

硬件木马防护技术研究

王侃, 陈浩, 管旭光, 顾勇

(密码科学技术国家重点实验室, 北京 100878)

摘要: 对硬件木马防护技术进行了深入研究, 提出一种新的硬件木马防护分类方法, 系统全面地介绍了近年来主流的预防与检测技术, 并通过分析比对, 给出各方法的特点和存在的问题。最后, 提出新的防护技术设计思路, 对未来研究方向和趋势进行了展望, 并给出了基于木马库的硬件木马检测技术设计思路。

关键词: 硬件木马; 预防技术; 检测技术; 侧信道分析

中图分类号: TP402

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00197

Research on hardware Trojan defense

WANG Kan, CHEN Hao, GUAN Xu-guang, GU Yong

(State Key Laboratory of Cryptology, Beijing 100878, China)

Abstract: The definition and features of hardware Trojan were described firstly. After that, recent researches of defense and detection techniques were categorized with complete comparison and analysis. Then, current researches limitations were discussed based on the concepts and the trends perspectives of hardware Trojan defense and detection were proposed.

Key words: hardware Trojan, defense technology, detection technology, side-channel analysis

1 引言

随着集成电路技术的不断发展, 芯片的设计和制造逐步全球化。为了缩短芯片设计周期, 降低设计风险, 越来越多的芯片公司使用第三方EDA工具或采用第三方IP的方式实现相应模块, 芯片的制造、封装工作也多由第三方公司或代工厂完成^[1]。在这些过程中, 芯片有可能被植入恶意电路, 即硬件木马^[2]。研究发现, 硬件木马不仅会影响芯片的性能, 还会泄露芯片关键信息、改变电路功能、造成芯片失效等^[3]。

近年来, 硬件问题导致的安全事件层出不穷^[4]。2007年, 以色列轰炸叙利亚东北部的潜在核设施时, 由于通用处理器被植入后门, 叙利亚预警雷达形同虚设, 没有发出任何警报。2012年, 伊朗

布什尔核电站在物理隔绝的环境下依然遭受震网病毒的攻击。作为信息系统的重要支持, 芯片的安全至关重要。如果硬件木马被植入医疗、金融、军事等领域的核心安全系统或实时性系统的芯片中, 都将导致致命的后果, 严重威胁国家安全。

硬件木马的潜在安全威胁, 引起了国际广泛的关注。许多科研机构提出了硬件木马防护方法, 为芯片的安全保护提供了保障。根据芯片设计生产的一般流程, 硬件木马防护主要包括预防技术和检测技术。预防技术是在芯片设计时, 为防护硬件木马进行特别设计, 增强芯片抗修改的能力和自检测能力, 主要技术包括自检逻辑、激活单元、可测性设计、混淆技术以及专用架构技术等。检测技术是在芯片生产制造后, 通过检测方法判断硬件木马的存在, 常用的检测技术包括反向工

程、逻辑测试、侧信道分析、运行时监控等。

在以往的工作中,有很多针对硬件木马防护技术的综述研究,然而这些研究大都面向检测技术,侧重于侧信道分析、逻辑检测、反向工程等方面,而缺乏针对预防技术和其他检测技术的总结。为此,本文对硬件木马防护技术深入地进行了研究,提出了一种新的硬件木马防护分类方法,并对主流的防护方法进行更系统全面的分析,为下一步硬件木马防护的研究提供重要依据。

2 硬件木马

2.1 硬件木马定义

硬件木马是指在设计、生产和制造过程中通过植入、篡改等方式加入原始电路的恶意电路,意在窃取(或泄露)、破坏、改变电路或电路信息。

如图1所示,典型的硬件木马包含2个部分:触发电路和负载电路^[5]。触发电路在特定输入信号的条件会被触发,从而激活实现了恶意功能的负载电路部分,实施恶意攻击。

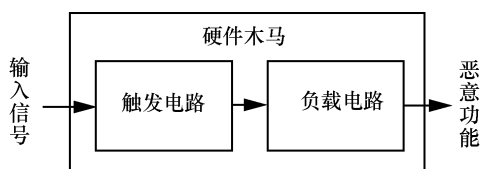


图1 硬件木马结构示意图

2.2 硬件木马特点和分类

一般来说,硬件木马具有以下几个基本特点。

1) 恶意性: 硬件木马一般都是有目的地恶意攻击,意在窃取重要数据,混淆、破坏原始电路功能,泄露秘密信息等。

2) 触发性: 在一般情况下,硬件木马处于非激活状态;在满足特殊条件或一定信号激励下,才会触发相应功能。

3) 隐藏性: 相对于一般电路,硬件木马电路尺寸小、功耗小、激活概率低,且在非激活状态不会影响原始电路运作,不易发现,具有很高的隐藏性。

4) 多样性: 根据实现方式、激活方式、目标性的不同,硬件木马可以分为不同类别,几乎存在于芯片设计生产的每一个阶段,如图2所示^[6],种类繁多,排查难度大。

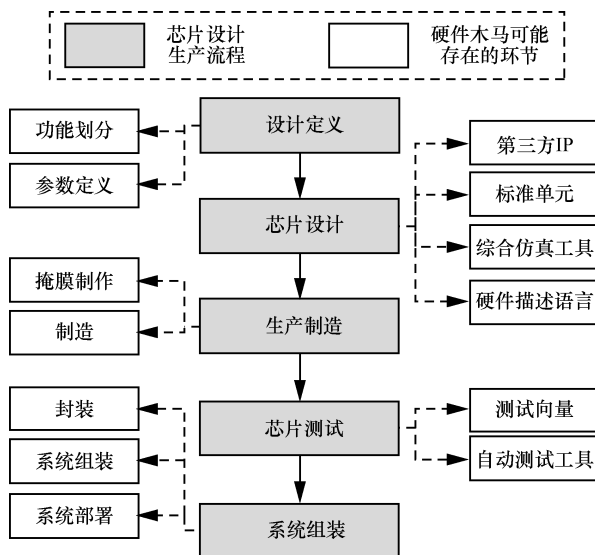


图2 硬件木马可能的植入阶段

硬件木马可以按照植入阶段、植入层次、激活方式、功能影响、存在形式和存在位置等因素进行分类^[7]。其中,按照植入阶段不同,硬件木马可以在设计、制造、测试等各个阶段植入;按照植入层次不同,硬件木马可以在系统级、寄存器级、门级、晶体管级甚至物理级植入;按照激活方式不同,硬件木马可以分为常开型、内部触发型和外部触发型等;按照功能影响不同,硬件木马可分为改变功能型、降低性能型、泄露信息型和拒绝服务型等;按照存在形式不同,可分为组合型、时序型、模拟型等;按照存在位置不同,硬件木马可以位于处理器、存储器、输入输出端口、电源模块、时钟网络、ASIC、DSP以及FPGA中。

