信息安全概论

第六章 信息隐藏与版权管理

黄 玮

温故 密码学的传统应用：数据安全和通信安全

- 对称加密
- 公钥加密
- 数字证书
  - —对称加密
  - —公钥加密
  - —消息鉴别
  - —散列算法
  - —数字签名
- PKI
  - —数字证书

机密性

完整性

身份认证

授权

不可抵赖性

- 数字媒体技术发展的需要

内容安全

本章内容提要

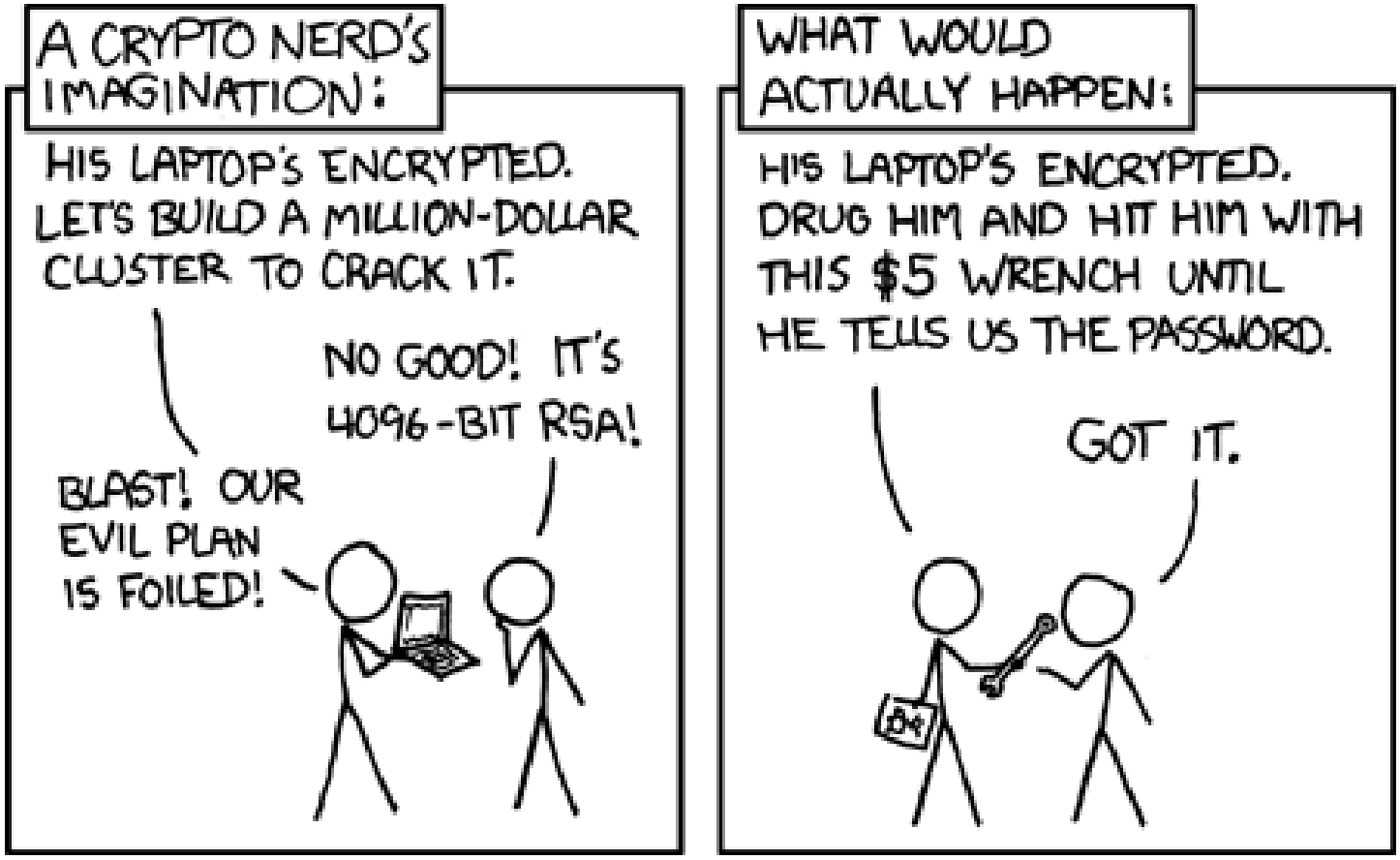
- **信息隐藏**
- 版权管理

本节内容提要

- 信息加密与信息隐藏
- 信息隐藏概述
- 信息隐藏与通信
- 信息隐藏的应用与演示

信息加密与信息隐藏

为什么有了加密还需要研究信息隐藏?




