RV与芯片评论.20210227.第9周(总第31期)

重点聚焦

CNRV ： "第一届RISC-V中国峰会 (From mp.weixin.qq.com 2021.02.27)"

> 2021年6月21日 – 2021年6月27日
> 上海市浦东新区上海科技大学

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）：
- PLCT开源进展：(Github，zhihu）：
- RT-Thread： （oschina）：
- 科技爱好者周刊： （yuque）：
- "RISC-V双周报2月10日-2月24日 (From mp.weixin.qq.com 2021.02.27)"

技术动态

"当IMG GPU遇上RISC-V (From www.eet-china.com 2021.02.27)"

> 赛昉科技将在2021年1月发布的星光人工智能（AI）单板计算机的后续量产版本上加入Imagination GPU，以添加强大、灵活的图形处理性能，使该单板计算机的功能更加完善。

"俄罗斯Kraftway开发自主SSD主控， 完善Elbrus生态系统 (From finance.sina.com.cn 2021.02.27)"

> Kraftway计划在未来几个月内生产1万块基于其K1942BK018控制器的固态硬盘，以争取将其使用在目标市场的PC上。有趣的是，除了基于ARM Cortex-R5的K1942BK018主控外，还有两款基于RISC-V的SSD和U盘主控是在俄罗斯的圣彼得堡开发设计的。

"openEuler RISC-V 背后的故事 (From my.oschina.net 2021.02.27)"

Linux动态

"Linux内核5.11发布,支持WiFi 6E、RTX Ampere GPU！ (From zhuanlan.zhihu.com 2021.02.27)"

> Linux5.11不是LTS（长期支持）版本，是2021年发布的第一个内核版本。较之以往有许多变化，包括对Wi-Fi 6的支持、更好的发挥AMD CPU性能、对Intel Iris Xe以及AMD Van Gogh APU的支持等。Linux Kernel 5.11对RISC-V CPU架构进行了重大改进和支持，包括对LiteX SoC控制器驱动程序的OpenRISC支持以及对SoC的常规支持。

一周问答

"如何评价乐鑫推出的RISC-V 内核 ESP32-C3芯片，是否是Wi-Fi MCU领域新的里程碑？（From www.zhihu.com 2021.02.27)"

"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 2021.02.27)"

"如何给riscv移植linux操作系统？（From www.zhihu.com 2021.02.27)"

社区动态

"万向区块链正式加入RISC-V基金会，联合生态合作伙伴发起成立“区块链行业工作组”(From news.tom.com 2021.02.27)"

> 2021年2月23日，在2021世界移动通信大会上，万向区块链、摩联科技正式宣布成为RISC-V基金会战略会员，并联合跃昉科技、赛昉科技、SiFive共同在RISC-V基金会发起成立“区块链行业工作组”（Blockchain SIG），从而进一步推动区块链技术在RISC-V社区的融合和可信数据底座的生态发展。

"Security + RISC-V ： 国产安全“芯”路径 ——“AIoT安全技术研讨会”(From mp.weixin.qq.com 2021.02.27)"

> 主办单位：珠海南方集成电路设计服务中心
> 主办单位：深圳市纽创信安科技开发有限公司
> 主办单位：芯来科技
> 协办单位：珠海新经济资源开发港有限责任公司
> 会议时间：2021年3月19日 星期五 14:00-17:30
> 会议地点：广东省珠海市高新区哈工大路1号经济港博士楼三楼国际会议厅

产业风云

"5G基站芯片变局：X86、Arm以及RISC-V阵营均想入局（From ee.ofweek.com 2021.02.27)"

> Open RAN在5G基站芯片市场正逐渐成为核心,X86、Arm以及RISC-V阵营均属意利用其架构作为入局的方式。而在政治和市场的共同驱使下,产生了强烈的变局。

"英伟达(NVDA.US)收购ARM 弊大于利？（From finance.eastmoney.com 2021.02.27)"

