第5章 系统安全硬件基础

5.1 问题与发展背景

- 纯软件安全机制的不足
  - 纯软件安全机制的不足
  - 数据的泄露
- 可信计算发展状况
  - TCB(Trusted Computing Base)
  - TPM(Trusted Platform Module)
- 可信计算的前期基础
  - 1991，基于安全协处理器的Dyad系统模型
  - 1994，基于智能卡的引导完整性令牌系统
  - 1997，安全引导体系结构模型
  - 2003，IBM的可信计算组织

问题与发展背景

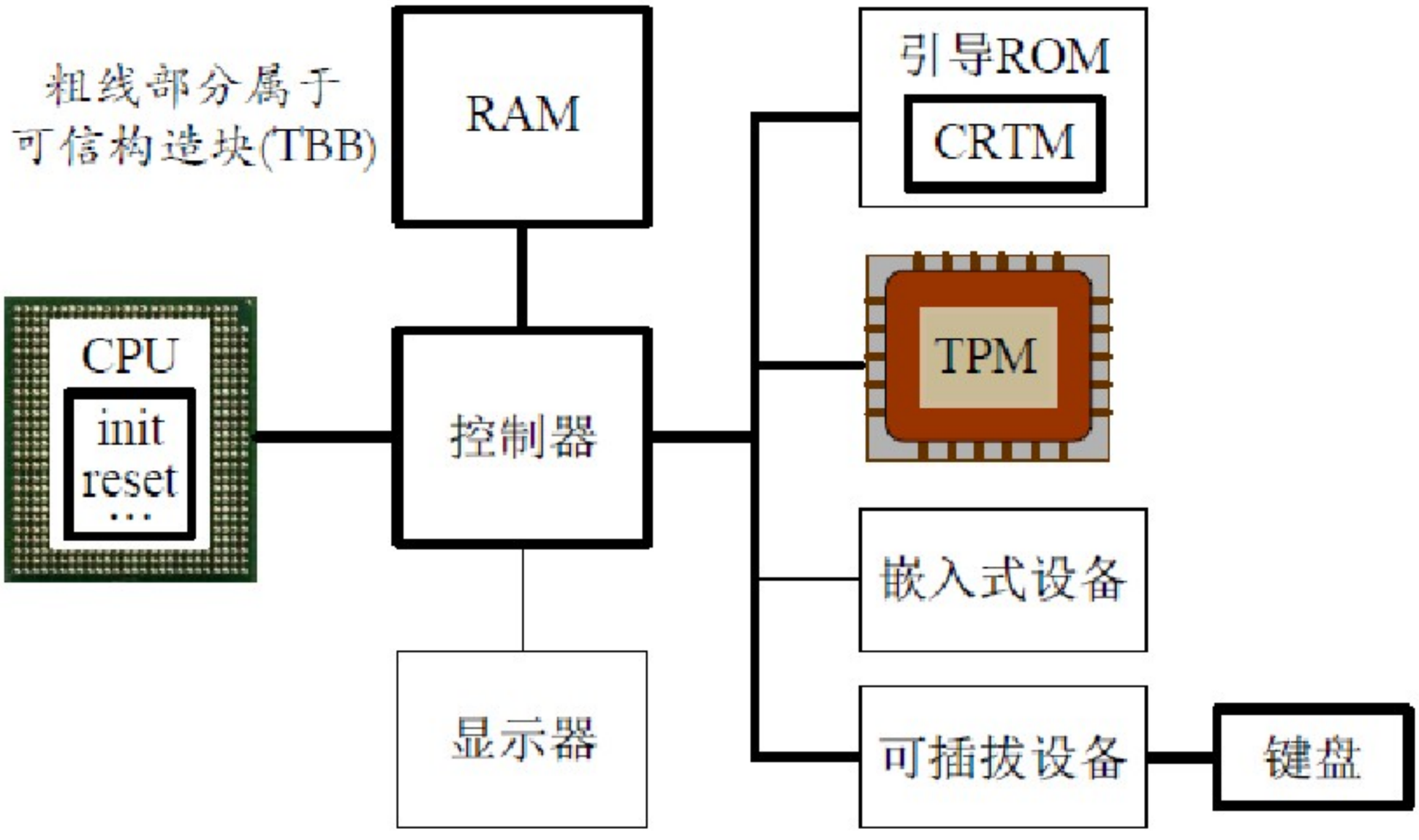
- 可信计算发展状况
  - TCPA==>TCG
  - TPM1.2==>TPM2.0

5.2 可信平台基本思想

- 基本概念
  - ① 信任
  - ② 信任根
  - ③ 度量核心信任根（CRTM, Core Root of Trust for Measurement）
  - ④ 信任传递
  - ⑤ 信任链
  - ⑥ 可信平台模块TPM
  - ⑦ 受保护功能
  - ⑧ 受保护存储区
  - ⑨ 可信构造块TBB
  - ⑩ 可信计算基

