

基于遗传算法的硬件木马检测方法

刘燕江^{1,2}, 何春华¹, 王力伟¹, 恩云飞¹, 谢少锋¹, 谢 云²

(1 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; 2 广东工业大学 自动化学院, 广东 广州 510006)

摘 要: 针对硬件木马严重威胁到芯片的安全性和系统的可靠性的问题, 提出了一种基于遗传算法的集成电路硬件木马检测方法, 该方法将 K 均值算法的局部收敛能力和遗传算法的全局收敛能力结合起来, 提取旁路信息间的微小特征差异, 实现硬件木马的在线自动检测. 本实验在 FPGA 芯片实现硬件验证, 以全局时钟、动态功耗和环形振荡器的输出三个信号作为研究对象, 搭建集成电路硬件木马检测系统采集三维旁路信息, 对 160 个样本芯片数据进行聚类分析, 实验结果证明该方法可准确有效地检测出硬件木马, 检测分辨率达到 10^{-4} 量级.

关键词: 硬件木马; 遗传算法; 特征提取; 旁路分析

中图分类号: TP31

文献标识码: A

文章编号: 1000-7180(2016)11-0074-04

A Novel Hardware Trojan Detection Method Based on Genetic Algorithm

LIU Yan-jiang^{1,2}, HE Chun-hua¹, WANG Li-wei¹, EN Yun-fei¹,
XIE Shao-feng¹, XIE Yun²

(1 Science and Technology on Reliability Physics and Application of Electronic
Component Laboratory, The Fifth Electronic Research Institute of the Ministry of Industry and
Information Technology, Guangzhou 510610, China;

2 School of Automation, Guangdong University of Technology, Guangzhou 510000, China)

Abstract: Hardware Trojan, a malicious circuit inserted into the golden circuit, causes a serious risk to the security of Integrated Circuits and the trust of critical system. Thus, hardware Trojan detection is of great significance. A novel hardware Trojan detection method based on clustering analysis algorithm is presented in this work, which employs the global optimized ability of genetic algorithm and the local searching capability of K-means algorithm to automatically fulfill the detection online. Side-channel signals, such as global clock signal, reset signal and a ring oscillator signal of a chip, are applied as the inputs of the clustering algorithm, since they may be altered by the Trojan circuit. Experimental results implemented with FPGAs demonstrate that the tested chips can be clustered into two categories, and the Trojan chips can be distinguished from the Golden chips accurately. The detection resolution achieves about 10^{-4} , which indicates the proposed novel detection method is feasible and effective.

Key words: hardware trojan; genetic algorithm; characteristics extraction; side-channel analysis

1 引言

随着半导体制造工艺不断提高, 集成电路广泛应用在国民生活中, 尤其是军事、通信、金融、交通等关乎国家命脉的行业, 而集成电路的设计、制造、测

试和封装也随着经济全球化的趋势逐渐分离, 越来越多的第三方公司和人员参与进来, 芯片在设计与制造过程中不完全自主可控, 攻击者可以在任何阶段篡改原始电路设计形成恶意电路, 监视电路的状态, 在特定的状态下激活电路, 使电路系统暂时性瘫

痪、芯片失效、功能紊乱或者信息泄露等. 集成电路作为现代信息系统硬件设备的核心,而硬件木马在底层硬件方面严重冲击了现代信息系统的安全性,如何保证集成电路的可信任性引起了世界各国的广泛的关注^[1].

近年来随着对硬件木马的研究逐渐深入,在硬件木马的检测技术方面取得了很多成果,主要有物理检测、功能检测、旁路信号分析三种. 旁路信号分析主要是通过采集芯片在工作时泄漏的旁路信息(如功耗、温度、电磁辐射等),利用信号处理技术(相关性分析、主成份分析、投影寻踪等)进行空间变换和压缩实现特征提取,对非木马芯片和待测芯片的旁路特征进行差异判别,如果差异超出阈值,则认为待测芯片中存在硬件木马,否则,待测芯片是非木马芯片^[2,3]. 旁路信号分析具有检测成本低、精度高、移植性好等优点,一经提出就展示出较为乐观的应用前景,成为当前硬件木马检测方法的主流^[4]. 但是由于测量仪器的精度限制和工艺噪声的影响,小面积的硬件木马的物理特征不明显,容易被噪声淹没,如何把硬件木马的特征放大到可以检测的程度是研究的重点.