3 硬件木马预防与检测技术

为避免硬件木马带来的安全隐患,近年来,国内外学者纷纷提出硬件木马防护的技术和方法,根据实施方式不同,主要分为芯片生产前的预防技术^[8-19]和芯片生产后的检测技术^[20-72],如图3所示。

3.1 预防技术

硬件木马预防技术是指在芯片设计阶段,通过修改原有设计或加入额外的检测电路等方法,增强芯片对电路修改或植入的检测能力,提高被植入硬件木马的激活概率,增加芯片对硬件木马的防护能力。

3.1.1 自检逻辑设计

一些研究在设计时加入了特定电路,形成自

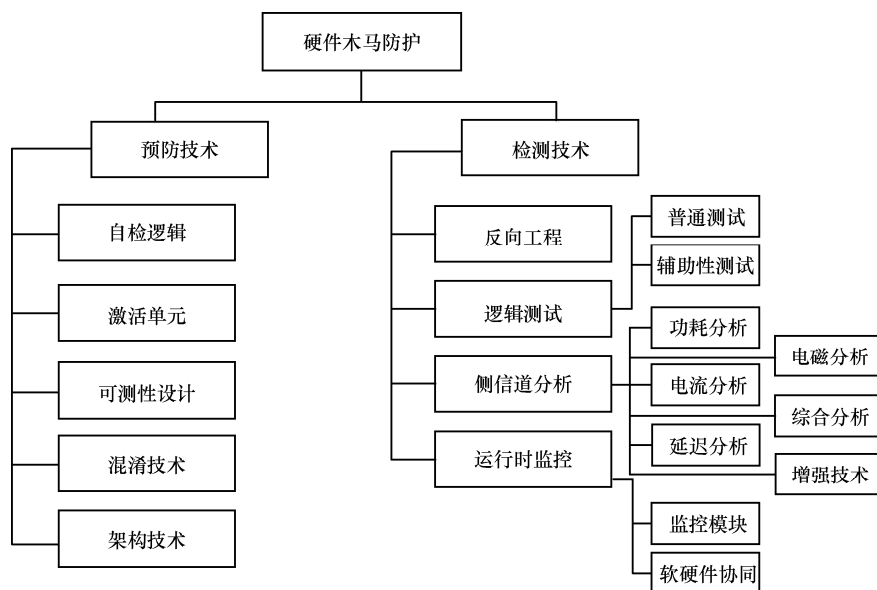


图3 硬件木马预防技术分类

检逻辑，以实现在硬件木马植入时的自检测。其中，Chakraborty 等^[8]利用攻击者会选用电路中的低可达状态节点和低可观测输出端点进行攻击的特点，提出一种防硬件木马设计方法。该方法在低可达状态节点添加控制逻辑（由特定密钥启动），能够触发节点状态并生成相关“签名值”，并根据在特定输入密钥下输出“签名值”的变化判断系统是否包含硬件木马。

Xiao 等^[9]利用攻击者会采用空白区域植入木马的特点，提出了一种防止木马植入的内建自认证技术。该技术在布局阶段利用芯片的空白区域填充具有实际功能的标准单元，并将标准单元连接形成芯片的自检电路，输出特定范围的签名值。一旦标准单元被删除或破坏，就会产生错误的签名值，通过对签名值的判断实现自认证的功能。

Li 等^[10]提出了一种将传感器作为自检模块来实现硬件木马预防的方法。该方法在芯片设计时加入传感器，预测特定操作序列下的时延特征，与基准数值进行比较。若比对结果存在较大差距，则可判定硬件木马的存在。

此外，Kitsos 等^[65]利用环形振荡器来预防硬件木马的植入。研究发现，硬件电路的改变会通过环形振荡器的频率变化体现。Zhang 等^[66]建立了环形振荡器网络，并将网络分布在整个芯片以监控预防硬件木马。Ferraiuolo 等^[67]还针对环形振

荡器的位置对检测的影响进行了分析研究，通过优化振荡器的位置提高自检的效率。

3.1.2 激活单元设计

另外一部分研究通过添加特定单元，最大化地激活硬件木马，以辅助生产后的硬件木马检测，提高检测成功率。

Salmani 等^[11]提出了一种提高硬件木马激活概率的方法。文章首先分析了激活硬件木马的可能性，并通过几何分布（GD, geometric distribution）方法预估硬件木马激活概率以及所需要的时钟周期。然后在激活概率较低的节点线路上添加虚拟触发器，提高这些节点状态的可达概率，如图4所示，其中，图4(a)中括号左侧数据表示该节点状态为真概率，右侧数据表示状态为假概率。实验结果显示，这种方法可以在对芯片面积不明显增加的情况下，大大减少激活硬件木马的时间，提高硬件木马检测的效率。

Zhou 等^[12]在电路中添加多路复用器，将激活概率最低的线路通过复用器屏蔽掉，保证低激活率的线路不被选择，从而提高激活的概率。

3.1.3 可测性设计

可测性设计是芯片功能测试的重要手段。有部分研究基于传统可测性设计理念提出了针对硬件木马的可测性设计方法，在设计时加

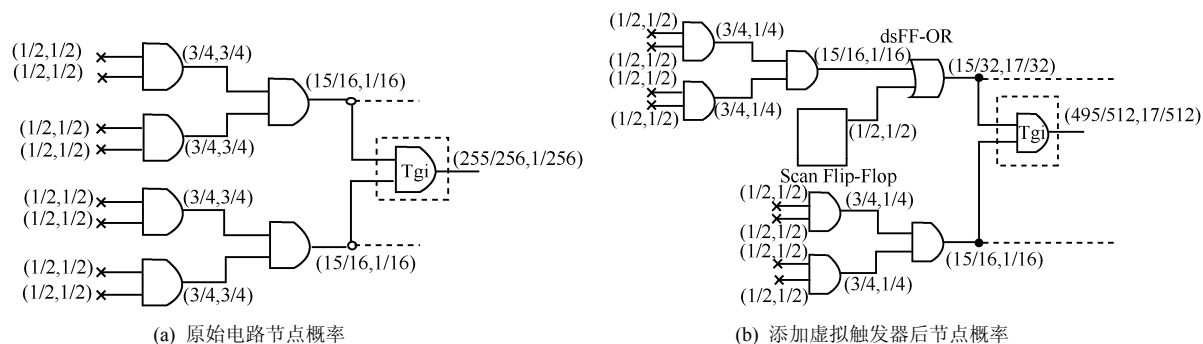


图 4 虚拟触发器示意

入可测点以辅助逻辑检测, 提高硬件木马检测的效率。

其中, Jin 等^[13]根据攻击者一定会攻击关键信号路径的特点, 提出了一种硬件木马可测性设计方法 (DFTT, design for Trojan test)。该方法通过代码分析、敏感路径搜索和检测点插入这 3 个环节, 实现对关键信号路径的保护, 以防止泄露型硬件木马的植入。此外, Banga 等^[14]提出了一种非扫描的可测性设计方法, 利用触发器的 $\bar{Q}$ 信号增加可达的状态空间, 从而提高木马被触发的概率, 如图 5 所示。



