

RV与芯片评论.20210220.第8周(总第30期)

[相关周报](#)

[技术动态](#)

[一周问答](#)

[博文推荐](#)

[一周论文](#)

[安全](#)

[Library Implementation and Performance Analysis of GlobalPlatform TEE Internal API for Intel SGX an...](#)

[\[PDF\] Comparison of RISC-V and transport triggered architectures for a post-quantum](#)

[\[PDF\] Exploiting the Back-Gate Biasing Technique as a Countermeasure Against Power Analysis Atta...](#)

[\[PDF\] Hardware Information Flow Tracking](#)

[\[HTML\] Cryptographic Software IP Protection without Compromising Performance or Timing Side-c...](#)

[Towards Linux based safety systems—A statistical approach for software execution path coverage](#)

[SeRoT: A Secure Runtime System on Trusted Execution Environments](#)

[架构](#)

[\[PDF\] Vectorizing Posit Operations on RISC-V for faster Deep Neural Networks: Experiments and Co...](#)

[Nonconventional Computer Arithmetic Circuits, Systems and Applications](#)

[EDA](#)


[\[PDF\] Machine Learning for Electronic Design Automation: A Survey](#)

[Standard-compliant parallel SystemC simulation of loosely-timed transaction level models: From bar...](#)

[一周专利](#)

[CONFIGURABLE PROCESSOR FOR IMPLEMENTING CONVOLUTION NEURAL NETWORKS](#)

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](#)): 2021-02-17 第085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

"[全球首个5Ghz频率的RISC-V芯片的新进展](#) (From [www.sohu.com](#) 2021.02.20)"

日前, Micro Magic公司宣布, 其超低功耗64位RISC-V核心为1GHz消耗仅为10mW。Micro Magic的设计技术允许其5GHz处理器在低电压下运行以节省功率, 同时仍可实现高性能。通过将工作电压降低到350mV, Micro Magic的64位RISC-V内核以1GHz运行, 并能够在16nm FinFET工艺中达到2500 Coremarks。结果是打破了250,000 Coremarks / Watt的记录。

一周问答

"[如何看待阿里自研RISC-V 芯片成功运行Android10?](#) (From [www.zhihu.com](#) 2021.02.20)"

博文推荐

"[【RISC-V MCU CH32V103测评】BH1750光强检测](#) (From [bbs.eeworld.com.cn](#) 2021.02.20)"

"[【RISC-V MCU CH32V103测评】+ DMA传输ADC转换结果](#) (From [bbs.eeworld.com.cn](#) 2021.02.20)"

[【读书笔记】RISC存储程序机的电路设计 \(1\)](#)

[【读书笔记】RISC存储程序机的电路设计 \(2\)](#)

[【读书笔记】RISC存储程序机的电路设计 \(3\)](#)

[【读书笔记】RISC存储程序机的电路设计 \(4\)](#)

[【读书笔记】RISC存储程序机的电路设计 \(5\)](#)

[【读书笔记】RISC存储程序机的电路设计 \(6\)](#)

"[macOS 下搭建环境、编译运行 6.S081 课程的 mit-pdos/xv6-riscv 系统](#) (From [blog.csdn.net](#) 2021.02.20)"

"[RISC-V 伪指令tail](#) (From [zhuanlan.zhihu.com](#) 2021.02.20)"

"[用 Rust 写操作系统 | 清华 rCore OS 教程介绍](#) (From [zhuanlan.zhihu.com](#) 2021.02.20)"

"[lattice CrosslinkNx LIFCL-40应用连载4-RISC-V处理器访问I2CFIFO](#) (From [mbb.eet-china.com](#) 2021.02.20)"

一周论文

安全

[Library Implementation and Performance Analysis of GlobalPlatform TEE Internal API for Intel SGX and RISC-V Keystone](#)

K Suzuki, K Nakajima, T Oi, A Tsukamoto – ... Conference on Trust, Security and Privacy ..., 2020

可信执行环境(TEE)成为当前CPU上流行的安全扩展(如Arm TrustZone、Intel SGX和RISC-V Keystone), 但每个TEE都有其原有的SDK, 无法保持软件的可移植性。GlobalPlatform (GP) 定义了名为 "TEE内部API" 的通用API, 智能手机主要使用这些API。另外, GP API的实现是以Trusted OS为前提的, 部分TEE不能直接实现。另外, 有些TEE提供了Enclave定义语言(EDL), 用于普通应用和可信应用之间的安全通信, 而GP API不承担这个功能。为了解决这些问题, 我们提出在每个TEE SDK上实现GP TEE内部API的库。我们选择了架构依赖型或独立型(如安全存储和时间)的GP API。架构无关的API需要Linux的帮助, 或者可以通过CPU特定指令有效实现。它们在每个架构上的实现都是尽可能的相同。该库是为每个EDL设计的(例如, Intel SGX上的 "edger8r", RISC-V上的 "keyedge"), 并保持通信的安全性。该库在Intel SGX和RISC-V Keystone上实现。对性能进行了测量, 并与在Arm TrustZone上实现的可信操作系统风格的OP-TEE进行了比较。通过比较可以看出每个实现的特点。

