XUANTIE

第4届 2024 RISC-V 中国峰会

QEMU for RISC-V 的整体进展

刘志伟

阿里巴巴达摩院 技术专家

目录

Contents

01

QEMU for RISC-V支持情况

整体进展和推动力量

02

QEMU for RISC-V最新特性介绍

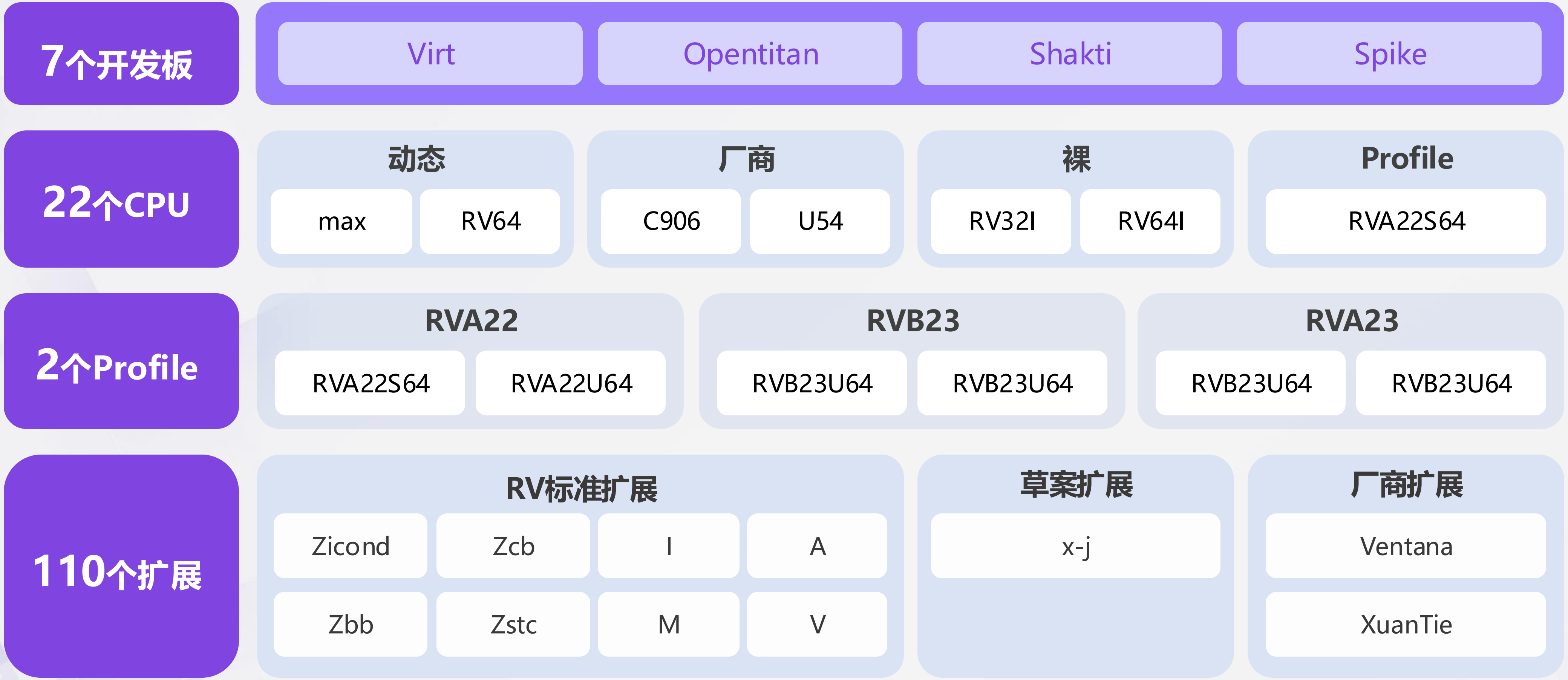
以 Profile 等5个特性为例

03

未来规划和展望

社区未来一年的工作

QEMU 对 RISC-V 的支持概况



7个开发板
- Virt
- Opentitan
- Shakti
- Spike

22个CPU
- 动态: max, RV64
- 厂商: C906, U54
- 裸: RV32I, RV64I
- Profile: RVA22S64

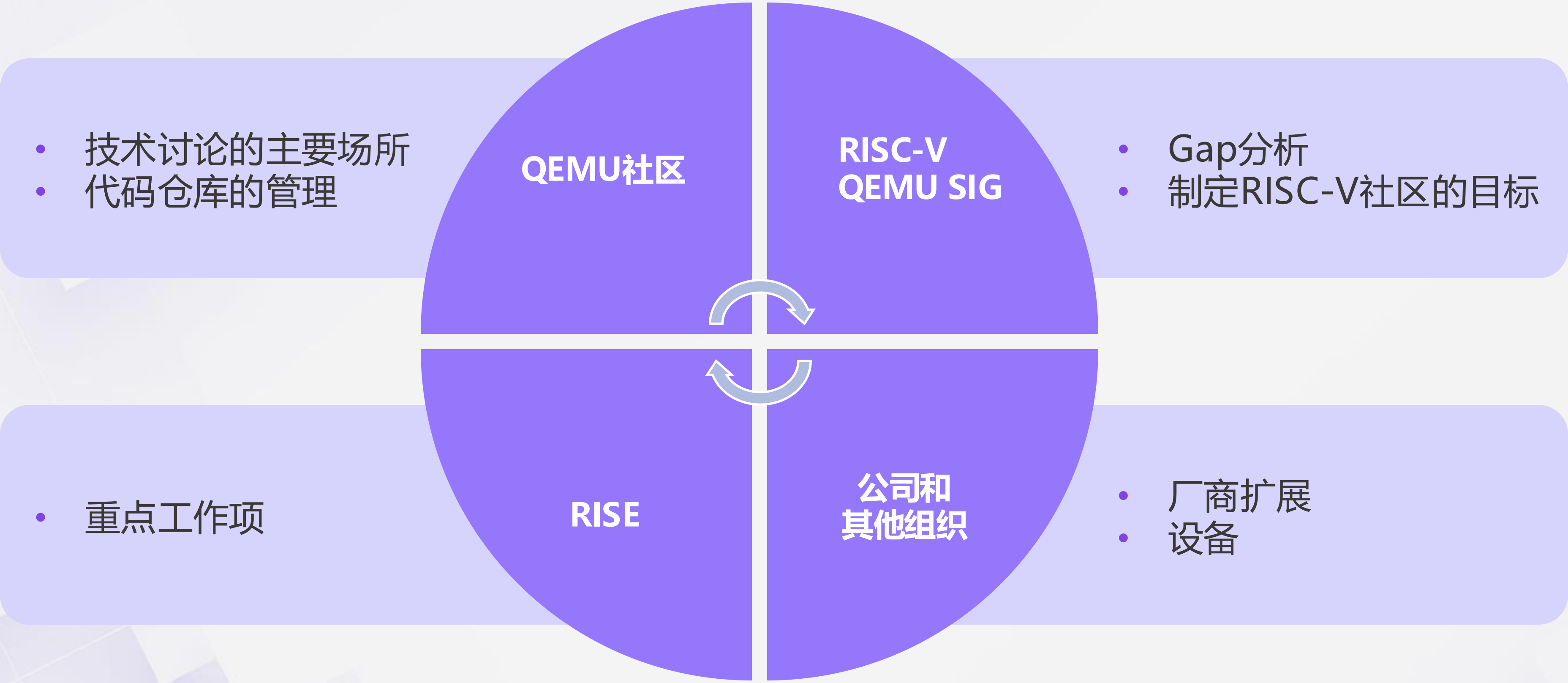
2个Profile
- RVA22: RVA22S64, RVA22U64
- RVB23: RVB23U64, RVB23U64
- RVA23: RVB23U64, RVB23U64

110个扩展
- RV标准扩展: Zicond, Zcb, I, A, Zbb, Zstc, M, V
- 草案扩展: x-j
- 厂商扩展: Ventana, XuanTie

