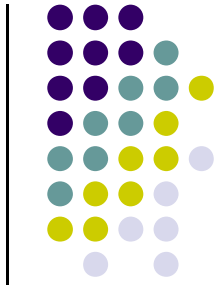


可信计算实验

wqdai@hust.edu.cn

大纲

- 参考资料
- 原理部分
- 实验部分

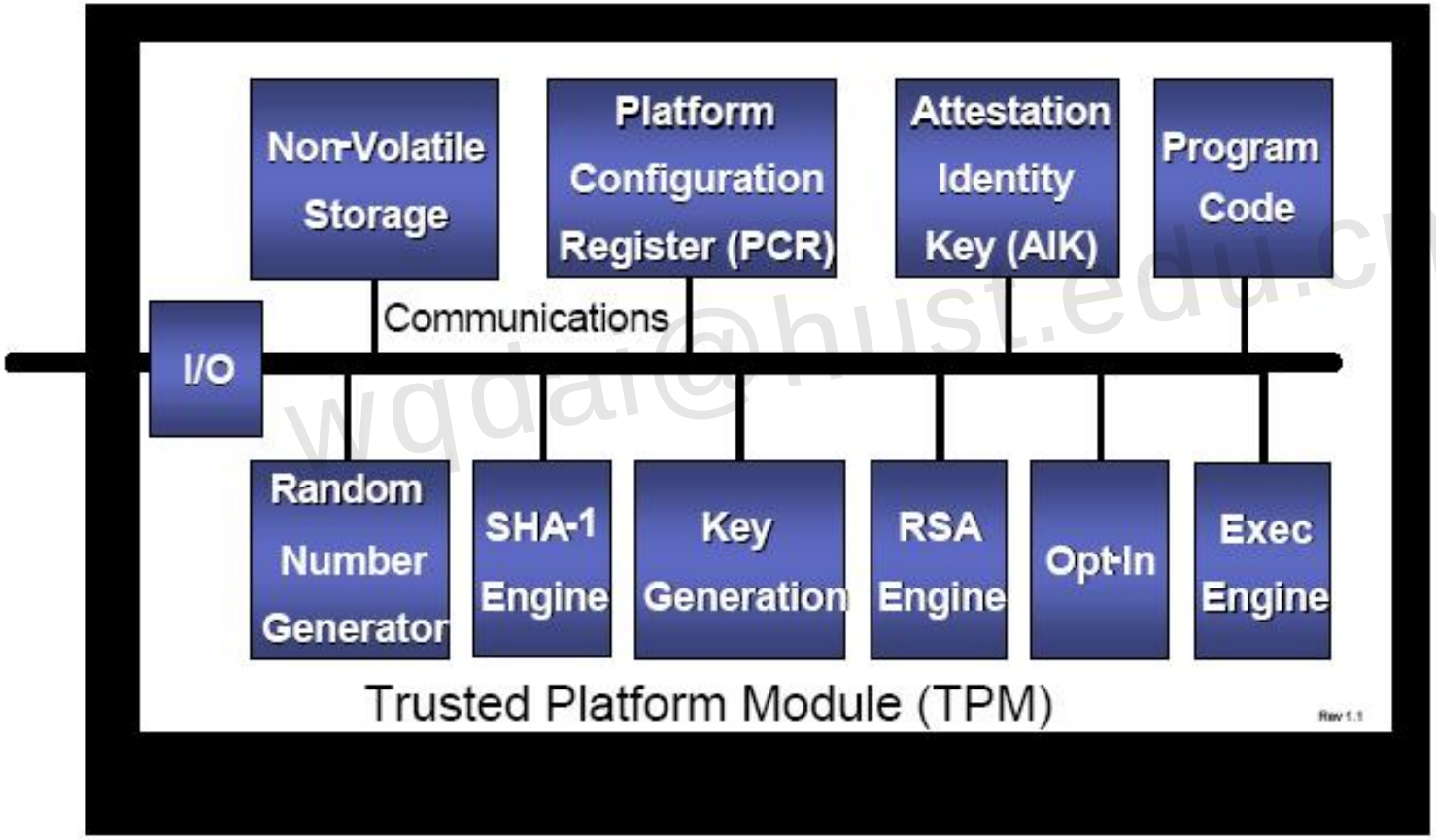
wqdai@hust.edu.cn

参考资料

- TCG TPM Specification Version
  - TPM Main--Part 1 Design Principles
  - TPM Main--Part 3 Commands
  - TPM Main--Part 2 TPM Structures
- TCG Software Stack (TSS) Specification Version 1.2

