专业硕士学位论文

中国科学技术大学

(专业学位类型)

RISC-V 指令集模拟器的设计与实

现

作者姓名:王昊

专业领域:软件工程

校内导师:汪增福教授

企业导师:侯锐研究员

完成时间:二〇二二年一月二十八日

University of Science and Technology of China

A dissertation for master’s degree

(Professional degree type)

Design and implementation of

RISC-V instruction set

simulator

Author:

Speciality:

Supervisors:

Advisor:

Finished time:

Wang Hao

Software Engineering

Prof. Wang Zengfu

Prof. Hou Rui

January 28,2022

中国科学技术大学学位论文原创性声明

本人声明所呈交的学位论文,是本人在导师指导下进行研究工作所取得的成果。除已特别加以标注和致谢的地方外,论文中不包含任何他人已经发表或撰写过的研究成果。与我一同工作的同志对本研究所做的贡献均已在论文中作了明确的说明。

作者签名:\_\_\_\_\_\_\_\_\_\_\_签字日期:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

中国科学技术大学学位论文授权使用声明

作为申请学位的条件之一,学位论文著作权拥有者授权中国科学技术大学拥有学位论文的部分使用权,即:学校有权按有关规定向国家有关部门或机构送交论文的复印件和电子版,允许论文被查阅和借阅,可以将学位论文编入《中国学位论文全文数据库》等有关数据库进行检索,可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。本人提交的电子文档的内容和纸质论文的内容相一致。控阅的学位论文在解除后也遵守此规定。

□公开□控阅(\_\_\_\_年)

作者签名:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_导师签名:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

签字日期:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_签字日期:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

摘要

现行计算机编程语言的内存管理存在很多不安全的因素。像 C/C++将内存的使用交由程序员处理,这会导致许多与内存相关的安全漏洞,其中控制流劫持是利用内存安全漏洞所实施的一类常见且危害严重的攻击手段。它通过改变程序运行方向而实现攻击,针对这类攻击业界提出了许多相关的防御机制,但是这些防御机制由于自身的局限性和缺点,无法在安全性与性能上达到较好的平衡。如对C/C++语言实现的完全内存安全防御通常会产生较大的性能损耗,而部分地内存防御通常被证明不具有较强的安全保证。

为了解决这个问题一项针对代码重用攻击的防御机制被提出,其中的代码指针完整性(Code Pointer Integrity,CPI)的概念可以在安全性和性能开销之间取得很好的平衡,从而在保证控制流完整性的同时不会造成较大的性能开销。CPI的关键思想是将内存划分为常规区和安全区,并利用安全区来保护与程序控制流相关的数据。在此基础上增加了相关的程序跳转检查,保证了每一个控制流转移的正确性,从而实现对控制流劫持攻击的防御。但是随着相关的深入研究发现,CPI 在 X86-64架构上利用信息隐藏来隔离安全区的做法会导致较弱的安全性。攻击者可以利用程序中的内存信息泄漏探测到安全区位置,从而容易地对安全区实施攻击。

CPI 是一项很有潜力的安全技术,我们在 LLVM 编译器平台上实现了基于英特尔内存保护扩展(Memory Protection Extensions,MPX)硬件辅助机制的 CPI防御模型,同时我们改进安全区隔离方式来防止内存泄漏攻击,对安全区内存页施加一种基于硬件原语的读写保护机制来限制安全区域的读写权限,保证了即使安全区位置泄漏依然可以限制恶意代码的读写,这种强化的安全区隔离方法能够完全阻止对安全区的非法访问。为了验证所提方法的有效性,我们对所提出的相关模型进行了评估和验证。

关键词:代码指针完整控制流劫持内存保护扩展信息隐藏

ABSTRACT

There are many unsafe factors in memory management of current computer programming languages. Leaving the use of memory in the hands of programmers like C/C ++ can lead to many memory-related security vulnerabilities, among which control-flow hijacking is a common and serious attack method to exploit memory security vulnerabilities. It realizes the attack by changing the running direction of the

program. Many related defense mechanisms have been put forward in this kind of attack,

but these defense mechanisms cannot achieve a good balance between security and performance because of their own limitations and shortcomings. For example, full memory security defense for C/C++ implementations usually results in a high performance loss, while partial memory defense usually proves to be not a strong security guarantee.

To solve this problem, a defense mechanism against code reuse attacks is proposed,

in which the concept of Code Pointer Integrity (CPI) can strike a good balance between security and performance costs, so as to ensure the integrity of control flow without causing a large performance cost. The key idea of CPI is to divide memory into regular zones and safe zones, and use the safe zones to protect data related to program control flow. On this basis, related program jump check is added to ensure the correctness of each control flow transfer, so as to realize the defense against control flow hijacking attack. However, further research revealed that CPI's use of information hiding to isolate security zones on x86-64 architecture resulted in weak security. An attacker can exploit memory leaks in a program to detect the location of a security zone, making it easy to attack a security zone.

CPI is a security technology with great potential. We implemented CPI defense model based on Intel MPX hardware assist mechanism on LLVM compiler platform. Meanwhile, we improved security isolation method to prevent memory leak attacks. A read/write protection mechanism based on hardware primitives is applied to the security zone memory pages to limit the read/write permissions of the security zone, ensuring that malicious code can be restricted even if the security zone location is leaked. This enhanced security zone isolation method can completely prevent illegal access to the

security zone. In order to verify the

effectiveness of the proposed method, we evaluate and verify the proposed model

Keywords: code pointer integrity , control flow hijacking , memory protection

extensions,information hiding

目 录

摘 要 . I ABSTRACT . III 第 1 章 绪 论 . 1

1.1 研究背景 . 1

1.2 国内外发展现状 . 3

1.3 本文工作 . 6

1.3.1 CPI 缺点分析 . 6

1.3.2 具体工作 . 6

1.4 章节内容 . 6

第 2章 相关技术分析 . 8

2.1 LLVM 介绍 . 8

2.2 CPI 原理分析 . 14

2.3 英特尔 MPX 分析 . 16

2.4 英特尔 MPK 的分析 . 错误!未定义书签。

第 3章 系统需求分析 . 20

3.1 可行性分析 . 20

3.1.1 技术可行性 . 错误!未定义书签。

3.1.2 硬件可行性 . 错误!未定义书签。

3.2 功能性分析 . 21

3.2.1 功能概述 . 24

3.2.2 初始化需求 . 25

3.2.3 静态分析需求 . 25

3.2.4 动态插桩需求 . 26

第 4章 系 统 设 计 . 28

4.1 设计概述 . 28

4.1.1 系统功能模块概述 . 错误!未定义书签。

4.1.2 系统逻辑层次概述 . 错误!未定义书签。

4.2 静态分析模块设计 . 29

4.3 动态插桩模块设计 . 31

4.3.1 控制流检查 . 32

4.3.2 安全区保护锁 . 33

第 5章 系 统 实 现 . 34

5.1 概述 . 35

5.2 初始化实现 . 35

5.3 静态分析实现 . 38

5.4 控制流检查实现 . 51

5.5 安全区保护锁实现 . 错误!未定义书签。

第 6章 系 统 测 试 . 58

6.1 测试概述 . 58

6.2 测试方案 . 58

6.3 正确性分析 . 59

6.4 测试数据 . 60

第 7章 结论与展望 . 64

7.1 总结 . 64

7.2 未来工作 . 64

参 考 文 献 . 65

致 谢 . 69

1.1系统开发背景

近几十年来信息技术飞速发展,对芯片的各种要求越来越高,各种新型处理器不断面世。芯片的设计需要考虑其是否能够具有足够的市场竞争力,这与支持这款芯片的指令集架构的软件种类数量密切相关。例如,Inter x86架构的服务器和个人主机,在经过多年的发展,如今在商用和家用领域具有很高的市场占有率。考虑到成本和利润因素,芯片厂家在设计新的芯片时偏向于选用具有成熟生态环境的指令集架构。

进入21世纪以后,各国都在积极发展信息安全技术,同时由于知识经济以及人工智能、全球互联时代的到来,集成电路产业在国民经济中发挥着越来越不可替代的作用。我国的集成电路产业经过了几十年的发展,在某些应用领域也取得了不错的成绩,但在高性能处理器以及芯片设计的关键技术中,仍然面临着巨大的挑战。此外,我国的集成电路产业发展还承担着许多来自国际的压力[1-3]。不管是2018年中美贸易战中"中兴事件"和"华为事件"的发生,还是其他大国对我国实行的禁运政策,都让我国在市场竞争竞争中处于下风。

中国的芯片设计行业起步较晚,即使经过几十年的发展,它们仍未占据技术的制高点,自主指令集架构处理器的生态环境还没有完善。国内也还没有相对成熟的指令集架构,很多芯片的设计需要靠国外的技术授权,这不仅极大的提高芯片设计的成本,还会受到授权厂商的制约,市场竞争力不强,而且信息安全也有很大的问题。所有这些都极大地限制了国产自主架构处理器的应用和推广。

我国的集成电路产业经过了几十年的发展,在某些应用领域也取得了不错的成绩,但在高性能处理器以及芯片设计的关键技术中,仍然面临着巨大的挑战。此外,我国的集成电路产业发展还承担着许多来自国际的压力[1-3]。不管是2018年中美贸易战中"中兴事件"和"华为事件"的发生,还是其他大国对我国实行的禁运政策,都让我国在市场竞争竞争中处于下风。

[1]胡振波.手把手教你设计 CPU——RISC-V 处理器篇[M].人民邮电出版  
社,2018; TP332.021/22

[2]胡振波. RISC-V 架构与嵌入式开发快速入门[M].人民邮电出版  
社,2019; TP332/204

[3]胡伟武.计算机体系结构[M].清华大学出版社.机械工业出版  
社;2017; TP303-43/100

虽然近几年来我国的集成电路的出口量额程不断增长的态势,但该产业在国际贸易中仍处于较大逆差的状态,在国际贸易的竞争中,不管是2018年中美贸易战中"中兴事件"和"华为事件"的发生,还是其他大国对我国实行的禁运政策,都让我国在市场竞争竞争中处于下风。我过对该产业的发展有着最真实的、迫切的需求。历史的经历告诉我们,中国电子产业的整体发展必须要从中国制造向中国创造转型,否则高度依赖于他国的设计必定会对国家经济带来严重影响,如此以往将会成为我国国家安全的一大隐患。大力支持与发展我国的集成电路产业发展,并最终实现集成电路产业带动其他产业的工业化、信息化,为其他产业转型升级保驾护航,让我国在国际竞争中处于优势地位。

电子信息产品的核心就是 CPU 的芯片设计,它蕴含了众多的半导体技术,同时拥有重要的战略意义,象征着国家实力,也代表着国家发展水平[4]。

[4]朱子玉,李亚民. CPU 芯片逻辑设计技术[M].清华大学出版  
社,2005[14]

我国是世界上最大的发展中国家,为了持续提升本国的综合实力,就必须提高创造自主知识产权的能力,而发展国产 CPU 是提高信息产业自主创新能力、转变经济增长方式最佳切入点[5]。

[5]李华伟,李晓维等.可测试性设计在一款通用 CPU 芯片中的应用[J].计算机工程与应用,2002,16:191-194.

2014年公布的《国家集成电路产业发展推进纲要》就表明了国家对于集成电路产业发展的支持,这使得集成电路在近几年中成为了国家的战略产业。而作为一种特殊的集成电路,处理器芯片已经渗透到计算机、通信以及人们在生活所  
密切相关的所有行业中[1]

[1]郑永贵.基于 FPGA 的32位 RISC 微处理器的设计与实现[D].河北工业大学,2012.

在集成度越来越高的今天,面对数千万乃至上亿晶体管的规模,那种"设计硬件原型-实现-评估-改进-再实现"的模式已经无法满足现代设计应用的需求[1]

[1]金立忠,窦勇.微处理器体系结构模拟器 SimpleScalar 分析与优化[J].计算机应用研究,2006,8:197-198.

研究表明,如果在 CPU 的方案论证和设计阶段,没有及时发现问题与瓶颈,将会使后续的工作变得更为困难且代价更加高昂[3]。因此,在开发一个新的体系结构处理器时,为了确保处理器功能特性和性能参数达到设计的预期目标,对体  
系结构进行验证是一个必不可少的步骤[4]

[3] Neil V, Matthew I, Chinmay A, et al. Chip Multi-

Processor Scalability for Single-

Threaded Applications, ACM SIGARCH Computer Architecture News,2005,33(4):44-53.

[4]何锐. GPGPU 多核流体系结构与功耗模拟研究[D].国防科学技术大学,2010.

指令集架构(ISA, Instruction Set Architecture)[2]是软硬件之间至关重要接口,是处理器的灵魂。世界上第一块复杂指令集(CISC)微处理器芯片是在上世纪70年代由 Intel 公司工程师霍夫研发出来的,这款芯片就是 X86体系架构芯片,标志了 Intel 公司成为芯片领域巨头的开始。摩尔定律推动芯片事业蒸蒸日上,但是随着集成的指令集数量越来越多,硬件负荷增大,复杂指令系统无形中

增加了功耗和设计难度。针对这些弊端,David Patterson 提出了精简指令集(RISC)

计算机结构[2]

[2]包云岗.关于RISC-V成为印度国家指令集的一些看法[R].中国计算机学  
会通讯,2018年第1期

1.2国内外发展现状

LSE(Liberty Simulation Environment)是由普林斯顿大学开发的用于计算机系统建模的集成开发环境[15],该开发环境主要用来对计算机系统的并行结构化部件进行建模,然后自动生成模拟器,在模拟器的开发过程中可以最大限度地重用已有的组件,从而达到降低开发成本和难度的目的。利用 LSE 开发模拟器的过程如图1.1所示。

[15] M. Vachharajani, N. Vachharajani, D. A. Penry, et al. The Liberty Simulatio

n Environment: A Deliberate Approach to High-

Level System Modeling. ACM Transactions on Computer Systems,2006,24(3):211~249.

此外,比较著名的研究项目还有法国的嵌入式多体系结构模拟器 Qemu[24]、上海同济大学研制的 PEMU[25]以及浙江大学开发的 WuKong 系统[26]等。

[24] Bellard. The QEMU CPU Emulator[EB/OL]. http://fabrice.bellard.free.fr/qemu/,2004.

[25] Huang Yichun. ProEmulator Plug-

in Developer's Guide[EB/OL]. http://sourceforge.net/docman/,2004.

[26]柯化成.嵌入式系统全系统模拟器框架设计与实现[D].杭州:浙江大学,2006.

加利福尼亚大学伯克利分校发布了以 RISC-V 为基础,以硬件构造语言 Chisel 设计的全开放式硬件系统 Rocket[9]和 Boom[10]。

[9] Asanović, K., Avizienis, R., Bachrach, J., et al. The Rocket Chip Generator[R].EECS Department,University of California,Berkeley,Apr 2016.