图 5 可测性设计方法

3.1.4 混淆技术

混淆技术是防止反向分析攻击和芯片修改的有效方法, 通过对芯片进行迷惑性的设计, 使攻击者不易找到真实电路, 增加木马植入的难度。此外, 混淆设计还可以使设计者在木马植入后及时发现芯片的改变。

Chakraborty 等^[15]使用文献[8]的思想, 提出一种基于混淆手段的 SoC 设计方法。该方法在芯片中创建了屏蔽实际功能模块的“网关”, 并使用特定的密钥激活, 通过这种方式对攻击者进行迷惑, 从而保护门级 IP 不被硬件木马植入。研究发现, 混淆技术可以保证在不影响面积、功耗和延迟的情况下, 有效提高木马检测的效率, 增加硬件木马植入的难度。随后, 该方法被应用于 RTL 级 IP 的检测和保护^[16]。Chakraborty 在文献[17]中, 将混淆状态

机划分为初始状态机和隔离状态机这 2 个部分, 一旦有错误的输入, 就会跳入隔离状态机无法跳出。实验证明其在对抗硬件木马植入方面效果显著。

3.1.5 架构技术

此外, Das 等^[18]提出了一种预防信息泄露型木马的总线架构, 其通过在 CPU 和内存之间设置一个守护核, 对 CPU 写内存的操作流进行监控, 及时发现与正常的操作流不符的写操作, 防止恶意硬件对关键信息的泄露。

Bloom 等^[19]提出了一种面向 FPGA SoC 的设计架构, 通过局部运行可重构 (PRR, partial runtime reconfiguration) 技术和硬件抽象层 (HAL, hardware abstraction layer), 运用片上资源重组、加密执行、功能等价变体等防御机制, 有效防止恶意木马的植入, 保护芯片的关键敏感信息。

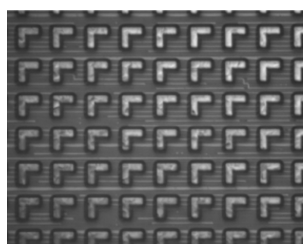
3.2 检测技术

不同于软件木马, 硬件木马一旦植入就无法被删除, 因此包含硬件木马的电路与原有电路一定会存在不同。硬件木马检测是指芯片在流片后通过反向分析、逻辑测试、侧信道分析等技术对芯片进行检测, 对比芯片流片前后存在的不同, 从而判断硬件木马是否存在。一个好的检测方法能够最大化提高测试的成功率, 并能避免因误差导致的检测错误。

3.2.1 反向分析法

反向分析法是迄今为止最彻底、最精确的木马检测方法。它通过逆向工程方法将封装 (或管芯) 的芯片电路打开, 逐层扫描拍照电路, 然后使用图形分析软件和电路提取软件重建电路结构图, 将恢复出的设计与原始设计进行对比分析, 如图 6 所示^[21], 根据电路的不同判断硬件木马的

存在^[20]。该检测方法能准确发现电路中的任何恶意修改, 对结构较简单的芯片检测效果不错, 但相对比较耗时, 而且费用较高。



(a) 目标芯片的 M6 布局



(b) 目标芯片的版图

图6 反向分析示意图

为此, 不少研究针对反向分析提出了优化方法。其中, Bhasin 等^[21]针对传统光学检测的不足提出了改进措施。研究显示, 具有高利用率(一般大于 80%)的硬件木马都会影响到高金属层。因此, 该方法只比较最高几层金属层的镜像(与 GDSII), 并通过计算 GDSII 和高分辨率的高金属层镜像之间的互相关性来检测。Zhou 等^[22]提出一种光学方法以检测和确定硬件木马位置。该方法首先将填充单元进行修改, 使其对近红外的波长光能够强反射, 然后对芯片进行反面拍摄, 利用填充单元生成的亮点作为芯片的水印, 判别芯片是否被篡改。Bao 等^[23]提出一种反向工程实施方案, 采用了成熟的机器学习方法, 通过一类支持向量机(one-class support vector machine)来实现版图比对和硬件木马检测。随后 Bao^[24]基于该方法提出一种反向分析辅助方法, 通过对每个单元敏感性的分析和对标准单元的划分, 降低反向分析时的难度。此外, 文献[25,26]也都针对反向分析方法的效率和成本进行了改善。

3.2.2 逻辑测试法

逻辑测试法通过产生测试向量, 试图触发隐藏的木马激活条件, 使硬件木马生效并显现相应

功能。由于芯片密度不断增大, 要找到覆盖所有节点的测试向量几乎不可能, 因此逻辑测试的难点在于定义合适的测试向量激活硬件木马^[27]。对于典型的硬件木马, 其设计的一个指标就是隐藏性, 因此通过标准测试向量激活木马的方法难度很大。

为此, 不少研究人员提出了提高激活概率的逻辑测试方法。Zhang 等^[28]提出了一种完善的硬件木马逻辑测试检测流程, 通过可疑信号检测、覆盖率分析、冗余电路删除、ATPG 生成以及等价定理分析等环节, 填补了传统流程不能测试第三方 IP 的不足。其中, 覆盖率分析用于识别出可疑信号, 冗余电路删除和等价定理用于减少可疑信号数量, 而 ATPG 生成则用于产生激活硬件木马的激励信号。此外, Jha 等^[29]提出了一种随机分布方法, 通过比较原始电路和现实电路的逻辑功能区别, 即时发现硬件木马。Salmani^[30]和 Banga^[14]等提出了一种辅助逻辑测试的硬件木马激活方法, 并分析了它的平均激活时间。

3.2.3 侧信道分析方法

基于侧信道分析的硬件木马检测方法是目前使用最多、最有效的检测方法之一。该方法通过比对电路中物理特性和旁路信息的不同, 发现电路的变化, 如图 7 所示^[21]。它基于的思想是任何硬件电路的改变都会反映在一些电路参数上, 如功率、时序、电磁、热等。在侧信道分析方法中, 需要有一个比对芯片, 即没有被植入的“纯净芯片”。

