

RV与芯片评论.20210320: 2021年第12周(总第34期)

重点聚焦

[龙芯与MIPS转RISC-V](#)

[两会](#)

[相关周报](#)

技术动态

[一周问答](#)

产业风云

其他动态

[博文推荐](#)

一周论文

架构

[\[PDF\] An Ultra-Low-Power Embedded Processor with Variable Micro-Architecture](#)

[\[PDF\] Scaling Concurrency Reasoning to Relaxed Memory Models and Beyond](#)

[Balancing Specialized Versus Flexible Computation in Brain-Computer Interfaces](#)

[\[PDF\] Ultra-Elastic CGRAs for Irregular Loop Specialization](#)

[Enhancing Atomic Instruction Emulation for Cross-ISA Dynamic Binary Translation](#)

[\[PDF\] A Study on Improvement of Low-power Memory Architecture in IoT/edge Computing](#)

安全

[\[PDF\] SoCCAR: Detecting System-on-Chip Security Violations Under Asynchronous Resets](#)

[\[PDF\] Efficient Subobject-granularity Spatial Memory Safety Enforcement with In-fat Pointer](#)

仿真验证, EDA, 敏捷开发

[\[PDF\] Towards Agile Hardware Designs with Chisel: a Network Use-case](#)

[\[PDF\] Enabling Reproducible and Agile Full-System Simulation](#)

加速, 硬件算法

[\[PDF\] An Architecture of Area-Effective High Radix Floating-Point Divider With Low-Power Consump...](#)

[\[PDF\] Project-Based Learning and Evaluation in an Online Digital Design Course](#)

[\[PDF\] Efficient Implementation of NIST LWC ESTATE Algorithm Using OpenCL and Web Assembly fo...](#)

本期概要

- 关于MIPS投RISC-V，EDN：“对龙芯无影响”
- 盘点国内RISC-V内核MCU厂商系列文章
- 两会和RISC-V
- 字节跳动，汇顶，君正和格兰仕

重点聚焦

龙芯与MIPS转RISC-V

"MIPS放弃自研架构，转投RISC-V，可用处理器种类进一步减少 (From finance.sina.com.cn 2021.03.20)"

"MIPS转投RISC-V是龙芯新征程的开始 (From www.ednchina.com 2021.03.20)"

上周，EDN报道了关于MIPS Technologies宣布将放弃继续设计MIPS处理器，转向了RISC-V的消息。引起了网友们的热议，有人认为龙芯要完。但业内人士但铁流认为，这完全是不了解龙芯具体情况的臆测。特别是在龙芯开发自主指令集LoongArch之后，已经在指令集方面走上了独立自主道路。他认为，MIPS投RISC-V，对于龙芯而言，是新征程的开始。

"MIPS 已死，转身投靠 RISC-V (From www.36kr.com 2021.03.20)"

"基于自主指令集的龙芯3系列处理器即将问世 (From zhuanlan.zhihu.com 2021.03.20)"

"龙芯5000系列处理器将于年内发布，未来有望加入RISC-V架构的设计 (From post.smzdm.com 2021.03.20)"

据TomsHardware报道，龙芯3A5000处理器将采用12nm工艺制造，基于MIPS64指令集兼容的新架构，配置了新的内存控制器以及更大的缓存，拥有4核心，频率为2.5GHz，在性能上与AMD最后一代推土机架构产品相当。龙芯3C5000处理器则拥有16核心，支持4至16路服务器。

HKEPC称，代工的可能性会是中芯国际。

两会

"全国政协常委李家杰：培育成熟的开源芯片生态 实现科技自立自强 (From finance.sina.com.cn 2021.03.20)"

在今年的全国两会上，李家杰带来包括《培育成熟的开源芯片生态实现科技自立自强》《关于大力推动RISC-V开源架构在信创产业应用的提案》以及《推动以智慧能源为核心的零碳示范城市试点助力实现2060碳中和国家战略》在内的三份提案。