优酷
스테가노그래피(Steganography)
=隐写术（Steganography）
把特定信息（文件）隐藏在照片或者音乐中的技术=-

最“朴素”的信息隐藏方法


A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, A'LA'IH, A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, DO'NEH'LINI, A'LA'IH, A'LAIH, DO'NEH'LINI, A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, DO'NEH'LINI . . .
FOR ADDED SECURITY, AFTER WE ENCRYPT THE DATA STREAM, WE SEND IT THROUGH OUR NAVAJO CODE TALKER.
... IS HE JUST USING NAVAJO WORDS FOR "ZERO" AND "ONE"?
WHOA, HEY, KEEP YOUR VOICE DOWN!

信息加密与信息隐藏

- **信息加密**
  - —对秘密信息本身进行保护
  - —信息的传递过程是暴露的

- **信息隐藏**
  - —掩盖秘密信息存在的事实
  - —表面上看是A，其实真正传递的信息是B

林乌信我无机事，
息精息气养精神。
宫墙隐嶙围野泽，
天水藏来玉堕空。

信息隐藏概述

信息隐藏的研究领域

- 信息隐藏　　守
  - —在信息载体中隐藏尽可能多的信息
  - —不能引起任何可察觉的变化
    - 感观变化
    - 信息统计分析变化
- 信息隐藏分析　　攻
  - —在看似正常的信息载体中找出隐藏其中的秘密信息，篡改或破坏隐藏其中的秘密信息

信息隐藏的载体分类

- 图像
- 视频
- 音频

} ⟶ 感观冗余度

- 数据集合
  - —文本
  - —二进制数据
    - – Word / Excel / EXE …

信息隐藏基本思想

- 利用人类感知系统的冗余
- 利用计算机处理系统的冗余
- 利用各种潜信道

信息隐藏的支撑技术

- 数字信号处理理论
  - —图像信号处理
  - —音频信号处理
  - —视频信号处理
- 人类感知理论
  - —视觉理论
  - —听觉理论
- 现代通信技术
- 密码技术

信息隐藏的基本方法分类

- 时域（空域）替换技术
- 变换域技术
- 扩展频谱技术
- 统计方法

信息隐藏算法设计的安全性需求

- 非恶意破坏
  - —信息载体在传输过程中叠加了噪声
  - —有损压缩
- 恶意破坏
  - —消除隐藏的秘密信息

恶意破坏举例

- 数字图像

  —图像加噪、低通滤波、有损压缩、图像剪切、图像拼接、图像大小变化、图像旋转、打印扫描等。

- 数字视频

  —加噪、视频压缩编码、丢帧、插帧、帧重组、视频流剪切和拼接等。

- 数字音频

  —加噪、滤波、语音压缩编码、数模模数转换、重采样、采样率变化等。

- 数据集合

  —数据跨平台的格式转换，数据删除、数据添加等。

信息隐藏的应用领域

- 广义信息隐藏
  - —在某种载体中嵌入数据
- 两个分支
  - —信息隐藏
    - 伪装式隐蔽通信
  - —数字水印
    - 数字产品的版权保护（数字版权管理DRM）

