

中国科学技术大学
University of Science and Technology of China

计算机系统与安全课题组
中国科学技术大学
Computer Systems & Security Group, USTC

2025年12月

一. 团队介绍

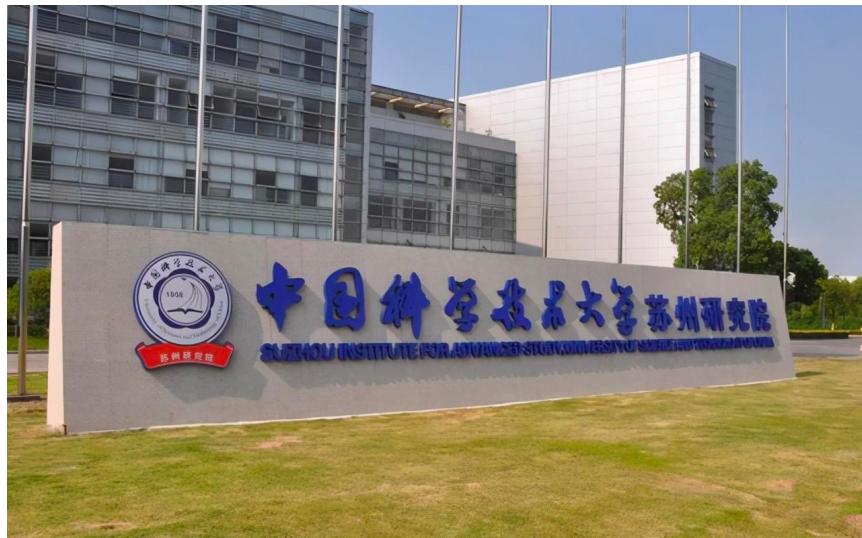


中国科学技术大学
University of Science and Technology of China

计算机系统与安全课题组 (Computer Systems & Security Group) 依托于中国科学技术大学苏州高等研究院和中国科学技术大学软件学院，组内现有教师4名，研究生20+人。和计算机学院、软件学院等研究团队保持紧密合作。

课题组自成立以来，致力于**发展跨学科的研究**，研究方向广泛覆盖编程语言设计、编译器实现、类型系统与形式化验证，信息安全到软件工程等多个前沿领域，近年来，团队在ISSRE、SANER、JCRD等顶级会议/期刊上发表论文50余篇、出版研究著作5部。

同时，课题组高度**重视与产业界的紧密合作**，已与多家知名企建立长期稳定的合作关系，围绕编程语言与编译器、程序分析、编译优化等方向展开挑战课题联合攻关，推动研究成果在合作伙伴实际业务场景中落地应用，支撑合作伙伴商业价值。



二. 研究方向



- 聚焦计算机系统与安全的前沿交叉方向，以程序语言和编译器技术为基本研究主线
- 跨学科研究
 - 编程语言
 - 编译器、AI编译器
 - 软件工程
 - 信息安全
 - 异构体系结构
 - ...

三. 课程建设



中国科学技术大学
University of Science and Technology of China

围绕编程语言与编译的研究方向，先后开设多门研究生课程，在中国科学技术大学软件学院教授的课程：

1、程序设计语言原理：研究生课程。讲授现代程序语言的设计原理

• 该课程连续2年入选教育部-华为“智能基座”产教融合协同育人基地项目

2、形式化方法：研究生课程。讲授形式化方法及其在软件工程中的应用

3、高级编译原理：研究生课程。讲授程序优化、静态程序分析、函数式编译、异构编译等高级编译课题。

4、信息安全：研究生课程。讲授软件安全、Web安全、网络安全等

5、大规模并行计算：研究生课程。讲授大规模并行程序设计，案例既包括传统的Cuda、也包括新兴的triton或cutile等范式

四. 研究成果



近2年论文发表情况 (部分)

