系统可信性是系统所提供服务与其功能规格的一致程度，规格从功能和性能两方面对系统进行描述。另一方面，系统所提供的服务是用户所感知的系统行为。从广义角度来看，可信性包含可用性、可靠性、安全性、完整性和可维护性等属性，如表1.1所示[2]。

表1.1 可信性属性

属性	定 义
可用性	系统必须就绪地提供正确的服务
可靠性	系统必须持续地提供正确的服务
安全性	系统必须避免人为的或环境的灾难性后果
完整性	系统必须避免不恰当的状态修改
可维护性	系统必须具备可修改和可维护的能力
机密性	系统必须避免非授权的信息泄露

安全性更为具体，侧重于可用性、完整性和机密性。系统安全性需求包括对于授权行为的可用性、未授权操作的完整性，以及机密性。信任是指一个系统（系统A）对另外一个系统（系统B）的依赖程度，因此系统A的可信性受到系统B可信性的影响。系统的信任度是指确保系统能够按照预期运行[2]。

现代社会极其依赖集成电路（IC）或者芯片，它们是所有电子产品的大脑。如今，出于经济因素考虑，大多数公司通常将IC外包到海外生产制造，从而致使IC越来越容易受到恶意行为的攻击，比如修改设计以破坏功能或者伪造集成电路。

1.1 硬件安全与信任

如图1.1所示，一个计算机系统的开发包括几个步骤，这些步骤没有必要在同一个设计室内完成。第一步是根据用户需求确定系统规格。一个复杂系统可能需要多种多样的组件，比如存储器以及具备不同应用及功能的芯片。

在提供系统规格、确定系统结构及其所需的组件之后，设计开发需要使用不同的工具。每一个组件都需要受到特定关注以确保其能够满足所有系统要求。

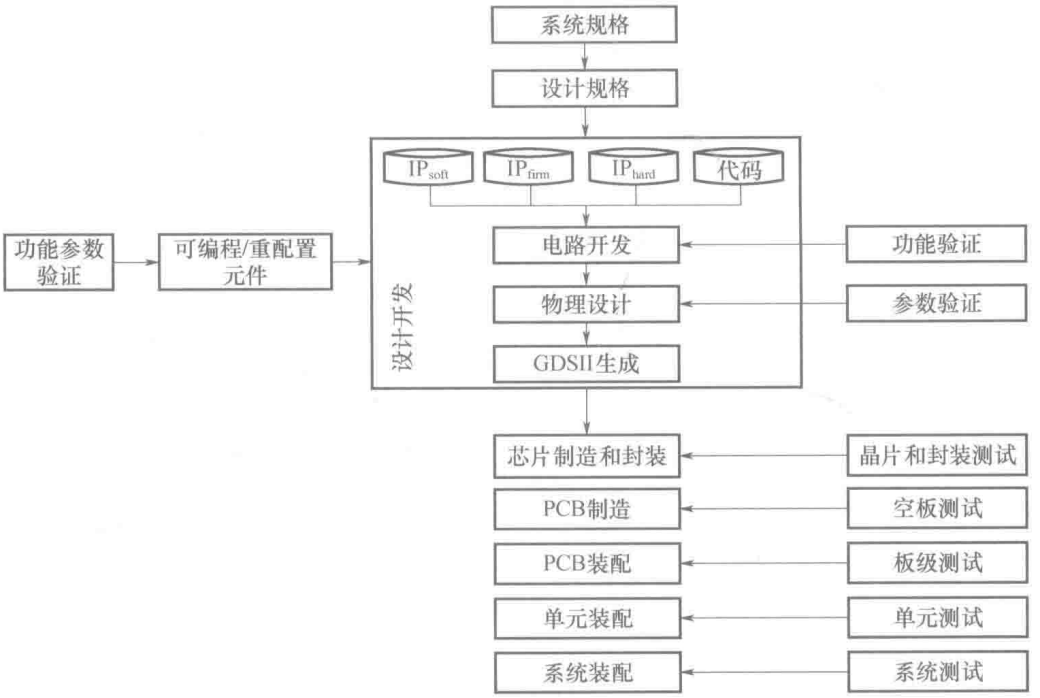

图 1.1　系统集成和测试方法

为了加快系统开发并降低最终成本,外包已逐渐取代内部加工。第三方知识产权(IP)核已经取代内部可综合逻辑单元库。商业软件已经代替自研的计算机辅助设计(CAD)工具。接下来,设计好的芯片进入生产环节。现在大多数公司没有生产线,而是将掩模生产及制造外包出去。除了定制设计外,企业还能够通过使用现货产品(COTS)、可编程模块,例如微控制器、可重配置组件,或者现场可编程门阵列(FPGA)来减少总成本并加快系统开发。之后,制造印制电路板(PCB)并在上面装配系统组件。最后,将 PCB 放到一起形成一个个单元,这些单元集成在一起就是整个系统。

