基于电磁辐射信号分析的芯片硬件木马检测

张 鹏,王新成,周 庆
(信息保障技术重点实验室,北京 100072)

摘 要: 集成电路芯片在制造过程中可能被嵌入恶意硬件电路,形成硬件木马.提出一种新的利用芯片电磁旁路泄漏信息的硬件木马无损检测方法.对芯片表面进行区域划分,通过随机选优算法生成硬件木马测试向量集;利用基于负熵指标的投影寻踪技术将芯片高维旁路信号投影到低维子空间,在信息损失尽量小的前提下发现原始数据中的分布特征,从而实现芯片旁路信号特征提取与识别.针对示例性高级加密标准(AES-128)木马电路的检测实验表明,该技术可以有效分辨基准芯片与硬件木马测试芯片之间的电磁信号特征差异,实现硬件木马检测.

关键词: 集成电路; 硬件木马; 电磁分析; 投影寻踪; 检测
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112 (2014)02-0341-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.02.020

Hardware Trojans Detection Based on Electromagnetic Emission Signals Analysis

ZHANG Peng, WANG Xin-cheng, ZHOU Qing
(*Science and Technology on Information Assurance Laboratory, Beijing* 100072, *China*)

Abstract: Integrate circuits(ICs) may be inserted malicious circuits as a hardware Trojan during fabrication. A novel hardware Trojans non-destructive detection technique using the electromagnetic side channel signals of chips is proposed. The technique includes two steps. Firstly, the surface of chip is divided into smaller sub-blocks, and a suitable input vector set is generated with a special selection algorithm. Secondly, based on the projection pursuit with negative entropy index, the detector could find out the data structure enables reflect high dimension special rules without obvious information loss, so as to attain the goal of feature abstraction and identification on side channel signals of IC chips. The detection experiments against an exemplary AES-128 hardware Trojan circuit showed that the technique proposed in this paper could distinguish the difference of side channel signal's feature between the genuine chip and tested chip, and consequently could detect the existence of the hardware Trojan.

Key words: integrate circuit(IC); hardware Trojans; electromagnetic analysis; projection pursuit; Trojans detection

1 引言

当前,由于集成电路设计与制造过程相分离,攻击者可能在原始集成电路芯片中植入具有恶意功能的冗余电路,形成硬件木马(Hardware Trojans),并在特定条件下实现破坏性功能或泄露芯片内部秘密信息,从而对集成电路的安全性与可靠性造成重大威胁[1].采取有效措施预防和检测硬件木马具有十分重要的意义.

对芯片硬件木马进行检测是一项极具挑战性的工作.目前国内外比较流行的检测方法主要有物理检测、功能检测、内建自测试、旁路分析(Side channel analysis, SCA)等.学术界与产业界普遍认为旁路分析检测技术是当前最有前途的一种检测方法[2].

利用芯片在运行过程中产生的功耗[3,4]、电路辐射、内部时延[5]等旁路信息,对同一生产批次的全部芯片进行硬件木马检测的典型流程为[6]:(1)从该批芯片中随机选择少量样本作为基准;(2)对基准芯片进行足够多的 I/O 测试以触发所有预期的电路工作,同时获取旁路信号;(3)对旁路信号进行特征提取;(4)对基准芯片进行剖片检测以确认其与原始设计一致;(5)对其余芯片(以下称测试芯片)进行相同的 I/O 测试、旁路信号采集与特征提取,并与基准芯片的结果进行比对,从而在不破坏测试芯片的情况下确定其中是否含有硬件木马.显然,硬件木马旁路检测技术是一种对照检测法,要求测试者具备芯片的原始设计知识,或者具备可信的基准芯片.实现检测的关键在于:(1)选择合适的测试向

收稿日期:2013-01-22;修回日期:2013-07-09;责任编辑:马兰英
基金项目:中国博士后科学基金(No.2012M512073)

量,以对部分或全部硬件木马电路进行激活,以改善检测效果[7];(2)旁路特征的刻画与差异判别,以对基准电路与硬件木马电路的旁路信号本质特征进行提取分析并进行区分[6,8].