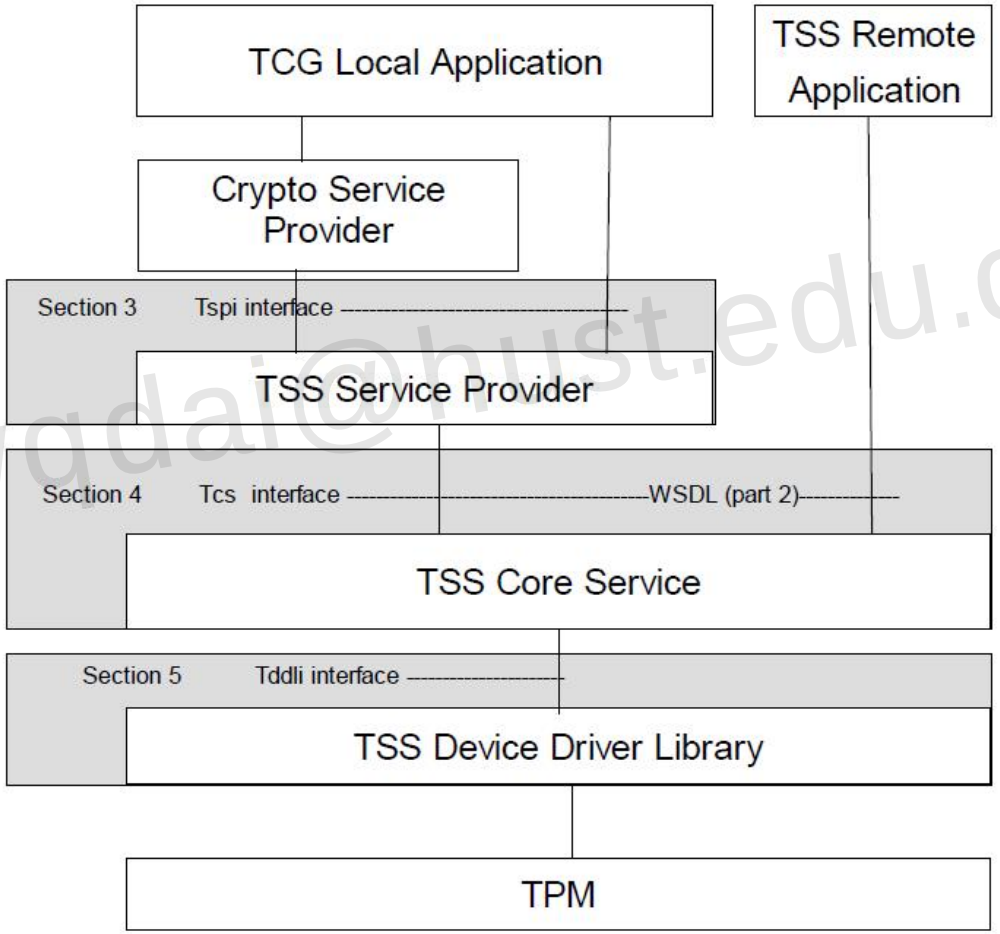
wqdai@hust.edu.cn

TPM架构（原理部分）



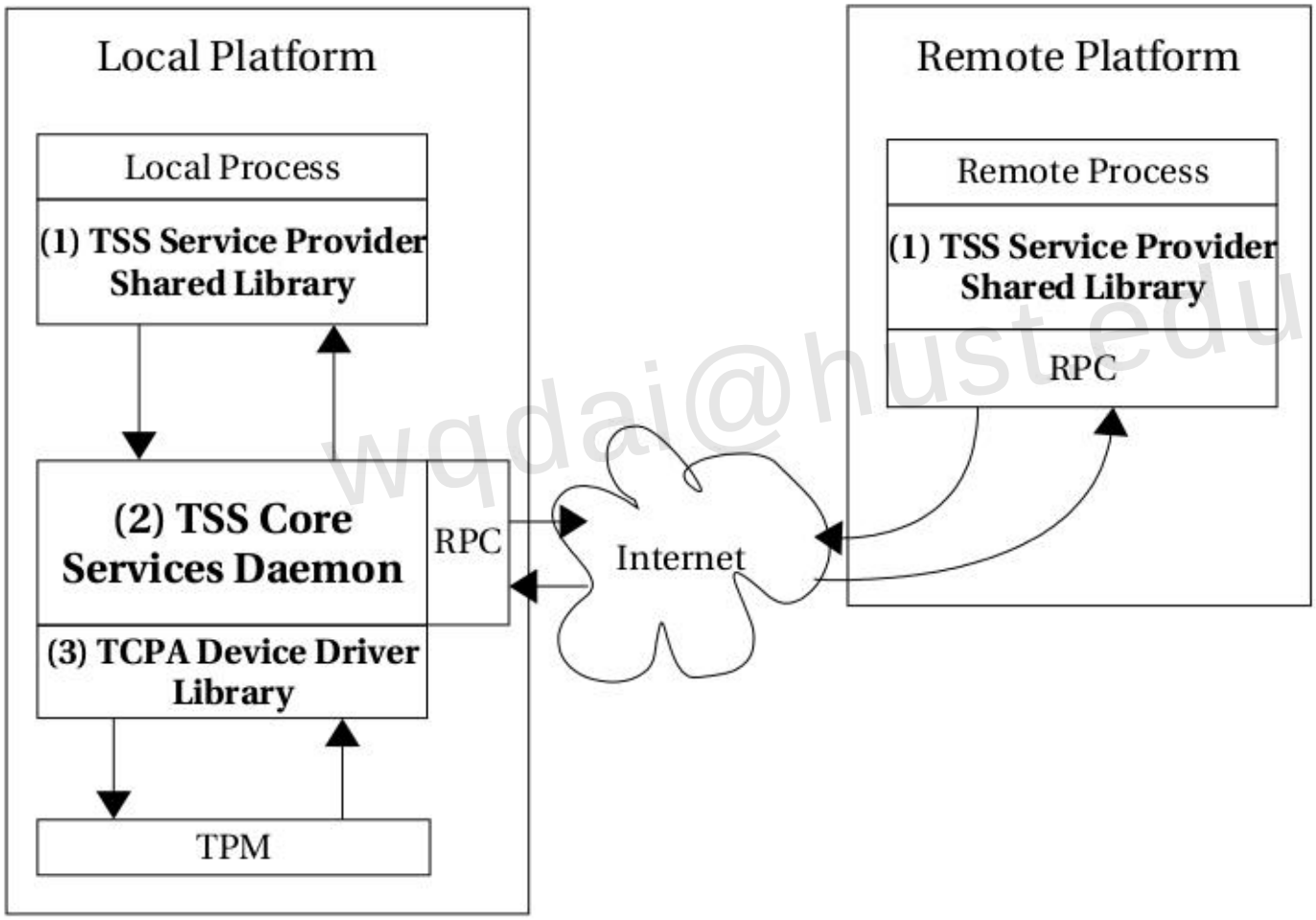
wqdai@hust.edu.cn

TCG软件栈（原理部分）



