基于遗传算法的硬件木马检测方法

刘燕江 1,2，何春华 1，王力纬 1，恩云飞 1，谢少锋 1，谢　云 2
（1 工业和信息化部电子第五研究所 电子元器件可靠性物理及其应用技术重点实验室，
广东 广州 510610；2 广东工业大学 自动化学院， 广东 广州 510006）

摘　要： 针对硬件木马严重威胁到芯片的安全性和系统的可靠性的问题，提出了一种基于遗传算法的集成电路硬件木马检测方法，该方法将 K 均值算法的局部收敛能力和遗传算法的全局收敛能力结合起来，提取旁路信息间的微小特征差异，实现硬件木马的在线自动检测. 本实验在 FPGA 芯片实现硬件验证，以全局时钟、动态功耗和环形振荡器的输出三个信号作为研究对象，搭建集成电路硬件木马检测系统采集三维旁路信息，对 160 个样本芯片数据进行聚类分析，实验结果证明该方法可准确有效地检测出硬件木马，检测分辨率达到 10-4 量级.

关键词： 硬件木马；遗传算法；特征提取；旁路分析

A Novel Hardware Trojan Detection Method

Based on Genetic Algorithm

LIU Yan-jiang1,2, HE Chun-hua1, WANG Li-wei1, EN Yun-fei1,
〖JZ〗XIE Shao-feng1, XIE Yun2
（1 Science and Technology on Reliability Physics and Application of Electronic Component Laboratory, The Fifth Electronic Research Institute of the Ministry of Industry and Information Technology, Guangzhou 510610, China;
2 School of Automation, Guangdong University of Technology, Guangzhou 510000, China）

Abstract： Hardware Trojan, a malicious circuit inserted into the golden circuit, causes a serious risk to the security of Integrated Circuits and the trust of critical system. Thus, hardware Trojan detection is of great significance. A novel hardware Trojan detection method based on clustering analysis algorithm is presented in this work, which employs the global optimized ability of genetic algorithm and the local searching capability of K-means algorithm to automatically fulfill the detection online. Side-channel signals, such as global clock signal, reset signal and a ring oscillator signal of a chip, are applied as the inputs of the clustering algorithm, since they may be altered by the Trojan circuit. Experimental results implemented with FPGAs demonstrate that the tested chips can be clustered into two categories, and the Trojan chips can be distinguished from the Golden chips accurately. The detection resolution achieves about 10-4, which indicates the proposed novel detection method is feasible and effective.

Key words： hardware trojan; genetic algorithm; characteristics extraction; side-channel analysis

作者简介：
刘燕江　男，(1990-)，硕士研究生.研究方向为硬件木马检测.
何春华（通讯作者）　男，(1988-)，工程师.研究方向为硬件木马检测.E-mail:hechunhua@pku.edu.cn.