[10] Celio, Christopher, Chiu, Pi-

Feng, Asanovic, Krste, et al. BROOM: An Open-Source Out-of-

Order Processor With Resilient Low-Voltage Operation in 28-nm CMOS[J]. IEEE Micro,39(2):52-60.

IBM 于2012年某研讨会中做了题为"IBM 使用模拟器的经验"的报告[16],对于 IBM 如何在处理器设计过程中使用模拟器进行了介绍.在处理器早期设计研究期间,IBM 使用 Mambo[17]模拟器的时钟精确模式进行微结构探索和粗粒度微结构定义.Mambo 模拟器对微结构主要模块和结构进行了模拟,该阶段 Mambo 由踪迹(trace)驱动,主要运行和研究用户态应用,对处理器的产品竞争力进行横向比较研究[16].在微结构设计实现期间,IBM 使用基于公司内部专用"T"语言编写的时钟精准模拟器 M1进行详细模拟处理器微结构[16],如图3所示.M1是以 Mambo 模拟器或者硬件上抓取的踪迹作为输入,并且可以收集非  
常详细的微结构数据进行性能评估.

为了加速 M1模拟器的执行速度,需要对所抓取的踪迹进行取样,同时为了方便调试,M1支持微结构性能数据可视化功能.在处理器验证阶段,IBM 使用 Mambo[17]作为处理器验证参考模型辅助进行验证,此阶段 Mambo 可以为处理器功能正确性提供参考结果.Mambo 模拟了所有处理器的功能特征,把某些性能相关的微结构维护操作(例如 cache 维护类指令)翻译成空(nop)操作,对于计算类指令产生准确的结果,并精准追踪处理器寄存器的状态变化,同时支持指令撤销操作,为处理器验证提供参考.IBM 基于 Mambo 模拟器曾发现PowerPC CPU 的一个控制寄存器存在竞争条件,使得该设计错误在流片之前就被发现并修改[17].在该阶段, IBM 还使用自研的由多个

FPGA(field programmable gate array)组成的 VHDL(very-high-

speed integrated circuithardware description language)仿真加速器 Twinstar[18]进行处理器综合验证.Twinstar 是时钟精准的仿真加速器,其推进方式是事件驱动模式,可以对整个处理器芯片进行仿真,以二进制程序作为输入,还支持详细的指令踪迹和处理器状态的实时追踪.该平台运行速度可以达到4MHz 并可以运行

未经修改的系统软件.类似 Twinstar 的验证平台还有帕拉丁[19]等.

在系统软件开发方面,IBM 基于 Mambo(加速模式)[17],Simics[20],BGLsim[21]等多种平台,在流片之前就开始进行固件、操作系统、虚拟机管理器等软件的早期开发.IBM 基于 Mambo 模拟器曾开发了 K42操作系统,在芯片可用之后1周内就启动了操作系统[17].IBM 基于 BGLsim-multi[21]平台和基于OMNeT++[22]开发的

MARS(message passing interface application replay simulation)模拟平台还可以对机群网络相关的功能进行模拟,模拟器由可执行程序或者踪迹驱动,其中 MARS

平台还可以对 MPI(message passing interface)类应用进行调优.

[16] Michael K. Experiences in simulation at IBM[EB/OL].2012. http://csa.cs.pitt.ed

u/presentations/csa2012\_kistler-michael.pdf

[17] Bohrer P, peterson J, Elnozahy M, et al. Mambo: A full system simulator for the

PowerPCarchitecture [J]. ACM SIGMETRICS Performance Evaluation Review,2004  
.31(4):8-12

[18] Asaad S, Bellofatto R, Brezzo B, et al. A cycle-accurate, cycle-

reproducible muti-FPGA system for accelerating multi-

core processor simulation [C]//Proc of the ACM/SIGDA Int Symp on Field Program

mable Gate Arrays. New York: ACM,2012:153-162

[19] Cadence. Palladium Z1 enterprise emulation platform datasheet [EB/OL].[2019-

01-23]. https://www/cadence.com/content/dam/cadence-

www/global/en\_US/documents/tools/system-design-verification/palladium-z1-ds.pdf [20] Magnusson P S, Christensson M, Eskilson J, et al. Simics: A full system simulati

onplatform [J]. Computer,2002,35(2):50-58

[21] Ceze L, Strauss K, Almasi G, et al. Full circle: Simulating Linux clusters on Linux clusters[C]//Proc of the 4th LCI Int Conf on LInux Clusters: The HPC Revolution.

New York: ACM,2003

[22] OpenSim Ltd. OMNeT++[EB/OL].[2019-01-

23]. http://ispass.org/ispass2007/keynote2.pdf

1.3本文的主要工作

1.3.1硬件设计与验证中的软件仿真

1.3.2具体工作

1.4章节内容

第2章相关技术分析

由于本系统是基于RISC-V指令集的体系结构模拟器,目标是模拟处理器执行RISC-V 汇编指令前后的软硬件行为,故本章首先介绍 RISC-V 指令集架构相关的内容以及体系结构模拟器的相关技术.

2.1常见的指令集架构概述

指令集架构是微处理器指令集架构(instruction set architecture)的缩写,有时也被称为"架构"。微架构(Microarchitecture)是指处理器的特定硬件实现方法。同种指令集架构,可以通过使用不同的微架构来设计不同性能的处理器,其制造的成本、性能可能会有差异,但是,只要是同一种架构的处理器,软件就可以直接运行在同种指令集架构的不同处理器上,而不需要做任何修改。而不同指令集架构的处理器上的软件就难以实现直接相互共用。

指令集架构不仅仅是指指令的集合,它还定义了处理器的一些硬件信息,比如寻址模式、寄存器设置、存储器、数据类型等等一些需要让程序员了解的硬件信息,以方便程序员进行软件开发。随着信息技术的发展,在这几十年间,世界上诞生了许多指令集架构,也消亡了很多指令集架构,现在保留的比较知名的

有 X86指令集架构和 ARM 指令集架构。下面就简单介绍下这两款指令集架构。

1978年,英特尔公司推出了第一款使用 X86指令集架构的处理器——英特尔

8086。在那个时代,CISC(复杂指令集架构)仍然是主流的指令集架构,但是经过几十年的发展,发现还是 RISC(精简指令集架构)才是未来发展的趋势。虽然是这样,但是因为 Intel 的 X86架构拥有完整的生态环境,并经过几十年的发展和其具有向后兼容性,使得其市场竞争力还是十分强大。又因为 IMB 公司也选用 X86指令集架构,并和 Intel 一起维护 X86的生态环境,这也再次使得

X86指令集架构的竞争力变得更强。X86指令集架构最开始诞生还是16位的指令集架构,但经过几十年的发展,经过32位,如今已经发展成64位架构。也因为 Intel 和 IMB 公司的大力发展,他们几乎垄断了个人计算机软硬件领域,

并因此获得了巨大的利润。X86是复杂指令集架构。它的指令长度是可变的,且编码比较混乱。给硬件设计和软件开发都带来了很大的困难,但是其具有先发优势,占据市场,还具有向后兼容性,使得其现今还是主流的架构。而且 Intel 公司也已经做出了很多优化。例如,Intel 采用"微码化"先把复杂的 CISC 指令

用硬件解码器翻译,变成简单的指令序列,然后再运行,采用流水线的方法,使得即使是 CISC 架构的 X86也可以借鉴 RISC 架构的优点。但是这样也带来了额外的硬件开销,影响其性能,但是这是作为 CISC 架构的 X86不得不付出的代价。X86架构不仅在 PC 领域取得巨大成功,它还进入服务器领域,并在服务器领域也取得了成功。X86架构的成功不仅带来了巨大的利润,也为其他架构的设计提供了参考。相对与 Intel 公司的 X86,ARM 架构是一种 RISC(精简指令集架构)。它具有32位固定长度的指令。1978年,一家 CPU 设计公司在英国剑桥诞生,之后,其设计并提出了 ARM(Acorn RISC Machine)指令集架构。如今,ARM 架构处理器因为其具有成本低、执行效率高等特点,在许多嵌入式系统被广泛使用。ARM 采用 RISC 架构,通常一个周期执行一条指令,并使用流水线操作来提高执行效率。它使用大量寄存器,使用寄存器进行操作,以及加载和存储指令,以批量读取和写入内存中的数据,从而提高了数据传输的效率。而且 ARM 的盈利方式也与 X86的不同,他不仅仅直接生产处理器芯片,而且还向其他 CPU 设计制造商提供知识产权(IP),并通过收取专利许可费来获取利润。如今,ARM 处理器占领了32位嵌入式处理器的大部分市场,并且是世界上使用最广泛的32位处理器体系结构。来自世界各地的数十家著名的半导体公司都在使用 ARM 的授权。然后通过自己的外围电路设计,开发的 ARM 处理器可用于许多领域。

2.2 RISC-V架构

第五代精简指令集(RISC-V, Reduced Instruction Set Computer - Five)是由加州大学伯克利分校的 David.Paterson 教授团队研发的一套指令集架构,其设计初衷是为了支持计算机体系结构的研究和教育,如今 RISC-V 已经成为行业实施的标  
准免费开源指令集架构

体系结构模拟器理论基础,硬件仿真器、软件模拟器,模拟开发流程图,解释型模拟 spike/Gem5(取值译码执行流程图)、编译型模拟 qemu(流程图),RISC-V 简介,相关开源社区工具介绍。

在 RISC-V 指令子集中,包括基础指令集和扩展指令集,在使用过程中必须实现基础指令集,而作为 RISC-V 的基础指令集-RV32I,仅包含了47种指令、且每种指令的编码方式都非常统一、富有规律,简单明了的使用文档也让许多初

学者能快速上手[7,8]。

[7] A Waterman. Y Lee. D APatterson. et al. The RISC-

V Instruction Set Manul. Volume I: User-

Level ISA [J].Eecs Department.2011.7(9):475.

[8] Andrew Waterman, Yunsup Lee, David Patterson, et al. The RISC-

V Instruction Set Manual, Volume I: User-

Level ISA, Version 2.1[R]. California: EECS Department, University of California,

Berkeley,2016.1-121

第五代精简指令集(RISC-V,Reduced Instruction Set Computer - Five)是加州大学伯克利分校研发的一款新的指令集架构,其设计初衷是为了支持计算机体系结构的研究和教育,如今 RISC-V 已然成为行业实施的标准免费开源指令集  
架构[22]。其特点如下:

(1)一个完全开放的指令集架构,可供学术界和工业界免费使用;

(2)适用于直接本机硬件实现,而不仅仅是模拟或二进制转换的真正的 ISA;

(3)避免在微体系结构(例如:顺序、乱序、解耦微处理器)或微技术(例如:全定制、ASIC、FPGA)实现中"过渡架构",并且在这些实现中更有效率  
的一款指令集架构;

(4) RISC-V 可以将指令集架构分成一个小的基本整数指令集架构,具备可选的标准扩展,以支持通用软件开发,并且可用于自定义加速器开发或教学;

(5)支持2008年修订的浮点 IEEE-754标准;

(6)一款支持广泛的用户级 ISA 扩展和专用变体的指令集架构;

(7)适用于应用程序,操作系统内核以及计算机硬件实现32位或64位地  
址空间变体;

(8)该指令集架构支持包括异构多核处理器在内高度并行多核的实现;

(9)可供用户选则的可变长度指令格式,对可用指令编码空间进行扩展,指令集架构所支持的可选密集指令编码用以提高性能,减小静态代码大小以及提升  
能量效率;

(10)完全可虚拟化的 ISA,可简化虚拟机管理程序开发;

(11)一个简化了新的管理员级和管理程序级的 ISA 设计。

RISC-V 指令集架构 ISA 定义为基本整数指令集架构,以及基本指令集架构的可选扩展,存在于任何以该指令集实现的硬件中。除了没有分支延迟槽并支

持可选的可变长度指令编码外,RISC-V 基本整数指令集架构与早期 RISC 处理器非常相似。该基础被严格限制为一组最小的指令集并且足以为编译器、汇编器、链接器和操作系统提供合理的目标,提供了方便的 ISA 和软件工具链,是一款可以构建更多定制处理器的指令集架构。

RISC-V 是一个典型的三操作数、以加载-存储为访存形式的精简指令集架构。

仅有 load 和 store 两类指令与外设存储地址交互数据,所以在指令的实现上相对简单,避免了大量的指令访问存储系统造成不必要的访问时间,这也是使用

RISC-V 设计的处理器高速化的一个重要因素[22-24]。指令集组成如表2.1所示。

指令集类型类型简写指令数说明

基本指令集 RV32I 47基本整数指令集,包含算数指令、访存指

令、环境调用

等指令,具有32个32-bit 通用寄存器,

32位寻址空间

RV32E 47 RV32I 指令集简化版本,专为嵌入式设

计,与 RV32I

相比寄存器数量减少为16个

RV64I 59整数指令,32个64-bit 通用寄存器,64

位寻址空间

RV128I 71整数指令,32个128-bit 通用寄存器,

128位寻址空间

扩展指令集 M 8乘除扩展,4条取余数,4条除法,5条

乘法操作指令

A 11原子扩展,包含原子读-修改-写、原子加

减或、异或等

F 26单精度浮点扩展,单精度访存、单精度浮

点运算指令

D 26双精度浮点扩展,双精度访存、双精度浮

点运算指令

Q 26四倍精度浮点指令扩展

C 46压缩指令扩展,16位指令编码,减少静/

动态代码大小

示 Integer,基本整数集包含了整数计算指令、整数加载指令、整数存储指令和控

其中,名称前缀中 RV32和 RV64表示处理器使用 RISC-V 指令集同时表明处理器中寄存器的位宽。在该指令集架构中基本整数指令集使用简写"I"来表

制流指令,实现基本整数指令集是任何一款基于 RISC-V 指令集架构的微处理器所必须满足的;标准的整数乘法和除法扩展使用简写"M"表示 Multiply,并添加指令以对整数寄存器中保存的值进行乘法和除法操作;标准的原子指令扩展使用简写"A"表示 Atomic,添加原子性的读取、修改和写入内存的指令,保证了多核处理器间的访存一致性;单精度浮点扩展使用简写"F"来表示 Float,该扩展增加了浮点寄存器、单精度计算指令和单精度加载以及存储指令;标准的双精度扩展使用简写"D"表示 Double,扩展了浮点寄存器,并且增加了双精度计算、加载和存储指令。整数基数集加上四个标准扩展(即"IMAFD")可以缩写为"G",表示实现通用标量指令集。

RISC-V 的指令集使用模块化的方式进行组织,每一个模块使用一个英文字母来表示。RISC-V 最基本也是唯一强制要求实现的指令集部分是由 I 字母表示的基本整数指令子集,使用该整数指令子集,便能够实现完整的软件编译器。其他的指令子集部分均为可选的模块,具有代表性的模块包括 M/A/F/D/C,如表1所示。

