

一种基于核最大间距准则的 硬件木马检测新方法

李雄伟, 王晓晗, 张 阳, 陈开颜, 徐 璐

(军械工程学院信息工程系, 河北石家庄 050003)

摘 要: 在功耗旁路信号统计模型的基础上, 提出了一种基于核最大间距准则的硬件木马检测方法, 将原始功耗旁路信号映射到高维空间, 使其具有更高的可分性, 然后再投影到低维子空间, 从而发现原始数据中的非线性差异特征, 实现功耗旁路信号的非线性特征提取与识别. 针对 AES 加密电路中木马电路的检测实验表明, 该方法测得超出检测边界的样本数(792)多于 Karhunen-Loève 变换(400), 取得更好的检测效果.

关键词: 集成电路; 硬件木马; 旁路分析; 核函数; 最大间距准则

中图分类号: TN918

文献标识码: A

文章编号: 0372-2112 (2017)03-0656-06

电子学报 URL: <http://www.ejournal.org.cn>

DOI: 10.3969/j.issn.0372-2112.2017.03.023

A New Hardware Trojan Detection Method Based on Kernel Maximum Margin Criterion

LI Xiong-wei, WANG Xiao-han, ZHANG Yang, CHEN Kai-yan, XU Lu

(Department of Information Engineering, Ordnance Engineering College, Shijiazhuang, Hebei 050003, China)

Abstract: A hardware Trojan detection method based on kernel maximum margin criterion and an improved detection method are proposed on basis of the statistical model of power side-channel signal. The methods can map the raw power side-channel signal into a higher dimensional space, where it had a higher separability, and then it is projected onto a low-dimensional subspace, so that non-linear characteristics of differences in the raw data are found, and nonlinear characteristics extraction and recognition of power side-channel signal are achieved. The detection experiment against the Trojan circuit in AES encryption circuit shows that, the number of samples beyond the detection boundary by the method (792) is more than Karhunen-Loève Transform (400), which gets a better detection result.

Key words: integrated circuit; hardware Trojan; side channel analysis; kernel method; maximum margin criterion.

1 引言

集成电路(Integrated Circuit, IC)由于体积小、性能好、可靠性高等优点,被广泛应用于军事、航空、医疗等领域,成为人们生活中不可或缺的工具.然而,由于当前IC芯片的设计与制造分离,导致IC芯片面临越来越多的安全威胁^[1],主要包括:①赝品IC;②逆向工程;③硬件木马(Hardware Trojan).其中,硬件木马能够在特定条件下实现破坏功能或者泄露芯片中的秘密信息,给芯片及其应用安全带来了极大威胁.因此,加强IC芯片中硬件木马的检测与防护研究显得尤为迫切和重要.

目前,国内外的检测方法主要有破坏性检测、逻辑

测试和旁路分析等^[2].其中旁路分析(Side Channel Analysis, SCA)方法通过检测原始电路与待测电路之间旁路信号的差异来实现木马检测,相比较其他几种方法而言,具有成本低、灵敏度高等特点,成为当下主流的检测方法^[3].基于旁路分析的硬件木马检测主要是寻找“金片”(不含木马的IC)与待测电路的旁路信号之间的差异来检测木马,其相关研究主要分为两部分:获取反映木马特征的旁路信号和特征提取与差异判别.前者主要是研究硬件木马对芯片运行过程中产生的不同类型的旁路信号的影响,以一种或几种旁路信号建立“指纹”并通过比对来检测硬件木马,例如功耗旁路信号^[4]、热信号、电路延迟信息以及多参数等.后者则致

力于通过信号处理等方法寻找旁路信号之间的差异,如 Karhunen-Loève 变换(简称 K-L 变换)^[4]、奇异值分解^[5]、投影寻踪^[6]等,该类方法的主要思路是以某种投影指标来构建投影子空间,通过比对子空间中的投影来检测木马。

在采用旁路分析检测硬件木马的过程中,噪声是主要干扰因素。由于噪声的影响,旁路信号随时间作无规律、随机性的变化,每次测得的旁路信号形式不确定,很难从少量信号中发现潜藏的木马,需进行统计分析以检测硬件木马,而此时测得的“金片”和含小规模木马 IC 的旁路信号相互交叠,使得采用信号处理方法 K-L 变换进行木马检测时,效果并不理想。鉴此,本文根据功耗旁路信号的统计模型,提出了一种新的信号变换分析方法,通过核函数方法(kernel method)将旁路信号投影到更高维空间,使“金片”和含木马 IC 的旁路信号具有更高的可分性,从而实现硬件木马的检测。