可信平台基本思想

- 可信构造模块

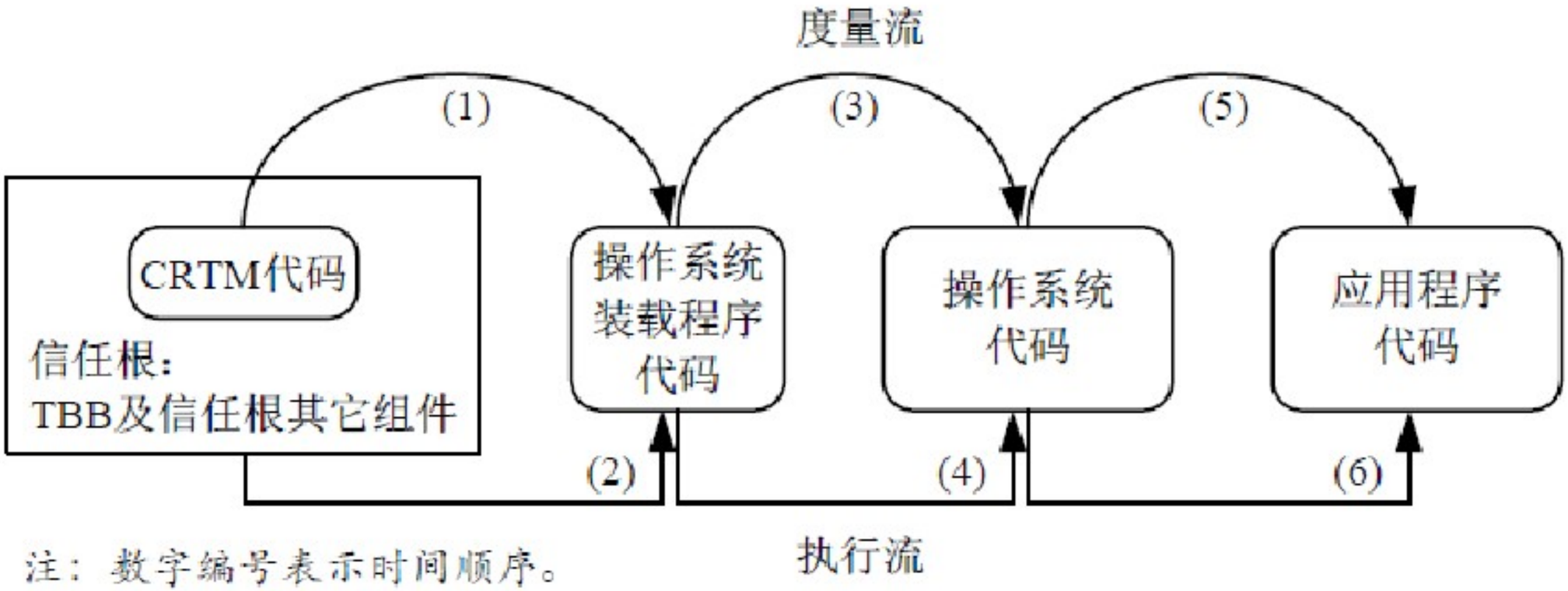


可信平台基本思想

- 信任根的构成
  - ① 度量信任根RTM
  - ② 存储信任根RTS
  - ③ 报告信任根RTR

可信平台基本思想

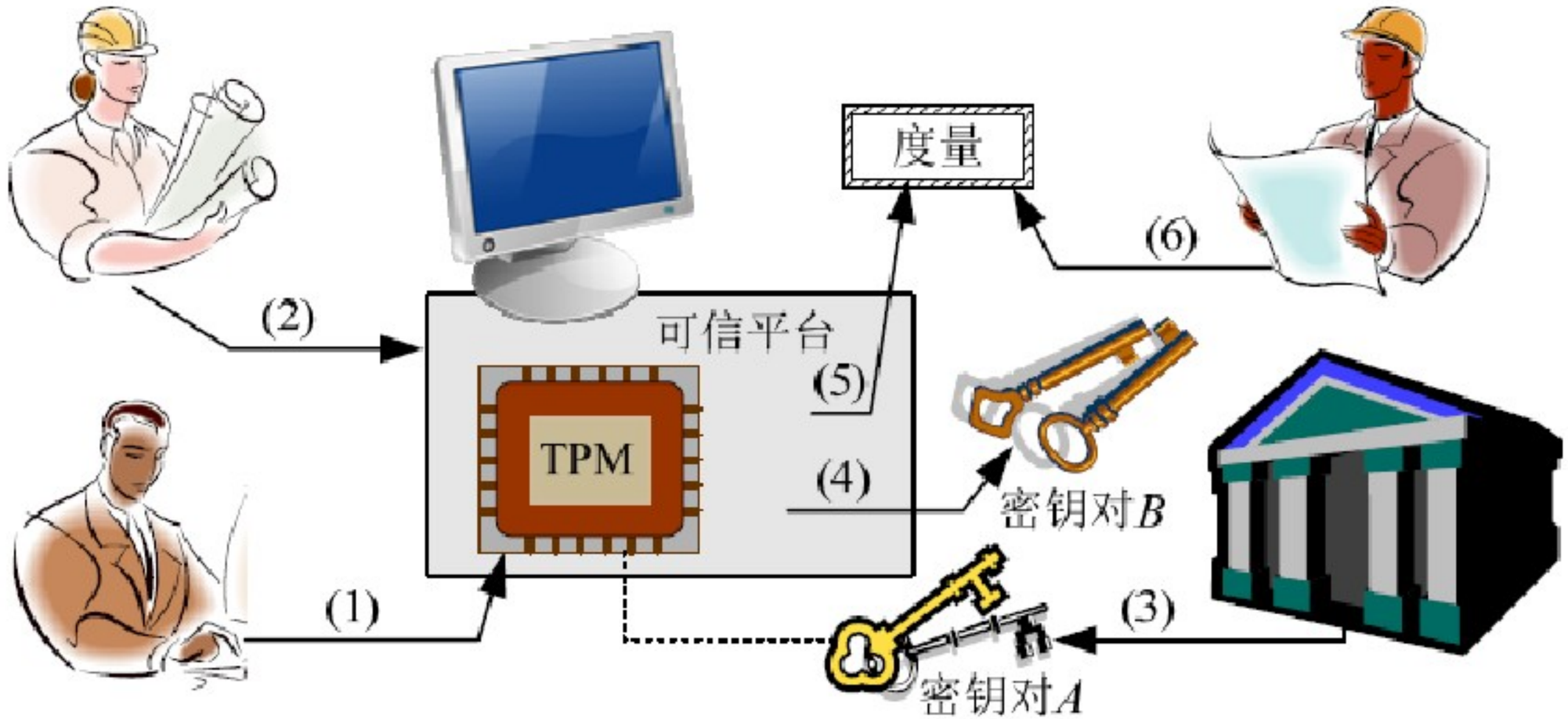
- 系统引导过程的信任传递



