RV与芯片评论.20210130.第5周(总第27期)

[PDF] VP Float: First Class Treatment for Variable Precision Floating Point Arithmetic-Poster

Comparison of RISC-V and transport triggered architectures for a postquantum cryptography applic...

一周专利

[PDF] Multi-chip stacked devices

METHOD FOR EXECUTING A BINARY CODE OF A SECURE FUNCTION WITH A MICROPROCESSOR

重点聚焦

平头哥AOSP专题

- 本专题上周报道：https://www.yuque.com/riscv/rvnews/20210123#4ae3ff22
- OSDT Monthly Meetup 2021-01-24关于AOSP的汇报：
  - PLCT吴伟&汪辰
  - 1. 平头哥的开源比较彻底，为其它RISCV厂商铺平了道路。
  - 2. 硬件配置和驱动部分未开源，是prebuilt/binary，符合android的惯例（我记得是）
  - 3. 工具链部分可能有平头哥的自定义改动，不过不属于AOSP项目，是否开源/其它厂商是否需要自己做，还不清楚，当前时间没分析到。
  - 📎wangchen-t-head-aosp-riscv.pdf
- 相关新闻
  - 包永刚："直戳Arm长处！首个RISC-V版安卓10系统顺畅运行 (From www.leiphone.com 2021.01.31)"
  - "阿里平头哥：首个RISC-V版安卓10系统顺畅运行 (From www.guancha.cn 2021.01.31)"
  - "阿里“平头哥”移植安卓，Risc-V会在中国替代ARM吗? (From www.donews.com 2021.01.31)"
- 相关讨论
  - "如何评价平头哥完成了安卓 10 对 RISC-V 的移植并开源代码？对 RISC-V 生态有何意义? (From www.zhihu.com 2021.01.31)"

RISC-V国际开源论坛

1月27日至28日，帕特森RISC-V国际开源实验室(RIOS)、RISC-V 国际基金会、鹏城实验室携手举办“第二届 RISC-V 国际开源论坛

- "探索计算浪潮的下一个十年！第二届RISC-V国际开源论坛即将在深开幕 (From finance.eastmoney.com 2021.01.31)"

第一届RISC-V技术及生态研讨会

> 拟于2021年6月28日（暂定）在上海召开。会议由中国科学院软件研究所主办，聚焦于 RISC-V 相关的原创性研究、系统应用及生态建设，包括新的软件架构设计、系统实现、开发工具、验证及测试工具等。

"第一届RISC-V技术及生态研讨会 (From rvte.github.io 2021.01.31)"

相关周报

- semi engineering Week In Review:
  - Blog Review：Jan. 27
  - Design, Low Power：*CXL 2.0 published; power and signal signoff for multi-die; encrypting data in HPC SoCs; RISC-V validation test suites.*
  - Manufacturing, Test：Intel's packaging investment; D2S platform; etch; Advantest, Lam, TEL, UMC results.
  - Auto, Security, Pervasive Computing：*Flex Logix on AI edge; DARPA SSITH success; Emotet downed*
- IoT News：（Site）：Jan. 29, 2021
- OSDT Weekly：(zhihu，Github)：" 2021-01-27 第082期
  - OSDT Monthly Meetup 2021-01-24：https://www.bilibili.com/video/BV1fA411H7sW
- 泰晓咨询：（Site）：
- PLCT开源进展：(Github，zhihu）：第18期·2021年02月01日
- RT-Thread：（oschina）：【20210122期AI简报】保姆级深度学习环境配置指南、寒武纪首颗AI训练芯片亮相
- 科技爱好者周刊：（yuque）：
- 硅农亚历山大: "RISC-V双周报1.12-1.26 (From mp.weixin.qq.com 2021.01.31)"

技术动态

一周问答

- 包云岗："大学想学一下risc-v cpu设计，应该怎么入门？（From www.zhihu.com 2021.01.26)"
- "从技术的角度来看，RISC-V 能对芯片发展、科技自主起到哪些作用？（From www.zhihu.com 2021.01.31)"