2 功耗旁路信号的统计模型及问题分析

基于功耗旁路信号的硬件木马检测是在同等条件下运行“金片”与待测 IC,并测量其工作电流,通过比较电流的差异来判断待测 IC 中是否含有木马。根据文献[7]可知,对于同种工艺的集成电路(无论是否含有木马),每一时刻的能量消耗均服从同一正态分布。此时,离散旁路信号($X(t_1), X(t_2), \dots, X(t_n)$)为高斯信号,其联合分布为 n 维高斯分布,若将一条旁路信号看作 n 维空间的一个样本点,由于相邻时刻的能量消耗之间存在一定的相关性,并且不同时刻的噪声波动范围不固定(执行的操作、运算不同),一组旁路信号在该空间中的分布构成一个超椭球。则“金片”与含木马 IC 的功耗旁路信号可以看作是大小和形状相同而位置不同的两个超椭球,噪声扰动决定了超椭球的半径,木马的触发、运行时间、大小等条件,决定了两个超椭球的相对位置,木马检测可以看作是分布相同的两类区分问题。

对于该模型而言,文献[4]中的 K-L 变换,其本质是以样本方差为指标来寻找一组正交的投影方向,通过比对两个超椭球在每个投影方向上的投影的差异来判断是否含有木马,虽然仿真实验结果表明 K-L 变换能够检测出电路中的木马,但是仍然存在一定的改进空间。首先,相比于仿真实验,物理实验中噪声扰动更大,可检测到的木马规模不如仿真理想。其次,以样本方差为指标寻找的投影方向虽然也能用于体现差异,但对于区分两类而言却不是最优的,如图 1(a),以二维子空间为例,其中浅色样本代表“金片”的旁路信号样本,深色样本代表含木马 IC 的旁路信号样本,直线 d 表示由木马引起的两种信号样本的位置偏移, a 和 b 为通过 K-L 变换得到的两个正交投影方向,沿投影方向的深色区

域和浅色区域分别为两种信号样本在该方向上的投影,很明显这两个投影方向不能有效的区分样本,而投影方向 c 仍能有效区分样本,这种投影方向是本文需要的投影方向。最后,当木马再度减小时,两个超椭球相互重叠,此时线性投影方向无法有效区分样本,如图 1(b),即使最优投影方向上的投影也出现重叠。通过分析采用 K-L 变换检测木马的几点不足可知,不同类别数据间的可分离性是木马检测过程中的主要干扰因素,木马越小,噪声干扰越大,“金片”和待测 IC 的旁路信号的可分离性越差,越难检测出木马,若能有效提高数据间的可分性,将极大增强较小木马的检测效果。

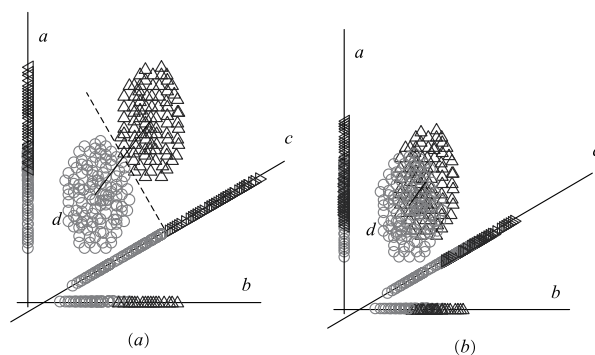


图1 投影方向分析

3 核最大间距准则

3.1 概述

事实上,注重降维的线性方法(以某种指标寻找线性投影方向)无法从根本上改变原始数据的可分离性,而非线性方法(寻找非线性投影方向)能够增强数据间的线性可分离性^[8]。对于前文中两个重叠的超椭球(高维)而言,直接寻找区分两者的非线性映射是不可行的,一方面这种非线性映射十分复杂,很难获取;另一方面,计算过程中很容易造成维数灾难,实用价值低。因此,本文引入核函数方法来解决上述问题。

