RV与芯片评论.20210213.第7周(总第29期)

[PDF] Compact Native Code Generation for Dynamic Languages on Micro-core Architectures

一周专利

Reliable communications using a point to point protocol

相关周报

- semi engineering Week In Review:
  - Blog Review：
  - Design, Low Power：
  - Manufacturing, Test：
  - Auto, Security, Pervasive Computing：
- IoT News：（Site）：Feb. 12, 2021
- OSDT Weekly：(zhihu，Github)：2021-02-10 第084期
- 泰晓咨询：（Site）：
- PLCT开源进展：(Github，zhihu)：
- RT-Thread：（oschina）：
- 科技爱好者周刊：（yuque）：

技术动态

"FreeBSD 13.0 Beta 1发布 正式版预估3月21日发布 (From www.cnbeta.com 2021.02.19)"

> FreeBSD 13.0-RELEASE 目标在今年 3 月底发布，而根据路线图本周末推出了 FreeBSD 13.0-BETA1 版本。在候选版本发布之前，预估每周都会发布 Beta 版本更新。如果一切顺利的话，FreeBSD 13.0 将在 3 月 21 日左右正式发布。

社区动态

"阿里云天池×平头哥芯片开放社区“RISC-V应用创新大赛”正式开赛！ (From www.geekpark.net 2021.02.19)"

产业风云

"乐鑫科技CEO张瑞安发表员工信：为建立世界上最好的AIoT公司而奋斗 (From www.sohu.com 2021.02.19)"

"芯片框架结构RISCV新权力赶快兴起睿思芯科产物本年终量产 (From www.caijingshuju.com 2021.02.19)"

"逆天而行？这家公司放弃RISC-V，选择OpenPower (From xueqiu.com 2021.02.19)"

> LibreSOC一直在设计100%开源的混合CPU / GPU。该项目最初的想法是旨在成为RISC-V Vulkan加速器，当时该项目被称为Libre RISC-V。但是他们最终放弃了RISC-V，选择基于OpenPOWER ISA的设计，无需使用NDA和其他组织问题
> 作者：张竞扬

"深耕RISC-V架构，中科蓝讯蓝牙音频SoC 13款应用案例汇总 (From www.52audio.com 2021.02.19)"

> 中科蓝讯是国内RISC-V架构芯片出货量最大的IC设计公司之一

"50家中国IC设计初创公司调查统计汇编 (From www.eet-china.com 2021.02.19)"

> Aspencore《电子工程专辑》分析师团队对中国本土的芯片设计初创公司进行了第一手调查和网络汇编整理，从众多初创公司中挑选50家，分别从核心技术、代表产品、典型应用场景等多个维度进行了分析。

评论文集

"什么趋势最有可能在2021年主导智能科技行业？ (From article.cechina.cn 2021.02.19)"

"【牛年大吉】十大关键词总结电子行业过去这一年 (From www.eet-china.com 2021.02.19)"

其他动态

博文推荐

"【RISC-V MCU CH32V103测评】驱动OLED (From bbs.eeworld.com.cn 2021.02.19)"

"【RISC-V MCU CH32V103测评】RTC电子时钟 (From bbs.eeworld.com.cn 2021.02.19)"

"RISC-V MCU CH32V103测评】IIC硬件测试 [(From bbs.eeworld.com.cn 2021.02.19)"

"【RISC-V MCU CH32V103测评】IIC硬件测试(二) (From bbs.eeworld.com.cn 2021.02.19)"

"【RISC-V MCU CH32V103测评】+ 硬件SPI驱动OLED显示DHT11温湿度 (From bbs.eeworld.com.cn 2021.02.19)"

"RISC-V GD32VF103 开发笔记 – (1) 创建模板程序 (From zhuanlan.zhihu.com 2021.02.19)"

"RISC-V GD32VF103 开发笔记 – (5.1) TIMER – 定时 Interrupt (From zhuanlan.zhihu.com 2021.02.19)"

"RISC-V GD32VF103 开发笔记 – (5.2) TIMER – 输出 PWM 驱动舵机 (From zhuanlan.zhihu.com 2021.02.19)"

一周论文

架构

[PDF] Microarchitectural Timing Channels and their Prevention on an Open-Source 64-bit RISC-V Core

N Wistoff, M Schneider, FK Gürkaynak, L Benini...

