

基于基准曲线的硬件木马检测技术研究

王 林 1,2, 魏敬和 2, 周 昱 2

(1 江南大学 物联网工程学院, 江苏 无锡 214122; 2 中国科技集团第 58 研究所, 江苏 无锡 2014072)

摘 要: 目前硬件木马的检测方法主要有逻辑测试和旁道参数分析法, 然而在木马面积较小并且存在较大的工艺漂移的情况下, 这两种方法的检测覆盖率并不高. 对此利用电路自身的动态电流 (I_{ddt}) 和最高频率 (f_{max}) 之间的固有关系构造出一条基准曲线, 将实测曲线与基准曲线进行对比来检测硬件木马. 前期利用 Synopsys 工具对理论进行仿真验证, 然后设计专用 PCB 测试板, 选取合适的测量设备和 FPGA 芯片搭建测试系统进行实测. 实测结果表明, 该测试系统可以有效地降低工艺漂移对检测结果的影响, 并且可以较好地提高硬件木马的检测精度.

关键词: 硬件木马; 基准曲线; 工艺漂移; 专用 PCB; 测试系统

The Study of Hardware Trojan Detection Based on Reference Curve

WANG Lin 1,2, WEI Jing-he 2, ZHOU Yu 2

(1 School of IOT Engineering, Jiangnan University, Wuxi 214122, China; 2 No.58 Research Institute, China Electronics Technology Group Corporation, Wuxi 2014072, China)

Abstract: Currently the main detection approaches to the Hardware Trojan are logical test and side-channel analysis, however, these methods suffers from decreased sensitivity toward small Trojans and large process variation. In this paper, we take advantage of the intrinsic relationship between dynamic current and maximum operation frequency of the circuit to formulate a reference curve, then compare the measured curve with the reference curve to detect the Hardware Trojan. At the beginning we use the Synopsys tool to validate the theory, then design specified PCB test board, choose the appropriate measure device and FPGA to set up the test system. The test result shows that this system can reduce the influence of the process variation on the detect result efficiently and improve the detection accuracy.

Key words: hardware trojan; reference curve; process variation; specified PCB; test system

作者简介:

王 林 男 (仡佬族), (1991-), 硕士. 研究方向为数字集成电路设计和测试.

魏敬和 (通讯作者) 男, (1975-), 博士. 研究方向为大规模数字集成电路设计与测试.

E-mail:920770745@qq.com.