每一步骤都会执行不同的验证或者测试来确保其正确性,如图 1.1 所示。功能验证和参数验证确保设计在服务及相关要求方面(如功耗和性能)正确实现。在定制设计投入制造之后,通过晶片和封装测试将有缺陷的部件分离出来,并保证交付的芯片品质。PCB 制造是一个光刻过程,容易产生缺陷,因此在 PCB 上安装器件之前应当对其进行测试。在 PCB 装配之后,需要再次测试 PCB 以验证组件是否被正确安装,以及在 PCB 装配过程中没有被损坏。用测试过的 PCB 组成单元及最终系统,但在发货前还要对系统进行现场操作测试[12]。

系统开发的每一步都很容易受到安全漏洞的影响。敌手可能改变系统规格致使系统容易受到恶意活动的攻击或者容易受到功能故障的影响。由于外部资源,如第三方 IP 和 COTS 广泛应用于设计过程和系统集成中,敌手可能在其中隐

藏额外的电路，从而在特定时间破坏系统或获得控制权。非可信代工厂问题的根源在于设计制造的外包。建立一个芯片制造厂代价高昂，并且近年来大多数半导体公司已经没有生产线，而是让代工厂按照其设计制造产品，从而降低总成本。然而第三方可能通过增加额外电路来改变设计，如从芯片中获取机密信息的后门，或者改变电路参数，如改变线宽引发使用中的可靠性问题。因为可在正品组件的接口间增加额外组件，因此 PCB 组装更加可疑。总之，系统合作开发的过程为恶意团体控制系统并进行恶意活动创造了机会。因此，应当将安全特性的设置作为系统开发过程的一部分，从而提高可信性和可验证性，并揭示任何对正品规格的偏离。

1.2 硬件木马

敌手能够通过增加额外的电路（硬件木马）破坏原始设计[1]，因此为了经济利益而将设计和制造外包的行为已经引起了人们对国家安全问题的关注。一般来说，硬件木马被定义为对设计的任何有意修改从而改变设计的原有特性。它具有隐蔽性，并且能够在特定条件下改变设计功能。硬件木马可以作为一个定时炸弹，在特定时间使系统失效，或者通过旁路信号来泄露秘密信息。

一个木马可能影响电路的交流电参量，比如延迟和功耗；它同样能够在特定条件下引起故障。如图 1.2 所示，硬件木马由木马负载和木马触发组成[16]。一个功能木马将主电路的内部线路作为输入连到木马负载，并通过木马负载重新连接主电路中的其他一些线路，从而修改设计功能。木马触发决定激活条件，在该条件下木马负载能够向主电路传递错误值。

