

基于基准曲线的硬件木马检测技术研究

王 林^{1,2}, 魏敬和², 周 昱²

(1 江南大学 物联网工程学院, 江苏 无锡 214122; 2 中国科技集团第 58 研究所, 江苏 无锡 2014072)

摘 要: 目前硬件木马的检测方法主要有逻辑测试和旁道参数分析法, 然而在木马面积较小并且存在较大的工艺漂移的情况下, 这两种方法的检测覆盖率并不高. 对此利用电路自身的动态电流(I_{delt})和最高频率(f_{max})之间的固有关系构造出一条基准曲线, 将实测曲线与基准曲线进行对比来检测硬件木马. 前期利用 Synopsys 工具对理论进行仿真验证, 然后设计专用 PCB 测试板, 选取合适的测量设备和 FPGA 芯片搭建测试系统进行实测. 实测结果表明, 该测试系统可以有效地降低工艺漂移对检测结果的影响, 并且可以较好地提高硬件木马的检测精度.

关键词: 硬件木马; 基准曲线; 工艺漂移; 专用 PCB; 测试系统

中图分类号: TP393

文献标识码: A

文章编号: 1000—7180(2017)03—0082—04

The Study of Hardware Trojan Detection Based on Reference Curve

WANG Lin^{1,2}, WEI Jing-he², ZHOU Yu²

(1 School of IOT Engineering, Jiangnan University, Wuxi 214122, China;

2 No. 58 Research Institute, China Electronics Technology Group Corporation, Wuxi 2014072, China)

Abstract: Currently the main detection approaches to the Hardware Trojan are logical test and side-channel analysis, however, these methods suffers from decreased sensitivity toward small Trojans and large process variation. In this paper, we take advantage of the intrinsic relationship between dynamic current and maximum operation frequency of the circuit to formulate a reference curve, then compare the measured curve with the reference curve to detect the Hardware Trojan. At the beginning we use the Synopsys tool to validate the theory, then design specified PCB test board, choose the appropriate measure device and FPGA to set up the test system. The test result shows that this system can reduce the influence of the process variation on the detect result efficiently and improve the detection accuracy.

Key words: hardware trojan; reference curve; process variation; specified PCB; test system

1 引言

随着集成电路设计的日益复杂, 制造成本日趋高昂, 集成电路产业正在朝着全球化合作的趋势发展^[1]. 迫使很多集成电路厂商不得不放弃对整条产业链的掌控, 将一些中间环节外包给第三方厂商. 而这也使得集成电路容易被人植入硬件木马, 在实际使用过程中会受到攻击.

硬件木马指攻击者在设计或者制造阶段对原有的设计电路所进行的恶意篡改^[2]. 它可能会引起某些区域的电路失效, 降低芯片的可靠性, 也可能泄露

芯片内部的敏感信息如密钥等, 更有甚者当系统达到某个预先设定的状态时摧毁整块芯片. 与制造缺陷不同, 硬件木马由于其本身的多样性和隐蔽性, 传统的 VLSI 测试方法很难检测到它的存在. 硬件木马可以在从设计到制造的任何阶段中植入. 为攻击者在芯片制造阶段植入硬件木马提供了绝佳机会.

近几年来, 人们对硬件木马进行了大量研究, 提出了一些流片后测试硬件木马检测方法, 大致可以将其分为两种. (1) 逻辑测试法^[3]. 传统的结构和功能测试目的在于功能验证和故障覆盖率, 并不适用于硬件木马的检测. (2) 旁道参数分析法^[4]. 这种方

法也存在不足之处,当工艺进入深亚微米级的时候,工艺变量的增多会加大工艺漂移对测试结果的影响,造成木马检测精度下降.因此如何校准工艺漂移,提高木马的检测精度成为一个亟待解决的问题.

本文通过在原始电路中插入环形振荡器电路来校准工艺漂移,利用原始芯片自身的动态电流(I_{ddt})和最高频率(F_{max})之间的固有关系构造出一条基准曲线,通过检测待测芯片绘制出实测曲线,并将实测曲线与基准曲线进行对比来检测木马的存在.