相关周报

-  semi engineering Week In Review:
 - Blog Review:
 - Design, Low Power:
 - Manufacturing, Test:
 - Auto, Security, Pervasive Computing:
 - IoT News: ([Site](#)) :
 - OSDT Weekly: ([zhihu](#), [Github](#)):
 - 泰晓咨询: ([Site](#)) : 3月 / 第二期 / 2021
 - PLCT开源进展: ([Github](#), [zhihu](#)) :
 - RT-Thread: ([oschina](#)) :
 - 科技爱好者周刊: ([yuque](#)) :
 - [硅农亚历山大: RISC-V双周报](#)
 - 痞子衡嵌入式半月刊: ([zhihu](#)) : 第 27 期
-

技术动态

"[RISC-V, China, Nightingales](#) (From [interconnected.blog](#) 2021.03.20)"

介绍中国国产芯片的动态。

"[苹果正自研5G基带，有望2024年使用](#) (From [www.eet-china.com](#) 2021.03.20)"

苹果继自研A系列手机芯片、M系列电脑芯片后，将再一次扩大自研芯片比重。最新消息显示，苹果正在打造自家 5G 基带，最快 2024 年开始扩大设计采用。

"[What happens when you load into x0 on RISC-V?](#) (From [commaok.xyz](#) 2021.03.20)"

目的地为x0的加载仍然必须引发任何异常，并导致任何其他副作用，即使该加载值被丢弃也是如此。

"[FPGA厂商如何降低开发难度？基于应用的平台化策略成首选](#) (From [www.eet-china.com](#) 2021.03.20)"

Lattice继2019年公布sensAI，2020年公布mVision 1.0和Sentry 1.0之后，日前，mVision 2.0和Sentry 2.0版本也正式面世。

"[极海为加速国产芯片产业化提四大技术案例](#) (From [www.ednchina.com](#) 2021.03.20)"

极海半导体有限公司CEO汪栋杰先生发表了《相信 坚持 突破——加快国产关键核心芯片研发与产业化》的精彩演讲。讲述了公司十多年来的发展历程，并分享了极海半导体在工控芯片市场及相关产品领域的研发情况和技术优势，同时深入解析了当前的市场现状及未来的发展趋势和技术挑战。

极海的芯片设计技术能力具备以下4个特点：

- CPU内核设计能力：极海具备16 / 32 / 64位自主内核及RISC-V内核独立设计能力
- 多核异构芯片设计能力：提供双核至七核SoC芯片设计，低功耗、高集成、高安全
- 混合架构芯片设计能力：实现国产玄铁C-SKY混编ARM内核，混编RISC-V内核，为产品提供出色的效能与安全性

- 安全加密嵌入式eSE芯片设计能力：实现嵌入式硬件级安全防护，在性能和成本方面具备极大优势

一周问答

"如何看待 MIPS 转投 RISC-V 阵营？对龙芯有什么影响？ (From www.zhihu.com 2021.03.20)"

产业风云

"字节跳动跑步进入芯片赛道 正自研云端AI和Arm服务器芯片 (From finance.sina.com.cn 2021.03.20)"

字节跳动正在积极组建AI芯片团队，选择从云端AI芯片和Arm服务器芯片布局芯片领域

"汇顶科技换帅，前德州仪器副总裁胡煜华入驻 (From www.ofweek.com 2021.03.20)"

以产品来说，汇顶科技所擅长的领域，如微控制器，虽然加入了新型架构Risc-V。但事实上，这种芯片的成本几乎是公开的，而汇顶科技作为芯片设计商，他们的利润也是定死的，不像处理器芯片那样，越高的制程象征了越高的利润。

"AWE2021：格兰仕首次携“中国芯”参展 (From finance.sina.com.cn 2021.03.20)"

2021中国家电及消费电子博览会（AWE2021）即将在上海开幕，值得关注的是，国民家电格兰仕将携“中国芯”生态圈伙伴跃昉科技和应用自主开源芯片的智能家电参展。这是首家在AWE上展出自主芯片的家电科技企业。

"北京君正：近几年来一直在推进RISCV CPU核的研发 (From www.sohu.com 2021.03.20)"