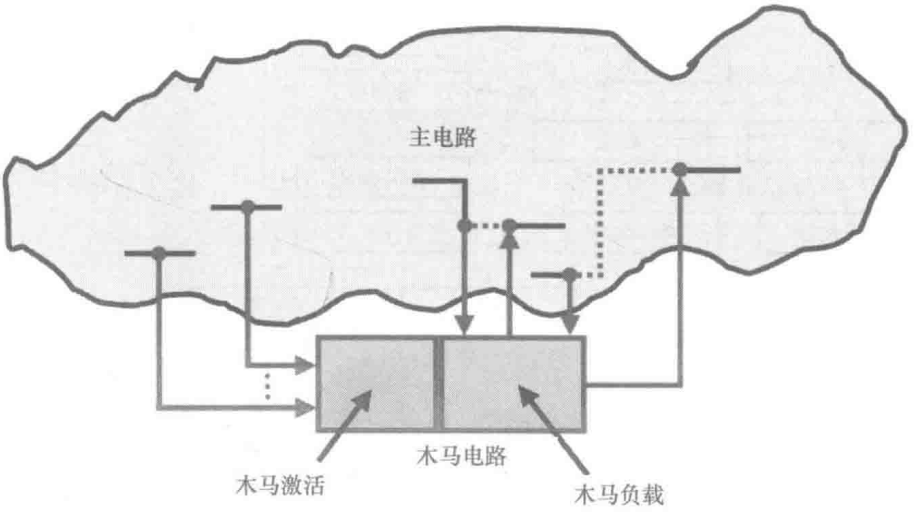

图 1.2 功能性木马实现

Wang,Tehranipoor 和 Plusquellic 首次提出了详尽的硬件木马分类方法[7,8]。该分类方法可以让研究人员针对不同类型的木马来验证其检测方法。目前,行业内缺少评估木马检测方法有效性的度量标准。这样的度量标准有助于形成综合的木马分类方法,从而有助于分析木马检测方法。考虑到芯片结构和功能可能存在多种形式的恶意修改,Wang 等根据木马的物理特征、激活特征和行为特征将木马分为三类,如图 1.3 所示。尽管木马可能是多种分类特征的混合(例如,木马可能包含多种激活特征),该分类方法仍能够体现木马的基本特征,并且有助于定义和评估各种检测策略。

物理特征分类描述了木马的多种外部特征。该分类将木马分为功能和参数两类。功能类包括在物理上增加或减少晶体管或门电路而实现的木马,而参数类是指通过修改既有线路和逻辑来实现的木马。规模特征是计算芯片中被增加、减少或者破坏的器件数目。分布特征描述芯片物理布局中的木马位置。结构特征指一个敌手被迫重新生成布局来植入木马的情况,这将引起芯片物理构成成分的变化。这些改变可能导致部分或者全部设计组件的位置不同。在物理布局上的任何恶意改变都可能改变芯片的延迟和功耗特征,这将有利于木马检测。Wang 等从最小化检测概率的角度分析了当前敌手的能力。

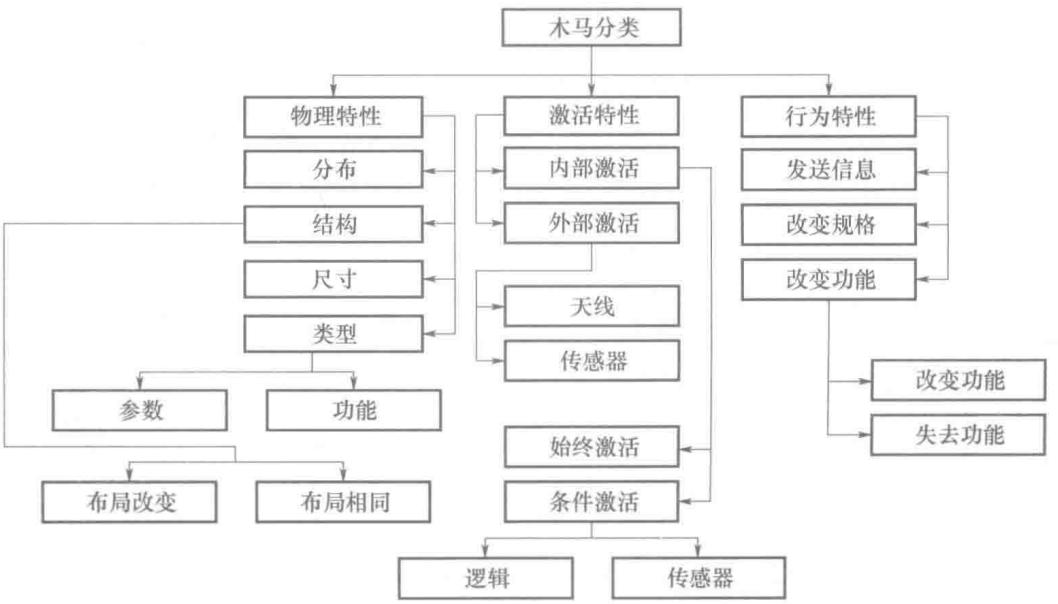

图 1.3　硬件木马分类

激活特征是指能使木马激活并实施破坏功能的条件。木马激活特征被分为两类:外部激活(例如,被与外部世界相互影响的天线或传感器激活)和内部激活(通常被进一步分为常开型和条件型),如图 1.3 所示。“常开型”是指木马始终处于活跃状态,它能够在任何时候中断芯片功能。该分类包含的木马能通过修改芯

