

同行专家业内评价意见书编号： 20250854464

附件1

浙江工程师学院（浙江大学工程师学院） 同行专家业内评价意见书

姓名： 陈芳

学号： 22260262

申报工程师职称专业类别（领域）： 电子信息

浙江工程师学院（浙江大学工程师学院）制

2025年05月26日

填表说明

一、本报告中相关的技术或数据如涉及知识产权保护、军工项目保密等内容，请作脱密处理。

二、请用宋体小四字号撰写本报告，可另行附页或增加页数，A4纸双面打印。

三、表中所涉及的签名都必须用蓝、黑色墨水笔，亲笔签名或签字章，不可以打印代替。

四、同行专家业内评价意见书编号由工程师学院填写，编号规则为：年份4位+申报工程师职称专业类别(领域)4位+流水号3位，共11位。

一、个人申报

(一) 基本情况【围绕《浙江工程师学院（浙江大学工程师学院）工程类专业学位研究生工程师职称评审参考指标》，结合该专业类别(领域)工程师职称评审相关标准，举例说明】

1. 对本专业基础理论知识和专业技术知识掌握情况(不少于200字)

本人在形式化方法验证领域系统掌握了计算机科学基础理论，包括离散数学、数理逻辑、自动机理论、程序语义学等支撑形式化验证的核心数学工具，能够熟练运用Hoare逻辑、时序逻辑构建程序规约。针对操作系统内核验证需求，深入研究了Rust语言类型系统的数学基础（如基于线性逻辑的所有权模型、生命周期静态分析算法）。在操作系统层面，系统掌握虚拟内存管理机制（如多级页表结构、地址转换算法）、硬件抽象层（HAL）与MMU交互原理，通过Isabelle/HOL定理证明器构建了页表保护机制的抽象状态机模型，实现了对页表权限配置、TLB一致性等关键属性的数学化描述与验证。研究方法上，融合了交互式定理证明，采用Isabelle工具完成从高层规约到Rust代码的形式化建模与证明。

2. 工程实践的经历(不少于200字)

在BlockSec的实习期间，我主要研究了Rust语言的形式化验证技术。随着计算机硬件的发展，传统操作系统的性能瓶颈日益显现。Rust语言因其出色的安全性和高性能，成为重写操作系统的一种新趋势，近年来，一些新兴的操作系统项目开始采用Rust语言进行开发，例如Redox OS、Tock

OS等。Rust语言的安全性可以有效减少操作系统中的安全漏洞风险，其高性能特性则能够提升操作系统的运行效率，传统的验证方法主要依赖于人工审计和测试，不仅效率低且覆盖范围有限，难以发现潜在的安全漏洞，而形式化验证技术通过严格的数学证明，可以显著提高验证的准确性和效率。通过对Rust语言的形式化验证研究，可以为Rust生态系统提供更强的安全保障，有利于Rust语言的进一步应用和推广，这项研究不仅有助于提升操作系统的安全性和性能，还为区块链等领域的技术发展提供了坚实的基础。

3. 在实际工作中综合运用所学知识解决复杂工程问题的案例（不少于1000字）

针对Rust语言的形式化验证工作，技术难点在于：①工具链的成熟度低。尽管形式化验证在学术界已有较长的发展历史，但针对Rust语言的形式化验证工具链仍在发展中，现有工具在功能和性能上尚未完全成熟，使用过程中遇到了不少限制和瓶颈。与其他成熟编程语言相比，Rust的形式化验证领域的研究和资源相对较少，需要更多的社区支持和资源投入。②高复杂性与规模选择。形式化验证需要对整个系统或系统关键模块进行详细建模，Rust语言的复杂性使得这项工作非常具有挑战性，尤其Rust的内存安全特性和并发编程模型需要特别仔细的分析和建模。形式化验证依赖于严格的数学证明，对于复杂系统来说，构建和验证这些数学证明需要深厚的理论基础和丰富的实践经验，确保证明的完整性和正确性是一个非常困难的任务。③性能与效率的平衡。形式化验证通常需要大量计算资源和时间，如何在确保验证准确性的同时提高验证效率，是一个需要重点解决的问题。