[\[PDF\] Comparison of RISC-V and transport triggered architectures for a post-quantum](#)

L AKCAY, ÖRS Berna

密码学是安全系统的基本现象之一。然而, 一些被广泛使用的公钥密码学算法可以通过使用量子计算机来破解。因此, 近年来提出了许多后量子密码学算法来处理这一问题。NTRU是这些量子安全算法中最重要的一种。除了加密算法的重要性外, 实现这些算法的架构也是必不可少的。在这项研究中, 我们开发了一个NTRU公钥密码系统的应用, 并设计了几种处理器来比较它们在许多方面的性能。在这项工作中, 我们解决了两种不同的架构。选择RISC-V是因为它是经典RISC架构的最新版本。更倾向于传输触发架构(TTA), 它具有高层次的定制化和可扩展性。

[\[PDF\] Exploiting the Back-Gate Biasing Technique as a Countermeasure Against Power Analysis Attacks](#)

BA Dao, TT Hoang, AT Le, A Tsukamoto, K Suzuki... – IEEE Access, 2021

完全耗尽绝缘体上硅(FD-SOI)技术以其反向栅偏置电压可控性而闻名。它允许使用FD-SOI技术制作的器件, 根据所需的应用, 通过适当的后栅偏差, 优化为低功耗或高性能。本文提出了利用后门偏置技术对抗功率分析攻击的新对策。讨论了理论解释, 并进行了针对65 nm STOB 32位RISC-V微控制器AES-128加密的真实差分功率分析(DPA)攻击, 以验证所提出的思想。实验结果表明, 与无偏置相比, 采用我们的第一个方案, 即使用前向后门偏置, 不仅提高了测试设备的性能, 而且增强了其对DPA攻击的抵抗能力。此外, 当反向后门偏置时, 对DPA攻击的漏洞保持不变, 以实现低功耗。当将反向栅偏压技术与较低的电源电压相结合时, DPA电阻甚至更为重要。在最好的情况下, 成功检索密钥所需的功率

跟踪数增加了14.5倍。当目标微控制器的后门偏置是动态随机的时，甚至可以获得更好的DPA抵抗，正如我们的第二个随机动态后门偏置(RDBB)建议的那样。当应用RDBB时，成功检索密钥所需的功率跟踪数显著增加了33.4倍。

[PDF] [Hardware Information Flow Tracking](#)

WEI HU, A ARDESHIRICHAM, R KASTNER

信息流跟踪(IFT)是一种基本的计算机安全技术，用于了解信息如何通过计算系统移动。硬件IFT技术专门针对与硬件电路的设计、验证、测试、制造和部署相关的安全漏洞。硬件IFT可以检测无意的设计缺陷、恶意电路修改、时序侧通道、访问控制违规和其他不安全的硬件行为。本文对硬件提升领域进行了研究。我们首先讨论IFT的基础知识，它的基础是由丹宁在20世纪70年代引入的。在此基础上，我们开发了硬件IFT的分类。我们用它来分类和区分硬件IFT工具和技术。最后，我们讨论有待解决的挑战。调查显示，硬件IFT提供了一种强大的技术来识别硬件安全漏洞，以及验证和执行硬件安全属性。

[HTML] [Cryptographic Software IP Protection without Compromising Performance or Timing Side-channel Leakage](#)

AK Biswas – ACM Transactions on Architecture and Code ..., 2021

程序混淆技术是一种广泛应用于嵌入式系统的密码软件知识产权保护技术。然而，很少有著作研究结合不同的混淆技术对混淆程序的晦涩性(逆向工程的难度)和性能(执行时间)的影响。在本文中，我们提出了一个基于遗传算法(GA)的框架，它不仅优化了混淆密码程序的模糊和性能，而且它还确保了非常低的时间侧信道泄漏。我们提出的时序侧信道敏感程序混淆优化框架(TSC-SPOOF)确定了混淆变换函数的组合，这些函数使用首选的优化参数产生优化的混淆程序。特别地，TSC-SPOOF使用归一化压缩距离(NCD)和信道容量分别测量模糊和定时侧信道泄漏。我们还使用运行在Xilinx Zynq FPGA设备上的RISC-V rocket core作为我们框架的一部分，以获得现实的结果。实验结果表明，与无导向混淆相比，我们提出的解决方案可以使密码程序具有更低的执行时间、更高的模糊度和更低的定时侧信道泄漏。

[Towards Linux based safety systems—A statistical approach for software execution path coverage](#)

I Allende, N Mc Guire, J Perez, LG Monsalve... – Journal of Systems ..., 2021

目前，一些工业领域正在开发与安全相关的创新自主系统，其特点是软件的复杂性和高性能需求不断增加。由于这些特性，不同的研究计划旨在为使用Linux开发这样复杂的安全相关系统铺平道路。然而，Linux内核的高执行路径可变性挑战了基于测试覆盖率的验证，这是安全标准高度推荐的(HR)技术。摘要本研究提出了一种适用于Linux内核执行路径覆盖率量化的统计分析方法，包括软件执行的不确定性估计。将该方法应用于一个简单、可重复的案例研究中，并对结果进行了分析和说明。

[SeRoT: A Secure Runtime System on Trusted Execution Environments](#)

J Liu, Y Qin, D Feng – 2020 IEEE 19th International Conference on Trust ..., 2020

... In these two levels, we prevent the adversary interfacing with malicious messages. Furthermore, we implement SeRoT on a RISC-V based platform and show our scheme

is average about 10% faster than Keystone on two popular and representative benchmarks

...

