清 华 大 学

综 合 论 文 训 练

题目：基于 RISC-V 的用户态中断扩展

系　　别：计算机科学与技术系

专　　业：计算机科学与技术

姓　　名：田凯夫

指导教师：陈　渝　副教授

2023 年 5 月 6 日

关于学位论文使用授权的说明

本人完全了解清华大学有关保留、使用学位论文的规定，即：学校有权保留学位论文的复印件，允许该论文被查阅和借阅；学校可以公布该论文的全部或部分内容，可以采用影印、缩印或其他复制手段保存该论文。

(涉密的学位论文在解密后应遵守此规定)

签　名：_____ 导师签名：_____ 日　期：_____

中文摘要

论文的摘要是对论文研究内容和成果的高度概括。摘要应对论文所研究的问题及其研究目的进行描述，对研究方法和过程进行简单介绍，对研究成果和所得结论进行概括。摘要应具有独立性和自明性，其内容应包含与论文全文同等量的主要信息。使读者即使不阅读全文，通过摘要就能了解论文的总体内容和主要成果。

论文摘要的书写应力求精确、简明。切忌写成对论文书写内容进行提要的形式，尤其要避免“第 1 章……；第 2 章……；……”这种或类似的陈述方式。

关键词是为了文献标引工作、用以表示全文主要内容信息的单词或术语。关键词不超过 5 个，每个关键词中间用分号分隔。

关键词：关键词 1；关键词 2；关键词 3；关键词 4；关键词 5

ABSTRACT

An abstract of a dissertation is a summary and extraction of research work and contributions. Included in an abstract should be description of research topic and research objective, brief introduction to methodology and research process, and summary of conclusion and contributions of the research. An abstract should be characterized by independence and clarity and carry identical information with the dissertation. It should be such that the general idea and major contributions of the dissertation are conveyed without reading the dissertation.

An abstract should be concise and to the point. It is a misunderstanding to make an abstract an outline of the dissertation and words “the first chapter”, “the second chapter” and the like should be avoided in the abstract.

Keywords are terms used in a dissertation for indexing, reflecting core information of the dissertation. An abstract may contain a maximum of 5 keywords, with semi-colons used in between to separate one another.

Keywords: keyword 1; keyword 2; keyword 3; keyword 4; keyword 5

目　录

插图索引

表格索引

主要符号表

PI	聚酰亚胺
MPI	聚酰亚胺模型化合物，N-苯基邻苯酰亚胺
PBI	聚苯并咪唑
MPBI	聚苯并咪唑模型化合物，N-苯基苯并咪唑
PY	聚吡咙
PMDA-BDA	均苯四酸二酐与联苯四胺合成的聚吡咙薄膜
MPY	聚吡咙模型化合物
As-PPT	聚苯基不对称三嗪
MAsPPT	聚苯基不对称三嗪单模型化合物，3,5,6-三苯基-1,2,4-三嗪
DMAsPPT	聚苯基不对称三嗪双模型化合物（水解实验模型化合物）
S-PPT	聚苯基对称三嗪
MSPPT	聚苯基对称三嗪模型化合物，2,4,6-三苯基-1,3,5-三嗪
PPQ	聚苯基喹噁啉
MPPQ	聚苯基喹噁啉模型化合物，3,4-二苯基苯并二嗪
HMPI	聚酰亚胺模型化合物的质子化产物
HMPY	聚吡咙模型化合物的质子化产物
HMPBI	聚苯并咪唑模型化合物的质子化产物
HMAsPPT	聚苯基不对称三嗪模型化合物的质子化产物
HMSPPT	聚苯基对称三嗪模型化合物的质子化产物
HMPPQ	聚苯基喹噁啉模型化合物的质子化产物
PDT	热分解温度
HPLC	高效液相色谱（High Performance Liquid Chromatography）
HPCE	高效毛细管电泳色谱（High Performance Capillary lectrophoresis）
LC-MS	液相色谱-质谱联用（Liquid chromatography-Mass Spectrum）
TIC	总离子浓度（Total Ion Content）
ab initio	基于第一原理的量子化学计算方法，常称从头算法
DFT	密度泛函理论（Density Functional Theory）
E_a	化学反应的活化能（Activation Energy）
ZPE	零点振动能（Zero Vibration Energy）