为了提高代码密度,RISC-V 架构也提供可选的"压缩"指令子集,由英文字母 C 表示。压缩指令的指令编码长度为16比特,而普通的非压缩指令的长度为

32比特。以上这些模块的一个特定组合"IMAFD",也被称为"通用"组合,由英文字母 G表示。因此 RV32G 表示 RV32IMAFD,同理 RV64G 表示 RV64IMAFD。

为了进一步减少面积,RISC-V 架构还提供一种"嵌入式"架构,由英文字母E 表示。该架构主要用于追求极低面积与功耗的深嵌入式场景。该架构仅需要支持16个通用整数寄存器,而非嵌入式的普通架构则需要支持32个通用整数寄存器。

通过以上的模块化指令集,能够选择不同的组合来满足不同的应用。譬

如,追求小面积低功耗的嵌入式场景可以选择使用 RV32EC 架构;而大型的64位架构则可以选择 RV64G。

如图2.1所示,RISC-V 基本指令格式有 R/I/S/U 四种及其变种类型。所有固定的32位指令在内存中必须4-byte 对齐。其中使用 I 类型指令格式的指令有:整型计算指令中的寄存器-立即数操作指令、左移右移指令、直接跳转指令、Load 指令以及系统调用指令。使用 R 类型指令格式的有:整型计算指令中的寄存器-寄存器操作指令、扩展原子类指令、单精度浮点算数指令。使用 S 类型指令格式的有:Store 类指令。使用 U 类型指令格式的有:LUI 以及 AUIPC 指令。

RISC-V 指令集架构所使用的定点通用寄存器如表2.2所示,浮点通用寄存器如表2.3所示。

寄存器助记符描述调用与被调用

x0

x1

x2

x3

x4

x5

x6-7

x8

x9

x10-11

x12-17

x18-27

x28-31

zero

ra

sp

gp

tp

t0

t1-2

s0/fp

s1

a0-1

a2-7

s2-11

t3-6

硬编码为0

返回地址寄存器

堆栈指针寄存器

全局指针寄存器

线程指针寄存器

临时/备用链接寄存器

临时寄存器

保存的寄存器/帧指针

保存的寄存器

函数参数/返回值寄存器

函数参数寄存器

保存的寄存器

临时寄存器

-

调用者

被调用者

-

-

调用者

调用者

被调用者

被调用者

调用者

调用者

被调用者

调用者

寄存器助记符描述调用与被调用

f0-7

f8-9

f10-11

f12-17

ft0-7

fs0-1

fa0-1

fa2-7

浮点临时寄存器

浮点保存寄存器

浮点参数/返回值寄存器

浮点参数寄存器

调用者

被调用者

调用者

调用者

f18-27

f28-31

fs2-11

ft8-11

浮点保存寄存器

浮点临时寄存器

被调用者

调用者

2.3体系结构模拟器

体系结构模拟器根据模拟的详细程度可以分为功能模拟器(指令集模拟器 ISS,Instruction Set Simulator)和性能模拟器(时钟周期精确模拟器)两类。前者只模拟目标系统的指令集体系结构,比如寄存器状态、指令语义、存储器状态等功能特性;后者除了模拟功能特性外,还模拟目标系统的微体系结构,比如  
流水线、分支预测、Cache 层次等[13]

[13]喻之斌,金海,邹南海.计算机体系结构软件模拟技术[J].软件学报,2008,4:1051-1067.

踪迹驱动模拟将每条指令顺序执行所产生的所有信息作为模拟器的输入,从

而模拟某种体系结构处理器的功能和性能[30]

[30] Belady L.A study ofreplacement algorithms for a virtual storage computer.IBM System Journal,1966,5(2):78-101.

解释型 ISS 最大的特点在于直接将硬件行为映射到软件[31]

[31] Dwarkadas S,Jump J.Execution-Driven simulation of mu1tipr0cess0rs:Address and timing analysis.ACM Trans.on Modeling and Computer Simulation,

1994,4(4):314-338.

模拟器是体系结构量化分析的重要手段,对架构设计、芯片开发有重要的指导作用.基于模拟器辅助进行集成电路设计可以追溯到1980年代,自此模拟器便一直是处理器设计过程中不可或缺的工具.在芯片开发过程中,体系结构模拟  
器可以缩短处理器的设计时间,降低开发成本,其具体作用如图1所示:

由图1可知:

1)在芯片开发早期,基于模拟器可以进行微结构探索和粗粒度微结构定义,

此时模拟器的开发抽象层次较高.

2)随着处理器设计的不断推进和模拟器的不断完善,基于模拟器可以持续对

芯片微结构进行评估、修改和取舍.

3)当模拟器趋于成熟,可以对微结构、多核互联系统、一致性协议等进行详

细性能分析,基于分析结果对微结构进行微调.

4)在对处理器逻辑设计进行验证的阶段,模拟器可以作为参考模型辅助进行

验证,可以快速定位逻辑设计错误.

5)在未流片之前基于模拟器就可以开展系统软件开发和适配工作,这样可以

在芯片流片结束后以最快速度启动系统软件.

6)流片结束后,基于模拟器可以辅助进行芯片硅后验证环境的搭建以及测试用例编写工作.为了保证模拟器可以顺利辅助进行处理器设计,在整个芯片开发过程中,需要持续对模拟器进行校准,通过持续对比模拟器和寄存器传输层(Register-Transfer Level, RTL)之间的差别,可以互相校准并发现模拟器或者 RTL的设计错误.

模拟开发的基本流程如图2.1所示。进行模拟,首先通过对实际硬件系统建模来将之具体化。建模与具体化的过程中必须保证所建模型的结构与实际硬件系统相近或一致,以确保所建模型的精确性,只有精确度较高的模型才能真实的模拟出硬件系统的行为,最终获得正确的结果。在对硬件系统的建模过程中,需要考虑所选择的算法是否合适。评价一种算法是否合适的准则在于是否符合模拟的要求和硬件系统的特征。为了保证最终的模拟精度,必须确保所选择算法的精度够高,稳定性够好。选定合适的算法后,进行程序设计,即用程序语言将模型描述出来。待确定程序模型的正确以后,就可以用这个模型来进行模拟实验,得到相应的结果。最后分析模拟结果,结果分析既可以是针对模型本身的数据,对模型本身进行评价或研究;也可以是对模拟的目标系统性能作出评价。

体系结构模拟器的驱动方式主要分为两种:执行驱动(又叫程序驱动)和踪迹驱动,这两种驱动方式对应的指令集模拟策略分别是编译型模拟和解释性模拟.

加州大学伯克利分校设计的开放指令集 RISC-V 已成为处理器设计和研究领域的热门,为了实现处理器的敏捷开发,伯克利分校还开发了高度参数化的硬件构建语言 Chisel[55].使用 Chisel语言设计处理器,可以直接使用面向对象的设计方法学描述处理器功能,这与传统意义上开发周期精确模拟器的方式很像,但特别之处在于:通过编写一次硬件代码可以生成包含 C++时钟精准模拟器、FPGA Verilog和 ASIC Verilog这3个目标[55].具体地在生成模拟器方面,基于最新 Chisel3编写的硬件代码可以产生 Firrtl中间描述语言(inter-mediate representation,IR),从 Firrtl

可以直接翻译或者转换成 Verilog,进而通过 Verilator工具可以生成时钟精准的 C++模拟器和测试框架.但是,通过这种方式生成的模拟器代码可读性和可修改性都比较差.Chisel 语言使逻辑设计和模拟器开发得到了统一,使得处理器设计效率提高一个数量级[56],因此可以大幅加速硬件设计,这是新的硬件敏捷开发方法学,同时也是未来处理器设计和模拟器发展的  
一个重要方向.

2.2.1执行驱动模拟

随着体系结构的研究越来越深入,其设计的复杂度越来越高,这给模拟器的性能带来了一定的负面影响。为了提高模拟性能,研究者们对模拟过程进行了改进,引入了编译的思想——采用一次翻译多次执行的方法来缩短模拟过程中指令译码的时间。译码就是将目标指令翻译成宿主机可识别的指令,宿主机通过这些指令来完成对目标机状态的操作。根据译码过程处于编译还是运行时,编译型指令集模拟器又可分为静态编译型指令集模拟器(Static Compiled ISS)和动态编译型指令集模拟器(Dynamic Compiled ISS)。由 Zhu and Gajski 给出的静态编译型指令集模拟器将本处于运行时的指令译码过程转移至编译时,如图2.5所示。目标机二进制代码经编译器编译,之后由代码生成器优化生成宿主机的二进制代码,并最终运行于宿主机。

该技术有一个缺点,那就是要求程序代码为静态的,这就使得静态编译技术只能为一小部分数字信号处理器所使用。与典型的 DSP(数字信号处理器)应用不同的是,微处理器通常面向的是完整的操作系统,而操作系统有一个重要的特点——程序代码在运行时是动态的,这就局限了静态编译型模拟器的广泛使用。

动态编译型指令集模拟器的典型代表为 Embra[33]及 Shade[34],其工作流  
程如图2.6所示:

其基本思想是复用译码信息,即在内存中取出一条指令后,判断该条指令是否是第一次执行,若是,那么对其进行译码,并在译码完成后将译码信息保存到Cache 中,然后执行;若不是,则直接在 Cache 中调用该指令的译码信息执行。由于该技术在程序运行时进行指令译码,因此很难进行代码优化。

对于执行驱动模拟,存在两种不同的观点:一种认为执行驱动模拟器输入的是程序的二进制文件(可执行指令),而不是踪迹信息,因此,模拟器的输入集大小只与程序的静态指令数相关,而与动态指令数无关。如图2.3(a)所示,由模拟器来执行程序的所有可执行指令。还有一种观点认为,执行驱动模拟器的输入信息(程序的可执行指令)分成两部分:一部分由宿主机代为执行,另一部分则  
2.2.2踪迹驱动模拟

由模拟器执行。如图2.3(b)所示,这类模拟器只执行与所研究问题相关的指令,其它指令则由宿主机代替执行。这样做的优点在于模拟速度较快,但是这种模拟方式要求宿主机与目标机的指令集体系结构一致,这就限制了它的应用范围。

执行驱动模拟器将用高级语言编写的应用程序经编译和链接后得到的二进制文件作为输入信息,在模拟过程中会模拟系统的动态特征,如动态指令的生成和分支预测等,因此更加接近目标系统的真实情况,精确度更高。然而,也正是由于需要模拟目标系统的动态特征,使得执行驱动模拟器的模拟速度较踪迹驱动模拟器更慢。

长期以来,由于工作原理简单和模拟精度高,解释型指令集模拟器受到了广泛的关注(如 Gem5、SimpleScalar 等)。解释型 ISS 最大的特点在于直接将硬件行为映射到软件[31],从而模拟出真实的硬件环境。由于其对指令进行逐条翻译,使得指令的执行可以很好的被控制。解释型指令集模拟器的工作流程很简单,通常是取指(fetch)-译码(decode)-执行(execute)的循环,如图2.4所示。

1)取指:从模拟器的内存空间中取出一条指令.

2)译码:对取出的指令进行翻译,得到指令的操作码、操作数、执行函数等信息.

3)执行:执行指令所对应的执行函数,并修改相应寄存器的值,包括 PC 寄存器.

解释执行的工作流程使得解释型 ISS 设计原理比较简单,易于设计和实现,且灵活性较好,模拟精度高。由于其对指令进行逐条翻译然后执行,使得其可以很容易的实现调试机制。但是也正是由于需要对指令进行逐条翻译,导致模拟器需要在译码阶段花费大量的时间,所以解释型指令集模拟器的模拟速度一般不是很高。

第2章相关技术分析

踪迹驱动模拟将每条指令顺序执行所产生的所有信息作为模拟器的输入,从而模拟某种体系结构处理器的功能和性能。其模拟过程如图2.2所示。

假设要模拟的目标系统为 T,目标系统上执行的应用程序为 w,则模拟 T 中 w 执行的问题可以分解为两个部分:生成踪迹信息以及输入踪迹信息进行模拟。如果把生成踪迹信息的系统命名为 G,那么,踪迹信息就是 G 执行 w 时产生的所有信息。接下来将踪迹信息作为模拟器的输入,在目标系统 T 中模拟执行 w。踪迹驱动的优点在于比较简单,而且可以不关心其它无关部分而只对局部进行详细的模拟。但是这种方式要求生成踪迹的系统 G 与模拟的目标系统 T的体系结构相似,否则由 G 生成的踪迹信息不能正确反映 w 在 T 上的实际运行情况,从而导致获得错误的模拟结果。踪迹驱动的另外一个缺点在于模拟器的输入信息是静态的,不能对目标系统的动态特征进行研究。

2.4本章小结

第2章相关技术分析

第3章系统需求分析

需求分析是软件生产周期中的一个重要环节,本章将采用面向对象分析的方法对体系结构模拟器的需求进行具体分析与建模.明确模拟器所需实现的功能性需求和非功能性需求.

3.1需求导出

近几十年来信息技术飞速发展,对芯片的各种要求越来越高,各种新型处理器不断面世。芯片的设计需要考虑其是否能够具有足够的市场竞争力,这与支持这款芯片的指令集架构的软件种类数量密切相关。例如,Inter x86架构的服务器和个人主机,在经过多年的发展,如今在商用和家用领域具有很高的市场占有率。考虑到成本和利润因素,芯片厂家在设计新的芯片时偏向于选用具有成熟生态环境的指令集架构。

中国 CPU 设计行业起步较晚,即使经过几十年的发展,它们仍未占据技术的制高点,自主指令集架构处理器的生态环境还没有完善。国内也还没有相对成熟的指令集架构,很多芯片的设计需要靠国外的技术授权,这不仅极大的提高芯片设计的成本,还会受到授权厂商的制约,市场竞争力不强,而且信息安全也有很大的问题。所有这些都极大地限制了国产自主架构处理器的应用和推广。而且,芯片设计属于核心技术,与国家战略有关,国家和科研机构都迫切需要采用独立自主的指令集架构的处理器,来消除中国在电子信息领域和国防信息安全等方面的问题。

Fpga/流片上的系统软件移植测试:软件交叉编译(vmlinux 5min),粘贴 fsbl,vivado 平台烧录(15min)/流片验证就是烧写平台(20min),xilinx SoC,启动bbl,内核启动,然后只有单步命令行调试,或者 jtag。

软硬件行为的模拟,忽略一些指标如缓存加速等硬件性能指标类的测试。主要关注寄存器状态,内存状态,中断系统工作情况,调试交互信息等。

功能性需求:前端设计(gui、text/寄存器/内存/pc 指令流、交互/设置断点/中断下发/内存查询/调试过程、保存快照);指令集注册/解析(riscv-opcodes);单条指令 step 前后的寄存器/内存状态转移(指令对应的功能函数/主要的行为模拟)/即指令的单步执行模拟(这部分是重点,包括寄存器和其他存储部件的模拟)/指令流执

行的驱动方式;中断系统模拟(clint 时钟/软中断;plic 外部中断);调试模块的设  
计,主要是在功能函数前后进行断点检查(针对寄存器/内存状态的检查)

非功能性需求:可拓展性,UI 易用性,速度,模拟精度,代码膨胀率

在芯片设计及验证的流程中,对于基础系统软件尤其是操作系统,底层驱动等的适配和验证往往是反馈硬件设计缺陷最频繁的部分,这部分的工作不仅是对于前期硬件设计的重要测试,也是后续用户态程序开发的基础。对于系统软件的移植和适配工作,有两种主流方式,一种是在模拟芯片硬件特性的 FPGA 开发板上仿真,另一种是通过软件模拟。两种方法各有利弊,FPGA 开发板更加接近真实硬件环境,能够获取精确的仿真信号,但是速度相对较慢,并且能够提供的调试信息较少。而模拟器环境下的开发,其运行速度接近宿主机,并且调试方便,虽然信号精度与真实硬件有差异,但是能够在测试的前期反馈大部分的缺陷。所以真实的开发和测试流程一般是先使用模拟器验证,再上 FPGA 平台仿真,这样既能够提高开发效率,又不失精度.