> RISC-V生态系统在过去几年中不断发展，对于物联网设备的多样化应用和低成本要求，RISC-V生态系统可能是一个非常有竞争力的候选人。无论如何，ARM将占据物联网市场最大份额的说法，与数据中心的说法一样，远未得到证实。

"小米关联公司入股芯片开发公司 或与AIoT战略有关 (From finance.eastmoney.com 2021.02.27)"

> 2月18日，长晶科技工商信息发生变更，新增湖北小米长江产业基金合伙企业(有限合伙)、OPPO广东移动通信有限公司等近十家投资人，同时，该公司注册资本也从原来的3.17亿元变更为3.57亿元，增幅达12.67%。
>
> 从2020年二季度以来，小米已先后投资了8家芯片企业，包括云英谷科技、比亚迪半导体、灿芯半导体等8家芯片公司，并主要集中在战略融资阶段。产品类型覆盖了显示芯片、集成电路(IC)及功率器件、RISC-V架构、ASIC芯片等。
>
> "小米、OPPO共同投资多家半导体企业 造芯之路任重道远 (From finance.sina.com.cn 2021.02.27)"

"因重仓特斯拉而实现惊人业绩的ARK Investment Management近日发布了2021年年度投资报告 (From caifuhao.eastmoney.com 2021.02.27)"

> 在今年的报告中，“牛市女皇”Cathie Wood带领她的ARK研究团队提出了15个宏大而前景广阔的投资主题。
>
> ARK认为ARM、RISC-V和图形处理器(GPU)可能会成为新的、强大的处理器，将从现在的0%的市场份额，在2030年扩大到71%的服务器市场份额，同时以45%的年增长率将营收扩大到合计190亿美元。

"一文读懂先进计算产业最新发展趋势 (From www.china-riscv.com 2021.02.27)"

> 展望2021年，器件、架构、软件呈现多路演进，自主演进架构生态加速形成，巨头争先抢滩布局，产业蕴含巨大市场潜力。与此同时，我国先进计算产业在开源、融合、适配、生态、技术短板等方面仍面临问题与挑战，有待尽快明确目标市场预期，强化生态迁移和适配，加速应用落地进程，与区域共同谋划推进部署。

"北京：发力建设区块链、量子等新型研发机构 (From www.bj.xinhuanet.com 2021.02.27)"

> 北京市重点支持建设了包括微芯院在内，北京量子信息科学研究院、北京脑科学与类脑研究中心、北京智源人工智能研究院等一批新型研发机构
>
> 基于RISC-V开源芯片指令集架构研发的芯片，它具有超高集成度、超低功耗和低成本等特点。它的技术完全自主可控。将助力国内首个自主可控区块链软硬件技术体系“长安链”的运算速度提至每秒10万笔以上，达到全球领先水平。

"芯来科技9.9元的嵌入式培训 (From zhuanlan.zhihu.com 2021.02.27)"

"乐鑫科技2021年限制性股票激励计划（草案）摘要公告 (From stock.stockstar.com 2021.02.27)"

"联发科投资的这家IP公司，将借道RISC-V挑战Arm? (From news.moore.ren 2021.02.27)"

> 晶心科是中国台湾唯一一家嵌入式处理器IP授权公司，可说是「台版Arm（安谋）」，但过去长年被Arm压制，难施拳脚。营收规模5.8亿，联发科持股13%、蔡明介兼任董事长的晶心科，这半年股价却暴涨约2倍，俨然成为联发科的小金鸡。

评论文集

"David Patterson：RISC-V开源的产学研之路该怎么走? (From www.riscv-mcu.com 2021.02.27)"

> RISC-V国际开源实验室（RIOS）、清华-伯克利深圳研究院与鹏城实验室共同举办了“第二届RISC-V国际开源论坛”。该论坛邀请了国内产学研界的专家学者，围绕RISC-V的人才培养、IP保护、开源供应链、开发板、高性能计算和生态进行了讨论。