核函数方法是人们为了解决非线性变换中的维数灾难和推广能力差等缺陷,在线性方法的基础上推广的一种非线性分析方法^[9]。其基本思想是采用核函数内积计算的方式将原始数据映射到更高维空间(计算上的高维),在该空间中样本具有更高的可分性,然后采用线性方法进行特征提取(寻找线性投影方向)。在计算过程中使用者不需要知道非线性映射具体是什么形式,以及映射到高维空间中的投影作何分布。该方法虽然是一种非线性方法,但是整个求解的过程都是通过线性手段来完成的,根据选取的线性方法不同(不同的投影指标),实现不同的非线性变换。

3.2 基于核最大间距的木马投影分析

对于两类区分问题,理想的投影方向应当使两类

样本投影尽可能的分离,即两类投影之间的距离尽可能大,样本投影方差(投影范围)尽可能小,因此,本文选取最大间距准则^[10]作为核函数方法中的线性手段.

令不含木马的功耗轨迹记为类 $w_1 = \{\mathbf{x}_1^1, \dots, \mathbf{x}_{N_1}^1\}$, 含木马的功耗轨迹记为类 $w_2 = \{\mathbf{x}_1^2, \dots, \mathbf{x}_{N_2}^2\}$, N 表示样本总数,即 $N = N_1 + N_2$, 根据再生核理论, w_i 类样本在高维空间中样本投影的均值向量和类内离散度矩阵分别为:

$$(\mathbf{M}_i)_l = \frac{1}{N_i} \sum_{j=1}^{N_i} k(\mathbf{x}_l, \mathbf{x}_j), l=1 \dots N \quad (1)$$

$$\mathbf{S}(w_i) = \mathbf{P}(\mathbf{I} - \mathbf{1}_{N_i}) \mathbf{P}_i^T, i=1, 2 \quad (2)$$

其中, $k(\mathbf{x}_l, \mathbf{x}_j)$ 为核函数, $\mathbf{1}_{N_i}$ 为所有元素都为 $\frac{1}{N_i}$ 的矩阵, $\mathbf{I}$ 为单位矩阵, $\mathbf{P}_i$ 为 $N \times N_i$ 维矩阵, $(\mathbf{P}_i)_{NN_i} = k(\mathbf{x}_l, \mathbf{x}_j)$, $l=1 \dots N, j=1 \dots N_i$. 核最大间距准则方法求得的一组非线性正交投影方向即为矩阵 $\mathbf{H} = ((\mathbf{M}_1 - \mathbf{M}_2)(\mathbf{M}_1 - \mathbf{M}_2)^T - \sum_{i=1,2} \mathbf{S}(w_i))$ 的前 d 个特征值对应的特征向量 $\mathbf{A}_d = \{\mathbf{A}_1^d, \dots, \mathbf{A}_N^d\}$. 则样本 $\mathbf{x}_l$ 在投影方向 $\mathbf{A}_d$ 上的投影值 $z(\mathbf{x}_l)$ 为:

$$z(\mathbf{x}_l) = \sum_{j=1}^N A_j^d k(\mathbf{x}_j, \mathbf{x}_l), l=1 \dots N \quad (3)$$

由于核函数方法对核函数具有一定的不敏感性,只要参数选取恰当,不同的核函数可以达到同样的检测效果^[8],因此,本文选取常用的径向基(RBF)核函数 $k(\mathbf{x}, \mathbf{x}') = \exp(-\frac{\|\mathbf{x} - \mathbf{x}'\|^2}{\sigma^2})$ 进行计算.

3.3 方法改进

核函数方法是根据总样本个数来构建高维空间,通过计算一个样本与所有训练样本之间的核函数来进行高维空间中的特征抽取,若将每个核函数运算看作是两个样本之间的相互作用力,则每个样本在高维空间中的投影是所有样本对该样本施加一个合作力的结果,然而这种做法没有考虑已知的类信息,且由于样本个数的限制以及原空间中两类物体重叠度比较高等因素,该方法的区分效果可能不明显. 一个样本的邻样本距离该样本越近,对其作用力越大,反之则越小,在已知类信息的情况下,如果增大同类样本之间作用力的权重,减少不同类样本之间作用力的权重,则在高维空间中的两类样本投影区分更明显. 鉴此,本文利用样本已有的类信息简单的改进核最大间距准则,使高维空间中两类样本投影具有更高的可分性,具体做法为:通过设置式(4)中的两个参数 θ_1 和 θ_2 来改变样本间核函数(作用力)的权重,同类样本间的核函数运算用参数 θ_1 调整,不同类样本间的核函数用参数 θ_2 调整,即判断样本 $\mathbf{x}_l$ 和 $\mathbf{x}_j$ 是否属于同一类,若为同类,则执行 $k(\mathbf{x}_l, \mathbf{x}_j) = k(\mathbf{x}_l, \mathbf{x}_j) \times \theta_1$, 否则执行 $k(\mathbf{x}_l, \mathbf{x}_j) = k(\mathbf{x}_l, \mathbf{x}_j) \times \theta_2$.