随着 RISC-V 开源社区的日益壮大,更多的芯片设计厂商选择 RISC-V 作为其指令集架构,在芯片的验证过程中,软硬件适配工作作为测试的重点,往往需要模拟器环境的支持,当前开源社区的指令集模拟器 spike 由 SiFive 公司维护,能够定期地更新 RISC-V 的最新特权级指令,是各厂商优先考虑使用的基础模拟器。厂商可以根据自身产品特性,拓展 spike 支持的设备,并在此基础之上进行软件移植工作和前期软硬件设配工作,以此来提高芯片验证与测试工作的效率。因此,模拟器的优化与拓展,应该在硬件层面上与待验证芯片的硬件特性相符合,又要在软件层面上满足调试功能易用性的要求。

RTL 级,register transfer level,指的是用寄存器这一级别的描述方式来描述电路的数据流方式,rtl 级可以理解为,可以直接给综合工具生成你要的网表的代码。

目前RISC-V开源社区的指令集模拟器是spike,由SiFive公司维护,spike模拟实际代码执⾏过程中的软硬件⾏为,提供指令级别的仿真,本质上就是C++程序模拟每条指令执行过程中的软硬件行为,当前最新版本的spike模拟的设备包括总线,内存,时钟,处理器,和调试模块,这些部分能够使得spike运行一个简单的代理内核,并运行一些简单的RISC-V指令集架构的程序。但是对于真正进行RISC-V芯片设计工作的团队来说,spike模拟的内容还远远不够。真实的设计要复杂得多。

spike 模拟器的运行过程包括三个部分,模拟器自身部分,面向开发者(用户)的串口调试部分,以及目标程序部分。目标程序一般指的是移植到 RISC-V 平台

的通用基础软件,如 linux 内核,处理器所支持外设的驱动程序等,这部分程序涉及到的资源就是模拟器应该支持的部分。因此,本次课题涉及到的需求分为两个部分,一个就是对上述功能模块提供模拟器支持的需求,另一部分是优化串口调试模块的需求。

3.2分析建模

指令集模拟器的主要参与者是进行系统软件开发和移植的程序员,通过对实

际芯片开发验证过程的分析和归纳,得出模拟器所需要的主要功能有:

1)设置模拟器启动配置,包括 elf 文件路径添加,指令集模块注册,运行模式选择等.

2)模拟器执行流程控制.包括正常运行模式下的 uart 串口交互,暂停执行进入调试模式,模拟器重启.

3)调试功能.在调试模式下,进行断点设置,内存查询,历史指令查询,单步执行等.

4)模拟外部中断信号发送.

综上所述可以得出如表1.1所示的用户需求描述表.名称参与者说明

模拟器配置并启动系统软件开发/移植程序员设置模拟器启动参数并

运行

切换至调试模式系统软件开发/移植程序员模拟器从运行模式切换

为调试模式

切换至运行模式系统软件开发/移植程序员模拟器从调试模式切换

为运行模式

重启模拟器系统软件开发/移植程序员重新加载当前配置项并

运行

断点设置系统软件开发/移植程序员调试模式下进行断点添

加/移除

内存查询系统软件开发/移植程序员调试模式下对虚拟地址/

物理地址内容查询

中断信号发送系统软件开发/移植程序员点击外部中断源按钮,发

送对应的外部中断到plic

根据用例描述表可以得出系统软件开发/移植程序员的用例图如图1.1所示

下面分别对系统软件开发/移植程序员的五个主要用例进行详细描述.

用例名称模拟器配置并启动

用例描述设置模拟器启动参数并运行

触发条件勾选模拟器配置选项,输入 elf 文件路

径

后置条件模拟器解析配置参数,启动程序

基本事件流(1)输入 elf 文件路径

(2)选择启动模式是否为调试模

式

(3)其他参数勾选,包括核心数,模

拟外设路径等

异常事件流配置参数错误,启动失败

用例名称切换至调试模式

用例描述模拟器从运行模式切换为调试模式

触发条件点击 run/stop 按键

后置条件模拟器进入调试模式/模拟器进入运行

模式

基本事件流在运行模式下点击 run/stop 按键

异常事件流运行模式下点击 run 按键/调试模式下

点击 halt 按键

用例名称断点设置

用例描述调试模式下进行断点添加/移除

触发条件在调试窗口勾选断点类型,输入断点条

件,点击"应用"

后置条件点击 run 进入运行模式,模拟器运行至

断点条件触发调试中断,进入调试模式

基本事件流(1)调试窗口添加/移除断点

(2)程序运行,触发断点

(3)进入调试模式,打印断点信息

异常事件流断点信息填写错误导致无效断点条件

用例名称内存查询

用例描述调试模式下对虚拟地址/物理地址内容

查询

触发条件查询窗口输入内存地址,点击查询

后置条件输出内存对应地址内容

基本事件流选择地址类型为虚拟地址/物理地址,

虚拟地址需要指定核心,输入16进制

地址,点击查询

异常事件流输入无效地址导致访存失败

用例名称 mailbox 中断信号发送

用例描述点击外部中断源按钮,发送对应的外部

中断到 plic

触发条件点击对应中断源的中断信号发送按键后置条件模拟器响应中断,执行中断处理程序基本事件流(1)点击 mailbox 中断源发送中断  
信号

(2)弹出 mailbox 消息窗口,填写消

息,点击发送

(3)系统接受外部中断,执行自定

义的中断处理函数,显示在 mailbox 窗

口

异常事件流 mailbox 中断发送后系统无响应

3.2.1串口调试模块

spike 本身具备单步调试的功能,但是在模拟真实硬件行为的复杂场景下,命令行式的单步调试显然难以使用,根据以往的调试经验,人性化的 UI 设计需要涉及到处理器状态寄存器,当前特权级模式,程序运行窗口等信息,还需要设置对应多核的寄存器触发条件,实现 mailbox 中断主动触发,保存快照方便复现bug 等功能。

第3章系统需求分析

这部分的功能需求主要有:

(1)对于多核心独立 csr 寄存器触发条件的支持

(2)对内存/指令格式等触发条件的支持

(3)能够查询历史指令序列执行情况

(4)实时监测状态寄存器,当前特权级模式

(5)主动发送 mailbox 中断信号

3.2.2平台级中断控制器 PLIC

RISC-V 核心(hart)包含 local 中断源和 global 中断源。只有 global 中断源可以被 PLIC Core 响应,通常为 I/O 设备,PLIC 负责将中断源(global interrupt sources)链接到中断对象(interrupt targets),也就是处理器核心。spike 自身不支持 PLIC 设备,所以对于外部中断的支持只能通过轮询来实现,效率相当低下,并且不符合实际处理器的特性。因此,首先对 spike 的拓展便是PLIC 的支持,对于 uart,spi 等串口控制器,可以在后续通过设备树直接挂载为 PLIC 的中断源。多个外设作为独立的中断源,通过 PLIC Core 仲裁,将外部中断信号传递给相应的核心。PLIC 中断控制流程如图1所示。

第3章系统需求分析

图1 PLIC 中断控制流程

对 PLIC 设备模块的需求是,模拟器启动 linux 内核,并且 uart 以中断号2成功挂载到 PLIC,通过查看/proc/interrupts 进行验证,具体的设计见系统概要设计部分。

3.2.3 uart16550串口控制器

spike 提供 HTIF 模拟串口通信控制器, HTIF 是伯克利处理器的非标准工具,因此没有文档。随着 RISC-V 平台规范的发布和内核的更新为自托管,HTIF很快就会消失。HTIF 是主机/目标接口,它通过 riscv-fesvr 与目标设计(Sodor)通信。riscv-fesvr 通过 HTIF mem 端口将二进制文件加载到 Sodor 内存中,然后通过状态寄存器告知内核。程序完成后,Sodor 告诉 riscv-fesvr,它通过重置主机 CSR 完成交互,模拟结束。

在 bootloader 加载内核之前,串口通信控制器就必须能够工作,提供裸机的交互功能,是前期进行串口调试的重要工具,能够结合 spike 的单步调试功能完成前期的大部分调试工作,其实现的优先级很高。

总体来说,HTIF 提供了串口通信的功能,但是其本质上还是需要主机的轮询查询,效率很低,考虑到实际硬件设计中必不可少的串口通信控制模块(uart16550a 芯片),需要为 spike 添加 uart模拟,通过外部中断的方式实现串口通信.也可以在模拟器上完成对 uart 的前期测试,包括波特率的设置,传输模式的选择等等.

3.2.4 mailbox 核间通信模块

由于本次设计涉及到的芯片是一款主动安全处理器芯片,通过和其他厂商计算核心的互联发挥作用,核间的 mailbox 通信部分至关重要.区别于 ipi 处理器内部中断方式, mailbox 是一种框架,通过消息队列和中断驱动信号处理多处理器间的通讯.

对 mailbox 的模拟,需要满足高并发的异步通信需求,鉴于无法真实模拟与另一个计算核心的通信,需要对模拟器核心间通信添加 mailbox 支持,来模拟真实的交互环境.

3.3非功能性需求

该指令集模拟器的非功能性需求有:

(1)准确性:体系结构模拟器的首要需求就是准确性,只有准确模拟出真实硬件的行为,才能在模拟器上进行后续的软件开发和移植工作.由于本模拟器的模拟精度在指令级别,不涉及到流水线,乱序执行,分支预测等更细粒度的模拟,因此要求模拟器要和真实硬件在寄存器级别完全一致.

(2)可靠性:可靠性要求模拟器要能够在使用过程中持续稳定运行,不会因为宿主机上程序的设计缺陷导致模拟过程发生崩溃.如果遇到异常情况,模拟器需要能够在不修改启动配置的情况下重启成功,且模拟过程是可复现的.

(3)实时性:作为一个基于指令集翻译的体系结构模拟器,虽然本身的设计初  
衷不是为了测试 CPU 性能,但是模拟器运行速度

(4)友好性:

4.1系统概述

本系统是针对RISC-V芯片开发团队在系统软件开发和移植过程中使用的体系结构模拟器.将编译好的 RISC-V 架构可执行代码加载到模拟器上运行,观察执行结果,能够脱离实际硬件平台进行系统软件的调试,也能帮助开发人员及时发现硬件实现可能存在的缺陷,从而提高整个芯片开发过程的效率。

指令集模拟(riscv-opcodes),取值译码执行过程;寄存器/存储器设计;中断系统设计;前端设计。整体各模块层次图。

4.2系统静态结构

RISC-V 指令集模拟器的整体功能模块如图1.1所示,主要包含四个功能模块:预加载模块,指令流执行模块,调试模块和 UI 显示模块。其中,预加载模块包括模拟器参数配置,指令集注册,加载 elf 文件功能;指令流执行模块包括了主要的 Hart 模拟,中断控制器模拟,内存模拟,外设模拟等功能,是模拟器的主体功能模块;调试模块包括断点设置,内存查询,模拟中断信号发送功能;UI显示模块包括目标层序执行窗口,调试窗口等的可视化界面和模拟器状态查询功能。

指令流执行模块是模拟器的主体功能模块,该模块模拟了单条指令执行过程的硬件行为,包括寄存器,总线,内存,MMU,缓存,通过内存映射的 I/O 设备等。

RISC-V 的不同寻常之处,除了在于它是最近诞生的和开源的以外,还在于:

模拟出的 RISC-V CPU 整体架构如图1.1所示,每个处理器都有独立的寄存器组,内存管理单元,所有处理器共享同一个 ICache,dCache,紧随其后的是

L2Cache 和主存。处理器通过总线和其他内存映射的 I/O 设备通信,包括BootRom,RTC,UART,PLIC,Mailbox,Debug Module.

指令集架构:

RV32I 是一个 load-store 体系结构,也就是说,只有 load 和 store 指令可以访问存储器,而算术指令只在 CPU 寄存器上进行操作运算。RV32I 提供了一个32位用户地址空间,它是字节寻址并且是小端的。执行环境将定义这个地址空间的  
哪些部分是可以合法访问的

和几乎所有以往的 ISA 不同,它是模块化的。它的核心是一个名为 RV32I 的基础 ISA,运行一个完整的软件栈。RV32I 是固定的,永远不会改变。这为编译器编写者,操作系统开发人员和汇编语言程序员提供了稳定的目标。模块化来源于可选的标准扩展,根据应用程序的需要,硬件可以包含或不包含这些扩展。这种模块化特性使得 RISC-V 具有了袖珍化、低能耗的特点,而这对于嵌入式应用可能至关重要。RISC-V 编译器得知当前硬件包含哪些扩展后,便可以生成当前硬件条件下的最佳代码。惯例是把代表扩展的字母附加到指令集名称之后作为指示。例如,RV32IMFD 将乘法(RV32M),单精度浮点(RV32F)和双精度浮点(RV32D)的扩展添加到了基础指令集(RV32I)中。

第二章已经详细介绍了 RISC-V 指令集架构,本系统模拟了 RV64imafd 共  
196条指令,这些指令的添加参照

由于本系统忽略了具体硬件实现上的流水线细节,所以就指令控制流程来说本模拟器是一个单周期的 CPU,流水线对应的取值,译码,执行,在模拟器上对应解码器解析汇编指令,执行汇编指令对应的功能函数。

4.3系统动态结构

本模拟器是 trace-accurate 的指令集模拟器(功能模拟器),模拟器运行的基本结构如图1.1所示。

首先使用 RISC-V 交叉编译工具链将目标程序编译为 RISC-V 架构的 ELF 文件,然后模拟器解析该 elf 文件,将对应的指令流搬运到 bootrom,模拟器在配置启动后为处理器注册指令集,绑定解码器,逐条进行译码,执行。指令译码器完成包括操作数在内的指令信息提取,找到该条指令注册时对应的功能函数,执行该功能函数,然后将更新后的寄存器状态信息,内存状态信息同步到前端 UI 显示模块。在模拟器运行的过程中,用户还可以通过前端交互调试窗口来切换模拟器运行模式,设置断点触发条件,进行单步调试,状态查询等操作。

4.3.1解码器与指令集功能函数

RISC-V 指令集是模块化的,它的核心是一个名为 RV32I 的基础 ISA,可选的标准扩展包括 MAFDC,根据应用程序的需要,硬件可以包含或不包含这些扩展。本模拟器实现了特权指令集1.9版本,和用户指令集2.1版本的标准拓展指令集共196条指令的模拟。模拟器预加载时通过解析配置参数选择相应的指令集模块进行注册,并初始化解码器,流程如图1.1所示。

4.3.2指令流程控制

指令的执行,分为取指、译码、执行三个步骤。对于单条指令,在逻辑上这三个步骤是顺序的,同步的。所以对于功能模拟器,仍然可以把实际的流水线设计看作是单周期的 CPU。

4.3.3平台级中断控制器

由前面的章节可以知道,RISC-V 汇编指令的格式是非常明晰的,图1.1展示了  
4.3.4交互调试模块

系统的详细设计主要是对概要设计中各个功能模块的实现细节进行阐述,给出具体的设计方案.本章节将分别对模拟器四个主要功能模块的具体设计和实现细节进行阐述和说明.