"【2020-2021年度专题】RISC-V的“熵减”(From www.163.com 2021.02.27)"

> 在当下，国内RISC-V生态应抓住千载难逢的黄金发展期，加大研发和资金投入，实现配套的软硬件、工具链、OS等的均衡发展，形成整体的产业化结构，构建起符合国内“气候”的RISC-V生态。

"RISC-V 没你想象的那么好 (From wemp.app 2021.02.27)"

> ISA 的开放性对于用户来说并没有什么用
> ISA 碎片化对于通用的计算机和计算机上运行的操作系统来说则不是个好消息
> 许多有关 RISC-V 的吹捧则希望它能成为个人电脑或服务器的主力。然而这不太可能实现
> 开放性不会影响到用户（以控制根源信任），因为用户对于晶圆工厂并没有任何影响
> RISC-V 在 CPU 设计方面没有任何进步，甚至出现了一些诸如寻址模式错误等初级的错误
> 总的来看，RISC-V 会给希望节省经费的学术项目和嵌入式开发带来一场革命，但不太可能影响到用户和开发者。
> https://sporks.space/2021/02/01/risc-v-isnt-as-interesting-as-you-think/

"RISC-V 正在成为芯片世界中的 Linux (From www.qter.org 2021.02.27)"

> 参考链接：https://www.zdnet.com/article/risc-v-the-linux-of-the-chip-world-is-starting-to-produce-technological-breakthroughs/

"2020年RISC-V十大事件，逆流而上的的开源架构 (From bbs.21ic.com 2021.02.27)".

> 本文收录了10大与RISC-V紧密相关的大事，从一个年度盘点的角度来看这个不受约束的开源框架为何在逆境下仍有如此大的能量。

"深度：RISC-V指令集架构如何全球落地？ (From bbs.21ic.com 2021.02.27)"
"突破ARM与x86重围，RISC-V后发制人面临的挑战与机遇 (From bbs.21ic.com 2021.02.27)"
"X86 "将死"？RISC-V 正当立 (From www.sohu.com 2021.02.27)"
"RISC-V发展研究报告 (From www.rvmcu.com 2021.02.27)"

其他动态

项目推荐

"T-K-233/RISC-V-Single-Cycle-CPU (From githubmemory.com 2021.02.27)"

博文推荐

"【RISC-V MCU CH32V103测评】+ EXTI中断输入开关OLED (From bbs.eeworld.com.cn 2021.02.27)"
"RISC-V MCU CH32V103测评】UART串行通讯 (From bbs.eeworld.com.cn 2021.02.27)"
"【RISC-V MCU CH32V103测评】- 5：离开API进入Assembly不成，重返API (From bbs.eeworld.com.cn 2021.02.27)"

"Qemu ARM64 and RISCV 环境构建 (From zhuanlan.zhihu.com 2021.02.27)"
"RISC-V与DSA计算机架构 (From blog.csdn.net 2021.02.27)"
"RISC-V 工具链 & QEMU 虚拟机 (From johnwestonnull.github.io 2021.02.27)"
"嵌入式领域的Rust语言 (From zhuanlan.zhihu.com 2021.02.27)"

一周论文

架构

[PDF] Stream Floating: Enabling Proactive and Decentralized Cache Optimizations

Z Wang, J Weng, J Lowe-Power, J Gaur, T Nowatzki

> 随着多核系统规模和片上内存容量的不断增长，片上网络带宽和延迟成为问题瓶颈。正因为如此，数据传输的开销、一致性协议和替换策略变得越来越重要。不幸的是，即使是在结构良好的程序中，由于传统缓存层次结构的反应性和集中性，许多自然优化也难以实现，所有的请求都是由核心发起的短时、缓存行粒度的访问。例如，持久的访问模式可以从共享缓存中流转，而无需核心的请求。间接内存访问可以通过链式访问从缓存内发出的请求来进行，而不是不断返回核心。

