

ExaGear: 动态二进制翻译技术原理及应用实践

吕研冬 博士



关注 InfoQ Pro 服务号

你将获得：

- ✓ InfoQ 技术大会讲师 PPT 分享
- ✓ 最新全球 IT 要闻
- ✓ 一线专家实操技术案例
- ✓ InfoQ 精选课程及活动
- ✓ 定期粉丝专属福利活动

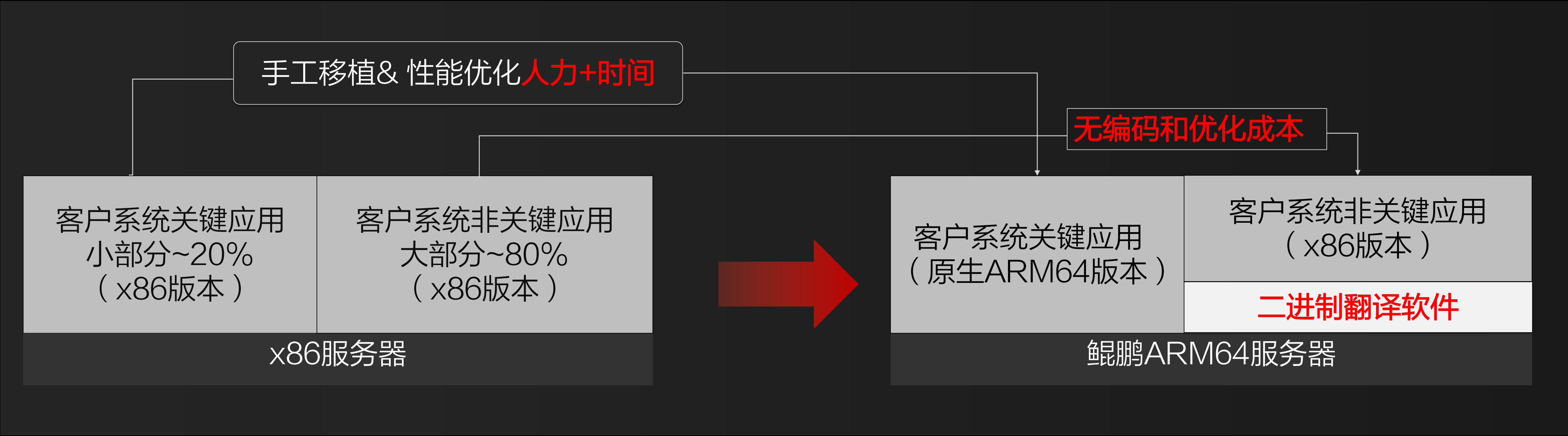
大纲

- 01 动态二进制翻译技术背景
- 02 ExaGear技术解读
- 03 ExaGear性能优化
- 04 ExaGear应用与技术约束
- 05 总结与展望

动态二进制翻译技术协助迁移x86应用到ARM64平台

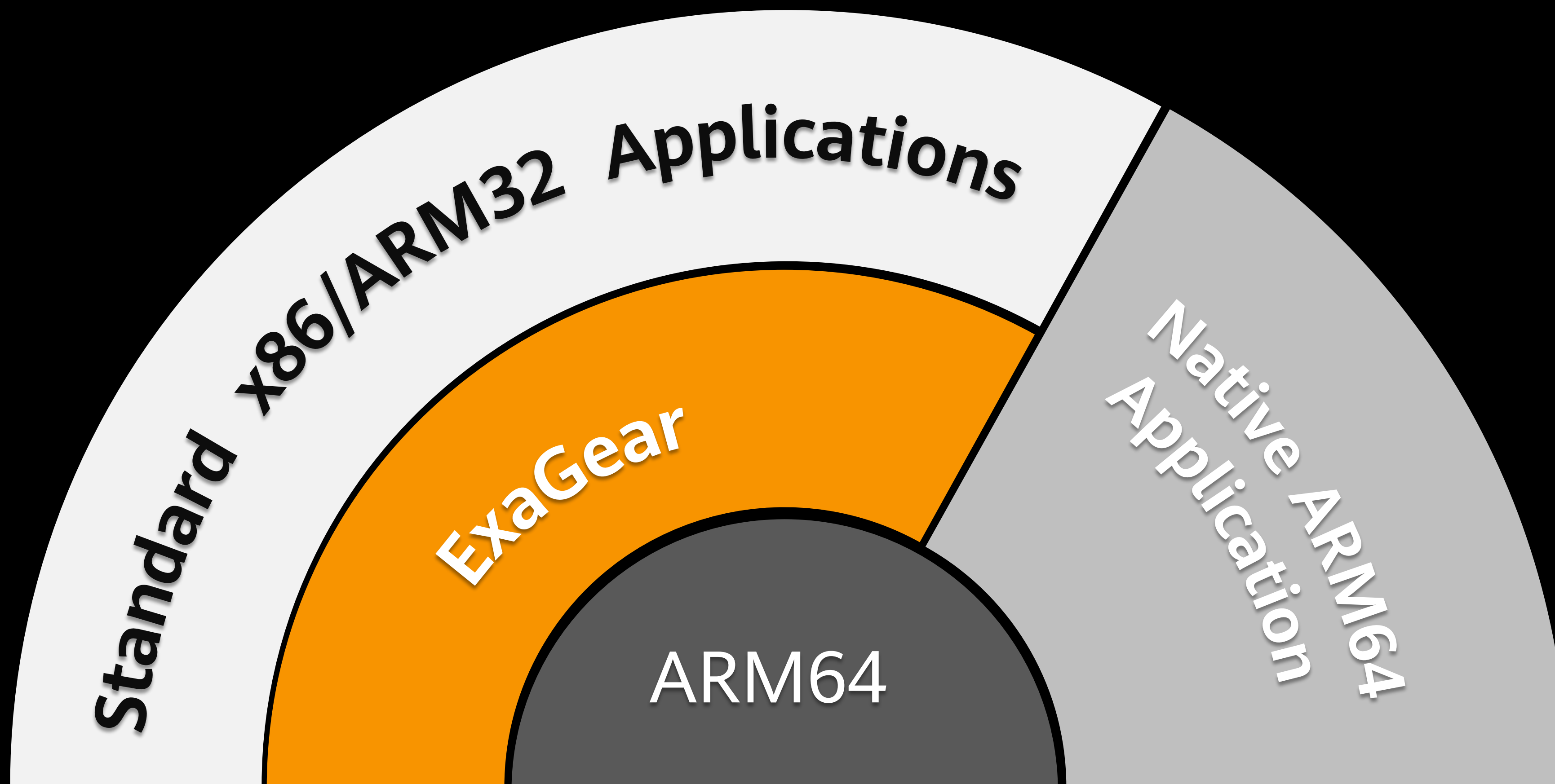
痛点和问题： 客户原有运行在x86上的软件系统无法完整移植到鲲鹏ARM64平台

- 关键应用通过人工移植到ARM server，并且手工优化做到性能最佳，以原生方式运行；
- 系统中还有一定数量既无ARM版本又无源码的非关键软件，则通过指令到指令动态编译的方式，屏蔽底层平台差异性，零成本解决存量应用的平滑迁移，释放鲲鹏平台澎湃算力。



ExaGear是什么?