社区动态

- "2021年集创赛“芯来RISC-V杯”等你来战！（From www.riscv-mcu.com 2021.01.31)"
- "2021年首场嵌入式AI峰会正式启动，3月上海见 | GTIC 2021（From www.sohu.com 2021.01.31)"

产业风云

- "高通前CEO再创业！用RISC-V把5G平台功耗降低10倍 (From www.leiphone.com 2021.01.31)"
- "33年技术老兵重回Intel辅佐新CEO基辛格：之前是RISC-V架构掌门人 (From 3g.163.com 2021.01.31)"
    - "英特尔聘请33年资深老将Sunil Shenoy来领导设计工程团队 (From www.cnbeta.com 2021.01.31)"
- "国家大基金突然减持三大半导体龙头：千亿巨头在列 什么信号？ (From finance.sina.com.cn 2021.01.31)"

评论文集

- "2020年，RISC-V乘风破浪！ (From mp.weixin.qq.com 2021.01.25)"
- "高云半导体访谈：国产FPGA公司如何在全球FPGA市场进行差异化竞争？ (From www.ednchina.com 2021.01.31)"
- "RISC-V至少可以在嵌入式领域取得一定成功！ (From www.sohu.com 2021.01.31)"

其他动态

博文推荐

- "【RISC-V MCU CH32V103测评】+首次使用 (From bbs.eeworld.com.cn 2021.01.31)"
- "【RISC-V MCU CH32V103测评】 ---前进的维子---USB枚举概念 (From bbs.eeworld.com.cn 2021.01.31)"
- "【RISC-V MCU CH32V103测评】使用USART2 [(From bbs.eeworld.com.cn 2021.01.31)"
- "RISC-V嵌入式开发（1）：PIO入门 & 点亮LED (From zhuanlan.zhihu.com 2021.01.31)"
- "[RISC-V MCU 应用开发] 第六十四章、CH32V103应用教程——USART-中断 (From bbs.21ic.com 2021.01.31)"
- "Windows/Ubuntu qemu虚拟机xv6-riscv利用riscv-gnu-toolchain编译安装方法 (From blog.csdn.net 2021.01.31)"
- "MIT 6.S081 2020 LAB4记录 (From zhuanlan.zhihu.com 2021.01.31)"

一周论文

架构改进

Customizable Vector Acceleration in Extreme-Edge Computing: A RISC-V Software/Hardware Architecture Study on VGG-16 Implementation

M Olivieri, A Cheikh, F Menichelli, A Mastrandrea... - 2021

相对于云计算而言，云边缘连续体中的计算，依赖于物联网层次结构的极端边缘的高性能处理。硬件加速是实现性能要求的强制性解决方案，然而它可能与特定的计算内核紧密相连，甚至在同一应用中。面向向量的硬件加速已经重新获得了兴趣，以支持卷积网络或分类算法等人工智能应用。我们对可配置的矢量加速子系统所能达到的性能和功耗效率进行了全面的调查，获得了所提出的微架构的高潜力和对软件程序完全透明的硬件定制优势的证据。

Floating Point CGRA based Ultra-Low Power DSP Accelerator

R Prasad, S Das, KJM Martin, P Coussy – Journal of Signal Processing Systems, 2021

粗粒度可重构阵列(CGRAs)作为高能效的加速器正在兴起，为学术界和工业界提供了高等级的灵活性。然而，随着最近算法的进步和应用的性能要求，只支持整数和逻辑运算限制了经典/传统CGRA的兴趣。在本文中，我们提出了一种新型的CGRA架构和相关的编译流程，同时支持整数和浮点运算，以实现DSP应用的节能加速。实验结果表明，与DSP优化的、基于RISC-V的超低功耗CPU相比，所提出的加速器在执行发作检测时实现了最大4.61倍的加速，而发作检测是范围广泛的脑电信号处理应用的代表，面积开销为1.9倍。与单核CPU相比，提出的CGRA实现了最高6.5×的能效。而与8核的多核CPU执行比较，提出的CGRA实现了高达4.4×的能量增益。