因此,本文提出了一种基于遗传算法的硬件木马检测方法,该方法利用了遗传算法的优秀的全局搜索能力,同时又兼顾了收敛速度,寻找木马芯片和非木马芯片之间的特征相似性,确定样本的所属类别,该方法可以有效识别木马芯片与非木马芯片的微小的旁路特征差异,从而提高硬件木马的检测精度.

2 遗传算法的聚类分析

2.1 算法原理

遗传算法模拟生物进化机制,从任意一个初始种群出发,评价个体的优劣,从父代中选择并保留优秀个体,在搜索空间内随机迭代进化,最后进化到一个最优个体^[5]. 遗传算法是一种高度并行、随机、自组织、自学习和自适应优化算法,适用于求解一些非线性、多模型、多目标和多参数的复杂系统的全局总体优化问题. 针对木马芯片与无木马芯片在旁路信号的微弱的特征差异问题,可利用遗传算法的优秀的全局搜索能力,在搜索空间内寻找最优化的聚类,从而有效识别出木马芯片与无木马芯片的微小特征差异.

利用遗传算法的聚类分析来处理硬件木马的特征识别问题,需要解决以下三个问题:选择高效的编

码策略,评判个体的优劣,遗传算子的操作方式.

遗传算法需要结合实际的问题,选择合适的编码方案,将问题的解空间编码成遗传算子所能处理的遗传空间. 本文考虑到样本归属类号是一个无意义的数值,故采用符号编码方法,其中位串长度为160位,样本归属类号是1~2.

个体的评价是模拟自然选择过程,根据实际的评估标准评判个体的优劣程度,优良个体的基因在进化过程中被保留,而非优良个体的基因在进化过程中逐渐被淘汰. 个体的评价是通过计算个体的评估值和适应度来实现. 本文根据实际的聚类问题,利用K均值算法来分类样本,距离度量方式为类内和类间欧式距离之和 Δ , Δ 的数学表示如(1)所示. Δ 越小,则表示样本的分类越好. 聚类分析的目的是搜索使 Δ 最小的样本聚类,因此个体的评估值函数 $f = 1/\Delta$,其中 $\overline{X^{(w_i)}}$ 为第 i 个类的聚类中心,如式(2)所示,centerNum为聚类数目, N_i 为第 i 个类的样本数目.

$$\Delta = \sum_{i=1}^{\text{centerNum}} \sum_{j=1}^{N_i} ||X_j^{(w_i)} - \overline{X^{(w_i)}}||^2 \quad (1)$$

$$\overline{X^{(w_i)}} = \frac{1}{N_i} \sum_{j=1}^{N_i} X_j^{(w_i)} \quad (2)$$

遗传算法利用遗传算子(选择、交叉、变异)模拟遗传学中的繁殖、变异现象,产生下一代种群个体和实现种群进化. 为了避免优秀基因的损失,选择算子根据个体的适应度,选择优良个体,淘汰劣质个体. 本文采用的选择操作方法是排序选择法,它将个体的适应值按大小排序,计算第 i 个体的选择概率 $m_pop(i).fitness$,如式(3)所示,它只与序号有关,其中 α 排序因子,index是个体适应度的排列次序. 根据个体的选择概率建立选择数组cFitness来生成中间群体,如式(4)所示,popSize为种群规模.

$$m_pop(i).fitness = \alpha(1 - \alpha)^{\text{index}-1} \quad (3)$$

$$cFitness(i) = \frac{\sum_{k=1}^i m_pop(k).fitness}{\sum_{m=1}^{\text{popSize}} m_pop(m).fitness} \quad (4)$$

交叉和变异算子是模仿自然界的基因重组和变异过程,为了保留父代个体的优良基因,同时保持种群中个体的多样性,探索新的基因空间,生成更复杂结构的新个体. 交叉操作决定遗传算法的全局搜索能力,它根据交叉方法,将两个个体的部分基因互换. 变异操作作为辅助算子,根据变异方法,随机改变个体的基因值,它决定遗传算法的局部搜索能力,有

效解决了算法的结束缓慢问题. 交叉和变异算子作为随机化搜索算子, 需要设定优化的交叉概率和变异概率, 兼顾全局搜索能力和局部搜索能力, 这可以有效避免搜索阻滞和随机搜索, 大大提高算法的收敛能力和搜索效率^[6].

2.2 算法流程

基于遗传算法的硬件木马检测方法的流程图如图 1 所示.

(1) 确定实际问题的参数集, 对问题的解空间进行编码.