由于芯片级的功耗等旁路信号十分微弱,而一般硬件木马电路的规模很小,其有效旁路信号相对于原始电路信号来说甚至相差几个数量级.同时,硬件木马电路与芯片原始电路之间的旁路信号不是简单的叠加,往往是通过一些耦合方式融合在一起,这些都导致硬件木马电路的旁路信号分布十分复杂,对其特征进行提取与识别十分困难.Agrawal 等人提出一种方法,通过 Karhunen-Loève 变换(简称 K-L 变换,其本质是主成分分析 Principal Component Analysis,PCA)对旁路功耗信号建立"指纹"并进行比对检测[6].这是一种传统的证实性多元分析(Confirmatory Data Analysis,CDA)方法,对于微弱、高维、分布复杂的芯片旁路信号来说效果不一定最佳.

本文在上述硬件木马旁路检测典型流程框架内,提出一种新的信号变换分析硬件木马检测方法.以芯片电磁辐射信号为测试对象,采用芯片电路区域划分方式,选取更可能激发硬件木马特征信号的测试向量;通过选取不同指标的投影寻踪(Projection Pursuit,PP)技术将芯片高维旁路信号投影到低维子空间,在信息损失尽量小的前提下发现原始数据中的分布特征,从而实现芯片旁路信号特征提取与识别,并有效实现硬件木马检测.

2 测试向量生成

为了对硬件木马的信号特征进行刻画,必须找到一个较小、无冗余的测试向量集以提供芯片功能的足够覆盖,特别是使得硬件木马(如果存在)能够被完全或部分激活,以提供相应的旁路信号泄漏.一般来说,硬件木马的完全激活非常困难.但是许多硬件木马由于需要监控激活条件,因此有部分电路始终处于激活状态.本文根据电磁测量可以精确定位的特点,采用随机选优的方式确定测试向量集.

2.1 区域划分

硬件木马通常仅占据整个芯片空间中很小的一部分.检测者并不能预测硬件木马在芯片中的位置,可以采用分而治之的方法来尝试对它进行分离.为此,对芯片表面区域进行划分,如图 1 所示:

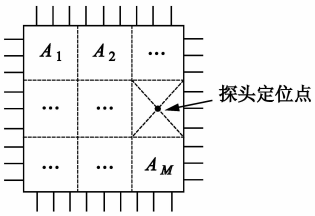


图1 芯片表面区域划分示意图

图 1 将整个芯片表面共划分为 M 个区域,硬件木马可能分布在其中 1 个或多个区域之中.每个区域的中心位置作为电磁探头的测量定位点.

2.2 测试集生成

对于每一个芯片区域,选择一组测试需要的激励向量.向量选取原则是使得当前区域的电磁辐射信号与其它区域相比差别较大,从而导致当前区域的电磁辐射效应在整个电路效应中凸显出来.如果当前区域中存在硬件木马,硬件木马信号效应相应得以增强.

测试向量集详细生成步骤描述如下:

Step 1 随机选择 D 个不同输入,记为向量 $\boldsymbol{d}=(d_1,d_2,\cdots,d_D)^{\mathrm{T}}$,在每一个区域,分别测量芯片在进行 D 次运算时的电磁泄漏.令 $\boldsymbol{t}_{a,i}=(t_{a,i,1},t_{a,i,2},\cdots,t_{a,i,T})$表示在区域 a,输入 d_i 对应的电磁泄漏轨迹,其中 T 代表轨迹长度.则全部电磁轨迹可表示为 M(M 为区域总数)个 $D\times T$ 的矩阵 $\boldsymbol{T}_a=(t_{a,1},t_{a,2},\cdots,t_{a,D})^{\mathrm{T}}$.