2 理论分析

对于一个门电路,其动态电流可以表示为^[5]

$$I_g = k_g (V_{\text{DD}} - V_{\text{th}})^\alpha \quad (1)$$

式中, V_{DD} 是电压, α 是值在1-2之间速率饱和指数, V_{th} 是阈值电压, k_g 是栅常数.其中 V_{th} 可以由表示成归一化的阈值电压 V_{T} 与晶圆间的工艺漂移 ΔV_{Ti} ,以及随机漂移数 ΔV_{Tg} ,因此式(1)可以表示为

$$I_g = k_g (V_{\text{DD}} - V_{\text{T}} - V_{\text{Ti}})^\alpha \cdot \left[1 - \frac{\Delta V_{\text{Tg}}}{V_{\text{DD}} - V_{\text{T}} - V_{\text{Ti}}}\right]^\alpha \quad (2)$$

将上述公式展开,并忽略高阶项,假设

$$\frac{\Delta V_{\text{Tg}}}{V_{\text{DD}} - V_{\text{T}} - \Delta V_{\text{Ti}}} \ll 1, \text{ 上述式(2)又可以表示为:}$$

$$I_g \approx (V_{\text{DD}} - V_{\text{T}} - \Delta V_{\text{Ti}})^\alpha [k_g - C_i \cdot k_g \cdot \Delta V_{\text{Tg}}] \quad (3)$$

式中, $C_i = \frac{\alpha}{V_{\text{DD}} - V_{\text{T}} - \Delta V_{\text{Ti}}}$ 是对当前考虑的晶体管来说是一个常数,把每一个门的电流都加起来后,就得到:

$$I_{\text{ddt},i} = \sum_{g \in IC_i} I_g \approx (V_{\text{DD}} - V_{\text{T}} - \Delta V_{\text{Ti}})^\alpha \left[k_{\text{av}} n_{\text{tot},i} - C_i \sum_{g \in IC_i} k_g \cdot \Delta V_{\text{Tg}} \right] \quad (4)$$

式中, $k_{\text{av}} n_{\text{tot},i} = \sum_{g \in IC_i} k_g$, $n_{\text{tot},i}$ 是所有正在翻转的门的数量, $\sum_{g \in IC_i} k_g \cdot \Delta V_{\text{Tg}}$ 是几个随机数的和,且每个随机数的平均值为0.所以上述式(4)又可以表达为

$$I_{\text{ddt},i} \approx k_{\text{av}} n_{\text{tot},i} \cdot (V_{\text{DD}} - V_{\text{T}} - \Delta V_{\text{Ti}})^\alpha \quad (5)$$

此外,每个门的延时可以用式(6)来表达:

$$t_d = \beta_g (V_{\text{DD}} - V_{\text{th}})^{-\alpha} \quad (6)$$

式中, β_g 是另一种栅常数,将式(6)用之前的方法近似等效得到式(7):

$$t_d \approx \beta_g (V_{\text{DD}} - V_{\text{T}} - \Delta V_{\text{Ti}})^{-\alpha} [\beta_g + \beta_g C_i \Delta V_{\text{Tg}}] \quad (7)$$

将关键路径上的每个门的延迟相加得到:

$$T_{\text{crit},i} = \sum_{g \in P_{\text{crit},i}} t_d \approx \beta_{\text{av}} \cdot n_{\text{crit},i} \cdot (V_{\text{DD}} - V_{\text{T}} - \Delta V_{\text{Ti}})^{-\alpha} \quad (8)$$

因此其最大频率可以表示为

$$f_{\text{max},i} = \frac{1}{T_{\text{crit},i}} \approx \frac{1}{\beta_{\text{av}} \cdot n_{\text{crit},i}} \cdot (V_{\text{DD}} - V_{\text{T}} - \Delta V_{\text{Ti}})^\alpha \quad (9)$$

根据式(5)和式(9),动态电流与频率的关系可以表达为

$$\frac{I_{\text{ddt},i}}{f_{\text{max},i}} \approx k_{\text{av}} \cdot \beta_{\text{av}} \cdot n_{\text{crit},i} \cdot n_{\text{tot},i} \quad (10)$$

通过式(10)我们看出,动态电流与最大工作频率之间的关系即使在不同的工艺漂移下,在基于一阶等效定理的前提下是接近线性关系的.同理,当电路内被植入硬件木马后,其电流与频率的关系可以表达成:

$$\frac{I_{\text{ddt},i,\text{trojan}}}{f_{\text{max},i}} \approx k_{\text{av}} \cdot \beta_{\text{av}} \cdot n_{\text{crit},i} \cdot (n_{\text{tot},i} + n_{\text{trojan},i}) \quad (11)$$

从式(11)可以看出,即使电路被植入硬件木马以后,动态电流与最大频率之间的关系并没有改变,改变的只是该曲线的截距.