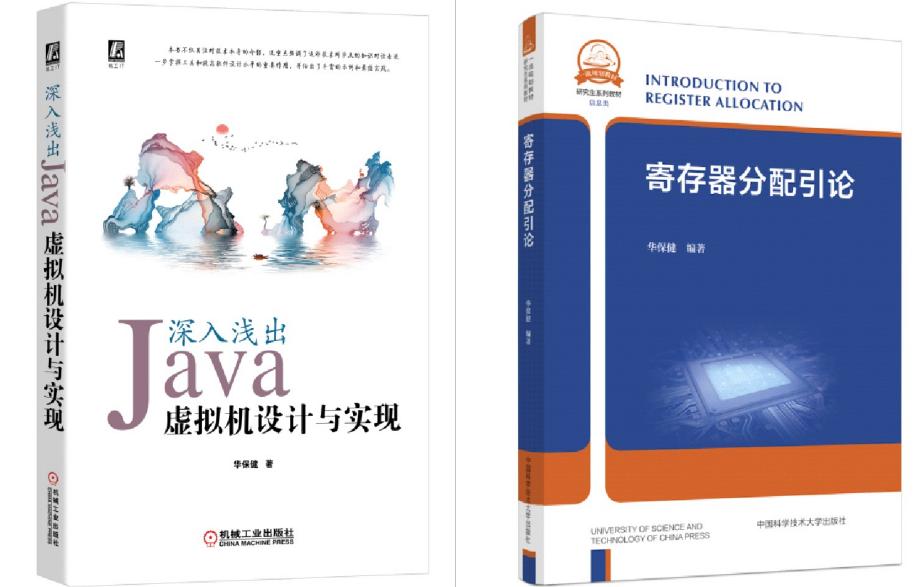
1. ORThrus: Detecting Deep Learning Compiler Bugs via Optimization-Resistance Transformations.
2. GPU Canary: Effectively Protecting GPU Memory with Indexing Canaries.
3. DeepLancet: Effectively Detecting Deep Learning Library Bugs via LLM-assisted Testcase Generation.
4. Are We There Yet? Unraveling the State-of-the-Art Binary Feedback-directed Optimizations.
5. RustGuard: Detecting Rust Data Leak Issues with Context-Sensitive Static Taint Analysis.
6. Shard: Securing GPU Kernels with Lightweight Formal Methods.
7. WaShadow: Effective Wasm Memory Protection with Virtual Machine-Aware Shadow Memory.
8. EdgeNAT: Transformer for Efficient Edge Detection.
9. Efficient Transformer-Based Edge Detector.
10. MePof: A Modular and End-to-End Profile-Guided Optimization Framework for Android Kernels.
11. Towards a Large-Scale Empirical Study of Python Static Type Annotations.
12. Code Duplication Removal in C to Rust Conversion via Unstructured Transfer Specialization.