注：数字编号表示时间顺序。

可信平台基本思想

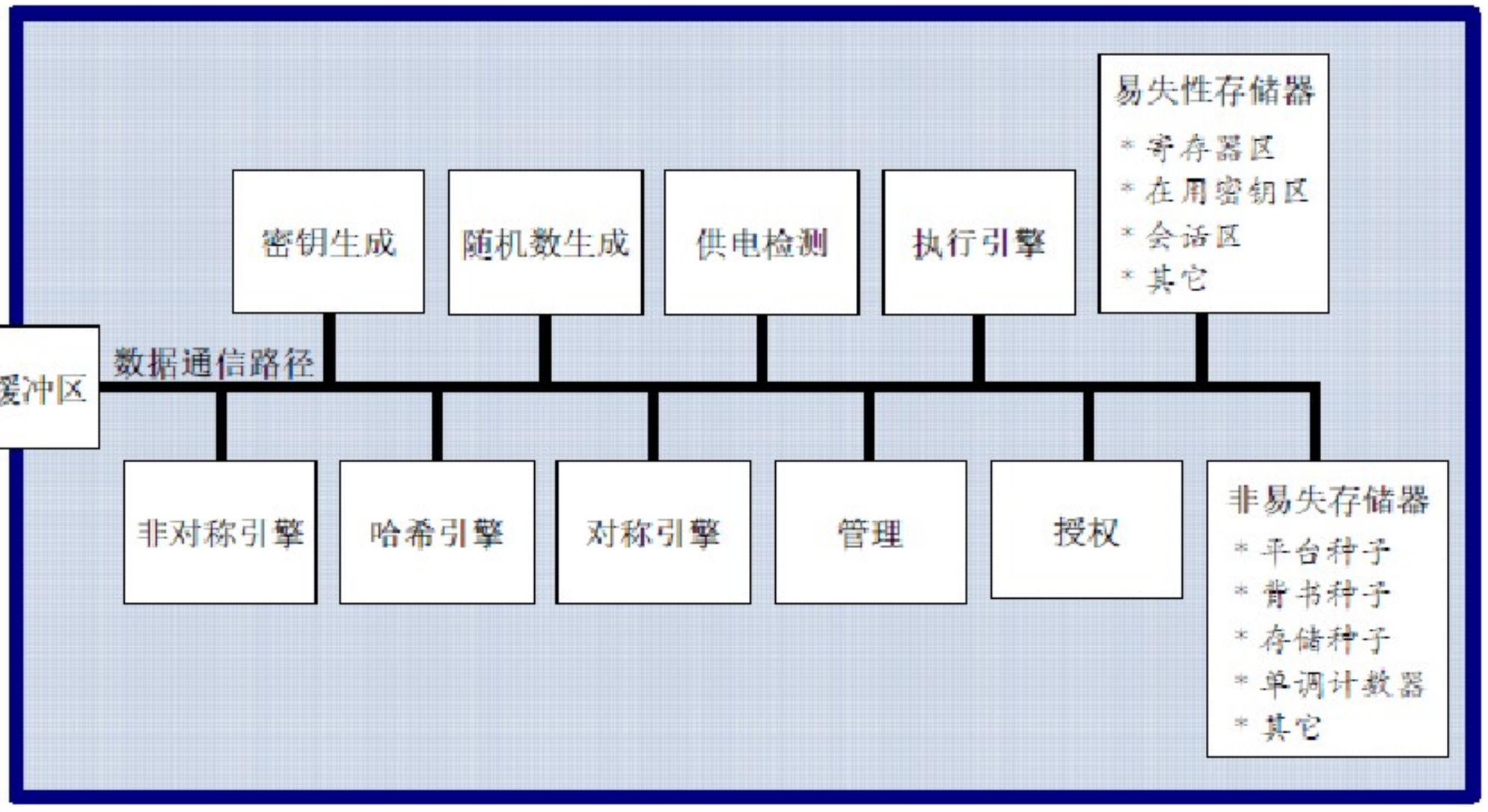
- 对外证明



(1) 外部实体证明TPM的真实性
(2) 外部实体证明平台拥有信任根
(3) 证明机构证明密钥对属于TPM
(4) 平台证明密钥对受TPM保护
(5) 平台证明那是平台度量的状态
(6) 外部实体证明被度量对象的可信性