> 微架构时序通道利用对有限硬件资源的竞争导致的事件时序变化，违反操作系统的安全策略而泄露信息。这种通道在简单的内序RISC-V核上也存在，我们在开源的RV64GC Ariane核上进行了演示。最近在seL4微内核中提出并实现的时间保护，旨在防止定时通道，但依赖于微架构状态的受控重置。利用Ariane，我们表明，执行这种复位的软件技术是不够的，而且效率很低。我们证明，增加一个单一的刷新指令就足以关闭所有五个评估通道，而硬件成本可以忽略不计，同时只需要对软件堆栈进行轻微修改。

[PDF] EVEREST: A design environment for extreme-scale big data analytics on heterogeneous platforms

C Pilato, S Bohm, F Brocheton, J Castrillon, R Cevasco...

> 高性能大数据分析(HPDA)应用的特点是大量的分布式和异构数据，需要高效的计算来进行知识提取和决策。设计师们正朝着将HPC、云和物联网解决方案与人工智能（AI）紧密结合的计算系统的方向发展。将应用和数据需求与底层硬件的特性相匹配是提高预测能力的关键因素，这得益于高性能和更好地利用资源。

模块

[PDF] Design and implementation of testable fault-tolerant RISC-V system

M Rodan - 2020

> 本论文旨在研究和实现一种基于RISC-V的容错节能型片上系统（SoC）。该SoC的主要特点是低功耗片上嵌入式存储器的可测试性和可靠性。设计并实现了片上存储器的内置自检（BIST），以按需运行诊断测试，检测存储器的制造错误。它结合了三种不同的算法来测试常见的存储器制造故障。使用纠错码单元(ECC)检测和纠正运行时的软错误，它最多可以纠正两个错误。ECC与RISC-V内核和存储器集成在一起，提高了SoC在低电压下的容错能力。随着电源电压的降低，软错误的概率增加，ECC元件的重要性也随之增加。当电源电压从1.2V降至0.8V时，模拟整个系统的功耗节省高达46%。加入ECC元件后，核心面积增加了3.5%。集成内存内置自检又使核心面积增加了24.4%。

[PDF] CASTLE: Architecting Assured System-on-Chip Firmware Integrity

S Ray, APD Nath, K Raj, S Bhunia

> 现代片上系统(SoC)设计包括大量执行自定义固件的嵌入式微控制器。固件提供了更新安全功能的灵活性，即它可以根据新出现的安全威胁、错误或不断变化的需求进行补丁或内嵌式更新。不幸的是，目前

的固件更新机制是复杂的，手动的，而且容易出错。在本文中，我们提出了CASTLE，一个架构框架，以实现系统化和有保证的SoC固件更新。CASTLE的主要工作原理是在SoC中建立一个集中的专用IP，负责接收、验证和安装补丁。该架构与片外固件验证平台合作，例如，基于云的服务，用于验证拟议的补丁，并识别SoC中其他常驻固件的兼容性限制。其结果是一个全面的基础设施，可以跨架构、供应商和服务提供商无缝工作，同时满足部署和可用性要求。我们展示了所提出的框架在解决现有的固件补丁机制的功能和安全问题上的应用，包括固件不兼容、验证不足以及检查时间与使用时间（TOCTOU）的限制。

General hardware multicasting for fine-grained message-passing architectures

M Naylor, SW Moore, D Thomas, JR Beaumont... - 2021

出于能效和可扩展性的考虑，多核架构越来越倾向于采用消息传递或分区全局地址空间(PGAS)，而不是缓存一致性。然而，在没有缓存一致性的情况下，可能缺乏对一对多通信模式的硬件支持，而这种通信模式在某些应用领域很普遍。为了解决这个问题，我们提出了用于机架规模多核系统中多播通信的新硬件基元。这些基元可保证向主机托管和分布式目的地的交付，并可精确捕获大型非结构化通信模式。因此，在任何拓扑结构中连接的任何数量的软件任务之间的可靠组播传输都可以完全卸载到硬件上。我们在一个由50K RISC-V线程组成的研究平台中实现了新的基元，该平台分布在48个FPGA上，并在一系列使用高级顶点中心编程模型表达的应用中展示了显著的性能优势。