ExaGear是华为自主可控的动态二进制翻译软件，通过将guest应用的x86(32/64-bit)或ARM32指令翻译成ARM64指令，并模拟guest应用调用的操作系统API，使得Linux x86(32/64-bit)或ARM32的程序可运行在ARM64的服务器上。



二进制翻译是业界解决跨芯片体系软件兼容问题必选方案

| 公司 | Intel | 微软/高通 | Apple | Transmeta |
|----|----------------------------|---|---|--|
| 指令 | ARM → x86 | x86 → ARM64 | x86 → ARM64 | x86 → VLIW |
| 场景 | 解决Intel手机芯片兼容ARM安卓APP运行的问题 | 解决ARM Win10系统的软件生态问题，以二进制翻译的方式兼容海量现存x86软件 | 最新发布的Rosetta 2，协助苹果MacBook完成生态ARM化，打通终端和个人PC的生态融合 | 开发兼容Intel x86的处理器芯片，通过二进制翻译技术支持x86软件执行 |

案例 1：Intel Houdini ARM→x86二进制指令翻译框架

- **场景需求：** Intel移动芯片面临着大量的软件生态挑战，绝大多数安卓应用以及游戏只有ARM版本
- **关键技术：**
 - ARM-to-x86二进制翻译
- **应用效果：**
 - 让Intel x86芯片得以运行为ARM开发的安卓应用
- **现状：** 已在Intel平台手机里正式商用，后因Intel芯片战略调整，x86芯片退出移动市场，该项目未再进一步演进。

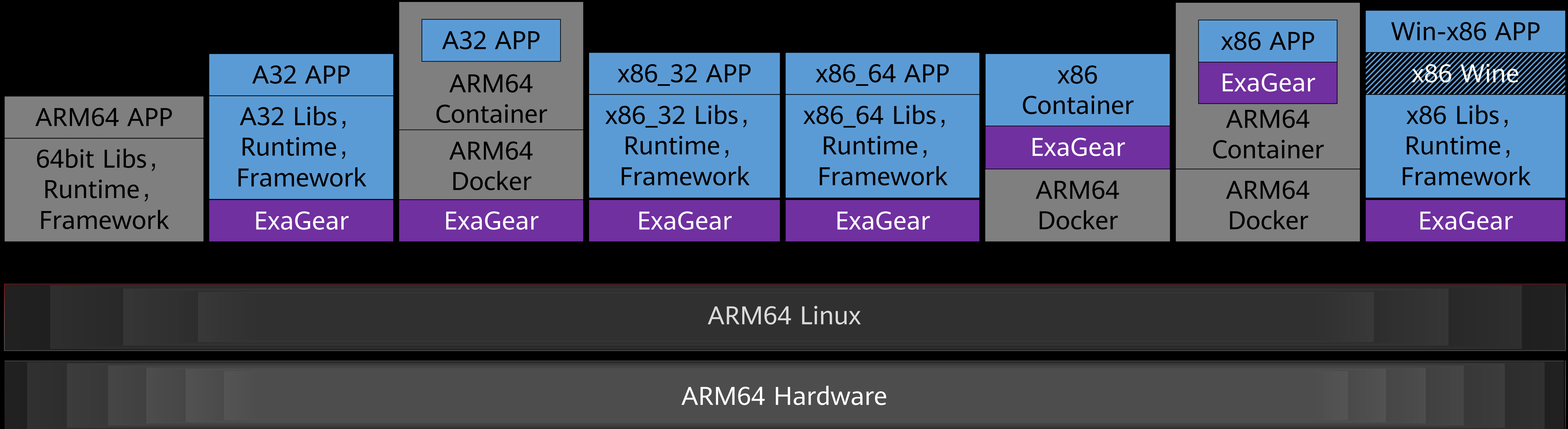
案例 2：微软/高通 Win 10系统x86→ARM方案

- **场景需求：** 将已有的Windows-x86软件生态直接移植到高通的ARM64芯片平台之上
- **关键技术：**
 - x86-to-ARM二进制翻译
- **应用效果：**
 - ARM Win10笔记本可运行大部分32位Windows应用
 - 性能达到原生ARM64应用的约40%-50%
- **现状：** 在Win10 ARM64版本里商用发布，x86_64的应用的支持尚在开发中。