QEMU for RISCV 推动力量

组织协作

社区组织及工作职责



QEMU社区

- 技术讨论的主要场所
- 代码仓库的管理

RISC-V QEMU SIG

- Gap分析
- 制定RISC-V社区的目标

RISE

- 重点工作项

公司和其他组织

- 厂商扩展
- 设备

XUANTIE

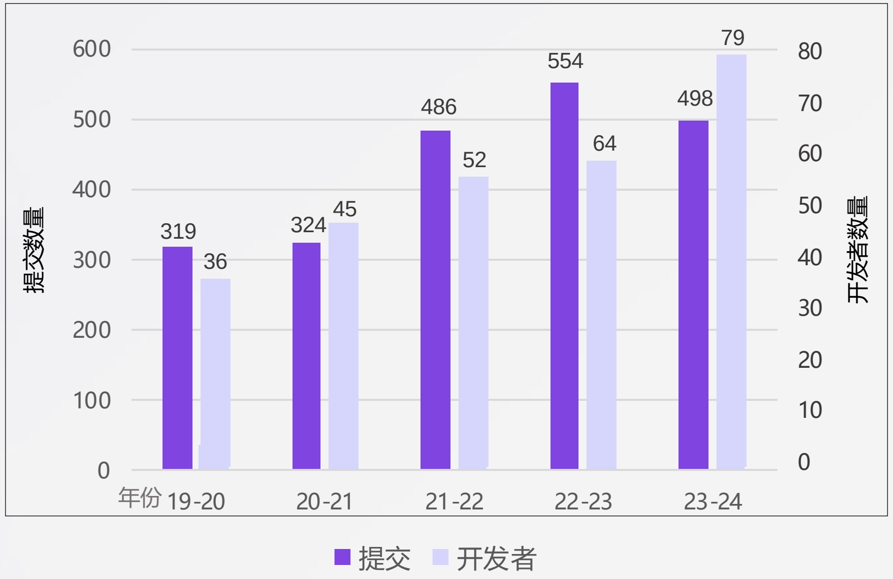
QEMU for RISCV 推动力量

开发者参与情况

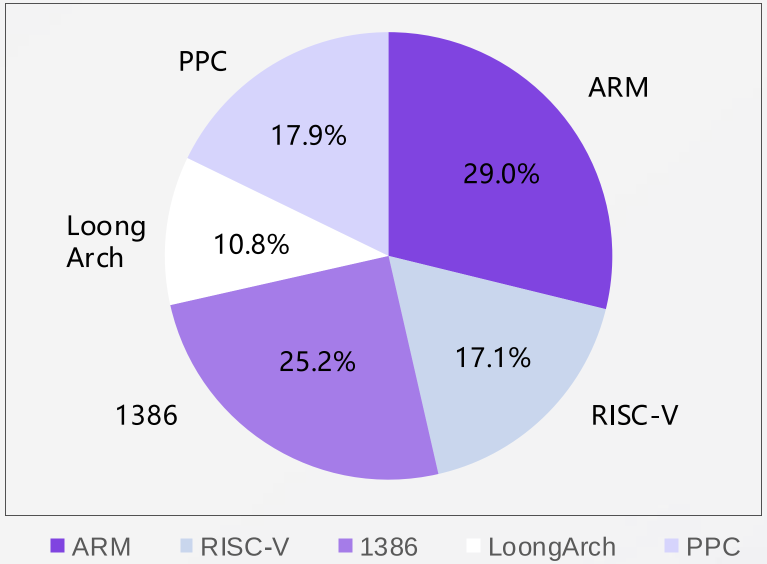
开发活跃度评价

- 提交数
- 评审数
- 开发者数目
- 和其他ARCH的对比
- 历年数据对比

RISC-V年度代码提交和开发者数量



2023-2024年度各架构代码提交占比

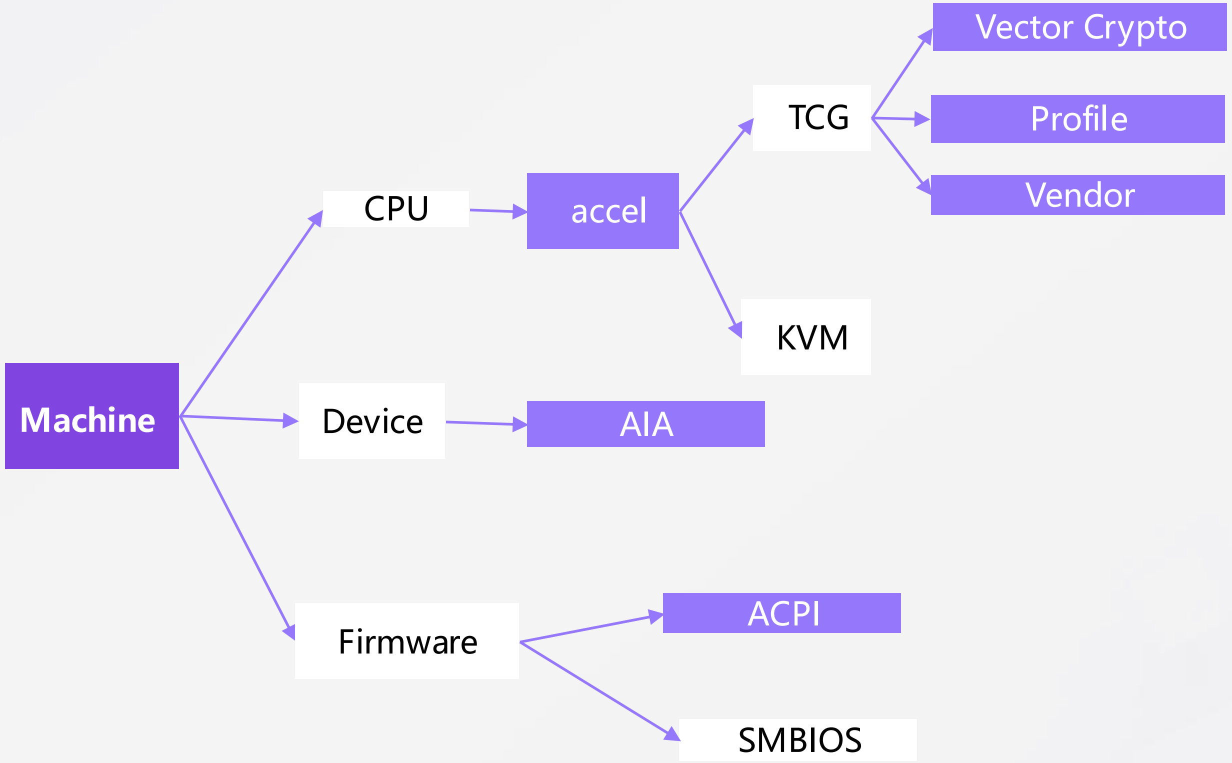


QEMU for RISCV 进展

最近一年合入的重要特性

RISCV架构的工作进展

- 建立Profile支持机制
- 建立加速器机制
- 完善动态XLEN
- 支持Vector crypto，AIA， ACPI等重要扩展
- 在PMU，调试等方面也有了进一步的支持
- 完善了对厂商扩展的支持
- 完善了host探测机制，在后端支持了B扩展

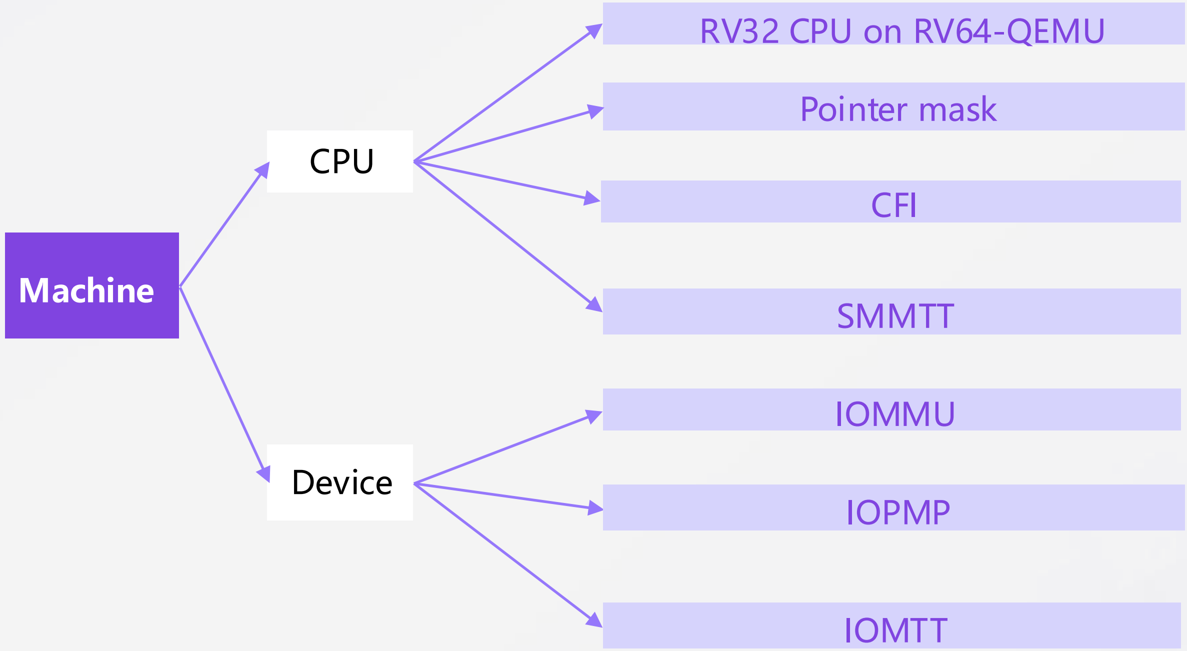


QEMU for RISCV 进展

社区在进行的工作

RISCV架构的工作进展

- 实现IOMMU， IOPMP， 完善对虚拟化的支持
- 实现SMMTT， IOMTT等，支持机密计算
- 实现CFI， Pointer Masking等安全特性
- TCG后端支持Vector