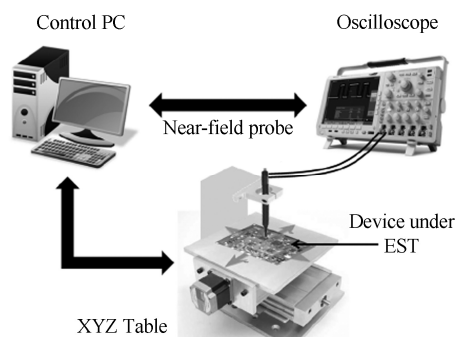


图7 侧信道分析平台示意图

根据旁路信息的不同, 侧信道分析可分为基于功耗^[31~37]、静态电流^[38~41]、电磁信息^[42~44]、路径时延信息^[45~48]等的分析方法。除此以外, 还有

针对多种旁路信息的综合分析和侧信道分析增强技术^[53-57]的研究。

1) 功耗分析

Agarwal 等^[31]首次提出利用侧信道信息检测硬件木马的方法,该方法获取芯片的功耗特征,通过 K-L 扩展分析法生成芯片指纹,再将待测芯片与“纯净芯片”的功耗特征进行比对,以判断芯片是否被篡改。Banga 等^[32]利用“持续向量技术”将功耗信息放大,使包含硬件木马的芯片特征更加凸显。Marchand 等^[33]在 FPGA 上实现并完成了硬件木马测试。Liu 等^[34]在前人基础上提出了新的功耗分析方法。

在国内方面,大多数工作侧重于功耗特征分析方法的研究。其中,刘长龙等^[35]基于相关性分析(Pearson 相关系数)对芯片中的功耗信息进行分析比对,根据功耗特征的变化实现硬件木马的检测。张鹏等^[36]提出了一种硬件木马无损检测方法,即通过基于绝对信息散度指标的投影寻踪技术,实现功耗特征提取识别与分析。薛明富等^[37]提出了一种针对微弱木马的信号检测技术,通过时域约束估计器和主成分投影技术、子空间投影和重构信号分析方法,实现对芯片功耗信息的分析检测。

2) 漏电流分析

除分析动态功耗方法以外,还有一些针对漏电流的研究。其中,Wang 等^[38]提出一种通过电流信息检测硬件木马的方法。在该方法中,芯片漏电流和电流信息作为芯片的指纹信息被提取,并与“纯净芯片”相比对。不同于直接使用电流信息,该文使用电流整合技术来降低检测误差。Rad 等^[39]提出了一种基于漏电流和瞬变电流的信息分析方法,利用 4 种信号校准机制提高判断的准确性。Wei 等^[40]通过追踪漏电流信息来判断芯片是否含有硬件木马。Wilcox 等^[41]在最近的研究中通过多个芯片中拓扑分布的端点进行漏电流的测试以降低噪声影响。

3) 电磁信息

Soll 等^[42]提出一种基于电磁信号的硬件木马检测方法。该方法基于 FPGA 实现了 AES 并植入硬件木马,分析了其在不同位置、不同逻辑分布情况下对硬件木马检测的影响。Balasch 等^[43]在

FPGA 上实现了极小的硬件木马,并通过电磁信号进行分析检测,实验验证了检测方法的有效性,同时对小尺寸硬件木马的检测难度给予了评定。李雄伟等^[44]利用 K-L 变换对芯片中的电磁信号进行特征提取,通过信号分析等方法实现硬件木马的检测。

4) 路径延迟信息

此外,路径延迟也会因为硬件木马的植入发生变化。基于这个特性,Jin^[45]首次提出了利用芯片延迟信息生成芯片指纹实现硬件木马检测的方法。随后,基于该项工作,Cha^[46]和 Kumar^[47]等也先后提出了针对路径延迟的检测方法。Yoshimizu 等^[48]利用硬件木马会破坏芯片的一些路径对称性的特点,提出了一种基于对称路径的检测手段,通过对称路径搜索、路径延迟检测等步骤,检测硬件木马是否植入。

5) 综合分析

单一的测试可能会受到生产过程产生的噪声影响而使测试不准确,很多研究采用多种信息综合分析的思路。其中,Narasimhan^[49]分析了多个侧信道参数之间的相关性,并首次提出利用多项旁路信息进行硬件木马检测的方法。Nowroz 等^[50]利用芯片的热量和功耗分布进行侧信道分析。Cao^[51]和 Ngo^[52]等先后利用时延和功耗信息^[51]、时延和电磁信息^[52]进行了综合分析检测。

6) 增强技术

也有一些研究提出了针对侧信道分析的增强技术,以提高分析的效率和准确度。Banga^[53]、Xue^[54]和 Du^[55]分别提出基于芯片划分的检测方法,对不同芯片的不同区域分别提取侧信道信息进行统计分析,通过检测点部署、最大化激励测试向量生成以及信号校准等技术,改善检测的敏感性,去除片间的生产制造产生的噪声,从而提高侧信道检测时的效率和准确性。文献[51]同样采用了芯片划分的方法,每个区域都使用一个独立的电流传感器进行信息采集。

此外,Potkonjak 等^[56]提出了针对门级特性的侧信道分析方法,利用门级的漏电流、动态功耗和时延等特征信息,建立木马检测的线性规划模型,有效提高了侧信道分析的精度。Karunakaran 等^[57]采用了类似的方法,分别针对与、或、非、

表 1 硬件木马预防检测技术分析对比汇总

方法	复杂度	代价	有效性	覆盖范围	可实施性	可扩展性	增加面积	需要原型
预防技术	H	H	H	H	H	L	Y	N
反向工程	H	H	H	H	L	L	N	Y
逻辑测试	M	L	L	M	H	H	N	N
侧信道分析	M	M	H	M	H	M	N	Y
运行时监控	M	M	M	M	M	M	N	N
协同检测	M	M	H	H	H	M	N	Y/N

注：H 表示高，M 表示中，L 表示低；Y 表示是，N 表示否，Y/N 表示两者皆有。

与非、或非等门的漏功耗特性进行了研究，建立线性规划模型，通过求解该模型和表示硬件木马存在的变量，实现硬件木马的检测。

3.2.4 运行时监控方法

尽管上述的预防检测技术足以保证硬件木马的有效防护，但由于方法的局限性，依然不能覆盖所有的硬件木马。运行时监控方法就是在上述方法没有成功的情况下，发挥最后的屏障作用，即在芯片运转期间，实时监测重要信息，及时发现非法、恶意的操作，并采取相应措施防止恶意功能的运行。