Efficiently running SpMV on long vector architectures

C Gómez, F Mantovani, E Focht, M Casas - Proceedings of the 26th ACM SIGPLAN ..., 2021

> 稀疏矩阵-矢量乘法（SpMV）是并行数值应用的重要内核。SpMV显示出稀疏和不规则的数据访问，这使其矢量化变得复杂。这样的困难使得SpMV在利用SIMD并行的长向量ISA上运行时，经常会实验出非最佳的结果。在这种情况下，要想在新兴的长向量架构上实现高性能的SpMV执行，开发新的优化就成为根本。在本文中，我们通过提出几种新的SpMV优化，改进了最先进的SELL-C-σ稀疏矩阵格式。我们针对NEC Vector Engine等激进的长向量架构。通过结合几种优化，我们在考虑24个矩阵的异构集时，获得了比SELL-C-σ平均12%的改进。我们的优化提升了长向量架构的性能，因为它们暴露了高度的SIMD并行性。

安全

[PDF] Evolution of Embedded Platform Security Technologies: Past, Present & Future Challenges

F Siddiqui, S Sezer

> 近年来，智能嵌入式技术的扩散为新的服务和计算模式开辟了场所，提供了各种社会经济效益。这些智能技术通过共享和分析所产生的数据，催生了广泛的公共和私人应用。这包括智能家居、智能健康、智

能城市、自主车辆、智能电网和智能制造等。然而，这种数据共享带来好处和机会的同时，也带来了安全风险和挑战。这些技术的实现和原型设计需要一个以嵌入式平台形式广泛存在的计算硬件。这些平台的安全边界和攻击面依赖于其支持的安全和防御机制。本文旨在为安全研究界建立一个该领域的知识体系。它介绍了最先进的安全框架和架构，讨论了领先安全技术的架构缺陷和根源，而不是讨论漏洞和攻击。本文最后倡导安全设计平台方法，并对平台安全方法进行分类，以实现强大的嵌入式平台安全架构。

[PDF] LIRA-V: Lightweight Remote Attestation for Constrained RISC-V Devices

C Shepherd, K Markantonakis, GA Jaloyan – arXiv preprint arXiv:2102.08804, 2021

本文介绍了LIRA-V，这是一个轻量级系统，用于在使用RISC-V架构的受限设备之间执行远程认证。它提出使用RISCV物理内存保护（PMP）基元和只读内存来建立一个信任锚，用于远程认证和安全通道创建。此外，我们超越了现有的工作，提出了一种新型的双向认证协议，用于可信设备到设备的通信，并使用SCYTHER进行形式化的符号验证。我们介绍了使用现成的RISC-V微控制器设计、实现和评估LIRA-V，并展示了性能结果以证明其适用性。据我们所知，我们提出了第一个适合受限RISCV设备的远程验证机制，并应用于物联网（IoT）和网络物理系统（CPS）。

Top-down Physical Design of Soft Embedded FPGA Fabrics

P Mohan, O Atli, O Kibar, M Zackriya, L Pileggi, K Mai – The 2021 ACM/SIGDA ..., 2021

近年来，IC逆向工程和IC制造供应链安全已经发展成为设计者、系统集成商和终端客户的重大经济和安全威胁。许多现有的逻辑锁定和混淆技术已经表明，一旦攻击者通过逆向工程或通过不受信任的制造设施获得设计网表，就容易受到攻击。我们介绍了软嵌入式FPGA重编，这是一种硬件混淆方法，允许设计者用可合成的eFPGA结构替代设计中的安全关键IP块。这种方法完全隐藏了关键IP的逻辑和路由，并与标准ASIC流程兼容，便于集成和工艺移植。为了证明eFPGA节录，我们混淆了一个RISC-V控制路径和一个GPS P码发生器。我们还表明，修改后的网表对SAT攻击具有弹性，且VLSI开销适中。安全的RISC-V设计有1.89倍的面积和2.36倍的延迟开销，而GPS设计在工业22nm FinFET CMOS工艺上实现时有1.39倍的面积和可以忽略不计的延迟开销。