3 EDA 仿真测试

3.1 木马模型

仿真测试电路为128位AES加密电路,木马选用时序型计数器木马——“时间炸弹”.时序型木马只有在出现某一个特定的序列或者周期性的连续操作时才会触发.最简单的时序型木马是同步计数器,当计数器到达一个特定值的时候就会触发木马.图1所示为一个同步K位计数器,当计数器的值为 $2^k - 1$ 时木马触发,将信号ER的值改为 ER^* .

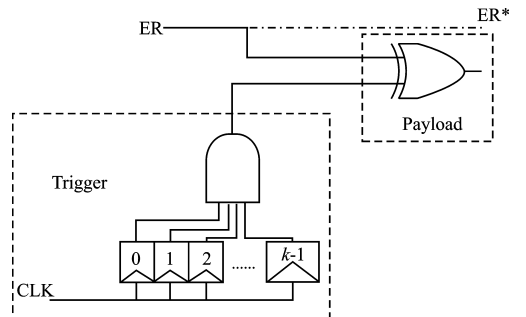


图1 时序型计数器木马——“时间炸弹”

3.2 环形振荡器电路

测试中用于校准工艺漂移的环形振荡器电路结

构如图 2 所示^[7],它由 16 个反相器和一个 2 输入与非门构成. 当 en 信号为 1 时振荡器起振,输出 q 端的信号会在 0 和 1 之间不断跳变,当检测到 q 的上升沿时,外部计数器 1 的值加 1. 外部计数器 2 检测时钟信号的上升沿,当检测到上升沿时计数器的值加 1. 最后在某个时刻将两个计数器的值读取出来进行运算得出 $f_{\max}$.

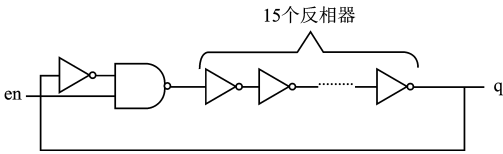


图 2 环形振荡器

3.3 EDA 仿真流程及测试结果

仿真选取的木马类型为“时间炸弹”,根据图 3 所示的仿真流程,有无木马的 AES 电路经过 P&R 后的版图如图 4 所示,图(b)中白色圆圈所表示的部分即植入的硬件木马,其面积约占整体面积的 2.84%. 将 AES 电路分别在 SMIC55 nm 和 180 nm 工艺下进行了仿真测试. 通过在 Hsim 中进行蒙特卡洛仿真来模拟工艺漂移,最后测量结果如图 5、图 6 所示,其中标记为 Golden 和 Trojan 的曲线分别代表 AES 电路和植入木马的 AES 电路. 由于 SMIC 0.18 μm 单元库在建模的时候只考虑了晶圆间(die-to-die)的工艺漂移影响,但对于更小尺寸的工艺如 55 nm 而言,工艺漂移不仅存在于晶圆间,也存在于晶圆内部各管子之间(within-die),且同一晶圆内部各管子之间的工艺漂移往往大于晶圆之间. 所以从图 5 中可以看出,55 nm 工艺下同一最大频率所对应的电流值会有一个较小的波动,但总体而言动态电流(I_{ddt})和频率($f_{\max}$)依然呈现出线性关系,与公式的推导结果一致.