北京君正（300223.SZ）3月18日在投资者互动平台表示，我们认为RISC V将在业界得到快速发展，公司近几年来一直在推进RISCV CPU核的研发，CPU核的研发相对复杂度较高，公司将在时机成熟时推出基于RISC V核的芯片产品

其他动态

博文推荐

"riscv-v-spec-1.0（矢量指令）学习理解（1-5 & 18 segment） (From blog.csdn.net 2021.03.20)"

"盘点国内MCU级RISC-V内核IP厂商 (From zhuanlan.zhihu.com 2021.03.20)"

"盘点国内RISC-V内核MCU厂商(2018年发布产品) (From zhuanlan.zhihu.com 2021.03.20)"

"盘点国内RISC-V内核MCU厂商(2019年发布产品) (From zhuanlan.zhihu.com 2021.03.20)"

"盘点国内RISC-V内核MCU厂商(2020年发布产品) (From zhuanlan.zhihu.com 2021.03.20)"

"盘点国内RISC-V内核MCU厂商(2021年发布产品) (From zhuanlan.zhihu.com 2021.03.20)"

" [【RISC-V MCU CH32V103测评】简易文本阅读器的功能实现](#) [(From bbs.eeworld.com.cn 2021.03.20)"]

" [【RISC-V MCU CH32V103测评】+RTC使用](#) (From bbs.eeworld.com.cn 2021.03.20)"

" [【RISC-V MCU CH32V103测评】- 9: 电动机控制板](#) (From bbs.eeworld.com.cn 2021.03.20)"

一周论文

架构

[PDF] [An Ultra-Low-Power Embedded Processor with Variable Micro-Architecture](#)

W Ma, Q Cheng, Y Gao, L Xu, N Yu – Micromachines, 2021

嵌入式处理器被广泛应用于各种系统中，工作在不同的任务上，工作负载不同。更复杂的微架构会带来更好的峰值性能和更差的功耗。关闭为提升性能而设计的单元，可以提高低工作负载情况下的能源效率。在本文中，我们评估了各种嵌入式处理器中的能量分布。根据分析，为了更好的峰值性能而采用的流水线寄存器和动态分支预测器，对能量效率有很大的影响。因此，我们提出了一种具有可变微架构的超低功耗处理器。该处理器基于4级流水线核心，采用Gshare分支预测器，所有单元都工作在高性能模式下。在正常模式下，关闭Gshare预测器，使用AlwaysNot-Taken预测。在低功耗模式下，部分流水线寄存器被旁路，以避免不必要的能量消耗，提高执行效率。模式寄存器(MR)被设计用来指示当前的工作模式。不同模式之间的切换由软件控制。所提出的核心是在40纳米技术和Embentch 17基准的痕迹模拟实现。各模式的平均功耗分别为41.7 μ W、59.7 μ W和71.1 μ W。结果显示，普通模式(N模式)和低功耗模式(L模式)比高性能模式(H模式)的平均功耗分别低16.08%和41.37%。在最好的情况下，它们可以比H模式多节省25.36%和49.30%的电力。考虑到以每周期指令(IPC)评估的执行效率，建议的处理器每条指令的能耗比基线内核少7.78%或51.57%。建议的处理器面积仅比基线内核大7.19%，H模式下的功耗仅多3.08%。

[PDF] [Scaling Concurrency Reasoning to Relaxed Memory Models and Beyond](#)

HHAI DANG

推理并发性是很难的。在像C/C++或Rust这样包含许多交织复杂特性的完整的非玩具语言中推理并发性就更难了。然而，现实的并发性涉及到放松的内存模型，这比简单的、传统的并发性模型即顺序一致性的推理要难得多。为了在这种复杂的语言中进行现实并发性的验证，我们需要几个要素。(1)模块化推理，这样我们就可以将较小的验证结果组成较大的验证结果；(2)强大但抽象的推理原则，这样我们就可以对棘手的语言特征进行推理，而不必处理底层并发模型的繁琐细节；(3)推理的可扩展性，这样我们就可以为复杂的语言特征和算法推导出新的推理原则，而不必从头开始重建我们的逻辑；(4)具有强大自动化支持的机器检查证明，这样我们就可以在验证中错过潜在的不健全性。直到最近，在并发分离逻辑框架Iris的帮助下，才有可能同时获得这些要素。在这个提案中，我将介绍我们在松弛内存模型的验证方向上所取得的成果。特别是，我将总结我们在用松弛内存模型验证Rust的类型系统方面的努力。然后，我

