ISCAS 中国科学院软件研究所学术年会’2021
暨计算机科学国家重点实验室开放周
学术论文

PEC-V:基于RISC-V协处理器的内存溢出防御机制

张雨昕,芮志清, 李威威, 张画, 罗天悦, 吴敬征

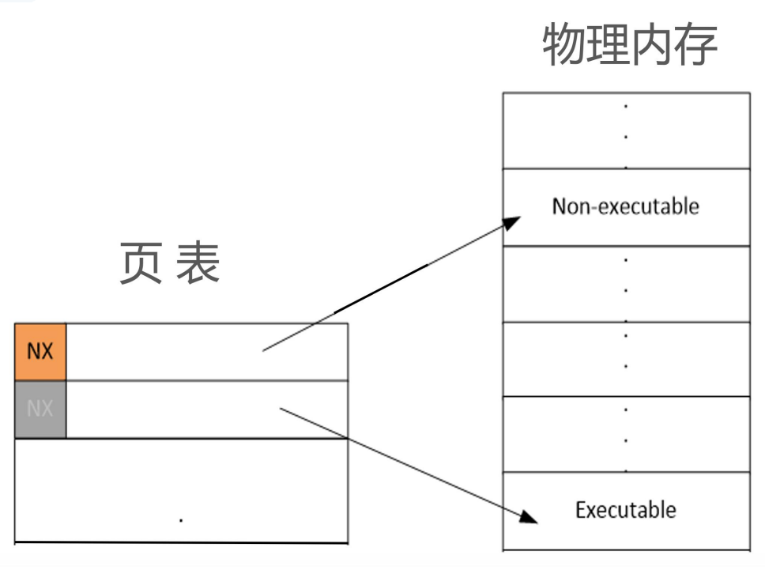
PEC-V: Memory Overflow Defense Mechanism Based on RISC-V Coprocessor

计算机系统应用，2021(11)

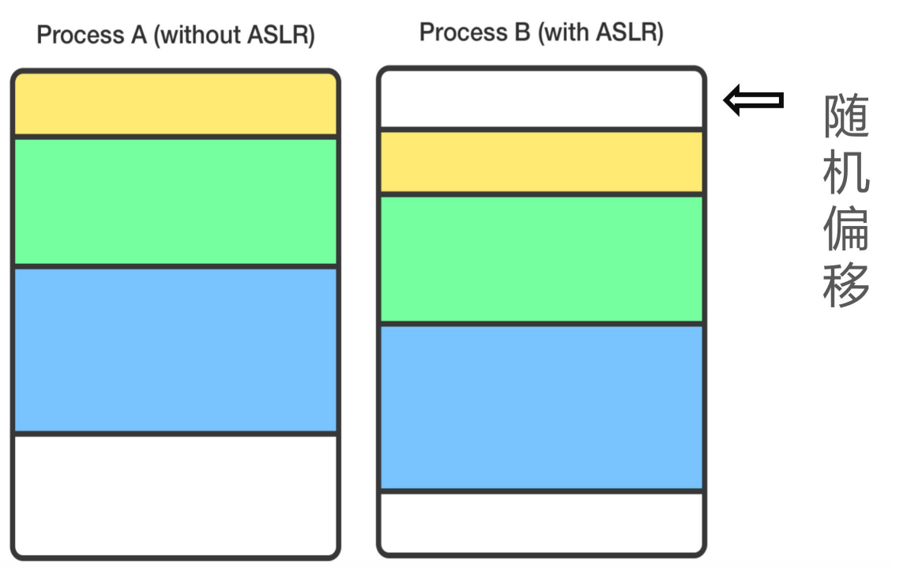
联系方式: 吴敬征 18910958184 jingzheng08@iscas.ac.cn

概述

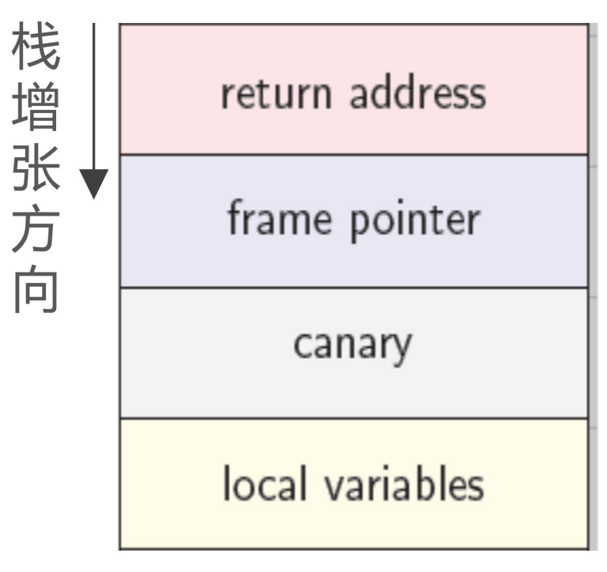
缓冲区溢出是一种十分常见且危害较大的漏洞, 攻击者可利用此类漏洞执行一系列违规操作，达到控制程序、操作系统的目的。针对缓冲区溢出漏洞的防御机制的研究较多，如下图为几种常见的机制:



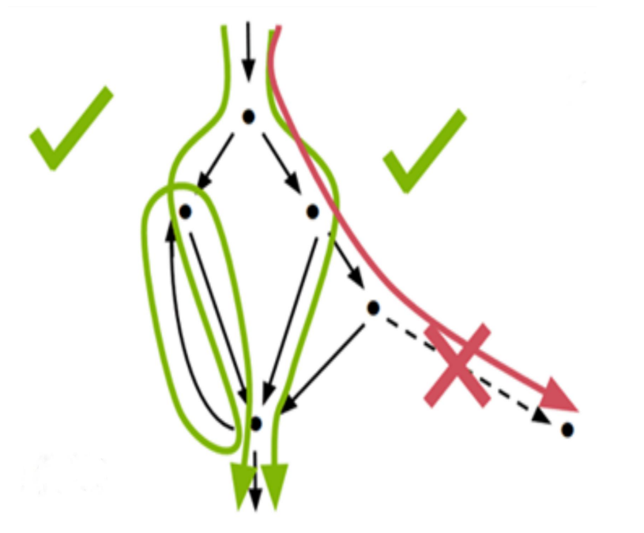
- 数据不可执行



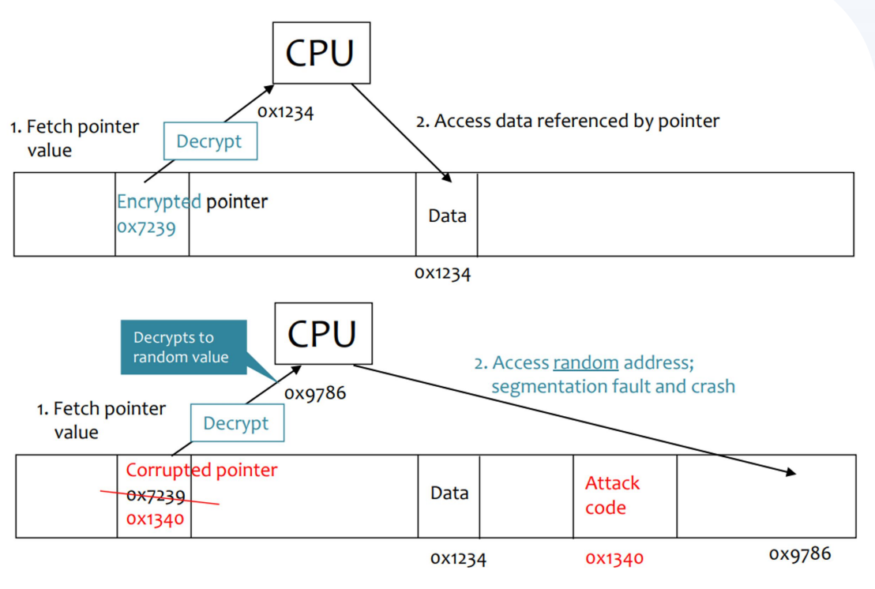
- 内存地址空间随机化



- Stack canary



- 程序控制流完整性

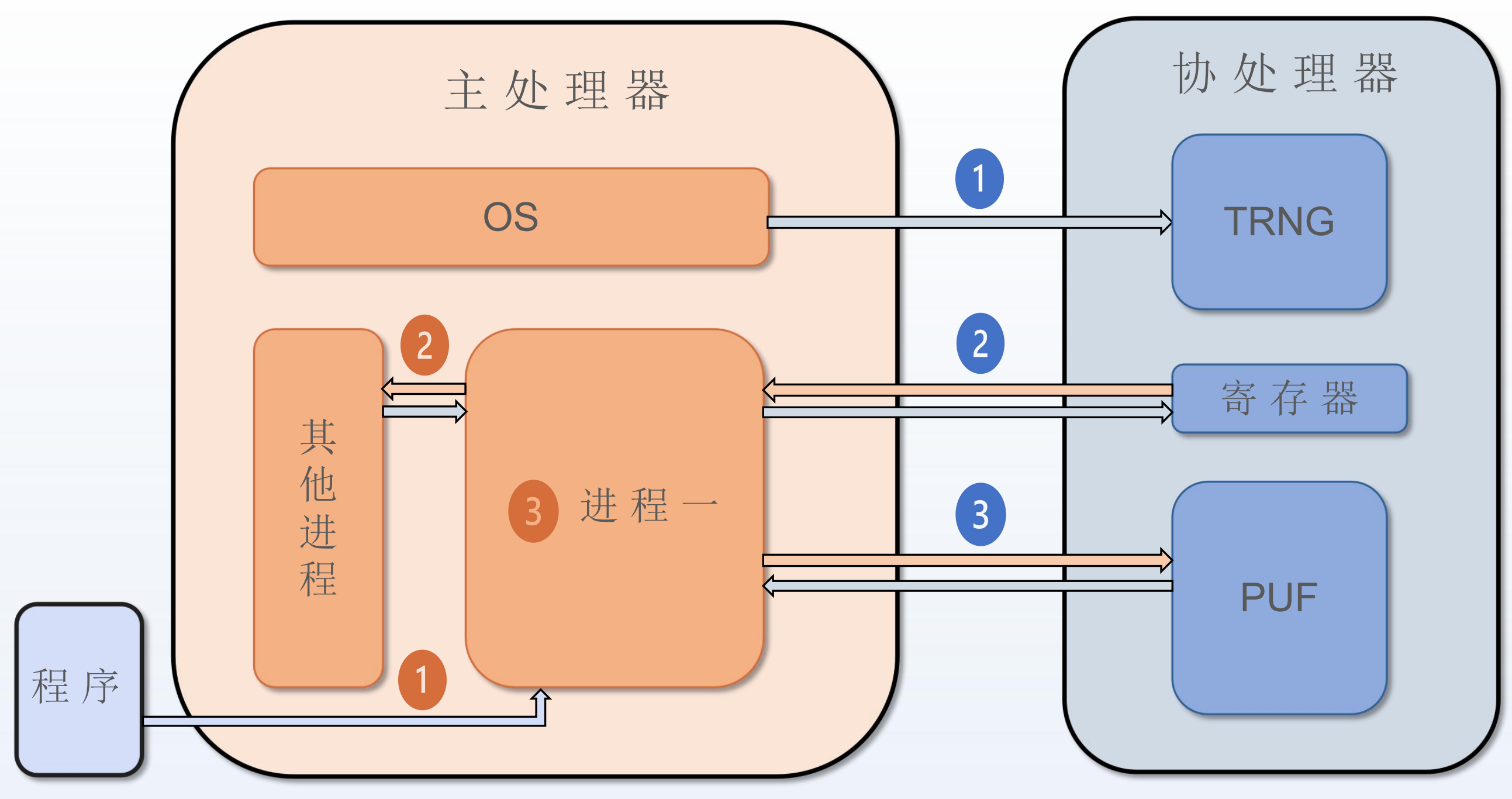


- 指针加密

数据不可执行、内存地址空间随机化等机制，防御性能有限，需要与其他方式相结合使用。而Stack Canary，程序控制流完整性等方式存在对堆上溢出无法防御，或实现方式太过复杂等问题，因此，针对上述问题，本文实现了PEC-V，使用**指针加密机制**作为内存溢出防御的主要原理，通过**硬件方式**在RISC-V架构上实现，以达到更好的安全性和更高的效率。

PEC-V机制概述：使用RocketChip的RoCC(Rocket Custom Coprocessor)接口挂载一个实现的**指针加密机制**的**协处理器**，通过向RISC-V指令集中添加新增的**自定义指令**控制协处理器加解密返回地址和函数指针等值达到阻止溢出攻击的目的。