五. 研究著作



中国科学技术大学
University of Science and Technology of China

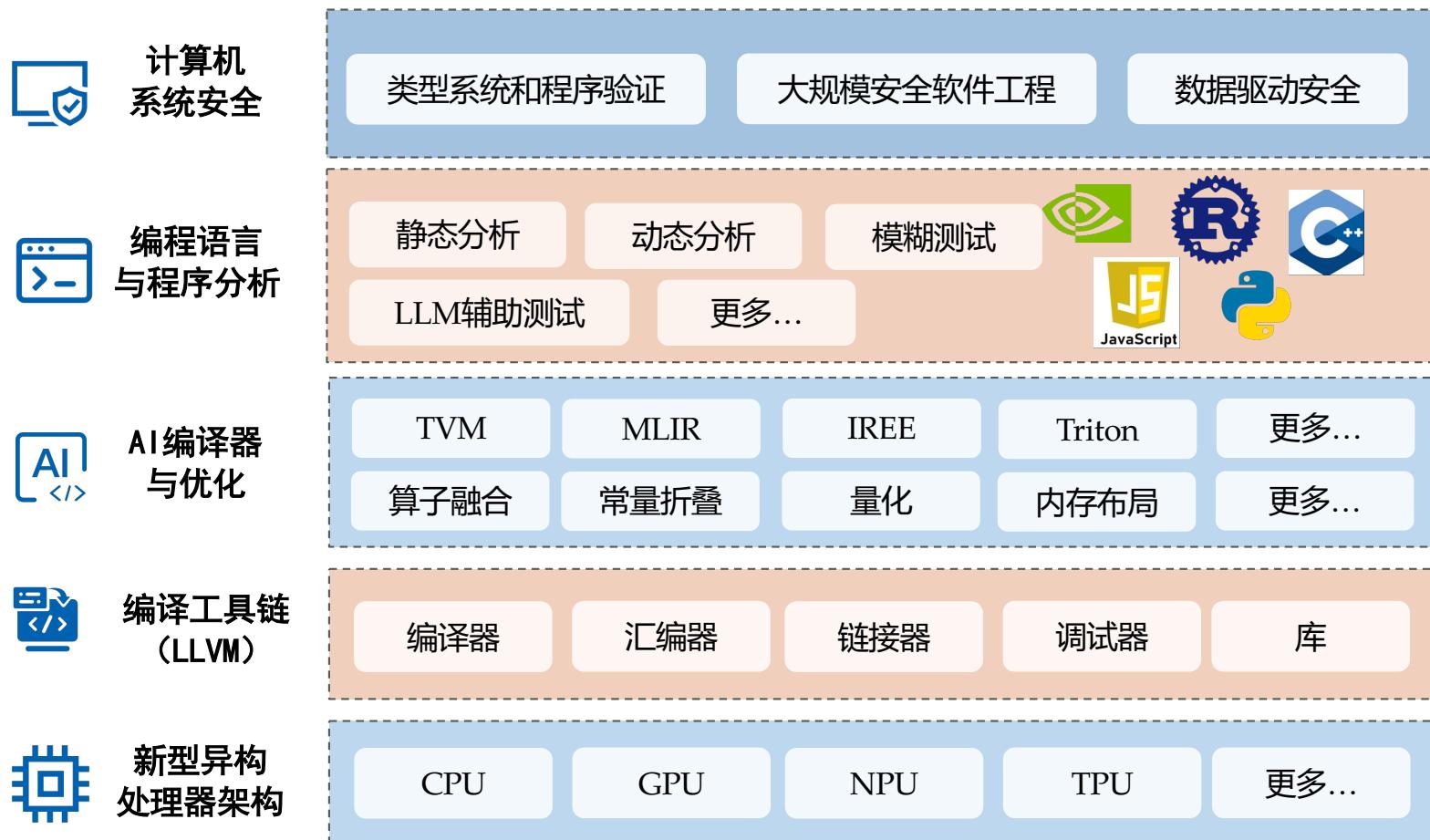
1. 《高级编译原理》：2026年将出版。入选教育部101课程教材建设计划。
2. 《深入浅出Java虚拟机设计实现》，2020年，47.2万字，机械工业出版社
3. 《寄存器分配引论》，2021年，20万字，中国科学技术大学出版社
4. 《毕昇编译器原理与实践》，2022年，40万字，清华大学出版社
● 和高耀清合著（华为2012实验室）
5. 《形式化方法：理论及应用》，2024年，60万字，中国科学技术大学出版社



六. 研究课题



研究课题范围：在计算机系统快速发展及新型计算范式持续创新的背景下，计算机系统安全成为信息系统的关键环节，其技术研究创新尤为重要。计算机系统安全课题组针对计算机系统的全场景，进行全栈研究。



