

BMCFuzz: 限界模型检测与模糊测试双向融合的处理器的验证方法

申世东, 刘锦宇, 冯维直, 宋富, 吴志林

The 44th International Conference on Computer-Aided Design (ICCAD 2025)

开源工具: <https://github.com/iscas-versys/BMCFuzz>

联系人: 申世东 shensd@ios.ac.cn 19929931316

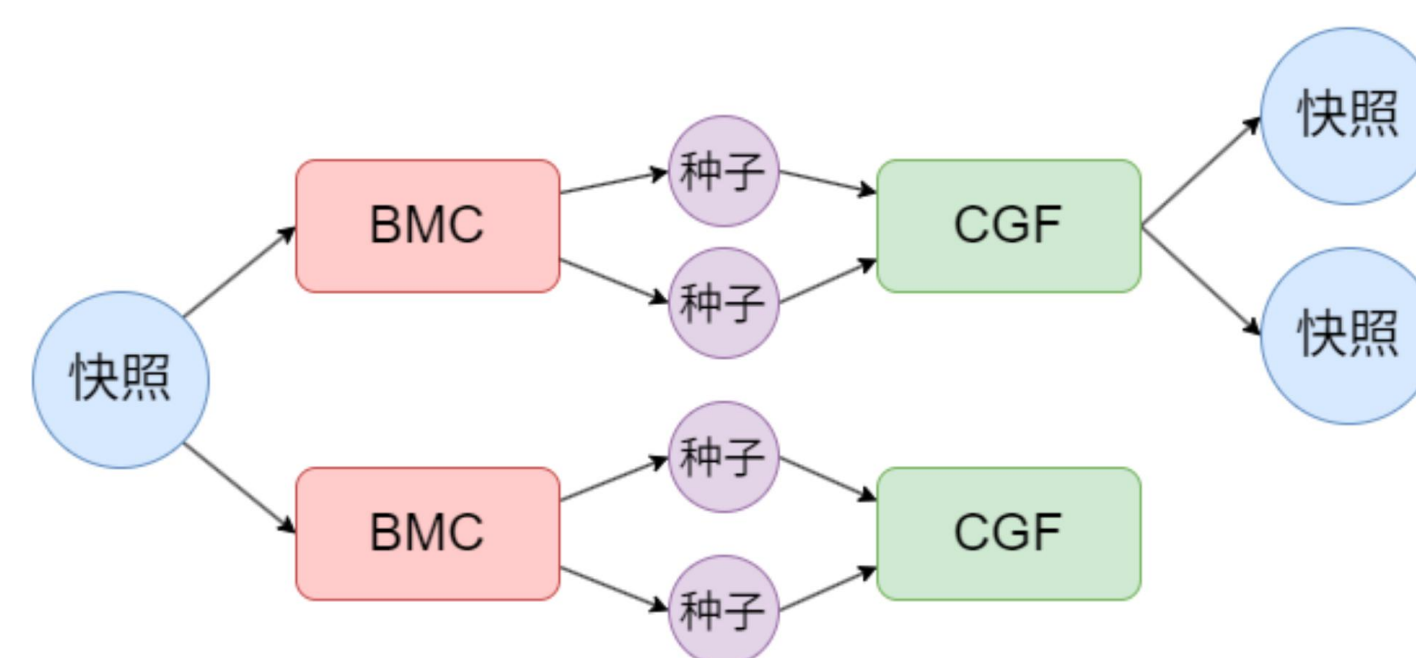
背景介绍

在处理器验证领域, 形式化验证因**状态空间爆炸**面临探索深度受限的问题, 难以覆盖复杂处理器设计中关键路径; 而模糊测试虽高效, 但严重依赖**种子质量**, 难以系统性触达深层状态。已有方法尝试结合形式化验证与模糊测试, 但都为**单向融合**, 即形式化验证方法仅用于提升模糊测试性能, 缺乏模糊测试对形式化验证过程的反馈与支持。本工作提出**BMCFuzz**方法, **首次实现了模型检测与模糊测试的双向融合**。