McIntyre 等^[58]提出了基于功能等价变体（functionally equivalent variants）的检测方法，通过不同变体在不同核中的运行结果，判断多核系统中的硬件木马植入。Abramovici 等^[59]利用可重构芯片中的可重构核，对芯片的操作进行实时监控，排查非法操作。Bloom 等^[60]提出了一种软硬件协同设计，在操作系统层面，协助硬件木马的检测。Forte^[61]和 Bao^[62]等提出了一种根据芯片运行时的热分布情况进行实时监控和检测的方法，其在芯片设计时加入热传感器，并在芯片运行时采集热量信息，通过去噪处理和数据分析，实时检测硬件木马的存在。在文献[63]中，一旦异常操作产生，芯片中的警戒模块就会关闭芯片的相关功能，并触发芯片安全机制，防止硬件木马的进一步攻击。此外，Cui 等^[64]针对第三方 IP 核提出了硬件木马实时检测方法。该方法通过 8 条设计规则以及时延、面积、操作序列、开销等约束，分析判断 IP 核的可信度，并提出了使硬件木马失效的快速恢复策略。

此外，还有部分研究通过在芯片顶层增加金属屏蔽层，以主动实时监测探针探测和 FIB 修改等物理攻击^[68]。其中，Zhang 等^[69]提出一种应用于高安全芯片的抗侵入式物理攻击防篡改检测技术，利用芯片顶层金属对侵入式攻击进行主动监测，可有效地防止对电路存储关键信息的提取。Briais 等^[70]利用旅行商算法和遗传算法生成有源金属屏蔽层，其生成的屏蔽层可以与检测电路连接，有效防止芯片表面被探测攻击。Shahrjerdi 等^[71]提出了一种金属屏蔽层设计方法，通过添加传感器等器件，以实时监测物理攻击，从而实现芯片的保护。Cioranescu 等^[72]还针对 Mesh 结构的金属防护层提出了密码保护方法。

4 硬件木马防护技术分析

4.1 现有方法对比分析

在实际的硬件木马防护中，不会将所有的预防与检测技术全部应用，而是根据各种方法的特点和应用领域，有选择性地采用合适的方法实施防护。为此，本文将所有的预防与检测技术按照复杂度、代价、有效性、覆盖范围、可实施性、可扩展性、是否增加面积、是否需要原型等特性进行了分析比对，为方法的选择提供依据，如表 1 所示。使用者可以根据资金状况、设计周期、应用范围等因素采用最合适的方法。

从表 1 中可以看出，每种方法的特性都不尽相同。在代价方面，由于反向工程会破坏芯片，且需要搭建专门的平台，因此硬件开销较高；振荡器网络等预防方法需要额外的电路设计，也会带来芯片面积、功耗等开销；相比较而言，逻辑

测试不需要额外的检测平台和电路设计,成本相对较低。在有效性方面,预防技术、反向工程和侧信道分析技术都有不错的效果,而逻辑测试由于难以找到合适的测试向量,因此效果不佳。在覆盖范围方面,基于逻辑测试的方法基本可以应对大多数硬件木马,而其他方法在覆盖范围方面都存在局限;相比较单种测试方法,采用多种测试相结合的协同测试可以取长补短,增加测试的覆盖范围。在可实施性方面,预防技术、逻辑测试以及侧信道分析方面,都有较低的硬件开销,平台易搭建,实施性较强。在可扩展性方面,逻辑测试和侧信道分析都有易扩展的优点。由于预防技术需添加额外电路,因此会改变原有设计,增加芯片面积。在原型方面,反向工程需要有原始电路的版图作为比对原型,而侧信道分析则需要“纯净”电路作为测量基准。

4.2 现有方法存在的问题

尽管硬件木马预防检测技术的研究已经取得了许多成果,但其仍然是一个较新的研究领域,面临许多挑战。总体来讲主要分为以下几个方面。

1) 预防技术的不可预估性

由于硬件木马的多样性特点,在任何一种新型木马出现之前,都无法预测硬件木马的存在形式,因此要在芯片设计时考虑所有未知形式的硬件木马几乎不可能,这也为硬件木马预防技术提出很大的挑战。

2) 逻辑测试方法的局限性

逻辑测试方法的根本思想在于通过测试向量激活并显现硬件木马的相应功能,从而发现硬件木马的存在。然而,这种方式只能针对修改、破坏功能型的硬件木马,对于窃取、泄露型硬件木马没有效果。此外,逻辑测试对于一些无法通过外部逻辑信号激活的木马(如满足一定周期或计数条件激活)也不适用。

3) 反向分析技术的高开销成本

反向分析技术虽然有效,但其开销成本大且测试周期长,难以大范围实施。在实施反向分析后,原有的芯片会因遭到破坏而不能使用,因此反向分析方法只能采用抽样检测的形式,这就为部分或少量木马植入的攻击手段提供了机会,不能保证所有芯片的安全性。

4) 侧信道信息的提取困难大

侧信道方法对于功能较为简单的芯片或密度较低的芯片应用效果比较显著。但是,对于更为复杂的芯片尤其是在硬件木马比较分散的情况下,由于硬件木马的尺寸很小,对于整个芯片的功耗、电磁等旁路信号的影响微不足道,侧信道分析检测方法难以实施。此外,由于工艺噪声的存在,对于不同芯片或者同一芯片的不同批次,采集到的旁路信号不尽相同,这也给侧信道分析带来了极大困扰。

5) 运行时监控的漏洞多

运行时监控技术通过硬件或软硬件相结合的方式,在运行期间监控总线或设备上的操作序列。这种方法不仅需要额外的设计开销,而且会存在一些安全漏洞,仅能防止特定类型的硬件木马,而无法应对绕过监控点的恶意攻击。

5 硬件木马防护技术展望

硬件木马和防护是黑与白的对抗,攻与防的较量,有新型的木马出现,也会相应地有新的检测手段问世。因此,为保证密码芯片的绝对安全,要不断深入研究新型硬件木马安全防护技术。根据现有硬件木马研究的一般特点,未来硬件木马防护技术的研究可以从以下几个方面开展。

5.1 新的预防方法研究

传统的硬件木马预防技术大都采用自检模块、虚拟触发器等方式,而利用时延特性进行敏感路径的设计也是一种有效的方法。此外,硬件木马在结构设计等方面的研究,以及对硬件木马通用特性的提取和描述,对硬件木马预防技术的研发有很大帮助,也是未来研究的一个可行方向^[27]。

5.2 新的检测方法研究

如上文提到的,传统的检测方法都存在一些不足。一方面,可以在现有方法基础上提出改善措施,降低成本,提高检测效率,如采用自顶向下和分层的策略实现反向分析方法,与可测性设计相结合的测试向量生成方法,或者在物理设计时加入更多的测试点、提供更多的侧信道信息等。另一方面,可以通过研究新的方法,丰富检测手段,提高检测成功率,如利用不可克隆函数(PUF)^[73]和时延信息对路径敏感的特性,为芯片