将密码学与信息隐藏相结合，就可以同时保证信息本身的安全和信息传递过程的安全

信息隐藏问题描述

- 囚犯问题

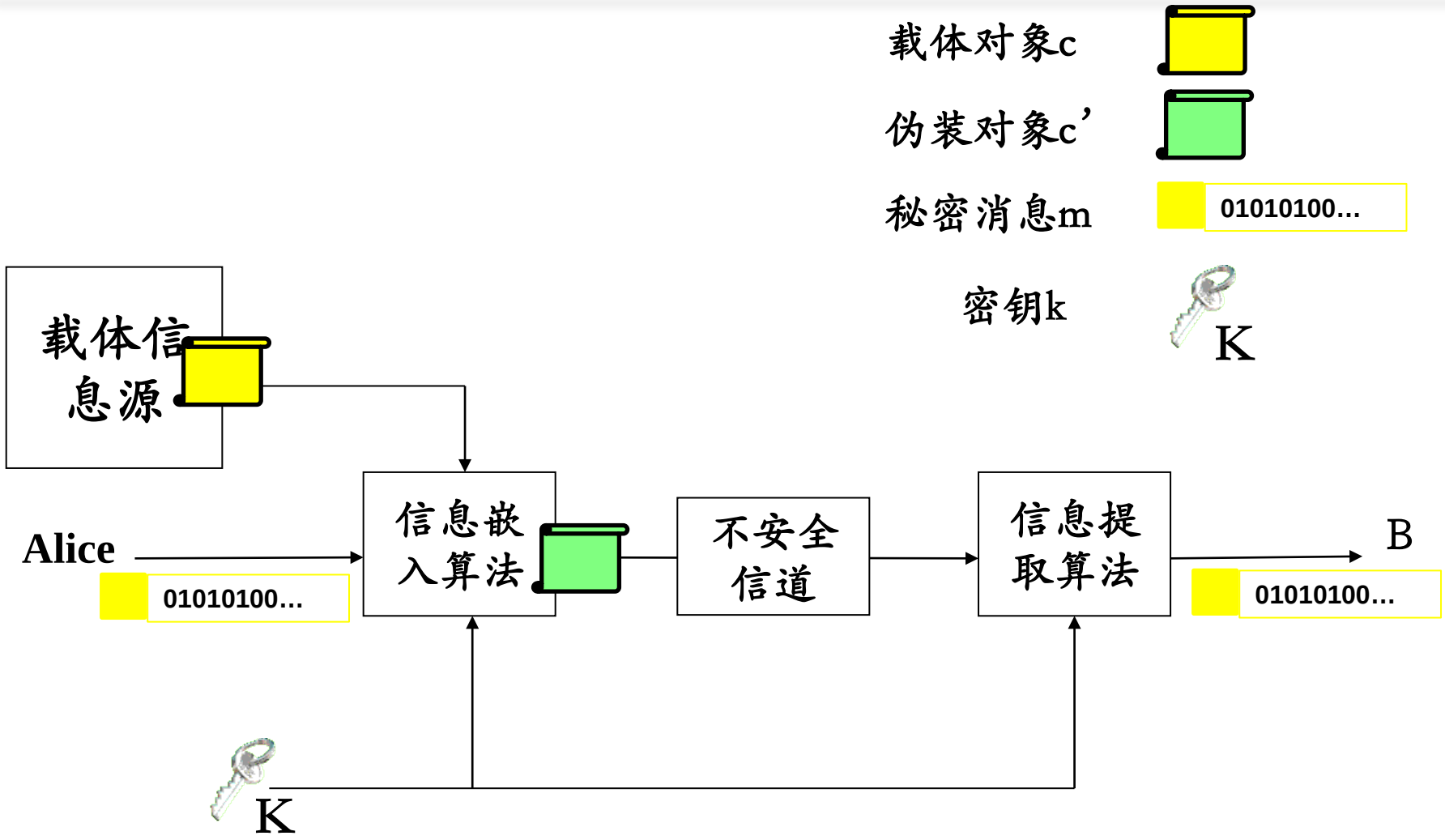
  —两个囚犯A和B被关押在监狱的不同牢房，他们想通过一种隐蔽的方式交换信息，但是交换信息必须要通过看守的检查。因此，他们要想办法在不引起看守者怀疑的情况下，在看似正常的信息中，传递他们之间的秘密信息

- 看守者

  —被动看守者：只是检查传递的信息有没有可疑的地方

  —主动看守者：故意去修改一些可能隐藏有信息的地方，或者假装自己是其中的一个囚犯，隐藏进伪造的消息，传递给另一个囚犯

信息隐藏的原理框图


载体对象c
伪装对象c’
秘密消息m
01010100…
密钥k
K
载体信息源
Alice
01010100…
信息嵌入算法
不安全信道
信息提取算法
B
01010100…
K

