# 基于探索式分区和测试向量生成的硬件木马检测方法

薛明富[1,2,3,4],胡爱群[2],王 箭[1,4]
(1. 南京航空航天大学计算机科学与技术学院,江苏南京 210016; 2. 东南大学信息科学与工程学院,江苏南京 210096;
3. 中国民航大学中国民航信息技术科研基地,天津 300300;4. 软件新技术与产业化协同创新中心,江苏南京 210023)

**摘 要:** 本文提出基于分区和最优测试向量生成的硬件木马检测方法. 首先,采用基于扫描细胞分布的分区算法将电路划分为多个区域. 然后,提出测试向量重组算法,对各区域依据其自身结构生成近似最优的测试向量. 最后,进行分区激活和功耗分析以检测木马,并采用信号校正技术消减制造变异和噪声的影响. 优点是成倍提高了检测精度,克服了制造变异的影响,解决了面对大电路的扩展性问题,并可以定位木马. 在基准电路上的验证实验表明检测性能有较大的提升.

**关键词:** 硬件安全; 硬件木马检测; 探索式分区; 最优测试向量生成
**中图分类号:** TP309 **文献标识码:** A **文章编号:** 0372-2112 (2016)05-1132-07
**电子学报 URL:** http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.05.017

# A Novel Hardware Trojan Detection Technique Using Heuristic Partition and Test Pattern Generation

XUE Ming-fu[1,2,3,4], HU Ai-qun[2], WANG Jian[1,4]
(1. *College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu* 210016, *China*;
2. *School of Information Science and Engineering, Southeast University, Nanjing, Jiangsu* 210096, *China*;
3. *Information Technology Research Base of Civil Aviation Administration of China, Civil Aviation University of China, Tianjin* 300300, *China*;
4. *Collaborative Innovation Center of Novel Software Technology and Industrialization, Nanjing, Jiangsu* 210023, *China*)

**Abstract:** A novel hardware Trojan detection method based on heuristic partition and optimal test pattern generation is proposed. First, we use a scan cell distribution based heuristic partition to divide the circuit into regions. Then, we propose a test vector ordering algorithm to generate near-optimal test patterns based on the circuit's structure. Lastly, we activate each region separately and perform localized $I_{DDT}$ analysis to detect hardware Trojans while a signal calibration technique is used to eliminate the effect of process variations and noises. The benefits of this approach are that it can magnify detection sensitivity, eliminate the effects of process variations and noises, ensure the scalability of hardware Trojan detection facing large scale ICs, and determine Trojan's location. We evaluate our approach on benchmark circuits and the experiment results show that the detection sensitivity is greatly improved.

**Key words:** hardware security; hardware Trojan detection; heuristic partition; optimal test pattern generation

## 1 引言

硬件行业全球化的生产模式,使得集成电路(Integrated circuits,IC)容易受到恶意修改的威胁[1~7],俗称为硬件木马(Hardware Trojan,HT),它可以在特定条件或时刻触发,然后破坏、关闭、控制芯片/系统,或者泄露机密信息. 硬件所面临的安全威胁和巨额经济损失已经引起了工业界和敏感部门的高度重视,亟待研究解决.

文献[8]通过多次触发电路内部节点的稀有逻辑条件去增加逻辑测试的检测机率. 逻辑测试法很难触

收稿日期:2014-10-23;修回日期:2015-05-22;责任编辑:马兰英
基金项目:江苏省自然科学基金青年基金(No. BK20150758);中国博士后科学基金面上资助(No. 2014M561644);江苏省博士后基金科研资助(No. 1402034C);中国民航信息技术科研基地开放课题基金(No. CAAC-ITRB-201405);中央高校基本科研业务费专项资金资助(No. NS2016096)

发有着复杂触发条件的木马. 基于旁道参数分析的硬件木马检测方法被证实可以通过观测电路的时延、功耗、电流等来检测出木马[9,10]. 然而,原旁道参数分析法不足以克服制造变异(process variation,PV)和噪声的影响. 在现代纳米工艺下,制造变异对 IC 的影响不断增加,能完全覆盖掉木马对电路的影响[1~7]. 另外,这种观测电路全局信号的方式,面对大电路时不具有扩展性. 因此,一些区域化激活的方法被用来放大木马的影响[11~13],然而,这些方法都是采用大量的随机向量盲目地测试,或者辅以计算复杂度很高或者很耗时的测试向量训练过程,其检测灵敏度并不理想. 文献[14]提出信号校正技术消减 PV 的影响,然而,该方法没有考虑到测试向量的影响,测试向量引起的电路中其他元件的翻转活动也会覆盖掉木马对电路引入的异常.