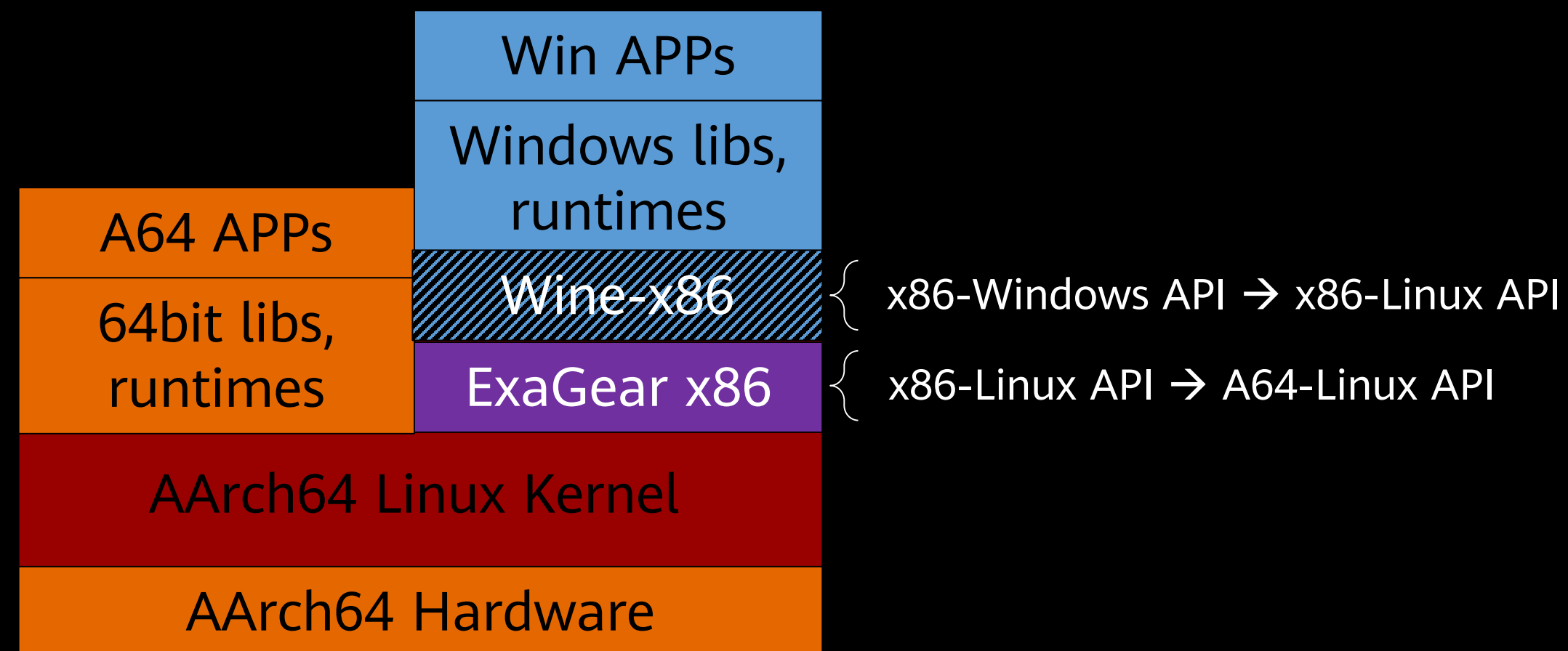


ExaGear 系统上下文 (用户态)

ExaGear是一种“中间件”软件解决方案，位于guest应用程序和ARM Linux OS之间。
ExaGear使用二进制转换技术将guest应用在运行时翻译为AArch64兼容的指令。

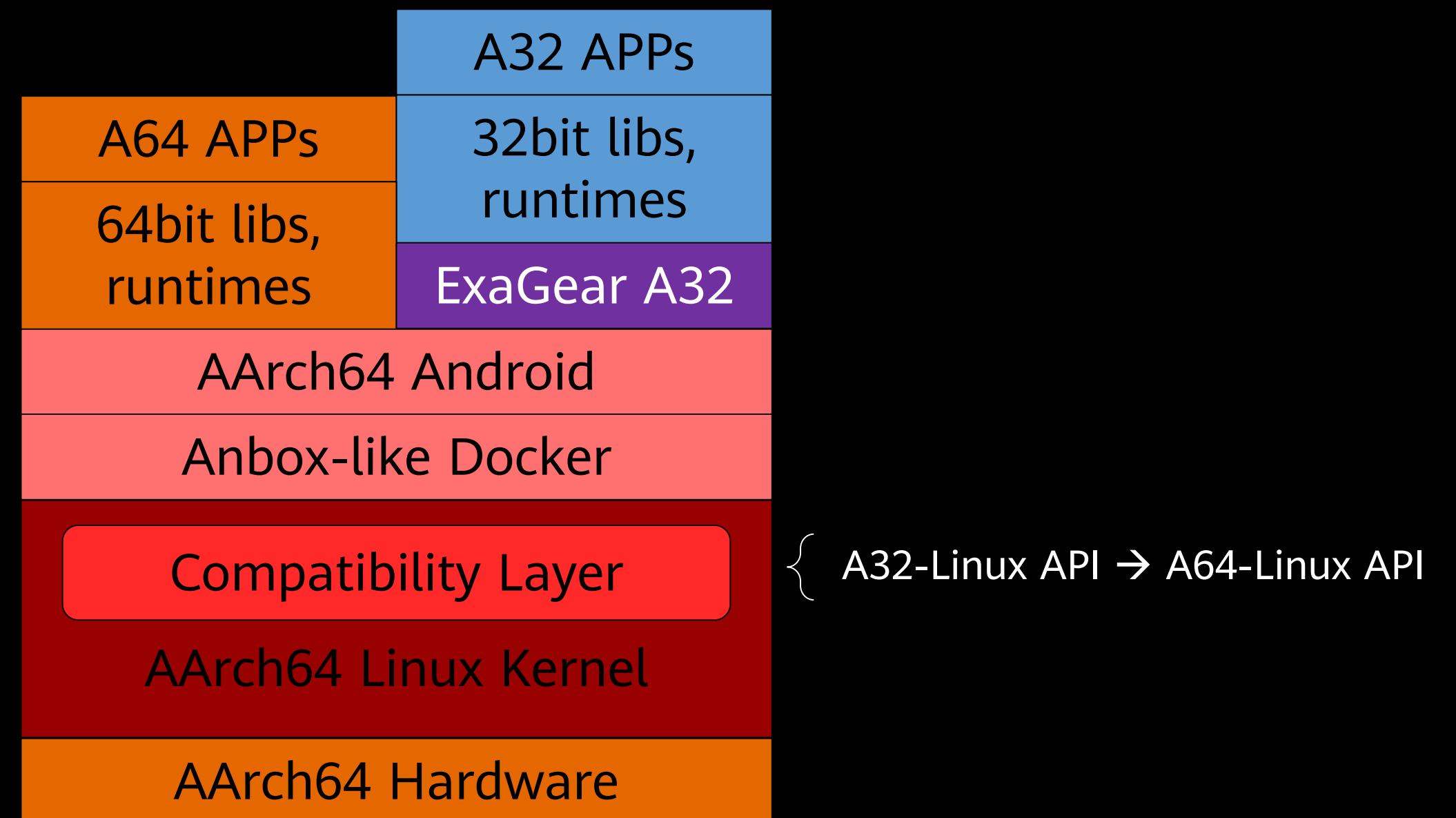


ExaGear 系统上下文实例：Windows 和 Android



ExaGear可以支持Windows应用在AArch64平台上的转码运行。

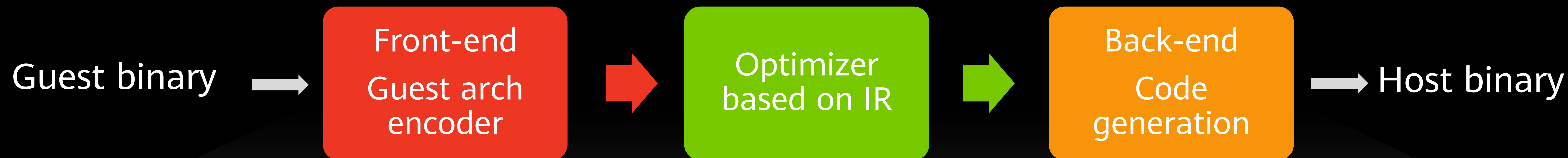
【注】此方案高度依赖Wine，兼容性风险较高，只能针对特定场景解决case by case的应用。ExaGear并不提供Wine组件。