4 测试系统设计与实测结果分析

4.1 测试系统设计

测试系统示意图如图 7 所示,由 PC、源表和 PCB 测试板组成. 为了解决能够单独测试 FPGA 消耗电流的问题,在设计 PCB 测试板时设计了两个电源系统, V_{cc} 作为整个测试板的输入电压为 5 V,通过电源适配器供给电压. 然后通过电源芯片将输入电压分为 V_{ccint} , V_{ccaux} 和 V_{cco} 分别给 FPGA 和外设供电,在测试板上做了一些拨码开关来控制各路电压的关断和开启. 在测试 FPGA 内核电压时将其其他外设全部关断,可以提高测量的精度. 测量仪器选用

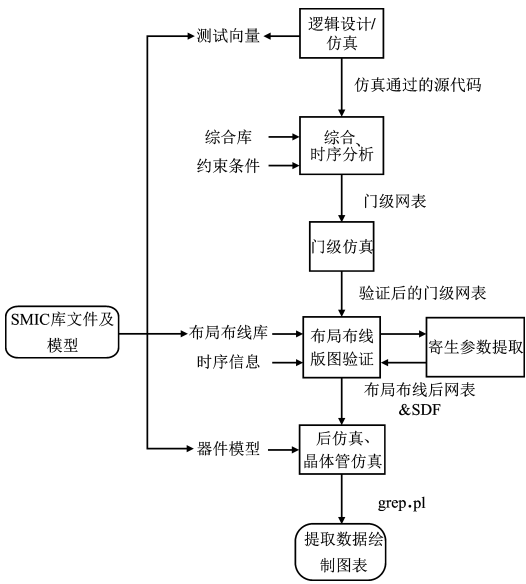
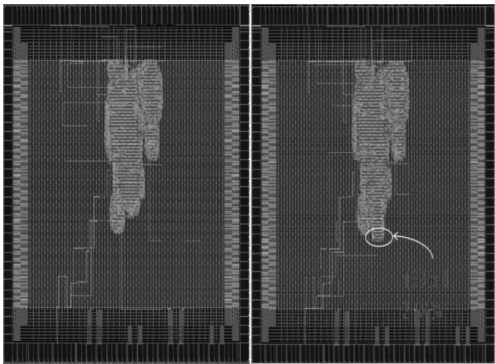


图 3 EDA 仿真流程



(a) 无木马电路 (b) 有木马电路

图 4 电路版图设计

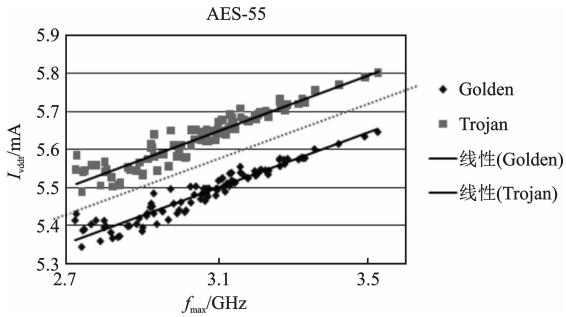


图 5 55 nm 有无木马的 AES 电路的动态电流与最高工作频率的关系

Keithley 公司的源表 2634B,其测量精度可达到 fA 级别. 源表既可以当成激励源来使用,又可以当成测量表使用. 在该测试系统中源表被作为电流表来使用,将源表串入电路中,与待测电路构成回路. 源表通过 LAN 口与 PC 相连进行通信,利用其配套软件 TSB 编写测试脚本来控制整个测试流程. 测试所用的 FPGA 芯片为 Spartan 6 XC6SLX45,封装型号

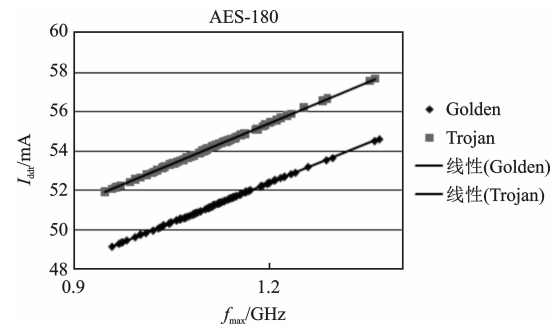


图 6 180 nm 有无木马的 AES 电路的动态电流与最高频率的关系

CSG324, 制造工艺为 45 nm 的 CMOS 工艺. ISE 通过 JTAG 口将 AES 电路程序烧写进 FPGA, 同时通过 ISE 自带的 chipscope 插件来读取环振计数中的值, 测试系统的实物图如图 8 所示.