创建识别密钥, 如图 8 所示^[74], 芯片内部电路任何的变化都可以通过密钥的生效情况来体现^[2]。

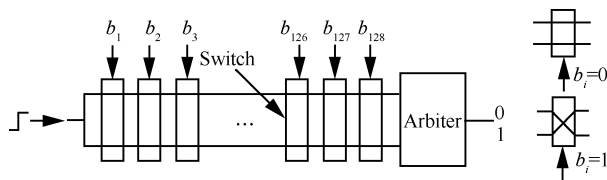


图 8 PUF 结构示意图

5.3 多方法协同检测研究

在传统的木马检测方法中, 多为针对某一种特殊木马或某一种特殊手段的研究。然而, 由于硬件木马的特殊性、多样性, 单一的检测手段已经不能满足需求, 而多方法协同检测的方式也成为研究的必然趋势。例如, 将可测性设计与侧信道分析技术相结合, 在芯片设计时提供用于信号提取的接口; 将反向工程与侧信道检测相结合, 将反向分析的结果作为侧信道检测的基础, 提高检测的成功率; 还可以将预防技术与逻辑测试、侧信道分析技术相结合实施协同检测。

5.4 木马病毒库和统一检测平台的建立

由于硬件木马的多样性特点, 将会出现越来越多形式的硬件木马, 如针对 FPGA 内部结构和比特流的硬件木马、针对第三方 IP“配合型攻击”硬件木马(单个 IP 无攻击性, 多个 IP 联合攻击)以及性能减低型/拒绝服务型硬件木马等, 这些硬件木马的存在形式在出现之前无法预知。在这种情况下, 采用类似软件木马病毒库的方式, 建立硬件木马库, 为每个新增木马建立模型, 并在反向工程中与原始版图进行比对, 是解决现有问题的一种可行方案。通过对已知木马电路类型进行建模, 录入木马库中, 再通过版图分析工具对反向得到的版图进行可疑电路搜寻, 与木马库中的木马电路模型进行匹配, 从而实现硬件木马的检测。此外, 建立专用的硬件木马检测 EDA 工具和统一的检测平台也成为必然需求, 这不仅包括同时考虑预防技术和检测技术的统一检测^[75], 也包括对多种木马类型的统一检测。

6 结束语

硬件木马的出现对信息安全构成了严重威

胁。硬件木马的预防与检测技术是硬件木马防护的有效手段。本文提出一种新的硬件木马防护分类方法, 并系统全面地介绍了近年来主流的预防与检测技术, 包括芯片设计时的预防技术, 芯片生产后的侧信道检测、逻辑测试、反向分析、运行时监控等。由于硬件木马的特点, 现有的防护手段仍不能满足安全防护的需求, 针对不同硬件木马存在形式的预防检测方法、统一检测平台以及多方法协同检测技术等是未来可行的研究方向。

参考文献:

- [1] BHASIN S, REGAZZONI F. A survey on hardware Trojan detection techniques[C]//IEEE international Symposium on Circuits & Systems(ISCAS). 2015.
- [2] TEHRANIPOOR M, KOUSHANFAR F. A survey of hardware Trojan taxonomy and detection[J]. Journal of IEEE Design & Test of Computers, 2010, 27(1): 10-25.
- [3] 牛小鹏, 李清宝, 王伟, 等. 硬件木马技术研究综述[J]. 信息工程大学学报, 2012, (6): 740-748.
NIU X P, LI Q B, WANG W, et al. Survey on the hardware Trojan technologies[J]. Journal of Information Engineering University, 2012, (6): 740-748.
- [4] LI H, LIU Q, ZHANG J. A survey of hardware Trojan threat and defense[J]. Integration the VLSI Journal, 2016, 55:426-437.
- [5] XUAN T N, BHASIN S, DANGER J L, et al. Linear complementary dual code improvement to strengthen encoded circuit against hardware Trojan horses[C]//IEEE International Symposium on Hardware Oriented Security and Trust (HOST). 2015: 82-87.
- [6] RAJENDRAN J, GAVAS E, JIMENEZ J. Towards a comprehensive and systematic classification of hardware Trojans[C]//IEEE international Symposium on Circuits and Systems (ISCAS). 2010: 1871-1874.
- [7] KARRI R, RAJENDRAN J, ROSENFELD K. Trustworthy hardware: identifying and classifying hardware Trojans[J]. Journal of Computer, 2010, 43(10): 39-46.
- [8] CHAKRABORTY R, PAUL S, BHUNIA S. On-demand transparency for improving hardware Trojan detectability[C]//The 2008 IEEE International Workshop on Hardware-Oriented Security and Trust (HOST). 2008: 48-50.
- [9] XIAO K, FORTE D, TEHRANIPOOR M. A novel built-in self-authentication technique to prevent inserting hardware Trojans[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2014, 33(12):1778-1791.
- [10] LI M, DAVOODI A, TEHRANIPOOR M. A sensor-assisted self-authentication framework for hardware Trojan detection[C]//Design, Automation & Test in Europe Conference & Exhibition. 2012:1331-1336.
- [11] SALMANI H, TEHRANIPOOR M, PLUSQUELLIC J. A novel