片的几何结构来实现，使得某个节点或者路径对故障有很高的敏感性。敌手可在一些很少使用的节点或路径上植入木马。“条件型”是指在特定条件下才激活的木马。激活条件可以基于传感器的输出，这些传感器可以监控温度、电压或任意类型外部环境条件（如电磁干扰、湿度、高度或温度）。另外，激活条件也可以基于内部逻辑状态，比如某个特定的输入模式，或者某个内部计数器的值。这几种木马可以通过在芯片中增加逻辑门和/或触发器来实现，并由此形成组合或时序电路。

行为特征描述了木马所造成的破坏行为类型。如图 1.3 所示的分类方案中，将木马行为分为三类：修改功能、修改规格以及发送信息。修改功能类指的是通过增加、移除或绕过现有逻辑来改变芯片功能的木马。修改规格类指的是改变芯片参数性能的木马，比如由敌手修改现有线路和晶体管几何结构而引起的延迟。发送信息类是指给敌方发送关键信息的木马。

木马电路设计非常诡秘，仅在罕见条件下触发，在其生命周期的大部分时间处于静默状态，相对于宿主设计规模非常小，而且对电路参数仅有微小影响。对 IC 开发过程的薄弱性进行分析需要了解设计、制造和测试等环节。为了保证客户 IC 的可信性，整个设计和制造过程必须可信，或者制造的 IC 应该通过客户的可信认证。拥有独立、安全的 IC 供应链是最佳选择，但是在经济上却不可行。现在，只有 Intel 和其他少数公司仍然在其自有制造工厂设计和制造芯片。其他芯片设计商已经没有了芯片制造生产线，而将芯片制造外包给海外公司，由此他们能够省去建立现代芯片制造厂的巨额开支。2007 年，该项开支高达 20 ~ 40 亿美元[1]。例如，据美国国防部报道，在美国安全设施中采购的超过 35 亿美元的集成系统中，仅有 2% 为美国公司制造[10]。这些现状导致需要有效的方法和技术对木马进行预防和检测。

1.3 木马检测方法

过去几年已经提出了一些木马检测方法。一般而言，检测方法可分为旁路信号分析或木马激活两类，主要是芯片级解决方案和体系结构级木马检测解决方案。

1. 基于旁路信号分析的木马检测

旁路信号（如时间和功耗）能够用于木马检测。木马通常改变设计的参数特征，例如，降低性能、改变功耗特征，或者降低芯片可靠性，这将改变原始电路中的线路及门电路的功耗和/或延迟特征。基于功耗的旁路信号使得 IC 内部活动和结构可见，从而有可能在非激活状态下检测出木马。基于延迟的旁路信号能够检测木马是否存在。有效的延迟测试方法对受影响路径上电路延迟的微小变化很敏感，并且能有效地从工艺扰动中区分木马。

1）基于功耗的硬件木马检测

在基于功耗的检测技术中，比较待认证 IC（IC under authentication，IUA）的功耗与无木马电路（金片①）的功耗。图 1.4 给出了特定的时间间隔内，无木马电路和有木马电路 V_{DD} 引脚上电流变化。每个电流测量包含若干元素，包括：①主电路电流消耗，该部分对于所有芯片都是一样的；②测量噪声，可以通过多次测量平均来消除；③工艺扰动，该部分随机且不能被抵消；④木马电流，如果存在木马则必然产生该部分电流。超过工艺扰动的任何可测量差异都可能是木马存在的迹象。