(2) 设置相关的控制参数和初始化种群: 根据实际问题的要求, 合理设置最大迭代次数、种群规模、聚类中心数目、交叉概率、变异概率、随机选择一组样本聚类结果作为初始种群.

(3) K 均值进行聚类分析: 根据评估标准将样本划分类别, 更新样本的聚类中心, 计算各个个体的适应度, 评价个体的优劣程度, 寻找最优个体并更新最优个体.

(4) 选择、交叉、变异算子操作, 生成新个体.

(5) 循环条件判断: 如果迭代次数未达到最大迭代数, 则程序跳转步骤(3)继续运行, 否则运算结束, 输出最优个体, 即问题的最优解.

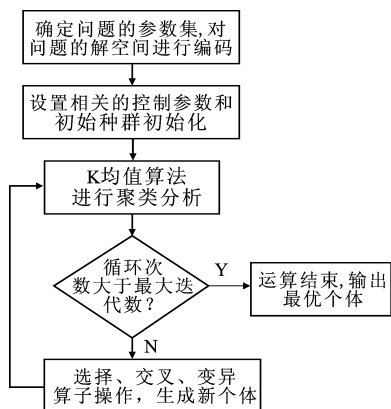


图 1 基于遗传算法的硬件木马检测方法的流程图

3 硬件木马检测方法

3.1 硬件木马检测平台设计

集成电路硬件木马旁路测试系统由 PC 机、NI 高速数字 IO 板卡、数字示波器和测试电路板四部分组成. 图 2 为集成电路硬件木马旁路测试系统的原理框图, 图 3 为集成电路硬件木马旁路测试系统的实物图.

测试电路板是以 XC3S500E FPGA 芯片为核心实现模拟 ASIC 环境, 同时为了凸显芯片间的工

艺偏差的影响, 测试电路板采用 ICsocket 方便 FPGA 芯片的更换, 如图 3 的右上角部分所示.

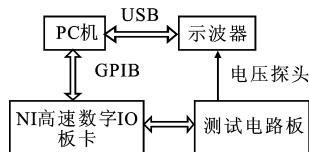


图 2 集成电路硬件木马旁路测试系统的原理框图

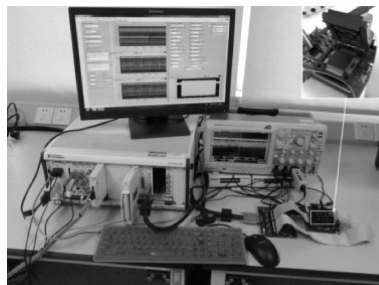


图 3 集成电路硬件木马旁路测试系统

PC 机是本系统的核心, 利用 LabVIEW 软件开发的硬件木马旁路测试系统实现系统参数配置与数据自动采集, 整个控制流程如下.

(1) 参数配置: 虚拟仪器控制平台配置示波器参数, 设置数据采集参数.

(2) 功能测试与数据采集: 虚拟仪器控制平台通过 NI 高速数字 IO 板卡产生测试向量, 为芯片提供输入激励信号, 同时采集芯片的输出响应信号, 如果输出响应信号与预期的响应信号一致, 则电路工作正常, 触发示波器自动采集并存储旁路信息, 并将波形数据通过示波器的 USB 口转储到 PC 机. 重复上述过程, 实现数据采集的自动化.

(3) 数据处理: 利用信号处理技术实现硬件木马特征的刻画与差异判别.

3.2 实验配置

硬件木马产生的额外的旁路信息与目标电路的旁路信息不是简单地叠加在一起, 而是以复杂的方式耦合在一起^[7]. 硬件木马不仅对芯片的动态电流、静态电流、电磁信号和热信号等旁路信息都产生一定程度的影响, 而且对电路的全局时钟、环形振荡器的输出频率等信号也产生一定的耦合影响. 例如, 植入硬件木马会改变原始电路的特征频率, 我们可以利用测试电路的特征频率的变化实现硬件木马的检测^[8].

本实验以全局时钟、动态功耗和环形振荡器的输出频率信号为研究对象, 采用 Cordic 电路作为基准电路, 硬件木马为 1 个计数器, 木马规模约占整体

电路规模的 5×10^{-4} .