已有工作大多假设可以通过可信的方式获得干净样本芯片,由样本芯片提供参考以检测木马. 这成为当下研究方法的普遍瓶颈. 已有少量工作开始探索如何不依赖于参考芯片去检测木马[15~17]. 这些探索均有一定的局限性,常见的代价是需要昂贵的计算量、复杂的 PV 模型,面对大规模芯片时为了确保精确度需要大量反复测试.

本文提出基于分区和最优测试向量生成的硬件木马检测方法. 首先,采用基于扫描细胞分布的探索式分区算法将电路虚拟划分为由扫描链控制的各个区域. 然后,针对已有工作均采用大量随机向量盲目测试的问题,基于权重翻转(Weighted Transition,WT)指标,提出了测试向量重组算法(Test Vector Ordering,TVO),该算法基于电路结构生成近似最优的测试向量,可以最大程度地触发目标区域. 然后,在各个区域中间放置功耗管脚进行局域化的功耗测量分析以检测木马. 最后,采用信号校正技术[14]消减制造变异和噪声的影响. 相比已有工作,优点是成倍提升了检测精度,解决了面向大电路的扩展性问题,克服了制造变异的影响,并可以定位木马的位置. 在 ISCAS89 基准电路上验证了本方案,并与已有检测方法[9,13,14]进行了比较,结果表明检测性能得到较大提升.

## 2　问题建模

电路中的功耗由静态功耗和动态功耗组成[18]. 静态功耗 $P_{st}$ 是由泄漏电流引起,动态功耗包括切换瞬态电流引起的功耗 $P_{sc}$ 和负载功放充放电引起的功耗 $P_d$. 因此,总功耗为:

$$P_{total} = P_{st} + P_d + P_{sc} \tag{1}$$

与 $P_d$ 相比,$P_{st}$ 和 $P_{sc}$ 是可以忽略的[18]. $P_d$ 约为:

$$P_d = \frac{1}{2} \times C \times V_{DD}^2 \times N_G \times f \tag{2}$$

其中,$C$ 是电容,$N_G$ 是门的输出翻转的总数目,$V_{DD}$ 是供应电压,$f$ 是工作频率. 因此,功耗与翻转次数成正比. 扫描链测试结构是时序电路常用的结构,可以近似地认为扫描链控制电路的翻转活动. 在扫描测试时,功耗正比于扫描链上的翻转数目.

本文定义评估木马检测能力的指标——功耗差异百分比(Percentage Difference Between Power Consumption,PDPC). 假设电路分为 $M$ 个区域,区域 $x$ 的 PDPC 定义如下:

$$PDPC(x) = \frac{P_{CUA}(x) - P_G(x)}{P_G(x)} \tag{3}$$

其中,$P_{CUA}(x)$ 是待测电路(Circuit Under Authentication,CUA)中区域 $x$ 的功耗,$P_G(x)$ 是样本芯片中区域 $x$ 的功耗.

## 3　整体方案框架

本方案步骤如下. 首先,采用基于扫描细胞分布的分区算法将电路划分为多个区域. 然后,连接同一个区域内的扫描细胞形成扫描链,电路就被划分为由扫描链控制的各个区域. 然后,执行测试向量生成算法以最大化目标区域的翻转活动. 最后,在每个区域中间放置电源管脚,插入小规模的校正电路[14]用于建模 PV 和噪