$$\theta_2 = 2 - \theta_1, 1 < \theta_1 \leq 1.1 \quad (4)$$

由于无法预知高维空间中样本投影的分布,本文仅定性的分析加入的参数对高维空间中投影分布的影响. 前文提到 w_i 类样本在高维空间中样本投影的均值向量和类内离散度矩阵分别为 $\mathbf{M}_i$ 和 $\mathbf{P}_i(\mathbf{I} - \mathbf{1}_{N_i})\mathbf{P}_i^T$ (正定矩阵),其维数与所有的样本个数有关,可根据样本类别将 $\mathbf{M}_i$ 和 $\mathbf{P}_i$ 分别分成两个子矩阵,即 $\mathbf{M}_i = [\mathbf{M}_{i1}, \mathbf{M}_{i2}]$, $\mathbf{P}_i = [\mathbf{P}_{i1}, \mathbf{P}_{i2}]^T$, 加入参数后, $\mathbf{M}_1 = [\theta_1 \times \mathbf{M}_{11}, \theta_2 \times \mathbf{M}_{12}]$, $\mathbf{M}_2 = [\theta_2 \times \mathbf{M}_{21}, \theta_1 \times \mathbf{M}_{22}]$,

$$\begin{aligned} \mathbf{S}(w_1) &= \mathbf{P}_1(\mathbf{I} - \mathbf{1}_{N_1})\mathbf{P}_1^T \\ &= \begin{bmatrix} \theta_1^2 \mathbf{P}_{11}(\mathbf{I} - \mathbf{1}_{N_1})\mathbf{P}_{11} & \theta_1 \theta_2 \mathbf{P}_{11}(\mathbf{I} - \mathbf{1}_{N_1})\mathbf{P}_{12} \\ \theta_1 \theta_2 \mathbf{P}_{12}(\mathbf{I} - \mathbf{1}_{N_1})\mathbf{P}_{11} & \theta_2^2 \mathbf{P}_{12}(\mathbf{I} - \mathbf{1}_{N_1})\mathbf{P}_{12} \end{bmatrix} \\ &= \theta_2^2 \begin{bmatrix} \frac{\theta_1^2}{\theta_2^2} \mathbf{P}_{11}(\mathbf{I} - \mathbf{1}_{N_1})\mathbf{P}_{11} & \frac{\theta_1}{\theta_2} \mathbf{P}_{11}(\mathbf{I} - \mathbf{1}_{N_1})\mathbf{P}_{12} \\ \frac{\theta_1}{\theta_2} \mathbf{P}_{12}(\mathbf{I} - \mathbf{1}_{N_1})\mathbf{P}_{11} & \mathbf{P}_{12}(\mathbf{I} - \mathbf{1}_{N_1})\mathbf{P}_{12} \end{bmatrix}, \end{aligned}$$

$$\begin{aligned} \mathbf{S}(w_2) &= \mathbf{P}_2(\mathbf{I} - \mathbf{1}_{N_2})\mathbf{P}_2^T \\ &= \begin{bmatrix} \theta_2^2 \mathbf{P}_{21}(\mathbf{I} - \mathbf{1}_{N_2})\mathbf{P}_{21} & \theta_1 \theta_2 \mathbf{P}_{21}(\mathbf{I} - \mathbf{1}_{N_2})\mathbf{P}_{22} \\ \theta_1 \theta_2 \mathbf{P}_{22}(\mathbf{I} - \mathbf{1}_{N_2})\mathbf{P}_{21} & \theta_1^2 \mathbf{P}_{22}(\mathbf{I} - \mathbf{1}_{N_2})\mathbf{P}_{22} \end{bmatrix} \\ &= \theta_2^2 \begin{bmatrix} \mathbf{P}_{21}(\mathbf{I} - \mathbf{1}_{N_2})\mathbf{P}_{21} & \frac{\theta_1}{\theta_2} \mathbf{P}_{21}(\mathbf{I} - \mathbf{1}_{N_2})\mathbf{P}_{22} \\ \frac{\theta_1}{\theta_2} \mathbf{P}_{22}(\mathbf{I} - \mathbf{1}_{N_2})\mathbf{P}_{21} & \frac{\theta_1^2}{\theta_2^2} \mathbf{P}_{22}(\mathbf{I} - \mathbf{1}_{N_2})\mathbf{P}_{22} \end{bmatrix}. \end{aligned}$$