总体思路

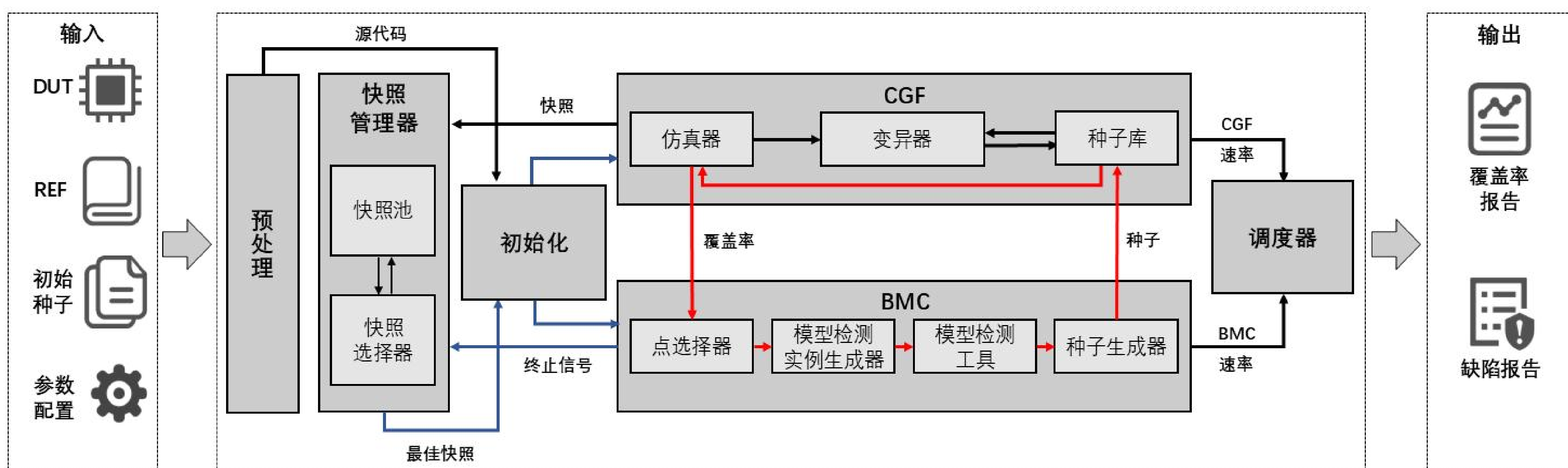
➢ 引入“**快照**”实现限界模型检测 (BMC) 与覆盖率引导的模糊测试 (CGF) 双向融合