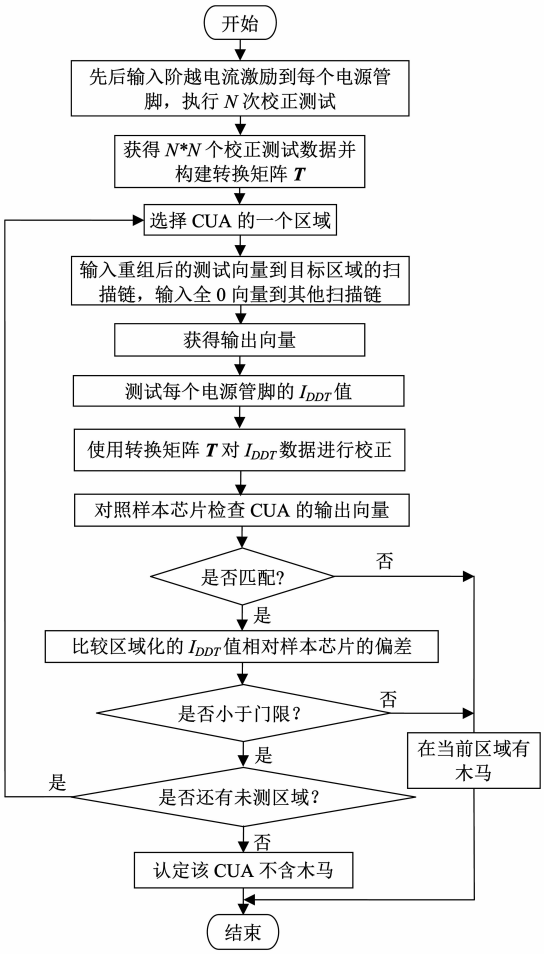



**图1　基于局域化活动控制和$I_{DDT}$分析的木马检测流程**

声的信息.

如图 1 所示($N$ 为功耗管脚数目),在检测阶段,首先执行校正测试去收集校正数据和构建转换矩阵. 然后,用 TVO 向量输入到目标区域的扫描链,其他区域的扫描链输入持续的 0 向量以保持背景活动是沉寂的. 此时,首先比较 CUA 与干净电路的输出是否一致,如果不一致,则检测出了木马,如果一致,则进入下一步. 然后,测量多个功耗管脚的瞬态电流,并进行信号校正. 最后,分析局域化 $I_{DDT}$(动态电流)数据用于木马检测.

## 4 基于扫描细胞分布的分区算法

### 4.1 分区算法

本文将文献[19]的聚类算法进行了修改应用于木马检测,伪代码如算法 1 所示. 首先,计算电路切割的数目. 然后,提取各扫描细胞的物理位置信息,移除扫描细胞之间已有的连接. 然后,将扫描细胞的物理信息表征为横纵坐标($X$、$Y$). 然后,将一个区域递归式的切割为扫描细胞数目相等的两个区域. 然后,重新连接同一区域内的扫描细胞,于是每个区域形成了一条扫描链. 接下来,优化扫描链布线以避免拥塞. 最后,在每个区域中间放置功耗管脚用于 $I_{DDT}$ 分析. 图 2 给出了在 ISCAS89 基准电路 s953 上实现的分区算法示意图.

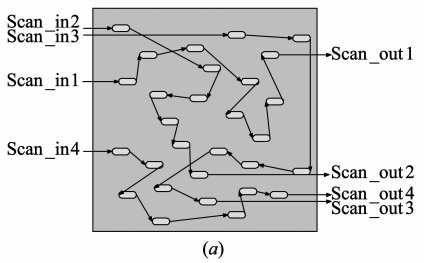



图2 s953的分区:(*a*) 分区前;(*b*) 分区后;(*c*) 扫描链重新连接和放置功耗管脚

**算法 1 探索式分区**

% Main:
1. 计算:*No. Cut* = $\lfloor \log_2(N) \rfloor$
2. 提取扫描细胞的物理信息
3. 移除扫描细胞之间的连接
4. *Current _ Region* = *Entire _ Region*
5. CutFunction(Current _ Region, No. Cut)
6. 重新连接每个区域内的扫描细胞,并优化布线拥塞
7. 保存

% CutFunction:
1. 当 *No. Cut* > 0 执行
2. 在 *Current _ Region* 内,计算 $\Delta X = X_{\max} - X_{\min}$;
3. 在 *Current _ Region* 内,计算 $\Delta Y = Y_{\max} - Y_{\min}$
4. 如果($\Delta X > \Delta Y$)
5. 按横坐标切割 *Current _ Region*;
6. 否则
7. 按纵坐标切割 *Current _ Region*;
8. *Current _ Region* 分割为 *Region*1 和 *Region*2.
9. CutFunction(Region1, No. Cut-1);
10. CutFunction(Region2, No. Cut-1);
11. 输出

### 4.2 时间复杂度分析及测试实验

硬件木马可能是紧凑型木马,插入在电路的一个或者相邻的几个区域,也可能是松散型木马,散布在多个区域,这就给分区检测带来了困难. 相关工作中[13]使用了所有区域激活的组合. 假设逻辑细胞的最大输入端数为 $I_{\max}$,电路分为 $M$ 个区域,则共有 $\sum_{i=1}^{I_{\max}} C_M^i$ 轮的区域激活组合,这将会是极为耗时的.