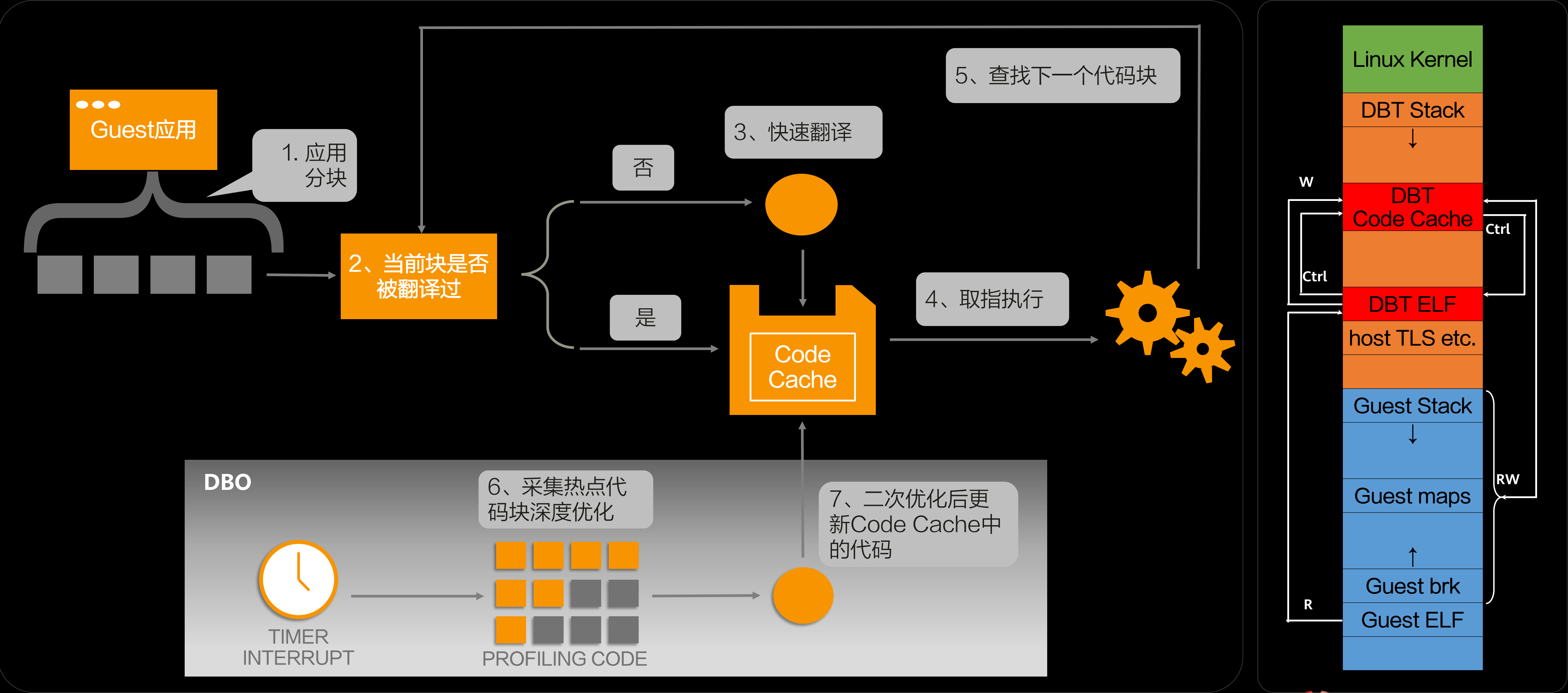
ExaGear可以支持Android应用在AArch64平台上的转码运行。

【注】需要重编译内核使能兼容层

ExaGear是通用的二进制翻译技术



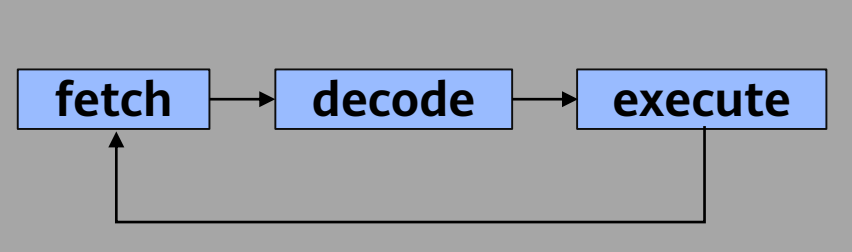
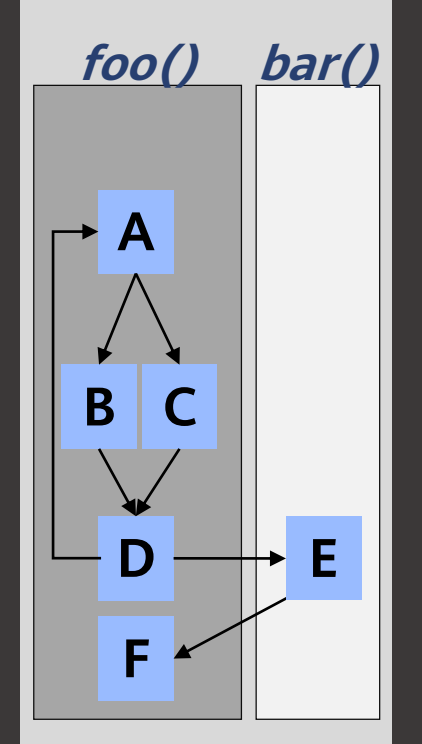
技术框架



技术框架 (2)