- technique for improving hardware trojan detection and reducing Trojan activation time[C]//The 2009 IEEE International Workshop on Hardware-Oriented Security and Trust (HOST'2009), IEEE Computer Society, 2009: 112-125.
- [12] ZHOU B, ZHANG W, THAMBIPILLAI S, TEO J. A low cost acceleration method for hardware Trojan detection based on fan-out cone analysis[C]//The International Conference on Hardware/Software Co-design and System Synthesis (CODES+ISSS). 2014: 1-10.
- [13] JIN Y, KUPP N. DFTT: design for Trojan test[C]//2010 IEEE International Conference on Electronics Circuits and Systems (ICECS'2010). 2010: 1166-1171.
- [14] BANGA M, MICHAEL S. ODTETTE: a non-scan design-for-test methodology for Trojan detection in ICs[C]//The 2011 IEEE International Workshop on Hardware-Oriented Security and Trust (HOST'2011), IEEE Computer Society, 2011: 18-23.
- [15] CHAKRABORTY R, BHUNIA S. HARPOON: an obfuscation-based SoC design methodology for hardware protection[J]. IEEE Transactions on CAD of Integrated Circuits and Systems, 2009, 28(10):1493-1502.
- [16] CHAKRABORTY R, BHUNIA S. Security through obscurity: an approach for protecting register transfer level hardware IP[C]//IEEE International Workshop on Hardware-Oriented Security and Trust(HOST). 2009.
- [17] CHAKRABORTY R, BHUNIA S. Security against hardware Trojan through a novel application of design obfuscation[C]//ICCAD. 2009: 113-116.
- [18] DAS A, MEMIK G, ZAMBRENO J, et al. Detecting preventing information leakage on the memory bus due to malicious hardware[C]//The Conference on Design, Automation and Test in Europe (DATE). 2010: 861-866.
- [19] BLOOM G, NARAHARI B, SIMHA R, et al. FPGA SoC architecture and runtime to prevent hardware Trojans from leaking secrets[C]//IEEE International Workshop on Hardware-Oriented Security and Trust(HOST). 2015: 48-51.
- [20] SANNO B. Detecting hardware Trojans [EB/OL]. http://www.crypto.rub.de/imperia/md/content/seminare/itss09/benjamin_sanno.semembsec_termpaper_20090732_final.pdf.
- [21] BHASIN S, DANGER J, GUILLEY S, et al. Hardware Trojan horses in cryptographic IP cores[C]//Fault Diagnosis and Tolerance in Cryptography. 2013:15-29.
- [22] ZHOU B, ADATO R. Detecting hardware Trojans using backside optical imaging of embedded watermarks[C]//ACM/IEEE Design Automation Conference (DAC). 2015.
- [23] BAO C, FORTE D, SRIVASTAVA A. On application of one-class SVM to reverse engineering-based hardware Trojan detection[C]//The International Symposium on Quality Electronic Design (ISQED). 2014: 47-54.
- [24] BAO C, XIE Y, SRIVASTAVA A. A security-aware design scheme for better hardware Trojan detection sensitivity[C]//IEEE International Symposium on Hardware Oriented Security and Trust (HOST). 2015: 52-55.
- [25] TORRANCE R, JAMES D. The state-of-the-art in semiconductor reverse engineering[C]//The 48th ACM/IEEE Design Automation Conference (DAC). 2011: 333-338.
- [26] COURBON F, LOUBET-MOUNDI P, FOURNIER J J A, et al. A high efficiency hardware Trojan detection technique based on fast SEM imaging[C]//Design, Automation & Test in Europe Conference & Exhibition. 2015:788-793.
- [27] MOEIN S, SUBRAMNIAN J, GULLIVER T A, et al. Classification of hardware Trojan detection techniques[C]//The 10th International Conference on Computer Engineering & Systems. 2016: 357-362.
- [28] ZHANG X, TEHRANIPOOR M. Case study: detecting hardware Trojans in third-party digital IP cores[C]//IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). 2011: 67-70.
- [29] JHA S, JHA S K. Randomization based probabilistic approach to detect Trojan circuits[C]//IEEE High Assurance Systems Engineering Symposium, IEEE Computer Society. 2008:117-124.
- [30] SALMANI H, TEHRANIPOOR M, PLUSQUELLIC J. A novel technique for improving hardware Trojan detection and reducing trojan activation time[J]. IEEE Transactions on Very Large Scale Integration Systems, 2012, 20(1):112-125.
- [31] AGRAWAL D, BAKTIR S, KARAKOYUNLU D, et al. Trojan detection using IC fingerprinting[C]//The 2007 IEEE Symposium on Security and Privacy(SP'07). 2007: 296-310.
- [32] BANGA M, HSIAO M S. A novel sustained vector technique for the detection of hardware Trojans[C]//The 2009 22nd International Conference on VLSI Design (VLSID'09). 2009: 327-332.
- [33] MARCHAND C, FRANCQ J. Low-level implementation and side-channel detection of stealthy hardware Trojans on field programmable gate arrays[J]. IET Computers Digital Technology, 2014, 8(6): 246-255.
- [34] LIU Y, HUANG K, MAKRI S Y. Hardware Trojan detection through golden chip-free statistical side-channel fingerprinting[C]//ACM/ IEEE Design Automation Conference. 2014: 1-6.
- [35] 刘长龙, 赵毅强, 史亚峰, 等. 基于相关性分析的硬件木马检测方法[J]. 计算机工程, 2013, 39(9): 183-195.
- LIU C L, ZHAO Y Q, SI Y F, et al. Hardware Trojan detection method based on correlation analysis[J]. Computer Engineering, 2013, 39(9): 183-195.
- [36] 张鹏, 王新成, 周庆. 基于投影寻踪分析的芯片硬件木马检测[J]. 通信学报, 2013, 34(4): 126-137.
- ZOU C, ZHANG P, DENG G M, et al. Design of hardware Trojan based on power side-channel exposure[J]. Computer Engineering, 2011, 37(11):135-137.
- [37] 薛明富, 胡爱群, 刘威, 等. 基于子空间域特征提取的硬件木马检测方法[J]. 东南大学学报(自然科学版), 2014, 44(3): 457-461.
- XUE M, HU A, LIU W, et al. Detecting hardware Trojan through feature extraction in subspace domain[J]. Journal of Southeast University(Natural Science Edition), 2014, 44(3): 457-461.