事实上,一个木马如果散布在不相邻的几个区域,那么它必然会影响电路的路径时延,因此可以轻易地用时延分析法检测出来. 因此,没有必要检测区域激活的组合,仅仅需要考虑紧凑型木马,检测时间可大幅缩短. 本文用实验来验证这一结论,对 ISCAS89 基准电路 s38417 进行分区,设计一个时序木马 *T*3(详见第 6 节),插入到第 15 区和第 16 区. 然后采用本方案进行分区激活,测量 PDPC 值. 结果显示两个 PDPC 值明显高于其他 PDPC 值,分别是第 15 区和第 16 区,这表明木马位于这两个区域. 然后,同时激活第 15 区和第 16 区. 上述独立激活和同时激活的结果如表 1 所示,同时激活这两个区域时,PDPC 值介于区域独立激活的 PDPC 值之间. 这表明两个区域的组合激活增加了背景噪声,相当于是更粗糙的分区,从而降低了检测灵敏度. 因此,即使木马有可能分布在两个或以上的区域中,也仅仅需要独立地检测每个区域. 所以总共只有 $M$ 种情况,相比 $\sum_{i=1}^{I_{\max}} C_M^i$,时间复杂度极大地降低了.

**表 1　区域组合激活和独立激活的 PDPC 值**

| 激活区域 | PDPC |
|---|---|
| 区域 15 | 0.00161354 |
| 区域 16 | 0.00042425 |
| 区域 15 和 16 | 0.00093746 |

## 5　最优测试向量生成算法

本文采用 *WT* 指标[20]去预测扫描测试时测试序列引起的功耗. *WT* 如下计算:

$$WT = \sum (k - P_T) \tag{4}$$

其中,*WT* 是翻转的数目,$k$ 是扫描链的长度,$P_T$是发生翻转的位置. 对于输入向量和输出向量,$P_T$的值是相反的. 当输入向量的第一比特与上一个输出向量的最后一个比特不同时,会产生额外的翻转,该翻转会传过整个扫描链.

TVO 算法的伪码如算法 2 所示. 算法的输入是一组测试向量及其输出向量,算法的输出是重组过的测试向量集. 下面以图 3(*a*)的样例序列介绍算法流程. 首先,计算每两位之间的比特差异数目. 然后,利用比特差异数目构建无向加权图,如图 3(*b*)所示,图中,每个顶点表示一位,每条边上的权重反映了这两位连接在一起时会产生的翻转数目. 然后,为了找到最大翻转顺序,将图中的权重改为其倒数,去使得这个问题等价于旅行商问题(Traveling Salesman Problem,TSP). 因为 TSP 是 NP-hard 的问题[21],本文采用遗传算法来解决这个问题,可以在很短时间内找到近似最优解. 本文的遗传算法中,将可能的比特顺序作为个体,采用部分映射交叉[22]和点突变算子[23]作为交叉算子和变异算子,用 *WT* 作为适应函数. 将上述步骤得到的比特位顺序表示为定向循环图,如图 3(*c*)所示. 然后,根据 *WT* 值评估 $k$ 种可能的情况,并选择拥有最大 *WT* 值的顺序. 最后,基于上述结果顺序执行测试向量重组,结果如图 3(*d*)所示.

