

doi:10.3969/j.issn.1007-7162.2013.04.012

电磁泄漏型硬件木马设计与检测

谢海^{1,2}, 恩云飞², 王力伟²

(1. 广东工业大学 材料与能源学院, 广东 广州 510006;
2. 工业和信息化部电子第五研究所 电子元器件可靠性物理及其应用技术重点实验室, 广东 广州 510610)

摘要: 针对集成电路在设计或制造过程中容易受到硬件木马的攻击, 从而威胁芯片与硬件安全性的问题, 介绍了硬件木马的基本原理及其分类方法, 在此基础上设计了一种电磁泄漏型硬件木马, 该木马电路能通过电磁发射的方式泄漏密码芯片的密钥. 搭建了基于现场可编程门电路 FPGA 的 AES(Advanced Encryption Standard)加密电路测试平台, 利用旁路分析的方法, 对该种结构类型的硬件木马电路进行了检测与分析. 实验结果表明: 该硬件木马电路能在使用者毫不知情的情况下成功获取 128 位的 AES 加密密钥; 硬件木马检测方法能发现 AES 加密电路中的这种木马电路, 并实现 10^{-2} 的检测分辨率.

关键词: 硬件木马; 芯片安全; 现场可编程门电路(FPGA); 检测

中图分类号: TN918 文献标志码: A 文章编号: 1007-7162(2013)04-0070-04

Design and Detection of Hardware Trojan Based on Electromagnetic Leakage

Xie Hai^{1,2}, En Yun-fei², Wang Li-wei²

(1. School of Materials and Energy, Guangdong University of Technology, Guangzhou 510640, China;
2. Science and Technology on Reliability Physics and Application of Electronic Component Laboratory, CEPREI, Guangzhou 510610, China)

Abstract: Aimed at the problem that integrated circuits (ICs) may be attacked by hardware Trojan during the process of design or fabrication, thereby posing a significant risk in terms of their trusted field operation, it introduces the basic principles and taxonomy of hardware Trojan, and proposes the design of a kind of hardware Trojan, based on electromagnetic leakage. The Trojan circuit can reveal the encryption key of cipher IC by using electromagnetic emission. Based on FPGA(Field Programmable Gate Array) chips, an automatic cipher circuit test platform of AES (Advanced Encryption Standard) was constructed. By the analysis of the side channel, the hardware Trojan circuit could be detected. The experimental results show that the hardware Trojan can secretly steal the 128 bit AES encryption key, and that the detection method can help to identify this type of Trojan in AES cipher circuit, achieving the detection rate of 10^{-2} .

Key words: hardware Trojan; IC Security; FPGA(Field Programmable Gate Array); detection

随着集成电路在设计和制造过程中复杂程度的加深, 集成电路芯片已经进入全球化外包发展趋势, 集成电路也越来越融入到军民生活的各个领域, 芯片安全也广泛地引起人们的重视. 其中, 针对芯片的硬件木马研究成为新的热点. 硬件木马^[1-3]指的是在

设计或制造过程中, 对手往原始电路中植入的恶意电路, 这种电路潜伏在原始电路之中, 当电路运行到某些特定状态时, 影响原始电路的正常工作. 随着芯片的供应链参与者越来越多, 生产日益复杂, 其受到硬件木马攻击的风险越来越大, 从而导致芯片的安

全性受到威胁^[4-6]。

1 硬件木马原理及分类

1.1 硬件木马基本原理

硬件木马在芯片设计或制造过程中被恶意植入,其植入来源主要包括^[7]:(1) 集成电路设计人员故意植入恶意逻辑,外购的IP核中包含恶意电路;(2) 掩模生产商在掩模中植入恶意电路结构;(3) 集成电路制造过程中,加工厂也可能植入恶意电路或结构。一般情况下,木马电路结构只占原始电路面积很小的一部分,而且如果木马没有被触发,则处于静默状态,不对正常电路造成干扰,因此木马电路所带来的影响,会淹没在测量噪声和芯片的工艺扰动中。

木马被触发的方式很多^[8],例如:芯片内部逻辑状态触发,传感器触发,电磁触发等。木马触发后带来的危害大体可分为以下两类:(1) 破坏功能:硬件木马能够改变芯片内部的数据或结构,导致原始电路的功能发生改变、失常,甚至物理上对芯片实施破坏;(2) 信息泄漏:硬件木马能够将芯片内部的重要信息或数据通过隐蔽的方式泄露出去,造成对信息安全的威胁。

1.2 硬件木马分类方法

硬件木马可按照其物理特征,触发特征和作用形式来分类^[9-10]:

1) 根据物理特征,木马的类型可分为参数型和功能型。参数型木马主要是修改原始电路的逻辑或互连线,例如,延长路径时延,削弱互连线或晶体管的可靠性等。而功能性木马可通过添加或删除晶体管、门级电路来实现木马。

2) 通过不同的触发方式把木马简单划分为外部触发型和内部触发型^[11]。利用外部天线或者其他传感器来激活的木马电路,称为外部触发型木马。在潜伏过程中监测芯片内部逻辑状态,通过计数或内部信号的特殊逻辑值而激活的木马,称为内部触发型木马。

3) 通过硬件木马被激活后执行的操作,将其分为修改芯片功能的木马、更改芯片参数的木马、泄露芯片关键信息的木马等类型。

2 电磁泄漏型硬件木马设计

2.1 电磁泄漏型硬件木马设计与植入

本文在AES密码电路设计实现了一种电磁泄漏型硬件木马。该木马电路能通过电磁发射的方式泄漏密码芯片的密钥,其电路结构如图1所示。

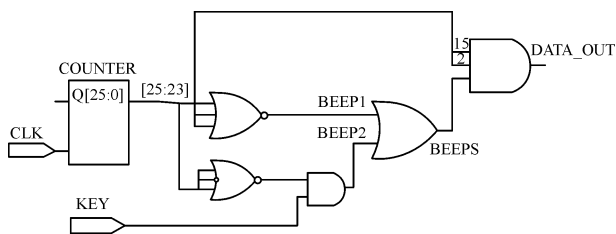


图1 电磁泄漏型硬件木马电路

Fig.1 Electromagnetic leakage based hardware Trojan circuit

密码芯片的密钥首先被转换为串行数据,然后通过KFY端口输入到木马电路中。木马电路主要是由一个26位的计数器构成,其输入时钟频率为50 MHz,用26位计数器的第15位输出形成762 Hz的音频信号,用计数器的第2位输出形成时钟频率为12.5 MHz的载波信号,上述两个信号与BEEPS信号一起经与门之后形成载波为12.5 MHz的调制信号,计数器的高3位用于产生间隔时间,DATA_OUT调制信号输出到电路板的一个闲置引脚上后,以无线电信号的方式被发射出去。该木马电路结构中,26位计数器构成了包含3个主要状态的状态机,它们分别为:第1个状态是发出“嘀”声;第2个状态是间隔;第3个状态是发出“嘀、嘀”声。如果密钥位是“0”则发出“嘀”声,然后是间隔时间;如果密钥位是“1”则发出“嘀、嘀”声,然后是间隔时间。

由图1可以看到,这种电磁泄漏型硬件木马的电路结构简单,只占用很少的FPGA逻辑资源,但却能把密码芯片的密钥调制成AM信号,通过无线电发射出去。为了能将信号发射到一定的距离,可以在电路板的闲置引脚上添加一段导线作为天线^[12],或者增大载波频率,收音机就能接收到“嘀”或“嘀、嘀”的声音信号,通过对这些声音的破解,就能还原原始的二进制密钥信息。

2.2 AES加密平台设计

为了验证上述电磁泄漏型硬件木马电路的功能,搭建了如图2所示的,包含该硬件木马的AES加密电路。该加密电路由4个模块组成:(1) aes_ciper模块: AES密码原型电路,用于实现AES加密算法;(2) rs232模块: 实现RS232串口协议,用于读取PC机发送的明文和密钥,并将加密后的密文回传给PC机;(3) rxd模块: 用于对rs232模块接收到的每帧8位PC机数据进行时序修整,然后把经过修整后的128位数据传送给aes_ciper模块;(4) txd模块: 把aes_ciper模块加密后输出的128位密文传递给rs232模块。

在 Xilinx Spartan 3E FPGA 开发板上实现了图 2 所示的 AES 密码芯片原型,并在 aes_ciper 模块中植入了电磁泄漏型硬件木马电路,该木马监视 RS232 串口上传输的 AES 电路的输入密钥,将其获取后再通过 PCB 板上的闲置引脚发送出去^[13-14]. 通过普通

的收音机,就能在一定的距离范围之内接收到密钥信号. 此外,笔者还基于 LabView 开发了串口通讯软件. 该软件通过串口连接开发板,实现数据的自动发送和接收,软件界面如图 3 所示,它能设置串口的各种参数,自动发送明文和密钥并接收加密后的密文.