6.1 面向国产嵌入式芯片的编译工具链研究

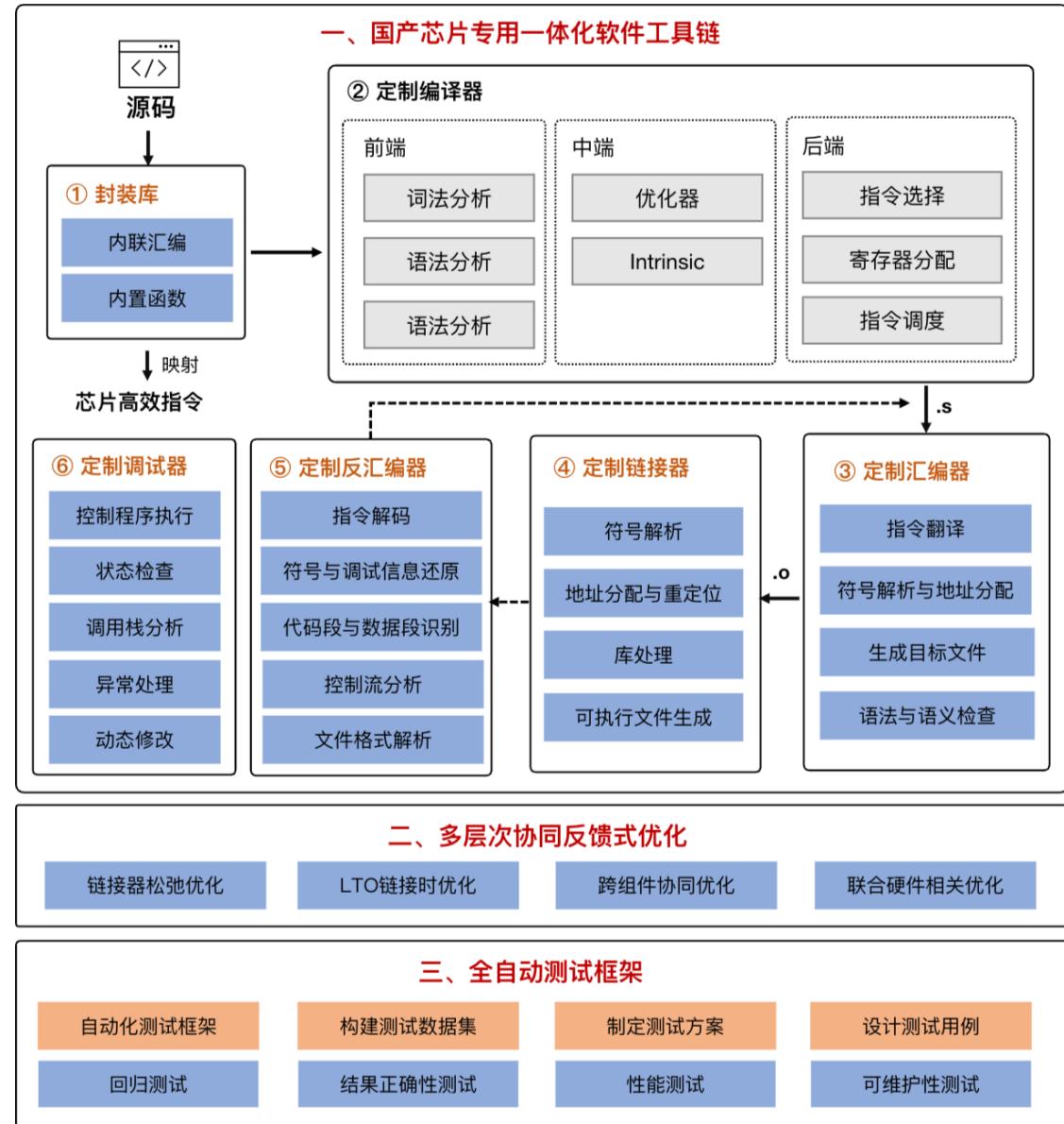


中国科学技术大学
University of Science and Technology of China

研究背景：作为国产芯片研发的关键，软件工具链的技术成熟度及稳定性尤为重要。本课题针对国产嵌入式芯片特性，构建了一套全栈LLVM编译工具链，极大提高芯片研发效率。

课题落地：在国内某领先MCU厂商的软件产品中落地

- **工具链设计实现：**编译器、汇编器、链接器、调试器、库等
- **定制优化策略：**松弛优化、链接时优化、代码大小优化等
- **工具链全面测试：**功能测试、正确