为了解决以上问题，我们从以下几个方面进行尝试：①竞争公司验证工作的研究：研究了业内其他公司在形式化验证领域的工作，包括验证技术的选择、应用场景、工具使用及其成功案例。这帮助我们了解了当前形式化验证的最佳实践，并识别出我们可以改进和创新的地方。②Rust验证研究现状分析：分析了现有文献和项目，了解Rust语言形式化验证的研究进展和挑战。这包括对学术论文、开源项目和行业报告的深入研读，帮助我们掌握了Rust验证的前沿技术和存在的问题。③Rust验证工具的调研及使用：对现有的Rust验证工具（如Prusti

、Kani等)进行了调研和评估,并在实际项目中进行了试用。我们评估了这些工具的功能、性能和易用性,确定了它们在不同场景下的适用性和局限性。④Rust语言使用生态的分析:研究了Rust语言在不同领域的应用情况,尤其是在操作系统和区块链中的应用。通过分析Rust生态系统的使用情况和发展趋势,我们可以更好地定位形式化验证的应用价值。⑤Rust形式化验证尝试:在具体项目中应用形式化验证技术,对Rust代码进行验证。这包括编写形式化规范、建立验证模型、运行验证工具并分析验证结果。

最终我们成功针对Rust实现的Hypervisor关键模块进行形式化建模与验证,确保其从需求层到源码实现的端到端安全。这种方法不仅提高了系统的安全性和稳定性,还为其他高安全性要求的软件系统提供了可参考的验证框架。

(二)取得的业绩(代表作)【限填3项,须提交证明原件(包括发表的论文、出版的著作、专利证书、获奖证书、科技项目立项文件或合同、企业证明等)供核实,并提供复印件一份】

1. 公开成果代表作【论文发表、专利成果、软件著作权、标准规范与行业工法制定、著作编写、科技成果获奖、学位论文等】

成果名称	成果类别 [含论文、授权专利（含发明专利申请）、软件著作权、标准、工法、著作、获奖、学位论文等]	发表时间/ 授权或申请时间等	刊物名称/ 专利授权或申请号等	本人排名/ 总人数	备注
一种面向 Rust 语言实现的操作系统页表保护形式化建模与验证方法	发明专利申请	2024年05月24日	申请号：202410655890.3	2/3	

2. 其他代表作【主持或参与的课题研究项目、科技成果应用转化推广、企业技术难题解决方案、自主研发设计的产品或样机、技术报告、设计图纸、软课题研究报告、可行性研究报告、规划设计方案、施工或调试报告、工程实验、技术培训教材、推动行业发展中发挥的作用及取得的经济社会效益等】

作为学生负责人参与华为技术有限公司委托的Rust高安嵌片形式化证明关键技术合作项目

(三) 在校期间课程、专业实践训练及学位论文相关情况	
课程成绩情况	按课程学分核算的平均成绩： 86 分
专业实践训练时间及考核情况(具有三年及以上工作经历的不作要求)	累计时间： 1 年（要求1年及以上） 考核成绩： 84 分
本人承诺	
个人声明：本人上述所填资料均为真实有效，如有虚假，愿承担一切责任，特此声明！	
申报人签名：陈芳	

工作单位考核评价：
合格
(公章)：  2025年5月

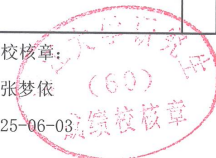
日常表现考核评价	非定向生由德育导师考核评价、定向生由所在工作单位考核评价： ☒优秀 ☐良好 ☐合格 ☐不合格 德育导师/定向生所在工作单位分管领导签字（公章）： 2025年5月26日
申报材料审核公示	根据评审条件，工程师学院已对申报人员进行材料审核（学位课程成绩、专业实践训练时间及考核、学位论文、代表作等情况），并将符合要求的申报材料在学院网站公示不少于5个工作日，具体公示结果如下： ☐通过 ☐不通过（具体原因： ） 工程师学院教学管理办公室审核签字（公章）： 年 月 日

攻读硕士学位研究生成绩表

说明: 1. 研究生课程按三种方法计分: 百分制, 两级制 (通过、不通过), 五级制 (优、良、中、及格、不及格)。
2. 备注中“*”表示重修课程。

成绩校核人：张梦依

打印日期: 2025-06-01





(12) 发明专利申请

(10) 申请公布号 CN 118503157 A

(43) 申请公布日 2024. 08. 16

(21) 申请号 202410655890.3

(22) 申请日 2024.05.24

(71) 申请人 浙江大学

地址 310058 浙江省杭州市西湖区余杭塘路866号

(72) 发明人 常瑞 陈芳 张卓若

(74) 专利代理机构 杭州中成专利事务所有限公司 33212

专利代理师 李亦慈 唐银益

(51) Int. Cl.

