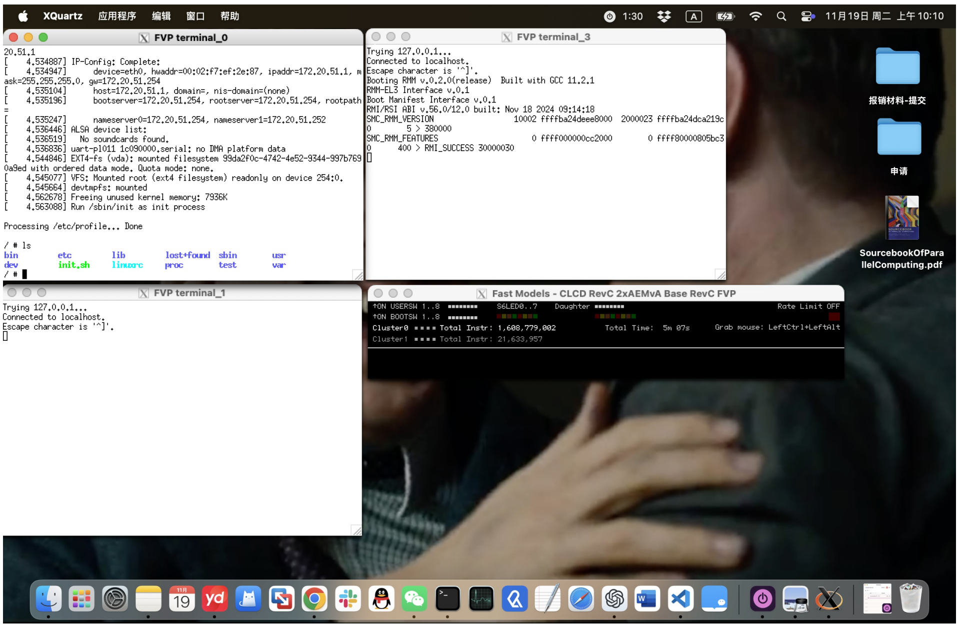
Lab 09 TEE

Name: Sicheng Zhou

SID: 12110644

Task 1 Launch FVP

Task 1.a: Please provide screenshots demonstrating that you have successfully booted the Linux Kernel on FVP. (20%)



```
20.51.1
[    4.534887] IP-Config: Complete:
[    4.534947]      device=eth0, hwaddr=00:02:f7:ef:2e:87, ipaddr=172.20.51.1, m
ask=255.255.255.0, gw=172.20.51.254
[    4.535104]      host=172.20.51.1, domain=, nis-domain=(none)
[    4.535196]      bootserver=172.20.51.254, rootserver=172.20.51.254, rootpath
=
[    4.535247]      nameserver0=172.20.51.254, nameserver1=172.20.51.252
[    4.536446] ALSA device list:
[    4.536519]   No soundcards found.
[    4.536836] uart-pl011 1c090000.serial: no DMA platform data
[    4.544846] EXT4-fs (vda): mounted filesystem 99da2f0c-4742-4e52-9344-997b769
0a9ed with ordered data mode. Quota mode: none.
[    4.545077] VFS: Mounted root (ext4 filesystem) readonly on device 254:0.
[    4.545664] devtmpfs: mounted
[    4.562678] Freeing unused kernel memory: 7936K
[    4.563088] Run /sbin/init as init process

Processing /etc/profile... Done

/ # ls
bin         etc         lib         lost+found  sbin        usr
dev         init.sh     linuxrc     proc        test        var
/ #
```

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Booting RMM v.0.2.0(release)  Built with GCC 11.2.1
RMM-EL3 Interface v.0.1
Boot Manifest Interface v.0.1
RMI/RSI ABI v.56.0/12.0 built: Nov 18 2024 09:14:18
SMC_RMM_VERSION                  10002 ffffba24deee8000  2000023 ffffba24dca219c
0        5 > 380000
SMC_RMM_FEATURES                     0 ffff000000cc2000        0 ffff80000805bc3
0      400 > RMI_SUCCESS 30000030
```

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
```

```
↑ON USERSW 1..8 ■■■■■■■■    S6LED0..7    Daughter ■■■■■■■■              Rate Limit OFF
↑ON BOOTSW 1..8 ■■■■■■■■
Cluster0 ■■■■ Total Instr: 1,608,779,002        Total Time:  5m 07s    Grab mouse: LeftCtrl+LeftAlt
Cluster1 ■■■■ Total Instr: 21,633,957
```

FVP boot

Task 1.b: What are the exception level and the security state of RMM? (10%)

EL2, realm security state.

