

旁路信号主成分分析的欧式距离硬件木马检测

苏 静^{1,2}, 赵毅强¹, 何家骥¹, 刘沈丰¹

(1 天津大学 电子信息工程学院, 天津 300072; 2 天津科技大学 计算机学院, 天津 300222)

摘 要: 针对集成电路中的硬件木马问题, 利用旁路信号分析技术, 设计了一种基于集成电路芯片的硬件木马检测模型. 在对提取出的旁路信号进行主成分分析降维基础上, 运用欧式距离分类法进行硬件木马的分类识别和检测. 最后运用功耗分析的方法进行了算法有效性验证.

关键词: 硬件木马; 主成分分析; 欧式距离; 旁路分析; 木马检测

中图分类号: TN918

文献标识码: A

文章编号: 1000-7180(2015)01-0001-04

Hardware Trojan Detection Based on Euclidian Distance of PCA on Side-channel

SU Jing^{1,2}, ZHAO Yi-qiang², HE Jia-ji¹, LIU Shen-feng¹

(1 School of Electronics and Information Engineering, Tianjin University, Tianjin 300072, China;

2 School of Computer Science and Information Engineering, Tianjin University of Sci&Tech, Tianjin 300222, China)

Abstract: In order to solve the hardware trojan problem in the integrated circuits, a new model of hardware trojan detection is proposed in this paper based on the side channel analysis. The new model uses the Euclidian distance classification method to achieve the detection of hardware trojan, after getting the reduction of dimensionality by PCA on side-channel. Finally the effectiveness of the model and the algorithm was validated on power side-channel.

Key words: hardware Trojans; principal component analysis; Euclidian distance; side channel analysis; Trojans detection

1 引言

与利用计算机软件系统漏洞侵入窃取信息的病毒程序和软件木马不同, 硬件木马是指在集成电路芯片设计或制造过程中所植入的多余电路的统称, 目的是使电路在某些特定条件下失效或泄露信息^[1]. 一旦芯片被恶意植入木马, 信息系统的安全性、可靠性将受到挑战, 随时可能遭到攻击、破坏, 导致系统瘫痪和敏感信息泄露.

对芯片硬件木马进行检测, 传统方法是对芯片进行破坏性检测. 近年来出现的基于旁路信号分析(side channel analysis)的硬件木马检测技术^[2], 是通过原始电路与待测试电路之间旁路测量信号的差异来检测硬件木马, 因其具有无损伤、低开销、高

性能等优点, 成为国际学术界与产业界的研究热点. 当前典型的基于旁路信号检测硬件木马的方法大多集中在利用旁路信号的空间变换与压缩进行特征提取, 进而对基准芯片与测试芯片的旁路信号特征进行刻画与差异判别. 文献[3]中首次提出采用电路的功耗信息来检测硬件木马的方法; 文献[4]中通过K-L变换对旁路功耗信号建立“指纹”并进行比对检测; 文献[5]中利用门级电路时序及功耗特征检测木马; 文献[6]中通过线性规划与奇异值分解的方法检测木马.

本文提出一种基于旁路信号的木马分类检测模型, 通过对低秩信号上的主成分特征提取, 将芯片高维旁路信号投影到低维子空间, 在此基础上, 运用欧式距离分类算法进行标准芯片和木马芯片的分类识

收稿日期: 2014-03-22; 修回日期: 2014-05-17

基金项目: 国家自然科学基金项目(61376032); 天津市自然科学基金重点项目(12JCZDJC20500)

别,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的检测.

2 基于 PCA 的数据降维处理

主成分分析(PCA)是模式识别中一种最为简单而有效的特征提取方法,其目的是用数量较少的特征对高维样本进行描述,即在低维空间中保留尽可能多的方差,或尽可能保持原有数据的属性以达到降低特征空间维数的目的^[7-8].

根据量纲和变化幅度不同带来的影响,首先要对数据集进行归一化处理;归一化的样本数据 PCA 过程如下:假设特征集由 l 个样本组成,即包含 l 个特征向量,每个特征向量有 n 个特征值,即特征向量的维数是 n ,数据零值化处理后构成的特征集矩阵

为: $X_{n \times l} = (x_1, x_2, \dots, x_l)$, 其中 $x_i \in R^n$ 且 $\sum_{i=1}^n x_i = 0$, 则样本协方差矩阵为

$$C = \frac{1}{l} \sum_{i=1}^l x_i x_i^T \quad (1)$$

求样本协方差矩阵 C 的特征值和特征向量,也就是求解以下问题:

$$\lambda_i u_i = C u_i, i = 1, 2, \dots, n \quad (2)$$

式中, λ_i 是 C 的一个特征值, u_i 是对应的特征向量;把 n 个特征值由大到小排列,取前 k 个特征值对应的特征向量构成矩阵 $U_{n \times k} = (u_1, u_2, \dots, u_k)$, k 值通过前 k 个分量的方差贡献率 η 来确定,当 η 大于设定的阈值(本文取 95%) 时,就认为前 k 个分量包含了原数据的主要信息.