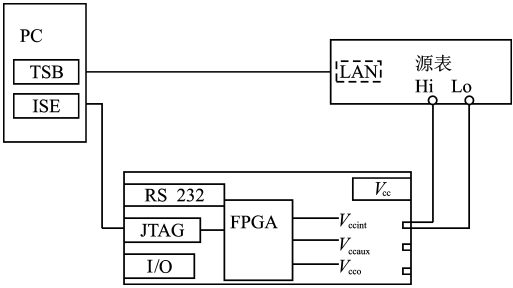


图 7 硬件木马测试系统示意图

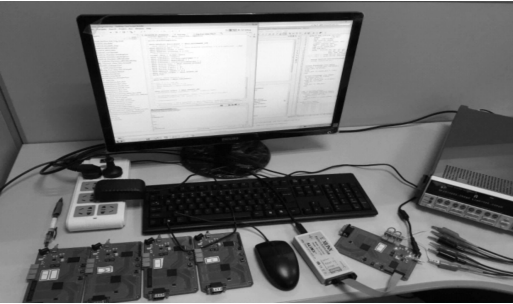


图 8 硬件木马测试系统实物图

4.2 实测结果分析

在 ISE 环境下, 分别将 AES 电路和植入硬件木马的 AES 电路进行综合、布局布线及生成 bit 文件的过程中, 为了保证用于校准工艺漂移的环形振荡器电路的有效性, 需要将其进行手动布局布线, 以保证其各路走线的一致. 如果选择系统自动布局布线, 环振电路将无法发挥校准工艺漂移的作用. 我们选取了 7 块型号相同的 FPGA 芯片进行测试, 测试结果如图 9 所示. 其中(a)、(b)分别表示自动布局布线和手动布局布线时不同芯片中环振电路所测到的最

高频率值. 从图 9(a)中可以看出对于某些 FPGA 芯片, 同一块芯片中无木马电路和有木马电路所测量到的环振的最高频率值会有较大的差异, 这主要是因为原始电路中植入硬件木马后, 植入的木马会改变原始电路的布局布线, 使得两次环振电路的布局布线出现差异, 从而导致同一芯片所测到的环振电路的最高频率值出现较大偏差. 将环振电路进行手动布局布线后, 可以保证其不会受到植入的硬件木马的影响, 测量结果如图 9(b)所示, 从图中可以看出, 对于同一块芯片而言, 其测到的环振电路的最大频率值是相同的. 最终动态电流和最高频率的实测结果如图 10 所示, 从图中可以看出芯片的动态电流和最高频率保持了较好的线性关系, 与理论推导和仿真结果一致, 有无木马的测试芯片也可以较好地区分开来. 其中植入 AES 电路的硬件木马面积约占芯片整体面积的 2.84%, 其产生的额外电流约为 5%.

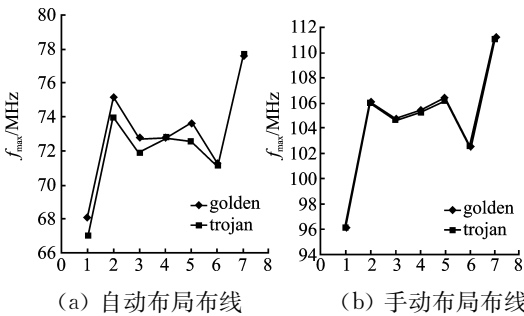


图 9 不同布局布线方式下环振电路的最高频率

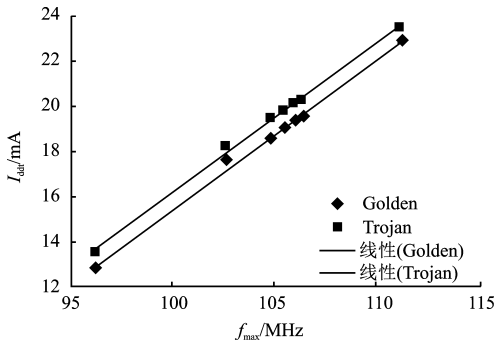


图 10 实测结果

5 结束语

本文根据芯片自身的动态电流与最大频率之间的固有关系, 利用环形振荡器来校准工艺漂移以去除工艺漂移对测量结果的影响, 并且通过搭建测试系统来验证方案的可行性. 根据实测结果表明, 该测试系统可以较好地克服工艺漂移的影响, 提高硬件木马的检测精度.