1. 为了保持一致性，本文所有的实验都采用了8个RI5CY核的PULP-cluster单一模板。Pulp-cluster会自动禁用其他不使用的核心。
2. PULP-cluster包含一个共享FPU集群，该集群本身由4个FPU组成，PULP-cluster自动禁用其他未使用的FPU。

芯片安全

[PDF] Kronos: Verifying leak-free reset for a system-on-chip with multiple clock domains

N Moroze – 2021

Notary[3]使用形式化验证为一个简单的片上系统(SoC)证明了一个称为确定性启动的硬件级安全属性。确定性启动要求SoC的状态被引导代码完全重置，以确保秘密不能跨越重置边界泄漏。然而，Notary的方法有几个限制。它的安全属性要求SoC的所有微架构状态都可以通过软件复位到已知值，而且该属性和证明技术只适用于具有单一时钟域的SoC。这些限制使得Notary的方法无法应用于更复杂的系统。本论文通过Kronos来解决这些局限性，Kronos是一个由经过验证的SoC组成的系统，它满足一个新的安全属性，称为输出确定性。输出确定性提供了与Notary相同的安全保证，而不要求SoC的所有状态被软件重置。Kronos中使用的SoC称为MicroTitan，基于开源的OpenTitan[16]，包括多个时钟域。本论文对Kronos进行了评估，并证明现有的开源硬件可以通过最小的改动来满足输出确定性，并且在证明输出确定性的过程中，可以发现违反预期安全保证的硬件问题。

[PDF] Enclaves in the Clouds: Legal considerations and broader implications

J Singh, J Cobbe, DL Quoc, Z Tarkhani – Queue, 2020

随着组织数据实践受到越来越多的审查，对能够协助组织履行其数据管理义务的机制的需求正在增长。TEEs(可信执行环境)提供了基于硬件的机制，具有各种安全属性，以协助计算和数据管理。TEEs关注的是数据、代码以及相应计算的保密性和完整性。由于主要的安全属性来自于硬件，所以即使主机特权软件栈存在漏洞，也可以提供一定的保护和保证。

Multi-Layer Security Framework for IoT Devices

A Vochescu, I Culic, A Radovici – 2020 19th RoEduNet Conference: Networking in ..., 2020

目前很多个人和公司都从安全问题的角度来看待物联网。许多与物联网技术相关的安全威胁都来自于软件和应用的实现方式，或者是使用的编程框架。更重要的是，随着应用越来越复杂，硬件设备越来越受限，很多安全机制无法应用。本文的目的是提出一个专门针对硬件受限设备的多层安全框架。

[PDF] CHANCEL: Efficient Multi-client Isolation Under Adversarial Programs

A Ahmad, J Kim, J Seo, I Shin, P Fonseca, B Lee – 2021

英特尔SGX旨在为未受信任的云机上的用户数据提供保密性。然而，处理机密用户数据的应用程序可能会包含泄露信息的bug，或者被恶意编程以收集用户数据。试图解决这个问题的现有研究并没有考虑单一飞地中的多客户端隔离。我们表明，由于SGX的限制，不支持这种飞地内隔离，当在不同的飞地进程中并发处理多个客户端时，它们会产生相当大的减速。
本文提出了CHANCEL，这是一个沙盒，设计用于在一个SGX飞地内实现多客户端隔离。特别是，CHANCEL允许程序的线程在服务请求时同时访问每个线程的内存区域和共享的只读内存区域。每个线程同时处理来自单个客户端的请求，并使用多客户端软件故障隔离（MCSFI）方案与其他线程隔离。此外，CHANCEL还支持各种圈内服务，如内存文件系统和屏蔽客户端通信，以保证程序与外界的交互完全调解。我们在SGX硬件上实现了CHANCEL，并利用微基准和现实的目标场景对其进行了评估，包括私人信息检索和产品推荐服务。我们的结果表明，CHANCEL在微基准上的性能比基线多进程沙盒高4.06–53.70倍，在现实工作负载上的性能比基线多进程沙盒高0.02–21.18倍，同时提供了强大的安全保障。