将提出几个进一步的研究方向作为完成本论文的潜在目标。这些方向包括 (i)线性化作为放宽内存库的更强规范；(ii)非易失性内存模型的程序逻辑，它扩展了放宽内存模型；(iii)最放宽架构(如ARM)的程序逻辑，即有前途的语义。

Balancing Specialized Versus Flexible Computation in Brain-Computer Interfaces

K Sriram, I Karageorgos, N Lindsay, X Wen, R Manohar... – IEEE Micro, 2021

我们正在构建HALO，这是一种灵活的超低功耗处理架构，用于直接与生物神经元进行实时通信的植入式脑机接口（BCI）。本文讨论了BCI设计者必须平衡的刚性功率、性能和灵活性的权衡，以及我们如何通过HALO;领域特定硬件加速器、通用微控制器和可配置互连的调色板来克服这些问题。我们使用从非人类灵长类动物体内收集的神经元数据进行评估，并采用全栈算法进行芯片协同设计，结果显示，与现有的植入式BCI相比，HALO实现了灵活性和卓越的每瓦特性能。

[PDF] Ultra-Elastic CGRAs for Irregular Loop Specialization

C Torng, P Pan, Y Ou, C Tan, C Batten

可重构加速器结构，包括粗颗粒可重构阵列(CGRAs)，已经重新引起人们的兴趣，因为它们允许快节奏的软件算法开发在制造后继续发展。CGRAs传统上针对的是具有数据级并行性的常规工作负载(如神经网络、图像处理)，但一旦集成到SoC中，它们就会被闲置，无法用于不规则工作负载。重新利用这些闲置资源的新趋势提出了如何有效地映射和执行通用循环的重要问题，这些循环可能具有不规则的内存访问、不规则的控制流和迭代间循环依赖性。最近的工作越来越多地利用CGRA中的弹性来缓解前两个挑战，但仅靠弹性并不能解决迭代间循环依赖性问题，而迭代间循环依赖性很容易造成整体性能的瓶颈。本文针对不规则环路特化的三个挑战，提出了超弹性CGRAs(UE-CGRAs)，这是一种新型的弹性CGRA，它克服了传统VLSI的挑战，加速了真正的依赖性瓶颈，并节省了不规则环路的能耗。UE-CGRAs允许对CGRA中的每一个可能的数百个微小的处理元件（PEs）进行可收缩的五谷动态电压和频率缩放（DVFS），使连接的PEs链在较低的电压和频率下 "休息 "以节省能量，而其他连接的PEs链可以在较高的电压和频率下 "冲刺 "以加速通过真正的依赖性瓶颈。UE-CGRAs依靠一种新型的比率同步时钟方案，精心叠加在PE间弹性互连上，以实现低延迟交叉，同时仍可通过商业静态时序分析工具进行完全验证。我们介绍了UE-CGRA的分析模型、编译器、架构模板和VLSI电路，并展示了UE-CGRA如何针对不规则环路进行特化，并以合理的面积开销比传统的无弹性和弹性CGRA提高性能（1.42–1.50×）或能效（1.24–2.32×），同时与RISC-V内核相比，也提高了性能（1.35–3.38×）或能效（高达1.53×）。

Enhancing Atomic Instruction Emulation for Cross-ISA Dynamic Binary Translation

Z Zhao, Z Jiang, Y Chen, X Gong, W Wang, PC Yew – 2021 IEEE/ACM International ..., 2021