Basic interpreter

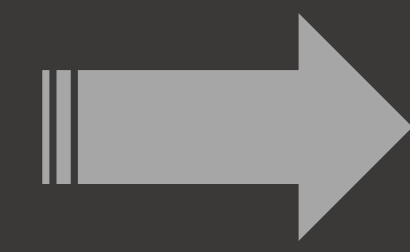
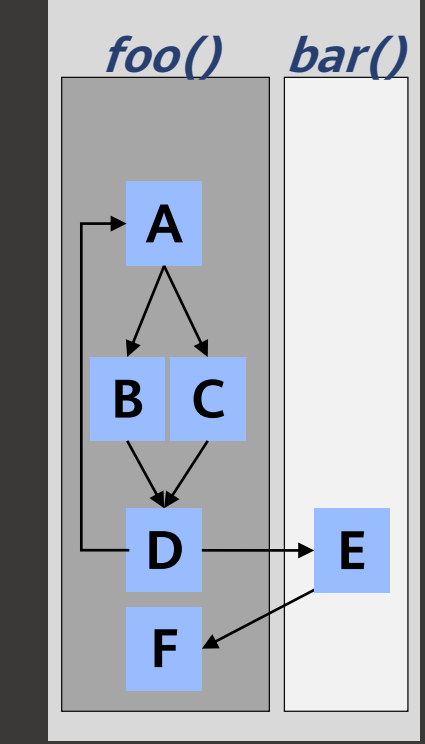
application code



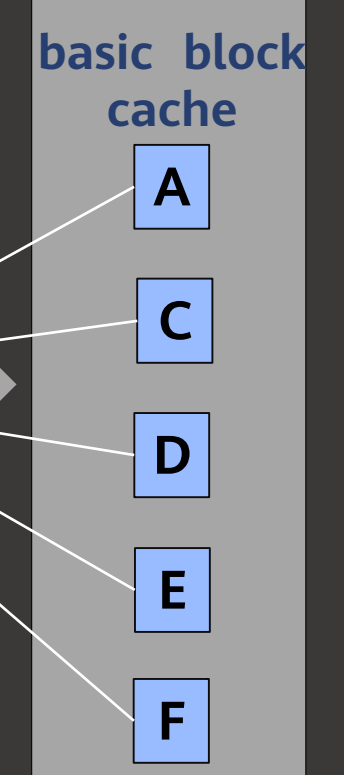
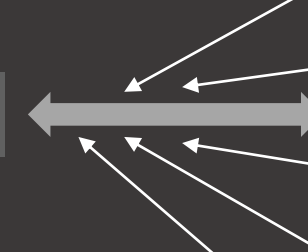
Slowdown: 300x

Improvement #1: Basic Block Cache

application code



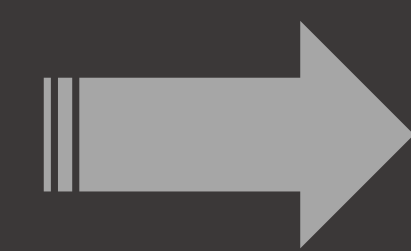
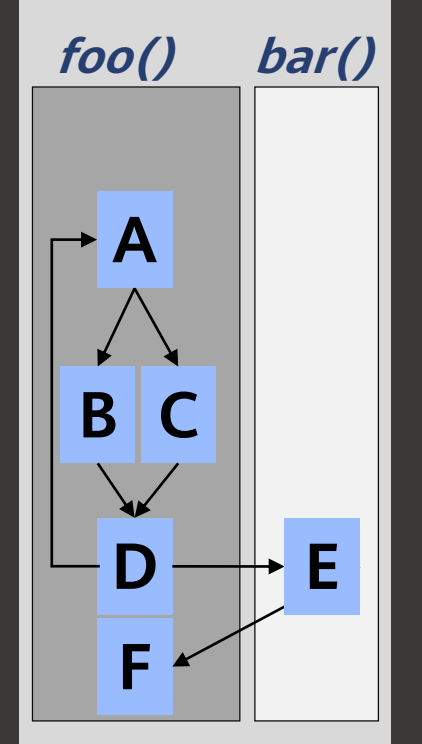
DBT