**算法 2　TVO 算法**

1. 计算比特差异
2. 构建加权图
3. 将加权图的所有权重改为其倒数
4. 采用遗传算法解决 TSP 问题:
   开始遗传算法
      随机选择 10000 比特顺序作为原始种群大小
      *No. Generation* = 0
      当 *No. Generation* > 10000,停止执行
      开始
         计算原始种群中所有个体的 *WT*
         选择拥有最高 *WT* 值的 50 个个体作为父辈
         使用部分映射交叉对选定的父辈生产 50 个孩子
         随机选择 1 个孩子采用点突变算子进行突变
         将这 50 个孩子加入到种群中
         将种群中 *WT* 值最低的 50 个个体移出种群
         *No. Generation* + + ;
      结束
      输出带有最高 *WT* 值的比特顺序
   结束遗传算法
5. 依据 *WT* 值评估 $k$ 种可能的方案
6. 选择拥有最高 *WT* 值的方案
7. 重组测试向量

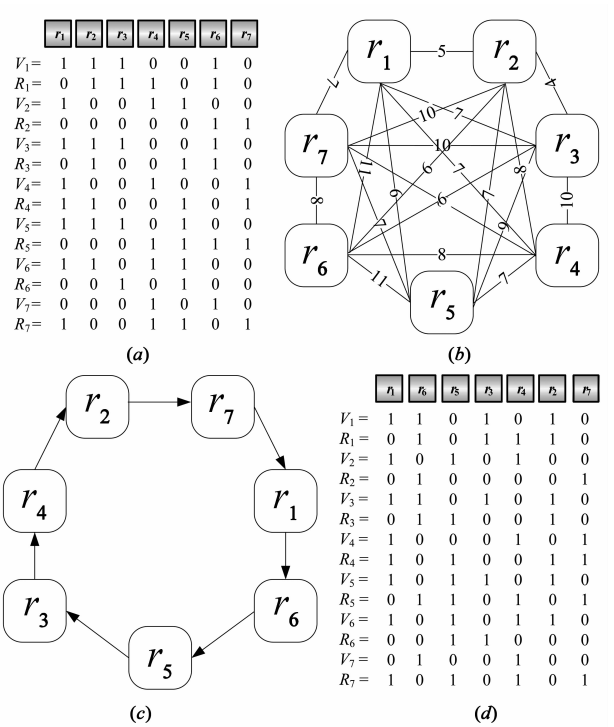



**图3　(*a*) 样例测试序列;(*b*)加权图;(*c*) 定向循环图;(*d*)最终测试序列**

## 6　验证实验

### 6.1　实验设置

本节给出验证实验,并与已有的代表性方法进行对比,包括原旁道参数分析法[9]、分区随机向量激活法[13]和信号校正法[14]. 评估的性能包括:定位、检测灵敏度、测试向量的影响、面临大电路的扩展性和信号校正的效果. 设计了两个组合木马(*T*1、*T*2)和一个时序木马(*T*3)插入到 ISCAS89 基准电路中,如图 4 所示,这些木马不具有真实的恶意功能,仅是对电路的微小改动用于评估本方案的检测能力.

### 6.2　实验结果

区域激活实验显示电路活动主要局限在目标区域,而其他区域只有微弱的翻转活动. 图 5 给出了电路 s15850、s35932 和 s38417 的分区激活检测效果. 结果表明,当激活了木马所在的区域时,木马引入的差异得到了大幅放大. 结果表征了木马所在的位置,因为有着较

高 PDPC 值的区域最有可能是木马所在区域.

