

基于 DCVSL 的硬件木马检测

程 伟,李 磊,成 祥

(电子科技大学 电子科学技术研究院,四川 成都 611731)

摘 要: 针对硬件木马检测问题,分析了 DCVSL(差分串联电压开关逻辑)电路的特性,激活的硬件木马引起 DCVSL 的输入非互补,电路就会产生一个异常的短路电流.在此基础上提出了基于 DCVSL 结构的固有特性,利用电路平均短路电流旁路分析的硬件木马检测方法.通过 HSPICE 蒙特卡罗分析仿真,以 C432 标准电路作为测试电路,植入一个微小的硬件木马,仍然检测出了电路中木马的存在,验证了方法的有效性.

关键词: 硬件木马;旁路分析;差分串联电压开关逻辑;平均短路电流

中图分类号: TN406

文献标识码: A

文章编号: 1000—7180(2017)04—0102—04

Hardware Trojan Detection Based on DCVSL

CHENG Wei, LI Lei, CHENG Xiang

(Research Institute of Electronic Science and Technology, UESTC, Chengdu 611731, China)

Abstract: Aimed at detecting hardware Trojans (HTs), the characteristics of CMOS circuits are analyzed, noncomplementary inputs of DCVSL(Differential Cascade Voltage Switch Logic) caused by the active HT result in abnormal short-circuit current. A hardware Trojan detection method based on inherent feature of DCVSL and average dynamic circuit current is proposed. By HSPICE Mento carlo simulation circuit in which we use a C432 standard circuit with a small hardware Trojan as a test circuit, we detecte the existence of Trojan in the circuit, and verify the validity of the method.

Key words: hardware Trojan; side-channel analysis; differential cascade voltage switch logic; average dynamic circuit

1 引言

集成电路(Integrated Circuit, IC)制造的全球化趋势使 IC 设计与制造相分离,一些不可信的制造商可能对集成电路的原始电路进行恶意篡改,以达到在无条件或在特定的触发条件下实现改变芯片功能,窃取机密信息或者使芯片失效的目的,这些具有恶意功能的冗余电路就是硬件木马(Hardware Trojan).简而言之,硬件木马就是在原始电路中插入的微小的恶意电路.因此,如何检测硬件木马已经成为信息安全领域研究的热点,也是集成电路安全性亟待解决的问题^[1-2].

目前为止,硬件木马检测尚没有形成成熟的行业检测技术,更多的研究还处于实验室阶段,但学术

界已经提出了一些检测方法^[3].现在比较流行的硬件木马检测方法主要有物理检测、功能检测、旁路分析检测等.由于物理检测与功能检测工作量大,成本高等原因而逐渐淡出人们的视野,因此目前对硬件木马检测的研究主要集中在旁路分析技术上^[4-6].旁路分析检测的主要思想是电路被植入硬件木马后,电路中的各种旁路信号(瞬态电流、功率、延时、电磁、热量等)都会受到木马电路的影响从而出现变化,通过收集、测试待测电路的旁路信号,再与原始电路旁路信号进行对比、分析来判断电路中是否存在硬件木马.文献[7-8]利用电路的功耗检测木马;文献[9]研究了电路的门级特性,能够检测出微小的木马.

本文提出了一种在不需要参考电路的情况下检

测微小硬件木马的方法,即利用 DCVSL(Differential Cascade Voltage Switch Logic,差分串联电压开关逻辑)固有的特性,通过 HSPICE 仿真观察电路的短路电流来实现硬件木马的检测.实验仿真结果表明在硬件木马被激活的情况下,电路的短路电流比木马没有被激活时大许多,并且在一段时间内保持一个常数值,通过分析硬件木马激活与未激活时的平均短路电流空间分布图来确定硬件木马的存在,验证了方法的有效性.

2 基于 DCVSL 的硬件木马检测方法

2.1 DCVSL 电路结构概述

DCVSL(Differential Cascade Voltage Switch Logic,差分级联电压开关逻辑)是 IBM 在 1980 年代开发出来的一类新的 CMOS 电路.如图 1 所示,DCVSL 电路中含有两个互补的 nMOS 开关结构,并交叉地连接到一对 pMOS 管的栅极,构成一个有正反馈的差分网络.下拉网络 PDN1 和 PDN2 采用 nMOS 器件互相排斥,当 PDN1 导通时,PDN2 关断;当 PDN1 关断时,PDN2 导通.