5.3 可信平台模块TPM

- TPM组成结构



可信平台模块TPM

- 对称签名与验证

$$HMAC(K,m) = H((K \oplus opad) || H((K \oplus ipad) || m))$$

opad = 0x5c5c5c…5c5c; (长度等于一个块的大小)

ipad = 0x363636…3636; (长度等于一个块的大小)

5.4 TPM的基本用法

- 基于数据包的对话

1	头部
2	句柄区
3	授权区大小
4	授权区
5	参数区

命令包的构成

1	头部
2	句柄区
3	参数区大小
4	参数区
5	授权区

响应包的构成

TPM的基本用法

- 一个命令包

偏移量	大小	成分名称	成分值	
0	2	标记	TPM_ST_SESSIONS	
2	4	命令包长度	211	头部
6	4	命令码	TPM_CC_Example	
10	4	句柄A	相应值	
14	4	句柄B	相应值	句柄区
18	4	授权区大小	61	数值
22	4	authHandle	相应值	
26	2	nonceCallerSize	20	
28	20	nonceCaller	相应值	
48	1	sessionAttributes	相应值	授权区
49	2	hmacSize	32	
51	32	HMAC	相应值	
83	4	dataSize	124	
87	124	data[dataSize]	相应缓冲区	参数区
211				

命令包

注：大小以8位为一个单位。

TPM的基本用法

- 一个响应包

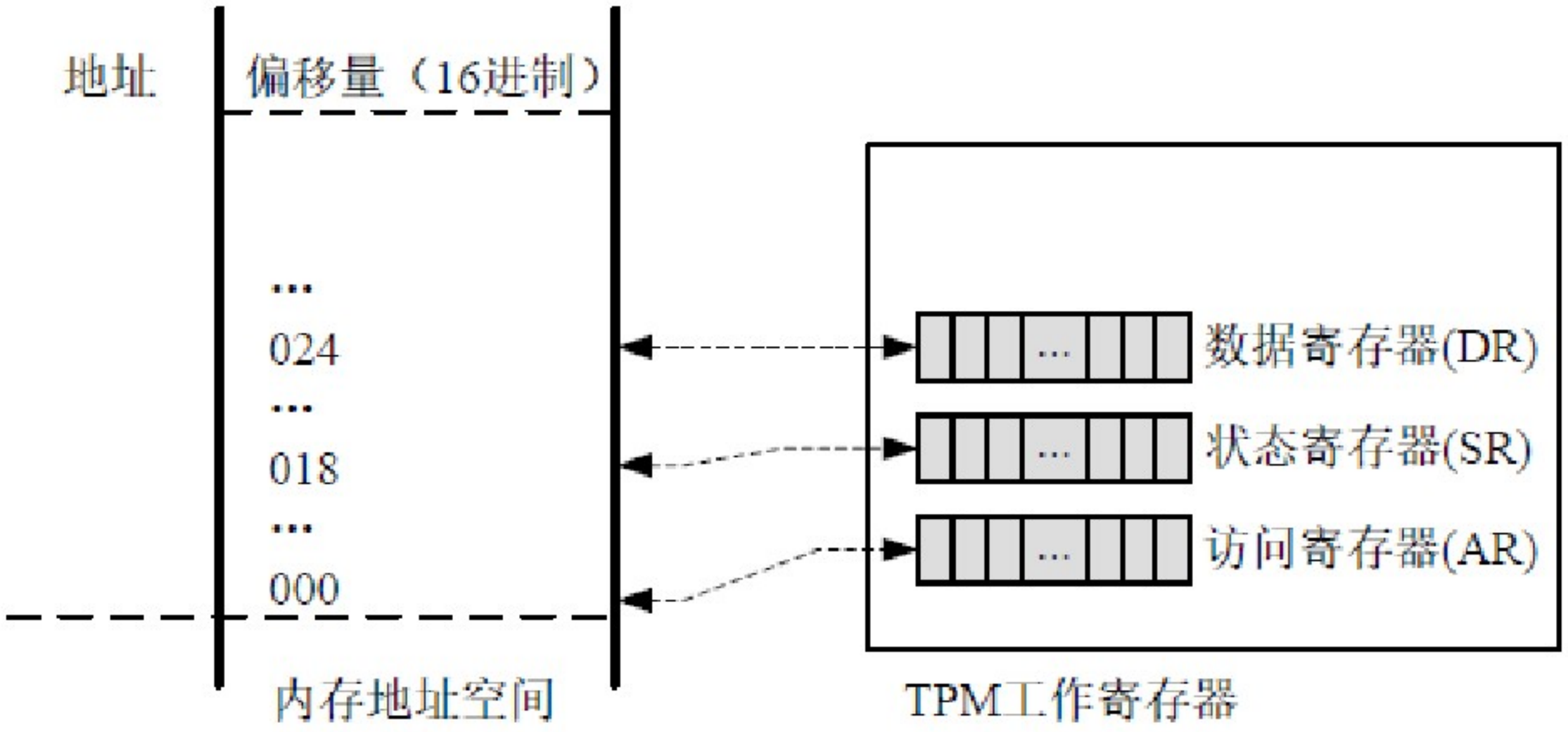
偏移量	大小	成分名称	成分值	
0	2	标记	TPM_ST_SESSIONS	
2	4	响应包长度	203	头部
6	4	响应码	0（表示成功）	
10	4	句柄	相应值	句柄区
14	4	参数区大小	128	数值
18	4	dataSize	124	
22	124	data[dataSize]	相应缓冲区	参数区
146	2	nonceTpmSize	20	
148	20	nonceTPM	相应值	
168	1	sessionAttributes	相应值	授权区
169	2	hmacSize	32	
171	32	HMAC	相应值	
203				