$$\eta = \frac{\sum_{i=1}^k \lambda_i}{\sum_{j=1}^n \lambda_j} \quad (3)$$

最后对 $X_{n \times l}$ 做如下正交变换:

$$S = U^T X \quad (4)$$

新的分量 S 称为主分量,特征集由 n 维降到了 k 维,而且 l 个 k 维数据之间是相互独立的.

3 基于类中心的欧式距离分类检测方法

3.1 欧氏距离

欧式距离又称泛数,被广泛应用于向量间的距离度量:

设有 M 个类别 $\omega_1, \omega_2, \dots, \omega_M$. 每类有 N_i 个样品,如 ω_i 类,可表示为

$$X^{(\omega_i)} = (X_1^{(\omega_i)}, X_2^{(\omega_i)}, X_3^{(\omega_i)}, \dots, X_{N_i}^{(\omega_i)})^T$$

对于任意待识别的样品 $X = (x_1, x_2, x_3, \dots, x_n)$, 计算基于类中心的欧式距离:

$$d^2(X, \omega_i) = (X - \overline{X}^{\omega_i})^T (X - \overline{X}^{\omega_i}) \quad (5)$$

式中, $\overline{X}^{\omega_i}$ 为第 i 类的类中心. 比较 x 到各类的距离如满足下式, 则 $X \in \omega_i$.

$$d(X, \overline{X}^{\omega_i}) < d(X, \overline{X}^{\omega_j}) j = 1, 2, \dots, M, i \neq j \quad (6)$$

3.2 实现方法

基于类中心的欧式距离分类方法对数据集进行分类识别的过程如下:

(1) 设有 M 个类别 $\omega_1, \omega_2, \dots, \omega_M$, 对每类样本 X_i , 分别计算类中心 $\overline{X}^{\omega_i}$;

(2) 计算待测样品 X 与训练集里每类样本 X_i 的欧式距离 $d^2(X, \omega_i)$;

(3) 循环计算待测样品和训练集中各类中心距离, 找出与待测样本最近的已知类别, 该类别就是待测样品的类别.

4 硬件木马检测方法

4.1 硬件木马检测流程

文中检测方法基于如下假设: 同批次电路芯片中能获得 N 个已经确认无硬件木马的集成电路芯片 ($K_1, K_2, \dots, K_N$) 和 M 个已确认植入同种硬件木马的集成电路芯片 ($L_1, L_2, \dots, L_M$). 文中的检测问题可描述为: 如何判断同批次其他集成电路芯片是否含有硬件木马. 其木马检测流程如图 1 所示^[9].

4.2 硬件木马检测方案

基于上述检测流程, 给出本文基于旁路信号主成分分析和欧式距离的硬件木马分类检测具体方案.

Step1: 旁路信息采集. 对 N 个无木马的标准芯片, M 个植入木马的木马芯片和 1 个待测芯片, 均选择 L 个测试向量, 输入芯片使之正常运行, 对芯片产生的功耗旁路信号进行采样, 采样深度为 E , 对应每个芯片可形成一 $L \times E$ 阶轨迹矩阵. 可分别得到标准芯片、木马芯片和待测芯片的轨迹矩阵分别记为

$$B_k = \{b(i, j) \mid i = 1, 2, \dots, L; j = 1, 2, \dots, E\} (k = 1, 2, \dots, N),$$

$$T_p = \{t(i, j) \mid i = 1, 2, \dots, L; j = 1, 2, \dots, E\} (p = 1, 2, \dots, M), P = \{p(i, j) \mid i = 1, 2, \dots, L; j = 1, 2, \dots, E\}.$$