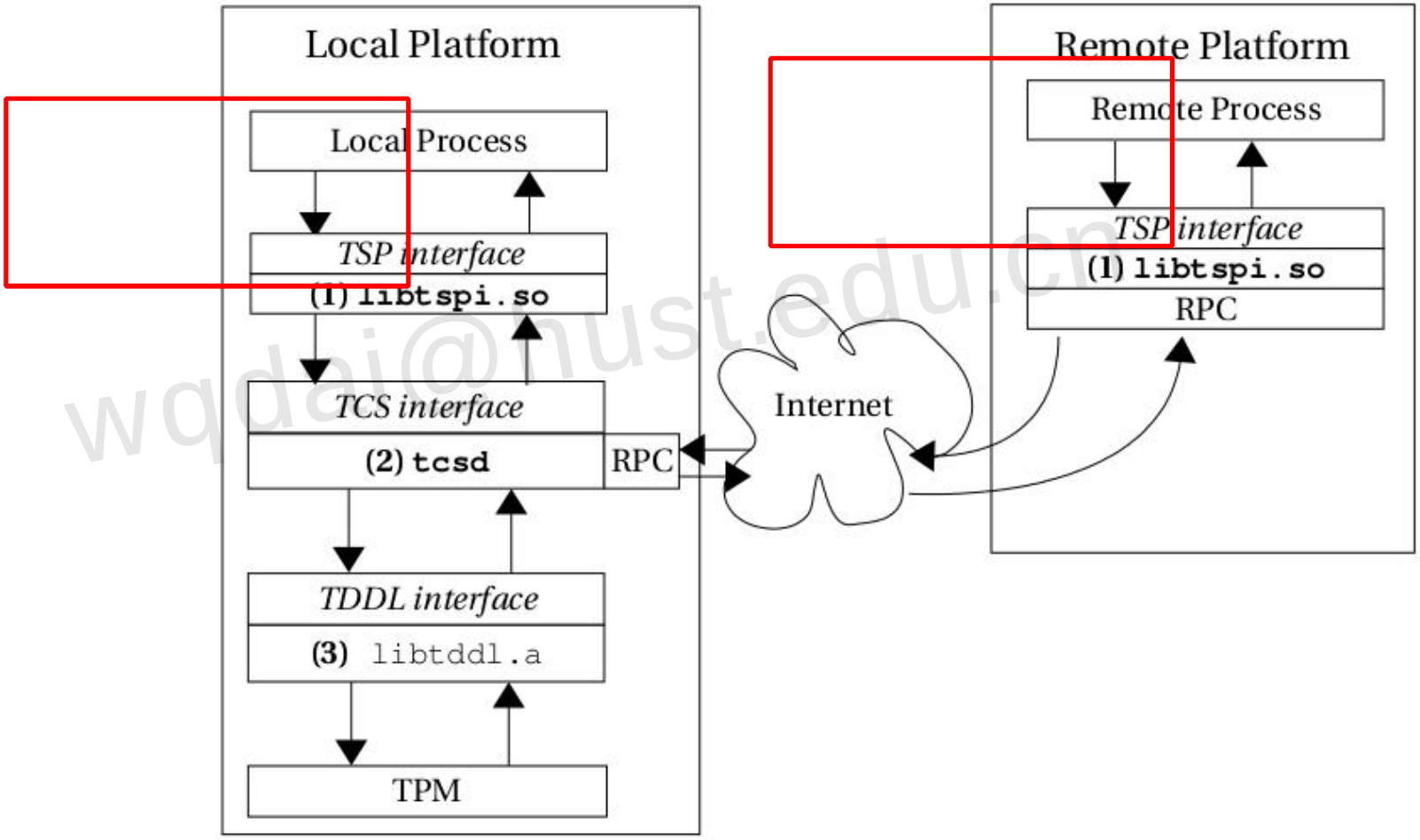
wgdai@hust.edu.cn

TSS软件栈（原理部分）



wqdai@hust.edu.cn

TSS软件栈（原理部分）



wqdai@hust.edu.cn

TakeOwnership（原理部分）

- Ownership即对TPM的拥有权
  1. 向TPM中加入“秘密”
  2. 生成SRK
  3. 只有TPM拥有者才能执行一些特殊操作
  4. 获得TPM拥有权用Tspi_TPM_TakeOwnership
  5. 清除TPM拥有权用Tspi_TPM_ClearOwner