文献[11]指出,离散度矩阵的对角线元素决定了样本分布的扁圆程度,非对角线元素决定样本分布线性相关程度(扁的方向),则加入参数以后,高维空间中 $\mathbf{M}_1$ 和 $\mathbf{M}_2$ 之间的距离增大了,又因为 $\theta_2^2 < 1$, 类的分布 ($\mathbf{S}(w_i)$) 与改进前相比,分布范围更小一些,更扁一些,使两类样本的分离性增强,此时寻到的投影方向上的两类样本投影的差异更明显,检测效果会更好. 以二维平面图为例,图2为加入参数对高维空间中样本分布的影响示意图, Y 轴与 w_1 类相关, X 轴与 w_2 类相关,实线圆(假设分布为圆形)为加入参数前两类样本分布,虚线椭圆为加入参数后的两类样本分布,直线 Z 为投影方向,很明显加入参数后在方向 Z 上的投影具有更大

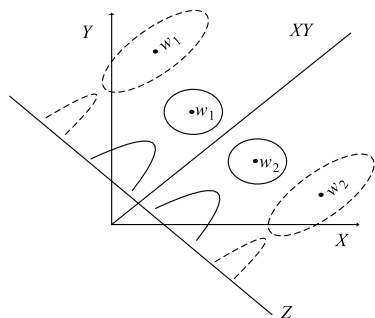


图2 参数对样本分布的影响

的可分离性.

3.4 木马检测算法设计

根据前文的分析,本实验将从统计的角度对旁路信号进行分析,算法 1 列出了木马检测过程中使用核最大间距准则对旁路信号进行变换的主要步骤,下面给出采用核最大间距准则的硬件木马检测方案.

算法 1 对旁路信号进行变换

输入:“金片”的旁路信号集 $L_1 (M * N)$,待测 IC 的旁路信号集 $L_2 (M * N)$

输出:变换后的旁路信号集 L'_1 和 L'_2

- 1: 读取旁路信号集 L_1 与 L_2 并计算特征向量集 Ψ
- 2: 计算两两样本间的核函数并生成矩阵 K
- 3: for all L_1 和 L_2 中的旁路信号 x_i do
- 4: 计算每条旁路信号与其他旁路信号的核函数 $k_{ij}(x_i, x_j)$
- 5: if (x_i 与 x_j 属于同一信号集 L) then
- 6: $k_{ij} = k_{ij} * \theta_1$
- 7: else then
- 8: $k_{ij} = k_{ij} * \theta_2$
- 9: end if
- 10: end for
- 11: 根据矩阵 K 计算两类样本在高维空间中的类间离散度矩阵 S_b 和类内离散度矩阵 S_w
- 12: for all 矩阵 K 中的元素 $k_{ij}(x_i, x_j)$ do
- 13: 根据 x_j 的类别将矩阵 K 分为两个子矩阵 P_1 和 P_2
- 14: 计算矩阵 P_1 和 P_2 的列均值作为高维空间中的类均值 M_1 和 M_2
- 15: 根据类均值 M_1 和 M_2 ,子矩阵 P_1 和 P_2 计算类间离散度矩阵 S_b 和类内离散度矩阵 S_w
- 16: end for
- 17: 计算矩阵 $S_b - S_w$ 的特征向量集 $\Psi (N$ 条)
- 18: * 对旁路信号 L_1 和 L_2 进行变换得到 L'_1 和 L'_2
- 19: for all L_1 和 L_2 中的旁路信号 x_i do
- 20: for all Ψ 中的特征向量 ψ_i do
- 21: 计算旁路信号在每个特征向量上的投影
- 22: end for
- 23: end for