响应包

注：大小以8位为一个单位。

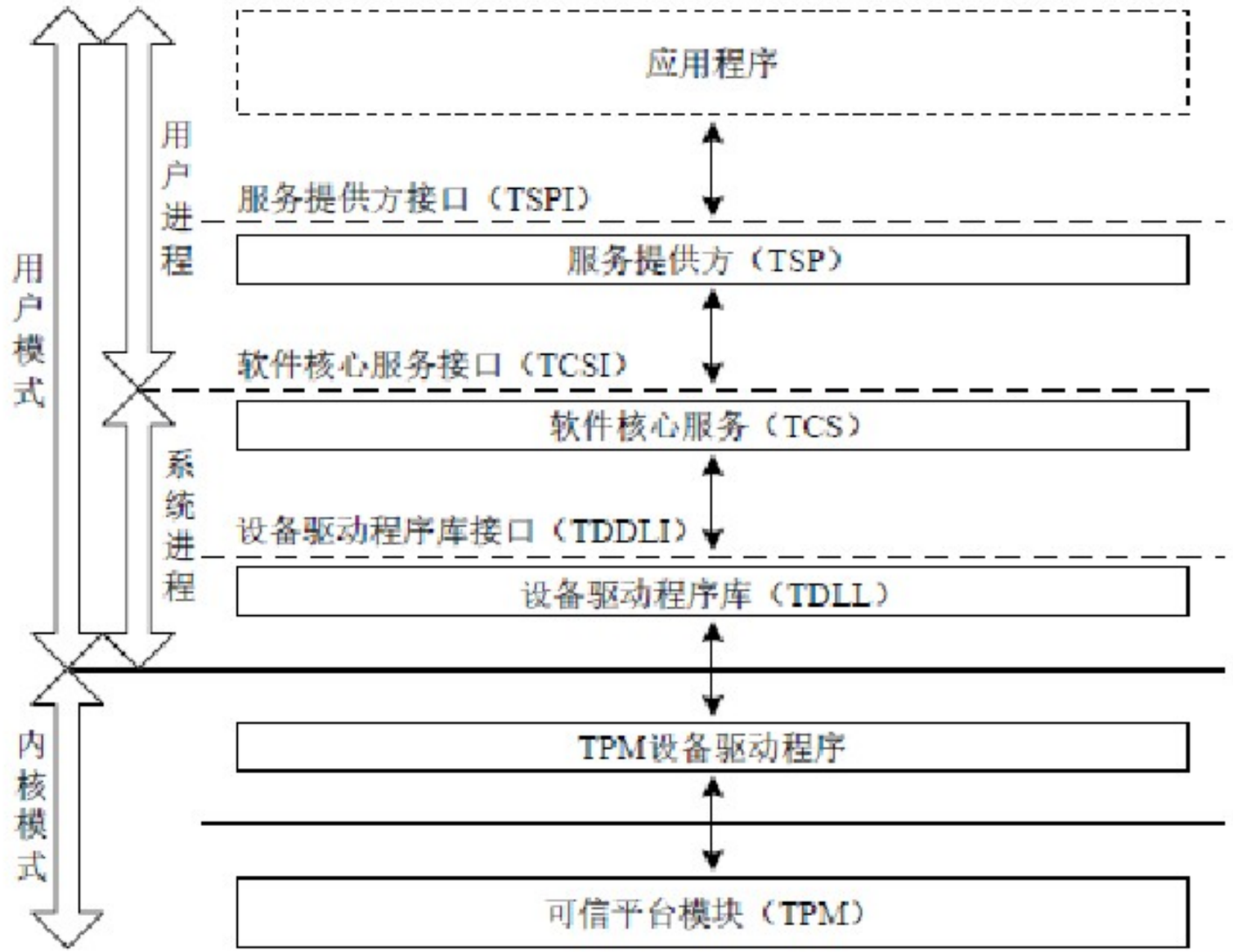
TPM的基本用法

- 原始的对话方法



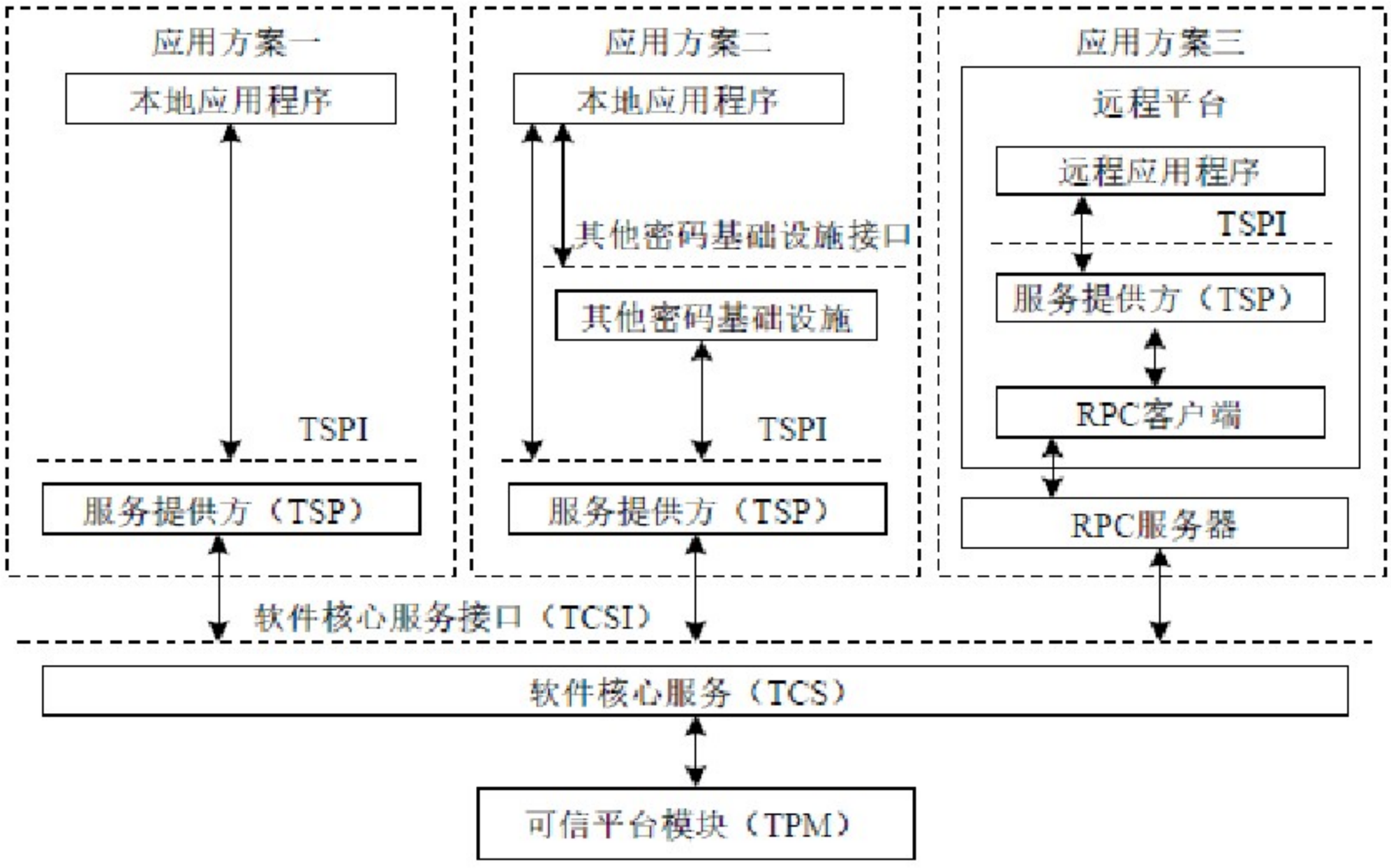
TPM的基本用法

❖可信平台软件体系结构



TPM的基本用法

❖可信平台应用方案类型



5.5 TPM应用案例

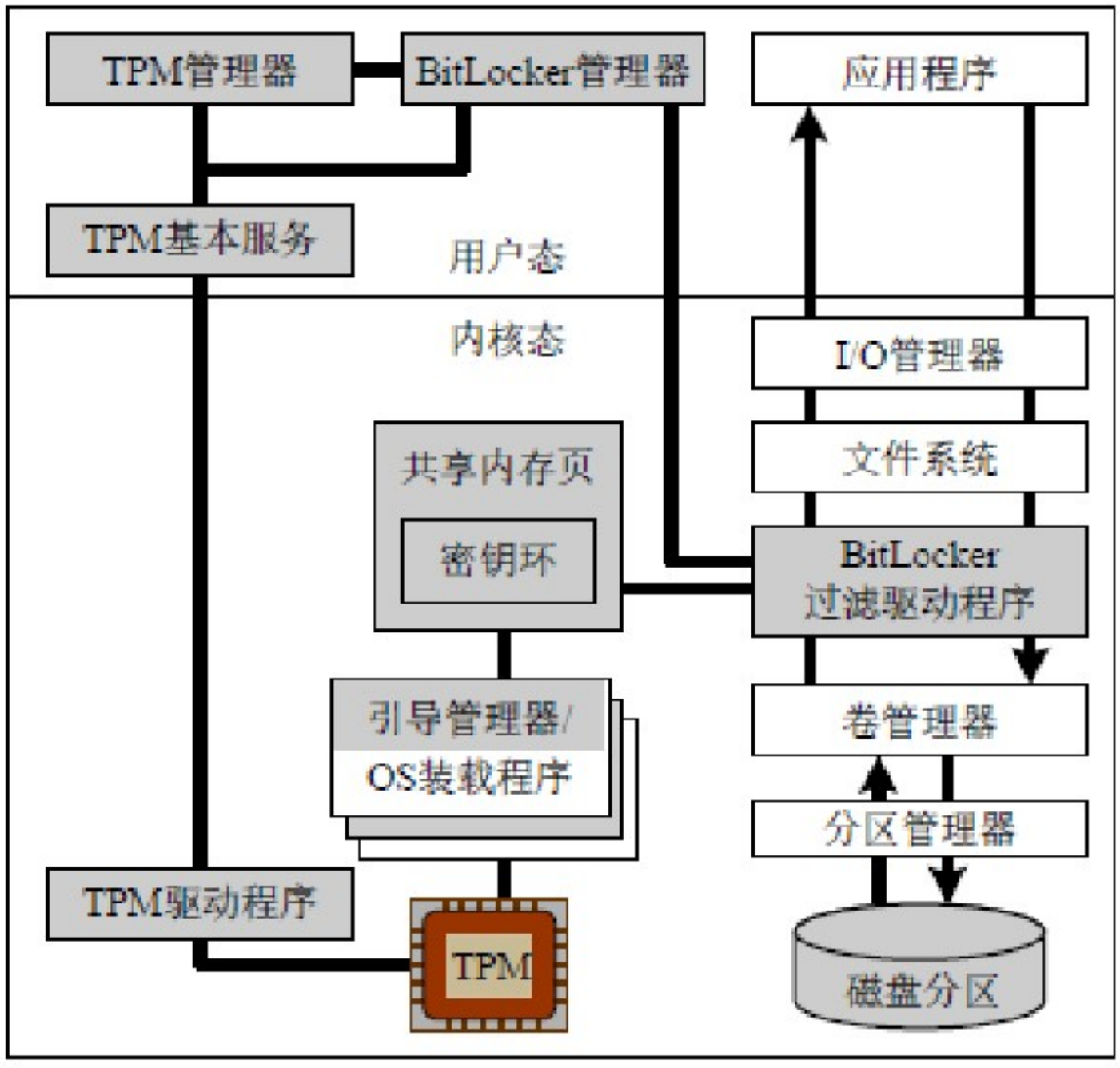
- BitLocker的主要功能
  - 整卷加密