wqdai@nust.edu.cn

TPM中的密钥（原理部分）

- 不可迁移密钥
- 可迁移密钥
- 存储密钥
- 签名密钥
- EK
- SRK

wqdai@hust.edu.cn

TPM中的密钥（原理部分）

- 密钥在TPM外部以密文的形式存在
- 只有加载到TPM中的密钥才以明文的形式存在
- 在TPM外部，TSS管理一棵以SRK为根的密钥树

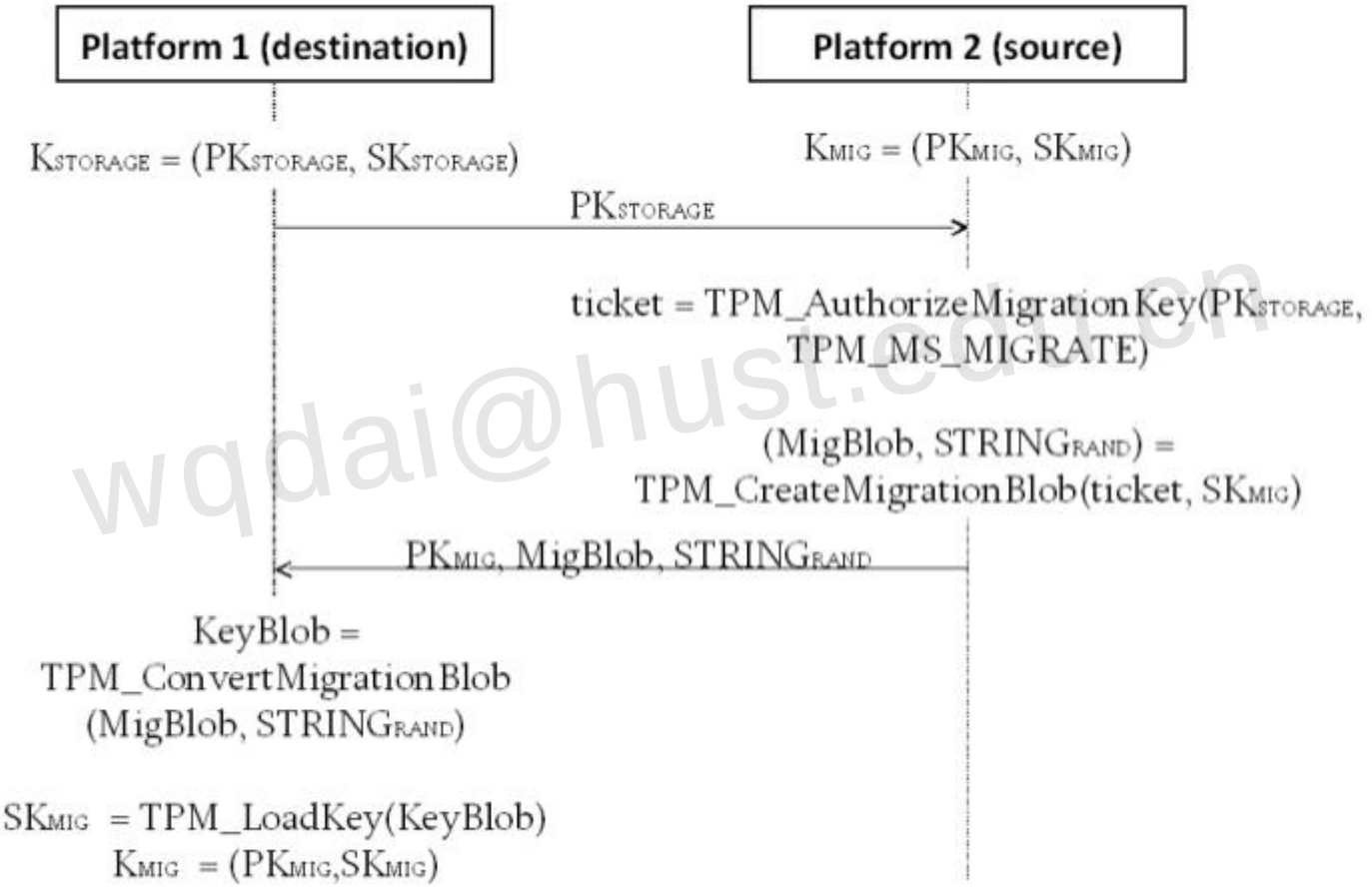
wqdai@hust.edu.cn

seal/unseal（原理部分）

- Seal时可以指定一组pcr的值，unseal时，只有这组pcr的值与预期相符才能解密
- pcr的值通过extend改变
- $PCR_{new}=SHA1(PCR_{old} || data)$