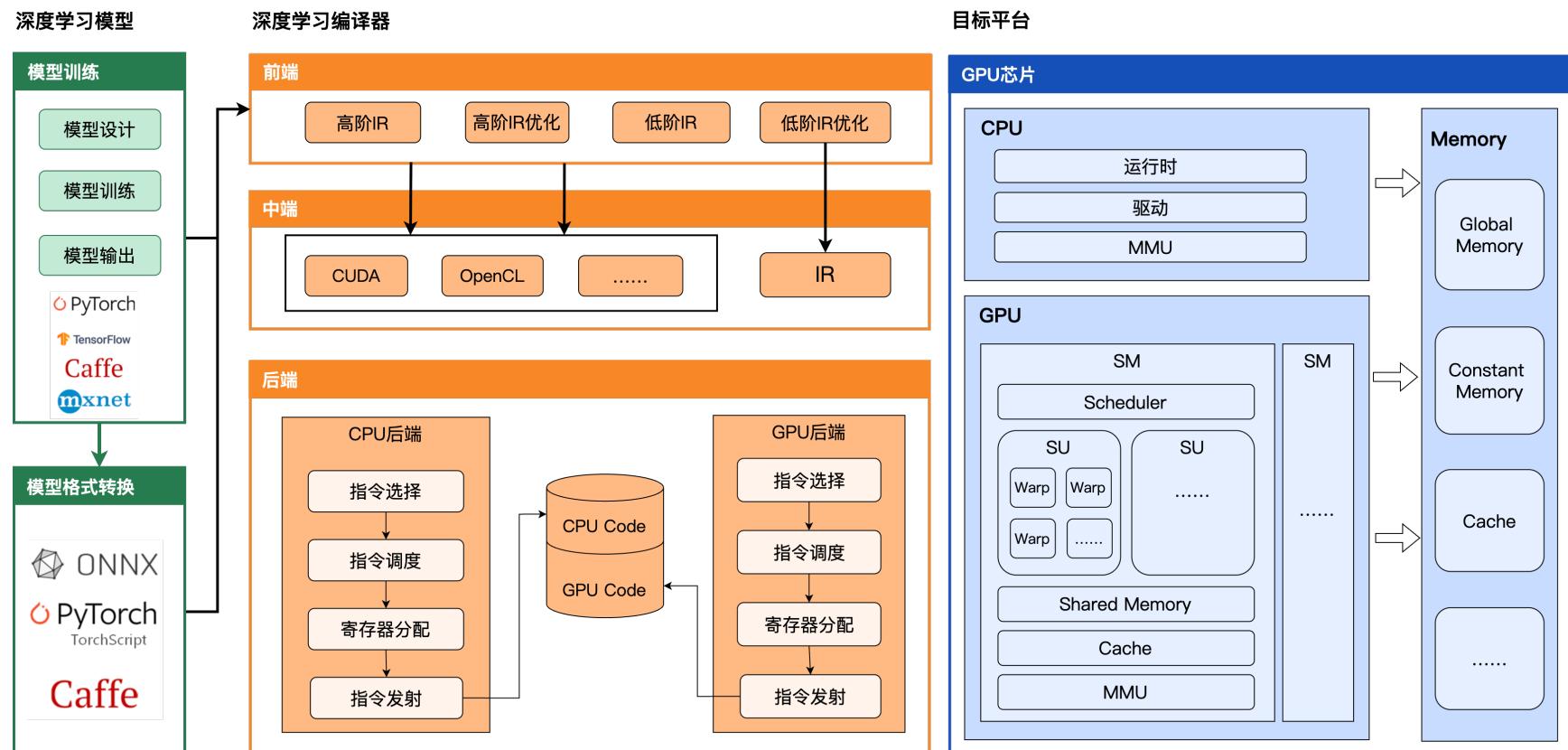


6.2 面向GPGPU芯片的深度学习编译器



研究背景：面向新一代深度学习加速器硬件GPGPU，进行端到端的深度学习编译器的研究与实现。研究内容涵盖深度学习框架适配、深度学习编译器设计与实现、以及运行时与驱动的实现，全面实现从深度学习编译器框架到自研GPGPU高效运行的可行性方案。