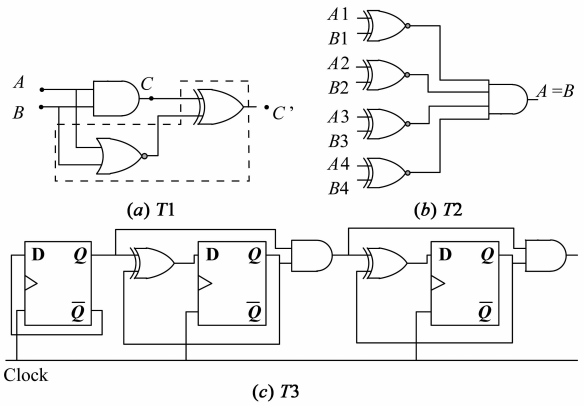



图4 硬件木马

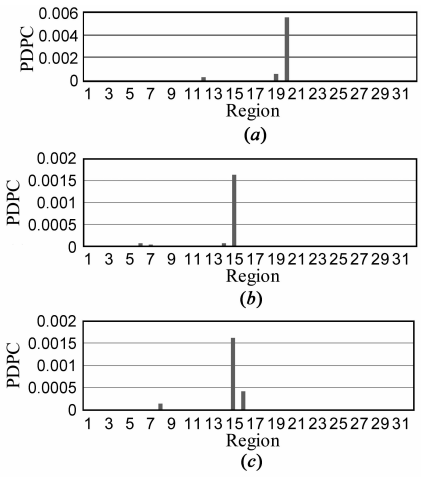



图5 木马*T*3检测结果：(*a*) s15850；(*b*) s35932；(*c*) s38417

表 2 给出了检测灵敏度分析与对比. 首先对比本方法与原旁道参数检测方法[9],即第 9 列对比第 3 列,很明显,经过分区、优化测试向量和信号校正之后,检测精度放大高达 37 倍(0.4641673%/0.0125487%). 如果不采用信号校正,即第 6 列对比第 3 列,可以看出,经过分区、优化测试向量后,检测精度放大高达 33.66 倍. 图 6 给出了原旁道参数分析法[9](全局测量)和分区数目分别为 4、16 和 32 时分区激活方案的检测结果. 由图可知,分区数目越高,检测精度也越高.

表 2 硬件木马检测灵敏度分析(PDPC 值)

| 木马 | 基准电路 | 原旁道参数法[9]：全局信号 | 分区数 | 分区,随机向量,未校正[13,14] | 分区,TVO 向量,未校正 | 相比原旁道参数法[9]的放大 | 相比随机向量[13,14]的提升 | 分区,TVO 模式,校正 |
|---|---|---|---|---|---|---|---|---|
| *T*1 | s344 | 0.73668% | 4 | 4.2186857% | 4.9012% | 6.652X | 16.1784% | 5.3859341% |
| *T*2 | s5378 | 0.1363465% | 16 | 1.1019834% | 1.3986248% | 10.26X | 26.9189% | 1.4888311% |
| *T*3 | s5378 | 0.0696237% | 16 | 0.9024156% | 1.1471224% | 16.48X | 27.1169% | 1.2605741% |
| *T*3 | s15850 | 0.0125487% | 32 | 0.3286527% | 0.4223922% | 33.66X | 28.5224% | 0.4641673% |
| *T*3 | s35932 | 0.0064399% | 32 | 0.1003652% | 0.14157% | 21.98X | 41.0549% | 0.163413% |
| *T*3 | s38417 | 0.0052319% | 32 | 0.1031243% | 0.1348378% | 25.77X | 30.7527% | 0.161354% |

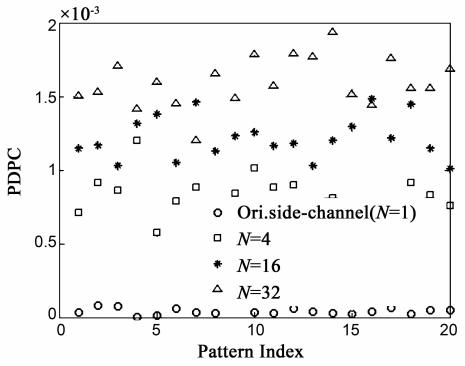



图6 不同分区数目的检测结果（*T*3在s38417中）：原旁道参数法（*N*=1），分区激活（*N*=4、16、32）

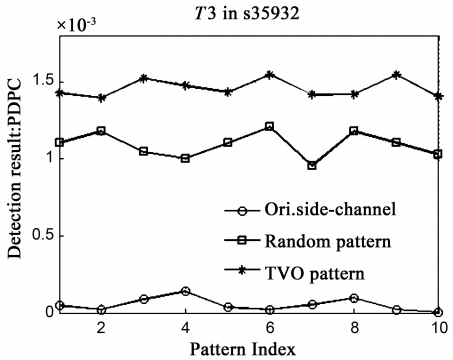



图7 随机向量与TVO向量检测性能比较（*N*=32）

图 7 给出了使用随机向量[13,14]和本文的 TVO 向量进行分区激活的检测效果对比,并绘出了原旁道参数法的检测结果用于参照. 可知,TVO 向量能够比随机向量取得更高的检测精度. 表 2 的第 6 列和第 5 列也给出了 TVO 向量和随机向量的比较,TVO 向量比随机向量的检测灵敏度提升高达 41.05%.