动态二进制转换(DBT)是跨ISA仿真、系统虚拟化、运行时仪表和许多其他重要应用的关键推动因素。在DBT的几个关键要求中，为原子同步指令提供等价的语义是非常重要的，例如加载-链接/存储-条件(LL/SC)，这些指令大多包含在缩减指令集架构(RISC)中，以及比较和交换(CAS)，这些指令大多包含在复杂指令集架构(CISC)中。然而，出于性能方面的考虑，最先进的DBT工具往往不能对这些原子指令进行完全正确的翻译，特别是从RISC原子指令（即LL/SC）到CISC原子指令（即CAS）的翻译。因此，有些可能会引起众所周知的ABA问题，从而导致错误的结果或程序崩溃。在我们对最先进的DBT--

QEMU的实验研究中，在Intel x86平台上（即使用CAS）运行用ARM指令集（即使用LL/SC）实现的多线程无锁堆栈操作时，经常在2秒内崩溃。尽管人们已经尝试为这种原子指令提供正确的仿真，但它们要么导致沉重的执行开销，要么需要额外的硬件支持。在本文中，我们提出了几种方案来解决这些问题，并在QEMU上实现它们，以评估它们的性能开销。结果表明，所有提出的方案都能提供正确的仿真，对于最佳方案，与现有基于软件的最佳方案相比，可以分别实现1.25x、3.21x、2.03x的最小、最大、geomean速度提升。

[PDF] [A Study on Improvement of Low-power Memory Architecture in IoT/edge Computing](#)

D Cho – Journal of the Korean Society of Industry Convergence, 2021

在物联网设备中，广泛使用的低成本设计方法非常受欢迎。在这样的网络设备中，存储器由闪存、SRAM、DRAM等组成，由于其处理的数据量大，存储器设计是影响系统性能的重要因素。因此，各设备根据市场需求选择功能、性能、成本等优化设计因素。可供低成本物联网设备使用的存储器架构设计非常有限，配置的存储器有SRAM、闪存和DRAM。为了在相同的空间内处理尽可能多的数据，通常会提供一种支持并行处理单元的架构。这种并行架构是一种以低成本提供高性能的设计方法。但是，它需要精确的软件技术来实现并行架构上的指令和数据映射。本文提出了一种支持优化并行处理性能的指令/数据映射方法。所提出的方法通过积极利用硬件和软件的并行性来优化系统性能。

安全

[PDF] [SoCCAR: Detecting System-on-Chip Security Violations Under Asynchronous Resets](#)

X Meng, K Raj, APD Nath, K Basu, S Ray

现代SoC设计包括几个复位域，可以实现异步部分复位，同时避免完全系统启动。遗憾的是，异步复位可能会引入安全漏洞，而这些漏洞通过传统的验证方式很难检测到。在本文中，我们通过一个新的安全验证框架SoCCAR来解决这个问题，该框架考虑了异步复位。该框架包括(1)在避免组合爆炸的同时，对复位控制事件进行efficient提取；(2)对提取的设计空间进行系统性探索的concolic测试。我们的实验表明，SoCCAR可以在现实的SoC设计上实现几乎完美的检测精度和几秒钟的验证时间。

[PDF] [Efficient Subobject-granularity Spatial Memory Safety Enforcement with In-fat Pointer](#)

S Xu – 2021

C和C++等编程语言缺乏内存安全，会使这些语言编写的程序存在可利用的内存损坏漏洞。空间内存安全防御可以捕捉到越界指针运算造成的内存损坏。然而，现有的作品都不能同时实现低开销、高兼容性和ne-grained保护。本论文提出了In-Fat Pointer，这是一种硬件辅助的空间内存安全防御，它将现有的使用对象元数据的标记指针方案的保护粒度提高到子对象约束粒度，同时保持其高兼容性和低开销。In-Fat Pointer引入了多种对象元数据方案，将指针标签位从对象元数据查找中饶出来，并将饶出来的位与内存中的类型元数据一起用于子对象绑定计算。硬件原型在FPGA板上实现，In-Fat Pointer在功能、运行时和内存性能、硬件成本估算等方面进行了评估。

仿真验证，EDA，敏捷开发

[PDF] [Towards Agile Hardware Designs with Chisel: a Network Use-case](#)