G06F 12/14 (2006.01)

G06F 21/78 (2013.01)

G06F 21/57 (2013.01)

G06F 9/448 (2018.01)

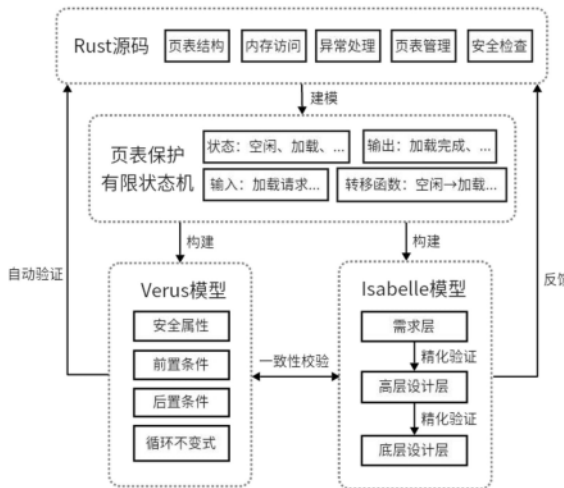
权利要求书2页 说明书6页 附图1页

(54) 发明名称

一种面向Rust语言实现的操作系统页表保护形式化建模与验证方法

(57) 摘要

本发明公开了一种面向Rust语言实现的操作系统页表保护形式化建模与验证方法,将交互式定理证明和自动验证两种方法结合起来,利用交互式定理证明方法的严格性和自动验证方法的高效性,对页表保护机制进行形式化建模和验证,实现针对页表保护的从源码层面至需求层面的端到端验证。本发明实现了一致性校验确保全面性,反馈机制确保模型准确性,提高开发和维护效率,可扩展性和复用性:所设计的形式化验证方法具有良好的可扩展性和复用性,可以应用于其他类似的操作系统安全机制的验证,为后续相关研究和开发提供了有价值的参考和工具支持。



学生参与科研项目的情况说明

项目名称：Rust 高安嵌片形式化证明关键技术合作项目

委托单位：华为技术有限公司

合同金额：40 万元

学生姓名：陈芳

学生排名：3

项目主要研究内容：

本项目研究基于分层形式化建模的 Rust 安全模块验证技术，设计并实现面向光产品线嵌入式系统的安全验证框架，提升高安全场景下 Rust 关键模块的可验证性与可靠性。

取得的经济社会效益：

1. 安全防护价值：应用分层形式化建模方法验证 Rust 关键模块，有效识别内存管理和权限控制方面的潜在风险，提升光通信设备的安全可靠性。
2. 经济效益：通过在开发阶段发现和修复安全问题，降低产品后期维护成本，减少因安全漏洞导致的产品迭代和修复投入。
3. 方法应用价值：将形式化验证方法应用于 Rust 嵌入式开发领域，为相关行业提供可行的安全验证方案参考，提升开发过程的安全保障水平。
4. 技术推广价值：研究成果为光通信设备的安全开发提供技术支持，推动形式化验证方法在嵌入式系统领域的实际应用。

学生承担的主要工作：

陈芳同学作为项目核心开发成员，主要负责页表保护与代码保护机制的形式化验证工作，针对高安全场景下 Rust 语言实现的虚拟机管理器完成功能需求及设计实现的分层形式化模型，定义系统抽象安全策略及威胁模型分析，在 Isabelle 中完成了共约三千余行的模型构建与证明，覆盖了页表权限管理、内核代码写保护等核心安全机制。相关工作已应用于辅助实际产品安全开发流程，为系统通过 EAL5+安全认证提供了关键技术支撑。

项目负责人签字：陈芳

2025 年 5 月 22 日



微信订阅号



微信服务号

首页 > 过刊浏览 > 2025年第36卷第8期 > 1-33. DOI:10.13328/j.cnki.jos.007353

PDF HTML阅读 XML下载 导出引用 引用提醒

面向Rust语言的形式化验证方法研究综述

DOI:

10.13328/j.cnki.jos.007353

作者:

张卓若 常瑞 杨申毅 陈芳

通讯作者:

常瑞, E-mail: crix1021@zju.edu.cn

中图分类号:

TP311

基金项目:

国家重点研发计划(2022YFB4501903)

Survey on Formal Verification Research for Rust Language

Author:

ZHANG Zhuo-Ruo CHANG Rui YANG Shen-Yi CHEN Fang

摘要 | 访问统计 | 参考文献 [90] | 相似文献 [20] | 文章评论

摘要:

Rust作为一种新兴的安全系统级编程语言,以其创新的所有权模型和借用检查机制提供了内存安全和并发安全保证。尽管Rust的设计宗旨在于安全性,但现有研究揭示了其仍面临诸多安全挑战。形式化验证作为一种基于严格数学基础的方法,为Rust安全性提升提供了强有力保障。通过构建精准清晰的语义模型,可以证明遵循Rust检查规则的程序满足安全性要求;借助Rust自动化验证工具能够帮助用户确保其Rust程序的安全性和正确性。对Rust形式化验证工作进行全面系统性分析。首先介绍Rust核心语义和复杂特性,并探讨Rust形式化语义的研究与验证工作,强调Rust类型系统在形式化验证中的潜力。其次,阐述面向Rust程序的自动化验证方法,并对对比分析不同验证工具的功能、支持的语言特性、采用的验证技术和适用场景,这对于在Rust项目实际开发流程中指导工具的选择和集成有重要意义。此外,还总结Rust程序验证的典型实例,展示形式化验证在确保程序正确性方面的显著成效,并结合验证实例总结工具使用建议供用户参考。最后讨论当前领域的技术挑战,并指出未来可能的研究方向,涵盖了unsafe Rust代码的验证、并发代码的验证、可信编译,以及大模型驱动的形式化验证等。旨在为Rust社区提供坚实的安全基础,并推动形式化验证在Rust开发中的应用。

关键词: 形式化方法; Rust语言; 程序验证; 形式语义; 内存安全

引用本文

张卓若,常瑞,杨申毅,陈芳.面向Rust语言的形式化验证方法研究综述.软件学报,2025,36(8):1-33

复制

分享



文章指标

点击次数: 430

下载次数: 310

HTML阅读次数: 0

历史

收稿日期: 2024-08-26

最后修改日期: 2024-10-14

在线发布日期: 2024-12-10

文章二维码



Abstract:

As an emerging system programming language with a focus on safety, Rust ensures memory and concurrency safety through its innovative ownership model and borrowing mechanism. Despite its design for safety, existing research has identified several safety challenges that Rust still faces. Formal verification, grounded in rigorous mathematical principles, provides robust assurances for enhancing Rust's security. By constructing precise and well-defined semantic models, it becomes possible to formally prove that programs adhering to Rust's type system meet safety requirements. Automated verification tools for Rust further enable users to validate the safety and correctness of their programs. This study presents a comprehensive and systematic analysis of formal verification approaches for Rust. It begins by introducing Rust's core semantics and complex features, followed by an exploration of research and verification efforts in Rust's formal semantics, emphasizing the role and potential of Rust's type system in formal verification. Next, the study systematically compares the capabilities, supported language features, underlying techniques, and application scenarios of various automated Rust verification tools. These comparisons are instrumental in guiding tool selection and integration within real-world Rust development workflows. In addition, this study summarizes exemplary cases of verified Rust programs, demonstrating the significant impact of formal verification in ensuring program correctness and providing practical tool usage recommendations for developers. Finally, it discusses the key challenges in the field and outlines promising directions for future research, including the verification of unsafe Rust code, concurrent code verification, trustworthy compilation, and large model-driven formal verification. This study aims to establish a strong security foundation for the Rust community and foster the broader adoption of formal verification methods in Rust development.

Key words: formal method; Rust language; program verification; formal semantics; memory safety

友情链接: [中国科学院软件研究所](#) [中国计算机学会](#) [中国科学院](#) [国家自然科学基金委员会](#) [CCF数字图书馆](#) [Int'l J of Softw Info](#) [计算机系统应用](#)

您是第19955849位访问者

版权所有: 中国科学院软件研究所 京ICP备05046678号-3

地址: 北京市海淀区中关村南四街4号, 邮政编码: 100190

电话: 010-62562563 传真: 010-62562533 Email: jos@iscas.ac.cn

技术支持: 北京勤云科技发展有限公司

 京公网安备 11040202500063号