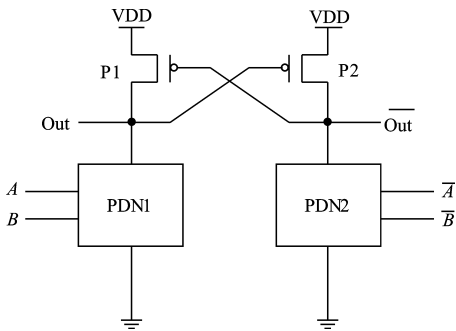


图 1 DCVSL 电路结构

如图 1 所示,每个 DCVSL 门需要互补的输入并产生互补的输出.在正常状态下,DCVSL 门的短路电流与 CMOS 逻辑门的短路电流相当,这个从 VDD 到地的短路电流时间与稳定状态保持时间相比非常短.当输入对是非互补的时候(同时为 0 或者 1),DCVSL 就失去了输出互补的特性,即输出为非互补的,这就导致短路电流持续时间比输入对为互补时要长很多.

以一个 2 输入的 NAND2-AND2 门为例,电路原理图如图 2 所示.在正常状态下,输入 $A=B=C=1$, $\bar{A}=\bar{B}=0$,NAND_OUT 端通过 NMOS 管 N0,N1 被拉低,NAND_OUT 被拉低之后,就会使 PMOS 管 P1 导通,P1 导通后使得 AND_OUT 被拉高,从而导致 P0 关断.因此 PMOS 和 NMOS 同时导通的时间就相

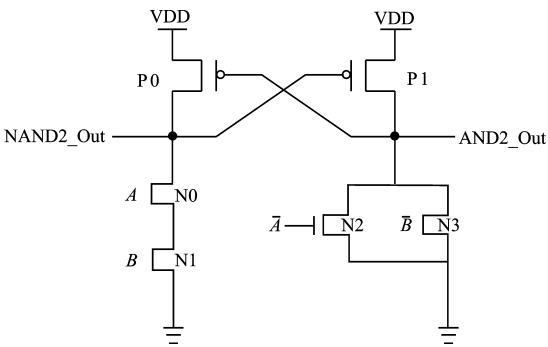


图 2 NAND2-AND2 的电路原理图

当短.当 $A=\bar{A}=1$ 时,这里就存在两条从 VDD 到地的路径:一条是通过 N0 和 N1,另一条是通过 N2.前一条路径使得 NAND_OUT 被拉低,从而 P1 导通,P1 导通将 AND_OUT 被拉高.同时,后一条路径通过 N2 尝试将 AND_OUT 拉低.如果 N2 比 P1 强(通常情况下),AND_OUT 被拉低并使 P0 导通.因此产生一条通过 N0,N1 和 P0 形成的 VDD 到地的导通路径,从而产生了一段较高值的短路电流,其持续时间与输入激励的时间相当.

2.2 短路电流

瞬间短路电流是电路状态转换过程中,电路内部信号电压切换频繁程度的直接表现.电路从当前的稳定状态变化到另一种稳定状态时,由于在不同时刻可能会有不同数量的门电路同时发生变化,因此短路电流的波形大多会出现多个尖峰.把短路电流在一个过渡过程内的平均值称为平均短路电流^[10].图 3、4 所示为 NAND2_AND2 电路分别在输入互补和非互补情况下,经过 HSPICE 仿真得到的电路短路电流波形.从图中可以看出,当 DCVSL 门电路输入互补时,短路电流只有一个尖峰;当输入非互补时,短路电路有一段持续时间,直到输入互补为止.