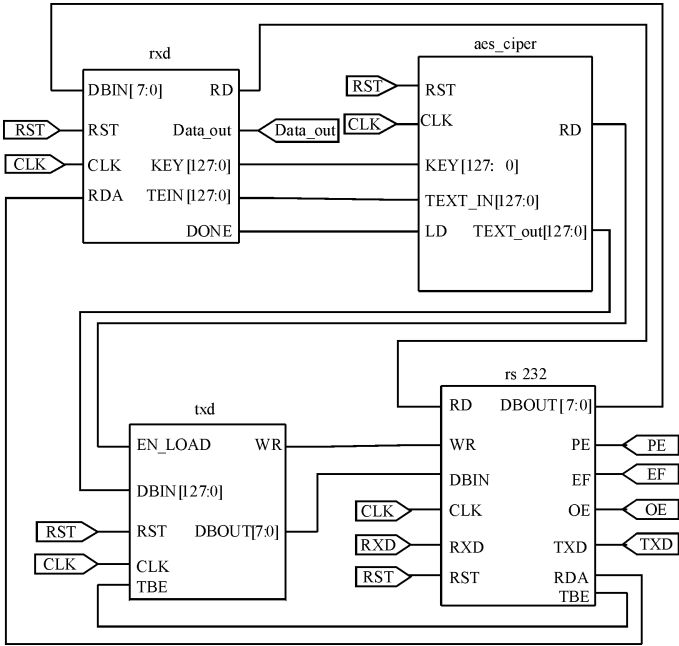


图 2 含木马的 AES 密码电路

Fig. 2 AES cipher circuit that contain hardware Trojan

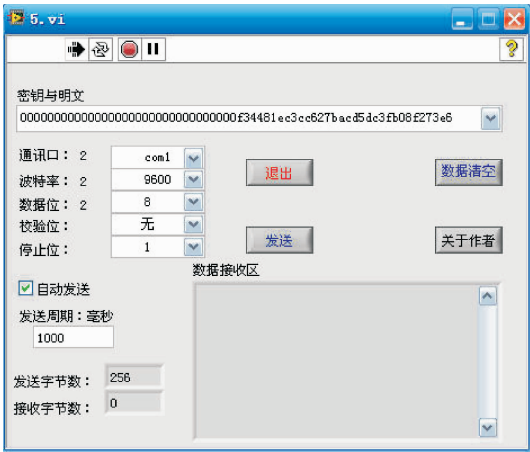


图 3 RS232 通讯控制软件

Fig. 3 RS232 communication controller software

3 电磁泄漏型硬件木马检测

3.1 检测方法原理

文献[15]提出了一种基于多参数的硬件木马检测方法. 考虑一批芯片中的第 i 个,在一阶近似的情况下,其瞬态电流 I_{ddt} 和最大工作频率 F_{max} 之间具有如下所示的线性关系:

$$\frac{I_{\text{ddt},i}}{f_{\text{max},i}} \approx k_{\text{av}} \cdot \beta_{\text{av}} \cdot n_{\text{tot},i} \cdot n_{\text{crit},i}, \tag{1}$$

其中 k_{av} 和 β_{av} 是基于门的常数,而 $n_{\text{tot},i}$ 是第 i 个芯片中开关门的总数, $n_{\text{crit},i}$ 是第 i 个芯片的关键路径上逻辑门的总数. 如果在第 i 个芯片中存在面积为 $n_{\text{trojan},i}$ 个等效门的硬件木马,那么式(1)可以重新写为

$$\frac{I_{\text{ddt},i,\text{trojan}}}{f_{\text{max},i}} \approx k_{\text{av}} \cdot \beta_{\text{av}} \cdot (n_{\text{tot},i} + n_{\text{trojan},i}) \cdot n_{\text{crit},i}. \tag{2}$$

比较式(1)和式(2),可以发现植入木马的最主要效果是改变了芯片的晶体管电流和最大工作频率之间线性关系的斜率. 在晶体管工作频率相同的前提条件下,对于集成电路的瞬态电流,植入硬件木马的芯片要比无硬件木马的芯片大.