原旁道参数分析法[9]是监测全局信号,不能够扩展到大电路. 图 8 给出了扩展性对比,可知,原旁道参数法仅能够检测到 s5378 中的 *T*3,随着电路规模的增大,其检测灵敏度不断衰减. 本方案可以有效地放大木马的影响,检测到所有基准电路中的 *T*3. 对于规模较大的电路,只需采用更多的分区数目即可保证检测精度,具有较好的扩展性.

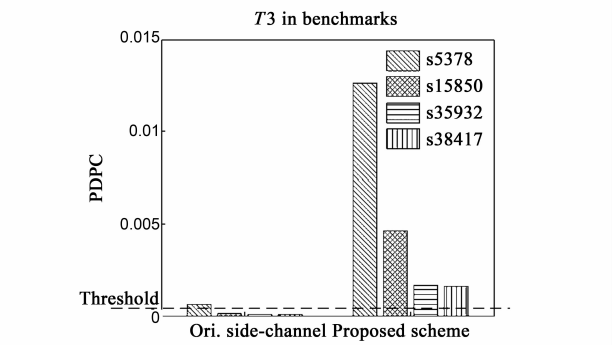



图8　原旁道参数法[9]和本方案的扩展性对比（$T3$）

表2的最后一列给出了采用信号校正后的检测结果,可以看出,使用信号校正技术之后,木马检测灵敏度有了明显增加.这个校正一定程度地消减了PV和噪声的影响,从而凸显了木马引入的异常.

## 7　小结

硬件木马已成为信息安全一个紧迫的新兴威胁.本文提出了基于分区和测试向量生成的局域化 $I_{DDT}$ 分析方法检测硬件木马.局域化分析可以放大检测灵敏度,确保面对大电路时的扩展性,并可定位木马的位置.本文还提出了优化向量生成方法,可以解决已有工作采用大量随机向量盲目测试的问题.实验显示所提方案可以大幅提升检测灵敏度.以后的工作将研究不需要样本芯片的硬件木马检测方案.

### 参考文献


[1] Jeyavijayan Rajendran, Ozgur Sinanoglu, Ramesh Karri. Regaining trust in VLSI design:Design-for-trust techniques [J]. Proceedings of the IEEE, 2014, 102 (8): 1266 – 1282.

[2] Swarup Bhunia, Michael S. Hsiao, Mainak Banga, Seetharam Narasimhan. Hardware trojan attacks: Threat analysis and countermeasures [J]. Proceedings of the IEEE,2014,102(8):1229 – 1247.

[3] Masoud Rostami, Farinaz Koushanfar, Ramesh Karri. A primer on hardware security:models,methods,and metrics [J]. Proceedings of the IEEE, 2014, 102 (8): 1283 – 1295.

[4] M Rostami,F Koushanfar,J Rajendran,R Karri. Hardware security:Threat models and metrics[A]. Proc. Int. Conf. Comput. -Aided Design (ICCAD)[C]. San Jose, CA, Nov. 2013. 819 – 823.

[5] S Bhunia,et al. Protection against hardware Trojan attacks: Towards a comprehensive solution[J]. IEEE Design Test Comput. ,2013,30(3):6 – 17.

[6] Mohammad Tehranipoor,Farinaz Koushanfar. A survey of hardware trojan taxonomy and detection[J]. IEEE design & test of computers,2010,27(1):10 – 25.

[7] Rajat Subhra Chakraborty, Seetharam Narasimhan, Swarup Bhunia. Hardware trojan: threats and emerging solutions [A]. IEEE International High Level Design Validation and Test Workshop (HLDVT)[C]. San Francisco,CA,Nov. 2009. 166 – 171.

[8] Rajat Subhra Chakraborty,Francis Wolff,Somnath Paul,et al. MERO:A statistical approach for hardware trojan detection[A]. Workshop on Cryptographic Hardware and Embedded Systems (CHES)[C]. Lausanne, Switzerland, Sep. 2009. 396 – 410.

[9] Dakshi Agrawal,Selcuk Baktlr,Deniz Karakoyunlu,et al. Trojan detection using IC fingerprinting[A]. Proceedings of IEEE Symposium on Security and Privacy (SP07)[C]. Berkeley,CA,May 2007. 296 – 310.

[10] Y Jin,Y Makris. Hardware trojan detection using path delay fingerprint[A]. Proceedings of IEEE International Hardware-Oriented Security and Trust (HOST08)[C]. Anaheim,CA,June 2008. 51 – 57.