QEMU for RISCV最新特性介绍

Profile机制

Profile的支持

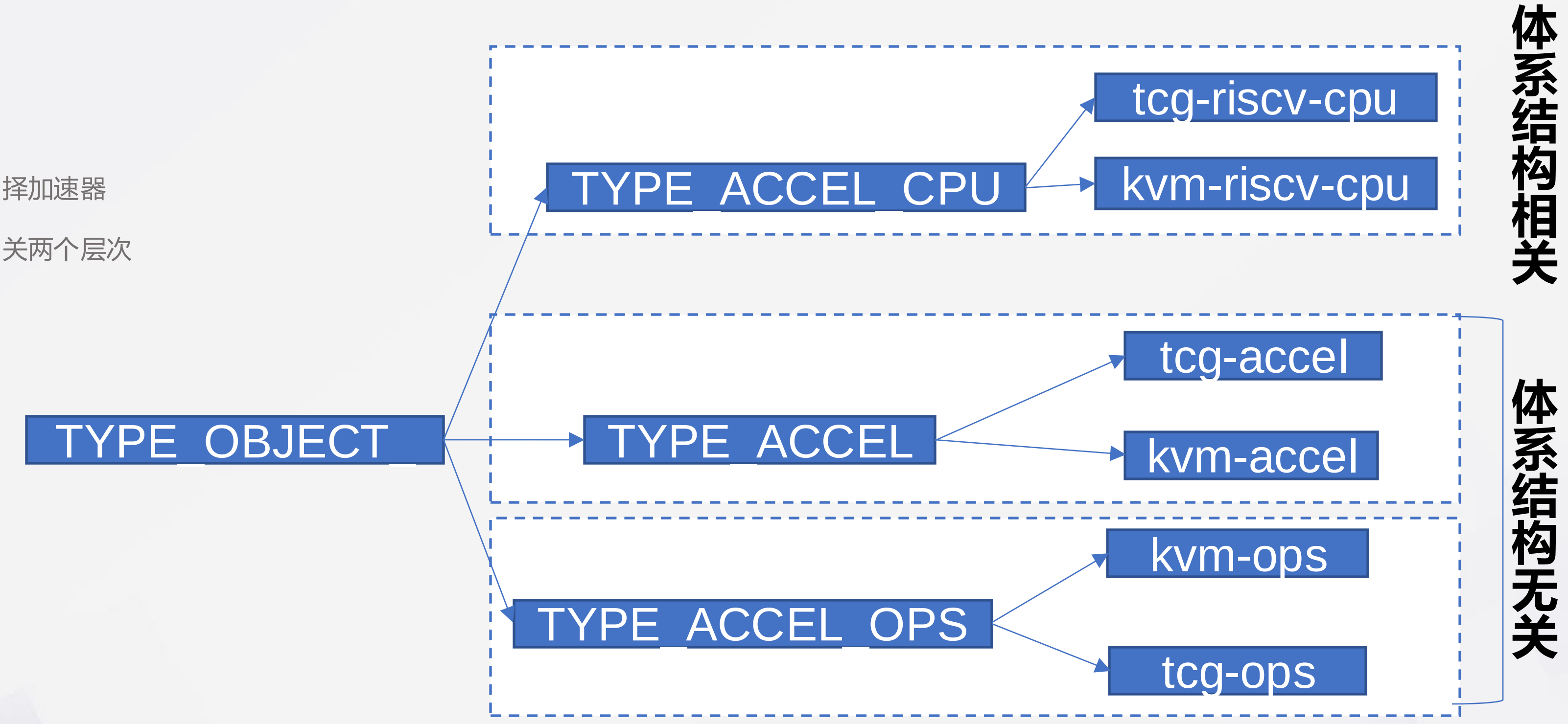
- 特性
  - 可以作为属性存在(-cpu rv64,rva22s64=on)，也可以作为cpu存在(-cpu rva22s64)
  - 只实现强制扩展
  - 支持继承
- 意义
  - 开发者可以聚焦Profile的实现
- 局限
  - 难以被直接使用。可以尝试通过扩展依赖直接打开M态扩展
  - 无法用于厂商CPU的初始化。厂商CPU通常是支持Profile的。

QEMU for RISCV最新特性介绍

加速器机制

加速器机制

- **意义**
  - 保持主干代码的统一， 屏蔽不同加速器的实现差异
  - 提高模块化程度
- **机制**
  - 动态模块加载，根据参数动态选择加速器
  - 体系结构无关提供和体系结构相关两个层次
- **探索方向**
  - 每个CPU子类设计一个加速器



TYPE_OBJECT

TYPE_ACCEL_CPU

tcg-riscv-cpu

kvm-riscv-cpu

体系结构相关

TYPE_ACCEL

tcg-accel

kvm-accel

TYPE_ACCEL_OPS

kvm-ops

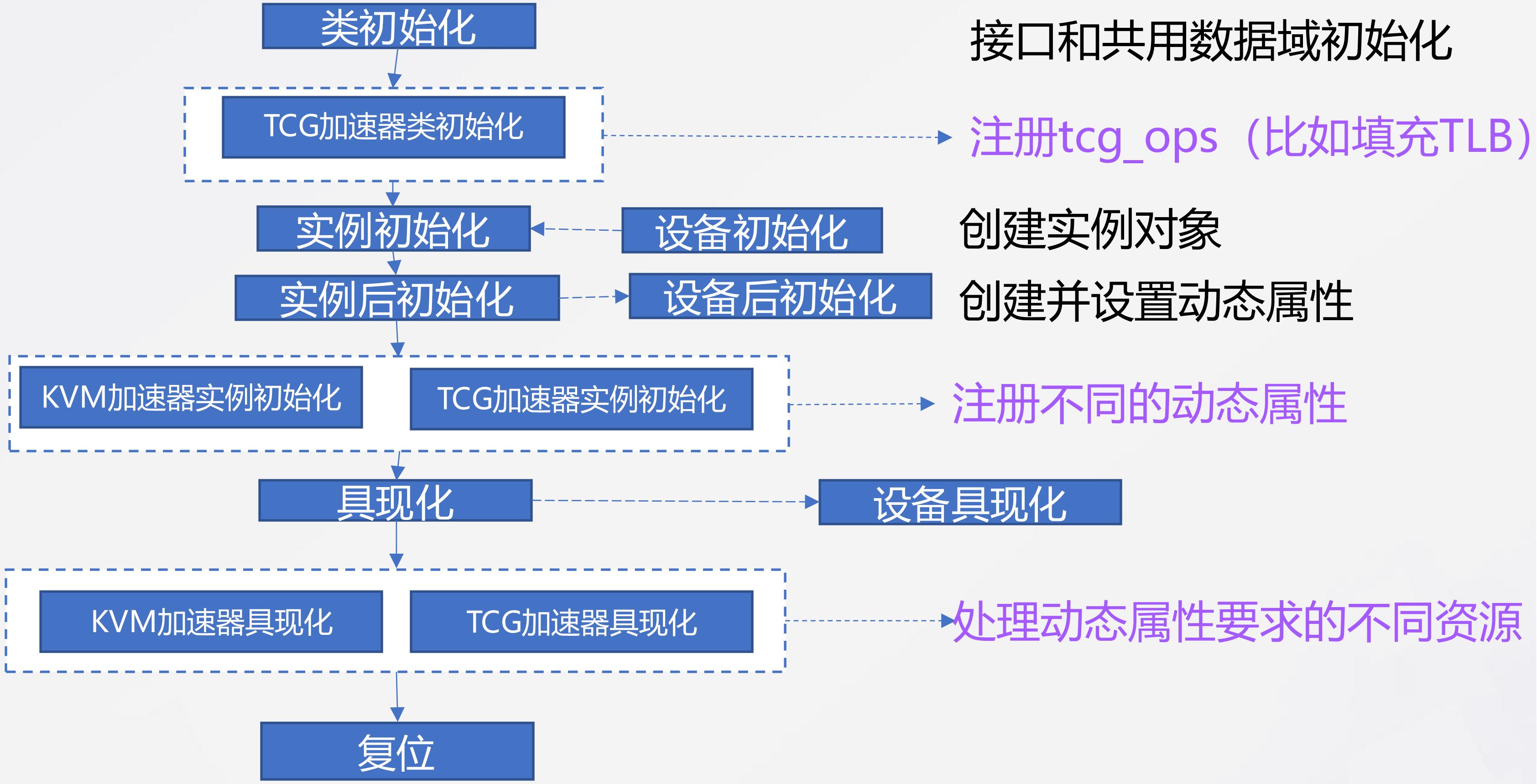
tcg-ops

体系结构无关

QEMU for RISCV最新特性介绍

加速器机制

CPU初始化的中加速器机制

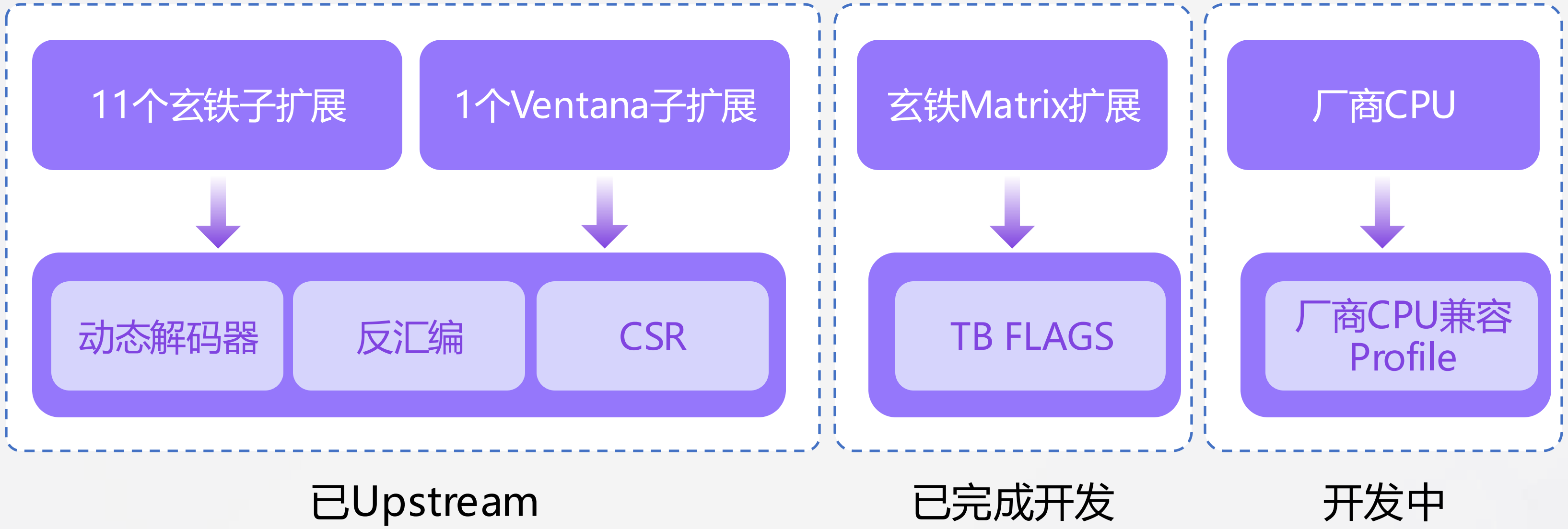


QEMU for RISCV最新特性介绍

厂商扩展支持

自定义扩展的支持框架（XuanTie + Vrull)