机制原理

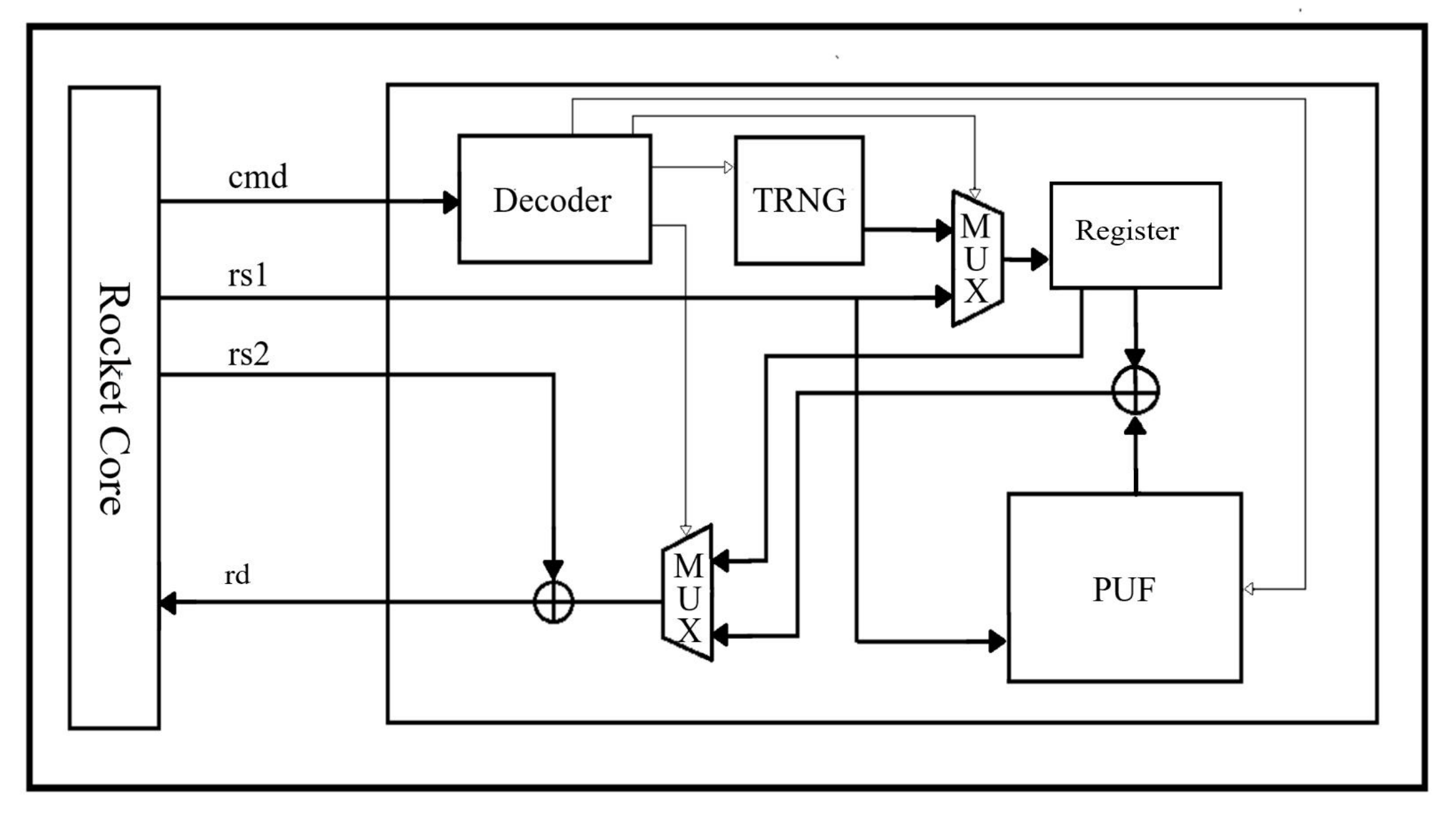


1	创建进程	初始化协处理器，生成进程唯一的真随机数 1
2	上下文切换	保存或恢复进程唯一的真随机数 2
3	进程运行	返回地址和函数指针传给协处理器加解密 3

图一

	31-25	rs2(19-14)	rs1(15-19)	12-14	rd(7-11)	0-6
指令一	0000000	/	/	000	/	0001011
指令二	0000001	/	Source	010	/	0001011
指令三	0000010	/	/	100	Destination	0001011
指令四	0000011	Source2	Source1	111	Destination	0001011