[11] M Banga,M Hsiao. A region based approach for the identification of hardware trojans[A]. Proceedings of IEEE International Workshop on Hardware-Oriented Security and Trust (HOST2008)[C]. Anaheim, CA, June 2008. 40 – 47.

[12] Sheng Wei,Miodrag Potkonjak. Scalable hardware trojan diagnosis[J]. IEEE Transactions on very large scale integration (VLSI) systems,2012,20(6):1049 – 1057.

[13] Hassan Salmani, Mohammad Tehranipoor. Layout-aware switching activity localization to enhance hardware trojan detection[J]. IEEE Transactions on Information Forensics and Security,2012,7(1):76 – 87.

[14] Jim Aarestad,Dhruva Acharyya,Reza Rad,et al. Detecting trojans through leakage current analysis using multiple supply pad IDDQs[J]. IEEE Transactions on information forensics and security,2010,5(4):893 – 904.

[15] Sheng Wei,Miodrag Potkonjak. Self-consistency and consistency-based detection and diagnosis of malicious circuitry[J]. IEEE Transactions on Very Large Scale Integration (VLSI) systems,2014,22(9):1845 – 1853.

[16] Azadeh Davoodi,Min Li,Mohammad Tehranipoor. A sensor-assisted self-authentication framework for hardware trojan detection[J]. IEEE Design and Test,2013,30(5): 74 – 82.

[17] Kan Xiao,Domenic Forte,Mohammed Tehranipoor. 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.

[18] Vinay Dabholkar, Sreejit Chakravarty, Irith Pomeranz, et

al. Techniques for minimizing power dissipation in scan and combinational circuits during test application[J]. IEEE Transactions on computer-aided design of integrated circuits and systems,1998,17(12):1325 – 1333.

[19] Y Bonhomme, P Girard, L Guiller, et al. Design of routing-constrained low power scan chains[A]. Proceedings of the Second IEEE International Workshop on Electronic Design, Test and Applications (DELTA 2004)[C]. Perth, WA, Australia, Jan. 2004. 287 – 292.

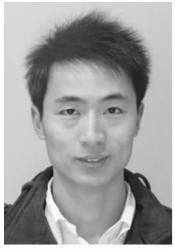
[20] Y Bonhomme, P Girard, C Landrault, et al. Power driven chaining of flip-flops in scan architectures[A]. IEEE International Test Conference (ITC)[C]. Baltimore, MD, USA, Oct. 2002. 796 – 803.

[21] P Larranaga, C M H Kuijpers, R H Murga, et al. Genetic algorithms for the travelling salesman problem: A review of representations and operators[J]. Artificial Intelligence Review,1999(13):129 – 170.

[22] Goldberg D E, Robert Lingle Jr Alleles. Loci and the TSP[A]. In Grefenstette, J. J. (ed.) Proceedings of the First International Conference on Genetic Algorithms and Their Applications[C]. Hillsdale, New Jersey, Lawrence Erlbaum,1985. 154 – 159.

[23] Ambati B K, Ambati J, Mokhtar M M. Heuristic combinatorial optimization by simulated darwinian evolution: A polynomial time algorithm for the traveling salesman problem[J]. Biological Cybernetics,1991,65(1):31 – 35.

## 作者简介



**薛明富(通信作者)** 男,1986 年 12 月出生,江苏南京人. 2014 年于东南大学获工学博士学位,2011 – 2012 年于新加坡南洋理工大学联合培养,现为南京航空航天大学计算机科学与技术学院讲师,主要从事硬件安全、硬件木马检测、硬件 IP 保护方面的研究.

E-mail: mingfu. xue@ nuaa. edu. cn

**胡爱群** 男,1965 年出生,东南大学信息科学与工程学院教授、博士生导师,东南大学信息安全研究中心主任,主要从事无线通信安全与移动终端安全方面的研究工作. 1987 年 6 月获南京工学院无线电技术专业学士学位,1990 年 4 月获东南大学信号电路与系统专业硕士学位,1993 年 4 月获东南大学信号与信息处理专业博士学位,1997. 11 – 1998. 10 在香港大学电机电子工程系从事博士后研究.

E-mail: aqhu@ seu. edu. cn