

第1部分

- ```
将 dmss_board.dts 转为 output.dtb
dtc -I dts -O dtb dmss_board.dts -o output.dtb

启动qemu
qemu-system-aarch64 \
 -cpu cortex-a57 \
 -smp 4 \
 -m 5G \
 -machine virt,virtualization=on \
 -bios u-boot.bin \
 -nographic \
 -device loader,file=output.dtb,addr=0x10c308 \
 -device loader,file=archlinux_fit.itb,addr=0x40200000 \
 -drive file=encrypted_filesystem.img,if=virtio,format=raw
```
- ```
# 输入启动qemu命令后，按任意键停止自动启动并进入 U-Boot 命令行
# 删除 .dtb 和 .itb 中的 “required ”属性，禁用 U-Boot 启动身份验证
fdt addr $fdtaddr

fdt rm /configurations/myconfig required

fdt addr $fdtcontroladdr

fdt rm /signature/key-verification required
```

第2部分

- ```
查看 LUKS 头/密钥信息
cryptsetup luksDump encrypted_filesystem.img

将口令添加到 encrypted_filesystem.img 中
cryptsetup luksAddKey -S 0 --pbkdf pbkdf2 encrypted_filesystem.img --key-file
default.key

将 new.key 添加到 encrypted_filesystem.img 中
cryptsetup luksAddKey -S 1 --pbkdf pbkdf2 encrypted_filesystem.img new.key

删除 default.key
cryptsetup luksKillSlot encrypted_filesystem.img 3

创建用于存储 new.key 的目录
mkdir key
cp new.key key/new.key

从 /work/key 创建虚拟 FAT 磁盘映像并使用它
qemu-system-aarch64 \
 -cpu cortex-a57 \
 -smp 4 \
 -m 5G \
 -machine virt,virtualization=on \
 -bios u-boot.bin \
```

```

-nographic \
-device loader,file=output.dtb,addr=0x10c308 \
-device loader,file=archlinux_fit.itb,addr=0x40200000 \
-drive file=encrypted_filesystem.img,if=virtio,format=raw \
-hdb fat:rw:/work/key

输入启动qemu命令后，按任意键停止自动启动并进入 U-Boot 命令行
将 cryptkey 更改为位于 /dev/vdb1 中的 new.key 并手动启动
setenv bootargs "console=ttyAMA0 mem=5G root=/dev/mapper/rootfs rw
cryptdevice=/dev/vda:rootfs cryptkey=/dev/vdb1:vfat:new.key"
boot

```

### ① Note

上述命令中，最后需要在 U-Boot 命令行手动修改环境变量，这个似乎方法不太符合题目描述 “an external keyfile based on, passed as an commandline parameter to QEMU.”

**有没有办法直接给 qemu-system-aarch64 命令传递下面的参数，而不需要进入 U-Boot 命令行手动修改环境变量？**

```

console=ttyAMA0 mem=5G root=/dev/mapper/rootfs rw cryptdevice=/dev/vda:rootfs
cryptkey=/dev/vdb1:vfat:new.key

```

1. 无法使用 `-append` 参数。 `-append` 需要在 `-kernel` 参数后面使用，而使用 `-kernel` 加载 `archlinux_fit.itb` 会报错：

```

----> FIT image device tree node
libfdt fdt_check_header(): FDT_ERR_BADMAGIC
Wrong Image Type for bootm command
ERROR -91: can't get kernel image!

```

2. 也无法使用通用加载器：

```

将环境变量写入文件
echo "console=ttyAMA0 mem=5G root=/dev/mapper/rootfs rw
cryptdevice=/dev/vda:rootfs cryptkey=/dev/vdb1:vfat:new.key" >
bootargs.txt

给 qemu-system-aarch64 添加以下参数
-device loader,file=bootargs.txt,addr=0x10000000

```

这并不起作用，可以在 U-Boot 命令行中输入 `printenv` 查看 `bootargs`，它并没有变化。（谁的问题？是方法本身不对还是 `addr` 不对？）