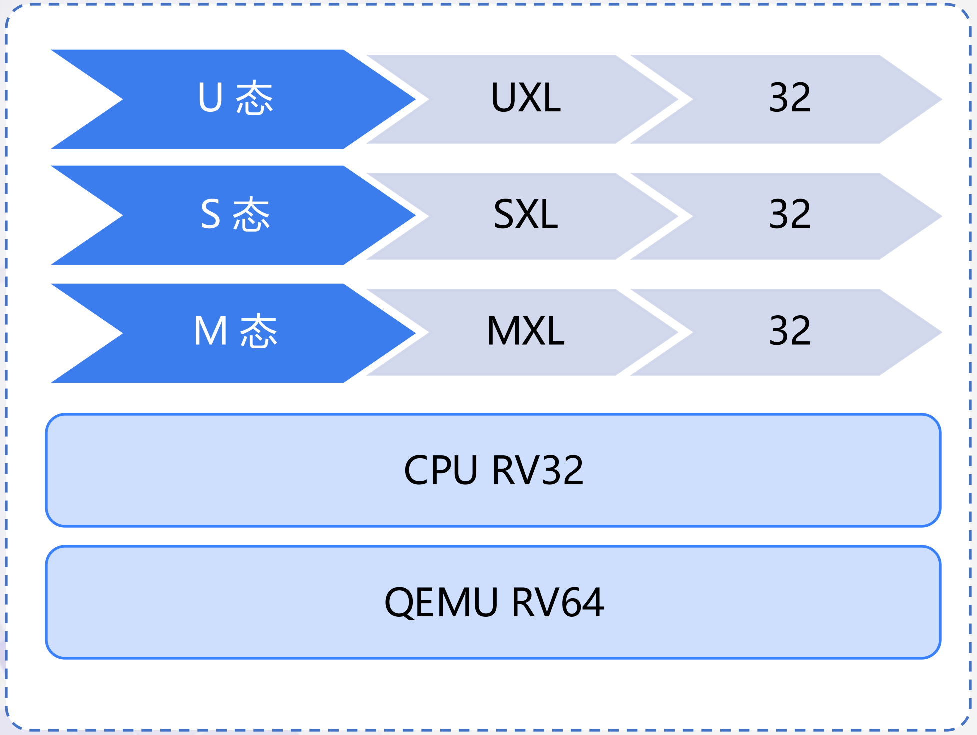
- 自定义扩展指令集解码
- 自定义扩展指令集反汇编支持
- 自定义扩展CSR支持
- 自定义扩展TB FLAGS
- 厂商CPU支持Profile



