

一种木马电路的实现与特征分析

郑朝霞, 韩 玲, 李 阳, 邹雪城

(华中科技大学 电子科学与技术系, 湖北 武汉 430074)

摘 要: 由于硬件木马等恶意电路的隐蔽性, 攻击者可以利用其窃取机密信息, 破坏硬件电路, 造成严重的经济损失与社会危害. 本文基于典型的芯片设计流程与 EDA 工具, 首先建立硬件木马的电路模型, 然后尝试在一简单 ADC 芯片中, 利用其电路的剩余空间, 设计实现了一种计数器木马电路. 该木马电路的规模大约占芯片总面积的 5.6%, 将受污染的电路与真实电路一起用标准 CMOS 工艺 HJ0.25 μm 流片, 然后采用旁路功耗分析技术进行深入分析. 实验数据表明, 在正常工作情况下, 受污染和没受污染的芯片功耗并无明显差异, 而当木马触发条件满足时, 受污染的芯片却成功的实现了攻击.

关键词: 芯片安全; 恶意电路; 硬件木马; 计数器

中图分类号: TN452

文献标识码: A

文章编号: 1000-7180(2012)10-0078-03

The Implementation and Analysis of a Trojan Circuit in IC Chips

ZHENG Zhao-xia, HAN Ling, LI Yang, ZOU Xue-cheng

(Department of Electronic Science & Technology, Huazhong University of Science & Technology, Wuhan 430074, China)

Abstract: Hidden Trojan circuits provide an attacker with a stealthy attack vector. Trojan circuits can bypass traditional defensive techniques as they occupy a layer below the entire software stack. We present the design and implementation of a counter Trojan circuits into a IC chip by standard CMOS technology HJ0.25 μm , then we analyze such flexible hardware allows powerful, general purpose attacks, while remaining surprisingly low in the amount of additional hardware.

Key words: ICs security; malicious hardware; trojan circuits; counter

1 引言

由于集成电路芯片规模迅猛激增, 为了缩短研发周期, 集成电路行业多购买第三方 IP 核, 或者采用自动布局布线工具. 这些工具并非理想, 使得芯片中有大量剩余空间, 攻击者可能在制造环节中, 向芯片的电路注入带有特定恶意目的的“硬件木马”电路. 集成电路芯片已广泛应用于国民经济的各个领域, 一旦出现“硬件木马”攻击, 将会带来严重后果. 近年来, “硬件木马”引起了世界各国工业界和学术界的极大关注, 很多国外大学和科研机构均就这一领域展开了研究, 并取得一些研究成果^[1].

本文针对一款真实的芯片电路, 成功在其中植入了一块隐蔽的恶意电路, 然后深入分析了硬件木马的植入对原始电路旁路参数特性的影响^[2], 以期了解更多硬件木马特性, 便于后续就硬件木马侦测技术研究工作的开展.

2 硬件木马电路模型建立

硬件电路是指注入带有特定恶意目的硬件电路. 硬件木马攻击的出现对半导体芯片的安全提出了极大的挑战. 硬件木马电路是整个硬件木马攻击的关键部件. 根据攻击者的要求, 硬件木马电路需要寄生在某一正常的功能电路之中, 成为该电路的旁路分支, 其模型如图 1 所示. 硬件木马攻击包括木马

收稿日期: 2012-02-28; 修回日期: 2012-03-28

基金项目: 国家自然科学基金项目(NSFC 61006020); 湖北省自然科学基金项目(2010CBD02705); 中央高校基本科研业务费专项资金(2011TS109)

注入、监听触发以及木马发作三个步骤:首先,攻击者需要在 Foundry 厂制造之前,将硬件木马电路注入到正常的功能电路中;待芯片投入使用后,硬件木马电路监听芯片功能电路中的特定信号;当特定信号达到某些条件后,硬件木马电路被触发,木马电路完成攻击者所期望的恶意攻击行为^[3]。