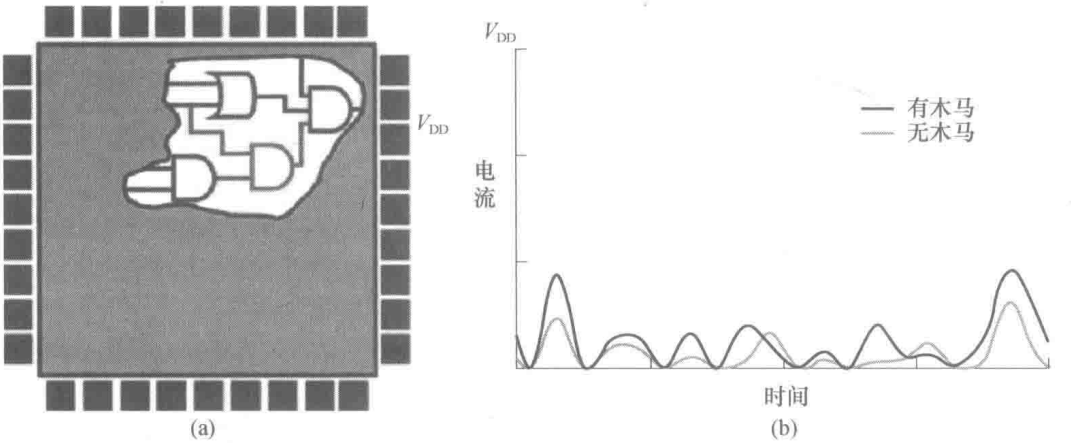

图 1.4　基于功耗分析的硬件木马检测

Agrawal 等首次使用功耗旁路信息来检测电路中木马[3]。为了获得无木马 IC（即正品芯片）的功耗签名，需应用随机模式并进行功耗测量。之后，从测量的 IC 中选出几个进行逆向设计分析，从而确保其不含木马。一旦获得参考签名，将同样的随机模式应用到待认证 IC 上。如果 IUA 的功耗签名不同于参考签名，这个 IUA 就是可疑的，可能含有木马。通过应用随机模式并比对签名，可以检测不同工艺扰动下不同规模的木马。如果木马规模占电路的比例较大，则其对电路瞬态电流的影响将较为显著，很容易测量。但是对于非常小的木马而言，工艺扰动能够掩盖其对电路功耗的影响。

Rad 等提出了基于区域的瞬时功耗信号分析方法来减少由工艺扰动和泄露电流增大所带来的影响[11]。区域是电路布局的一部分，它从周围的电源端口或者 C4 凸块②中获得电能。对每个电源端口分别应用模式进行测量。采用一组测试序列进行仿真，并基于瞬时电流检测算法对电源端口所产生的 I_{DDT} 波形区域进行统计分析，这里为每个电源端口的正交对构造散点图。作者对有木马设计和无木马设计使用若干个不同的工艺模型。对使用不同工艺模型的无木马设计进行分

① Golden Chip，金片，没有植入木马的安全芯片。译者注。

② C4，Controlled Collapsed Chip Connection 的缩写，可控塌陷芯片连接。译者注。

析,得到预测椭圆,以区分无木马和有木马设计。无木马设计的数据点散布是因未校准工艺和测试环境(PE)变化造成的。然而,单独采用区域分析不足以处理PE变化对检测分辨率的不利影响。有必要采用信号校准技术减弱和消除PE信号变化的影响,从而有效提高基于区域方法的检测分辨率。为每个芯片的各个电源端口分别执行校准,同时测量每个电源端口的脉冲响应。在应用每个测试模式之后,使用校准矩阵对响应进行校准。Rad等给出的结果显示校准能够增加不同工艺参数下无木马和有木马设计之间的差距。

Alkabani和Koushanfar提出了几种通过非破坏性测量构建门级延迟和功耗特征的方法[13]。每次测量形成一个方程,在进行线性次数的测量之后,形成了将测量特征映射到门级的方程组。Potkonjac等提出采用基于线性规划和奇异值分解的门级特征公式来检测木马[14],并对延迟和静态功耗进行测量,通过约束(方程)分析进行木马检测。该方法试图找到最大秩测量矩阵,并通过几种启发式方法来检测门电路特征与其原始特征存在的不一致。用学习、检验和置换的统计验证方法为正常(非恶意)特征进行边界评估。实验中考虑了非侵入式测量中的存在的误差,而非工艺扰动。由于门级特征刻画可以高度精确,因此其评估结果令人满意。门级特征分析方法能够为可控门找到特征,其可控性对静态功耗测量和I_{DDT}测试是很重要的。Alkabani和Koushanfar将门级评估的统计收敛和信号完整性用于木马检测[13],计算了有效健壮的门级功耗近似值并采用多重一致性校验检测出了恶意植入。

2)基于延迟的硬件木马检测

当然还有一些其他技术分析了木马对芯片设计性能的影响。任何附加的门或线路都将增加额外电容,因此在植入木马的路径上所发生的任何信号上升或者下降都会增加额外的翻转时间。图1.5表明在无木马的电路中Output_Tx信号比植入木马的电路改变要快。由于额外线路所致的电阻和电容效应以及木马门的传输延迟,高亮显示路径上经过额外线路和附加门的信号会导致额外的电路延迟。