Task 1.c: Review the source code of ’linux-cca’, identify at least two instances where RMIs are dispatched to RMM, and explain the functionality of these RMIs. (20%) (The definitions of RMIs can be found in the source code of ‘kvm_realm_rmi.h’.)

1. linux-cca/arch/arm64/kvm/rme.c, `rmi_check_version(void)`.

This function ensures that the RMM supports the required RMI ABI version for the KVM subsystem to function correctly. The code dispatches an RMI command (`SMC_RMI_VERSION`) to the RMM through the SMC mechanism

```c
static int rmi_check_version(void)
{
    struct arm_smccc_res res;
    int version_major, version_minor;

    arm_smccc_1_1_invoke(SMC_RMI_VERSION, &res);

    if (res.a0 == SMCCC_RET_NOT_SUPPORTED)
        return -ENXIO;

    version_major = RMI_ABI_VERSION_GET_MAJOR(res.a0);
    version_minor = RMI_ABI_VERSION_GET_MINOR(res.a0);

#ifdef PROTOTYPE_RMI_ABI_MAJOR_VERSION
    // Support the prototype
    if (version_major == PROTOTYPE_RMI_ABI_MAJOR_VERSION) {
        kvm_err("Using prototype RMM support (version %d.%d)\n",
            version_major, version_minor);
        return 0;
    }
#endif
    if (version_major != RMI_ABI_MAJOR_VERSION) {
        kvm_err("Unsupported RMI ABI (version %d.%d) we support %d\n",
            version_major, version_minor,
            RMI_ABI_MAJOR_VERSION);
        return -ENXIO;
    }

    kvm_info("RMI ABI version %d.%d\n", version_major, version_minor);

    return 0;
}
```

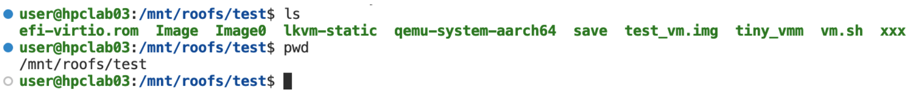
2. linux-cca/arch/arm64/kvm/rme.c, `realm_create_protected_data_page()`.

The function creates a secure data page within the Realm by interacting with the RMM. It handles granule delegation, data creation, and error recovery comprehensively. The function dispatches multiple RMIs (`rmi_granule_delegate`, `rmi_data_create`, `rmi_granule_undelegate`) to the RMM.

```
static int realm_create_protected_data_page(struct realm *realm,
                        unsigned long ipa,
                        struct page *dst_page,
                        struct page *tmp_page)
{
    phys_addr_t dst_phys, tmp_phys;
    int ret;

    copy_page(page_address(tmp_page), page_address(dst_page));

    dst_phys = page_to_phys(dst_page);
    tmp_phys = page_to_phys(tmp_page);

    if (rmi_granule_delegate(dst_phys))
        return -ENXIO;

    ret = rmi_data_create(dst_phys, virt_to_phys(realm->rd), ipa, tmp_
                  RMI_MEASURE_CONTENT);

    if (RMI_RETURN_STATUS(ret) == RMI_ERROR_RTT) {
        /* Create missing RTTs and retry */
        int level = RMI_RETURN_INDEX(ret);

        ret = realm_create_rtt_levels(realm, ipa, level,
                          RME_RTT_MAX_LEVEL, NULL);
        if (ret)
            goto err;

        ret = rmi_data_create(dst_phys, virt_to_phys(realm->rd), ipa,
                      tmp_phys, RMI_MEASURE_CONTENT);
    }

    if (ret)
        goto err;

    return 0;

err:
    if (WARN_ON(rmi_granule_undelegate(dst_phys))) {
        /* Page can't be returned to NS world so is lost */
        get_page(dst_page);
    }
    return -ENXIO;
}
```