模块设计

Memory System Design and Optimizations for Data Intensive Computing

X Wang – 2020

新兴的数据密集型应用，如图形分析和数据挖掘，表现出巨大的数据集和不规则的内存访问模式。研究表明，这些受内存束缚的应用无法有效利用传统基于缓存的内存系统中的数据定位和规则内存访问原则来缓解 "内存墙 "问题。数据量的膨胀同时推动了大规模计算系统中从单片架构向集成了离散和分布式节点的系统过渡。因此，多层软件基础设施已成为弥合异构商品设备之间差距的关键。然而，利用分歧接口的节点间内存操作不可避免地导致冗余延迟和性能下降。此外，现代分布式共享内存编程模型（即OpenSHMEM、MPI-RMA等）所采用的绕过操作系统和远程CPU的频繁单边远程内存访问也会暴露出

安全漏洞。现有的可信执行环境(TEE)或飞地系统，如ARM TrustZone、英特尔SGX、RISC-V Keystone等，提供本地内存隔离。遗憾的是，这些解决方案并不能为节点间的内存事务提供同样的保护。
在本论文研究中，我们首先探讨了基于3D堆栈内存设备的内存内优化，以提高数据密集型工作负载的性能。
我们设计了一个内存热点感知管理器（HAM），提供内存内请求聚合和热点预取。然后，我们通过引入内存访问聚合器(MAC)以及相关的新架构来优化节点内内存系统的性能，这些新架构利用3D堆叠内存设备，如混合内存立方体(HMC)和高带宽内存(HBM)。除了本地存储器系统，我们还为RISC-V指令集架构（ISA）引入了一个全局地址空间扩展，以实现高性能的节点间存储器系统。我们将这种RISC-V ISA扩展指定为扩展基础全局地址空间，或xBGAS。xBGAS扩展通过将远程对象映射到系统的扩展地址空间，为直接访问远程共享数据块提供了原生的ISA级支持。最后，我们介绍了一种基于xBGAS基础架构和Keystone（用于RISC-V系统的开源安全飞地）结合的可扩展飞地设计。我们展示了所提出的可扩展的飞地系统的设计，并与现有的作品进行了比较。我们还分析了潜在的威胁模型，并讨论了我们的设计如何抵御这些威胁。
使用HAM和带有MAC的本地内存系统设计的内存内优化利用了3D堆叠内存设备固有的大吞吐量和内存级并行性(MLP)，以满足带宽驱动应用的需求。考虑到数据密集型工作负载的不规则内存访问模式，我们的节点内内存系统优化提供了一个更大的潜力，通过重叠计算和通信来隐藏内存访问延迟，而不是通过缓存预取导致的延迟减少。正交上，xBGAS为高性能的远程内存访问提供了一个可扩展的节点间内存系统。因此，它在优化分布在离散节点上的海量数据集的数据密集型应用方面有很大的前景。在此，ISA级的节点间数据操作可以提高大规模计算系统中远程请求的注入率以及网络带宽利用率，而不需要引入桥接各种异构设备所需的繁琐软件基础设施。此外，xBGAS基于对象的数据管理模型使其非常适合数据中心规模的RISC-V服务器和未来的超大规模计算系统。此外，通过将数据对象ID映射到扩展的地址空间中，通过使用统一的内存访问简化了节点间的数据保护，其中权限位被用于对每个数据对象的访问控制。此外，xBGAS的低延迟远程数据操作也抵消了硬件权限检查过程的时间成本。这有助于缓解节点间环境中与飞地系统的物理内存隔离相关的性能下降。

[PDF] Quantifying Soft-Error Resilience of Embedded RISC-V Systems with Capability-based Memory Protection

M Bargholz

Leibniz结构尺寸的缩小和电源电压的降低加剧了器件在其寿命期内所经历的瞬态故障的数量。这些瞬态错误行为往往会导致广泛而昂贵的故障。因此，人们开发了大量的保护方案来解决弹性降低的问题。这些方案大多在硬件或运行时产生巨大的开销，而且对于商品电子产品来说，价格昂贵得令人望而却步。为了避免这些开销，设计者通常会寻求通过现有的保护方案（如内存保护）来增加软错误保护。CHERI保护模型通过使用称为能力的增强指针来保护系统的内存访问。为了评估CHERI的内存保护对系统软错误弹性的影响，我们比较了两种架构，一种是未保护的，一种是用CHERI保护的。它们各自的软错误恢复能力是通过使用故障注入对几个工作负载进行近似计算的。总之，CHERI减少了系统经历的无声数据损坏和超时的数量。此外，它还通过检测更多的错误和更快的检测速度来提高软错误的检测能力。因此，基于能力的内存保护提供了对软错误的有效保护，尽管它并没有明确的设计。 汉诺威大学