Step 1 旁路信号的采集. 根据前文中的模型,对“金片”和待测 IC 施加同一测试向量,并分别测量电路在该测试向量下的功耗旁路信号,每个待测电路测量 m 条旁路信号,每条旁路信号的采样长度为 n ,分别获得“金片”的功耗旁路信号集 $L_1 = \{b(i, j) | i = 1, 2, \dots, m_1; j = 1, 2, \dots, n_1\}$ 和待测 IC 的功耗旁路信号集 $L_2 = \{t(i, j) | i = 1, 2, \dots, m_2; j = 1, 2, \dots, n_2\}$, 此处 $m_1 = m_2, n_1 = n_2$.

Step 2 构建核函数矩阵. 计算 L_1 和 L_2 中任两个样本的核函数,构建核函数矩阵 $K = \{k(i, j) | i = 1, 2, \dots, m_1 + m_2; j = 1, 2, \dots, m_1 + m_2\}$. 则

$$k(i, j) = \exp\left(-\frac{\|x_i - x_j\|^2}{\sigma^2}\right), x_i, x_j \in L_1 \cup L_2 \quad (5)$$

Step 3 利用式(1),式(2)以及 Step 2 中的核函数矩阵计算矩阵 H .

Step 4 计算矩阵 H 的特征向量集 Ψ ,利用式(3)计算功耗旁路信号集 L_1 和 L_2 在各个投影方向上的投影,并获取信号集 L'_1 和 L'_2 .

Step 5 通过比对信号集 L'_1 和 L'_2 的差异来判断是否含有木马.

4 实验验证

4.1 实验配置

实验平台配置如图 3,平台采用日本的 SASEBO 旁路攻击标准评估板,该实验板上的 XC5VLX30 FPGA 芯片中运行 AES (Advanced Encryption Standard) 加密算法,通过修改 FPGA 比特流来获取“金片”和含木马 IC. 实验中植入的木马为常开型,电路规模约占 AES 加密电路的 2%,主要功能是对分组密钥的某些数据位进行异或运算,根据运算的结果改变 SASEBO 评估板上信号灯的状态. 对于特定明文条件下才被激活的硬件木马,当木马被激活时,文中提到的检测方法也同样适用. 为了避免植入木马对原始电路布局等造成影响,在综合时采用 ISE 的增量编译技术.

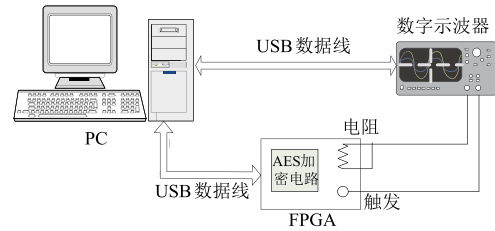


图3 旁路信号采集平台

该平台利用 PC 端用 LabVIEW 编写的虚拟仪器控制平台控制整个采集过程,采用 Tektronix DPO4104 示波器采集 FPGA 工作时的功耗旁路信号,整个采集过程中的数据传输都以 USB 数据线为媒介. 采集时,固定一组明文和密钥,采样频率设为 2.50GSa/s,采样时长为 0.4μs,每 1000 个采样点作为一条旁路信号,分别采得“金片”和含木马电路的功耗旁路信号各 1000 条,作为后期处理的样本集.

核函数中参数的选取直接影响检测效果,通过寻找最优参数 σ^2 (σ^2 代表核函数中的参数,下同) 来实现最优的检测结果. 本文主要遵循从大到小的原则(逐步增加非线性程度),设计了一种简单的遍历算法,从 1 开始,每次减少一个数量级,逐次遍历,直到能够检测出木马,或者遍历十次停止(此时认为检测不出木马).

4.2 实验结果分析

由于对离散旁路信号进行变换的本质是在一组正交投影方向上分别进行投影,只要某个方向上的投影

存在差异,即可判断含有木马.因此,本文以每个投影方向上“金片”样本投影的 $\mu \pm 3\sigma$ (σ 表示标准差,下同) 为检测边界,采用简单投票准则^[12] 对待测 IC 进行判别,认为待测 IC 的每个样本投影对判别的贡献都是相同的,若存在某个投影方向使得待测 IC 的样本投影超出检测边界的比例大于 $1/2$,则判定待测 IC 中含有木马,反之则不含木马.即分别统计待测 IC 在每个投影方向上落在 $\mu \pm 3\sigma$ 范围内的样本量与范围外的样本量,若范围外的样本数多于范围内的样本数则判定含有木马.因为实验采用 1000 条待测 IC 的旁路信号进行分析,因此设定检测阈值为 500,超出检测边界的样本数多于 500 则判定含有木马.