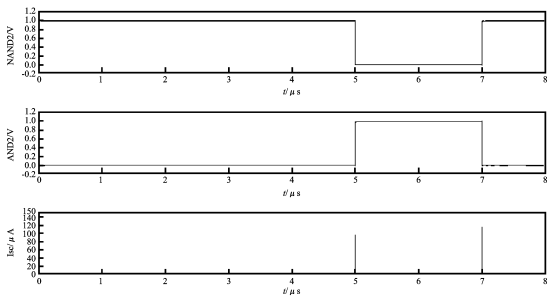


图 3 NAND2_AND2 输入互补时的仿真结果

2.3 检测方法概述

硬件木马的检测主要是在测试阶段,大量的测

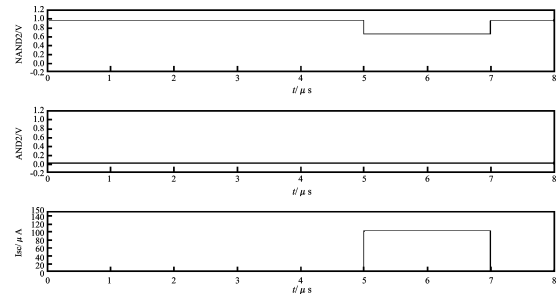


图 4 NAND2_AND2 输入非互补时的仿真结果

试向量被同时施加到待测单元(DUT)和黄金参考模型上. 由于真正干净的黄金参考模型很难得到, 因此常常采用行为模型作为参考. 工艺的偏差和计算机辅助设计工具中不完美的器件库都会导致使用行为模型作为参考的方法在检测小规模和小规模硬件木马电路时不精确. 此外, 为了缩短产品推向市场的时间, 验证和测试周期已经明显被压缩了, 要想完成完整的测试是不可能的任务, 因为这会花费大量的时间和金钱. 因此研究出一种既能不受硬件木马规模影响又不需要耗费很多时间才能执行芯片测试和授权的检测方法势在必行.

本文提出一个可以在测试过程中, 并且无需原始电路参考的硬件木马检测的方法, 此方法利用待测单元出现异常的短路电流来检测硬件木马. 图 5 具体说明了该方法. 与以往的基于功耗分析的木马检测技术最大的不同点在于该方法并不关心某个特定的功率值, 而是观察电流(可以转换成功耗)是否在一个相对长的时间段里保持一个比较大的常数, 如图 5 所示. 本文中使用 DCVSL 结构(产生一对互补的输出)来设计待测单元, 在 DCVSL 结构中, 如前所述, 非互补的输入(由激活的硬件木马引起的)将会导致长时间的短路电流, 直到输入互补为止, 利用 DCVSL 结构固有的这个特性来检测硬件木马的存在. 此外, 除了短路电流检测, 还可以利用 DCVSL 电路互补的输出进一步检测硬件木马, 如果输出是非互补的, 就说明待测电路中存在硬件木马. 因此, 这一对互补的输出可以作为待测电路没有产生异常的电流时检测硬件木马的辅助手段.

3 仿真分析

本文实验选取 ISCAS85 C432 标准电路作为测试电路, 并将其电路中的 CMOS 门电路全部使用 DCVSL 结构的门电路进行替换. 在电路中嵌入了一个 3 输入的 CMOS 与非门作为木马触发电路, 2 输入的 CMOS 异或门作为木马电路的载荷. 可以看

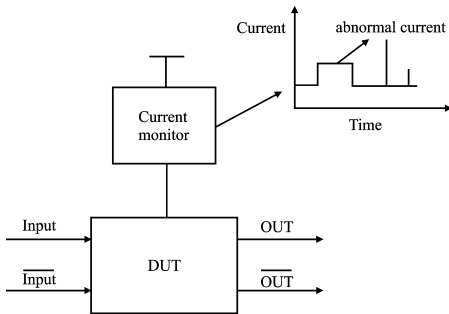


图 5 硬件木马检测方法

出, 其中木马电路只占了待测电路很小的一部分. 采用 SIMC90 nm 的工艺库提供的 HSPICE 器件模型对电路进行仿真. 然后通过 HSPICE 提供的函数计算在某个时间段内短路电流的平均值, 函数表达式如下:

$$AVG(I_{DDT}(t), T) = \int_{T_1}^{T_2} I_{DDT}(t) dt / (T_2 - T_1)$$

蒙特卡罗分析能模拟工艺噪声、随机噪声等因素对电路或器件的影响. 因此, 采用固定测试向量对 C432 电路在木马未激活和激活两种情况下分别进行 30 次蒙特卡罗分析. 通过计算平均短路电流构建出木马未激活和激活两种情况下的空间分布图, 其仿真结果如图 6 所示.