Task 2 Launch Realm VM

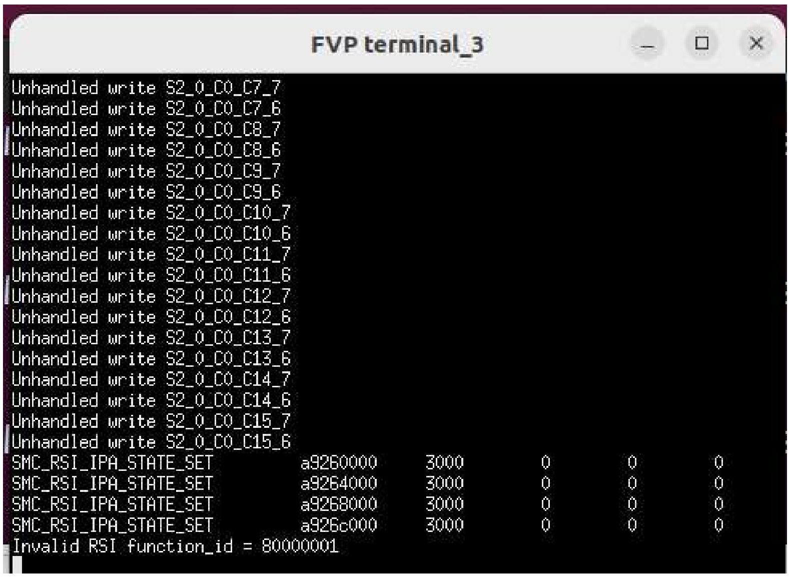
Task 2.a: Provide screenshots to show that you have already compiled kvmtool and copy it to FVP. (20%)



```
● user@hpclab03:/mnt/roofs/test$ ls
  efi-virtio.rom  Image  Image0  lkvm-static  qemu-system-aarch64  save  test_vm.img  tiny_vmm  vm.sh  xxx
● user@hpclab03:/mnt/roofs/test$ pwd
  /mnt/roofs/test
○ user@hpclab03:/mnt/roofs/test$ █
```