采用 K-L 变换的实验结果如图 4 所示,横坐标表示按照特征值大小排序的特征向量,纵坐标为每个特征向量上的投影值,深色部分为“金片”的投影分布,浅色部分为含木马 IC 的投影分布,两条黑色虚线为检测边界.经统计,K-L 变换超出 3σ 范围的样本投影数最多仅有 400 个(第二个特征向量),不能判断是否含有木马.

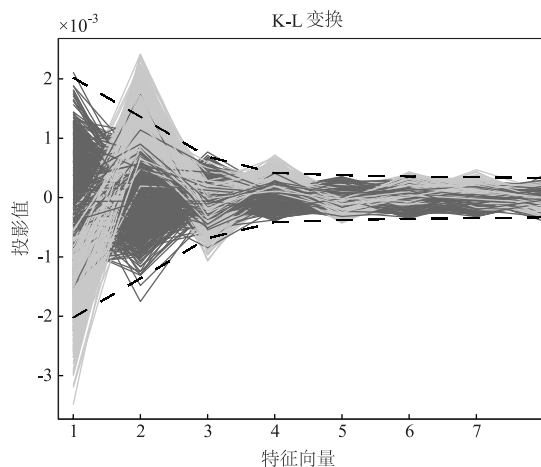


图4 基于K-L变换的木马检测

采用核最大间距准则的实验结果如图 5 所示,此时参数 σ^2 为 10^{-5} (遍历次数为 6 次).可以看出,在第二个特征向量上的样本投影区分较好,经过统计发现在该投影方向上超出边界的投影个数达到 792 个,能够检测出木马.

采用改进的核最大间距准则的实验结果如图 6 所示,此时参数 σ^2 为 10^{-3} (遍历次数为 4 次), θ_1 的取值为 1.01.可以看出,该方法在前四个投影方向上能够很明显的将两组信号分离(超出范围的样本数达到 1000),检测出木马.

实验结果表明,核最大间距准则测得检测边界外的样本数(792)多于 K-L 变换(400),具有更好的检测效果,但是在参数 σ^2 选取时比较困难(存在遍历次数多、计算量大、样本数不足等问题),检测效果不是很显

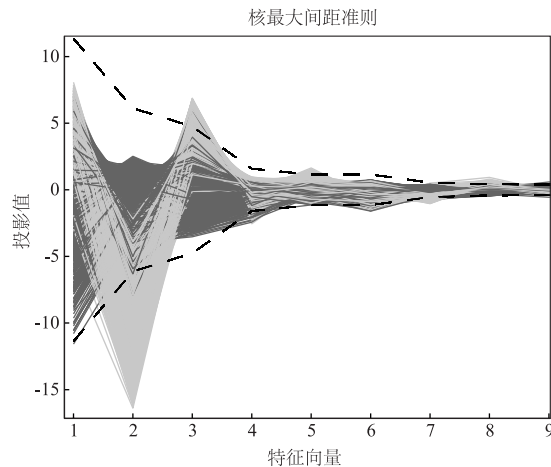


图5 基于核最大间距准则的木马检测

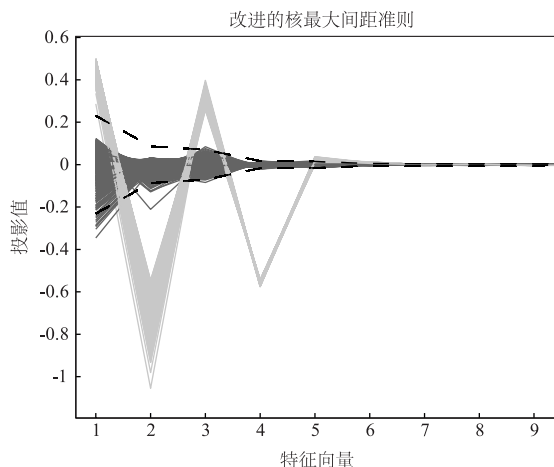


图6 基于改进的核最大间距准则的木马检测

著,加入参数 θ_1 和 θ_2 改进后,该方法能够明显的检测出木马,而且减少了参数 σ^2 的遍历次数,有助于检测更小规模的木马.