5.1指令集模块的实现

指令集模块主要实现了两个功能,指令集功能函数的翻译,以及解码器对指令列表的解析和注册.

对应单条汇编指令的取值,译码,执行过程,模拟器从 PC 地址读取一条32位的汇编指令,通过解码器进行解码,找到对应的功能函数,然后执行该功能函数.核心的数据结构就是指令类 insn\_t,除了包含32位的 uint 数据成员来保存指令内容,还定义了一系列的接口,方便读取 RISC-V 指令格式所定义的指令码,寄存器,立即数等的位域信息.下面详细介绍模拟器对于指令类数据结构的定义和实现.

RISC-V32I 所包含的全部六种指令类型的格式。在实际编码过程中,编码位置的安排都是有意义的。例如3个寄存器索引号在不同指令格式中的编码位置是永远不变的,Rd 在 bit 7-11,rs1在 bit 15-19,rs2在 bit 20-24。即使有些指令中可能没有用到部分寄存器,比如第二个指令类型 I-type 中没有 rs2,但是 rs1和 rd 的索引号也在对应的位置上。又例如在 S-type 里 funct3在 bit 12-14,与在 R-type中的位置一致。Opcode 是所有指令格式都有的,而且位置不变,永远都是 bit 0-6。

所以在指令类 insn\_t 中可以定义统一的接口来获取 RISC-V 指令中的位域信  
息.代码片段如下:

typedef quint64 insn\_bits\_t;

class insn\_t

public:

insn\_t()= default;

insn\_t(insn\_bits\_t bits): b(bits){}

insn\_bits\_t bits(){ return b;}

int length(){ return insn\_length(b);}

int64\_t i\_imm(){ return int64\_t(b)>>20;}

int64\_t s\_imm(){ return x(7,5)+(xs(25,7)<<5);}

int64\_t sb\_imm(){ return (x(8,4)<<1)+(x(25,6)<<5)+(x(7,1)

<<11)+(imm\_sign()<<12);}

int64\_t u\_imm(){ return int64\_t(b)>>12<<12;}

int64\_t uj\_imm(){ return (x(21,10)<<1)+(x(20,1)<<11)+(x(

12,8)<<12)+(imm\_sign()<<20);}

quint64 rd(){ return x(7,5);}

quint64 rs1(){ return x(15,5);} quint64 rs2(){ return x(20,5);} quint64 rs3(){ return x(27,5);}

quint64 rm(){ return x(12,3);}

quint64 csr(){ return x(20,12);}

int64\_t rvc\_imm(){ return x(2,5)+(xs(12,1)<<5);} int64\_t rvc\_zimm(){ return x(2,5)+(x(12,1)<<5);}

int64\_t rvc\_addi4spn\_imm(){ return (x(6,1)<<2)+(x(5,1)<<3)

+(x(11,2)<<4)+(x(7,4)<<6);}

int64\_t rvc\_addi16sp\_imm(){ return (x(6,1)<<4)+(x(2,1)<<5)

+(x(5,1)<<6)+(x(3,2)<<7)+(xs(12,1)<<9);}

int64\_t rvc\_lwsp\_imm(){ return (x(4,3)<<2)+(x(12,1)<<5)+

(x(2,2)<<6);}

int64\_t rvc\_ldsp\_imm(){ return (x(5,2)<<3)+(x(12,1)<<5)+

(x(2,3)<<6);}

int64\_t rvc\_swsp\_imm(){ return (x(9,4)<<2)+(x(7,2)<<6);}

int64\_t rvc\_sdsp\_imm(){ return (x(10,3)<<3)+(x(7,3)<<6);} int64\_t rvc\_lw\_imm(){ return (x(6,1)<<2)+(x(10,3)<<3)+(x   
(5,1)<<6);}

int64\_t rvc\_ld\_imm(){ return (x(10,3)<<3)+(x(5,2)<<6);}

int64\_t rvc\_j\_imm(){ return (x(3,3)<<1)+(x(11,1)<<4)+(x(

2,1)<<5)+(x(7,1)<<6)+(x(6,1)<<7)+(x(9,2)<<8)+(x(8,

1)<<10)+(xs(12,1)<<11);}

int64\_t rvc\_b\_imm(){ return (x(3,2)<<1)+(x(10,2)<<3)+(x(

2,1)<<5)+(x(5,2)<<6)+(xs(12,1)<<8);}

int64\_t rvc\_simm3(){ return x(10,3);}

quint64 rvc\_rd(){ return rd();}

quint64 rvc\_rs1(){ return rd();}

quint64 rvc\_rs2(){ return x(2,5);}

quint64 rvc\_rs1s(){ return 8+ x(7,3);} quint64 rvc\_rs2s(){ return 8+ x(2,3);}

private:

insn\_bits\_t b;

quint64 x(int lo, int len){ return (b >> lo)&((insn\_bits\_t(1)<<

len)-1);}

quint64 xs(int lo, int len){ return int64\_t(b)<<(64-lo-

len)>>(64-len);}

quint64 imm\_sign(){ return xs(63,1);}

};

我们可以在后续功能函数的实现中使用上述的接口,极大的提高模拟效率.区别于其他指令集架构的设计,RISC-V 的译码过程是比对 opcode 和 func 位域信息,通过 riscv-opcodes 工具生成的头文件包含了所有标准指令集模块的指令格式信息,每条汇编指令都包含一对 MASK和 MATCH 信息,真实的译码过程是将指令内容与 MASK 取位与运算,得到的结果和 MATCH 一致表示是该条汇编指令.

在模拟器实现过程中只需要为解码器开辟一块内存空间,存放(MATCH,MASK,insn\_t)的三元组即可,为了加快译码速度,在模拟器设计中,采用了哈希表的数据结构进行存储.具体的实现细节如图所示.

定义了指令数据结构和解码器之后,取指,译码的过程就完成了,接下来介绍执行步骤的核心内容,指令集功能函数的实现.

指令集功能函数是整个指令集模拟的核心部分,理论上说,汇编指令的功能函数需要和实际的硬件设计一一对应,由于硬件设计所参考的指令集架构版本已经定义了各个汇编指令的功能和具体行为,所以对于指令集的功能模拟只需要参照相应的指令集手册.本模拟器的设计过程依托于具体的芯片项目,由于大多数的硬件设计团队针对不同的性能指标往往会进行一些取舍,尤其是对于 RISC-V 这样的开源架构,实际的设计肯定会和官方版本有所出入,所以在模拟器的设计上还是需要参照硬件设计团队的代码.

本次设计依托的芯片开发项目使用 chisel 进行硬件设计,通过其生成的 scala代码,可以指导模拟器指令功能函数的翻译,如图1.1所示为 scala 代码到 c 语言模拟程序的翻译过程.

5.2 CPU和总线的实现

上一节介绍了指令集模块的实现,从一个较高的抽象层次对模拟器的功能进行了定义,本节将详细介绍硬件的模拟细节,主要包含 CPU 内部的各个功能部件,以及 CPU 与片外通信的桥梁-总线的设计与实现.

5.2.1寄存器模拟

寄存器是 CPU 预先定义的可以用来存储数据的位置,汇编指令的执行过程主要就是对寄存器和其他存储器的读写过程,因此对于寄存器的模拟需要做到精确且高效.

RISC-V 体系结构中,定义了两类寄存器,整数和浮点寄存器 XPR/FPR;控制与状态寄存器(control and status register, CSR).由于前者属于通用数据寄存器,在用户模式和机器模式下的访问方式一致,因此只需要将其定义为处理器类内部的共有成员,可以直接由处理器对象获取并修改.CSR 寄存器主要由特权集指令进行位操作,表示 CPU 状态的改变,后续的调试模块也需要重点关注 CSR 的状态,因此在模拟实现上需要提供统一的接口,一方面为了简化指令集功能函数的实现,另一方面也可以节省参数传递等过程带来的性能损失.

以状态寄存器 CSR\_MSTATUS 为例.mstatus 寄存器是一个 XLEN 位的可读/可写

寄存器类图如图1.1所示.总体设计上,三组寄存器均封装在 processor\_t 类内部,其中通用寄存器组可以被处理器类对象直接调用,进行读写操作;CSR 寄存器组被声明为类私有成员,对外提供 get\_csr(),set\_csr()统一接口.将 CSR 寄存器访问权限,状态寄存器位域信息获取等操作封装在接口内部,这样就可以使指令集功能函数的实现不必关心具体的寄存器实现细节.对于 CSR 寄存器接口的实现主要需

要考虑三个因素,检查寄存器组所需的指令集模块支持;处理器当前权限模式检查;以及状态寄存器写入格式的检查.

寄存器,其格式如图3.4所示。 mstatus 寄存器持续跟踪和控制硬件线程的当前操作状态。在写 status 寄存器的过程中,需要检查 VM,MPP,MPRV,PUM,MXR 位是否有变化,如  
果上述的位域发生改变,表示处理器

PRV[1:0]字段保存了硬件线程当前特权模式,其编码如表1.1所示。如果实现仅提供 M-mode,那么这两位被硬连线到11,处理器寻址不经过 MMU。IE 位指示了在当前特权模式,是否使能中断(1=使能,0=禁止),其主要用途是禁止中断,以便在与当前特权级的中断处理函数相关时,能够保证原子性。当一个硬件线程运行在一个给定的特权模式时,更高特权模式的中断总是使能的,而更低特权模式的中断总是禁用的。更高特权等级的代码可以在移交控制给较低特权级之前,使用每个中断单独的使能位,来禁用选定的中断。

为了支持嵌套的自陷,提供了一个 PRV 和 IE 位的栈,这个栈的深度与支持的特权模式数量相等,此处 PRV0是活跃的特权模式 PRV(即 PRV0-PRVN 对应 N 级特权模式),除了如果实现仅支持机器模式,在此种情形下,这个栈的深度是2,并且所有的 PRV 字段都被硬连线为11。当处理一个自陷时,这个栈被向左边 push,并且 PRV 被设置为活跃自陷处理函数的特权模式,且 IE=0。当从一个自陷处理函数返回时(使用 ERET 指令),栈被向右 pop,并且最左边的项(PRVN)被设置为所支持的最低特权等级,且使能中断(即,在一个只有 M 模式的机器上, PRV1=M 且 IE1=1,而在一个有两个或者更多模式的机器上,当从自陷处理函数返回时, PRVN=U 且 IEN=1)。在通常许不改变特权模式代码,特别是一个管理员级操作系统,来支持任意用户模式状态扩展。

操作中,这个栈应该包含从左到右单调增加的特权模式(最老的到最新的)。

MPRV 位修改了 load 和 store 执行的特权级。当 MPRV=0时,翻译和保护如同寻常一样。当 MPRV=1时,数据存储器地址就如同 PRV 被设置为当前 PRV1字段的值一样被翻译和保护。指令地址翻译和保护不受影响。当出现一个异常时, MPRV 被复位为0。

支持丰富的扩展,是 RISC-V 的一个主要目标,因此我们定义了一个标准接口,允

FS[1:0]和 XS[1:0]可读/可写字段被用于减少保存和恢复上下文的开销,这是通过设置和跟踪浮点单元和任何其他用户模式扩展的状态来实现的。 FS 字段编码了浮点单元的状况,包括 CSR fcsr 和浮点数据寄存器 f0-f31,而 XS 字段编码了任何额外用户模式扩展及相关联的状态的状况。 SD 位是一个只读位,指明了是否 FS 字段或者 XS 字段编码了一个脏的状态,需要将扩展的用户上下文写入到存储器中。在没有浮点单元的系统中, FS 字段被硬连线到零,而在没有需要新状态的额外用户扩展的系统中, XS 字段被硬连线到零。如果 FS 字段和 XS 字段都被硬连线到零,那么 SD 也总是零。

FS 字段和 XS 字段使用了相同的的状况编码,如表3.4所示,其四个可能的的状况值  
是 Off、 Initial、 Clean 和 Dirty

被特权代码读取。在执行指令时,状况字段也会被更新,而不管特权模式如何。

当的状况被设置为 Off 时,任何指令试图读写相应的状态都会导致一个异常。当的状况是 Initial 时,对应的状态应当具有一个初始的常数值。当的状况是 Clean 时,对应的状态可能与 Initial 时的状态不同,但与上下文切换时保存的最后的值相匹配。当的状况是 Dirty 时,对应的状态可能自上次上下文保存时以来,已经被修改。当进行一个上下文保存时,负责的特权代码仅在对应的状态的状况是 Dirty 时,才需要将上下文写入存储器,然后就可以复位其状况为 Clean。当进行一个上下文恢复时,仅在状况是 Clean 时(在恢复时,应该永远不会是 Dirty),才需要从存储器中读取上下文。如果状况是 Initial,在恢复上下文时,上下文必须被设置为一个初始值,以避免一个安全漏洞,但这不需要访问存储器即可完成。例如,浮点寄存器可以全部初始化为立即数值0。当继续一个用户上下文时, FS 字段和 XS 字段可被特权代码设置,并在保存上下文之前,

如图是汇编指令 mret 的定义以及功能函数实现

require\_privilege(PRV\_M);

set\_pc(p->get\_state().mepc);

reg\_t s = STATE.mstatus;

reg\_t prev\_prv = get\_field(s, MSTATUS\_MPP);

s = set\_field(s, MSTATUS\_UIE << prev\_prv, get\_field(s, MSTATUS\_MPIE));

s = set\_field(s, MSTATUS\_MPIE,1);

s = set\_field(s, MSTATUS\_MPP, PRV\_U);

p->set\_privilege(prev\_prv); p->set\_csr(CSR\_MSTATUS, s);

在set\_csr()接口的实现中,需要对于CSR的读写进行检查,一方面是为了确保读写时所处的特权级模式是否支持读写,另一方面需要针对状态寄存器的改变做出相应的动作,比如 tlb 的清除等.

case CSR\_MSTATUS:

if ((val ^ CSR.mstatus)&(MSTATUS\_VM | MSTATUS\_MPP | MSTATUS\_MPRV

| MSTATUS\_PUM | MSTATUS\_MXR))

mmu->flush\_tlb();

在 RISC-V 体系结构中,与 MMU 有关的 CSR 寄存器主要有控制与状态寄存器

reg\_t mask = MSTATUS\_SIE | MSTATUS\_SPIE | MSTATUS\_MIE | MSTATUS\_MPI

| MSTATUS\_SPP | MSTATUS\_FS | MSTATUS\_MPRV | MSTATUS\_PUM

| MSTATUS\_MPP | MSTATUS\_MXR ;

if (validate\_vm(max\_xlen, get\_field(val, MSTATUS\_VM)))

mask |= MSTATUS\_VM;

CSR.mstatus =(CSR.mstatus &~mask)|(val & mask);

bool dirty =(CSR.mstatus & MSTATUS\_FS)== MSTATUS\_FS;

dirty |=(CSR.mstatus & MSTATUS\_XS)== MSTATUS\_XS;

if (max\_xlen ==32)

CSR.mstatus = set\_field(CSR.mstatus, MSTATUS32\_SD, dirty);

else

CSR.mstatus = set\_field(CSR.mstatus, MSTATUS64\_SD, dirty);

xlen = max\_xlen;

break;

}

除了上述的寄存器,每个处理器对象都维护私有的 PC 程序计数器,初始化过程中 PC 被初始化为 bootrom 地址.