- [38] WANG X, SALMANI H, TEHRANIPOOR M, et al. Hardware Trojan detection and isolation using current integration and localized current analysis[C]//IEEE International Symposium on Defect and Fault Tolerance of VLSI Systems. 2008: 87-95.
- [39] RAD R, WANG X, TEHRANIPOOR M, PLUSQUELIC J. Power supply signal calibration techniques for improving detection resolution to hardware Trojans[C]//IEEE/ACM International Conference on Computer-Aided Design (ICCAD). 2008: 632-639.
- [40] WEI S, POTKONJAK M. Scalable hardware Trojan diagnosis[J]. IEEE Transactions on Very Large Scale Integration Systems, 2012, 20(6): 1049-1057.
- [41] WILCOX I, SAQIB F, PLUSQUELLIC J. GDS-II Trojan detection using multiple supply pad VDD and GND IDDQs in ASIC functional units[C]//IEEE International Symposium on Hardware Oriented Security and Trust (HOST). 2015: 144-150.
- [42] SOLL O, KORAK T, MUEHLBERGHUBER M, et al. EM-based detection of hardware Trojans on FPGAs[C]//IEEE International Symposium on Hardware-Oriented Security and Trust. 2014: 84-87.
- [43] BALASCH J, GIERLICH B, VERBAUWHEDE I. Electromagnetic circuit fingerprints for hardware Trojan detection[C]//IEEE International Symposium on Electromagnetic Compatibility. 2015: 246-251.
- [44] 李雄伟, 徐徐, 张阳, 等. 一种基于电磁旁路分析的硬件木马检测方法[J]. 计算机工程与应用, 2013, 49(12): 97-100.
- LI X, XU X, ZHANG Y, et al. Hardware Trojan detection method based on electromagnetic side-channel analysis[J]. Computer Engineering and Applications, 2013, 49(12): 97-100.
- [45] JIN Y, MAKRI S Y. Hardware Trojan detection using path delay fingerprint[C]//IEEE International Symposium on Hardware Oriented Security and Trust (HOST). 2008: 51-57.
- [46] CHA B, GUPTA S. Trojan detection via delay measurements: a new approach to select paths and vectors to maximize effectiveness and minimize cost[C]//Design, Automation and Test in Europe Conference and Exhibition (DATE). 2013: 1265-1270.
- [47] KUMAR P, SRINIVASAN R. Detection of hardware Trojan in SEA using path delay[C]//Electrical, Electronics and Computer Science. 2014:1-6.
- [48] YOSHIMIZU N. Hardware Trojan detection by symmetry breaking in path delays[C]//IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). 2014: 107-111.
- [49] NARASIMHAN S, DU D, CHAKRABORTY R S, et al. Multiple-parameter side-channel analysis: a non-invasive hardware Trojan detection approach[C]//IEEE International Symposium on Hardware-Oriented Security and Trust. 2010:13-18.
- [50] NOWROZ A, HU K, KOUSHANFAR F, et al. Novel techniques for high-sensitivity hardware Trojan detection using thermal and power maps[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2014 (33): 1792-1805.
- [51] CAO Y, CHANG C H, CHEN S. A cluster-based distributed active current sensing circuit for hardware Trojan detection[J]. IEEE Transactions on Information Forensics & Security, 2014, 9(12): 2220-2231.
- [52] NGO X, EXURVILLE I, et al. Hardware Trojan detection by delay and electromagnetic measurements[C]//Design, Automation and Test in Europe Conference and Exhibition (DATE). 2015: 782-787.
- [53] BANGA M, HSIAO M S. A region based approach for the identification of hardware Trojans[C]//IEEE International Workshop on Hardware-Oriented Security and Trust, IEEE Computer Society. 2008: 40-47.
- [54] XUE M, HU A, LI G. Detecting hardware Trojan through heuristic partition and activity driven test pattern generation[C]//Communications Security Conference. 2014:1-6.
- [55] DU D, NARASIMHAN S, CHAKRABORTY R S, et al. Self-referencing: a scalable side-channel approach for hardware Trojan detection[C]//The International Conference on Cryptographic Hardware and Embedded Systems (CHES). 2010:173-187.
- [56] POTKONJAK M, NAHAPETIAN A, NELSON M, et al. Hardware Trojan horse detection using gate-level characterization[C]//ACM/IEEE Design Automation Conference(DAC). 2009: 688-693.
- [57] KARUNAKARAN D K, MOHANKUMAR N. Malicious combinatorial hardware Trojan detection by gate level characterization in 90nm technology[C]//The International Conference on Computing, Communication and Networking Technologies. 2014: 1-7.
- [58] MCINTYRE D, WOLFF F, PAPACHRISTOU C, et al. Dynamic evaluation of hardware trust[C]//IEEE International Workshop on Hardware-Oriented Security and Trust. 2009: 108-111.
- [59] ABRAMOVICI M, BRADLEY P. Integrated circuit security: new threats and solutions[J]. China Gems & Jades, 2009:1-3.
- [60] BLOOM G, NARAHARI B, SIMHA R. OS support for detecting Trojan circuit attacks[C]//IEEE International Symposium on Hardware Oriented Security and Trust (HOST). 2009: 100-103.
- [61] FORTE D, BAO C, SRIVASTAVA A. Temperature tracking: an innovative run-time approach for hardware Trojan detection[C]//The International Conference on Computer-Aided Design. 2013: 532-539.
- [62] BAO C, FORTE D, SRIVASTAVA A. Temperature tracking: toward robust run-time detection of hardware Trojans[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), 2015, 34(10):1577-1585.
- [63] XUAN T N, DANGER J L, GUILLEY S, et al. Hardware property checker for run-time hardware Trojan detection[C]//European Conference on Circuit Theory and Design. 2015:1-4.
- [64] CUI X, MA K, SHI L, et al. High-level synthesis for run-time hardware Trojan detection and recovery[C]//ACM/IEEE Design Automation Conference (DAC). 2014:1-6.
- [65] KITSOS P, VOYIATZIS A G. FPGA Trojan detection using length-optimized ring oscillators[C]//Digital System Design. 2014:675-678.
- [66] ZHANG X, TEHRANIPOOR M. RON: an on-chip ring oscillator network for hardware Trojan detection[C]//Design, Automation and Test in Europe Conference and Exhibition. 2011: 1-6.
- [67] FERRAIUOLO A, ZHANG X, TEHRANIPOOR M. Experimental

- analysis of a ring oscillator network for hardware Trojan detection in a 90nm ASIC[C]//IEEE/ACM International Conference on Computer-Aided Design (ICCAD). 2012: 37-42.
- [68] NGO X, DANGER J, GUILLEY S, et al. Cryptographically secure shield for security IP protection[J]. IEEE Transaction on Computers, 2017, 66 (2): 354-360.
- [69] 张赞, 赵毅强, 刘军伟, 等. 一种抗物理攻击防篡改检测技术[J]. 微电子学与计算机, 2016, 33(4): 121-124.
- ZHANG Y, ZHAO Y Q, LIU J W, et al. A temper-resistant detecting technique against physical attack[J]. Microelectronics & Computer, 2016, 33(4): 121-124.
- [70] BRIAIS S, CIORANESCO J, DANGER J, et al. Random active shield[C]//Fault Diagnosis and Tolerance in Cryptography, 2012: 103-113.
- [71] SHAHRJERDI D, RAJENDRAN J, GARG S, et al. Shielding and securing integrated circuits with sensors[C]//ICCAD. 2014: 170-174.
- [72] CIORANESCO J, DANGER J, GRABA T, et al. Cryptographically secure shields[C]//HOST. 2014: 25-31.
- [73] ZHANG J, QU G, LV Y, ZHOU Q. A survey on silicon PUFs and recent advances in ring oscillator PUFs[J]. Journal of Computer Science and Technology, 2014, 29 (4): 664-678.
- [74] GASSEND B. Identification and authentication of integrated circuits: research articles[J]. Concurrency and Computation: Practice & Experience, 2004, 16(11): 1077-1098.
- [75] WU T, GANESAN K, HU Y, et al. TPAD: Hardware Trojan prevention and detection for trusted integrated circuits[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), 2016, 35(4):521-534.

作者简介:



王侃 (1987-), 男, 山东淄博人, 博士, 密码科学技术国家重点实验室工程师, 主要研究方向为芯片物理设计理论与算法、芯片安全性设计、嵌入式系统设计与开发。

陈浩 (1978-), 男, 河南信阳人, 密码科学技术国家重点实验室高级工程师, 主要研究方向为集成电路物理设计、芯片安全性设计。

管旭光 (1983-), 男, 黑龙江鸡西人, 博士, 密码科学技术国家重点实验室工程师, 主要研究方向为芯片设计与实现、芯片安全防护技术、嵌入式系统设计。

顾勇 (1986-), 男, 江苏盐城人, 密码科学技术国家重点实验室工程师, 主要研究方向为数模混合信号电路设计、集成电路物理设计、芯片安全防护技术。