Step 2 对于区域 a,输入 d_i 计算当前电磁信号与其它区域同输入对应电磁信号的差异如下:

$$dif_{a,i}=\sum_{\substack{a'=1\\a'\neq a}}^{M}\sum_{t=1}^{T}(t_{a,i,t}-t_{a',i,t})^2,\ i=1,2,\cdots,D \tag{1}$$

对于所有区域,可得到 $M\times D$ 的矩阵 $\boldsymbol{DIF}=(\boldsymbol{dif}_1,\boldsymbol{dif}_2,\cdots\boldsymbol{dif}_M)^{\mathrm{T}}$,其中 $\boldsymbol{dif}_a=(dif_{a,1},dif_{a,2},\cdots,dif_{a,D})$.

Step 3 从矩阵 $\boldsymbol{DIF}$ 的每个行向量中分别选取最大的 n 个元素,其对应输入作为相应区域的测试向量集.

通过上述步骤,最终可以生成 $M\times n$ 个元素组成的测试向量集,每个芯片区域分别对应 n 个输入.

3 硬件木马检测方案

通过测试向量集对芯片电磁辐射信号特征进行刻画,是硬件木马检测的核心内容.本文利用投影寻踪技术来实现高维电磁辐射信号的特征分析.

3.1 投影寻踪技术

3.1.1 概述

投影寻踪(PP)是分析非线性、非正态高维数据的一种新兴统计方法,其基本思想是把高维数据投影到低维(一般 1~3 维)子空间,寻找能反映原高维数据结构或特征的投影(称为"令人感兴趣"的投影),通过对投影数据的分析达到研究分析原始数据的目的[9].

衡量投影数据令人感兴趣的程度是通过称为"投影指标"的函数来实现.设 $\boldsymbol{X}$ 是 d 维随机向量,分布函数为 $F_{\boldsymbol{X}}$.$\boldsymbol{A}$ 是从 R^d 到 R^k 的一个线性投影(矩阵)($d\geq k$),$\boldsymbol{Y}=\boldsymbol{AX}$ 是一个 k 维随机向量,分布为 $F_{\boldsymbol{Y}}$.投影指标

是定义在 $\boldsymbol{Y}$ 上的实值函数.在实际中,$\boldsymbol{X}$ 的分布一般难以直接得到,只能得到它的样本,因此对于投影方向 $\boldsymbol{A}$,投影指标记为 $Q(\boldsymbol{Y})$或 $Q(\boldsymbol{AX})$,此时 $\boldsymbol{X}$ 是指得到的随机变量样本数据.PP 的目标就是找到一个或几个投影矩阵,使指标值达到最大或最小.

最常见的情形是一维投影($k=1$),此时矩阵 $\boldsymbol{A}$ 简化为一个向量 $\boldsymbol{\alpha}$($\boldsymbol{\alpha}^{\mathrm{T}}\boldsymbol{\alpha}=1$),投影指标简化为 $Q(\boldsymbol{\alpha}^{\mathrm{T}}\boldsymbol{X})$.如果将指标取为样本方差,即令 $Q(\boldsymbol{\alpha}^{\mathrm{T}}\boldsymbol{X})=\mathrm{Var}(\boldsymbol{\alpha}^{\mathrm{T}}\boldsymbol{X})$,那么使 $\mathrm{Var}(\boldsymbol{\alpha}^{\mathrm{T}}\boldsymbol{X})$取最大值的方向 $\boldsymbol{\alpha}_1$ 就是数据协方差阵的最大特征根对应的特征向量,即第 1 主成分;如果继续作投影,在与 $\boldsymbol{\alpha}_1$ 垂直的空间里求单位向量 $\boldsymbol{\alpha}_2$,即在约束条件 $\boldsymbol{\alpha}_2\perp\boldsymbol{\alpha}_1$ 下,使得 $\mathrm{Var}(\boldsymbol{\alpha}^{\mathrm{T}}\boldsymbol{X})$取最大值的方向 $\boldsymbol{\alpha}_2$ 是第 2 主成分……依次下去,可以证明 PCA 就是以样本方差为指标,寻找一系列正交投影的 PP[9].即文献[6]中的信号分析技术实际是 PP 方法的一种特例.