课题落地：已在国内某GPGPU公司自研的芯片中落地应用

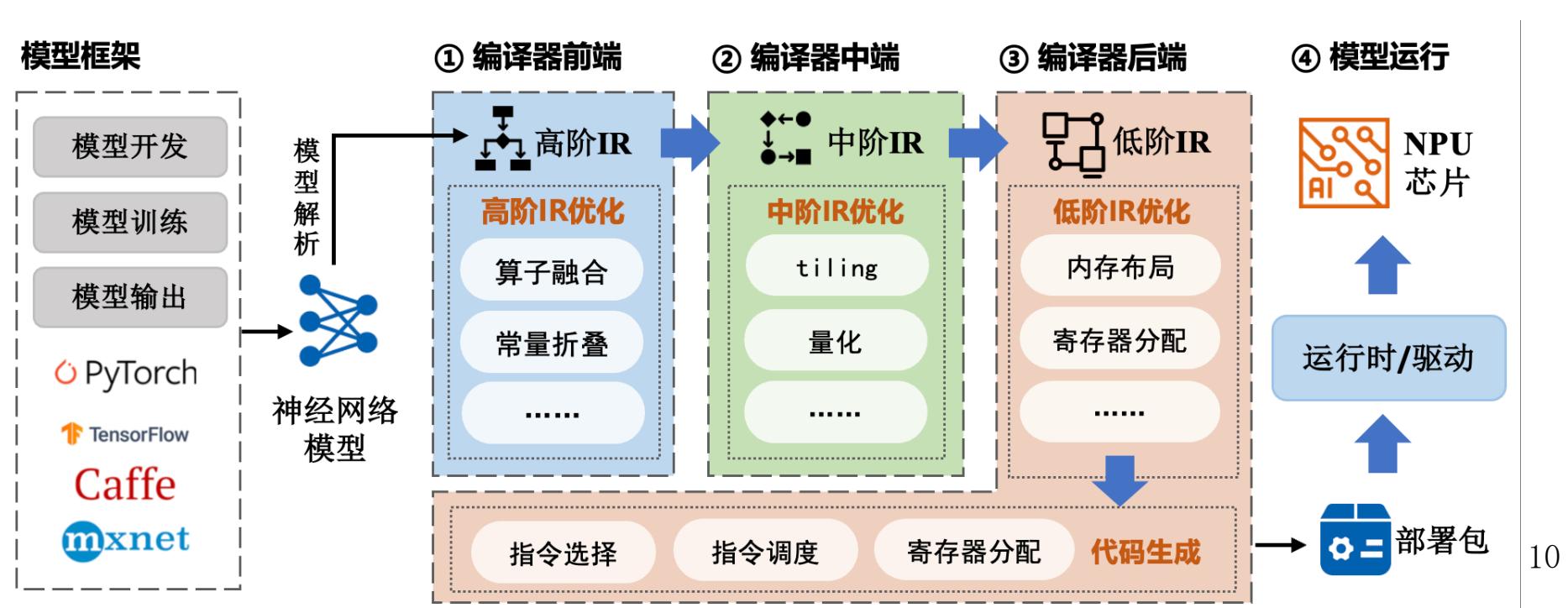


6.3 面向NPU芯片的深度学习编译器



研究背景：NPU编译器作为连接上层深度学习框架与底层硬件的关键桥梁，承担了模型描述、算子调度、图优化及指令生成等核心任务，成为充分发挥NPU硬件优势的关键环节。本课题研究并实现一套面向自研NPU架构的深度学习编译器，支持模型端到端完成编译与优化，提高整体开发效率，缩短芯片验证和开发周期。

