基于随机森林的硬件木马检测方法

张　磊，殷梦婕，王建新，董有恒，肖超恩，刘东阳，赵　成
（北京电子科技学院，　北京 100070）

摘　要：针对 BP 神经网络和 SVM 这两种机器学习算法中存在参数选择困难和时间开销较大的问题，本文提出了一种基于随机森林的硬件木马分类方法.首先，将硬件木马检测转化为二元分类问题，对芯片的能量消耗进行多次采样，再通过 PCA 对功耗曲线进行特征提取，最后利用随机森林分类模型对特征向量进行分类，达到检测硬件木马芯片的目的.实验结果表明，经 PCA 处理的相同硬件木马数据，随机森林的判别准确率与 BP 神经网络相比提高了 9.13%，与 SVM 方法相比判别准确率提高了 15.96%.而相比其他两种方法，时间开销也降低了 8 倍左右.

关键词：侧信道分析；硬件木马；分类器；随机森林

Hardware Trojan Detection Method Based on Random Forest

ZHANG Lei,YIN Meng-jie,WANG Jian-xin，DONG You-heng，
〖JZ〗XIAO Chao-en，ZHAO Cheng
(Beijing Electronic Science&Technology Institute, Beijing 100070，　China)

Abstract：　Aiming at the problem of parameter selection and time overhead for BP neural network and SVM algorithms, this paper proposes a Hardware Trojan classification method based on Random Forests. Firstly, the Hardware Trojan detection problem is modeled as a binary classification problem and the power consumption of the chip is sampled several times. Then the characteristics of the power consumption curve are extracted by the PCA (principal component analysis). Finally, RF (Random Forests) classification model is used to classify the feature vectors in purpose of identifying Hardware Trojan chips. The experimental results show that, considering the same Hardware Trojan horse data processed by PCA, the discrimination accuracy of RF is improved by 9.13% compared with the BP neural network. Compared with the SVM(support vector machine) method, the discrimination accuracy is increased by 15.96%. Compared to the other two methods, the time cost of RF is reduced by about 8 times.

Key words：side-channel analysis;hardware trojan;classifier;random forests

作者简介：
张　磊　男，（1979-），博士，副教授.研究方向为信息安全.
殷梦婕（通讯作者）　女，（1994-），硕士研究生.研究方向为信息安全.
E-mail：244241686i@qq.com.
王建新　男，（1977-），博士，副教授.研究方向为电磁防护.
董有恒　男，（1995-），硕士研究生.研究方向为信息安全.