蓝雷：一种基于二级方向预测器的SGX侧信道攻击

Bluethunder: A 2-level Directional Predictor Based Side-Channel Attack against SGX

作者：霍天霖, 孟筱妮, 王文浩, 郝春亮, 赵培, 翟健, 李明树

会议信息：IACR Transactions on Cryptographic Hardware and Embedded Systems 2020

联系方式：tianlin@nfs.iscas.ac.cn（霍天霖）

具体内容介绍

背景

SGX容易受到微架构侧信道攻击。其中，基于BPU中PHT的侧信道可以精准地恢复目标程序的控制流，但却具有“攻击速度慢” 等缺点。

Bluethunder攻击

本文提出Bluethunder——首个基于BPU中二级方向预测器的SGX侧信道攻击，可用于恢复目标程序的控制流。由于Bluethunder不依赖于大量指令来对二级预测器初始化，故可以大幅提升PHT攻击速度。Bluethunder包含两个阶段：激活二级预测器和利用二级预测器。

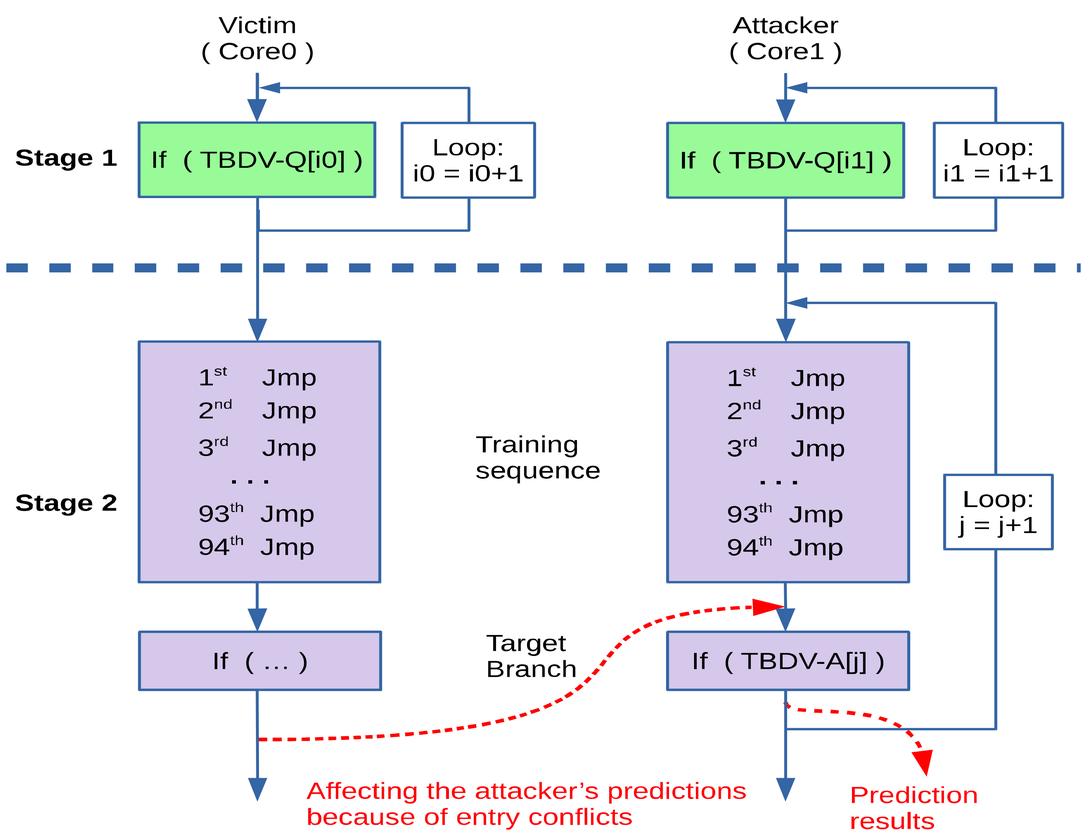

图1　Bluethunder顶层原理示意图

- 阶段一：激活二级预测器
  通过强制构造其他预测器的预测错误，最终诱使BPU选择二级方向预测器（即二级PHT）进行预测。

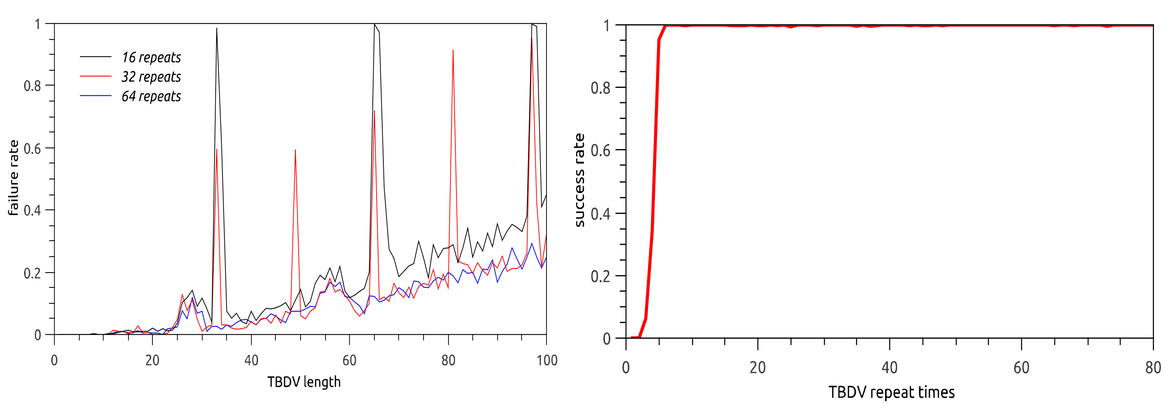

图2　预测器激活探测实验结果

- 阶段二：利用二级预测器
  首先攻击者基于相同目标指令地址（即PC值）和相同历史信息构造二级预测器项冲突，而后利用预测器内部运行机制来构建侧信道攻击。

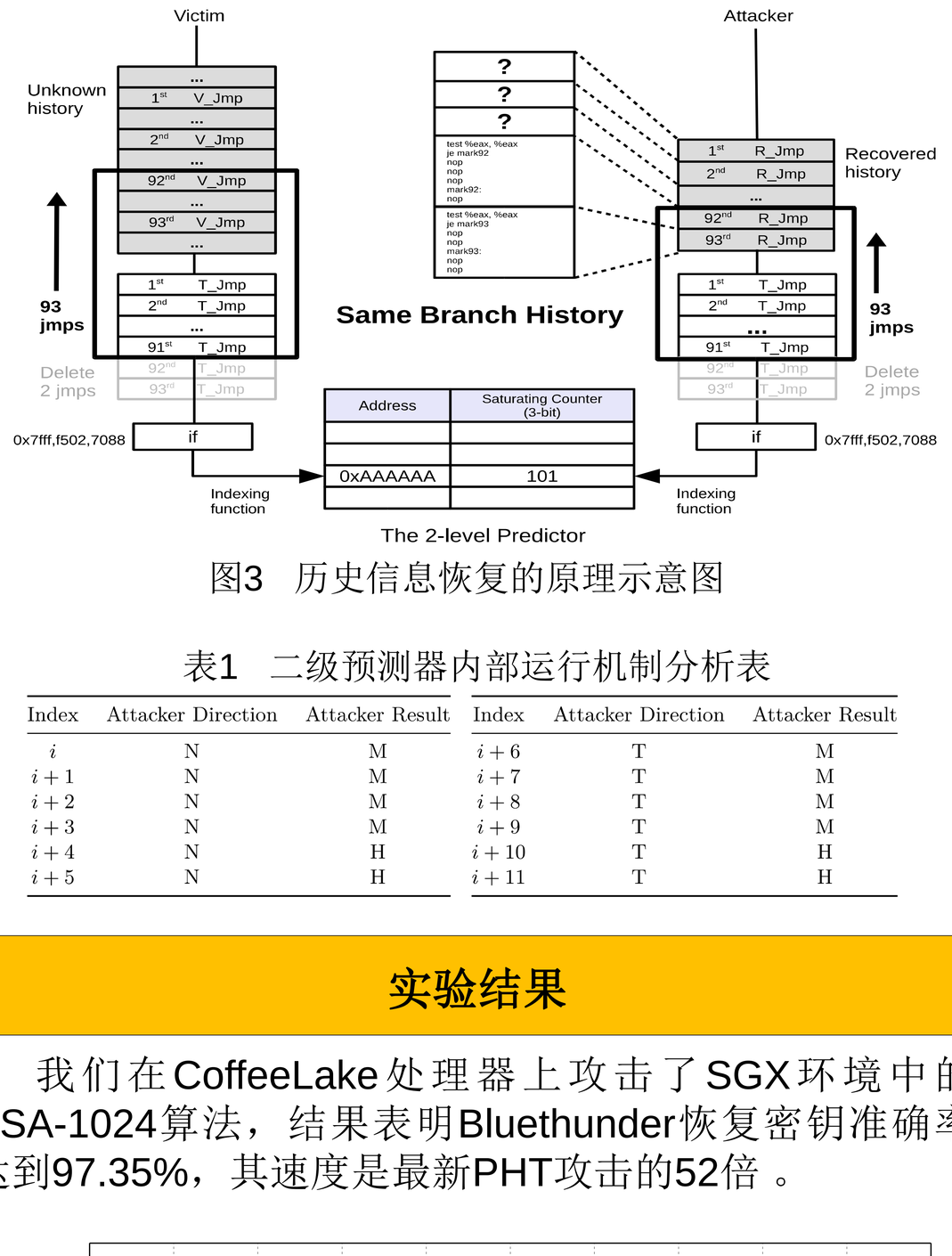

图3　历史信息恢复的原理示意图

表1　二级预测器内部运行机制分析表

Index	Attacker Direction	Attacker Result	Index	Attacker Direction	Attacker Result