PP 的过程一般采用迭代模式,即:选定投影指标→寻找最佳投影方向→将投影后的数据结构从原数据中去除,得到改进新结构.重复上述寻优过程,直到数据的投影不再显著含有我们感兴趣的结构为止.

3.1.2　投影指标

投影指标是 PP 成功与否的关键因素.对于硬件木马检测来说,方差指标可能并非是反映旁路信息的最佳投影指标.实际上,一般认为服从正态分布的数据含有的有用信息最少,因而通常受到关注的是与正态分布差别大的结构.多元正态分布的任何一维线性投影仍然服从正态分布,因此如果一个数据在某个方向上的投影与正态分布差别较大,那它就一定含有非正态的结构.高维数据在不同方向上的一维投影与正态分布的差别是不一样的,它显示了在这一方向上所含有的有用信息的数量,因此可以用投影数据的分布与正态分布的差别作为投影指标[9].

要对投影分布与正态分布之间的差别进行度量,通常采用信息散度(Information Divergence,ID)方式.由于 ID 具有非对称性,因此,对于两个连续的概率分布 $p(x)$与 $q(x)$,通常定义 $p(x)$、$q(x)$间的绝对信息散度(Absolute ID,AID):

$$J(p,q)=|d(p;q)|+|d(q;p)| \tag{2}$$

其中:

$$d(p;q)=\int_R p(x)\log\frac{p(x)}{q(x)}\mathrm{d}x \tag{3}$$

由于根据样本估计 $p(x)$, $q(x)$很麻烦,因此更简便有效的指标是用离散化的概率分布 p,q 分别代替连续密度函数$p(x)$,$q(x)$.此时定义:

$$J_D(p,q)=|D(p;q)|+|D(q;p)| \tag{4}$$

其中:

$$D(p;q)=\sum p_i\log\frac{p_i}{q_i} \tag{5}$$

式中 p_i,q_i 分别对应于p,q 中第 i 个元素.

若将 p 看作投影分布,q 选择为与p 同方差正态分布,则绝对信息散度可以很好地度量投影分布与正态分布之间的偏离程度.但是,由于式(4)中含有绝对值,在寻优过程中处理起来很麻烦;而且参考的 q 分布也需要预先予以确定,因此实际中应用 AID 指标存在困难.

本文采用信息论中的负熵作为偏离正态分布的广义信息理论测度.分布 $p(x)$与正态分布 $p_G(x)$之间的负熵定义为:

$$\begin{aligned}J_I(p)&=H(p_G)-H(p)\\&=\frac{1}{2}\log(2\pi)+\log(\sigma)+\int p(x)\log p(x)\mathrm{d}x\end{aligned} \tag{6}$$

其中,$p(x)$是分布密度函数,σ 是分布的标准差.由于正态分布的熵最大,因此式(6)是非负值.由于$p(x)$未知,所以必须由样本数据来估计它.一般常用矩函数近似值来逼近积分值.比如 Gram-Charlier 展开式直接利用分布的三阶、四阶累计量来对熵进行估计,其近似形式为[9]:

$$p(x)\approx\delta(x)\left[1+\frac{k_3}{3!}H_3(x)+\frac{k_4}{4!}H_4(x)\right] \tag{7}$$