此外,与 K-L 变换相比,核函数方法的计算代价有大幅度增加,主要是因为核函数方法通过计算样本之间内积的方式实现原始数据向高维空间的映射以及后续的特征提取,根据式(1)和式(2)可知,核函数方法所构建高维空间的维数会随原始空间中样本个数的增加而增加,样本个数越多,维数越高,计算代价越大.但是相对于芯片的安全性需求而言,该计算代价仍可以接收.

5 结论

基于核最大间距准则的硬件木马检测能够有效的将旁路信号映射到低维子空间,对样本集中的非线性结构进行分析与识别,在一定程度上避免了复杂的运算,为木马检测提供了一条新思路.然而,对于核函数方法计算代价大的问题,如何在保持检测效果的前提下减少样本,高效快速的对木马进行检测将是今后的研

究方向. 此外, 还需研究启发式方法寻找最优的参数 σ^2 , 降低核函数方法计算上的时间复杂度, 提高木马检测效率.

参考文献

- [1] Goertzel K M. Integrated circuit security threats and hardware assurance countermeasures [J]. Crosstalk Real-Time Information Assurance, 2013, 26(6): 33 – 38.
- [2] Bhunia S, Abramovici M, Agrawal D, et al. Protection against hardware Trojan attacks: towards a comprehensive solution [J]. IEEE Design Test Computer, 2013, 30(3): 6 – 17.
- [3] Chakraborty R S, Narasimhan S, Bhunia S. Hardware trojan: threats and emerging solutions [A]. Proceedings of the 2009 IEEE International High Level Design Validation and Test Workshop [C]. San Francisco: IEEE, 2009. 166 – 171.
- [4] Agrawal D, Baktir S, Karakoyunlu D, et al. Trojan detection using IC fingerprinting [A]. Proceedings of the 2007 IEEE Symposium on Security and Privacy [C]. Berkeley: IEEE, 2007. 296 – 310.
- [5] 王力伟, 罗宏伟, 姚若河. 基于旁路分析的硬件木马检测方法[J]. 华南理工大学学报(自然科学版), 2012, 40(6): 6 – 10.
Wang Li-wei, Luo Hong-wei, Yao Ruo-he. Side-channel analysis-based detection approach of hardware Trojans [J]. Journal of South China University of Technology, 2012, 40(6): 6 – 10. (in Chinese)
- [6] 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): 122 – 126.
Zhang Peng, Wang Xin-cheng, Zhou Qing. Hardware trojans detection based on electromagnetic emission signals analysis [J]. Acta Electronica Sinica, 2014, 42(2): 122 – 126. (in Chinese)
- [7] Mangard S, Oswald E, Popp T. Power Analysis Attacks [M]. Colorado: Springer Science & Bussiness Media, 2010.
- [8] 张学工. 模式识别[M]. 北京: 清华大学出版社, 2010.
- [9] 徐勇, 张大鹏, 杨健. 模式识别中的核方法及其应用[M]. 北京: 国防工业出版社, 2010.
- [10] Li H, Jiang T, Zhang K. Efficient and robust feature extraction by maximum margin criterion [J]. IEEE Transactions on Neural Networks, 2006, 17(1): 157 – 165.
- [11] 盛骤, 谢式千, 潘承毅. 概率论与数理统计[M]. 北京: 高等教育出版社, 2010.
- [12] 毛莎莎. 基于贪婪优化和投影变换的集成分类器算法研究[D]. 西安: 西安电子科技大学, 2014.
Mao Sha-sha. A study of classifier ensemble methods based on greedy optimization and projection transformation [D]. Xi'an: University of Electronic Science and Technology, 2014. (in Chinese)

作者简介



李雄伟 男, 1975 年 8 月出生, 河北定州人, 2003 年于军械工程学院获得博士学位. 现为军械工程学院副教授, 主要研究方向为信息安全与对抗.

E-mail: lxw-wys@163.com



王晓晗 男, 1992 年 2 月出生, 河北衡水人, 2015 年于军械工程学院获得硕士学位. 现为军械工程学院博士研究生, 主要研究方向为信息安全与对抗.

E-mail: wxh2225@126.com