加速

Design Space Exploration for Heterogenous SoC Integrated with Matrix Accelerator

J Wei, L Zhang, ZG Yu, D Liu - 2020 IEEE 2nd International Conference on Circuits ..., 2020

加速器作为一种提高计算能力的有效方法，在SoC系统中得到了广泛的应用。CPU与加速器的耦合方式有很多。本文设计了一种矩阵-矩阵乘法加速器，并将加速器与RISC-V CPU以独立加速器和指令加速器两种不同的形式进行耦合。然后我们对独立加速器和新型指令加速器的性能进行了评估。矩阵独立加速器与Rocket CPU相比，实现了高达19.6倍的加速。而矩阵指令加速器对Rocket CPU实现了高达44.5倍的加速。指令加速器比独立加速器快2.26倍。

Efficient Implementation of SHA-3 Hash Function on 8-Bit AVR-Based Sensor Nodes

YB Kim, H Choi, SC Seo - International Conference on Information Security and ..., 2020

Keccak算法在2015年被NIST选为标准的SHA-3散列算法，以取代目前使用的SHA-2算法。尽管SHA-3与SHA-2相比安全性有所提高，但其在软件实现上的低性能限制了它的广泛应用。在本文中，我们提出了一种优化的SHA-3在8位AVR微控制器（MCU）上的实现方法，该微控制器主要用于WSN中的传感器设备。到目前为止，尽管SHA-3的安全性非常重要，但只有少数研究对其进行优化。此外，在8位AVR MCU上优化哈希函数，尤其是SHA-3，是非常具有挑战性的。这是因为SHA-3的内部状态是1,600位，比AES、ARIA等对称算法（通常是128位）的内部状态大得多。换句话说，在AVR MCU的寄

存器上很难容纳SHA-3的全部内部状态，在计算过程中会产生大量的内存访问。因此，我们分析了SHA-3算法的结构，发现SHA-3中每个进程的内部状态的每个通道都可以独立执行。利用这一事实，我们提出了一种优化方法，可以有效地减少对内部状态的内存访问次数。通过这种优化方法，使内存访问次数最小化，我们实现的SHA3-256与之前在8位AVR单片机上的最佳工作相比，在散列500字节信息时，性能提高了约25.0%。据我们所知，我们的软件是迄今为止AVR平台上最快的SHA-3实现。此外，所提出的优化方法可以很容易地扩展到其他嵌入式MCU，如16位MSP430、32位RISC-V和基于ARM的MCU。

PIM-Align: A Processing-in-Memory Architecture for FM-Index Search Algorithm

XQ Li, GM Tan, NH Sun - Journal of Computer Science and Technology, 2021

基因组序列排列是基因组分析中最关键、最耗时的步骤。排列算法一般遵循种子和扩展模型。在现场可编程门阵列(FPGA)、特定应用集成电路(ASIC)和图形处理单元(GPU)等以计算为中心的架构中，已经对序列配准的扩展阶段的加速进行了很好的探索(如Smith-Waterman算法)。与扩展阶段相比，播种阶段更为关键和必要。然而，播种阶段受制于内存，即细粒度的随机内存访问，传统系统的并行性有限。在本文中，我们认为内存中处理(PIM)概念可能是解决这些问题的可行方案。本文介绍了 "PIM-Align"--应用驱动的序列对齐的近数据处理架构。为了利用3D堆栈动态随机存取存储器(DRAM)技术实现内存容量比例性能，我们提出了不同内存分区之间的轻量级消息机制，以及针对序列对齐的内存访问模式的专用硬件预取器。我们的评估表明，与现有的最佳ASIC实现和运行在32线程CPU上的软件相比，所提出的架构可以分别实现20倍和1 820倍的速度提升。

Evaluation of On-Chip Accelerator Performance Based on RocketChip

J Wei, ZG Yu, D Liu - 2020 IEEE 2nd International Conference on Circuits ..., 2020

在计算任务密集或算法复杂的人工智能和信号处理领域，研究人员通常会设计CPU+加速器的异构SoC，以提高系统的效率。在异构SoC中，加速器通常作为协处理器或通道加速器。本文为了研究加速器与CPU之间的耦合关系，分别设计了协处理器的CORDIC算法加速器、CORIDC通道加速器、协处理器的矢量点积加速器和基于RISC-V的开源项目-RocketChip的通道加速器。通过Modelsim对各加速器的加速效果进行仿真。经验证，CORDIC算法协处理器对CPU的加速比约为151倍，CORDIC通道加速器的加速比约为103倍。矢量长度越长，矢量点积加速器的加速效果越显著，矢量点积通道加速器的加速效果明显优于矢量点积协处理器。我们发现，协处理器的性能受到数据访问速度的限制。此外，当协处理器与CPU耦合不紧密时，会带来额外的时间开销。