  - 完整性检查

TPM应用案例

- BitLocker对分区的要求
  - 系统分区：引导系统所需的代码和数据
  - Windows分区：Windows操作系统和用户数据

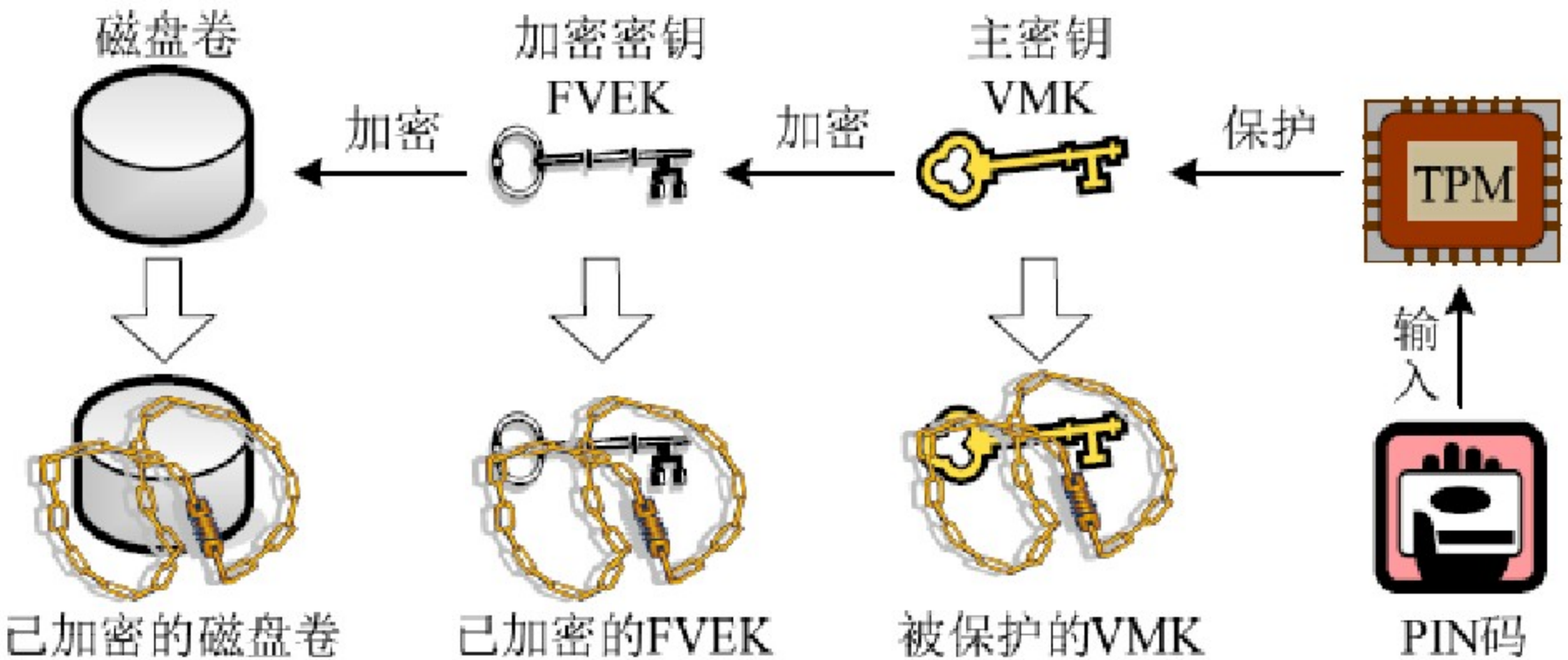
TPM应用案例

❖BitLocker的体系结构



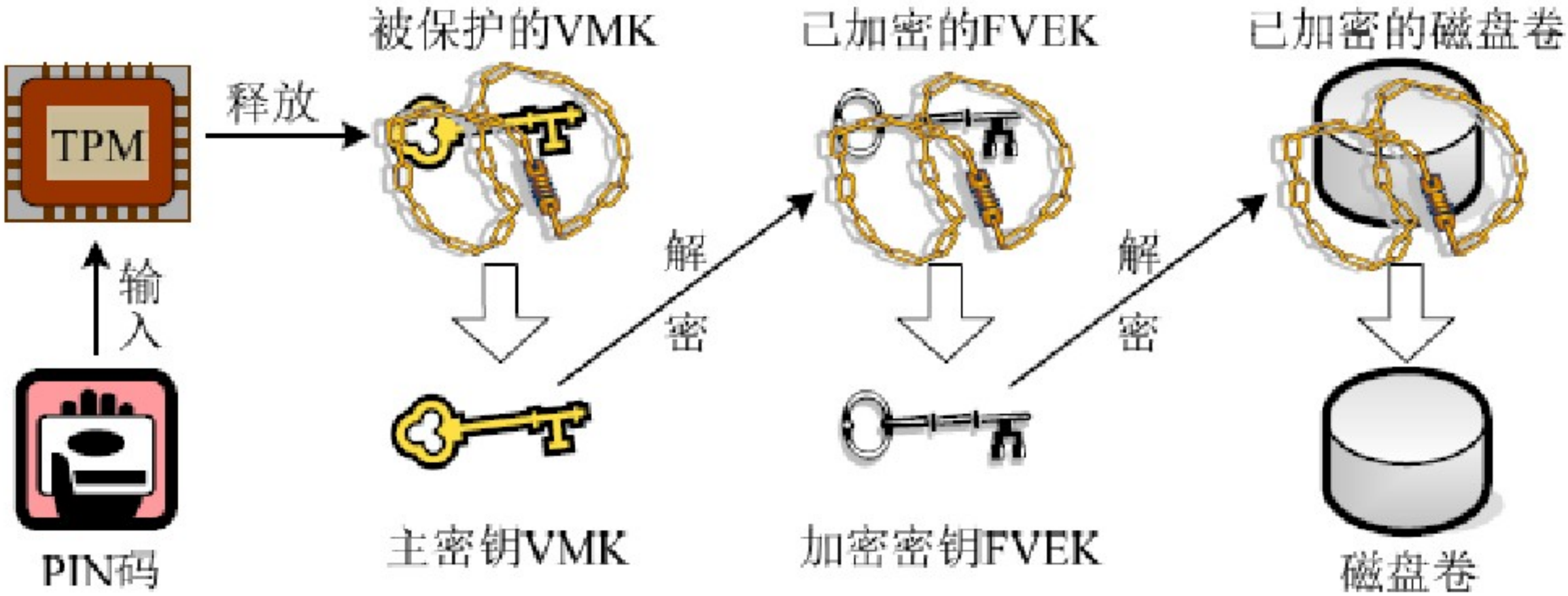
TPM应用案例

- BitLocker的加密原理



TPM应用案例

❖BitLocker的解密原理



TPM应用案例

- TPM的封装功能Seal
  - 加密<=+++++++++++++++++=PCR寄存器
  - PCR寄存器=++++++++++++=>解密

5.5 TPM应用案例

- 初次整卷加密时的封装
  - 计算机系统分区相关组件的哈希值
  - 把计算结果扩展到PCR寄存器
  - 用相应寄存器封装主密钥VMK

引导时的完整性检查

- 依次计算系统分区相关组件的哈希值
- 把计算结果扩展到PCR寄存器
- 试图解封装主密钥VMK

本章作业

1、为什么说纯软件安全机制在机密性和完整性方面都存在致命的不足？

2、验证一个TPM是否正宗的方法是检查它的背书密钥与背书证书是否匹配，匹配则正宗，不匹配则不正宗。请问以下验证需要检查什么匹配关系。

（1）验证一个平台是否拥有信任根；

（2）验证一对签名密钥是否属于某TPM；

（3）验证关于某被度量组件的可信性的结论是否真实。

本章作业

3、在一个可信平台上，当需要把受保护数据存放在宿主计算机硬盘中时，如何利用TPM保护这些数据的机密性和完整性？

4、假设没有引导 阶段的完整性检查，为什么向系统分区植入恶意代码就有可能破解BitLocker的数据保护机制？