J Bruant, PH Horrein, O Muller, T Groleat, F Pétrot – IEEE Design & Test, 2021

面对数量和强度都在不断增加的分布式拒绝服务（DDoS）攻击，云服务提供商的网络稳定性岌岌可危。缓解系统必须提供高度响应的防线，同时处理每秒TB的数据。FPGA结合了可重构性和保证吞吐量和延迟，是高速网络应用的公认目标。虽然传统的硬件开发平台难以做到快速响应，但硬件构造语言（HCLs）为硬件开发带来了新的机遇。本文通过对OVHcloud缓解系统中的核心网络处理模块——哈希表的三次连续开发迭代，展示了Chisel HCL如何释放敏捷开发方法论的力量。

[PDF] [Enabling Reproducible and Agile Full-System Simulation](#)

BR Bruce, A Akram, H Nguyen, K Roarty, M Samani...

在现代计算机架构模拟器中运行实验可能是一项困难且容易出错的工作。用户必须在模拟运行之间跟踪许多配置、组件和输出。gem5模拟器也不例外，需要研究人员收集、组织和创建大量的组件来进行一次仿真。在本文中，我们介绍了GEM5ART框架，这是一个帮助gem5用户更好地构建和运行架构仿真的工具，以及GEM5 RESOURCES，这是一套已知与仿真器兼容的资源。gem5项目的这些新成员使全系统仿真变得更加容易，使研究人员能够更专注于他们的架构创新，而不是建立仿真框架。GEM5ART框架会仔细记录gem5仿真中使用的资源，并将获得的结果放在数据库中，从而实现实验的简单复制。预置的资源使研究人员可以直接跳入运行模拟，而不必花费宝贵的时间来创建它们。GEM5ART的发布采用了允许性的开源许可，允许更广泛的计算机架构社区随着工作负载和工作流程的发展做出贡献。本文中介绍的数据和相关资料的档案可以在<https://doi.org/10.6084/m9.figshare.14176802>。

加速，硬件算法

[PDF] [An Architecture of Area-Effective High Radix Floating-Point Divider With Low-Power Consumption](#)

Y Yang, Q Yuan, J Liu – IEEE Access, 2021

本文提出了一种新型的低功耗的面积效益型高radix浮点除法器结构。通过扩展标准SRT算法的原理，该除法器可以用更简单的电路估计部分商数，并在每个递归周期中容忍一定的计算误差。另外，在递归过程中的误差积累可以自动消除，不需要额外的计算周期。分割器的延迟和面积成本与半径数呈线性关系，解决了高半径分割器中商数选择表面积成本高的问题。在提出的架构基础上，实现了一种单精度浮点除法器，该除法器在65nm工艺下的面积为6037.20 μm^2 。在250MHz时，该除法器的动态功耗仅为0.848mW。与文献报道的其他分频器相比，在计算精度和性能相同的情况下，面积成本可降低90%左右。

[PDF] [Project-Based Learning and Evaluation in an Online Digital Design Course](#)

I Skliarova – Electronics, 2021

处理器中的浮点(FP)单元一般仅限于支持IEEE 754标准定义的格式子集。因此，针对高性能计算的高效语言和优化编译器只支持IEEE标准类型，需要更高精度的应用涉及到繁琐的内存管理和对外部库的调

用，导致代码臃肿，使程序的意图不明确。我们提出了C类型系统的扩展，可以表示通用的FP操作和格式，支持静态精度和动态可变精度。我们设计并实现了一个编译流程，弥补了该类型系统与低级FP指令或软件库之间的抽象差距。我们通过基于LLVM的实现来证明我们解决方案的有效性，利用LLVM中的激进优化，包括Polly循环嵌套优化器，它针对两个后端代码生成器：一个用于可变精度FP算术协处理器的ISA，另一个用于MPFR多精度浮点库。我们以MPFR为目标的优化编译流程在连续执行Poly Bench和RAJAPerf套件时，分别比Boost编程接口的MPFR库性能高1.80×和1.67×，在OpenMP中的RAJAPerf，在8核（16线程）机器上的性能高7.62×。

