基于节点活性的硬件木马检测方法

冯秋丽 1,2，侯　波 1，刘燕江 2，恩云飞 1，王力纬 1
（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 材料与能源学院，广东 广州 510006）

摘　要：本文提出了一种基于节点活性的硬件木马检测方法，针对电路中的低活性节点生成测试向量，结合多参数旁路检测方法，实现对硬件木马的检测.以 AES 为目标电路并植入硬件木马，进行仿真及 FPGA 实验，实验结果表明与随机测试向量相比，本文生成的测试向量可将木马节点的翻转概率提高一个数量级、木马检测灵敏度分别提高 6.75%（仿真）、77.4%（FPGA），硬件木马的检测精度达到 10^{-4}.

关键词：芯片安全；硬件木马检测；节点活性；测试向量生成

A Novel Hardware Trojan Detection Method

Based on Node Activity State

FENG Qiu-li 1,2 ,HOU Bo 1 ,LIU Yan-jiang 1,EN Yun-fei 1,WANG Li-wei 1
（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 Material and Energy Resources, Guangdong University of Technology, Guangzhou 510000, China）

Abstract：In this paper, we propose a hardware Trojan detection method based on nodes activity state,in view of the low activity nodes of original circuit generate test vectors, Combined with the method of multi-parameter side channel signals to detect Hardware Trojan. The proposed method is verified by simulation and FPGA experiment carried on AES original circuit which is implanted with hardware trojan. The results show that compared with random test vector, the proposed method can improve the transition probability of the trojans of nodes an order of magnitude and increase the sensitivity of the Hardware Trojan detection by 6.75%(simulation),77.4%(FPGA), detecte the Hardware Trojan whose equivalent area is as small as 10 -4 of the total size of the circuit.

Key words：IC security; node activity state; hardware trojan detection;test pattern generation

作者简介：
冯秋丽　女，（1990-），硕士研究生.研究方向为硬件木马的检测.
侯　波（通信作者）　男，（1985-），工程师.研究方向为硬件木马检测.
E-mail：houbo@ceprei.com.