其中,k_3,k_4 分别为总体的偏度与峰度:

$$\delta(x)=\frac{1}{\sqrt{2\pi}}\exp(-x^2/2),\ k_3=\frac{E(x-\bar{x})^3}{\sigma^3},\ k_4=\frac{E(x-\bar{x})^4}{\sigma^4}-3$$

$$H_3(x)=4x^3-3x,\ H_4(x)=8x^4-8x^2+1$$

将式(7)代入式(6),可得负熵的近似值:

$$\hat{J}_I(p)=\sigma-\frac{(k_3)^2}{2\cdot3!}-\frac{(k_4)^2}{2\cdot4!}+\frac{5}{8}(k_3)^2k_4+\frac{1}{16}(k_4)^3 \tag{8}$$

显然,利用式(8)比利用式(4)在投影寻优过程中处理起来要更为简便.

3.2　硬件木马检测

下面给出采用负熵指标投影寻踪分析的硬件木马检测方案(符号意义与第 2 节相同):

Step 1　旁路信息采集.利用第 2 节中生成的 $M\times n$ 的测试向量集,输入基准芯片使之正常运行.获得 M 个 $n\times T$ 的电磁轨迹矩阵 $\boldsymbol{TB}_a=(tb_{a,1},tb_{a,2},\cdots,tb_{a,n})^{\mathrm{T}}$;类似的,以相同测试向量集针对测试芯片形成 M 个 $n\times T$ 的电磁轨迹矩阵 $\boldsymbol{TC}_a=(tc_{a,1},tc_{a,2},\cdots,tc_{a,n})^{\mathrm{T}}$.

Step 2　选择第 1 个基准矩阵 $\boldsymbol{TB}_1$ 进行投影,使之包含最多有用信息(即投影后分布与正态分布差异最大).令投影方向为 $\boldsymbol{\beta}=\{\beta(1),\beta(2),\cdots,\beta(T)\}$,则一维投影值 $zb(i)$可综合为:

$$zb(i)=\sum_{j=1}^{T}\beta(j)tb_1(i,j),(i=1,2,\cdots,n) \quad (9)$$

式中 $tb_1(i,j)$表示矩阵 $\boldsymbol{TB}_1$ 中的元素.

根据式(8),可以通过求解负熵指标函数最大化问题来估计最佳投影方向,即设定指标函数为:

$$\max \quad \hat{J}_I(zb)=\sigma-\frac{(k_3)^2}{2\cdot 3!}-\frac{(k_4)^2}{2\cdot 4!}+\frac{5}{8}(k_3)^2k_4+\frac{(k_4)^3}{16} \quad (10)$$

约束条件:s.t. $\sum_{j=1}^{T}\beta^2(j)=1$

式中 σ、k_3、k_4 分别为一维投影 $\boldsymbol{zb}$ 的标准差、偏度及峰度.由此可得最佳一维投影 $\boldsymbol{zb}_1(i)$及最佳投影方向 $\boldsymbol{\beta}_{zb}$.

Step 3 与步骤 2 类似,得到第 1 个测试矩阵 $\boldsymbol{TC}_1$ 含有最多有用信息一维投影值 $\boldsymbol{zc}_1(i)$及最佳投影方向 $\boldsymbol{\beta}_{zc}$.

Step 4 利用式(4),分别求 $\boldsymbol{zb}_1(i)$与 $\boldsymbol{zc}_1(i)$之间的 AID 值 $J_D(\boldsymbol{zb}_1,\boldsymbol{zc}_1)$及 $\boldsymbol{\beta}_{zb}$与 $\boldsymbol{\beta}_{zc}$之间的 AID 值 $J_D(\boldsymbol{\beta}_{zb},\boldsymbol{\beta}_{zc})$.前者可以衡量矩阵 $\boldsymbol{TB}_1$、$\boldsymbol{TC}_1$ 分别进行最佳一维投影后所得分布之间的偏离程度;后者可以衡量投影方向分布之间的偏离程度.若偏离程度十分明显,则意味着基准芯片与测试芯片在区域 1 中旁路信号存在明显差异,则可判断测试芯片区域 1 中可能存在硬件木马.偏离程度是否明显可以通过阈值范围判定,而阈值的确定可以通过对基准芯片进行多次测量计算先验获取.