wqdai@hust.edu.cn

密钥迁移（原理部分）



wqdai@hust.edu.cn

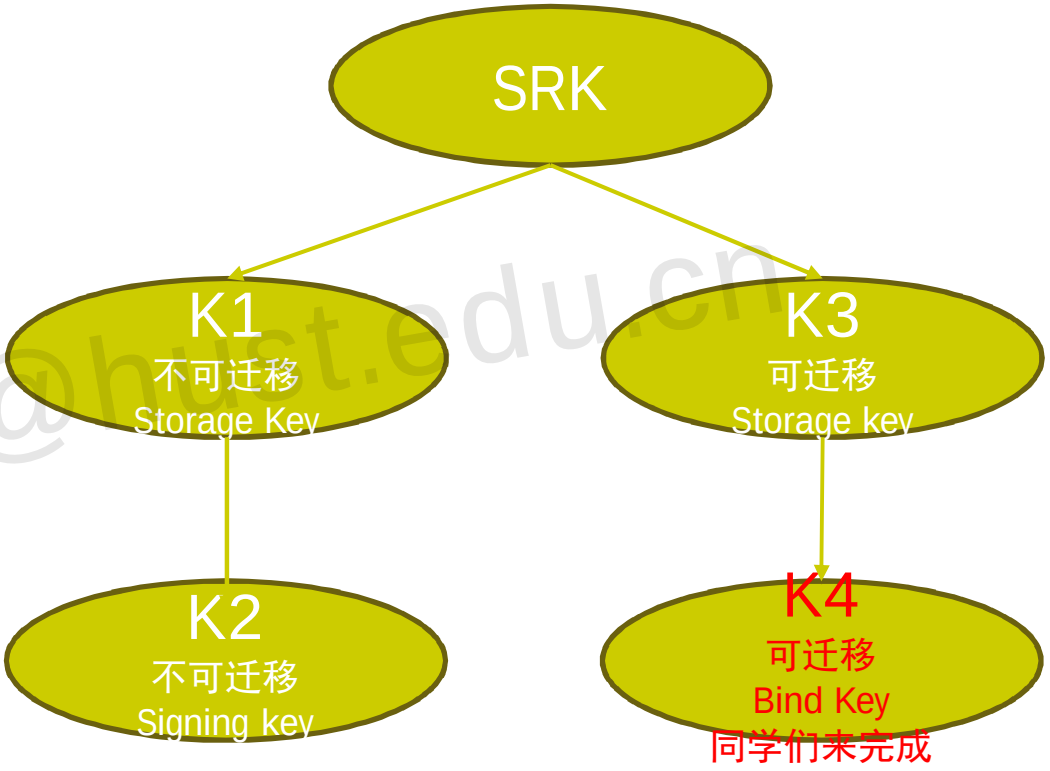
实验部分

- 按照后面的说明完善源代码中的TODO部分
- 详细步骤可以参考源码下的README文档

wqdai@hust.edu.cn

任务1 创建密钥层次（实验部分）

完善KeyHierarchy目录下create_register_key.c以及load_key.c中的TODO部分，创建如右图所示的密钥层次。



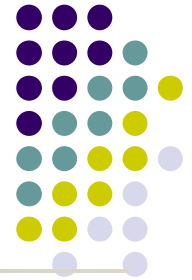
wqdai@hust.edu.cn

任务2 Seal、Unseal（实验部分）

1、进入SealUnseal目录
2、运行./seal -v 1.2 （成功）
3、运行./unseal -v 1.2 （成功）
4、运行./extend -v 1.2 （成功）
5、运行./unseal -v 1.2 （失败）
6、运行./seal_file test.c test.en（查看文件test.en的内容）
unseal_file.c 由同学们自己完成。
7、运行./unseal_file test.en test.de（查看文件test.de的内容）
8、运行./extend -v 1.2
9、运行./unseal_file test.en test.de（失败）

wgdei@hust.edu.cn

任务3 KeyMigration（实验部分）



1、进入Key Migration目录
platform_dst.c中的TODO部分由同学们自己来完成
2、在机器1中运行./platform_dst -g，会产生名为srk.pub的文件
3、把文件srk.pub拷贝到机器2中
4、在机器2中运行./platform_src，会产生名为mig.blob的文件
5、把文件srk.pub拷贝到机器1中
6、在机器1中运行./platform_dst -m

wgao@hust.edu.cn

任务4 远程证明（实验部分）

机器1：
1、进入Remote Attestation\init目录
2、运行./Create_AIK3、返回上级目录
4、运行./RAServer
机器2：
1、进入Remote Attestation目录
2、运行./RAClient 机器2的ip 机器1的ip （如，./RAClient 192.168.200.1 192.168.200.2）

wgdei@hust.edu.cn