基于环形振荡器的硬件木马检测

金瓯，李磊，周婉婷
(电子科技大学 电子科学技术研究院，四川 成都 611731)

摘要： 针对传统的边信道检测模型容易受到工艺偏差的影响，提出了一种集成在电路内部的检测方法，该方法将电路内部难以直接测量的待测信号转化直观的量化值输出，并通过后续的降噪、降维、分类算法的处理，实现硬件木马的检测.与传统信道检测方法相比，本检测方法的最大特点是：（1）有效的避免工艺偏差的影响；（2）即使木马尚未激活也能检测木马的存在；（3）能实现对木马位置的定位.FPGA 实验表明，对 Trust-hub 上的 RS232 木马电路能显著提高检测结果.
关键词： 硬件木马；工艺偏差；环形振荡器；边信道；FPGA

Hardware Trojan Detection Based on Ring Oscillator

JIN Ou, LI Lei,ZHOU Wan-ting
(Research Institute of Electronic Science and Technology, University of Electronic Science and Technology of China, Chengdu 611731, China)

Abstract： Aimed at the problem that the traditional side channel detection model is easily influenced by the process variation, a detection method integrated in the circuit is proposed. This method converts the signal which is difficult to be directly measured in the circuit into an intuitive quantization value of output, and through denoise method, dimension reduction, classification algorithms to achieve the detection of hardware Trojan. Compared with traditional side channel detection methods, the most prominent feature of this detection method is: (1) effectively avoid the influence of process variation; (2) Trojans can detect the presence of Trojans without activation; (3) achieve the location of the Trojan′ s position. FPGA experiments against RS232 hardware Trojan circuit on Trust-hub demonstrate that, this method can significantly improve the detection result about Trojan.
Key words： hardware trojan; process variation; ring oscillator; side channel; FPGA

作者简介：
金瓯男，（1990-），硕士研究生.研究方向为 ASIC 设计.
E-mail：growup_j@163.com.
李磊男，（1982-），博士，研究员.研究方向为专用集成电路设计.
周婉婷女，（1982-），博士.研究方向为 IC 抗辐射加固技术.