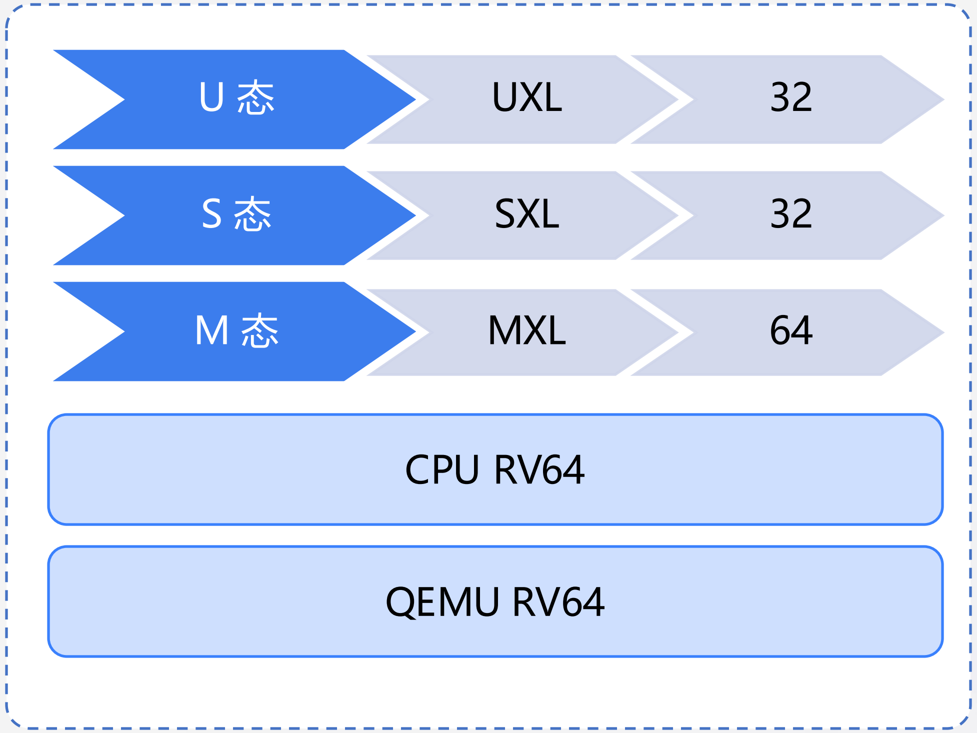
QEMU for RISCV最新特性介绍

动态XLEN支持

RV64 QEMU支持32位CPU

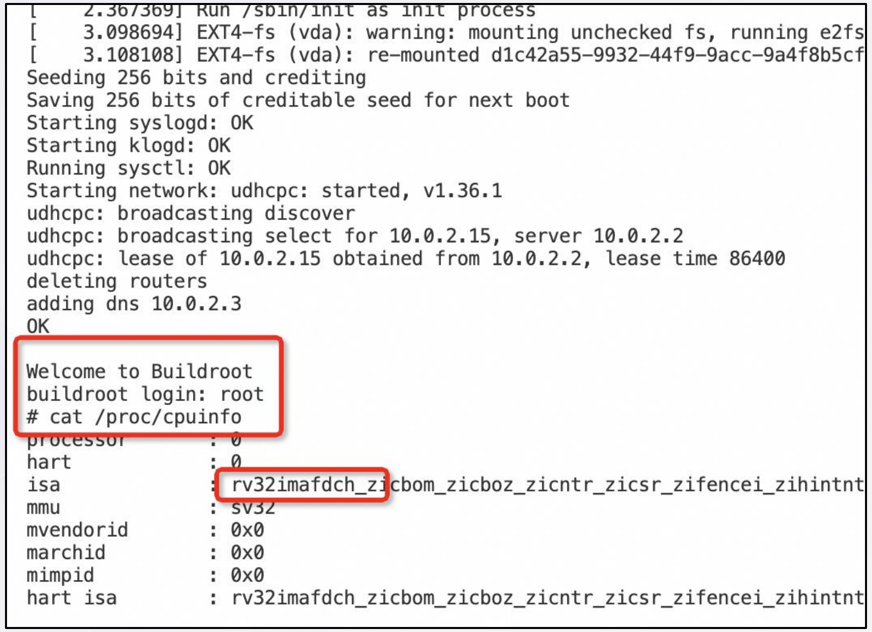


RV64 QEMU支持SXL32

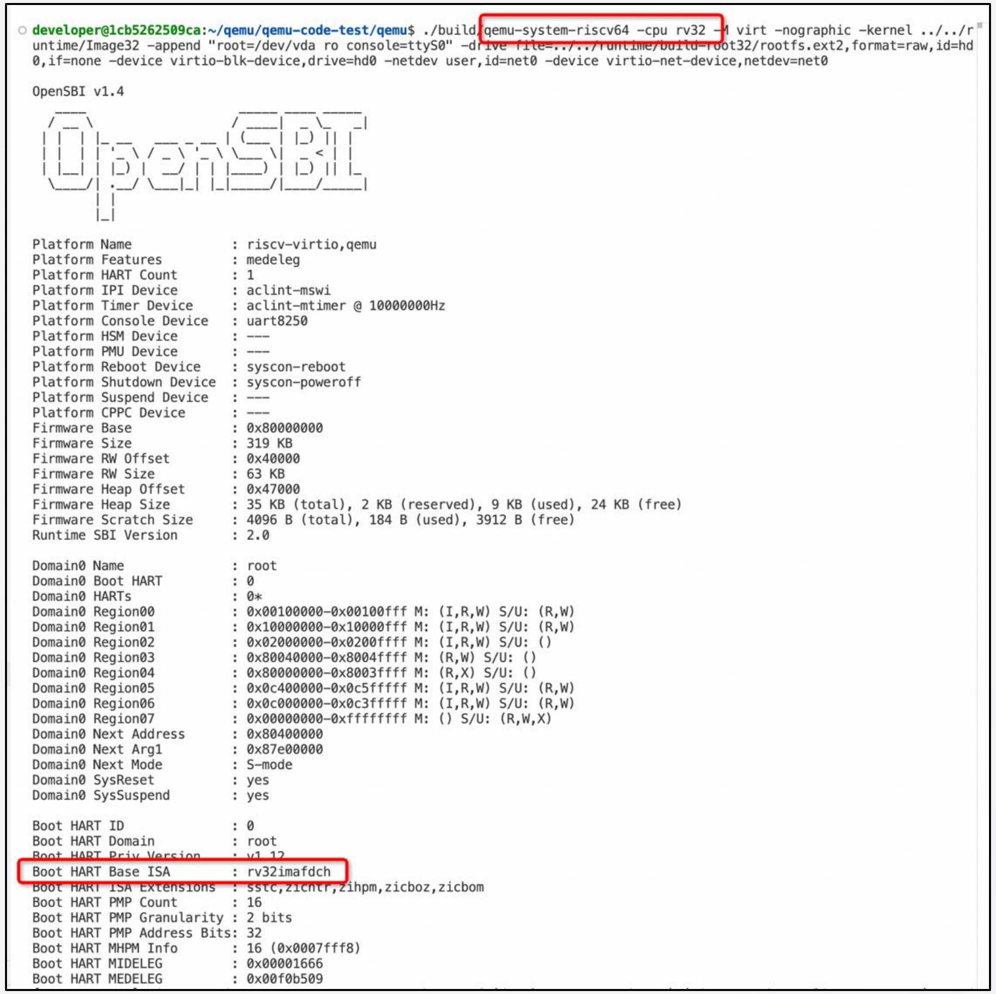


QEMU for RISCV最新特性介绍

RV64 QEMU支持32位CPU



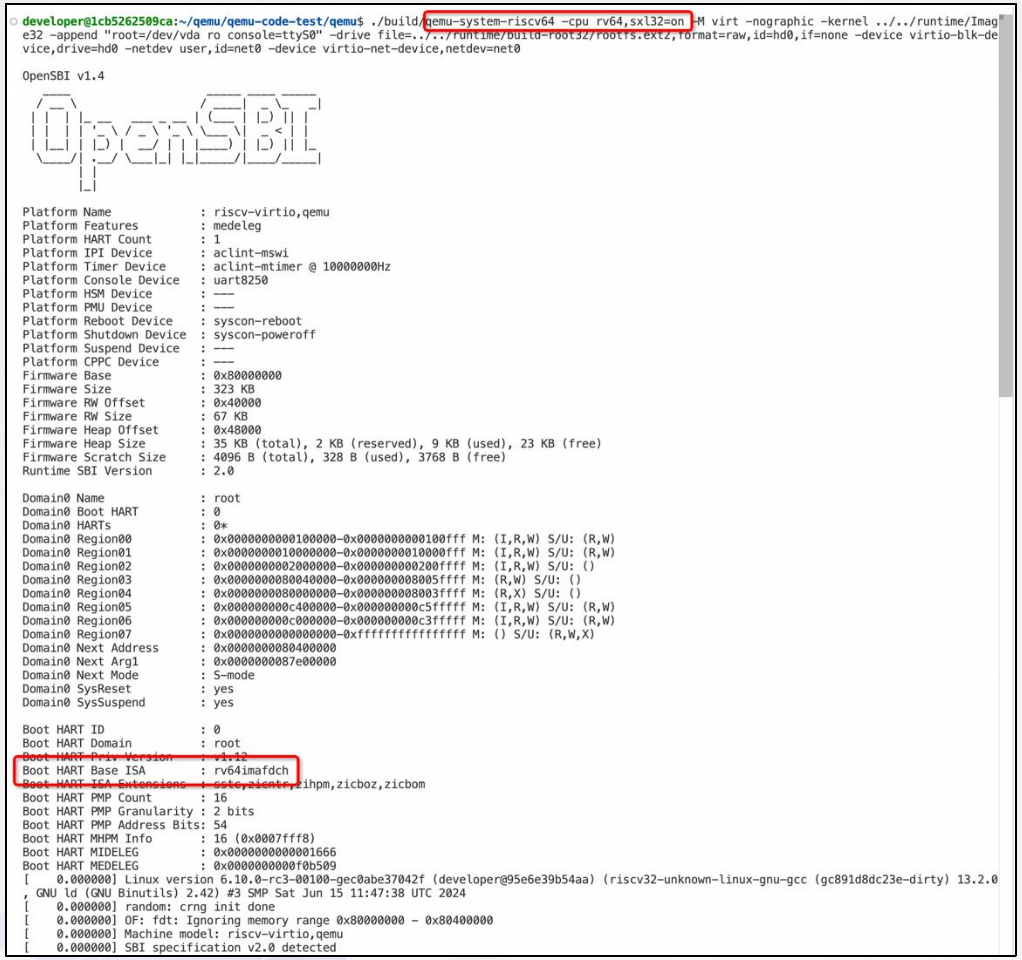
```
[    2.367369] Run /sbin/init as init process
[    3.098694] EXT4-fs (vda): warning: mounting unchecked fs, running e2fs
[    3.108108] EXT4-fs (vda): re-mounted d1c42a55-9932-44f9-9acc-9a4f8b5cf
Seeding 256 bits and crediting
Saving 256 bits of creditable seed for next boot
Starting syslogd: OK
Starting klogd: OK
Running sysctl: OK
Starting network: udhcpc: started, v1.36.1
udhcpc: broadcasting discover
udhcpc: broadcasting select for 10.0.2.15, server 10.0.2.2
udhcpc: lease of 10.0.2.15 obtained from 10.0.2.2, lease time 86400
deleting routers
adding dns 10.0.2.3
OK

Welcome to Buildroot
buildroot login: root
# cat /proc/cpuinfo
processor       : 0
hart            : 0
isa             : rv32imafdch_zicbom_zicboz_zicntr_zicsr_zifencei_zihintnt
mmu             : sv32
mvendorid       : 0x0
marchid         : 0x0
mimpid          : 0x0
hart isa        : rv32imafdch_zicbom_zicboz_zicntr_zicsr_zifencei_zihintnt
```



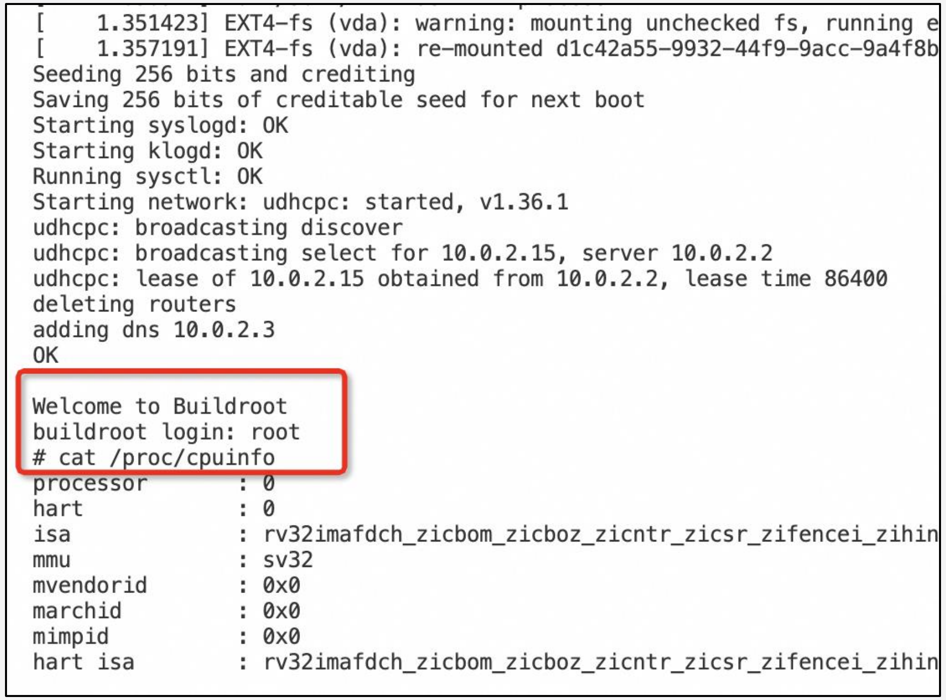
```
developer@1cb5262509ca:~/qemu/qemu-code-test/qemu$ ./build/qemu-system-riscv64 -cpu rv32 -M virt -nographic -kernel ../../r
untime/Image32 -append "root=/dev/vda ro console=ttyS0" -drive file=../../runtime/buildroot32/rootfs.ext2,format=raw,id=hd
0,if=none -device virtio-blk-device,drive=hd0 -netdev user,id=net0 -device virtio-net-device,netdev=net0

OpenSBI v1.4
   ____                    _____ ____ _____
  / __ \                  / ____|  _ \_   _|
 | |  | |_ __   ___ _ __ | (___ | |_) || |
 | |  | | '_ \ / _ \ '_ \ \___ \|  _ < | |
 | |__| | |_) |  __/ | | |____) | |_) || |_
  \____/| .__/ \___|_| |_|_____/|____/_____|
        | |
        |_|

Platform Name             : riscv-virtio,qemu
Platform Features         : medeleg
Platform HART Count       : 1
Platform IPI Device       : aclint-mswi
Platform Timer Device     : aclint-mtimer @ 10000000Hz
Platform Console Device   : uart8250
Platform HSM Device       : ---
Platform PMU Device       : ---
Platform Reboot Device    : syscon-reboot
Platform Shutdown Device  : syscon-poweroff
Platform Suspend Device   : ---
Platform CPPC Device      : ---
Firmware Base             : 0x80000000
Firmware Size             : 319 KB
Firmware RW Offset        : 0x40000
Firmware RW Size          : 63 KB
Firmware Heap Offset      : 0x47000
Firmware Heap Size        : 35 KB (total), 2 KB (reserved), 9 KB (used), 24 KB (free)
Firmware Scratch Size     : 4096 B (total), 184 B (used), 3912 B (free)
Runtime SBI Version       : 2.0

Domain0 Name              : root
Domain0 Boot HART         : 0
Domain0 HARTs             : 0*
Domain0 Region00          : 0x00100000-0x00100fff M: (I,R,W) S/U: (R,W)
Domain0 Region01          : 0x10000000-0x10000fff M: (I,R,W) S/U: (R,W)
Domain0 Region02          : 0x02000000-0x0200ffff M: (I,R,W) S/U: ()
Domain0 Region03          : 0x80040000-0x8004ffff M: (R,W) S/U: ()
Domain0 Region04          : 0x80000000-0x8003ffff M: (R,X) S/U: ()
Domain0 Region05          : 0x0c400000-0x0c5fffff M: (I,R,W) S/U: (R,W)
Domain0 Region06          : 0x0c000000-0x0c3fffff M: (I,R,W) S/U: (R,W)
Domain0 Region07          : 0x00000000-0xffffffff M: () S/U: (R,W,X)
Domain0 Next Address      : 0x80400000
Domain0 Next Arg1         : 0x87e00000
Domain0 Next Mode         : S-mode
Domain0 SysReset          : yes
Domain0 SysSuspend        : yes

Boot HART ID              : 0
Boot HART Domain          : root
Boot HART Priv Version    : v1.12
Boot HART Base ISA        : rv32imafdch
Boot HART ISA Extensions  : sstc,zicntr,zihpm,zicboz,zicbom
Boot HART PMP Count       : 16
Boot HART PMP Granularity : 2 bits
Boot HART PMP Address Bits: 32
Boot HART MHPM Info       : 16 (0x0007fff8)
Boot HART MIDELEG         : 0x00001666
Boot HART MEDELEG         : 0x00f0b509
```