成果落地：正在国内某上市公司的自研芯片中落地



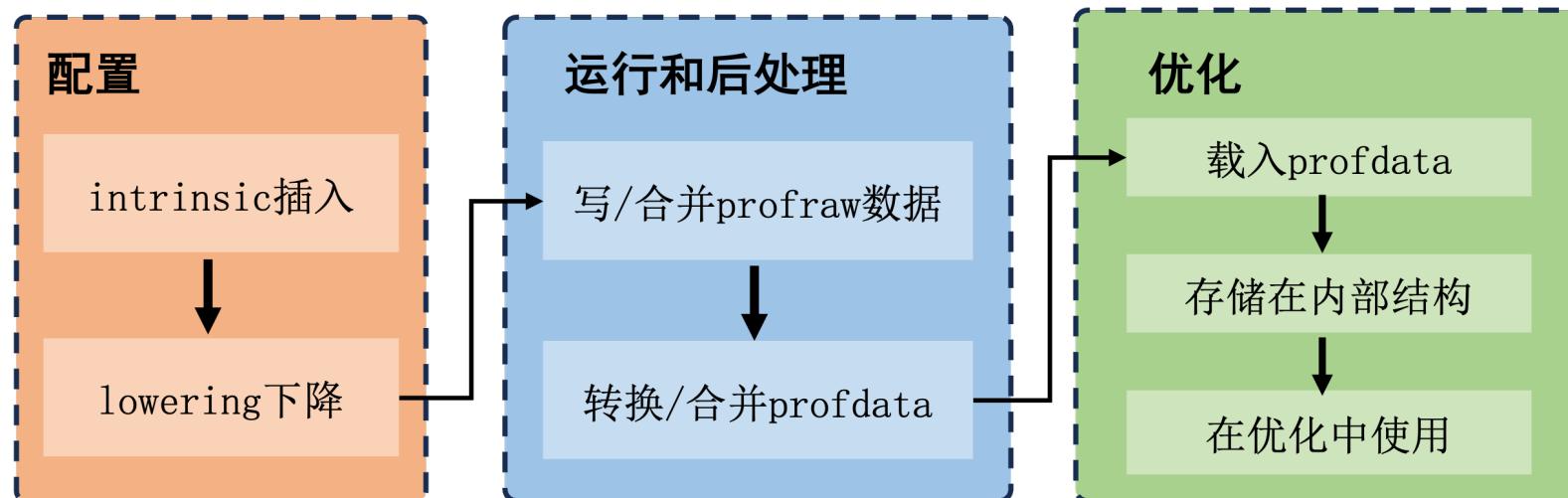
6.4 基于PGO技术的安卓内核优化研究



中国科学技术大学
University of Science and Technology of China

研究背景：内核性能优化是Android开发的关键任务之一，现有研究已提出将PGO技术应用于Android内核优化，但仍存在灵活性低、版本适配复杂等难题。本课题提出了基于PGO的端到端Android内核优化框架，经过大量实验分析，较原生内核整体性能提升14.43%。

成果落地：已在国内某Top3手机厂商落地



研究成果：

- An Automated and End-to-End Profile-guided Optimization Framework for Android. COMPSAC 2023
- [专利] 内核文件的***, 2022***
- [专利] 编译..., 2022***

6.5 声明式语言设计与编译

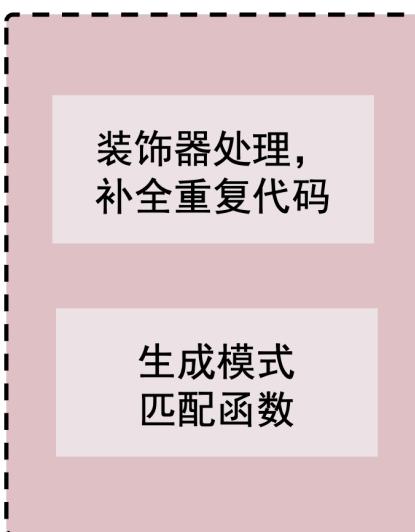


项目背景：现有声明式开发框架主要集中在声明式UI，缺少面向资源等重要编程对象进行编程，且传统开发框架不支持丰富的语义声明，缺少和运行时联动的优化机制。本课题面向设备资源，定义了一套编程更简洁、语义更丰富的编程范式，极大提高移动开发效率。