3.2 检测实验平台

依据上述基于多参数的硬件木马检测方法,笔者构建了硬件木马检测实验平台,并开展了硬件木马检测实验. 实验平台的结构框图如图 4 所示,在实验平台的 FPGA 芯片上实现了图 1 所示的 AES 密码

芯片原型。

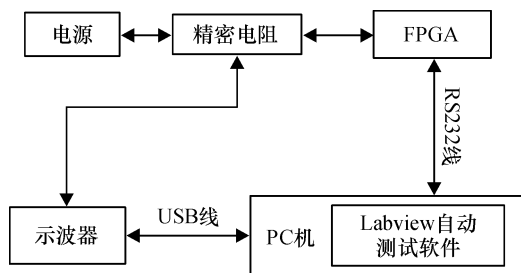


图4 检测实验平台框图

Fig. 4 Block diagram of detection experiment platform

基于多参数的硬件木马检测方法将待测芯片的供电电流与晶体管的工作频率关联起来,考虑到单个反相器延迟与晶体管的工作频率(充放电速度)成反比,因此可以把奇数个反相器串联成环形振荡器。基于反相器的环形振荡器的输出频率与单个反相器的延迟成反比,并且与晶体管的工作频率成正比,因此可利用环形振荡器的频率代替晶体管的工作频率。当芯片中环形振荡器的输出频率相同时,植入了木马电路的芯片,其所消耗的供电电流将会比无木马电路的芯片大。

以环形振荡器输出时钟的频率为横坐标,FPGA芯片所消耗的供电电流为纵坐标,不同输出频率对应不同供电电流,则输出频率与供电电流之间形成一条频率-电流曲线。依据式(1),该曲线应服从线性关系。可以绘制待测芯片与起参考作用的无木马芯片所对应的频率-电流曲线,并判断两条曲线是否发生显著分离:若出现显著分离,则可判断被测芯片中包含硬件木马电路;若两条曲线不发生显著分离,说明被测芯片在供电电流的消耗上与参考芯片无显著差异,则可判断被测芯片中不包含硬件木马。

为了绘制频率-电流曲线,环形振荡器的输出频率需要发生变化,而供电电压影响环形振荡器的输出频率,为此可利用直流电源单独向FPGA芯片的VCCINT核心电压端口供电,并且由1.2 V到1.5 V,以20 mV的步长等距调节供电电压16次。在每一种供电电压下,都会得到一个环形振荡器的输出频率。利用示波器记录一组测流电阻两端的电压瞬时值,16个电压值可对应得到16个频率值和16组电压瞬态值。根据每组电压瞬时值及检测电流的电阻可以计算出一组电流瞬时值,对该组电流瞬时值取算术平均值即可得到瞬时电流的平均值。

3.3 检测实验结果

检测实验中插入的木马电路如图1所示,它约占AES加密电路面积的1.7%。首先在FPGA芯片

中加载无木马的电路设计,并使供电电压从1.2 V递增至1.5 V,同时对输出频率和瞬态电压值进行采集;然后在FPGA芯片中加载植入了木马的电路设计,并按照相同的供电电压调整情况重新采集相应的频率和电压值,这一过程相当于对无木马和植入木马的两颗芯片分别进行了数据采集。对采集得到的数据处理后,绘制出频率-电流曲线如图5所示。

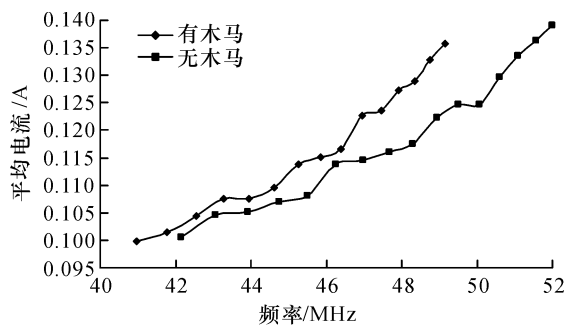


图5 检测实验结果

Fig. 5 Detection experiment results

图5所示的实验结果表明:有木马芯片的曲线与无木马芯片的曲线显著分离,且有木马芯片的曲线位于无木马芯片的上面。这意味着在相同频率下,有木马的芯片会消耗更多的电能,而且随着频率的增大,两种芯片的曲线的分离程度越来越显著。这一结果验证了基于多参数的硬件木马检测方法及本文构建的检测实验平台的正确性,此外还说明了该检测方法能实现 10^{-2} 的硬件木马检测分辨率。

4 结论

本文首先总结了硬件木马的基本原理及其分类方法,在此基础上在FPGA上设计实现了一种电磁泄漏型硬件木马,该木马电路能在AES加密电路工作过程中隐蔽地窃取其加密密钥,而且使得用户很难发现异常情况。此外,还根据多参数旁路分析的技术原理,成功实现了木马芯片的检测与分离,验证了其检测分辨率能达到 10^{-2} 。

参考文献:

- [1] Wang X X, Tehranipoor M, Plusquellet J. Detecting malicious inclusions in secure hardware: challenges and solutions [C] // IEEE Int Workshop on HOST. USA, CA, Anaheim, 2008: 15-19.
- [2] Banga M, Hsiao M. A novel sustained vector technique for the detection of hardware Trojans [C] // Int Conf VLSI Design. India, New Delhi, 2009: 327-332.