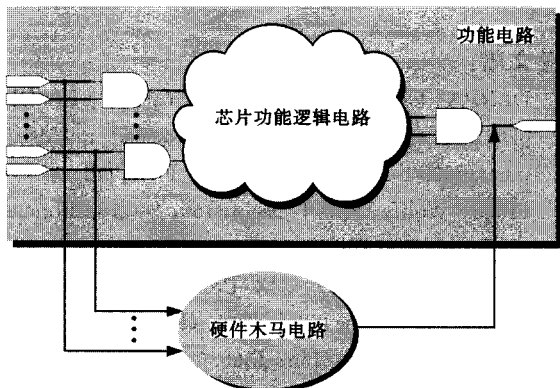


图1 硬件木马模型

硬件木马电路主要包括触发部分和负载两部分^[4-5]。负载通常有以下三类型功能:①把内部敏感信息(如明文、密钥)传输给攻击者;②修改电路功能,如用密钥代替输出密文;③毁坏芯片。对于触发机制,一般有如下三种:①攻击者可以接近加密芯片并且直接输入木马预设值来触发木马;②木马被内部条件触发,针对那些不能物理接近加密系芯片的攻击者。如在含有 GPRS 导航的系统中,可以设定某一确定坐标值为触发条件;③木马一直是激活的。

3 硬件木马电路设计

根据硬件木马的触发机制,重点研究了计数器型木马,其功能类似于定时炸弹,结构如2所示。一般情况下,木马电路并不影响信号 ER 的正常输出,但是当计数到 2^k-1 时,木马被触发,改变信号 ER,让其输出错误值 ER*。

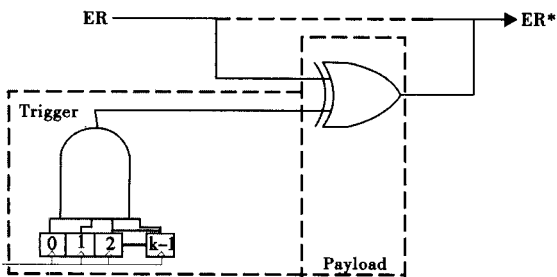


图2 计数器型木马结构

计数器木马具体电路设计如图3所示。采用十

位计数器,每输出一个被监测的数据,计数器的值就会自增一,直到到达预设值 N,木马即会被触发,输出值将被锁存 1。为了避免在设计者的功能测试环节木马即被触发,预设值 N 要尽可能的大。该木马电路采用 10 位计数器,只有当检测到输出为指定值“10'b1111111111”的时候,木马被触发,电路输出值被锁存为 1。

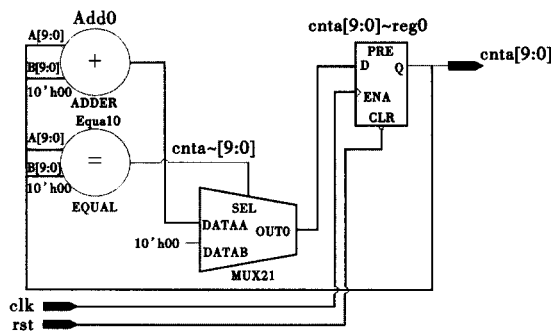


图3 10位计数器木马电路

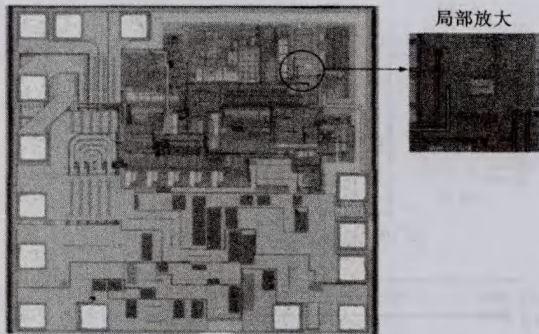
然后,设计一简单 ADC 芯片,该芯片电路规模相当于 4302 个 2 输入与非门。将该计数器木马的电路注入到该芯片版图右上角的空闲位置。硬件木马的电路规模很小,大约是芯片总面积的 5.6%,相当于 247 个 2 输入与非门。如果采用其它例如简单组合逻辑电路的木马,木马的规模还可以更小,甚至可以达到主体电路面积的 0.01%。最后受木马污染的电路和没受污染的原始电路均采用标准 CMOS 工艺 HJ0.25 μ m 流片,从晶圆切割下来的 die(即裸片)如图4所示。没受木马污染的裸片如图4(a)所示,放大其右上角,可以看到,该位置的未用空间没被其它电路填充;被硬件木马污染了的裸片如图4(b)所示,放大其右上角,可以看到,该位置的未用空间已经被计数器木马电路填充^[6]。