QEMU for RISCV最新特性介绍

SXL32支持



```
developer@1cb5262509ca:~/qemu/qemu-code-test/qemu$ ./build/qemu-system-riscv64 -cpu rv64,sxl32=on -M virt -nographic -kernel ../../runtime/Imag
e32 -append "root=/dev/vda ro console=ttyS0" -drive file=../../runtime/build-root32/rootfs.ext2,format=raw,id=hd0,if=none -device virtio-blk-de
vice,drive=hd0 -netdev user,id=net0 -device virtio-net-device,netdev=net0

OpenSBI v1.4
   ____                    _____ ____ _____
  / __ \                  / ____|  _ \_   _|
 | |  | |_ __   ___ _ __ | (___ | |_) || |
 | |  | | '_ \ / _ \ '_ \ \___ \|  _ < | |
 | |__| | |_) |  __/ | | |____) | |_) || |_
  \____/| .__/ \___|_| |_|_____/|____/_____|
        | |
        |_|

Platform Name             : riscv-virtio,qemu
Platform Features         : medeleg
Platform HART Count       : 1
Platform IPI Device       : aclint-mswi
Platform Timer Device     : aclint-mtimer @ 10000000Hz
Platform Console Device   : uart8250
Platform HSM Device       : ---
Platform PMU Device       : ---
Platform Reboot Device    : syscon-reboot
Platform Shutdown Device  : syscon-poweroff
Platform Suspend Device   : ---
Platform CPPC Device      : ---
Firmware Base             : 0x80000000
Firmware Size             : 323 KB
Firmware RW Offset        : 0x40000
Firmware RW Size          : 67 KB
Firmware Heap Offset      : 0x48000
Firmware Heap Size        : 35 KB (total), 2 KB (reserved), 9 KB (used), 23 KB (free)
Firmware Scratch Size     : 4096 B (total), 328 B (used), 3768 B (free)
Runtime SBI Version       : 2.0

Domain0 Name              : root
Domain0 Boot HART         : 0
Domain0 HARTs             : 0*
Domain0 Region00          : 0x0000000000100000-0x0000000000100fff M: (I,R,W) S/U: (R,W)
Domain0 Region01          : 0x0000000010000000-0x0000000010000fff M: (I,R,W) S/U: (R,W)
Domain0 Region02          : 0x0000000002000000-0x000000000200ffff M: (I,R,W) S/U: ()
Domain0 Region03          : 0x0000000080040000-0x000000008005ffff M: (R,W) S/U: ()
Domain0 Region04          : 0x0000000080000000-0x000000008003ffff M: (R,X) S/U: ()
Domain0 Region05          : 0x000000000c400000-0x000000000c5fffff M: (I,R,W) S/U: (R,W)
Domain0 Region06          : 0x000000000c000000-0x000000000c3fffff M: (I,R,W) S/U: (R,W)
Domain0 Region07          : 0x0000000000000000-0xffffffffffffffff M: () S/U: (R,W,X)
Domain0 Next Address      : 0x0000000080400000
Domain0 Next Arg1         : 0x0000000087e00000
Domain0 Next Mode         : S-mode
Domain0 SysReset          : yes
Domain0 SysSuspend        : yes

Boot HART ID              : 0
Boot HART Domain          : root
Boot HART Priv Version    : v1.12
Boot HART Base ISA        : rv64imafdch
Boot HART ISA Extensions  : sstc,zicntr,zihpm,zicboz,zicbom
Boot HART PMP Count       : 16
Boot HART PMP Granularity : 2 bits
Boot HART PMP Address Bits: 54
Boot HART MHPM Info       : 16 (0x0007fff8)
Boot HART MIDELEG         : 0x0000000000001666
Boot HART MEDELEG         : 0x0000000000f0b509
[    0.000000] Linux version 6.10.0-rc3-00100-gec0abe37042f (developer@95e6e39b54aa) (riscv32-unknown-linux-gnu-gcc (gc891d8dc23e-dirty) 13.2.0
, GNU ld (GNU Binutils) 2.42) #3 SMP Sat Jun 15 11:47:38 UTC 2024
[    0.000000] random: crng init done
[    0.000000] OF: fdt: Ignoring memory range 0x80000000 - 0x80400000
[    0.000000] Machine model: riscv-virtio,qemu
[    0.000000] SBI specification v2.0 detected
```



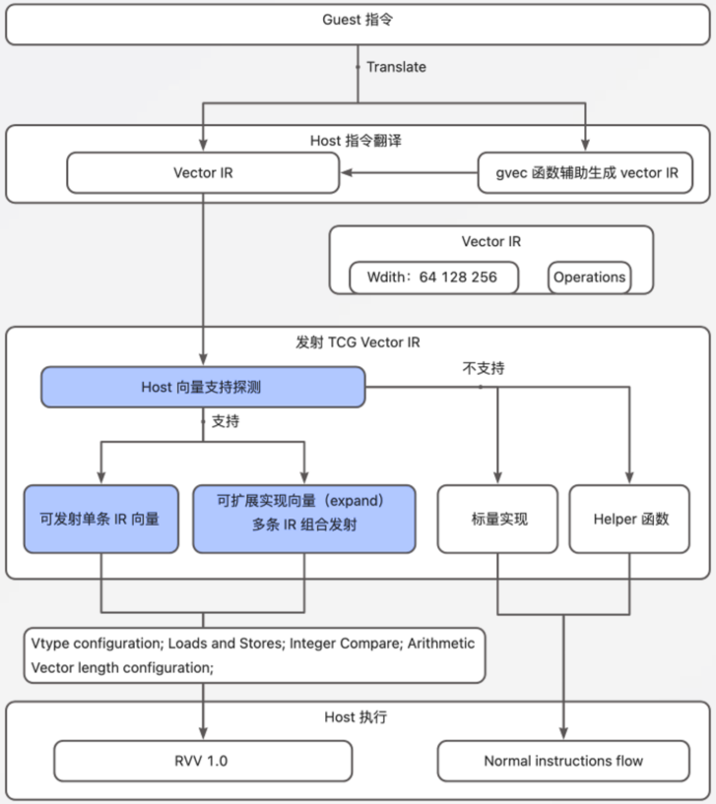
```
[    1.351423] EXT4-fs (vda): warning: mounting unchecked fs, running e
[    1.357191] EXT4-fs (vda): re-mounted d1c42a55-9932-44f9-9acc-9a4f8b
Seeding 256 bits and crediting
Saving 256 bits of creditable seed for next boot
Starting syslogd: OK
Starting klogd: OK
Running sysctl: OK
Starting network: udhcpc: started, v1.36.1
udhcpc: broadcasting discover
udhcpc: broadcasting select for 10.0.2.15, server 10.0.2.2
udhcpc: lease of 10.0.2.15 obtained from 10.0.2.2, lease time 86400
deleting routers
adding dns 10.0.2.3
OK

Welcome to Buildroot
buildroot login: root
# cat /proc/cpuinfo
processor       : 0
hart            : 0
isa             : rv32imafdch_zicbom_zicboz_zicntr_zicsr_zifencei_zihin
mmu             : sv32
mvendorid       : 0x0
marchid         : 0x0
mimpid          : 0x0
hart isa        : rv32imafdch_zicbom_zicboz_zicntr_zicsr_zifencei_zihin
```

QEMU for RISCV最新特性介绍

TCG后端支持RVV

TCG后端支持RVV (XuanTie + PLCT)