i	N	M	$i+6$	T	M
$i+1$	N	M	$i+7$	T	M
$i+2$	N	M	$i+8$	T	M
$i+3$	N	M	$i+9$	T	M
$i+4$	N	H	$i+10$	T	H
$i+5$	N	H	$i+11$	T	H

实验结果

我们在CoffeeLake处理器上攻击了SGX环境中的RSA-1024算法，结果表明Bluethunder恢复密钥准确率达到97.35%，其速度是最新PHT攻击的52倍 。

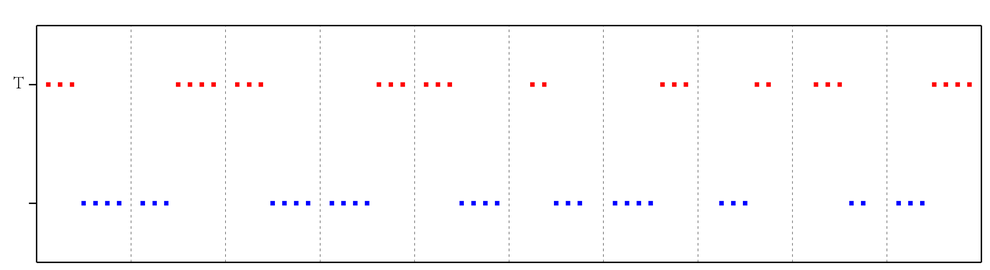

图4　RSA攻击结果图

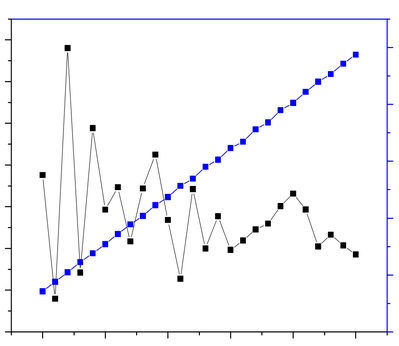

图5　攻击耗时/错误率与探测次数之间的关系

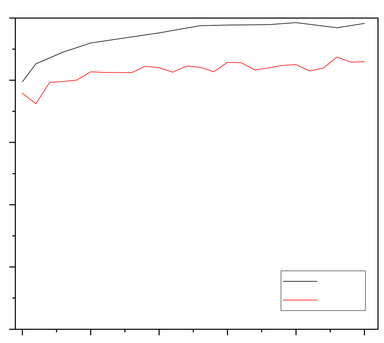

图6　基于RdTSC/PMC两种探测方法的攻击效果的对比