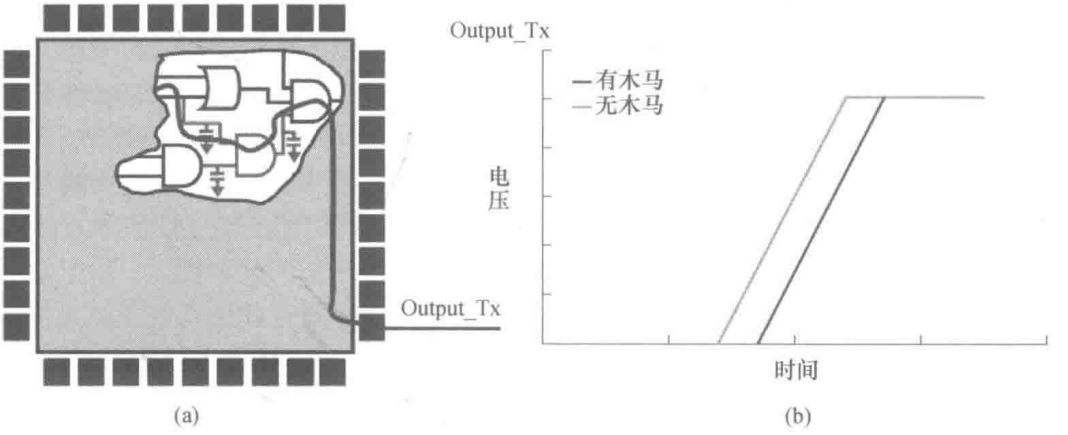

图1.5 基于延迟分析的硬件木马检测

文献[6]中提出的路径延迟指纹与文献[3]基本相似,只是前者是基于电路延迟分析。即使是在规模上相对于主电路非常小的木马,也至少会对一条路径产生影响。一个电路有很多路径,一条路径代表整个电路特征的一部分。该方法测量几个芯片上某些指定路径的延迟,并将工艺扰动考虑在内。然后,芯片通过反向设计来保证其为正品,并且将其测量值作为指纹。采用相同方法测量其他芯片,并与指纹相比较。任何不同都可能是含有木马的迹象。

文献[9]中提出另外一种基于延迟的方法。它提出基于影子寄存器的特殊延迟测量电路,从而测量候选路径中的延迟。该技术主要用于刻画 IC 特征,也能用来进行硬件木马检测。在两个寄存器之间(起始和目的寄存器)的一条指定路径的延迟由一个影子寄存器进行描述。影子寄存器有一个与寄存器时钟(clk1)相同频率的时钟(clk2),但是有负相移(例如,负偏移)。为了分析路径特征,使用不同时钟偏移的 clk2,直到获得不同的影子寄存器数据和目的寄存器数据。之后将 clk2 和应用于被测路径的模式同时存储。两次测量在设计和测试时完成。设计时测量是在不同工艺扰动的指定路径上为每个路径建立统计数据。测试时在每个路径上进行相同测量,并与存储的统计数据相比较。在设计时存储的 clk2 和在测试时获得的 clk2 之间的任何不同都表明存在木马。

2. 木马激活方法

木马激活策略能够加快木马检测进程,并且可在某些案例的分析过程中与功耗分析方法相结合使用。如果部分木马电路被激活,木马电路将消耗更多的动态功耗,从而有助于进一步区分有木马和无木马电路的功耗轨迹。现有木马激活方案可进行如下分类。

1) 区域无关的木马激活

这些方法不依赖区域,而是依赖于木马的偶然激活或系统激活。比如,Jha 和 Jha 提出基于随机概率的方法来检测木马[15]。其研究表明,在对电路应用特定概率模式的基础上,是有可能为电路构建唯一概率签名的。他们在 IUA 中应用基于特定概率的输入模式并比较其输出和原始电路的输出。如果两种输出存在差异,则表明存在木马。对于已制造 IC 的木马检测,模式应用的前提如下:在考虑原始设计与制造芯片是否一致的问题上应存在两者一致可信的可能性。Wolff 等分析了设计中的罕见节点组合[16],将罕见激活线路用作木马触发。同时,将低观测性的线路用作负载。Wolff 等生成向量集来激活这些线路。如果木马与这些线路相连,建议将生成向量集与传统 ATPG 测试向量相结合来激活木马并扩散木马的影响。

2) 区域相关木马激活

Banga 和 Hsiao 设计了两阶段测试生成技术,其目标是放大 IUA 和金片设计功耗波形之间的差异[4]。第一阶段(电路分区),区域感知模式帮助识别潜在的有木马区域。为了检测木马电路,一部分电路里的活动会增强而同时剩余部分电路