PES	势能面（Potential Energy Surface）
TS	过渡态（Transition State）
TST	过渡态理论（Transition State Theory）
$\Delta G^{\neq}$	活化自由能（Activation Free Energy）
κ	传输系数（Transmission Coefficient）
IRC	内禀反应坐标（Intrinsic Reaction Coordinates）
ν_i	虚频（Imaginary Frequency）
ONIOM	分层算法（Our own N-layered Integrated molecular Orbital and molecular Mechanics）
SCF	自洽场（Self-Consistent Field）
SCRF	自洽反应场（Self-Consistent Reaction Field）

第 1 章　引言

本文主要分为以下几个部分：

- **背景介绍**
- **软件实现**
- **硬件实现**
- **性能评估**

第 2 章　背景介绍

2.1　RISC-V N 扩展

2.2　x86 用户态中断

第 3 章　设计草案

在 RISC-V N 扩展的基础上，我们提出了 RISC-V 用户态中断扩展，通过引入新的 CSR、指令以及外部中断控制器，可以实现高效的用户态跨核中断。在普通的中断处理流程中，我们默认只有 M 态和 S 态可以接收或发送中断，且运行在这些特权态下的软件是可以信任的，但用户态程序的行为并不一定是合法的。因此通过硬件的参与，我们的设计在 N 扩展的基础上，解决了如下几个问题，这些问题都有可能导致某个核正常执行流程被非法的中断打断：

- 发送方尝试向未注册的目标核发送中断
- 接收方尝试修改自己的控制信息，将来自发送方的中断重定向到其他核
- 接收方没有在目标核上运行，但发送方发送了用户态中断

若无特殊说明，以下的描述均基于 **64** 位 RISC-V 指令架构。

3.1　CSR

`suirs`(User-Interrupt Receiver Status) 寄存器和 `suist`(User-Interrupt Sender Table) 寄存器分别用来索引接收方和发送方的状态。这两个寄存器均被设置为 U 态不可访问，U 态只能通过 `uipi` 指令间接地应用它们包含的信息。

对应位	名称	描述
0:15	UIRS Index	接收方序号
62:16	Reserved	保留位，硬件会忽略这些位
63	Enable	使能位，置 1 表示使能

表 3.1　接收方状态寄存器

对应位	名称	描述
0:43	PPN	发送方状态表基址页号
44:55	Size	发送方状态表页面数量
62:56	Reserved	保留位，硬件会忽略这些位
63	Enable	使能位，置 1 表示使能

表 3.2　发送方状态寄存器

对应位	名称	描述
0	Valid	有效位，置 1 表示有效
15:1	Reserved	保留位，硬件会忽略这些位
31:16	Sender Vector	中断向量
47:32	Reserved	保留位，硬件会忽略这些位
63:48	UIRS Index	接收方序号

表 3.3　发送方状态

3.2　UINTC

用户态中断控制器（UINTC，User-Interrupt Controller）作为设计的核心部分，主要负责维护接收方的状态信息，并响应来自读写端口的请求完成对应的操作。

对应位	名称	描述
0	Active	活跃位，置 1 表示可以向目标核发送中断
1	Mode	默认置 1，置 1 表示 64 位架构，置 0 表示 32 位架构
15:2	Reserved	保留位，硬件会忽略这些位
31:16	Hartid	正在运行该接受方的核号
63:32	Reserved	保留位，硬件会忽略这些位
127:64	Pending Requests	每一位对应一个中断向量，置 1 表示接收到中断请求

表 3.4　接收方状态

UINTC 为每一个接收方分配 32 B 的读写端口，每个操作都有可能从端口读出或向端口写入 8 B 数据，因此总共对应 8 种不同的操作，下表为不同操作对应的地址偏移量：

偏移量	读操作	写操作
0x00	Reserved	SEND
0x08	READ_LOW	WRITE_LOW
0x10	READ_HIGH	WRITE_HIGH
0x18	GET_ACT	SET_ACT

表 3.5　UINTC 操作码

其中 LOW 对应接收方状态的低 64 位，包括 Active，Mode，Hartid 等信息；HIGH 对应接收方状态的高 64 位，也就是 Pending Requests 。

SEND 操作会将数据中包含的中断向量写入到对应接收方状态的 Pending Requests 中，当 Active 为 1 且 Pending Requests 不为 0 时，UINTC 会拉高对应核的 `USIP` 位。

READ_HIGH 操作在读取 Pending Requests 后会将其清 0，而 **WRITE_HIGH** 操作则是将新的数据和原来的 Pending Requests 按位或，这样做是确保读写操作之间的中断请求不会被覆盖。