Step2: 基于 PCA 的信息特征降维. 合并已知

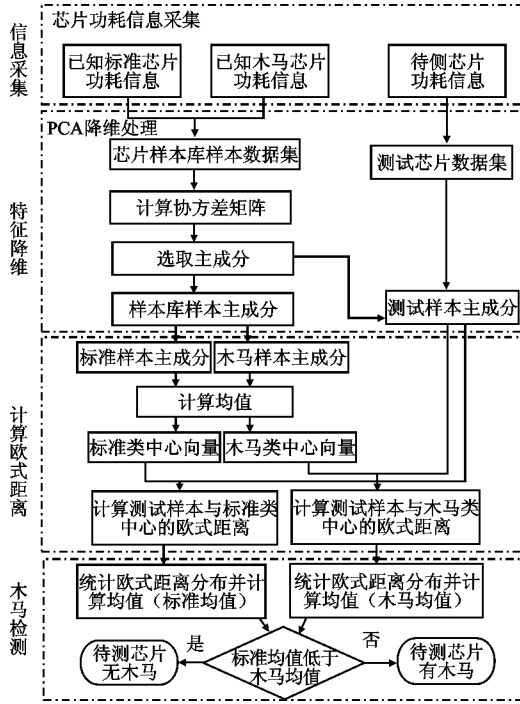


图 1 硬件木马检测流程图

标准芯片和木马芯片的全部功耗轨迹矩阵可构成样本库样本数据集矩阵 $X_{(N+M)L \times E}$, 计算样本数据集的协方差矩阵 $S_{E \times E}$, 取得 $S_{E \times E}$ 的特征值, 以及和特征值对应的特征向量 $C_{E \times E}$. 根据一定的贡献率, 本文选择 95%, 选取 $C_{E \times E}$ 的前 m 列, 使得

$$(\lambda_1 + \lambda_2 + \dots + \lambda_m) / (\lambda_1 + \lambda_2 + \dots + \lambda_E) \geq 95\%.$$

这时对应的 m 个主特征值对应的特征向量保留了原信号的足够多的信息, 用这 m 个主特征向量计算得到样本库样本主成分 $X_{(N+M)L \times m} = X_{(N+M)L \times E} C_{E \times m}$ 和待测芯片样本主成分 $P_{L \times m} = P_{L \times E} C_{E \times m}$.

Step3: 计算欧式距离. 根据已知芯片样本库的样本分类属性, 将样本库样本主成分 $X_{(N+M)L \times m}$ 分离为标准芯片样本主成分 $X_{NL \times m}$ 和木马芯片样本主成分 $X_{ML \times m}$, 分别计算两类样本主成分的中心向量, 得到标准类中心向量和木马类中心向量. 逐样本计算测试样本主成分 $P_{L \times m}$ 与两类中心向量的欧式距离并存储.

Step4 测试芯片木马检测. 分别统计测试芯片样本与两类中心向量的欧式距离分布情况, 并计算距离均值, 寻找与测试芯片样本最接近的已知类中心, 即比较欧式距离均值的大小. 如果测试芯片样本与标准类中心的欧式距离均值低于与木马类中心的距离均值, 即可判别该芯片没有硬件木马, 相反即可判别该芯片含有硬件木马.

5 硬件木马检测实验

5.1 硬件木马检测平台设计

图 2 中描述了基于 FPGA 的硬件木马检测平台的总体架构. 该系统主要由待测芯片、直流电源、信号探头、高性能数字示波器和 PC 上位机五个部分组成. 在硬件木马检测过程中, 利用信号探头对运行中的芯片的侧信道信息进行采样, 送至示波器中显示和存储, 然后再将测试数据上传至 PC 机进行数据分析. 在计算机上通过 MATLAB 编程实现标准电路和木马电路的特征提取和欧式距离分类检测, 从而实现对待测芯片的硬件木马分类检测^[10-11].

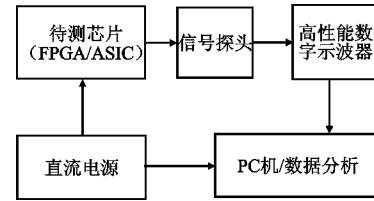


图 2 硬件木马检测平台整体架构

5.2 硬件木马检测电路设计

本文基于时序型硬件木马的载体电路进行硬件木马检测的数据分析实验^[12]. 按照图 3 中基于计数器的时序型硬件木马载体电路的设计方法, 设计一种基于定时器的硬件木马, 这是一种具有代表性的典型硬件木马结构, 能够使木马在特定时间激活. 当计数器记满归 0 时, 构成计数器的所有触发器都发生翻转产生较大功耗.

