一种基于随机指令延迟的抗旁路攻击处理器结构

李　红 1,2，贺章擎 3，徐元中 3

(1 湖北工业大学 计算机科学与技术学院，湖北 武汉 430068；

2 华中科技大学 计算机科学与技术学院，湖北 武汉 430074；

3 湖北工业大学 太阳能高效利用湖北省协同创新中心，湖北 武汉 430068)

摘　要： 提出了一种基于随机延迟的高效的抗旁路攻击处理器结构，综合采用随机指令调度、随机指令注入和随机流水段延迟技术以抵抗旁路攻击.基于 ARM7 处理器实现了该架构，实现结果表明本处理器比原始 ARM7 处理器增加了约 20%的硬件面积.通过相关系数分析攻击（Correlation Power Analysis, CPA）实验证明，采用本架构的处理器具备有极高的抗旁路攻击防护能力，可以应用在 USBKEY、智能卡(Smart CARD)等高安全应用场合.

关键词： 旁路攻击；随机延迟；随机指令调度；ARM7

An Efficient Processor Architecture to Resist Side Channel Attacks

LI Hong1,2，HE Zhang-qing3，XU Yuan-zhong3

（ 1 College of Computer Science and Technology , Hubei University of Technology, Wuhan 430068,China; 2 School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China; 3 Hubei Collaborative Innovation Center for High-efficiency Utilization of Solar Energy, Hubei University of Technology, Wuhan 430068, China）

Abstract： In this article, based on random delay insertion, an effective processor architecture resistant to side-channel attacks was proposed. It used a combination of randomized scheduling, randomized instruction insertion and randomized pipeline-delay to resist side-channel attacks. On the base of ARM7 processor, we implemented this architecture and the implementation results showed that this processor has increased approximate 20% in hardware area than the original ARM7 processor. The CPA attack experiment results suggested that our new secure processor have high capacity to resist side-channel attacks and thus could be used in USBKEY, Smart CARD and other application scenarios which require extremely high security level.

Key words： side-channel attacks; random delay; randomized scheduling; ARM7

作者简介：

李　红　女，(1981-)，博士研究生，讲师.研究方向为计算机系统结构.E-mail：lilyhong420@126.com.

贺章擎　男，(1980-)，博士，副教授.研究方向为信息安全与集成电路设计.

徐元中　男，(1974-)，副教授.研究方向为嵌入式系统设计。