SET_ACT 操作会默认将新的数据的最低位写入到 Active 中。

CPU 通过执行 `sd` 或 `ld` 指令向总线发送读写请求，读写地址会被转化为不同的接收方序号，以支持 512 个接收方的 UINTC 为例，地址映射如下表所示：

偏移量	位宽	属性	名称	描述
0x00000000	32 B	RW	UIRS0	0 号接收方
0x00000020	32 B	RW	UIRS1	1 号接收方
...	...	...	...	...
0x00003FC0	32 B	RW	UIRS511	511 号接收方

表 3.6　UINTC 地址映射

3.3　UIPI

`uipi` 是可以在 U 态直接执行的 R 型指令，共包括五条不同功能的指令：

0 `uipi.send` **rs1**：发送方发送用户态中断

1 `uipi.read` **rd**：接收方读取并清空中断等待位

2 `uipi.write` **rs1**：接收方写入中断等待位

3 `uipi.activate`：接收方准备接收用户态中断

4 `uipi.deactivate`：接收方拒绝接收用户态中断

这些指令执行到最后都需要读或写 UINTC 的端口，对 UINTC 中状态的影响与直接访问物理地址读写的影响是一致的。由于指令执行需要直接排除缓存系统访问外设，程序需要考虑指令乱序的问题。

`uipi.send` 指令传入发送方状态表的序号，根据 `suist` 寄存器中发送方状态表基址来读取内存中对应的表项，发送方在执行 `uipi.send` 指令后读到的物理地址为：

$$(PPN << 0xC) + (rs1 << 0x3)$$

其中页面大小默认为 4 KB，发送方状态表项的大小默认为 8 字节。若最后计算的地址超出了状态表的最大容量，该指令执行失败。若当前 `suist` 寄存器中使能位为 0，则该指令执行失败。硬件通过读出发送方指定的表项来获取中断向量和接收方序号，并写入 UINTC 对应的地址完成一次中断的发送。

其他的四条指令都需要根据 `suirs` 寄存器中接收方序号来获取 UINTC 读写端口的物理地址。若当前 `suirs` 寄存器中使能位为 0，则该指令执行失败。

`uipi.read` 指令直接访问 UINTC HIGH 端口读取数据；`uipi.write` 直接访问 UINTC HIGH 端口写入数据；`uipi.activate` 指令和 `uipi.deactivate` 指令直接访问 UINTC ACT 端口并向 Active 位写入 0 或 1 。

第 4 章　软件实现

4.1　QEMU

QEMU[1] 为操作系统和用户态程序提供虚拟的执行环境，通过动态的二进制转换，模拟 CPU 的行为，同时支持多种外设的仿真，在系统开发中扮演着重要角色。QEMU 支持模拟 RISC-V 运行环境，通过对 QEMU 的修改和测试，我们可以不断完善设计草案。对 QEMU 的修改主要分为四个方面：

- 指令翻译：引入对 `uipi` 指令的译码和执行；
- CPU 状态：维护 CSR 寄存器等 CPU 状态；
- 内存读写：`uipi` 指令需要直接访问物理内存和 UINTC 外设，直接调用 void cpu_physical_memory_rw(hwaddr addr, void *buf, hwaddr len, bool is_write) 函数完成对物理地址的读写；
- 核间中断：实现 UINTC 并向各个核发送中断。

4.1.1　指令翻译

QEMU 翻译一条指令的过程为：从客户机指令（Guest Instructions）到中间码（TCG，Tiny Code Generator），最后再到宿主机指令（Host Instructions）。QEMU 的翻译机制类似于 CPU 流水线中的译码阶段，需要定义模式串来帮助 QEMU 在执行到某一指令时调用对应的辅助函数。模式串的定义位于 target/riscv/insn32.decode：

```
1 uipi_send       0000000  00000 ..... 010 ..... 1111011 @r2
2 uipi_read       0000001  00000 ..... 010 ..... 1111011 @r2
3 uipi_write      0000010  00000 ..... 010 ..... 1111011 @r2
4 uipi_activate   0000011  00000 ..... 010 ..... 1111011 @r2
5 uipi_deactivate 0000100  00000 ..... 010 ..... 1111011 @r2
```