架构

[PDF] [Vectorizing Posit Operations on RISC-V for faster Deep Neural Networks: Experiments and Comparison with ARM SVE](#)

M Cococcioni, F Rossi, E Ruffaldi, S Sergio

随着开源RISC-V处理器架构的到来，有机会重新思考深度神经网络（DNNs）和信息表示和处理。在这项工作中，我们将利用以下想法：i)利用我们最近的发现和posit数系统的实现，减少表示DNNs权重所需的位数；ii)尽可能地利用RISC-V矢量化，以加快格式编码/解码、激活函数的评估(仅使用算术和逻辑运算，利用近似公式)和核心DNNs矩阵-矢量运算的计算。由于其封闭性和成熟性，与成熟的架构ARM Scalable Vector Extension(SVE)的比较是自然的，也是具有挑战性的。实验结果表明，如何在RISC-V上实现向量化的posit操作，在所有涉及的操作上获得大幅提速。此外，实验结果还强调了新架构如何在性能上赶上更成熟的ARM架构。为此，本研究非常重要，因为它预示了我们期望在拥有一个开放的RISC-V硬件协处理器，能够原生操作posits时取得的结果。

[Nonconventional Computer Arithmetic Circuits, Systems and Applications](#)

L Sousa – IEEE Circuits and Systems Magazine, 2021

算术在计算机中起着重要作用。它的性能和效率。构建由传统二进制算法和基于硅的技术支持的新的计算平台，以满足当今的需求？无论我们考虑的是嵌入式设备还是高性能计算机，计算机的应用正变得越来越具有挑战性。因此，为了研究更高效的算术电路和改进的计算机技术，以促进计算单元的发展，以满足新兴领域的应用需求，大量的研究工作已经投入到非常规数字系统的研究中。本文概述了非常规计算机算法的最新进展。分析了几种不同的替代计算模型和新兴技术，如纳米技术、超导体器件和基于生物和量子的计算，并讨论了它们在多个领域的应用。一个全面的方法是遵循对对数和剩余数系统，多维和随机计算模型，量子dna为基础的计算系统的算法和近似计算技术的调查。本文还讨论了解决这些非常规计算机算法系统的技术、处理器和系统，并考虑了一些最突出的应用，如深度学习或后量子密码学。最后得出了一些结论，并对未来非常规计算机算法的研究方向进行了讨论。

EDA

[PDF] [Machine Learning for Electronic Design Automation: A Survey](#)

FEI NING, Y MA, H YANG, BEI YU, H YANG, YU WANG – 2021

随着CMOS技术的小型化，超大规模集成电路(VLSI)的设计复杂度越来越高。尽管机器学习(ML)技术在电子设计自动化(EDA)中的应用可以追溯到上世纪90年代，但近年来机器学习技术的突破和EDA任务的日益复杂引起了人们对利用机器学习来解决EDA任务的兴趣。在本文中，我们提出了一个全面的回顾现有的ML为EDA研究，组织了EDA层次。

Standard-compliant parallel SystemC simulation of loosely-timed transaction level models: From baremetal to Linux-based applications support

G Busnot, T Sassolas, N Ventroux, M Moy – Integration, 2021

为了应对片上系统(soc)日益增长的复杂性和它们上市时间紧迫的限制，基于SystemC/TLM2.0的虚拟样机(VP)工具必须在保持准确性的同时获得更快的速度。然而，ASI SystemC参考实现仍然是顺序的，不能利用现代工作站的多核。在本文中，我们提出了SCale 2.0，一个新的并行和标准兼容的SystemC内核的实现，达到了前所未有的仿真速度。通过将并行SystemC内核与共享资源访问监视和进程级回滚耦合起来，我们可以在利用可用主机内核的同时保留SystemC原子线程评估。我们还生成了可用于为调试目的确定地重放任何模拟的流程交互跟踪。对裸金属应用程序的评估显示 × 15与使用33个主机核的ASI SystemC内核相比，达到每秒2300万条模拟指令(MIPS)以上的速度。通过在记录运行时达到 × 13，在回放运行时达到 × 24的加速，也解决了与现代操作系统并行仿真全软件堆栈相关的挑战。

一周专利

CONFIGURABLE PROCESSOR FOR IMPLEMENTING CONVOLUTION NEURAL NETWORKS

P Sinha – US Patent App. 16/933,859, 2021

Configurable processors for implementing CNNs are provided. One such configurable CNN processor includes a plurality of core compute circuitry elements, each configured to perform a CNN function in ac.

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
	高效服务器和存储技术国家重点实验室	inspur-risc-v	inspur-risc-v	riscv
RISC-V和芯片动态简报		RVWeekly	RVWeekly	RVWeekly
riscv rvnews				