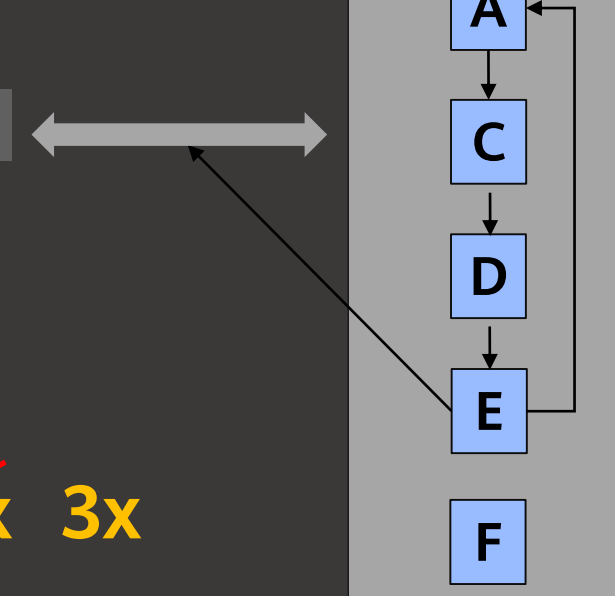
Slowdown: ~~300x~~ 25x

Improvement #2: Linking Direct Branches

application code



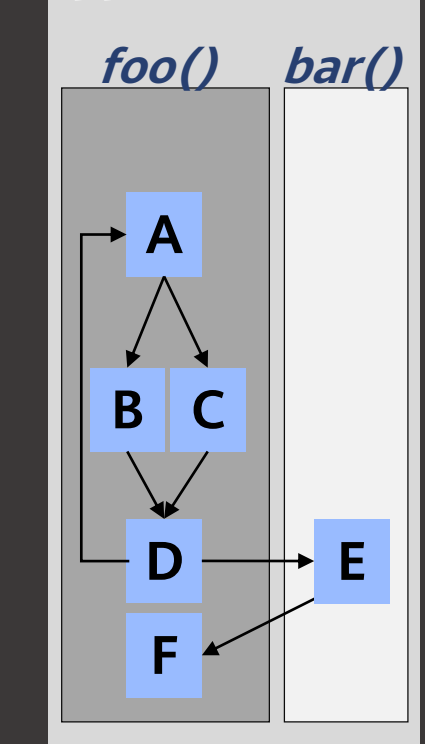
DBT



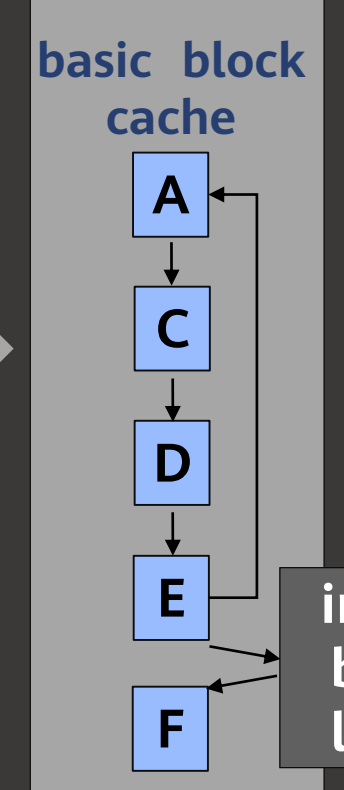
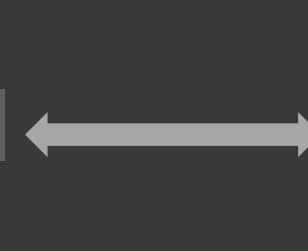
Slowdown: ~~300x~~ ~~25x~~ 3x