- RVV的标准实现及社区进展

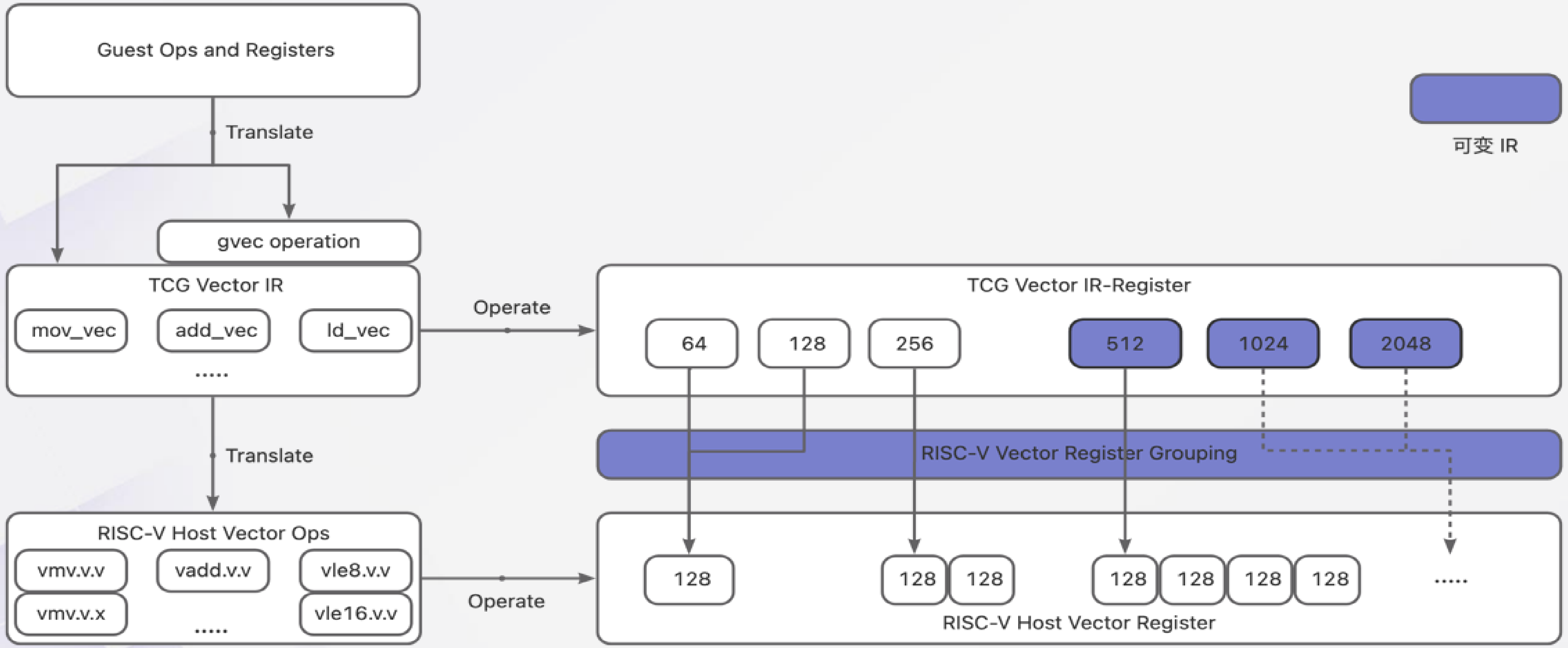


QEMU for RISCV最新特性介绍

TCG后端支持RVV

可变IR设计

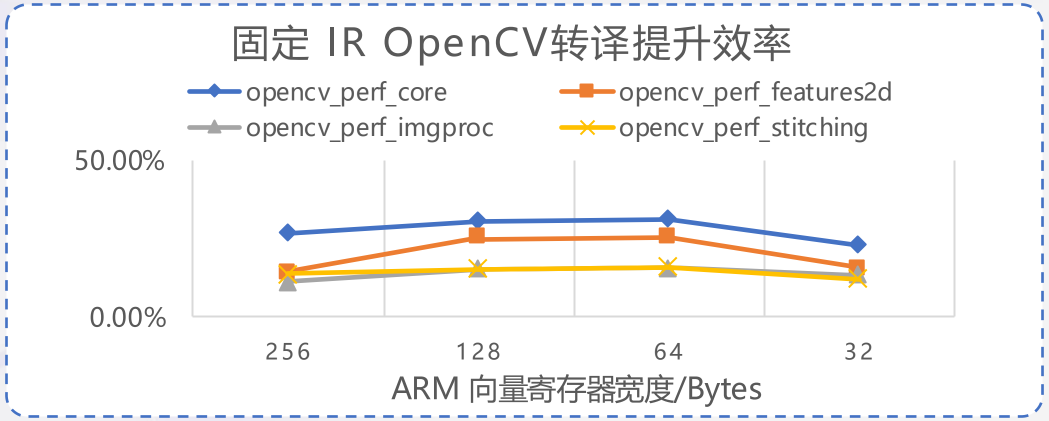
- RISC-V 支持 Vector Register Grouping，将多个向量寄存器组合成一个寄存器组，以支持更宽的向量运算。