[PDF] Provably Secure Hardware Masking in the Transition-and Glitch-Robust Probing Model: Better Safe than Sorry

G Cassiers, FX Standaert – IACR Transactions on Cryptographic Hardware and ..., 2021

有许多掩蔽方案来保护加密操作的实现不受旁路攻击。通常的做法是在探测模型或其变体中分析这些方案的安全性，该变体考虑了物理上的effects，如故障和过渡。虽然这两种effects在实践中存在，并导致泄漏，在硬件中实现的掩蔽方案通常只分析针对故障的安全性。在这项工作中，我们通过证明硬件掩码方案对过渡的安全性的古老条件来填补这一空白，从而导致新的掩码方案的设计和现有掩码方案在存在过渡时的安全性证明。此外，我们还给出了类似的结果，在更强的模型中，故障和过渡的effects被结合起来。

[PDF] Improving Security Through Egalitarian Binary Recompilation

D Williams-King – 2021

在本论文中，我们试图弥补哪些程序转换在源码级是可能的，哪些程序转换在二进制级是可能的。虽然二进制程序通常被视为不透明的人工制品，但我们的二进制重编译器Egalito(ASPLOS 2020)使用户能够在现有系统上解析和修改剥离的二进制程序。我们的二进制重组技术对反汇编中的错误并不健壮，但通过精确的分析，提供了近乎零的转换开销。我们用Egalito写了几个示范性的安全工具，包括代码随机化、控制流完整性、retpoline插入和一个模糊后端。我们还编写了Nibbler（ACSAC 2019，DTRAP 2020），它可以检测未使用的代码并将其删除。包括 Nibbler 在内的许多功能都可以与其他防御措施相结合，从而实现倍增式的更强或更有效的加固。通过我们的重新编译器，本论文的一个首要主题是我们对可部署软件转换的关注。Egalito已经被合作者在数以万计的Debian程序和库中进行了测试。我们在二进制安全的背景下创造了这个术语egalitarian。简单地说，一个平等主义的分析或安全机制是一个可以对自身进行操作的机制（并且通常因此更可部署）。作为这一理念的一个证明，我们创建了一个强大的、可部署的防御代码重用攻击的机制。Shuffler（OSDI 2016）随机化函数地址，每隔几毫秒定期移动函数。这使得攻击者的工作变得非常困难，尤其是当他们位于跨网络的情况下（这就需要ping时间）--JIT-ROP攻击需要2.3到378秒才能完成[1，2]。Shuffler是平等的，同时防御自己的代码和目标代码，Shuffler实际上是在洗牌自己。我们希望我们的可部署的、平等主义的二进制防御能够让其他人在最先进的基础上进行改进，并将二进制描绘成比过去更有可塑性的样子。

加速

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

S Sordillo, A Cheikh, A Mastrandrea, F Menichelli... - Electronics, 2021

相对于云计算而言，云边缘连续体的计算依赖于物联网(IoT)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，甚至在同一应用中也是如此。面向向量的硬件加速已经重新获得了支持卷积网络或分类算法等人工智能（AI）应用的兴趣。我们提出了一个全面的调查的性能和功率效率可实现的configurable矢量加速子系统，获得的证据表明，所提出的微架构的高潜力和硬件定制的优势，在完全透明的软件程序。

ZigZag: Enlarging Joint Architecture-Mapping Design Space Exploration for DNN Accelerators

L Mei, P Houshmand, V Jain, S Giraldo, M Verhelst - IEEE Transactions on Computers, 2021