对原始裸片和被木马污染的裸片完成封装后,原始芯片和植有硬件木马的芯片从外观上看,一模一样,无法通过肉眼分别哪块芯片里面有木马。

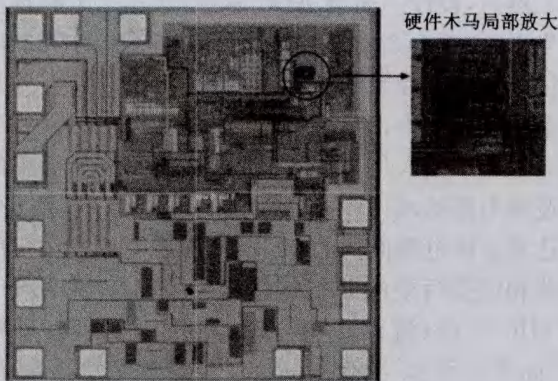
4 硬件木马攻击实验与分析

基于旁路分析的方法,对这种芯片进行旁路功耗分析,电路的时钟频率从 200MHz 逐级降低,实验分析数据如表1所示。可以看到,当时钟信号为 100MHz 时,从功耗上很难区分有木马的受污染电路和没有木马的原始电路。当时钟频率降为 10MHz 时,依然很难从功耗的差别上区分是否被插入木马电路。时钟频率降为 100 kHz 时,它们之间的功耗差异依然不明显。当木马电路相对整个芯片而言面

积较大,而工艺偏差较小时,用简单的功耗分析方法检测木马较为有效^[8].但是在复杂电路设计中,由于木马所占面积比较少,再加上深亚微米工艺偏差,原始电路的工艺偏差就可以大至 $\pm 7.5\%$,导致木马电路的功耗与整个芯片的功耗相比微不足道,简单的旁路信息分析法,在复杂电路如超大规模电路中不足以实现对硬件木马的检测.



(a) 无硬件木马的芯片



(b) 被植入硬件木马的芯片

图4 芯片裸片

表1 真实芯片与受木马污染芯片不同时钟频率下功耗分析

	真实芯片	受木马污染芯片
电路规模(门)	4302	4549
功耗(mW)		
f=100 MHz	403	402
功耗(mW)		
f=10 MHz	0.4	0.4
功耗(mW)		
f=100 kHz	0.004	0.005

5 结束语

本文设计了一种规模适中的计数器木马电路.将它植入在一个真实 IC 芯片中,当满足触发条件时,木马电路完成攻击者预设的功能,成功干扰了芯片中的时钟信号.

参考文献:

- [1] DARPA TRUST program information [EB/OL]. [2011-11-19]. http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf.
- [2] Francis Wolff, Chris Papachristou, Swarup Bhunia, et al. Towards trojan-free trusted ics: problem analysis and detection scheme [C]// Proc. Design, Automation and Test in Europe Conf. 2008. (DATE'08). Germany, Munich, 2008; 1362-1365.
- [3] Samuel T King, Joseph Tucek, Anthony Cozzie, et al. Designing and implementing malicious [C]// hardware. Proc. 1st USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET 08). USA, Berkeley, 2008; 1-8.
- [4] Yousra Alkabani, Farinaz Koushanfar. Extended abstract: designer's hardware trojan horse [C]// IEEE International Workshop on Hardware-Oriented Security and Trust 2008 (HOST' 08). USA, Anaheim: IEEE CS Press, 2008; 82-83.
- [5] Yier Jin, Nathan Kupp, Yiorgos Makris. Experiences in Hardware Trojan Design and Implementation [C]// 2nd IEEE In. Workshop on Hardware-Oriented Security and Trust (HOST' 09). USA; San Francisco, IEEE CS Press, 2009; 50-57.
- [6] Shiyankovskii Y, Wolff F, Papachristou C, et al. Hardware trojan by hot carrier injection [C]// CoRR2009. USA; San Francisco, 265-276.
- [7] 邓秋成,白雪飞,郭立. ECC 密码算法的差分功耗分析攻击研究 [J]. 微电子学与计算机, 2011, 28(2): 3-5.
- [8] 李浪,焦铭,李仁发,等. 一种 ECC 加密芯片抗功耗攻击研究 [J]. 微电子学与计算机, 2011, 28(1): 2-6.

作者简介:

郑朝霞 女, (1975—), 博士, 讲师. 研究方向为超大规模数字集成电路设计、嵌入式及其安全性研究.