以 `uret` 这条指令为例，在 target/riscv/insn_trans 目录下，有各种指令的翻译过程，主要用来将指令解析的结果（寄存器，立即数等）传递给辅助函数，将客户机指令拆解为宿主机指令来模拟目标指令的功能。对于 `uret` 指令的执行涉及到较多 CPU 状态的变化，会对 pc ，CSR 等产生影响，辅助函数的定义位于 target/riscv/helper.h，通过宏定义 DEF_HELPER_x 来声明辅助函数，例如：

```
DEF_HELPER_1(\Iuret, tl, env)
DEF_HELPER_4(csrrw, tl, env, int, tl, tl)
```

其中第一个参数对应辅助函数的名称，第二个参数代表函数的返回值类型（tl 表示 target_ulong），后面的参数都是辅助函数传入的参数类型。有了以上的参考，我们可以定义其他辅助函数：

```
DEF_HELPER_2(uipi_write, void, env, tl)
void helper_uipi_write(CPURISCVState *env, target_ulong src) {
    if (uipi_enabled(env, env->suirs)) {
        uint64_t addr = UINTC_REG_HIGH(env->suicfg, SUIRS_INDEX(
            env->suirs));
        cpu_physical_memory_write(addr, &src, 8);
    }
}
```

4.1.2 CPU 状态

CPU 状态的维护位于 target/riscv/cpu.h。这个结构同时考虑了 RV32、RV64、RV128 的情况，这些寄存器都是 CPU 运行时必要的状态。包括但不限于：

- pc
- 整数、浮点寄存器堆
- CSR，有些寄存器是 M 态和 S 态复用的，例如 `mstatus` 、`mip` 等
- PMP 寄存器堆
- 通过 kernel_addr、fdt_addr 等从指定位置加载镜像

在 target/riscv/cpu.h 文件末尾的表中注册 CSR 的操作函数。

中断异常、CSR 等宏定义位于 target/riscv/cpu_bits.h ，我们需要在其中添加和 U 态有关的中断控制位。CPU 中断异常处理函数位于 target/riscv/cpu_helper.c 的最后，这个函数对中断异常原因进行判断，并根据 CPU 当前的特权级做不同的处理。这个函数只给出了 M 态和 S 态的中断异常处理，我们需要额外在此处加入委托给 U 态的中断异常处理，也就是读写 `ustatus` ，`ucause` ，`uepc` 等寄存器。

4.1.3 核间中断

QEMU 支持对不同硬件环境的模拟，我们的运行环境主要为 -machine virt ，需要在这块板子中添加 UINTC 外设的配置并生成设备树信息。

UINTC 代码实现位于 hw/intc/riscv_uintc.c ，调用 riscv_uintc_realize 对 UINTC 进行初始化，将 UINTC 外设连接到总线上，并初始化总线地址空间。对外设中的状态寄存器（接收方状态寄存器，中断信号寄存器等）进行内存分配和初始化。通过调用 qdev_connect_gpio_out 默认将 UINTC 的中断信号绑定至每个核的 `uip` 寄存器中的 `USIP` 位。

```
for (i = 0; i < num_harts; i++) {
    CPUState *cpu = qemu_get_cpu(hartid_base + i);
    RISCVCPU *rvcpu = RISCV_CPU(cpu);
    qdev_connect_gpio_out(dev, i, qdev_get_gpio_in(DEVICE(rvcpu)
        , IRQ_U_SOFT));
}
```

最后完成对 UINTC 读写函数的注册，这样就可以直接通过物理地址访问 UINTC 外设的读写端口了：

```
static const MemoryRegionOps riscv_uintc_ops = {
    .read = riscv_uintc_read,
    .write = riscv_uintc_write,
    .endianness = DEVICE_LITTLE_ENDIAN,
    .valid = {
        .min_access_size = 8,
        .max_access_size = 8
    }
};
```

在 UINTC 的实现中，中断是通过每次写入 UINTC 的端口来触发的，这和真实的硬件实现其实存在差异。例如在 U 态，从目前的设计草案来看，需要同时满足以下几个条件才可以触发中断：

