

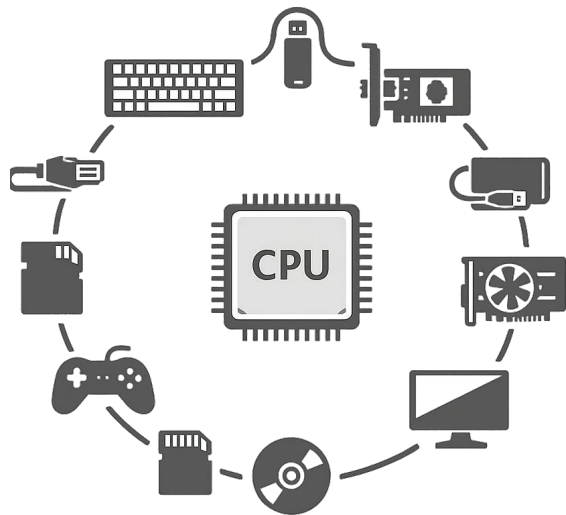
# Contributing to



Matheus Tavares – Qualcomm  
<https://matheustavares.dev/>

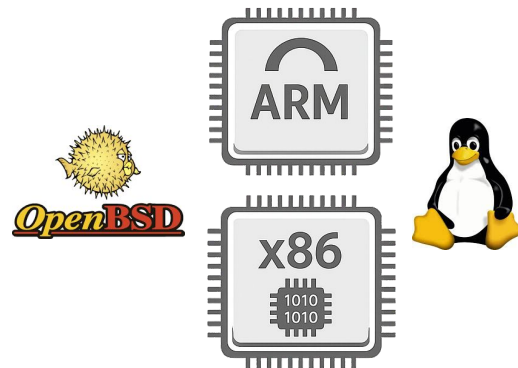
# QEMU: Quick EMULator

System emulation



aka "softmmu"

User mode emulation



# Translation



# Translation

Guest / Frontend

hexagon

decode

TCG (Tiny C Compiler)

TCG IR

emit

Host / Backend

x86

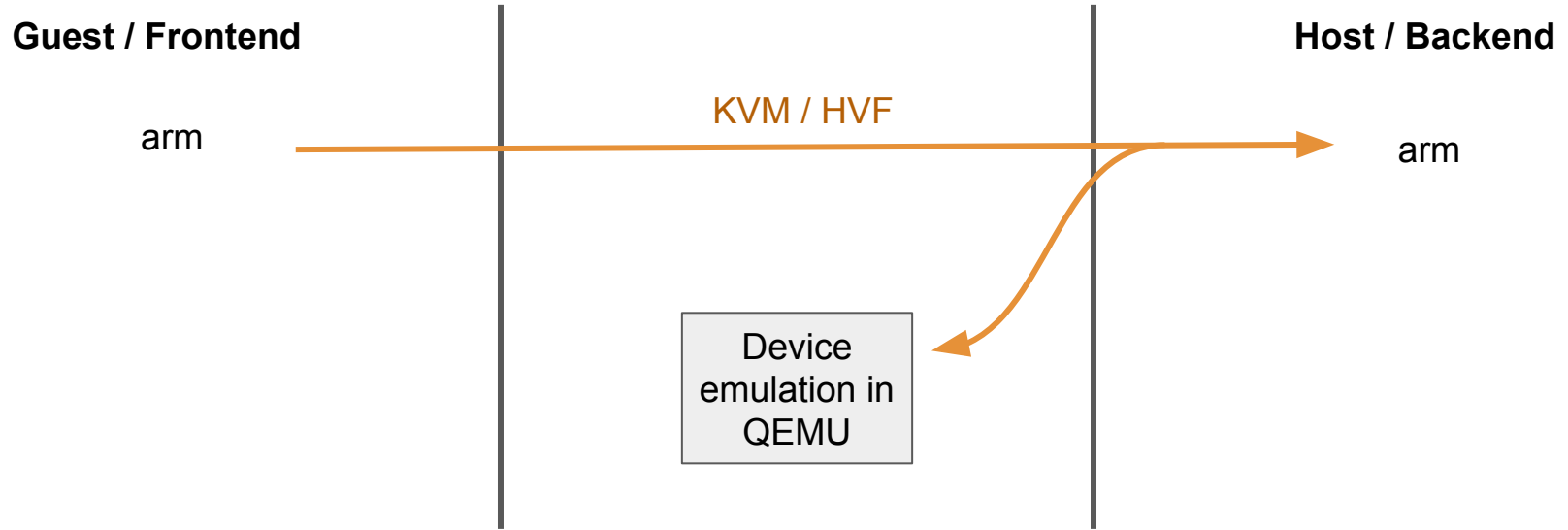
```
0x00007340: 0x00004300 { immext(#0xc000)
0x00007344: 0x78004500 R0 = ##0xc028
0x00007348: 0x5800c120 jump PC+576 }
```

```
mov_i32 r00,$0xc028
add_i32 exec_ctr_pkt,exec_ctr_pkt,$0x1
add_i32 exec_ctr_insn,exec_ctr_insn,$0x2
add_i64 t_cycle_count,t_cycle_count,$0x1
mov_i32 pc,$0x7580
call lookup_tb_ptr,$0x6,$1,tmp12,env
goto_ptr tmp12
set_label $L0
exit_tb $0x7fe56801c343
```

JIT compiled + optimized

```
0x7fe56801c400: movl    -0x14(%rbp), %ebx
0x7fe56801c403: testl  %ebx, %ebx
0x7fe56801c405: jl     0x7fe56801c459
0x7fe56801c40b: movb  $1, -0x10(%rbp)
0x7fe56801c40f: movl  $0xc028, (%rbp)
0x7fe56801c416: movl  0x3540(%rbp), %ebx
0x7fe56801c41c: incl  %ebx
0x7fe56801c41e: movl  %ebx, 0x3540(%rbp)
0x7fe56801c424: movl  0x3544(%rbp), %ebx
0x7fe56801c42a: addl  $2, %ebx
0x7fe56801c42d: movl  %ebx, 0x3544(%rbp)
0x7fe56801c433: movq  0x3538(%rbp), %rbx
0x7fe56801c43a: incq  %rbx
0x7fe56801c43d: movq  %rbx, 0x3538(%rbp)
0x7fe56801c444: movl  $0x7580, 0xa4(%rbp)
...
```

# Virtualization



# Repo structure

- Mostly C (with OOP). Some shell, python, and **Rust**.
- 3M LoC
- Build: configure, meson, make, ninja
- Overall structure

```
|— accel          # hypervisors (kvm, hvf, etc.)
|— hw            # HW devices (pci, usb, etc.)
|— linux-user,  # userspace emulation syscalls
   bsd-user
|— target        # per-arch front-end (decode & translation)
|— tcg           # TCG backend (JIT and generator)
|— tests
|— build         # qemu-system-hexagon, qemu-system-aarch64, etc.
|— ...
```

# Contributing

- Mailing list patches (like Linux kernel, git, etc.)
- [Gitlab](#) for CI and issue tracker
- GSoC and Outreachy

# Useful links

Really nice blogposts / talks:

- [rev.ng](#) getting started videos: [part 1](#) and [part 2](#)
- [Airbus' "gemu internals" blog](#)

Official (and sometimes a bit outdated) docs:

- [Getting started for devs](#) and [Submitting a patch](#)
- [Good first issues](#)
- [Code style](#)

# Thanks

Matheus Tavares – Qualcomm  
<https://matheustavares.dev/>