构建高效的嵌入式深度学习系统需要DNN算法、硬件以及算法与硬件之间的映射进行紧密的联合设计。然而，由于联合设计空间较大，通过物理实现寻找最优解变得不可行。为了解决这个问题，最近出现了一些设计空间探索(DSE)框架，但它们要么运行时间长，要么探索空间有限。本工作介绍了ZigZag，一个快速的DNN加速器架构映射的DSE框架。ZigZag对常见的DSE进行了扩展，加入了不均匀映射机会和智能映射搜索策略。不均匀映射将操作数(W/I/O)、内存层次结构和映射(时间/空间)解耦，为DSE开辟了一个全新的空间，从而与SotAs相比找到更好的设计点。为此，ZigZag采用了增强的嵌套for-loop格式作为统一的表示方式，将算法、加速器以及算法与加速器之间的映射进行整合。ZigZag由三个关键部分组成。1)一个分析能耗性能区间的硬件成本估算器，2)两个支持空间/时间均匀/不均匀映射搜索的映射搜索引擎，3)一个自动探索宽广内存层次设计空间的架构生成器。对比已发表的作品、内部加速器和

现有的DSE框架的基准实验，以及三个案例研究，显示了ZigZag的可靠性和能力。由于ZigZag的不均匀映射能力，与SotAs相比，发现高达64%的解决方案更加节能。

应用

[PDF] Mixed-Precision Quantization and Parallel Implementation of Multispectral Riemannian Classification for Brain--Machine Interfaces

X Wang, T Schneider, M Hersche, L Cavigelli, L Benini – arXiv preprint arXiv ..., 2021

有了运动图像(MI)的脑机接口(BMIs)，我们只需思考执行一个运动动作就可以控制机器。实际使用案例需要一个可穿戴解决方案，其中大脑信号的分类是在传感器附近使用嵌入在节能微控制器单元（MCU）上的机器学习模型在本地完成的，以确保隐私、用户舒适度和长期使用。在这项工作中，我们提供了关于嵌入式BMI解决方案的准确性-成本权衡的实际见解。我们提出的多谱黎曼分类器在4类MI任务上达到了75.1%的准确率。我们通过将模型量化为混合精度表示，进一步降低了模型的规模，最小精度损失为1%，这比目前最先进的嵌入式卷积神经网络的精度仍高出3.2%。我们在低功耗MCU上实现该模型，并行处理单元仅需33.39 ms，每次分类消耗1.304 mJ。

[PDF] A Compact Hardware Implementation of CCA-Secure Key Exchange Mechanism CRYSTALS-KYBER on FPGA

Y Xing, S Li – IACR Transactions on Cryptographic Hardware and ..., 2021

后量子密码系统应该在强大的量子计算机出现之前做好准备，以确保我们日常生活中的信息安全。2016年美国国家标准与技术研究所(NIST)发起了后量子标准化竞赛，已经有很多作品集中在different平台上对这些候选协议进行评估，主要是纯软件或通过软硬件协同设计方法。随着比赛进行到2020年7月的第三轮，只剩下7个候选者和8个候补候选者，应该考虑更多的专用和规格化的硬件设计来说明某个协议的内在属性，并实现更好的性能。为此，我们在FPGA平台上提出了一个独立的硬件设计CRYSTALS-KYBER，一个基于模块学习与错误(MLWE)的密钥交换机制(KEM)协议。通过对采样和数理变换(NTT)相关计算的精心调度，用有限的硬件资源实现了不错的性能。详细演示了Encode/Decode和调整后的Fujisaki-Okamoto变换的实现方式。还给出了关于最小化内存占用的分析。总之，我们在最小的Xilinx Artix-7器件上实现了自适应选择密码攻击(CCA)的安全Kyber，所有可选择的模块维度为k。我们的设计计算密钥生成、封装(加密)和解密(解密和再加密)阶段，当k=2时，需要3768/5079/6668个周期，当k=3时，需要6316/7925/10049个周期，当k=4时，需要9380/11321/13908个周期，消耗7412/6785个LUT、4644/3981个FF、2126/1899个片子、2/2个DSP和3/3个BRAM，在服务器/客户端以6.2/6.0 ns的关键路径延迟，在很大程度上优于相应的基于高电平综合(HLS)的设计或软硬件协同设计。

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