安全

Nonlinear Code-based Low-Overhead Fine-Grained Control Flow Checking

G Dar, G Dinatale, O Keren - IEEE Transactions on Computers, 2021

一种基于硬件的控制流监测技术能够检测到在处理器上执行的控制流和指令流中的错误。然而，正如在最近的出版物中所显示的那样，这些技术无法检测到基本块中对指令流进行的精心调整的恶意操作。本文提出了一种能够应对这一弱点的非线性编码器和检查器。它是一种基于MAC的控制流检查器，它的优

点是可以处理长度可变的基本块，可以检测到每一个错误，并实时执行计算。该架构可以很容易地进行修改，以支持不同的签名大小和错误屏蔽概率。

[PDF] uTango: an open-source TEE for the Internet of Things

D Oliveira, T Gomes, S Pinto – arXiv preprint arXiv:2102.03625, 2021

安全是物联网（IoT）的主要挑战之一。物联网设备主要由低成本微控制器(MCU)驱动，这些微控制器通常缺乏基本的硬件安全机制，无法将安全关键型应用与不太关键的组件分开。最近，Arm公司开始发布采用TrustZone技术(即TrustZone-M)增强的Cortex-M MCU，这是一种旨在为物联网设备提供强大保护的全系统安全解决方案。依靠TrustZone硬件的可信执行环境(TEE)一直被视为保护移动设备安全的避风港。然而，在过去的几年里，人们花费了相当大的精力来揭开数百个漏洞，并提出了一系列相关的防御技术来解决几个问题。当建立在TrustZone-M上的新的TEE解决方案开始兴起时，从研究界收集到的经验似乎还不够，因为这些新系统正陷入过去的似曾相识的陷阱中。在本文中，我们提出了UTANGO，现代物联网设备的第一个多世界TEE。UTANGO提出了一种新颖的架构，旨在解决目前影响TrustZone(-M)辅助TEE的主要架构缺陷。特别是，我们利用双重世界实现所使用的相同的TrustZone硬件基元，在正常世界中创建多个同样安全的执行环境。我们通过在真实的TrustZone-M硬件平台（即Arm Musca-B1）上进行广泛的评估来展示UTANGO的优势。UTANGO将开源并在GitHub上免费提供，希望能让学术界和工业界参与到保护可预见的万亿物联网设备的安全中来。

[PDF] Sovereign Smartphone: To Enjoy Freedom We Have to Control Our Phones

F Groschupp, M Schneider, I Puddu, S Shinde... – arXiv preprint arXiv ..., 2021

大多数智能手机不是运行iOS就是Android操作系统。这就形成了两个截然不同的生态系统，主要由苹果和谷歌控制--它们决定了哪些应用程序可以运行，如何运行，以及它们可以访问什么样的手机资源。除了安卓系统中的一些例外，不同的手机制造商可能有影响力，用户、开发者和政府几乎没有选择。具体来说，用户需要将自己的安全和隐私委托给操作系统厂商，并接受他们施加的功能限制。考虑到Android和iOS的广泛使用，立即离开这些生态系统是不切实际的，除非在小众应用领域。在这项工作中，我们提请大家注意这个问题的严重性，以及为什么这是一种不可取的情况。作为一种替代方案，我们提倡开发一种新的智能手机架构，在保持与现有丰富的智能手机生态系统兼容的同时，将控制权安全地转移回用户手中。我们基于ARM和RISC-V可信执行环境的进展，提出并分析了这样一种设计。

[PDF] Vertical IP Protection of the Next-Generation Devices: Quo Vadis?

S Rai, S Garg, C Pilato, V Herdt, E Moussavi...