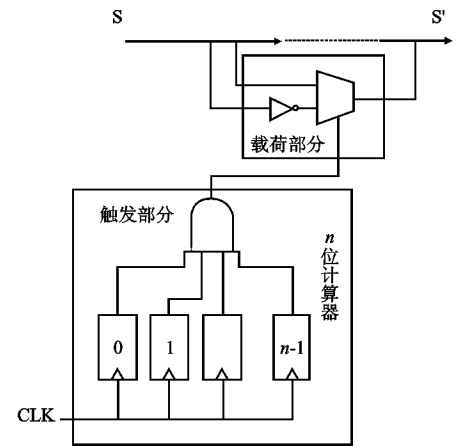


图 3 基于时序逻辑的硬件木马

5.3 基于欧式距离的分类检测算法

算法 1 木马分类检测

输入: 待测芯片的旁路信号矩阵, 即多向量样本 Sample $[N]$

输出: Y/N , 即待测芯片是否含有硬件木马

Function $y = \text{Euclid}(\text{sample})$

%加载已知芯片旁路信号样本数据

Load templet pattern;

%计算标准芯片和木马芯片的样本数据中值点

For $i = 1:2$

temp = mean(pattern(i), feature);

$p(:, i) = \text{temp}$

end;

%分别计算待测芯片旁路信号矩阵与两类样本库中值

向量的欧几里德距离

For $i = 1:2$

For $j = 1:N$

$d = (\text{sample}(j) - p(:, i))' * (\text{sample}(i) - p(:, i));$

sum_d = sum_d + d;

end

%比较均值距离

if $d_{\min} > \text{sum_d}/N$

$d_{\min} = \text{sum_d}/N;$

%类别 0 为标准芯片 1 为木马芯片

$y = i - 1;$

end

end

return y;

5.4 实验结果

分别对标准芯片和植入不同面积木马电路的芯片进行多次数据采样, 对每个测试激励向量重复采样 1 000 次, 作为一组功耗旁路初始数据, 用以模拟一块测试芯片的旁路信号, 保存足够多组数据, 每种情况采集 100 组实验测试, 并将数据导入 PC 中. 随机选取 20% 数据作为测试样本, 其余均为训练样本. 使用 MATLAB 对硬件木马的检测编写程序, 对全部样本的侧信道信息提取主成分, 选取累计方差贡献率达到 95% 以上的所有主成分. 计算测试样本与训练样本类中心的欧氏距离均值, 进行木马分类检测的结果测试, 以验证算法的有效性. 实验结果如表 1 所示.

表 1 实验结果

实验参数	标准芯片	面积为 20% 的木马芯片	面积为 8% 的木马芯片	面积为 4% 的木马芯片
训练样本数	80 000	80 000	80 000	80 000
测试样本数	20 000	20 000	20 000	20 000
原始维度	10 000	10 000	10 000	10 000
PCA 维数	1 708	1 708	1 708	1 708
样本芯片识别率/%	100	100	95	90

运用本文提出的方法, 可以识别测试芯片是否含有硬件木马, 测试数据准确率可以达到 90% 以上, 测试准确率会随着木马面积增大略有降低. 采用 PCA 特征提取算法可以较大幅度地降低原始数据集的维数, 同时保留了原始数据的主要信息且去除了数据间的相关性, 对计算量和识别率都有一定的改善.

参考文献:

- [1] Wang X, Tehranipoor M, Plusquelic J. Detecting malicious incursions in secure hardware: challenges and solutions[C]// 1st IEEE International Workshop on Hardware-Oriented Security and Trust (HOST). Anaheim, CA: IEEE Press, 2008: 15-19.
- [2] Tehranipoor M, Koushanfar F. A survey of hardware trojan taxonomy and detection[J]. IEEE Design & Test of Computers, 2010, 27(1): 10-25.
- [3] Wang X. Hardware trojan detection and isolation using current integration and localized current analysis[C]// Symp Defect & Fault Tolerance VLSI Syst. France Grenoble, 2008: 87-95.
- [4] Agrawal D, Baktir S, Karakoyunlu D, et al. Trojan detection using IC fingerprinting[C]// IEEE Symposium on Security and Privacy. USA, Berkeley, 2007: 296 - 310.
- [5] Alkabani Y, Koushanfar F. Efficient approximations for IC Trojan detection[C]// International Conference on Computer-Aided Design (ICCAD). USA: San Jose, 2009.
- [6] Potkonjak M, Nahapetian A, Nelson M, et al. Hardware trojanhorse detection using gate-level characterization[C]// Design Automation Conference (DAC). USA: Sanfrancisco, 2009.
- [7] 蒋玉娇, 王晓丹. 一种基于 PCA 和 ReliefF 的特征选择方法[J]. 计算机工程与应用, 2010, 46(26): 170-172.
- [8] 西奥多里蒂斯, 李晶皎. 模式识别[M]. 北京: 电子工业出版社, 2012.
- [9] 赵崇征, 邓高明. 基于旁路分析的集成电路芯片硬件木马检测[J]. 微电子学与计算机, 2011, 28(11): 5-9.
- [10] Koushanfar F, Mirhoseini A. A unified framework for multimodal submodular integrated circuits Trojan detection[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(1): 162-174.