5.2.2 MMU 和缓存模拟

内存管理单元(Memory Management Unit, MMU)是一种负责处理 CPU 内存访问请求的计算机硬件。它的功能包括虚拟地址到物理地址的转换(即虚拟内存管理)、内存保护、中央处理器高速缓存的控制等。 mstatus 和管理员页表基址寄存器 sptbr.

在 mstatus 状态寄存器中,虚拟化管理字段 VM[4:0]指示了当前活跃的虚拟化方案,包括虚拟存储器翻译和保护。表3.3给出了当前定义好的虚拟化方案。对于一个 RISC-V 硬件实现,只有 Mbare 模式是强制要求的,该模式没有存储器管理或翻译,因此所有的有效地址,无论其特权模式,都被认为是机器物理地址,是复位时进入的模式,理论上在该模式下不需要经过 MMU 进行地址翻译。Sv39和 Sv48是针对 RV64系统的基于页面的虚拟存储器体系结构,提供了一个39位或者48位的虚拟地址空间,被设计成支持现代管理员级操作性,包括基于 Unix 的系统。Sv39、 Sv48需要实现支持 M、 S 和 U 特权级。本模拟器支持上述三种虚拟化方案,但是为了实现方便,所有的主存访问请求都需要经过 MMU,通过 MMU 模块的统一接口进行访存,当 mstatus 寄存器 VM 位为0时,无需进行地址翻译.以 linux 内核加载过程中从物理地址向虚拟地址过渡的逻辑可以看出,当内核支持MMU时,会进入到relocate代码段进行页表基地址寄存器的初始化,以后首级页表会常驻内存,内核通过 setup\_vm()函数进行了首级页表的加载,然后在relocate 段计算了首级页表基地址,写入 sptbr 寄存器,然后通过一条 mret 指令跳转到U-mode 执行,接下来就全是加载虚拟地址了,MMU 开始工作.

#ifdef CONFIG\_MMU

relocate:

li a1, PAGE\_OFFSET

la a2,\_start

sub a1, a1, a2

add ra, ra, a1

la a2,1f

add a2, a2, a1

csrw CSR\_TVEC, a2

srl a2, a0, PAGE\_SHIFT

li a1, SATP\_MODE

or a2, a2, a1

la a0, trampoline\_pg\_dir

srl a0, a0, PAGE\_SHIFT

or a0, a0, a1

sfence.vma

csrw sptbr, a0

/\* Set trap vector to spin forever to help debug \*/

la a0,.Lsecondary\_park

csrw CSR\_TVEC, a0

/\* Reload the global pointer \*/

.option push

.option norelax

la gp,\_\_global\_pointer$

.option pop

csrw sptbr, a2

sfence.vma

ret

#endif /\* CONFIG\_MMU \*/

在本模拟器的实现中,MMU 模块包含了快表 TLB,加速地址翻译,本质上就是开辟了一片内存用来存放翻译过的地址映射,为了方便起见,只实现了直接映射的 TLB.另外,将iCache,dCache 的功能也一并放到 MMU 模块中,不再实现单独的缓存硬件模块,缓存采用只写的方式.这样的设计和真实硬件的差异很大,会导致缓存模拟的不准确.考虑到本模拟器并不进行缓存相关的性能模拟,所以可以忽略这部分的差别,在功能模拟上没有影响.模拟器的存储结构模型如图1.1所示.

MMU模块对取值做特殊处理,取值首先会查找iCache,当 iCache未命中时,退化为其余类型的访存.访存请求通过模板函数提供的统一的接口 load/store 进行请求,通过模板可以忽略具体的数据类型,在功能函数的实现中也可以更加方便的使用,直接调用 MMU   
的接口对存储单元进行操作.模板函数定义如下:

template<class T>

inline T load(reg\_t addr)

{

if (addr &(sizeof(T)-1))

throw trap\_t(trap\_load\_address\_misaligned,addr);

reg\_t vpn = addr >> PGSHIFT;

if (likely(tlb\_load\_tag[vpn % TLB\_ENTRIES]== vpn))

return \*(T\*)(tlb\_data[vpn % TLB\_ENTRIES]+ addr);

T res;

load\_slow\_path(addr, sizeof(T),(uint8\_t\*)&res);

return res;

}

其中,load\_slow\_path()意味着 TLB miss,需要查找页表,通过页表进行地址翻译的  
综上,整个 MMU 和缓存模块的实现流程如图所示.

总线在模拟器初始化的过程中会根据配置挂载设备,在总线类 bus\_t 中

5.2.3总线和 I/O 模拟

总线是 CPU 与外部设备进行数据交换的桥梁,按照功能划分可以分为地址总线,数据总线和控制总线.本模拟器对总线设备进行了抽象,将总线设计为某一块物理地址区间内的 IO 控制器,提供统一接口,处理 CPU 和内存映射的 IO 设备之间的通信.

维护一个物理地址和设备类对象的 map,模拟器在接收到访存请求时,首先检查物理地址是否是主存地址范围,不在主存地址区间内的 I/O 请求都是内存映射的 I/O 请求(Memory-Mapped I/O, MMIO),模拟器将调用总线设备的IO 接口,对内存映射的外设进行读写操作.

模拟器根据物理地址划分为主存,和内存映射的 IO 设备,图1.1是SiFive 公司提供的内存映射参考.

本模拟器的总线设备需要处理的内存映射空间就是

0x00000000~0x80000000,提供这块内存区间上的 IO 模拟.总线设备可以挂载各种通过内存映射的 IO 设备,某些具有特殊用途的寄存器也能够挂载在总线,比如 timecmp 寄存器,ipi 寄存器.

总线设备的定义如下:

class bus\_t : public abstract\_device\_t

public:

bool load(reg\_t addr, size\_t len, uint8\_t\* bytes);

bool store(reg\_t addr, size\_t len, const uint8\_t\* bytes);

void add\_device(reg\_t addr, abstract\_device\_t\* dev);

void add\_register(reg\_t addr, abstract\_device\_t\* dev,qint32 offset)

;

private:

std::map<reg\_t, abstract\_device\_t\*> devices;

struct device\_reg

{

device\_reg(){}

device\_reg(abstract\_device\_t \*dev,qint32 offset):dev(dev),offse   
t(offset){}

abstract\_device\_t \*dev;

qint32 offset;

};

QMap<reg\_t,device\_reg> regs;

};

bus\_t 类型的 load/store 属于 mmio 接口,首先会检查挂载在总线上的设备或寄存器地址是否匹配,然后才会对具体的设备进行读写操作.下面介绍几种以 MMIO 方式挂载在总线上的设备模拟.

所有支持 Secure Boot 的 CPU 都会有一个 bootrom 固件.CPU 在通电之后执行的第一条指令就在 bootROM 的入口。bootROM 拥有最高的执行权限,也就是机器模式 M-mode。它将初始化 Secure Boot 安全机制,加载 Secure Boot Key 等密钥、从存储器加载并验证 First Stage Bootloader(FSBL),最后跳转进 FSBL 中。本次芯片设计项目也包含了该部分的设计,但是由于涉密,在模拟器设计中并不涉及FSBL的加载和验证过程,bootrom固件程序仅仅用来跳转置目标程序入口.具体的实现方式包括以下的步骤,首先在配置中读取 bootrom 的地址,默认0x1000,然后初始化 bootrom 设备,填写 bootrom 固件内容,本模拟器的  
bootrom 程序内容如图所示,包含两条汇编指令:

auipc t0,0x7ffff

jr t0

在 CPU 运行过程中,存在两种指令流程,一种是常规的逻辑控制流,包括顺序

模拟器启动后,PC 初始化0x1000,以机器模式执行上述两条指令,跳转到主存起始位置,即目标程序的入口地址.接下来的一系列指令执行由目标程序决定,主要包括 bootloader 的 reset vector 以及加载 linux 内核的过程.

总线对象使用 add\_device 接口将物理地址0x1000和 bootrom 设备对象的映射保存在字典中.

mmio 的通信流程如图1.1所示.

5.3中断系统的实现

的指令流和分支跳转;另一种称为异常控制流,用来响应处理器状态的某些变化,表现为中断或异常.之前的章节已将介绍了 CPU 指令控制流程的模拟,其中包括了响应中断的逻辑,CPU 在取值之前检查当前是否有中断信号,根据状态寄存器判断是否响应中断,进入异常控制流逻辑.本节将详细阐述模拟器中断系统的实现.包括两种中断控制器以及部分中断源的模拟.

RISC-V 一共有两大类的中断类型:局部中断(Local Interrupts)以及全局中断(Global Inerrupts)。局部中断是指直接与 hart 相连的中断,可以直接通过 CSRs 当中的 xcause(mcause、scause、ucause)中的值得知中断的类型。在

局部中断当中,只有两种标准的中断类型:计时中断(timer)以及软件中断

(software)。全局中断实际上就是外部中断(External Interrupts)。它与 PLIC相连(Platform-Level Interrupt Controller,平台级中断控制器)。实际上全局中断在多个硬件线程的情况下最为常用。PLIC 用于对外部中断进行仲裁,然后再将仲裁的结果送入核内的中断控制器。

RISC-V 架构中规定了一些硬件行为来实现异常事件的响应和处理,这些行为通过控制状态寄存器来反应异常事件信息.涉及到如下几个寄存器.

寄存器功能

mstatus 状态寄存器,保存全局中断使能以及许多其他的状态。只

讨论机器模式的情况下,有效的域只有 MIE 和 MPIE。MIE 表示中断全局使能,只有该位有效时,才能产生中断。MPIE 位保存进入中断处理之前以及恢复现场之前 MIE 的状态。

mie 外部中断使能寄存器,外部中断响应的使能位有效时才能

进入处理

mtvec 异常入口基地址寄存器,可配置为查询或向量访问模式。高位 BASE 域表示异常向量的基地址。

mscratch 上下文切换时用于保存当前的指针信息

mepc 异常 PC 寄存器,进入中断处理时,硬件会自动将当前遇

到的中断的 PC 保存 mepc 中

mcause 异常原因寄存器,mcause[31]为中断域,其余位为异常编号域。如果是有中断事件待处理,会将 interrupt 位置1。Exception Code 字段保存待处理事件的标识代码。中间位读时返回0,作为保留位可以在之后用于支持异常编码的字段扩展 mip 外部中断事件标志信号,当有外部中断事件发生时,mip   
中对应中断标志位置高

mbadaddr

本模拟器实现了这部分的硬件行为,包括中断源的产生,和中断响应,下面进行详细的介绍.

在处理器类内定义了两个 uint64型数据,分别用来表示时钟中断和外部中断的 pending,总线上挂载的设备可以直接对这两个 pending 数据进行设置,用来模拟外设"异步"的中断请求发起.处理器在下一个取值周期之前,使用 try-catch 语句来处理可能的中断响应,如果处理器决定响应中断,就会抛出一个 trap\_t 类型的异常,

进入到响应中断的异步逻辑.trap\_t 的定义如下:

class trap\_t

trap\_t(){}

trap\_t(reg\_t type):cause(type),addr\_valid(false){}

trap\_t(reg\_t type,quint64 addr):cause(type),addr\_valid(true),addr(a   
ddr){}

reg\_t cause;

bool addr\_valid;

quint64 addr;

static QMap<reg\_t,QString> names;

static quint64 delegable\_exceptions;

QString &name(){return names[cause];}

};

处理器响应的流程如图1.1所示

模拟器抛出异常后,根据捕获到的 trap\_t,进入中断处理流程.RISC-V 特权架构对这部分的处理器行为做了一定规范,本模拟器的实现也参照了特权架构定义.

1)根据处理的中断类型将信号源编号记录到 mcause 寄存器中;

2)地址不对齐或者发生访问异常,将导致错误的指令部分保存到 mbadaddr;

3)更新状态寄存器 mstatus,记录中断处理前的状态;

4)保存当前 PC 到 mepc 寄存器中,以便于处理完中断后返回;

5)停止当前执行程序流,设置 PC 为 mtvec 中断向量表入口地址并开始执行.以上就是中断产生和响应过程对应的处理器硬件行为模拟,接下来将着重阐述平台级中断控制器 PLIC 的实现.

图1.1是 SiFive 公司给出的 PLIC 规范框架图.

5.3.1 PLIC 模拟

PLIC 的功能是接受外部中断源发出的中断信号,对中断请求进行裁决,将裁决结果和外部中断信号发送给处理器.本模拟器参照了 SiFive 公司的 PLIC 规范文档进行设计,通过设备树的挂载对内存映射的存储器进行读写,配置 PLIC.

中断源(interrupt sources)是挂载在PLIC上的设备的统称,一般是I/O设备.PLIC理论上支持任意多个中断源,每个中断源可以是不同触发类型,电平触  
发或者边沿触发、PLIC为每个中断源分配了如下的信息:

1)闸口(Gateway)和IP(interrupt pending).闸口控制中断源发送中断请

求.IP标识当前中断源是否有请求.IP拉高时,闸口不再接受该中断源的请求.

2)设备编号ID.PLIC为每个中断源分配了一个独一无二的编号ID.该ID也作为在多个sources具有相同优先级是的选择条件,数值较小优先级更高。

3)优先级(Priority).每个中断源都有一个内存映射的Priority寄存器,表示该中断源的优先级,软件可以通过配置(设备树)将其设置成不同的优先级.优先级的数字越大,表示优先级越高.

中断使能(Enable).每个中断源均分配了一个内存映射的中断使能寄存器,和优先级一样也可以通过设备树进行配置.IE寄存器配置为0表示该中断源被中断目标屏蔽,反之则是使能.