产业报告

[PDF] The Semiconductor Supply Chain: Assessing National Competitiveness

SM Khan, A Mann, D Peterson – 2021

> 半导体是推动科学进步、促进经济发展和确保国家安全的重要组成部分。本问题简报总结了半导体供应链的每一个组成部分，以及美国及其盟友拥有的最大影响力。相关的政策简报 "确保半导体供应链 "建议采取政策行动，以确保美国保持这种影响力，并利用这种影响力促进人工智能等新兴技术的有益利用。中国的芯片设计者可以在开源架构RISC-V和MIPS的基础上进行开发--成功可能需要数年时间，但这将消除中国对专有的英国和美国核心IP的依赖

EDA，软件和工具

Enabling High-Level Programming Languages on IoT Devices

T Severin, I Culic, A Radovici – 2020 19th RoEduNet Conference: Networking in ..., 2020

> 如今，物联网（IoT）已经不是一个新奇而暧昧的词汇。随着智能手表等物联网技术对日常生活质量的提高，人们对联网设备的依赖程度逐渐提高。然而，尽管普及率成倍增长，但用于将日常设备和嵌入式计算机连接到互联网的技术仍然有限。虽然网络和桌面应用的编程语言和运行时程范围变得更广，但物联网开发工具缺乏多样性。在这种情况下，本文旨在改编一种新的、流行的编程语言，用于构建物联网应用。D是一种易于使用且被广泛使用的编程语言，目前还没有被设计为在物联网领域内使用。通过改编D以运行在受限的设备上，我们希望使物联网原型设计更容易获得。

[PDF] VP Float: First Class Treatment for Variable Precision Floating Point Arithmetic-Poster

A Cohen – 2020

... To evaluate the portability of our approach, we also demonstrate our LLVM implementation targeting a coprocessor for a **RISC-V** Rocket core accelerating FP arithmetic in the UNUM format [1]. Unfortunately we hit hardware bugs ...

Comparison of RISC-V and transport triggered architectures for a postquantum cryptography application

L AKÇAY, ÖRS Berna – Turkish Journal of Electrical Engineering & Computer ..., 2021

> Cryptography is one of the basic phenomena of security systems. However, some of the widely used publickey cryptography algorithms can be broken by using quantum computers. Therefore, many postquantum cryptography algorithms are proposed in ...

一周专利

[PDF] Multi-chip stacked devices

VK Koganti, AK Kandala, S Yachareni – US Patent 10,886,921, 2021

US10886921B1 – Multi-chip stacked devices – Google Patents. Multi-chip stacked devices. Download PDF Info. Publication number US10886921B1. US10886921B1 US16/825,340 US202016825340A US10886921B1 US 10886921 ...

METHOD FOR EXECUTING A BINARY CODE OF A SECURE FUNCTION WITH A MICROPROCESSOR

O Savry – US Patent App. 16/918,144, 2021

... microprocessor 2. By way of illustration, the microprocessor 2 has a RISC (Reduced Instructions Set Computer) architecture and implements the "**RISC-V**" instruction set. Here, the unit 10 is an arithmetic logic unit of N inst bits. The ...

RISC-V与芯片评论编辑部 – RISC-V和芯片动态周报

每周六发布

欢迎批评，指正，评论和加入

关于本刊:

- 非特殊注明，本刊消息均来自于网络，如有版权问题，我们会立刻处理。
- 本刊部分消息来源

语雀	微信公众号	Gitee	Github	Inspur
RISC-V和芯片动态简报 riscv rvnews	高效服务器和存储技术国家重点实验室	inspur-risc-v RVWeekly	inspur-risc-v RVWeekly	riscv RVWeekly