Improvement #3: Linking Indirect Branches

application code



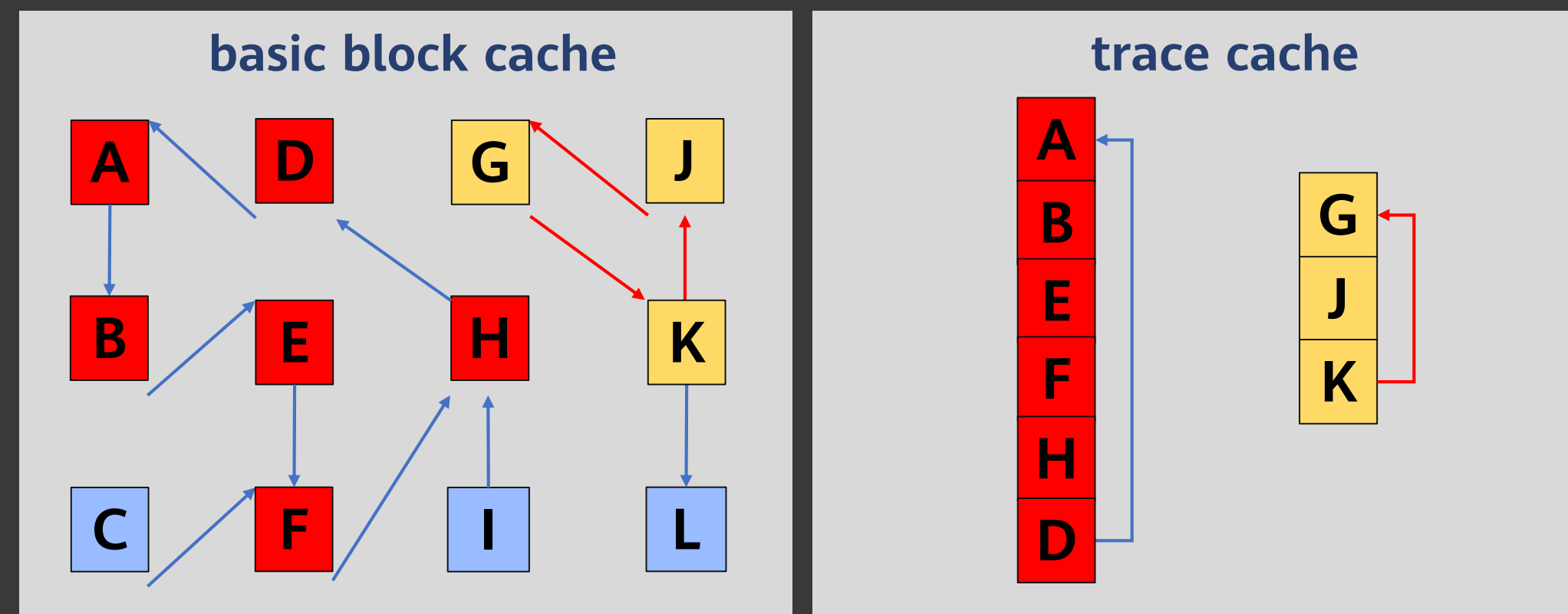
DBT



Slowdown: ~~300x~~ ~~25x~~ ~~3x~~ 1.2x

技术框架（3）

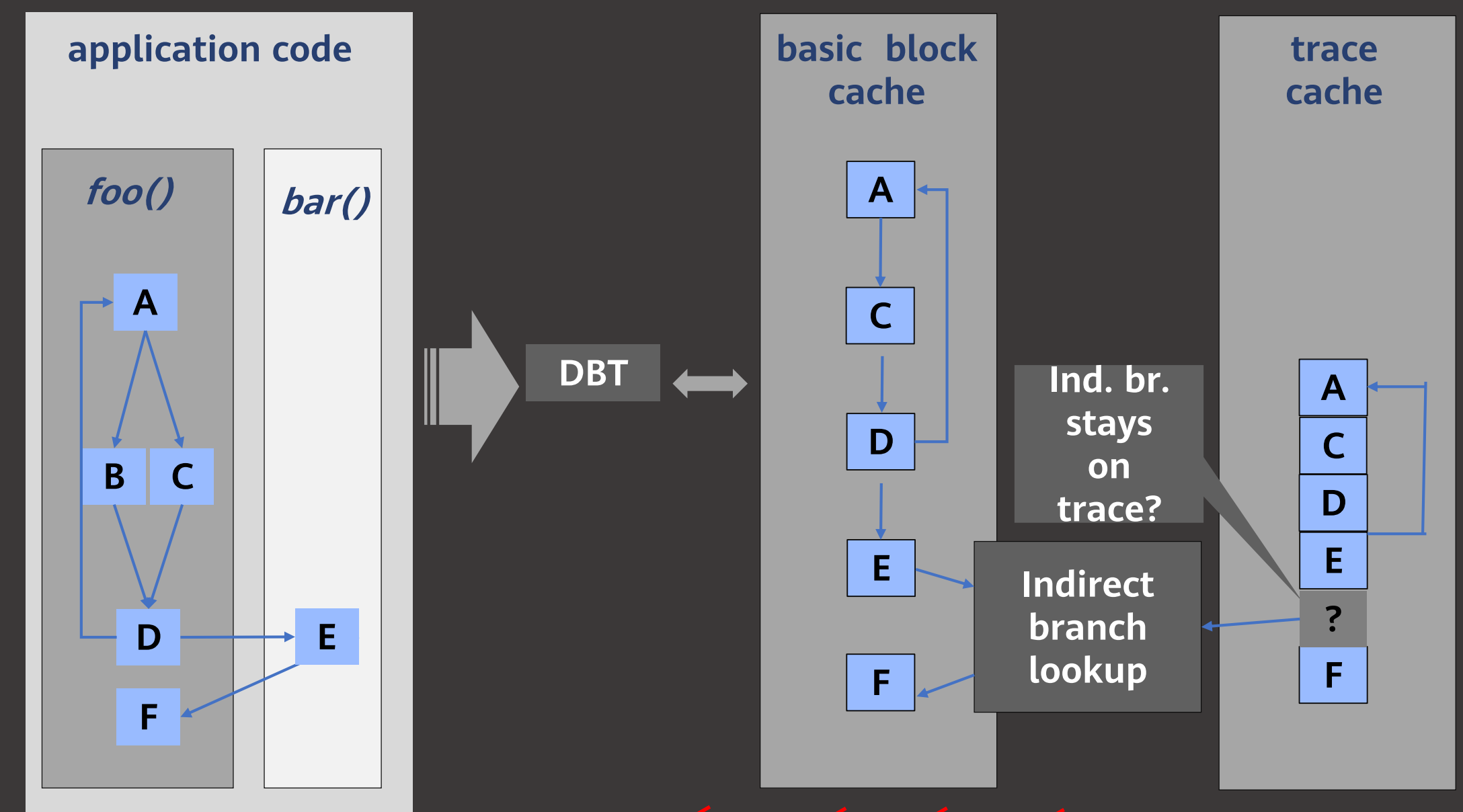
Improvement #4: Trace Building



构建trace可以减少分支个数:

- 改善内存布局和局部性;
- 减少间接跳转查找过程。

Improvement #4: Trace Building

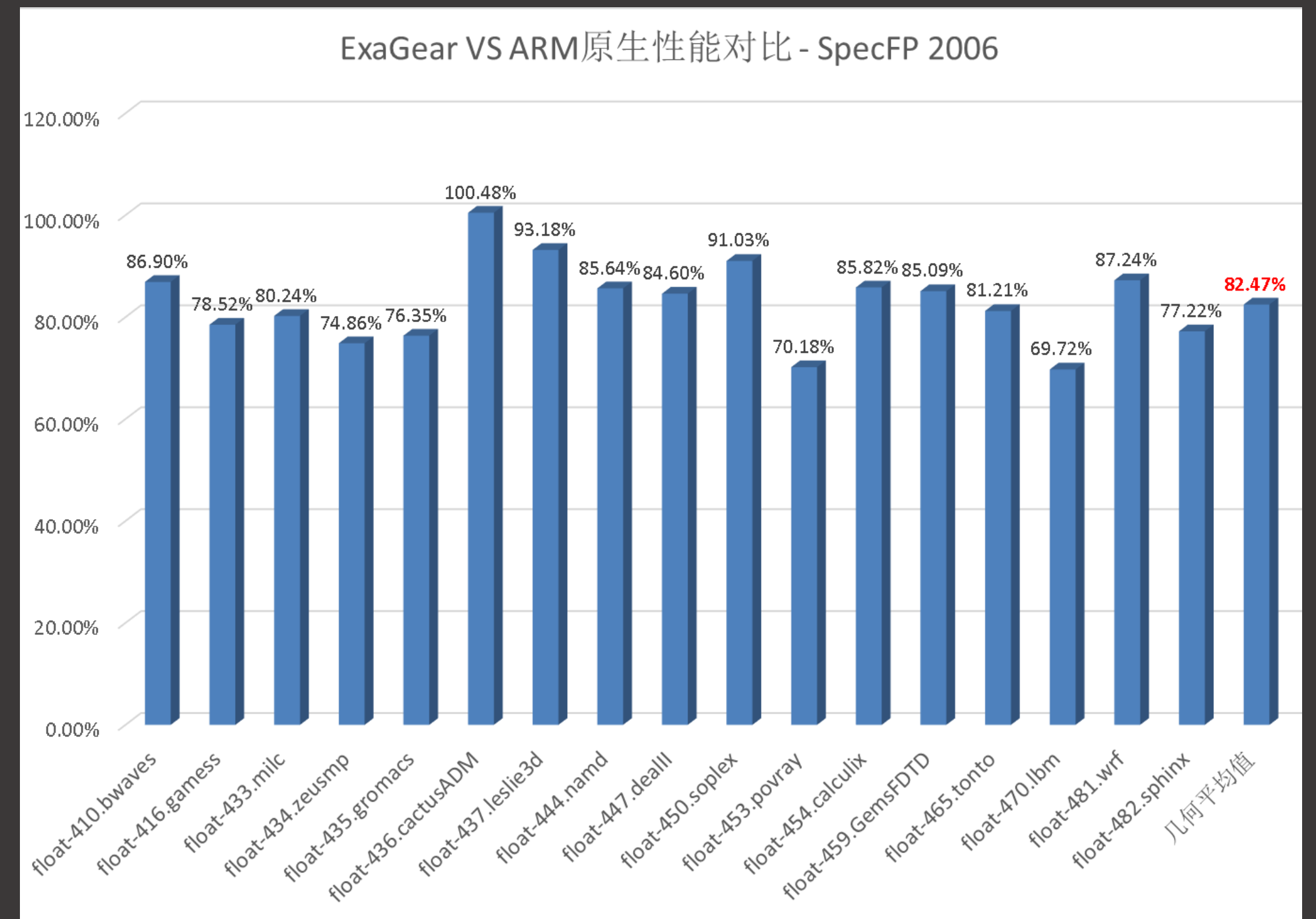
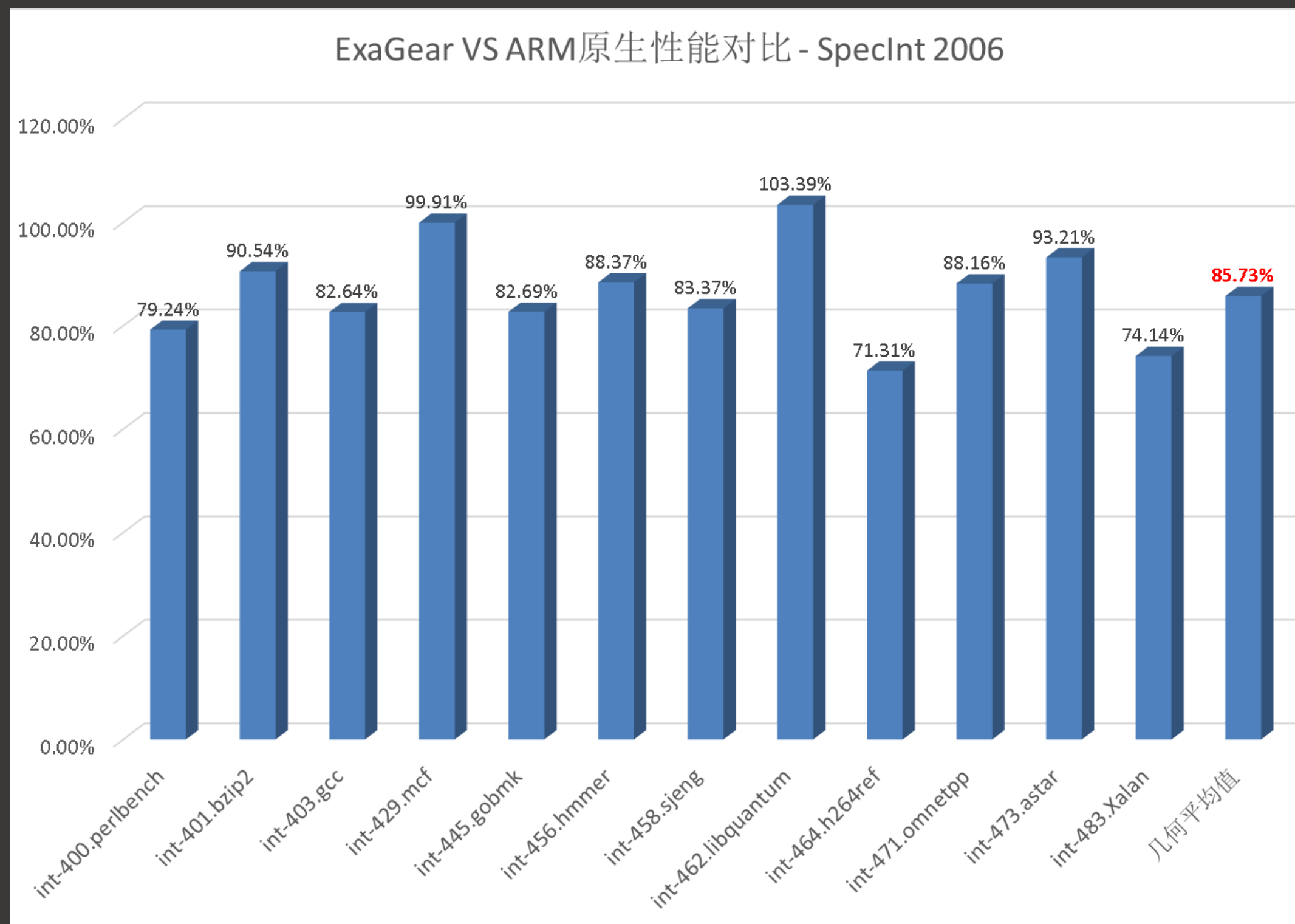