4 实验结果

利用上述的实验平台采集三维旁路数据(即全局时钟、动态功耗和环形振荡器的输出频率信号),配置示波器的采样率为 2.5 GHz/s,采样时间为 400 μ s,分别采集 80 个木马芯片和无木马芯片的三维旁路数据.如图 4 所示为 160 个芯片的三维结果图,其中 x 轴为全局时钟 Clk 的均值, y 轴为动态功耗 Power 的均值, z 轴为 15 级环形振荡器的输出频率 $f_{\max}$.由实验 4 结果可以看出,木马芯片和无木马芯片的特征差异不明显.

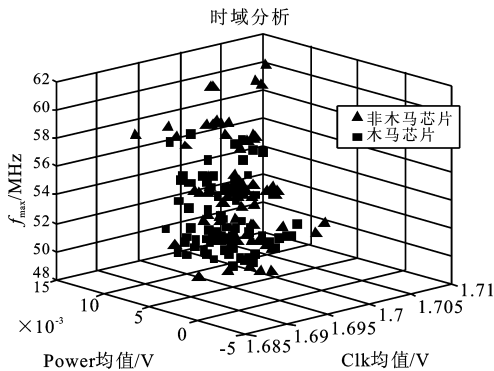


图 4 160 个样本芯片的三维原始旁路数据结果

为了提取木马芯片与无木马芯片在旁路信号上的微小特征差异,利用遗传算法进行聚类分析,将木马芯片和无木马芯片分离成两类,从而实现硬件木马的检测.图 5 所示为对 160 个待测芯片的聚类结果,1~16 号芯片为无木马芯片,17~32 号芯片为木马芯片,33~96 号芯片为无木马芯片,97~160 号片为木马芯片,从图中可以看出木马芯片聚为“1”类,无木马芯片聚为“2”类.该方法可有效的实现硬件木马的在线检测,大大减小的人工的干预,提高了数据的自动处理能力和硬件木马的识别效率.

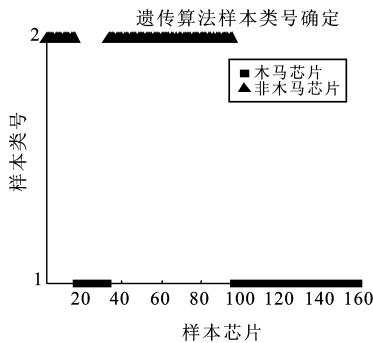


图 5 160 个样本芯片的聚类结果

5 结束语

本文以全局时钟、动态功耗和环形振荡器的输出三个信号为研究对象,木马芯片和无木马芯片的差别甚微,仅通过视觉观察会存在识别困难、误差大这些问题,因此木马芯片和无木马芯片的微小特征提取与识别是提高硬件木马分辨率的关键.本文利用遗传算法的聚类分析,借助于遗传算法的全局随机搜索能力,提取并识别木马芯片与无木马芯片之间的微小特征,将木马芯片和无木马芯片聚为两类,硬件木马的检测分辨率达到 10^{-4} 量级.

参考文献:

[1] Bhunia S, Hsiao M S, Banga M, et al. Hardware Trojan Attacks: Threat Analysis and Countermeasures[J]. Proceedings of the IEEE, 2014,10(8):1229-1247.

[2] 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.

[3] 苏静,赵毅强,何家骥,等.旁路信号主成分分析的欧氏距离硬件木马检测[J].微电子学与计算机,2015,32(1):1-4.

[4] Shila D M, Venugopal V. Design, implementation and security analysis of Hardware Trojan Threats in FPGA[C]//Proc of IEEE Communication and Information Systems Security Symposium. New York, NY, USA:ACM,2014:247-24 .

[5] Holland J H. Adaptation in natural and artificial systems: an introductory analysis with applications to biology, control, and artificial intelligence[M]2nd ed. Cambridge: MIT Press, 1992.

[6] 杨淑莹.模式识别与智能计算-Matlab 技术实现[M].第 2 版.北京:电子工业出版社,2011.

[7] 张鹏,王新成,周庆.基于电磁辐射信号分析的芯片硬件木马检测[J].电子学报,2014,42(2):341-346.

[8] Kitsos P, Voyiatzis A G. FPGA trojan detection using length-optimized ring oscillators[C]// Proc of 17th Euromicro Conference on Digital System Design. Paris kitsos:IEEE,2014:675-678.

作者简介:

刘燕江 男,(1990-),硕士研究生.研究方向为硬件木马检测.

何春华(通讯作者) 男,(1988-),工程师.研究方向为硬件木马检测. E-mail:hechunhua@pku.edu.cn.