kvmtool compiled

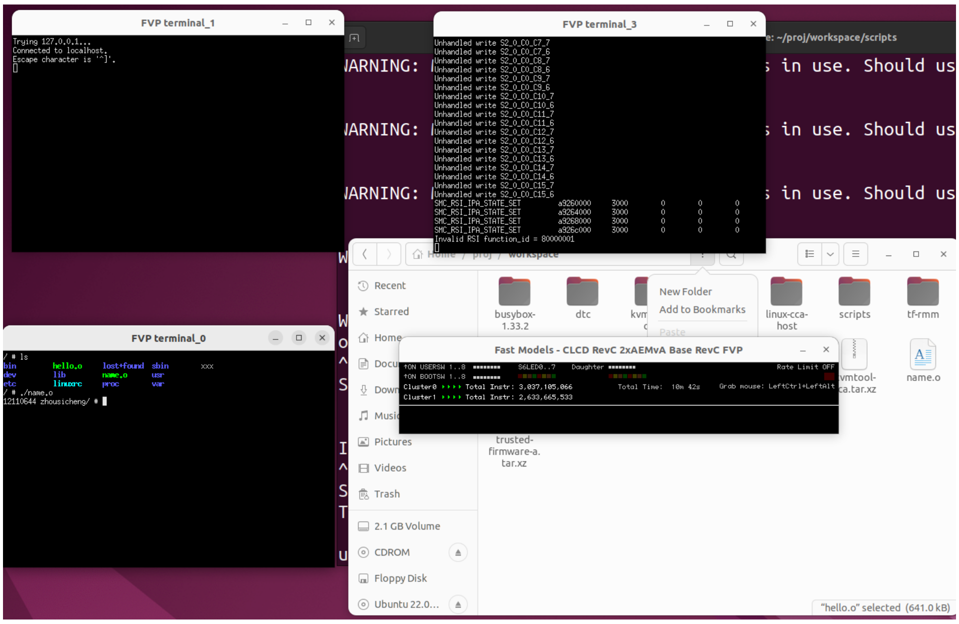
Task 2.b: Provide screenshots to show that you have already launched a Realm VM. (10%)



```
Unhandled write S2_0_C0_C7_7
Unhandled write S2_0_C0_C7_6
Unhandled write S2_0_C0_C8_7
Unhandled write S2_0_C0_C8_6
Unhandled write S2_0_C0_C9_7
Unhandled write S2_0_C0_C9_6
Unhandled write S2_0_C0_C10_7
Unhandled write S2_0_C0_C10_6
Unhandled write S2_0_C0_C11_7
Unhandled write S2_0_C0_C11_6
Unhandled write S2_0_C0_C12_7
Unhandled write S2_0_C0_C12_6
Unhandled write S2_0_C0_C13_7
Unhandled write S2_0_C0_C13_6
Unhandled write S2_0_C0_C14_7
Unhandled write S2_0_C0_C14_6
Unhandled write S2_0_C0_C15_7
Unhandled write S2_0_C0_C15_6
SMC_RSI_IPA_STATE_SET         a9260000     3000         0        0        0
SMC_RSI_IPA_STATE_SET         a9264000     3000         0        0        0
SMC_RSI_IPA_STATE_SET         a9268000     3000         0        0        0
SMC_RSI_IPA_STATE_SET         a926c000     3000         0        0        0
Invalid RSI function_id = 80000001
```

Realm VM launched

Task 2.c: Write a simpe application to print your Student ID and name, and execute it in the Realm VM. (10%)



```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
```

```
Unhandled write S2_0_C0_C7_7
Unhandled write S2_0_C0_C7_6
Unhandled write S2_0_C0_C8_7
Unhandled write S2_0_C0_C8_6
Unhandled write S2_0_C0_C9_7
Unhandled write S2_0_C0_C9_6
Unhandled write S2_0_C0_C10_7
Unhandled write S2_0_C0_C10_6
Unhandled write S2_0_C0_C11_7
Unhandled write S2_0_C0_C11_6
Unhandled write S2_0_C0_C12_7
Unhandled write S2_0_C0_C12_6
Unhandled write S2_0_C0_C13_7
Unhandled write S2_0_C0_C13_6
Unhandled write S2_0_C0_C14_7
Unhandled write S2_0_C0_C14_6
Unhandled write S2_0_C0_C15_7
Unhandled write S2_0_C0_C15_6
SMC_RSI_IPA_STATE_SET        a9260000    3000      0       0       0
SMC_RSI_IPA_STATE_SET        a9264000    3000      0       0       0
SMC_RSI_IPA_STATE_SET        a9268000    3000      0       0       0
SMC_RSI_IPA_STATE_SET        a926c000    3000      0       0       0
Invalid RSI function_id = 80000001
```

```
/ # ls
bin         hello.o     lost+found  sbin        xxx
dev         lib         name.o      usr
etc         linuxrc     proc        var
/ # ./name.o
12110644 zhousicheng/ #
```

```
↑ON USERSW 1..8  ■■■■■■■■     S6LED0..7    Daughter ■■■■■■■■                Rate Limit OFF
↑ON BOOTSW 1..8  ■■■■■■■■
Cluster0 ▸▸▸▸ Total Instr: 3,037,105,066         Total Time:  10m 42s    Grab mouse: LeftCtrl+LeftAlt
Cluster1 ▸▸▸▸ Total Instr: 2,633,665,533
```

print SID and name

Task 2.d: What is the exception level and the security state of kvmtool? (10%)

EL0, non-secure state.