(下转第 10 页)

实验 2 来看, F 值的平均值未达到 90% 以上的较高水平, 也表明该算法存在提升的空间. 一是由于本文仅使用了少有的几条规则, 如将问题定性、法律法规等作为关键维度, 并没有考虑从语义和最大匹配度的角度将与已分文档相似的文件直接分类, 同时忽略了文本相似度对分类的影响; 二是由于部分样本中因为分类界限模糊而存在错误样本, 这些错误样本对分类的准确度、召回率产生了破坏性影响; 三是在分类过程中强调规则和同义词对分类的影响, 并未制衡关键维度与非关键维度的影响程度. 以上几点将在以后的工作中进行优化, 使分类效果得到进一步的提升.

5 结束语

本文将信息抽取、文本分类技术应用于处理审计报告之中, 提出的面向审计领域的新方法, 有效克服了审计报告中的出现的样本高度不均衡、短文本特征稀疏和问题分类界限模糊对分类性能的影响, 实现了将审计问题按性质进行分类的目的, 获得了较好的准确率和召回率^[10-12].

该方法在处理审计报告的问题分类上仍具有改进的空间, 下一步工作将考虑结合相似度算法与基于规则方法来计算短文本中是否含有指定的规则, 或含有与规则相似度较高的短句, 加强规则对分类结果的影响, 进一步提高分类效果.

参考文献:

- [1] 苏金树, 张博锋, 徐昕. 基于机器学习的文本分类技术研究进展[J]. 软件学报, 2006(17): 1848-1859.
- [2] 李惠娟, 高峰, 管晓宏, 等. 基于贝叶斯神经网络的邮件过滤方法[J]. 微电子学与计算机, 2005, 22(4): 107-111.
- [3] 吕震宇, 林永民, 赵爽, 等. 基于同义词词林的文本特征选择与加权研究[J]. 情报杂志, 2008(5): 130-132.
- [4] 宁亚辉, 樊兴华, 吴渝. 基于领域本体的短文本分类[J]. 计算机科学, 2009, 36(3): 142-145.
- [5] 王细薇, 樊兴华, 赵军. 一种基于特征扩展的中文短文本分类方法[J]. 计算机应用, 2009, 29(3): 843-845.
- [6] 朱远平, 戴汝为. 基于 SVM 决策树的文本分类器[J]. 模式识别与人工智能, 2005, 18(4): 412-416.
- [7] 田久乐, 赵蔚. 基于同义词词林的词语相似度计算方法[J]. 吉林大学学报, 2010, 28(6): 602-608.
- [8] 陈沈焰, 吴军华. 基于本体的概念语义相似度计算及其应用[J]. 微电子学与计算机, 2008, 25(12): 96-99.
- [9] 李生琦, 天巧燕, 汤承. 基于《知网》词汇语义相关度计算的消歧方法[J]. 情报学报, 2009, 28(5): 706-711.
- [10] James G Shanahan, Norbert Roma. Boosting support vector machines for text classification through parameter-free threshold relaxation[C]// CIKM'03. New Orleans, 2003.
- [11] Joachim T. Text categorization with support vector machines; Learning with many relevant features [C] // Proceedings of the 10th European Conference on Machine Learning, Spain; Barcelona, 1998.
- [12] Takahashi F, Abe S. Decision-tree-based multiclass support vector machines[C]// Proceeding of the 9th International Conference on Neural Information Processing, Singapore, 2002.

作者简介:

伍 洋 男, (1989-), 硕士研究生. 研究方向为信息抽取、数据挖掘. E-mail: angenimy@sina.com.

钟 鸣 男, (1982-), 博士, 讲师. 研究方向为数据库理论与系统、图形数据库、大数据、信息检索.

姜 艳 女, (1983-), 硕士研究生. 研究方向为审计信息化.

李石君 男, (1964-), 博士, 教授. 研究方向为 Web 搜索与挖掘、数据挖掘、大数据.

(上接第 4 页)

- [11] Lamech C, Rad R, Tehranipoor M, et al. An experimental analysis of power and delay signal-to-noise requirements for detecting trojans and methods for achieving the required detection sensitivities [J]. IEEE Transactions of Information Forensics and Security, 2011, 6(3): 142-155.

- [12] 刘长龙, 赵毅强. 基于侧信道分析的硬件木马建模与优化[J]. 华中科技大学学报, 2013, 41(2): 53-57.

作者简介:

苏 静 女, (1979-), 博士研究生, 副教授. 研究方向为信息安全、机器学习. E-mail: sjnicelife@163.com.