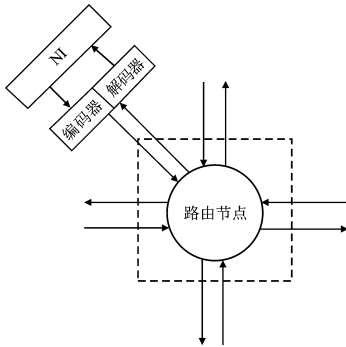


图 3 一次编码一次解码结构

中的开关功耗作为优化对象. 针对电路中信号的自翻转,选择互连线翻转编码来降低数据的翻转率,采用分组编码的方式,将原始的 32 bit 数据分为四组分别编码,并且不需要再额外添加冗余标志位. 同时引入格雷码对数据包中的数据包计数器和微片计数器编码. 实验结果表明,这种联合编码的方式可以有效降低 NoC 的功耗.

参考文献:

[1] Dally William J, Towles Brian. Route packets, not wires: on-chip inteconnection networks[C]// Design Automation Conference. ACM, 2001:684-689.

(上接第 85 页)

参考文献:

[1] 刘华峰, 罗宏伟, 王立纬, 硬件木马综述 [J]. 微电子学, 2011, 31(5): 709-713.

[2] Tehranipoor M, Salmani H, Zhang X, et al. Trust-worthy hardware: Trojan detection and design-for-trust challenges[J]. Computer, 2011, 44(7): 66-74.

[3] Seethram Narasimhan, Somnath Paul, Kaushilk Roy. Hardware Trojan detection by multiple-parameter side-channel analysis [J]. IEEE Transaction on Computers, 2013, 62(11): 2183-2195.

[4] Yier J, Makris Y. Hardware Trojans in wireless cryptographic ICs[J]. IEEE Design & Test of Computers, 2010, 27(1): 26-35.

[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

[2] Lee K, Lee S J, Yoo H J. SILENT: serialized low energy transmission coding for on-chip interconnection networks[C]// Computer-Aided Design, International Conference on. IEEE, 2004:448-451.

[3] Du G, Li M, Lu Z, et al. An analytical model for worst-case reorder buffer size of multi-path minimal routing NoCs[C]// Networks-on-Chip (NoCS), 2014 Eighth IEEE/ACM International Symposium on. IEEE, 2015:49-56.

[4] Stan M R, Burleson W P. Bus-invert coding for low-power I/O[J]. IEEE Transactions on Very Large Scale Integration Systems, 1995, 3(1):49-58.

作者简介:

杜高明 男, (1977-), 博士, 副研究员. 研究方向为多核集成电路体系结构、二维/三维片上网络集成体系结构.

李向阳(通讯作者) 男, (1977-), 硕士研究生. 研究方向为片上网络性能. E-mail: 597042025@qq. com.

马世碧 女, (1992-), 硕士研究生. 研究方向为片上网络体系结构.

宋宇鲲 男, (1975-), 博士, 副研究员. 研究方向为面向数据密集与计算机密集应用的 SoC/MPSoC 体系结构与实现.

张多利 男, (1976-), 博士, 研究员. 研究方向为多核处理器体系结构与设计方法、多媒体专用集成电路设计实现等.

版), 2013, 41(2): 53-57.

[6] Baumgarten A, Steffen M, Clausman M, et al. A case study in hardware Trojan design and implementation [J]. International Journal of Information Security, 2011, 10(1): 1-14.

[7] Rad R, Plusquellic J, Tehranipoor M. A sensitivity analysis of power signal methods for detecting hardware Trojans under real process and environmental conditions[J]. IEEE Transactions on Very Large Scale Integration Systems, 2010, 18(12): 1735-1744.

作者简介:

王 林 男(仡佬族), (1991-), 硕士. 研究方向为数字集成电路设计和测试.

魏敬和(通讯作者) 男, (1975-), 博士. 研究方向为大规模数字集成电路设计与测试. E-mail: 920770745@qq. com.