- 当前特权级为 S 态
- `ustatus` 中 `UIE` 位是 1

- uie 中 USIE 位是 1
- uip 中 USIP 位是 1

在硬件实现中，可以看成是几个信号的与操作，当其他所有信号都拉高时，任何一个信号从低电平拉高都会触发中断，根据 RISC-V 的特权态规范[2]，sret 会将特权态从 S 态切换回 U 态，uret 会将 ustatus 中的 UIE 位设置为 UPIE 位，在这两条指令后执行的第一条指令都有可能被中断打断并立刻进入中断处理的流程，因此我们需要在 QEMU 中模拟这个过程，在 sret 和 uret 指令中直接对上述条件进行判断和处理，例如在 sret 的辅助函数中：

```
if (riscv_has_ext(env, RVN)
    && prev_priv == PRV_U
    && get_field(env->mip, MIP_USIP)
    && get_field(env->mstatus, MSTATUS_UIE)
    && get_field(env->sideleg, MIP_USIP)) {
    retpc = env->utvec;      // 直接跳转到U态中断处理入口
    env->uepc = env->sepc;   // 指定 \Iuret 到同一条指令
    mstatus = env->mstatus;
    mstatus = set_field(mstatus, MSTATUS_UPIE, 1);
    mstatus = set_field(mstatus, MSTATUS_UIE, 0);
    env->mstatus = mstatus;
}
```

4.2 Linux

4.3 libc

4.4 APP

第 5 章　硬件实现

5.1　Rocket Chip

5.2　UINTC 用户态中断控制器

5.3　UIPI 协处理器

5.4　RISC-V N 扩展

第 6 章　性能评估

第 7 章　结论

参考文献

[1] Bellard F, the QEMU team. About QEMU[EB/OL]. 2023. https://www.qemu.org/docs/master/about/index.html.

[2] Waterman A, Lee Y, Avizienis R, et al. The RISC-V Instruction Set Manual Volume II: Privileged Architecture Version 1.10[R/OL]. EECS Department, University of California, Berkeley, 2017. https://riscv.org/wp-content/uploads/2017/05/riscv-privileged-v1.10.pdf.

致　　谢

衷心感谢导师 ××× 教授和物理系 ×× 副教授对本人的精心指导。他们的言传身教将使我终生受益。

在美国麻省理工学院化学系进行九个月的合作研究期间，承蒙 Robert Field 教授热心指导与帮助，不胜感激。

感谢 ××××× 实验室主任 ××× 教授，以及实验室全体老师和同窗们学的热情帮助和支持！

本课题承蒙国家自然科学基金资助，特此致谢。

声　　明

本人郑重声明：所呈交的学位论文，是本人在导师指导下，独立进行研究工作所取得的成果。尽我所知，除文中已经注明引用的内容外，本学位论文的研究成果不包含任何他人享有著作权的内容。对本论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确方式标明。

签　名：_____ 日　期：_____

附录 A　补充内容

附录是与论文内容密切相关、但编入正文又影响整篇论文编排的条理和逻辑性的资料，例如某些重要的数据表格、计算程序、统计表等，是论文主体的补充内容，可根据需要设置。

A.1　图表示例

A.1.1　图

附录中的图片示例（图 A.1）。

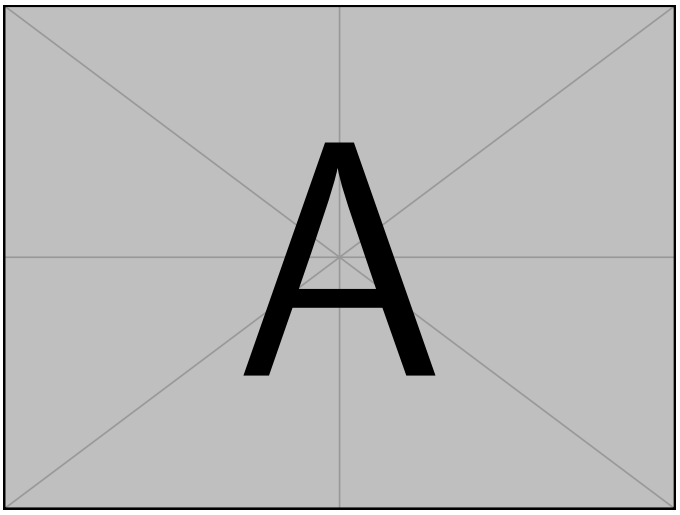

图 A.1　附录中的图片示例

A.1.2　表格

附录中的表格示例（表 A.1）。

A.2　数学公式

附录中的数学公式示例（公式（A.1））。

$$\frac{1}{2\pi \mathrm{i}} \int_{\gamma} f = \sum_{k=1}^{m} n(\gamma; a_k) \mathscr{R}(f; a_k) \tag{A.1}$$

表 A.1　附录中的表格示例

文件名	描述
thuthesis.dtx	模板的源文件，包括文档和注释
thuthesis.cls	模板文件
thuthesis-*.bst	BibTeX 参考文献表样式文件
thuthesis-*.bbx	BibLaTeX 参考文献表样式文件
thuthesis-*.cbx	BibLaTeX 引用样式文件