中断目标(interrupt targets)对应为RISC-V处理器核心的各个特权级模式。

PLIC产生的外部中断请求会分别标示在处理器的mip寄存器的meip/seip位,对应于机器模式和监管模式。每个中断目标都有对应的内存映射的优先级门限(priority threshold)寄存器,只有中断源优先级高于该门限,PLIC才会将中断源ID发送给对应中断目标。

PLIC Core负责所有中断请求的仲裁和分发.图1.1展示了PLIC处理外部中断的流程.

中断源首先通过闸口给PLIC core发送中断请求,PLIC core将对应中断源的pending寄存器置位,并将该中断源闸口关闭.PLIC core进行中断信号裁决,获得最高优先级的中断源,通过对mip寄存器meip/seip置位将外部中断信号发送给处理器.当处理器接受了外部信号,会发送一个claim信号给PLIC core,表现为读取裁决结果的最高优先级中断源,同时将对应的该中断源pending拉低.当处理器完成了中断处理,发送一个中断完成信息给PLIC core.表示中断完成,打开对应中断源闸口.

根据以上的流程,模拟器实现的PLIC设备类图如图1.1所示.

将中断源和中断目标分别抽象成plic\_dev\_info\_t类和plic\_core\_info\_t类,中断完成信息,具体的动作就是对PLIC中断源指定位置claim寄存器发送一条

在外设模拟中,通过connect\_plic接口初始化设备类中的plic\_dev\_info\_t对象,并将自身挂载到 PLIC 设备上,后续设备的 IO 请求可以通过plic\_dev\_info\_t::raise()接口发送到PLIC设备,模拟了闸口的功能.PLIC设备类型plic\_t中定义了accept\_interrupt接口用来拉高对应设备的pengding寄存器,plic\_t::raise()接口实现了中断信号裁决,将裁决后的中断ID写入mclaim和sclaim寄存器,并且向处理器发送外部中断信号,当处理器响应中断时,会读取这两个寄存器的值,然后进入中断向量表,查找对应的中断处理函数,通常会调用定义在内核drives目录下的驱动程序.中断处理结束后,处理器会给PLIC core发送

store指令,根据SiFive公司给出的规范,中断源ID为n的的claim/complete寄存器内存映射位置等于(plic基地址+0x200004+0x1000\*n),因此该位置进行store请求时直接调用处理器对应plic\_core\_info\_t对象的gate\_open()接口来打开闸口.此时plic完成一次外部中断请求周期,可以挂起下一次的中断请求.

interrupt notification,由PLIC Core 发给各target的中断请求,PLIC Core为每个target赋予了一个(external interrupt pending bit) EIP,表示有待处理的中断。EIP的值可以被source,target或者其他源进行修改。EIP发送给target的过程被称为interrupt notification。PLIC Core只支持multicasting,即中断信号会发给所有符合条件的target,并不会选择其中之一发送。这样虽然响应较快,但会带来一些冗余处理。软件可以通过控制IE 位间接改善。首先claim的target会负责该中断的处理,PLIC Core只保证对于EIP的修改所有对应的targets都可见。

interrupt claim,由target返回给PLIC Core的响应信号,表示请求接受。PLIC Core收到claim后,会选出最高优先级的source ID,并将其对应的IP清除。这个ID会发送给target。如果ID为0,表示没有需要处理的中断。claim被PLIC Core接受后,次优先级的中断会显现出来,因此对应的EIP可能并不会被清0。因此target可以在退出中断服务程序前检查本地Xeip 位(X表示当前特权模式),确认是否有pending 的EIP。PLIC支持target在EIP=0的情况下仍然发起claim。这是为了支持某些target的threshold设置为最高,不接受中断打断,但使用claim方式进行查询。

interrupt completion,由target 返回给PLIC Core的完成响应信号。

global interrupt handling,基本过程是,global sources 首先发送给interrupt gateway,由 gateway 负责产生 interrupt request,发送给 PLIC Core, PLIC Core 将每个 interrupt request 储存在内部的(interrupt pending bits) IP 中,如果该 targets 有 enabled pending interrupt,并且 priority超过了 per-target threshold ,PLIC Core 将 interrupt notification 发送给一个或者多个 targets。当 target 接受了该外部中断,会发送一个 interrupt claim request 给 PLIC Core,用以取得对应该 target 的最高优先级的 pending interrupt,同时将对应的 IP 位清零,当 target 完成了中断服务,需发送一个interrupt completion message 给对应的 interrupt gateway 表示中断完成。接下来 gateway 可以发送另一个 interrupt request 给该 target。

5.3.2 RTC 模拟

CLINT(Core-Local Interruptor, PLIC)局部中断控制器是一个存储器地址映射模块,CLINT 只负责处理软件中断和时钟中断,因为这两个中断是 RISC-V 架构中定义的,经过 CLINT 不需要进行任何的仲裁,直接将中断信号写入对应的寄存器内即可。软件中断只需要向 CLINT 的 MSIP0或者 SSIP0寄存器的最高位写1即可,处理完中断后,将其置为0,这样就能够清除掉软件中断的标志位。计时器中断作为 riscv 内核特有的中断,其用法就是往 MTIMECMP 或者 STIMECMP 中写特定的值,当 mtime 达到该值时产生中断,此时继续填写特定的 tick 就可以继续产生下个中断,反复如此,便可产生周期性的 tick 中断。

5.3.3外部中断源模拟

5.4调试模块和 UI的实现

调试模块能够提供断点设置,单步执行,寄存器/内存查询等功能.UI 显示界面主要包含了断点设置窗口,查询窗口和执行交互窗口.本模块使用 Qt 的 UI Designer 工具进行开发,通过拖拽摆放各种窗口控件并进行属性设置,观察界面整体效果,可以方便地进行可视化界面的设计.另外 QtWidget 库还提供了信号(Signals)和槽(Slots)机制,用于对象间通信,只需要在对应窗口子类化 widgets 来添加自定义信号,然后实现自定义的槽函数,连接到该信号即可.

模拟器前端整体界面如图1.1所示

前端 UI 窗口和后端模拟器之间的信号定义如下:

enum sim\_cmd

{

sim\_cmd\_pause\_sim,

sim\_cmd\_run\_sim,

sim\_cmd\_run\_sim\_silently,

sim\_cmd\_step\_sim,

sim\_cmd\_reset\_sim,

sim\_cmd\_access\_memory,

sim\_cmd\_set\_breaks,

sim\_cmd\_key\_input,

sim\_cmd\_mailbox\_input

};

enum window\_cmd

{

window\_cmd\_update\_reg, window\_cmd\_update\_mem, window\_cmd\_sim\_output, window\_cmd\_gst\_output,

window\_cmd\_pause\_sim,

window\_cmd\_update\_mailbox

};

其中 sim\_cmd\_key\_input 和 sim\_cmd\_mailbox\_input 信号分别用来模拟 UART和 mailbox 外部中断源信号.其余信号用于断点和查询信息的交互,以及模拟器单步运行等流程的控制.

断点设置窗口如图所示,可以添加任意多个断点,断点匹配类型分为如下几种:PC,寄存器,内存,中断类型.当模拟器包含多核时需要指定相应的核心 id 号.当模拟器处于调试模式时,中断指令流程,此时可以进行断点设置,内存查询等操作,点击运行按键,模拟器恢复至正常运行模式,在每一次指令执行周期完成后模拟器将对当前断点信息进行检查,一旦匹配上任意断点,将发送window\_cmd\_sim\_output 信号用于告知触发断点信息,并接着发送window\_cmd\_pause\_sim 信号,中断指令流程,模拟器进入调试模式.每发送一次单步执行信号,模拟器都需要将寄存器更新信号发送给 UI 前端,刷新寄存器窗口.模拟器单步执行的流程如图所示.

5.6本章小结

本章主要在概要设计的基础上对 RISC-V 指令集模拟器四个功能模块的详细设计和实现细节进行了阐述,并根据实际工程项目中使用的设备和具体型号 IP文档,进行了部分外设的功能模拟,验证了模拟器的可用性,最后完成了前后端所有功能模块的代码实现,并给出了相应的演示效果图.

6.1测试概要

系统测试是系统开发过程中必不可少的重要阶段,是确保系统开发质量的关键,它贯穿于系统开发的整个过程,尽可能地发掘系统中存在的问题和错误,可以及时地进行纠错,促进系统开发工作高效有质量地进行.

6.1.1测试环境

RISC-V 模拟器的测试环境分为软件模拟环境和硬件对照环境,软件模拟环境是系统设计使用到的第三方库和模拟器的宿主机环境,硬件对照环境主要是芯片开发过程中的 FPGA 开发板 S2C Single U440平台以及流片后的真实芯片环境.具体的模拟器环境如表1.1所示.

名称说明

Ubuntu20.04模拟器的宿主机环境

Qt5 Qt5的 UI 类库

BBL(berkele-bootloader) RISC-V 官方的 bootloader

linux-v5.10目标程序 linux 内核版本

busybox-1.32.1 linux 命令集合

6.1.2概述

本模拟器的测试采用测试驱动开发方式进行,主要过程如下:

(1)根据需求分析中确定的芯片开发团队成员需求和系统概要设计中划分的四个功能模块,采用黑盒法设计对应的测试用例,当各个功能模块代码实现后立刻开始测试.

(2)根据需求分析中的需求规格说明,使用场景法对模拟器进行配置项测试,测试模拟器的业务功能是否满足需求.

(3)最后进行系统测试,重点测试 linux 内核移植过程中的 MMU 启动,挂载PLIC 外设,以及调试功能是否满足后续的系统软件移植开发需求.

6.2测试分析

测试分析主要对模拟器的测试需求进行分析,包含可以直接获取的显式功能性需求和系统中隐含的隐性需求比如模拟器运行速度.在系统开发的不同阶段,测试的需求也有所不同,本节所分析的测试需求有:模块测试需求,配置项测试需求和系统测试需求.下面对主要的测试需求展开分析.

6.2.1模块测试需求获取

根据系统概要设计,本模拟器分为四个功能模块,下面对各个功能模块的测试

需求进行分析:

(1)指令集模块:该模块解析模拟器启动参数,获取指令集配置,对相应的指令集模块进行注册,为后续的指令译码,以及功能函数调用提供所需的数据,依据概要设计的要求,主要测试该模块能否将所需指令集全部注册进解码器,并且在后续译码执行过程中调用正确的功能函数.

(2) CPU 和总线模块:该模块用于模拟处理器执行过程中的硬件行为,依据概要设计的要求,主要测试该模块的寄存器读写过程;访存请求涉及到的MMU行为,包括快表查询,iCache查询,通过页表的地址翻译过程;经过总线的mmio请求过程.主要测试其正确性.

(3)中断模块:该模块用于模拟中断控制器的软硬件行为,依据概要设计的要求,主要测试通过 PLIC 挂载设备的中断请求过程能够被处理器响应,中断控制器能够做到规范文档的功能要求.

6.2.2配置项测试需求获取

根据 RISC-V 指令集模拟器的需求规格说明书,对于系统软件开发测试人员的需求进行配置项测试,主要是对模拟器加载目标程序的流程测试,以及后续目标程序的流程控制测试,包括设置断点,单步调试,寄存器/内存查询,外部中断信号发送.系统软件开发测试人员通过对目标程序的流程控制,可以方便地进行软件移植工作,加快系统软件的开发迭代.

6.2.3系统测试需求获取

根据需求规格说明书,本模拟器需要进行系统软件的移植测试.包括了bootload 和 linux 内核,在此移植过程中,对模拟器的整体功能部件进行测试,

主要有 linux 加载过程中的 MMU 启动,PLIC 挂载外设,并将中断源通过设备注册到操作系统.

6.3测试用例设计

针对系统开发的各个阶段,测试用例的设计和采用的设计方法都有所不同,下面对各个阶段的测试用例进行设计.

6.3.1模块测试用例设计

依据模块测试的需求,对RISC-V指令集模拟器的四个功能模块进行测试,各  
个模块的测试用例设计如下:

(1)指令集模块:根据测试需求,该模块的功能是根据模拟器启动参数加载对应的指令集模块,对指令列表进行注册,将指令格式和对应的功能函数绑定起来,完成解码器的初始化工作,该模块检测到未定义指令模块,会发出告警信息,提示未定义行为.具体的测试用例设计如表1.1所示.

序号输入预期输出说明

1指令集标准拓展

rv64imafdc

模拟器注册指令列表的

全部内容,解码器保存

指令格式和功能函数的

验证功能模块的

有效性

序号输入预期输出说明

(3)中断控制器模块:根据测试需求,该模块的功能是将内存映射的 I/O 设备  
序号输入预期输出说明

(2) CPU 和总线模块:根据测试需求,该模块的功能是模拟指令执行过程中的硬件行为,包括寄存器,MMU,缓存,内存,IO 控制器等,测试目的是验证该模块的硬件行为模拟和真实硬件行为一致.该模块的输入总是已注册的指令,不会有其他未定义输入,主要检测是否达到预期输出,具体的测试用例设计如表1.1所示.

挂载到中断控制器,和处理器进行通信.测试目的为了验证中断控制器能够对外部中断信号源进行有效裁决,并配合处理器完成外部中断的流程,以及测试当外部中断源优先级低于处理器门限寄存器时能否屏蔽该中断源.具体的测试用例设计如表1.1所示.

映射

2未定义指令集拓展

rv64jkl

提示未定义的指令集拓

展

验证功能模块的

健壮性

3未定义功能函数的自定

义指令

解码器提示功能函数未

定义

验证功能模块的

健壮性

4汇编指令 ld t01000通用数据寄存器 t0内容

0x1000

验证功能模块的

有效性

5汇编指令 csrw mtevc, t0 CSR 寄存器 mtevc 被写  
入 t0寄存器的值

验证功能模块的

有效性

6机器模式下的内存查询

请求

MMU 显示 Mbare 模式,

不进行地址翻译

验证功能模块的

有效性

7监管模式下的 sv39内存

查询请求

MMU 查询页表,输出地

址翻译过程

验证功能模块的

有效性

8和序号7同一地址的监

管模式下的 sv39内存查

询请求

MMU 查询快表,TLB 命

中,输出查询内容

验证功能模块的

有效性

9对 UART 的 mmio 请求前端窗口输出请求回复

内容

验证功能模块的

有效性

10 UART 以优先级2挂载

到 PLIC,处理器机器模

式和监管模式的门限优

先级设置为3

处理器不再响应 UART

中断源的外部中断请求

验证功能模块的

健壮性

(4)调试模块和 UI:根据测试需求,该模块的功能是对目标程序运行流程进行控制,切换至调试模式进行断点设置,寄存器/内存查询,单步调试等功能,测试目的是验证该模块通过 UI 将调试信号发送给后端模拟器,并进行断点匹配的过程,还有验证寄存器/内存查询的正确性,以及查询无效内存地址给出告警信息的过程.具体测试用例设计如表1.1所示.