Slowdown: ~~300x~~ ~~25x~~ ~~3x~~ ~~1.2x~~ 1.1x

Ref: CGO 2017 Tutorial: Building Dynamic Tools with DynamoRIO on x86 and ARMv8 <https://dynamorio.org/tutorials/tutorial-cgo17.html>

ExaGear性能

使用Benchmark评测x86的程序经过ExaGear指令翻译的性能与原生AArch64的程序性能对比。
当前在DBO开启的情况下已经优化到AArch64 Native的80%+能力。



ExaGear性能影响及应对

业务场景

无源码存量业务宜采用ExaGear+ 鲲鹏算力；CPU计算密集型不可避免有明显性能损耗，尽量采用源码迁移

- 单线程应用

DBO优化，缩小性能差距；

IO密集型影响较小；

- 多线程应用

充分发挥鲲鹏多核优势，提升端到端性能，抵消转码性能损耗。

技术约束与限制

| 技术限制 Limitation of ExaGear | 限制描述 Limitation description | 支持示例 example of already supported | 不支持示例 example of not yet supported |
|----------------------------------|------------------------------------|--|---|
| | 1) 目前支持基于kernel 3.0+的Linux X86应用。 | 目前聚焦在EulerOS，其他流行的Linux发行版（如Ubuntu，CentOS，Fedora，Suse，Redhat，基于Linux的国产OS）也可以按需集成。 | Windows应用（如Microsoft office），不支持转换。 |
| | 2) 目前仅支持用户态应用，不支持内核态的应用。 | iperf工具，gcc，nginx等 | Linux内核模块(如X86网卡硬件驱动程序) |
| | 3) 目前不支持单独翻译.so库 | 支持进程级的翻译，如主程序+依赖的.so库一起翻译。 | 示例1：Java应用通过ARM上的Java JDK（如openJDK)移植，只翻译JNI.so库 示例2：主程序手动移植到ARM版本，so库仍是x86版本，只翻译.so库。 |
| 技术约束 constraint of ExaGear | 约束描述 constraint description | 支持示例 example of already supported | 不支持示例 example of not yet supported |
| | 1) 指令转换后维持原应用行为逻辑。 | 原应用没有限制使用的CPU数，指令转换后也不限制，可以尽可能多的使用CPU核。 | 如果原应用最大只能使用4个CPU核，指令转换后不能改变可使用的最大CPU核数。 |

总结

ExaGear利用动态二进制翻译技术，结合动态二进制优化能力，能够稳定支持无源码的ARM32和x86存量业务运行在鲲鹏平台上。

性能优越： 目前ExaGear优化水平能够达到业界领先的20%以内性能损耗。

应用建议： 1) 性能不敏感的无源码应用； 2) 无源码多线程业务，充分发挥鲲鹏多核优势，提升整体性能。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home and
organization for a fully connected,
intelligent world.

Copyright©2020 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

Huawei Confidential



QCon+ 案例研习社



扫码学习大厂案例

学习前沿案例，向行业领先迈进

40[↑]

热门专题

—
行业专家把关内容筹备，
助你快速掌握最新技术发展趋势

200[↑]

实战案例

—
了解大厂前沿实战案例，
为 200 个真问题找到最优解

40^场

直播答疑

—
40 位技术大咖，每周分享最新
技术认知，互动答疑

365^天

持续学习

—
视频结合配套 PPT
畅学 365 天