(下转第106页)

- 1534.
- [6] Ying Z Z. Antennas in cellular phones for mobile communications[J]. Proceedings of the IEEE, 2012; 2286-2296.
- [7] Li J F, Chu Q X. Tri-band antenna with compact conventional phone antenna and wideband MIMO antenna[J]. Antennas and Propagation Society International Symposium, 2012; 1-2.
- [8] Tang C L, Sze J Y, Wu Y F. A compact coupled-fed pentaband antenna for mobile phone application[J]. Microwave Conference Proc., 2010; 2260-2263.
- [9] Ying L J, Ban Y L, Chen J H. Low-profile coupled-fed printed PIFA for internal seven-band LTE/GSM/UMTS mobile phone antenna[J]. 2011 Radio Science and Wireless Technology Conference, 2011; 418-421.
- [10] Bhatti R A, Seong-Ook P. Internal multiband monopole antenna for modern multifunctional mobile phones[J]. Applied Sciences & Technology, 2009; 93-95.
- [11] Cheng-Tse Lee, Kin-Lu Wong, Planar monopole with a coupling feed and an inductive shorting strip for LTE/GSM/UMTS operation in the mobile phone[J]. Transaction on antennas and Propagation, 2010, 58(7): 2479-2483.
- [12] Rowell C, Lam E Y. Mobile-phone antenna design[J]. IEEE Antennas and Propagation Magazine, 2012, 54(2): 14-34.
- [13] Gao X, Zhang H. Low-Profile planar tripolarization antenna for WLAN communications[J]. IEEE Antennas and Wireless Propagation Letters, 2010, 9(3): 83-86.
- [14] Fujimoto K. Mobile antenna systems handbook[M]. Norwood, MA, Artech House, 2008; 219-313.
- [15] Kivekas O, Ollikainen J, Lehtiniemi T, et al. Bandwidth, SAR and efficiency of internal mobile phone antennas[J]. Transactions on Electromagnetic Compatibility, 2004, 46(2): 1012-1015.

(上接第73页)

- [3] Mohammad T, Farinaz K. A Survey of hardware Trojan taxonomy and detection[J]. IEEE Design And Test of Computers, 2010(1): 10-25.
- [4] Rajat S C, Seetharam N, Swarup B. Hardware Trojan: threats and emerging solutions[R]. 2009; 166-171.
- [5] Adeel S. The hunt for the kill switch[J]. IEEE Spectrum, 2008, 45(5): 34-39.
- [6] DARPA, TRUST in integrated-circuits proposer information pamphlet, 2007. [Online]. Available: <http://www.Darpa.Mil/MTO/solicitations/baa07-24/index.html>.
- [7] 涂浩. 基于旁路分析的硬件木马设计实现[D]. 长沙: 国防科技大学, 2010.
- [8] Yier J, Nathan K, Yiorgos M. Experiences in Hardware Trojan design and implementation[C]. IEEE International Workshop on Hardware. Oriented Security and Trust (HOST), 2009; 50-57.
- [9] Defense Science Board. High performance microchip supply [EB/OL]. [2011-08-11]. http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf.
- [10] Tehranipoor M, Sunar B. Hardware Trojan Horses. [EB/OL] <http://www.springerlink.com/content/r1h6518t98x10411>, 2010.
- [11] Rad R M, Wang X X, Monhammad T, et al. Power supply signal calibration techniques for improving detection resolution to hardware Trojans[C]//Int Conf Comp Aid Des, San Jose, NJ, USA, 2008. 632-639.
- [12] Wang X X, Salmani H, Tehranipoor M, et al. Hardware Trojan detection and isolation using current integration and localized current analysis[C]//Proc. IEEE Int'l Symposium on Fault and Defect Tolerance in VLSI Systems, 2008; 87-95.
- [13] Reza M, Rad, Wang X X, et al. Power supply signal calibration techniques for improving detection resolution to hardware Trojans[C]//Int. Conf. Computer-Aided Design, 2008; 632-639.
- [14] Seetharam N, Du D D, Rajat S C et al. Multiple-parameter side-channel analysis: a non-invasive hardware Trojan detection approach[C]//IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). USA, 2010; 13-18.
- [15] Agrawal D, Baktir S, Karakoyunlu D, et al. Trojan detection using IC fingerprinting[C]//2007 IEEE Symp Security and Privacy. Oakland.