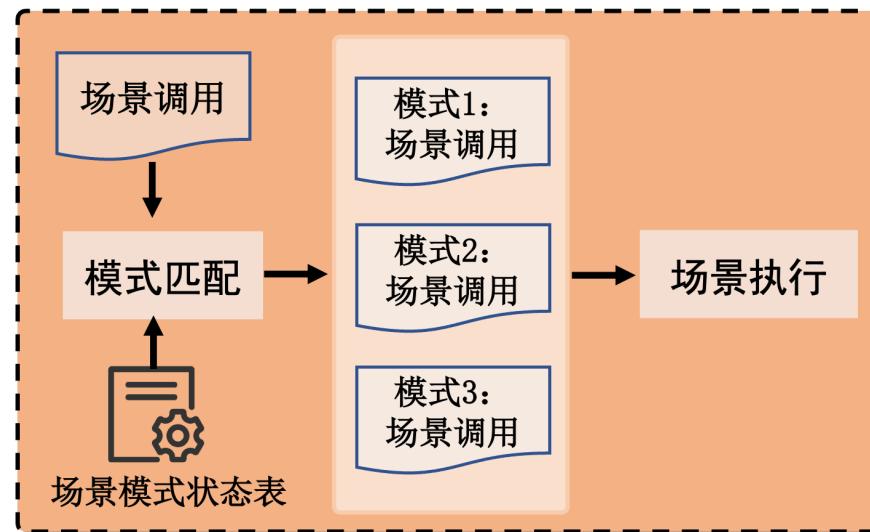
成果落地：已在国内某Top3手机厂商应用
开发时



编译时



运行时



研究成果：

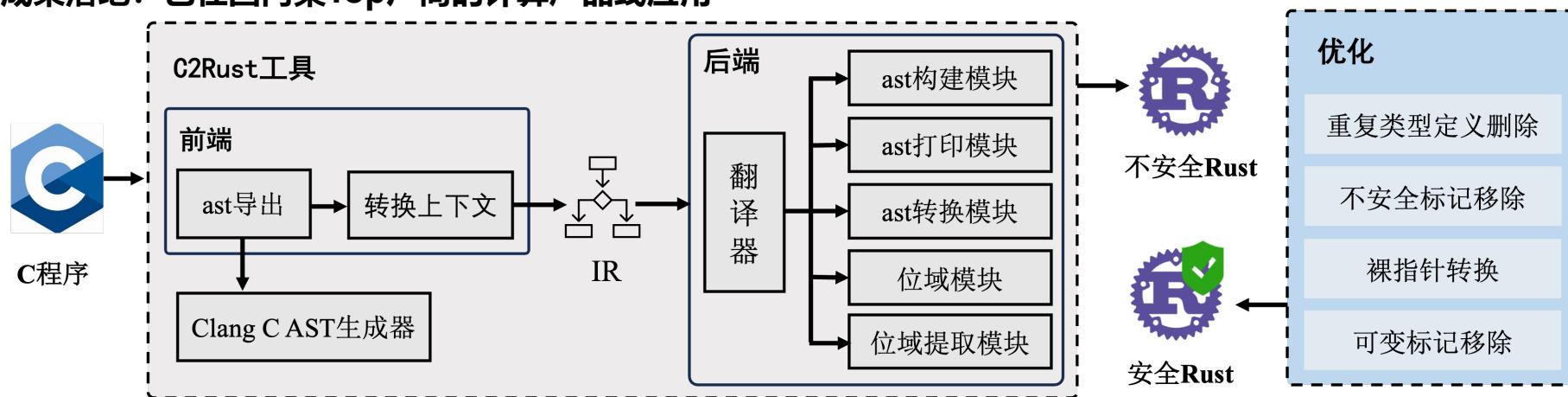
- [1] JasLoad: Dynamically Analyzing JavaScript Bytecode via A Load-Time Instrumentation Approach.QRS2025
- [2] JasFree: A Grammar-free Program Analysis for JavaScript Bytecode.TrustCom2024
- [3] An Empirical Study of Lightweight JavaScript Virtual Machines.QRS2023

6.6 C-To-Rust编译系统开发



研究背景：现有的源到源转换工具，能够快速将C程序转换为Rust程序，然而现有工具转换得到的Rust程序存在明显安全问题，无法充分发挥语言本身内存安全的特性，针对该问题，本课题研究并实现了一个比现有工具更有效、更安全的C2Rust 自动转换原型系统。

成果落地：已在国内某Top厂商的计算产品线应用



研究成果：

- [1] Security Risks of Transpiling C Programs to Rust. TrustCom2025
- [2] RustCheck: Safety Enhancement of Unsafe Rust via Dynamic Program Analysis. QRS2023
- [3] CRust: Towards a Unified Cross-Language Static Analysis Framework For Rust. QRS2022
- [4] Code Duplication Removal in C to Rust Conversion via Unstructured Transfer Specialization. QRS2022



CSS Lab 主页

课题组主页：

<https://csslab-ustc.github.io/>



中国科学技术大学

University of Science and Technology of China

感谢!