[PDF] Efficient Implementation of NIST LWC ESTATE Algorithm Using OpenCL and Web Assembly for Secure Communication in Edge Computing Environment

BS Park, SC Seo – Sensors, 2021

在边缘计算服务中，边缘设备从一些嵌入式设备，如传感器、CCTV（闭路电视）等收集数据，并与应用服务器进行通信。由于边缘计算服务中的通信有很大一部分是在无线中进行的，因此需要对传输的数据进行适当的加密。另外，应用服务器(简称边缘设备)负责对边缘设备(简称终端设备)的大量数据进行加密或解密，因此，在服务器端和边缘设备端都需要对加密操作进行优化。实际上，数据的确凿性和完整性对安全通信至关重要。在本文中，我们提出了两个版本的安全软件，可以在边缘设备端和服务端使用，以实现边缘计算环境下它们之间的安全通信。我们的软件基本上是基于网络的应用，因为它的通用性，软件可以在任何网络浏览器上执行。我们的软件使用了ESTATE(Energy efficient and Single-state Tweakable block cipher based MAC-Then-Encrypt)算法，它是NIST LWC(National Institute of Standards and Technology LightWeight Cryptography)竞赛的一个有前途的候选算法，它不仅提供数据确证，而且提供数据认证。它还使用Web Assembly实现了ESTATE算法在边缘设备上的有效使用，并利用底层块密码的特性优化了算法的性能。我们应用了几种方法来有效地操作ESTATE算法。在ESTATE算法的操作过程中，我们使用条件语句对扩展调整值进行XOR。为了消除这个不必要的过程，我们采用了通过预计算来扩展和存储调整值的方法。对用Web Assembly实现的ESTATE算法和参考的C/C++ ESTATE算法的测量结果进行了比较。作为Web Assembly实现的ESTATE是在Web浏览器Chrome、FireFox和Microsoft Edge中测量的。为了提高服务器端的效率，我们使用了OpenCL，这是一个并行计算框架，以便同时处理多个数据。此外，在使用OpenCL实现时，使用条件语句会导致性能下降。为了消除性能下降，我们使用循环展开的方法消除了条件语句。此外，OpenCL的操作方式是将要加密的数据移动到本地内存，因为本地内存的运行速度很高。TweAES-128和TweAES-128-6与AES算法结构相同，可以应用之前研究的T表法。另外，对输入值16字节进行并行处理和计算。此外，由于它可能会受到缓存定时攻击，因此采用之前研究的T表洗牌方法可以安全地进行操作。我们的软件涵盖了边缘计算服务中从边缘设备到服务器的必要安全服务，并且由于它们都是基于Web的应用，因此可以轻松地用于各种类型的边缘计算设备。

Seamless Compiler Integration of Variable Precision Floating-Point Arithmetic

TT Jost, Y Durand, C Fabre, A Cohen, F P  rrot – 2021 IEEE/ACM International ..., 2021

处理器中的浮点(FP)单元一般仅限于支持IEEE 754标准定义的格式子集。因此，针对高性能计算的高效语言和优化编译器只支持IEEE标准类型，需要更高精度的应用涉及到繁琐的内存管理和对外部库的调用，导致代码臃肿，使程序的意图不明确。我们提出了C类型系统的扩展，可以表示通用的FP操作和格式，支持静态精度和动态可变精度。我们设计并实现了一个编译流程，弥补了该类型系统与低级FP指令

或软件库之间的抽象差距。我们通过基于LLVM的实现来证明我们解决方案的有效性，利用LLVM中的激进优化，包括Polly循环嵌套优化器，它针对两个后端代码生成器：一个用于可变精度FP算术协处理器的ISA，另一个用于MPFR多精度浮点库。我们以MPFR为目标的优化编译流程在连续执行Poly Bench和RAJAPerf套件时，分别比Boost编程接口的MPFR库性能高1.80×和1.67×，在OpenMP中的RAJAPerf，在8核（16线程）机器上的性能高7.62×。

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](#)