- 快照记录待测处理器设计在某一时刻的完整电路级状态
- 监控**特权级**与**关键CSR寄存器**保存快照
- 五种快照评分准则和动态优先级评分算法



双向协同机制

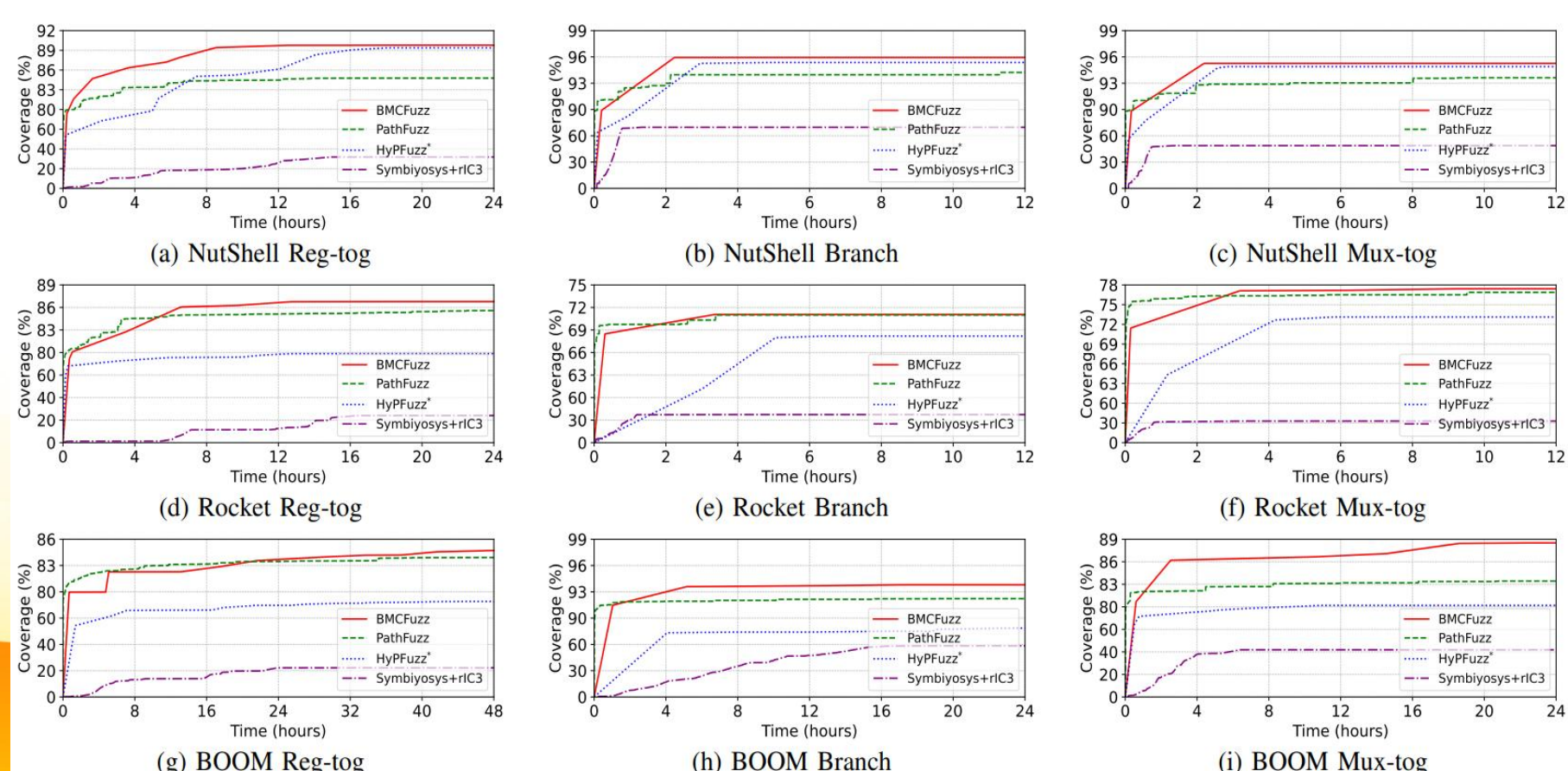
➢ 缓存式**内存抽象**优化模型检测效率



总体框架(蓝色:快照循环; 红色:BMC-CGF循环)

实验结果

实验选择三个知名开源 RISC-V 处理器**NutShell**、**Rocket**与**BOOM**作为验证对象, 在寄存器翻转覆盖率 (Reg-Tog)、分支覆盖率 (Branch) 以及多路选择器翻转覆盖率 (Mux-Tog) 三种评价指标上进行实验, 我们的方法均达到了最高覆盖率, 覆盖率较原SOTA方法最高提升了**15.28%**, 且成功新发现NutShell上3个新缺陷和BOOM上的1个新缺陷。



各工具覆盖率随时间变化曲线

处理器	缺陷编号	缺陷描述	是否新发现	设计者已确认
NutShell	N1	非叶子页表项的 D/A/U 保留位未清零, 与 RISC-V 规范及 Spike 行为不符	✓	✓
NutShell	N2	启用 Sv39 时, TLB 异常不会正确向上传播, 导致处理器挂起	✓	✓
NutShell	N3	medeleg 掩码错误 (使用 0xbfff 而非规范要求的 0xb3ff)	✓	✓
BOOM	B1	未实现 Svnoprot 时, 页表项第 63 位未清零, 应触发页缺失异常却未触发	✓	✗

实验发现的缺陷列表