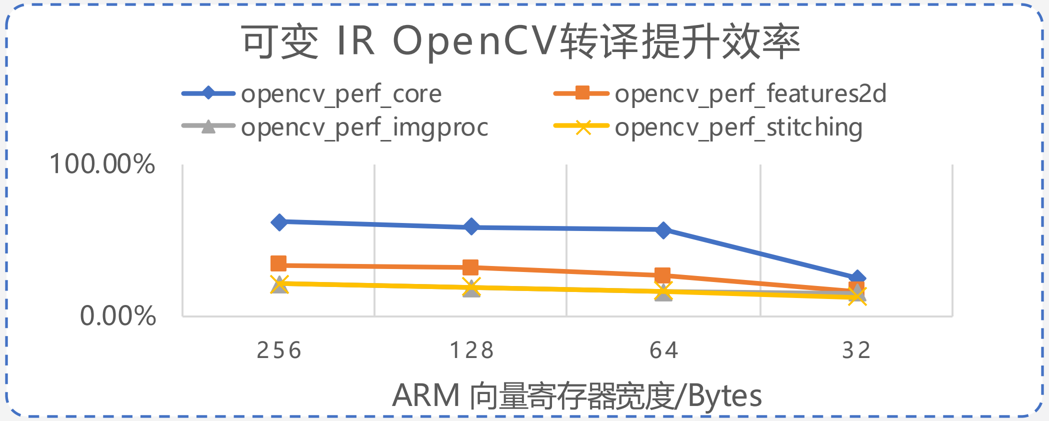


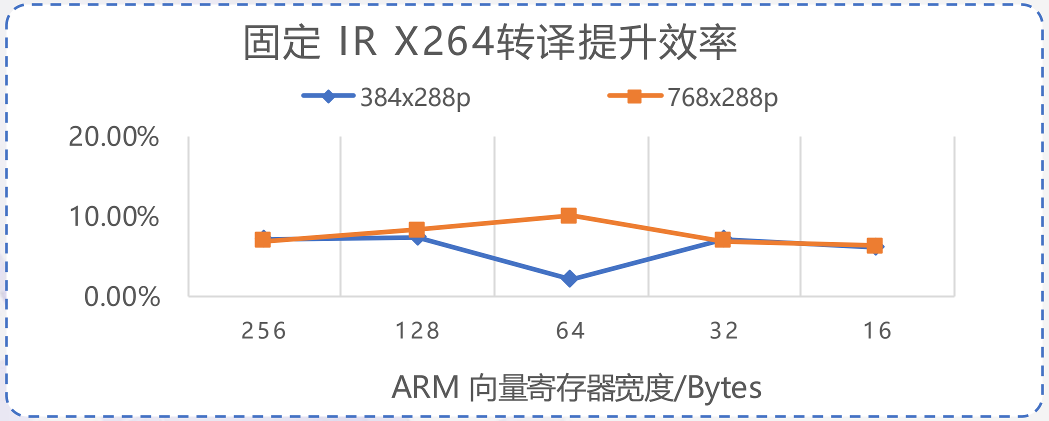
QEMU for RISCV最新特性介绍

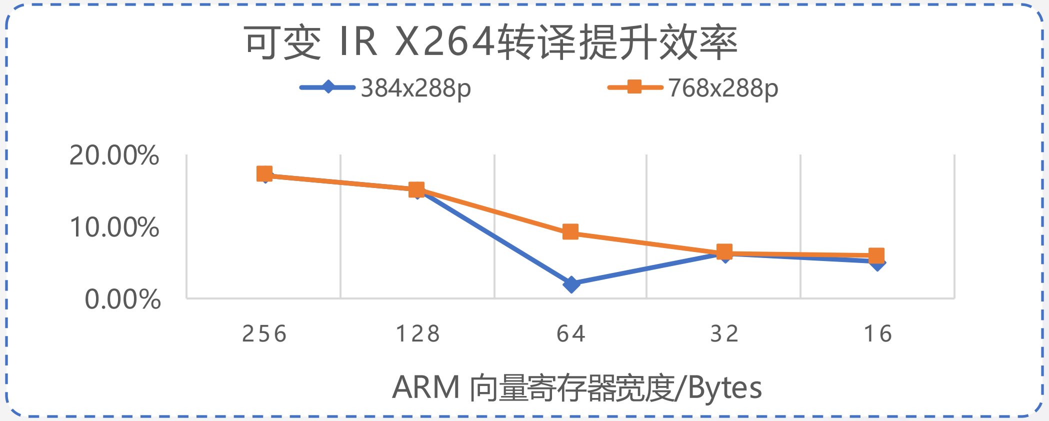
TCG后端支持RVV

RVV支持对转译效率的提升


固定 IR OpenCV转译提升效率


可变 IR OpenCV转译提升效率

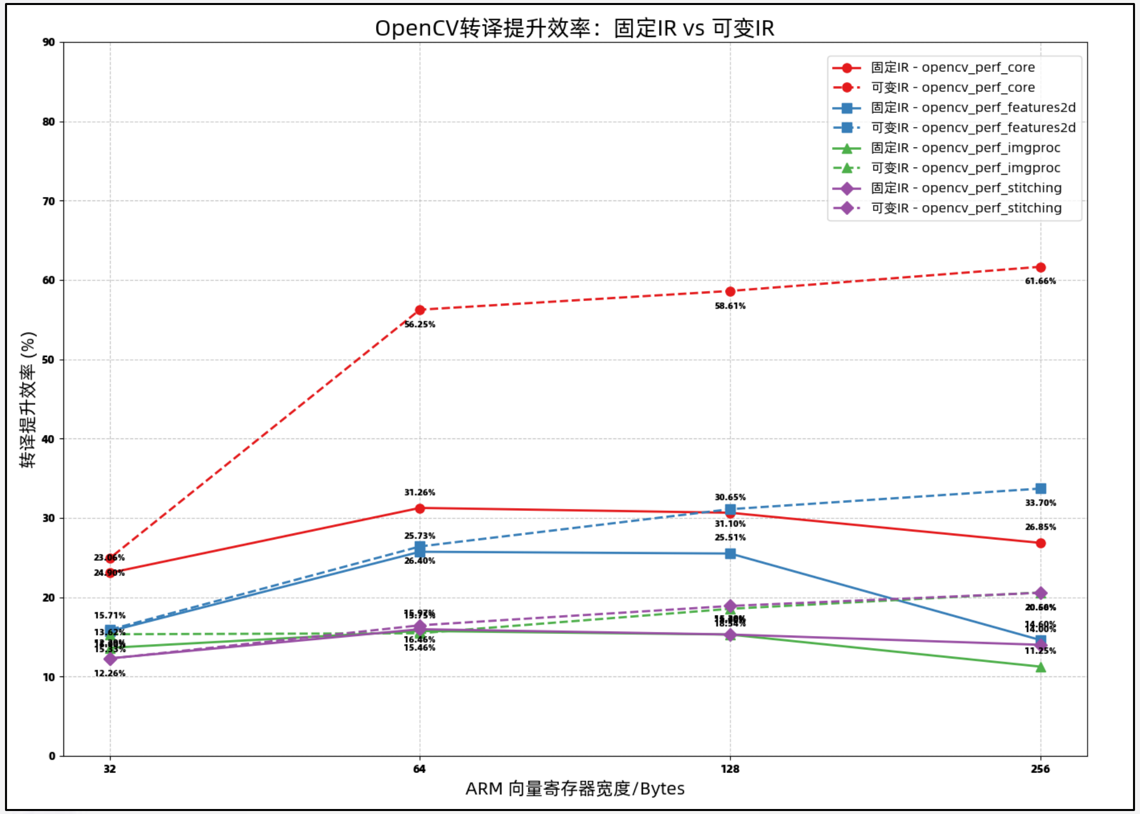

固定 IR X264转译提升效率


可变 IR X264转译提升效率

QEMU for RISCV最新特性介绍

TCG后端支持RVV

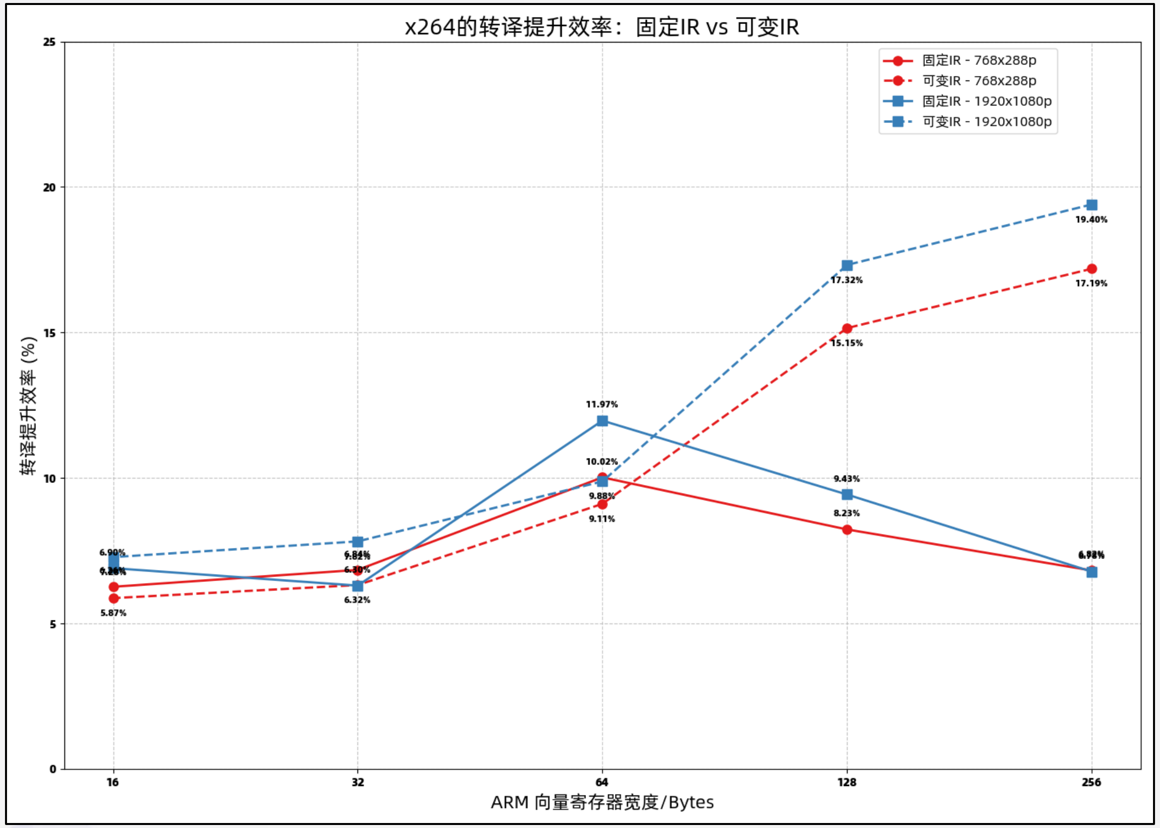
RVV支持对转译效率的提升



QEMU for RISCV最新特性介绍

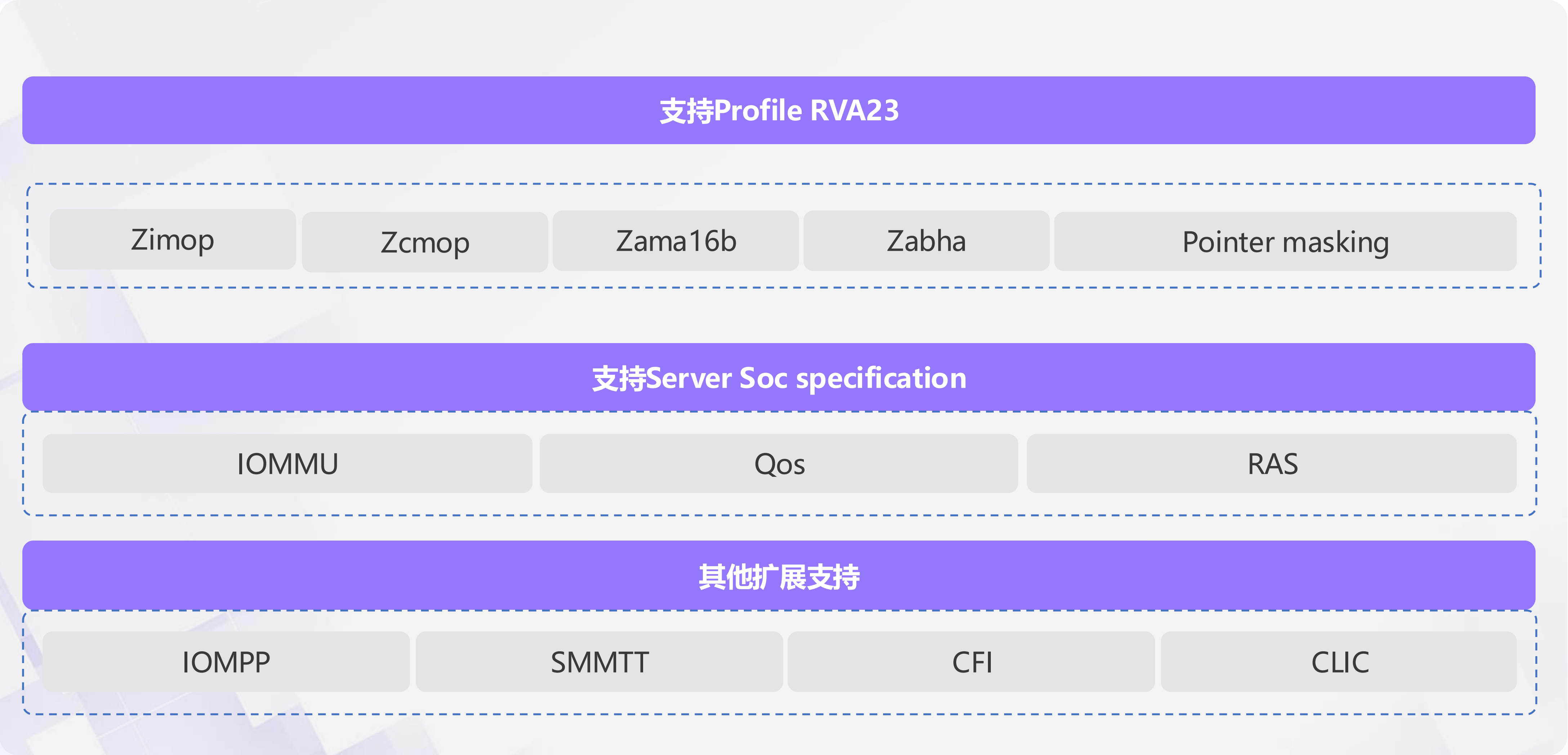
TCG后端支持RVV

RVV支持对转译效率的提升



未来规划和展望

未来一年社区的主要工作



支持Profile RVA23

- Zimop
- Zcmop
- Zama16b
- Zabha
- Pointer masking

支持Server Soc specification

- IOMMU
- Qos
- RAS

其他扩展支持

- IOMPP
- SMMTT
- CFI
- CLIC

Thank you

玄铁公众号

玄铁中文站

玄铁海外站