6.3.2配置项测试用例设计

依据配置项测试需求,采用基于实际业务的场景设计法对 RISC-V 指令集模拟器的 RISC-V 架构目标程序调试功能进行测试用例设计.该功能设计的基本流有:1.设置断点信息,点击应用后,调试窗口发送断点信号到模拟器后端,添加新的断点信息到处理器断点检测列表;2.删除处理器断点检测列表中的某一项;3.点击单步执行,模拟器进行一次取值,译码,执行周期,更新寄存器状态窗口,输出当前指

令到指令历史窗口;4.输入待查询内存地址,点击查询,模拟器进入 MMU 访存逻辑,

查询当前地址内容;5.点击运行,模拟器进入运行模式,将交互信息输出到交互窗口;该功能的备选流有:1.设置断点信息错误,导致处理器断点检测列表添加失败;

2.输入无效地址导致内存查询失败,发出告警信息.基本流和备选流可以组合成各个场景,进而对每个场景设计测试用例,具体的测试用例设计如表1.1所示.

序号输入预期输出说明

11调试模式下单步执行信

号

模拟器执行完一条指令

后发出更新信号,前端

UI 刷新寄存器状态

验证功能模块的

有效性

12断点信息 pc core0

0x80000000

核0在 PC=0x80000000

处匹配断点,进入调试模

式,输出断点信息

验证功能模块的

有效性

13内存地址0x80000000查

询信号

0xif80006f

对应汇编指令 j pc+504

表示跳转到 reset\_vector

验证功能模块的

有效性

14内存地址0xffffffff 查询

信号

发出警告信息,无效内存

地址

验证功能模块的

健壮性

6.3.3系统测试用例设计

依据系统测试需求,主要对 RISC-V 指令集模拟器进行稳定性测试,容

错性测试和性能测试,下面分别对各个测试进行测试用例设计:

(1)稳定性测试:依据系统测试需求,模拟器需要在加载给定的目标程序后不间断地稳定运行.因此稳定性测试设计为模拟器加载 linux 内核运行top 程序三天,预期结果是模拟器可以一直持续运行,并且实时检测模拟CPU 的进程状态.

(2)容错性测试:依据系统测试需求,从一下两个方面进行测试用例设计:加载含有未定义指令的程序,检测程序能否陷入对应的异常(illegal instruction);设置错误的断点信息,检测模拟器在端点检测逻辑是否会发生因设计错误导致的程序崩溃.

(3)性能测试:依据系统测试需求,记录模拟器在断点检测列表为空的状态下,和含有断点检测列表的状态下的 MIPS(Million instruction per-second),和实际的硬件 MIPS 做对比,测试模拟器模拟速度.另外从模拟器进行系统软件调试的功能考虑,记录了在模拟器和真在实硬件平台上的调试周期,进行对照测试,分析模拟器在软件移植/开发/测试流程中的性能.

6.4测试结果及分析

使用各个测试阶段所设计的测试用例,对 RISC-V 指令集模拟器展开了单元  
测试,配置项测试和系统测试,具体测试结果如下:

(1)在单元测试中对模拟器的四个功能模块都进行了测试,经过五次回归实

序号操作预期输出说明

15设置断点信息,点击应

用

处理器断点检测列表添加

成功

基本流1,备选流1

16删除某一断断点信息删除成功基本流2

17点击单步执行寄存器状态更新,指令历

史窗口更新

基本流3

18输入内存地址,点击查

询

对应内存地址的内容基本流4,备选流2

19调试模式下点击运行更新目标程序的交互信息基本流5

验后,各个功能模块实际输出与预期输出达成一致,各个模块的功能和健壮性都得到了验证,达到了需求规格说明书中的需求。

(2)在配置项测试中对模拟器的目标程序调试功能进行测试,各个测试用例的实际输出与预期输出一致,所测业务功能满足设计需求。

(3)在系统测试中对模拟器进行稳定性测试、容错性测试和性能测试.稳定性测试时系统正常运行情况如图1.1所示;容错性测试达到了预测的结果.从测试结果可以看出吸烟检测系统的可靠性满足需求规格说明书中的需求;通过和真实硬件平台的对照,在系统软件移植开发流程中,模拟器的软件迭代周期要明显比硬件平台效率更高,性能要求也达到了预期的结果.

7.1总结

7.2未来工作

参 考 文 献

[1] Szekeres L , Payer M , Tao W , et al. SoK: Eternal War in Memory[C]// IEEE Symposium on Security & Privacy. IEEE Computer Society, 2013.

[2] 邵思豪, 高庆, 马森,等. 缓冲区溢出漏洞分析技术研究进展[J]. 软件学报, 2018, 029 (005):1177-1198.

[3] 王清. 0day 安全:软件漏洞分析技术(第 2 版)[J]. 信息安全与通信保密, 2013(11):130-131.

[4] Kangjie Lu, Chengyu Song, Taesoo Kim, and Wenke Lee. UniSan: Proactive Kernel

Memory Initialization to Eliminate Data Leakages. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016.

[5] VAN DER V EEN , V., D UTT S HARMA , N., C AVALLARO , L., AND BOS , H.

Memory errors: The past, the present, and the future. In Proceedings of the 15th International Symposium on Research in Attacks, Intrusions and Defenses, 2012.

[6] 张超. 针对控制流劫持攻击的软件安全防护技术研究[D]. 北京:北京大学, 2013.

[7] 柳童,史岗,孟丹.代码重用攻击与防御机制综述[J].信息安全学报, 2016,1(02):15-27.

[8] 王丰峰,张涛,徐伟光,孙蒙.进程控制流劫持攻击与防御技术综述[J].网络与信息安全学 报, 2019(06).

[9] Microsoft. A Detailed Description of the Data Execution Prevention (DEP) Feature in

Windows XP Service Pack 2,Windows XP Tablet PC Edition 2005, and Windows Server 2003.https://support.microsoft.com/en-us/kb/875352.

[10] 黄志军,郑滔.基于 Return-Oriented Programming 的程序攻击与防护[J].计算机科学, 2012,39(S1).

[11] Kornau T. Return oriented programming for the ARM architecture[D]. Master’s thesis, Ruhr-Universität Bochum, 2010.

[12] T. Bletsch, X. Jiang, V.Freh, and Z. Liang. Jump Oriented Programming:A New Class of

Code-Reuse[C]. In Proceedings of the 2016 the 6th ACM Symposium on Information, Computer and Communications Security(ASIACCS ’11), 2011:30-40.

[13] 邢骁. 自动化构造 Jump-Oriented Programming 攻击[D].南京大学, 2012.

[14] PAX Team. "Address Space Layout Randomization" http://pax.grsecurity.net/docs/aslr.txt,

[15] 林键,郭玉东,周少皇,蔄羽佳.基于基址重定位的地址随机化技术[J].信息工程大学学报, 2016,17(06):748-753.

[16] SNOW K Z, MONROSE F, DAVI L, et al. Just-in-time code reuse: on the effectiveness

of fine-grained address space layout randomization[C]. IEEE Symposium on Security and Privacy, 2013:574-588.

[17] BITTAU A, BELAY A, MASHTIZADEH A, et al. Hacking blind[C]. IEEE Symposium on Security and Privacy, 2014:227-242.

[18] J. Seibert, H. Okhravi, and E. Soderstrom. Information Leaks Without Memory

Disclosures: Remote Side Channel Attacks on Diversified Code[C]. In Proceedings of the 21st ACM Confer- ence on Computer and Communications Security (CCS), 2014.

[19] R. Strackx, Y. Younan, P. Philippaerts, F. Piessens,S. Lachmund, and T. Walter. Breaking

the memory secrecy assumption[C]. In Proceedings of the Second European Workshop on System Security (EUROSEC '09), 2009.

[20] M. Abadi, M. Budiu, J. Ligatti, and U. Erlingsson. Control-Flow Integrity[C]. in Proc the 12th ACM Conference on Computer and Communications Security(CCS’05), 2005:340-353. [21] Oleksenko O , Kuvaiskii D , Bhatotia P , et al. Intel MPX Explained: A Cross-layer

Analysis of the Intel MPX System Stack[J]. In Proceedings of the ACM on Measurement and Analysis of Computing Systems, 2018, 2(2):1-30.

[22] Evans I , Fingeret S , Gonzalez J , et al. Missing the Point(er): On the Effectiveness of Code Pointer Integrity[C]. IEEE Symposium on Security and Privacy, 2015.

[23] J. P. Anderson. Computer security technology planning study[N]. volume 2. Technical report, DTIC Document,1972.

[24] X. Chen, D. Caselden, and M. Scott. New zero-day exploit[J]. targeting internet explorer versions 9 through 11 identified in targeted attacks, 2014.

[25] S. Nagarakatte, J. Zhao, M. M. Martin, and S. Zdancewic. Cets: compiler enforced temporal safety for c. In ACM Sigplan Notices, volume 45, pages 31-40. ACM, 2010.

[26] G. C. Necula, S. McPeak, and W. Weimer. Ccured: Type safe retrofitting of legacy code[J]. ACM SIGPLAN Notices, 2002,37(1):128-139.

[27] Dan G , Hicks M , Jim T , et al. Cyclone: A Type-Safe Dialect of C[J]. C-C++ Users Journal, 2005, 23(1):6,8,10,12-13.

[28] P. Akritidis. Cling: A memory allocator to mitigate dangling pointers[C]. In USENIX Security Symposium, 2010:177-192.

[29] N. Nethercote and J. Seward. Valgrind: a framework for heavyweight dynamic binary instrumentation[J]. In ACM Sigplan Notices, volume 42, ACM, 2007:89-100.

[30] N. Hasabnis, A. Misra, and R. Sekar. Light-weight bounds checking[C]. In IEEE/ACM Symp. on Code Generation and Optimization, 2012.

[31] K. Serebryany, D. Bruening, A. Potapenko, and D. Vyukov. Addresssanitizer: A fast address sanity checker[C]. In USENIX Annual Technical Conference, 2012:309-318.

[32] MASHTIZADEH A J, BITTAU A, MAZIERES D, et al. Cryptographically enforced control flow integrity[J]. arXiv preprint arXiv, 2014:1408-1451.

[33] CRISWELL J, DAUTENHAHN N, ADVE V. KCoFI: complete control-flow integrity for

commodity operating system kernels[C]. IEEE Symposium on Security and Privacy, 2014:292-307.

[34] ZHANG C, WEI T, CHEN Z, et al. Practical control flow integrity and randomization for binary executables[J]. IEEE Symposium on Security & Privacy, 2013:559-573.

[35] ZHANG M, SEKAR R. Control Flow Integrity for COTS Binaries[C]. Presented as part of the 22nd Security Symposium, 2013:337-352.

[36] L. Davi, A. Sadeghi, D. Lehmann. and F. Monrose, Stitching the Gadgets On the

Ineffectiveness of Coarse-Grained Control-Flow Integrity Protection[C]. In Proceedings of the 23rd USENIX Security Symposium.(Usenix’14), 2014:401-416.

[37] E. Athanasopoulos.H. Bos,G. Portokalidis, and E. Goktas. Out of Control Overcoming Control-Flow Integrity[C]. IEEE Symposium on Security and Privacy.(SP’14),2014:575-589. [38] Lu K , Song C , Lee B , et al. ASLR-Guard: Stopping Address Space Leakage for Code

Reuse Attacks[C]. In Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS '15). ACM, 2015.

[39] GIUFFRIDA C, KUIJSTEN A, TANENBAUM A S. Enhanced operating system security

through efficient and fine-grained address space randomization[C]. Presented as Part of the 21st USENIX Security Symposium (USENIX Security 12), 2012:475-490.

[40] Chen X , Xue R , Wu C . Timely address space rerandomization for resisting code reuse attacks[J]. Concurrency and Computation, 2017, 29(16):1-14.

[41] CHEN Y, WANG Z, WHALLEY D, et al. Remix: on-demand live randomization[C]. The sixth ACM Conference on Data and Application Security and Privacy, 2016: 50-61.

[42] HAWKINS W, NGUYEN-TUONG A, HISER J D, et al. Mixr: flexible runtime rerandomization for binaries[C]. The 2017 Workshop on Moving Target Defense. 2017:27-37. [43] BIGELOW D, HOBSON T,RUDD R, et al. Timely rerandomization for mitigating

memory disclosures[C]. ACM Sigsac Conference on Computer & Communications Security,

[44] 雷啸. 内存信息泄露的运行中随机化防御方法的研究与改进[D]. 南京: 南京大学, [45] MORTON M, KOO H, LI F, et al. Defeating zombie gadgets by re-randomizing code

upon disclosure[C]. International Symposium on Engineering Secure Software and Systems, 2017:143-160.

[46] V. Kuznetsov, L. Szekeres, M. Payer, G. Candea, R. Sekar, and D. Song. Code-pointer

integrity[C]. In Proceedings of the 11th USENIX Symposium on Operating Systems Design and Implementation, 2014:6-8.

[47] Hedayati M , Gravani S , Johnson E , et al. Hodor: intra-process isolation for high-

throughput data plane libraries[C]. In the Proceedings of the 2019 USENIX Annual Technical Conference, 2019:10-12.

[48] Park S , Lee S , Xu W , et al. libmpk: Software Abstraction for Intel Memory Protection Keys [J]. 2018.

[49] Linux. The Linux Kernel Archives[OL]. https://www.kernel.org/doc/html/v5.4/x86/intel\_mpx. html.

[50] N. Burow, X. Zhang and M. Payer, SoK: Shining Light on Shadow Stacks[J], 2019 IEEE Symposium on Security and Privacy (SP), 2019:985-999.

[51] Ben Niu and Gang Tan. Modular control-flow integrity[C]. In Proceedings of the 35th

ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI '14), 2014:577-587.

[52] P. Akritidis, C. Cadar, C. Raiciu, M. Costa and M. Castro, Preventing Memory Error Exploits with WIT.[C]. IEEE Symposium on Security and Privacy (sp 2008), 2008:263-277. [53] N. Carlini and D. Wagner. Rop is still dangerous: Breaking modern defenses[C]. In USENIX Security Symposium, 2014:20-24.

致谢

忙碌的读研生活就要结束了,而我也将再一次经历别离,两年时光里我遇到了许许多多博学可爱的人,在这邻近毕业之际我也只能通过这短短的几句话来表  
达我对身边可敬之人的感谢

首先我要感谢我的论文指导老师汪老师,感谢老师在论文完成过程中的给予的帮助。其次我要感谢实习单位的领路人应师兄,师兄在我实习的过程中给予了极大的帮助,教授了我许多的知识,在我们平常的学习,论文的撰写都给予了许多宝贵的意见。我也感谢科大给了我学习的机会,在以后的生活中我会一直会以是科大学子而感到自豪,最后感谢各位百忙之中参加评审答辩的老师。

而今我坐在这窗台前,迎着清晨第一缕阳光写下这最后一句话,再见了我18年的学生生涯。

2021年10月28日