Step 5 对芯片其它区域,类似重复上述步骤 2~4.如果判定所有区域均不存在硬件木马,则芯片中不存在硬件木马,否则可判定存在硬件木马并且对其进行区域定位.

在上述检测方案中,负熵指标作为确定高维旁路信号投影方向的投影指标;而 AID 作为投影后判断硬件木马是否存在的判定指标.

4 硬件木马检测实验

4.1 实验配置

实验基准芯片是一个带串行通讯接口的高级加密标准(Advanced Encryption Standard, AES-128)加密器.测试芯片包括两片,其中一片与基准芯片完全相同,而另一片中加入一个载波调制辐射泄漏型硬件木马[10],FPGA 电路结构如图 2 所示.

硬件木马模块设计见图 3.其中 Counter、Trans、Comp 分别为计数器、密钥并串转换、明文比较模块.当加密明文中含有"Lucky"字符串时硬件木马被完全激活,该木马首先将并行密钥转换为串行输出,根据密钥位形成不同的音频信号,通过载波调制后输出到芯片闲置引脚上发射,攻击者通过接收机接收并解调后就能恢复密钥.该硬件木马在不被激活时仍有部分电路处于工作状态.

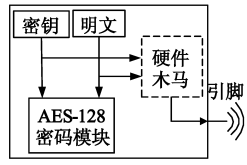


图2 FPGA内部电路结构图

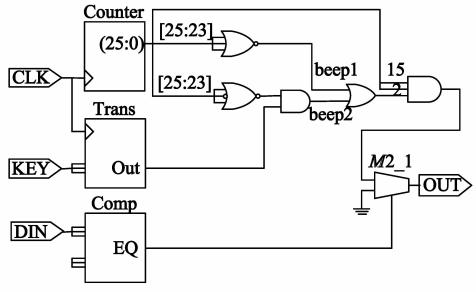


图3 硬件木马电路示意图

实验芯片采用 Xilinx 公司的 FPGA-XC3S400,设定运行频率 50MHz.芯片表面积约 3cm×3.5cm,被划分为 9 个区域.为减小 FPGA 布局布线不同对检测效果的影响,通过区域约束技术尽量将原始电路与木马电路约束到固定区域中.实验原始电路共占据 1039 个 slice,木马电路占据 78 个 slice,木马电路规模约占整体电路规模的 7%.

采用与文献[11]类似的芯片电磁信息采集平台(LANGER RF-B 3-2 型近场电磁探头,PA303 型前置放大器),采样频率为 500MSa/s,采样时长 0.2μs,每条轨迹采样长度为 100.在每次测试实验中,初始随机输入 10000 个,以基准芯片为标准,利用 2.2 节所述方法,在每个区域分别选择 50 个测试向量,共生成 50×9 的测试向量集,然后以每个向量为输入采集电磁信号.为减少噪声影响,每个测试向量均重复输入并采样 20 次,求均值后得到对应电磁轨迹.最终基准芯片与测试芯片在每个区域均生成 50×100 阶的电磁信号矩阵.

投影过程中寻找最佳投影方向是一个复杂的带约束的优化问题,选取何种寻优算法直接影响寻优效率,甚至影响能否获得最优解.本文采用 Matlab7 优化工具箱中的有约束非线性优化工具(序列二次规划 SQP 法)执行这一寻优过程.为增加寻优精度,本文设计了一种初始值加速处理方式,即首次初始值为随机选取,然后将第一次的寻优结果设置为初始值进行二次寻优,依此类推,将执行 10 次初始值加速寻优过程后的结果作为本次寻优的最终结果.