图二



图三

图一为PEC-V整体架构图，图二为新增的RISC-V指令格式，图三为协处理器内部电路图。

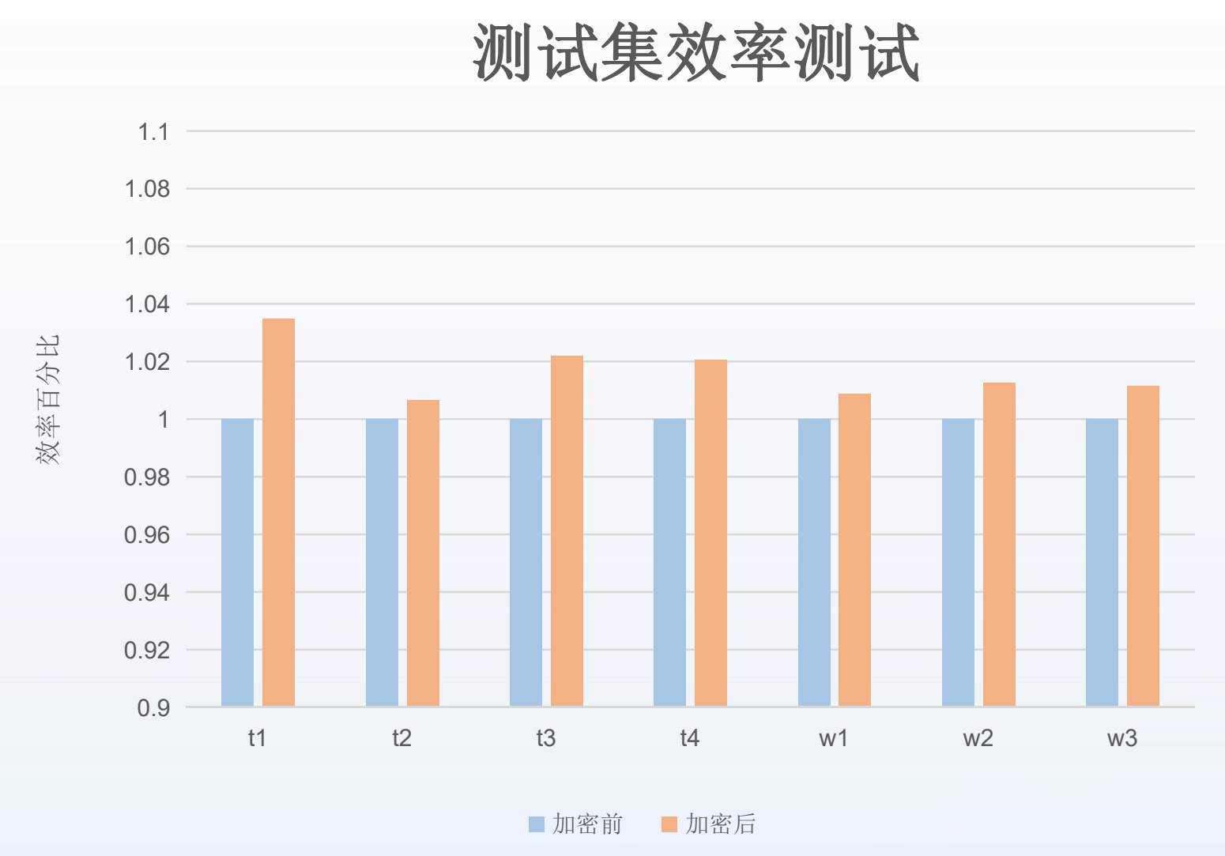
如图一所示，**此机制主要可以分为三部分来介绍：**

一．操作系统创建进程，操作系统发送指令一给协处理器，使协处理器中的TRNG生成进程唯一的随机数，并将此随机数存储到协处理器寄存器中。

二．当进程上下文切换时，操作系统用指令二、三分别存储和恢复进程唯一的随机数。

三．当程序运行时，当存入或使用返回地址，函数指针等数据时，进程发送指令四给协处理器进行加解密。加解密方式如图三所示：rs1中为数据在内存中的地址，rs2为数据的值，**PUF**的响应和Register中存储的真随机数做为加解密的键值与rs2异或后输出。

实验&总结



实验结果分析：本论文使用**RocketChip**的**C++ cycle-accurate emulator**进行测试。

一．安全性方面，对于**Wilander测试集中**几种针对返回地址和函数指针的溢出攻击方式，PEC-V都具有很好的防护性能。

二．效率方面，本实验选用**Juliet Test Suite**和**Wilander testbed**中的测试程序进行测试；此外，本文还增加对程序中嵌套调用函数和多次使用函数指针的情况的测试。实验结果如上图所示，可以看出PEC-V对程序运行效率并未造成显著影响。

贡献总结:

一、本文**首次**使用协处理器设计了RISC-V架构上的指针加密方法PEC-V;

二、 并使用RocketChip的C++仿真器证明了PEC-V的安全性与效率;

三、PEC-V可在对**性能影响较小**的情况下**有效防御**各类缓冲区溢出攻击。

** 本文已在首届RISC-V中国峰会(2021.6.24)上分享，欢迎各位在峰会主页查看演讲视频。*

** 本文将刊登于2021年11期的《计算机系统应用》RISC-V技术及生态专刊。*