随着5G和物联网应用的出现，由于各种子系统之间的大量相互通信所造成的迫在眉睫的风险，对硬件安全的要求也越来越高。因此，集成电路的安全漏洞对于电子系统的制造商和用户来说都是高风险。特别是在知识产权保护领域，迫切需要在所有抽象层次上设计安全措施，以便我们能够领先于任何形式的对抗性攻击。从系统级到设备级的安全措施，从讨论各种攻击方法如逆向工程、硬件木马植入，到提出新时代的保护措施如多值逻辑锁、安全信息流跟踪等，多角度地介绍知识产权保护措施。本专场将全面介绍目前最先进的措施，以及我们对下一代电路和系统的准备情况。

Custom Instruction Support for Modular Defense Against Side-Channel and Fault Attacks

K Heydemann, P Schaumont – Constructive Side-Channel Analysis and Secure ...

> 针对主动和被动对手的软件对抗措施的设计是一个具有挑战性的问题，近年来许多作者都在解决这个问题。所提出的解决方案采用了一个理论基础（如泄漏模型），但往往没有提供具体的参考实现来验证这个基础。为了对这一工作的实验维度做出贡献，我们提出了一个名为SKIVA的定制化处理器，支持针对广泛的实现攻击设计对策的实验。基于位片编程和文献中的最新进展，SKIVA提供了一个灵活和模块化的组合，以对抗基于功率和基于时序的侧通道泄漏和故障注入的对策。侧通道保护和故障保护的多种配置使程序员能够为每个位片选择所需的份额数和所需的冗余级别。通过自定义指令集扩展，硬件中支持重复性和安全敏感操作。新指令支持位分片、秘密份额生成、冗余逻辑计算和故障检测。我们从侧通道分析和故障注入的角度演示和分析了多个版本的AES，此外还对受保护的设计进行了详细的性能评估。据我们所知，这是第一个经过验证的面向比特片的模块化对策的端到端实现。

Processor Anchor to Increase the Robustness Against Fault Injection and Cyber Attacks

B Pecatte – Constructive Side-Channel Analysis and Secure ...

> 软件安全方面的一个重大进步是使用强大的处理器，它可以帮助代码开发人员挫败网络和物理攻击。本文介绍了一种基于硬件的解决方案，它通过检查任何微控制器上执行代码的完整性来提高安全性。与其他控制流完整性(CFI)保护不同，该解决方案不需要修改CPU流水线，而是依靠监控处理器与其指令缓存之间的接口。执行流和指令序列(称为基本块)的完整性由硬件通过预先计算的元数据进行检查。另一个模块专门用来加快对这些元数据的访问。本文显示了该方案的有效性，因为以使用内存空间与代码一起存储元数据为代价，对执行时间的影响平均高达21%。

敏捷开发

[PDF] Compact Native Code Generation for Dynamic Languages on Micro-core Architectures

M Jamieson, N Brown – arXiv preprint arXiv:2102.02109, 2021

> 微核架构将许多简单、低内存、低功耗的CPU内核组合到一个芯片上。这种技术有可能提供显著的性能和低功耗，不仅在嵌入式、边缘和物联网用途中具有极大的兴趣，而且有可能作为数据中心工作负载的加速器。由于这种CPU的限制性，这些架构传统上在编程方面具有挑战性，特别是由于非常受限的内存量（通常在32KB左右）和技术的特殊性。然而，最近，诸如Python这样的动态语言已经被移植到一些微内核上，但这些语言通常是以解释器的形式提供的，具有相关的性能限制。
> 针对动态语言的性能、无限制的代码大小、架构间的可移植性以及保持程序员生产力优势这四个目标，由于内存有限，动态语言编译器采用的经典技术，如即时编译（JIT）根本不可行。在本文中，我们描述了一种针对微核架构上动态语言的编译方法的构建，该方法旨在满足这四个目标，并以Python为载体，探索其在替代现有微核解释器的应用。我们的实验主要集中在性能、架构可移植性、最小内存大小和程

> 序员生产力等指标上，将我们的方法与编写原生C代码的方法进行比较。这项工作的成果是确定了一系列技术，这些技术不仅适用于编译Python代码，而且适用于微核上的各种动态语言。

一周专利

Reliable communications using a point to point protocol

P Sindhu, D Goel, SR Vegesna, A Zhou, S Kumar… – US Patent App. 17/063,210, 2021
US20210021696A1 – Reliable communications using a point to point protocol – Google Patents. Reliable communications using a point to point protocol. Download PDF Info. Publication number US20210021696A1. US20210021696A1 …

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