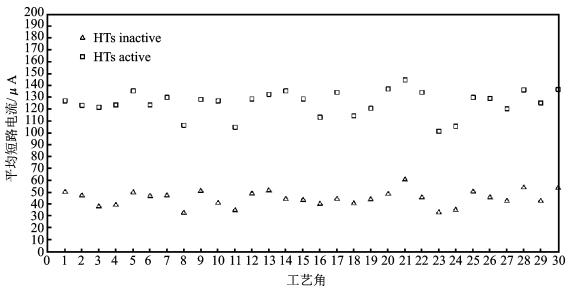


图 6 硬件木马激活和未激活条件下的蒙特卡罗仿真结果

从图 6 中可以看出由于工艺噪声的影响, 每次仿真得到的平均短路电流存在一定的随机误差. 虽然加入了工艺噪声的影响, 但是木马在激活和没有激活的情况下, 其平均电流的空间分布图仍然具有良好的分离度, 从而可以判断出电路中木马电路的存在. 因此利用 DCVSL 结构固有的特性可以有效地检测出电路中的硬件木马.

4 结束语

集成电路的发展和广泛使用, 使其安全性受到硬件木马的挑战. 为了提高集成电路的安全性, 对硬件木马检测技术的研究变得日趋重要. 本文提出了一种在测试阶段, 不需要模型参考和大量测试向量

的情况下,利用 DCVSL 结构本身的一些特性来检测硬件木马的方法.选取 ISCAS85 C432 标准电路作为测试电路,分别在硬件木马触发和未触发条件下,通过 HSPICE 对电路进行蒙特卡罗分析仿真,通过测量电路的平均短路电流来检测硬件木马的存在,验证了该方法的可行性,并且对使用 DCVSL 结构来设计电路检测硬件木马具有一定的实际参考价值.

参考文献:

[1] 刘华锋,罗宏伟,王力伟. 硬件木马综述[J]. 微电子学, 2011, 41(5):709-713.

[2] 倪林,李少青,马瑞聪,等. 硬件木马检测与防护[J]. 数字通信, 2014, 41(1):59-63 .

[3] 陈华锋,瞿有甜,姜燕冰. 硬件木马电路检测技术与发展趋势 [J]. 浙江大学学报(理学版), 2014, 41(1): 49-51.

[4] 赵崇征,邓高明,赵强. 基于旁路分析的集成电路芯片硬件木马检测[J]. 微电子学与计算机, 2011, 28(11): 5-9.

[5] 刘长龙,赵毅强,史亚峰,等. 基于侧信道分析的硬件木马建模与优化[J]. 华中科技大学学报(自然科学版), 2013, 41(2):53-57.

[6] Ni Lin, Li Shaoqing, Chen Jihua, et al. The influence on sensitivity of hardware Trojans detection by test vector[C]//Proceeding of 2014 Communications Security Conference(CSC2014). Beijing: [s. n.], 2014: 46 - 51.

[7] 赵志勋,倪琳,李少青. 硬件木马电路功耗的检测方法 [J]. 北京邮电大学学报, 2015, 38(4):128-132.

[8] 倪琳,李少青,赵志勋. 工艺偏差下基于功耗与延时的硬件木马检测有效性分析[J]. 数字通信, 2014, 41(5): 36-41.

[9] Wei S, Potkonjak M. Gate-level characterization: foundations and hardware security applications[C]//DAC . IEEE, 2010:483 -486.

[10] 李雄伟,王晓晗,张阳,等. 基于多旁路综合分析的硬件木马检测方法[J]. 计算机仿真, 2015, 32(3):216-219.

作者简介:

程 伟 男,(1987-),硕士研究生. 研究方向为微电子与固体电子. E-mail:380176931@qq. com.

李 磊 男,(1982-),研究员. 研究方向为专用集成电路 (ASIC).

成 祥 男,(1989-),硕士研究生. 研究方向为 EDA.

(上接第 101 页)

[4] 李涛,杨婷,易学渊,等. 萤火虫 2:一种多态并行机的硬件体系结构[J]. 计算机工程与科学, 2014, 36(2): 191-200.

[5] 韩俊刚,姚静,李涛,等. 多态并行机上的 3D 图像渲染[J]. 西安邮电大学学报, 2015, 20(2):1-6.

[6] 肖灵芝. GPU 存储管理系统的设计与实现[D]. 西安:西安邮电大学, 2013.

[7] 胡伟武. 计算机体系结构[M]. 北京:清华大学出版社, 2011.

作者简介:

杨 铮 男,(1990-),硕士研究生. 研究方向为软件工程. E-mail:yangzheng9004@163. com.

韩俊刚 男,(1943-),教授. 研究方向为软件和硬件形式化验证、图像处理器和计算机体系结构.

刘 欢 男,(1991-),硕士研究生. 研究方向为计算机系统结构.

李卯良 男,(1991-),硕士研究生. 研究方向为电路与系统.