4.2 实验结果

由于 PP 算法的非确定性与测量过程中的噪声影

响,木马检测结果具有一定的概率性.为此,本文通过多次测试的结果来对比判定上述 PP 寻优法的检测效力.利用 K-L 变换信号分析法[6]与 PP 寻优法分别进行 20 次硬件木马检测实验,最终检测成功率分别为 15%、80%,实验结果显示 PP 方法的成功率远高于 K-L 变换法.

图 4 为采用 K-L 变换法的典型实验结果,横坐标表示按主成分排序的特征向量,纵坐标表示对应的投影坐标值.理想情况下,基准芯片与含硬件木马的芯片具有不同的投影分布,表现为"截尾"子空间不同(即二者趋近于 0 的速度不同).但图 4 中没有表现出这种分布差异,这意味着该方法无法判断是否存在硬件木马电路.

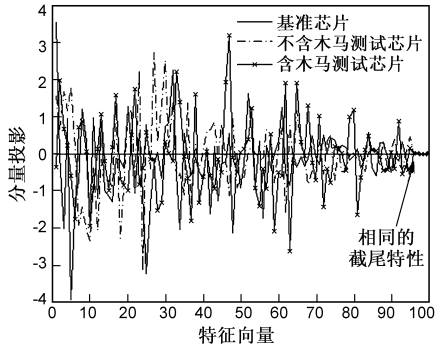


图4　采用K-L变换分析的硬件木马检测典型结果

图 5 为采用 PP 信号分析的典型实验结果.图中直观显示了基准信号与两种测试信号的最佳一维投影值分布之间的差别,差别的量化值由(4)式定义的 AID 计算得到.可以看到,基准信号与不含硬件木马测试信号

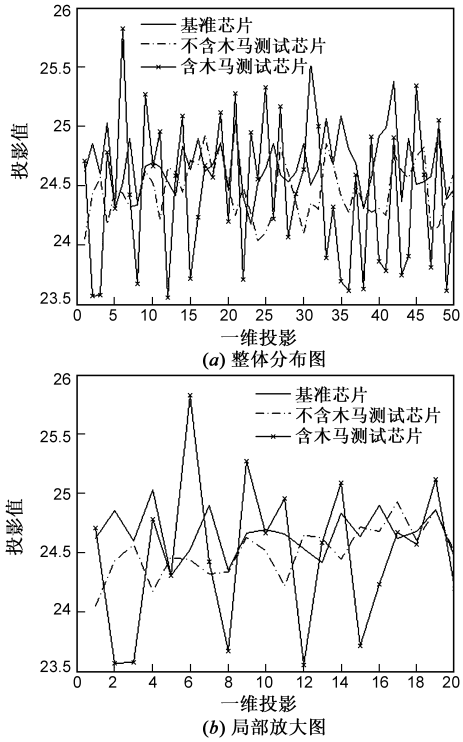


图5　采用PP分析的硬件木马检测典型结果

投影值分布明显更为接近(AID = 31.23),远小于基准信号与含硬件木马测试信号投影值之间的偏离程度(AID = 55.62).

实验表明:以负熵为投影指标、AID 为判定指标的 PP 对芯片旁路信息特征提取与识别的能力比 PCA(K-L 变换)更高,但计算代价有较大幅度增加.以实验针对的 50 × 100 维原始数据为例,在普通 PC 机上 PP 法分析耗时约 9s,是 K-L 变换法分析耗时的近 100 倍.随着数据维数增加,PP 法耗时增幅更加明显.由于硬件木马检测对实时性要求不高,相对于芯片的安全性需求来说,PP 检测方法的计算代价仍然可以接受.

5　结论

基于区域划分、随机选优测试向量生成及采用负熵指标的 PP 技术,能够将高维、分布复杂的芯片旁路信号数据映射到低维子空间,便于对样本数据分布特征进行分析与识别,为实现芯片硬件木马无损对照检测提供了一条值得探索的新途径.为了提高硬件木马检测效率,需要研究有效的全局优化算法,降低 PP 寻优耗时.采用遗传算法等智能优化算法是一条可行的途径.此外,本文通过随机选优生成测试向量,工作量小,但没有考虑芯片关键操作与关键指令的影响.下一步可研究有效的电路划分方法[12],通过合理的划分来生成更有效的测试向量集,并实现硬件木马的精确定位.

