



RISC-V 用户态中断

余泰来

2021 年 10 月 30 日

用户态中断的意义

操作系统可以利用中断...

- 实时响应外设
- 计时
- 跨核通信

应用程序

- 类似现用系统调用实现
 - 通过系统调用操作外设
 - 信号等 IPC 机制

用户态中断的意义

- 用户态驱动
- 不用陷入内核的 IPC

IPC type	Relative Latency (normalized to User IPI)
User IPI	1.0
Signal	14.8
Eventfd	9.7
Pipe	16.3
Domain	17.3

已有工作

Intel

- 去年公布了 x86 上的用户态中断扩展

RISC-V N 扩展

- 原有的用户态中断扩展
- 将 M、S 态的中断机制直接扩展到 U 态
- 意图用来支持只有 M、U 态、安全的嵌入式系统

贺鲲鹏、尤予阳同学的工作

- 完善并实现 N 扩展，在模拟器和 FPGA 上实现
- 多核扩展 rCore，在 rCore 和 SBI 中加入用户态中断支持
- 信号、用户态串口等演示

尚未完成的工作

无需陷入内核的用户态跨核中断支持：

- 扩展中断控制器 ACLINT，支持直接跨核发送用户态中断
- 应用程序查找中断目标进程所在 hart 的机制
- 未在运行的应用程序所接受中断的缓存

设计目标

能力

完成以上需求

效率

尽可能高效

陷入 >> 访存 >> 寄存器

模块化

区分对 N 扩展、中断控制器等的要求
考虑在不同场景、部分实现的情况

安全

尽可能避免旁路攻击

初步时间计划



目前进展

- 熟悉贺鲲鹏、尤予阳同学的工作，特别是 rCore-N 和 Qemu 部分
- 熟悉 Intel 的用户态中断机制
- 初步思考设计细节

ACLINT 扩展

- ACLINT 在 SiFive CLINT 基础上，增加 S 态跨核中断，通过写特定地址发送
- 可以简单扩展到用户态，至少 OS 可以直接发送跨核用户态中断
- 问题：
- 应用程序缺乏 OS 维护跨核数据结构的自由，而 ACLINT 只能发送一位信息，可能需要允许发送 utval

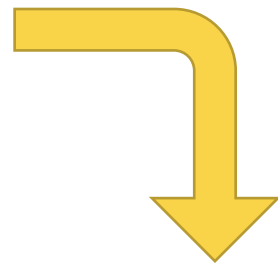
目标程序查找机制

- 图为 Intel 机制的简化版
- 初步设计：
- 增加指令发送用户态程序间中断
- 每个任务准备一张 UITT，由 OS 维护，参考页表，内核给出物理地址避免用户程序访问
- 如果目标程序在运行，“UPID”给出 ACLINT 中断地址，硬件直接填写
- 否则本地陷入内核
- 问题：
- 是否会影响模块化？
- 可能减少内存访问吗？

发送方应用程序



User-Interrupt Target Table

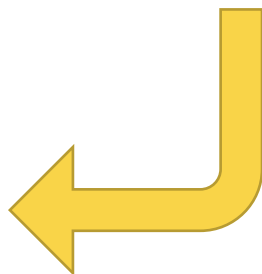


User Posted-Interrupt Descriptor

接收方应用程序



目标核



缓存机制

- 目标:
- 能够缓存 E、T、S 三类中断的 ucause 和 utval
- 对软件几乎透明 (参考 TLB)
- 在缓冲区满后, 在 OS 看来仿佛触发一次或若干次目标程序未在运行的用户态中断
- per app, not per hart
- 问题:
- 如何为较多任务分配有限数量的硬件 FIFO?



谢谢

余泰来

ytl19@mails.tsinghua.edu.cn