参考文献

[1] Tehranipoor M, Koushanfar F. A survey of hardware trojan taxonomy and detection[J]. IEEE Design & Test of Computers, 2010, 27(1): 10 – 25.

[2] 王晨旭,姜佩贺,喻明艳.芯片级木马检测技术研究综述[J].半导体技术,2012,37(5):341 – 346.
Wang C X, Jiang P H, Yu M Y. Survey of hardware trojan horse detection on chip[J]. Semiconductor Technology, 2012, 37(5): 341 – 346. (in Chinese)

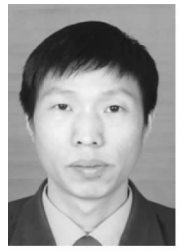
[3] Koushanfar F, Mirhoseini A. A unified framework for multimodal submodular integrated circuits trojan detection[J]. IEEE Transactions on Information and Security, 2011, 6(1): 162 – 174.

[4] 陈开颜,张鹏,邓高明等.物理可观测下 DES 的安全性研究[J].电子学报,2009,37(11):2389 – 2395.
Chen K Y, Zhang P, Deng G M. Research on the DES physical observable security[J]. Acta Electronica Sinica, 2009, 37(11): 2389 – 2395. (in Chinese)

[5] Jin Y, Makris Y. Hardware trojan detection using path delay fingerprint[A]. IEEE International Workshop on Hardware-Oriented Security and Trust (HOST)[C]. Anaheim: IEEE

Computer Society,2008.51 – 57.
[6] Agrawal D,Baktir S,Karakoyunlu D,et al.Trojan detection using IC fingerprinting[A].IEEE Symposium on Security and Privacy[C].Berkeley:IEEE Computer Society,2007.296 – 310.
[7] Banga M,Hsiao M.A region based approach for the identification of hardware Trojans[A].IEEE International Workshop on Hardware-Oriented Security and Trust(HOST)[C].Anaheim:IEEE Computer Society,2008.40 – 47.
[8] Wei S,Potkonjak M.Scalable hardware trojan diagnosis[J].IEEE Transactions on Very Large Scale Integration (VLSI) Systems,2012,20(6):1049 – 1057.
[9] 付强,赵小勇.投影寻踪模型原理及其应用[M].北京:科学出版社,2006.29 – 35.
[10] Alex C B.Preventing integrated circuit piracy using reconfigurable logic barriers[D].Ames:Iowa State University,2009.78 – 80.
[11] Zhang P,Deng G M,Zhao Q.An Automatic Experimental Platform for Differential Electromagnetic Analysis on Cryptographic ICs[A].Proceedings of the Second International Symposium on Test Automation & Instrumentation-ISTAI 2008[C].Beijing:World Publishing Corporation,2008.1078 – 1082.
[12] 朱文兴,程泓.VLSI 电路划分问题的分散搜索算法[J].电子学报,2011,40(6):1207 – 1212.
Zhu W X,Cheng H.Scatter search algorithm for VLSI circuit partitioning [J].Acta Electronica Sinica,2011,40(6):1207 – 1212.(in Chinese)

作者简介



张 鹏(通信作者) 男,1976 年 2 月出生,湖北罗田人.2010 年于军械工程学院获得博士学位.现为信息保障技术重点实验室博士后,主要研究方向为芯片安全防护技术.
E-mail:zhangp210@163.com

王新成 男,1969 年 12 月出生,湖南娄底人,2008 年于北京邮电大学获得博士学位.现为信息保障技术重点实验室高级工程师,主要研究方向为集成电路芯片设计.