术语解释

- A打算秘密传递一些信息给B，A需要从一个随机消息源中随机选取一个无关紧要的消息c，当这个消息公开传递时，不会引起怀疑，称这个消息c为**载体对象**
- 把需要秘密传递的信息m隐藏到载体对象c中，此时，载体对象c就变为**伪装对象**c’
- 秘密信息的嵌入过程需要密钥，此密钥称为**伪装密钥**

实现信息隐藏的基本要求

- 载体对象是正常的，不会引起怀疑
- 伪装对象与载体对象无法区分，无论从感观上，还是从统计分析上
- 信息隐藏的安全性取决于第三方有没有能力将载体对象和伪装对象区别开来
- 对伪装对象的正常处理，不应破坏隐藏的信息

信息隐藏的安全性

- 信息隐藏系统的安全性
  - —系统自身算法的安全性
  - —各种攻击情况下的安全性
- 攻击一个信息隐藏系统
  - —证明隐藏信息的存在
  - —篡改隐藏信息
  - —破坏隐藏信息
  - —提取隐藏信息
- 安全的：如果攻击者经过各种方法仍然不能判断是否有信息隐藏

攻击者：判断是否有隐藏

- 定义一个检验函数 $f: C \rightarrow \{0, 1\}$

$$f(c)=\begin{cases}1 & c\text{中含有秘密消息}\\ 0 & \text{其它}\end{cases}$$

判断结果

- 实际有隐藏，判断有隐藏——正确
- 实际无隐藏，判断无隐藏——正确
- 实际无隐藏，判断有隐藏——错误
  ——误判
- 实际有隐藏，判断无隐藏——错误
  ——漏判

实用的信息隐藏系统

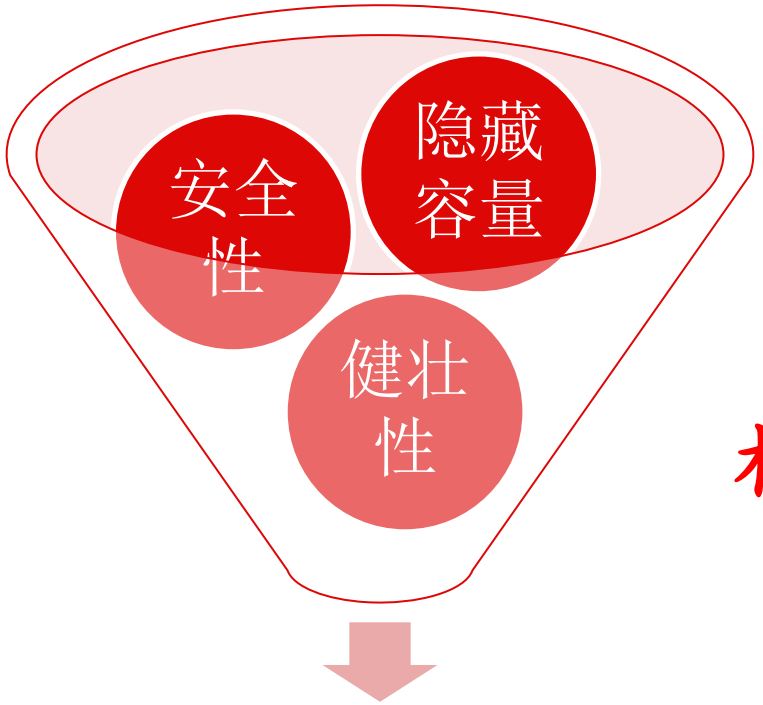
- 假设
  - —攻击者误判的概率为α
  - —攻击者漏判的概率为β
- 一个实用的信息隐藏系统应该尽可能使β最大
- 一个理想的信息隐藏系统应该有β=1
  - —所有藏有信息的载体都被认为没有隐藏信息而被放过，达到了信息隐藏、迷惑攻击者的目的

信息隐藏的攻击

- 被动攻击
  - —监视和破译隐藏的秘密信息
- 主动攻击
  - —破坏隐藏的秘密信息
  - —篡改秘密信息
- 非恶意修改
  - —压缩编码，信号处理技术，格式转换，等等

信息隐藏的健壮性

- 伪装载体受到某种攻击后，仍然能够从中提取出隐藏信息，称为算法对这种攻击是健壮的



相互制约

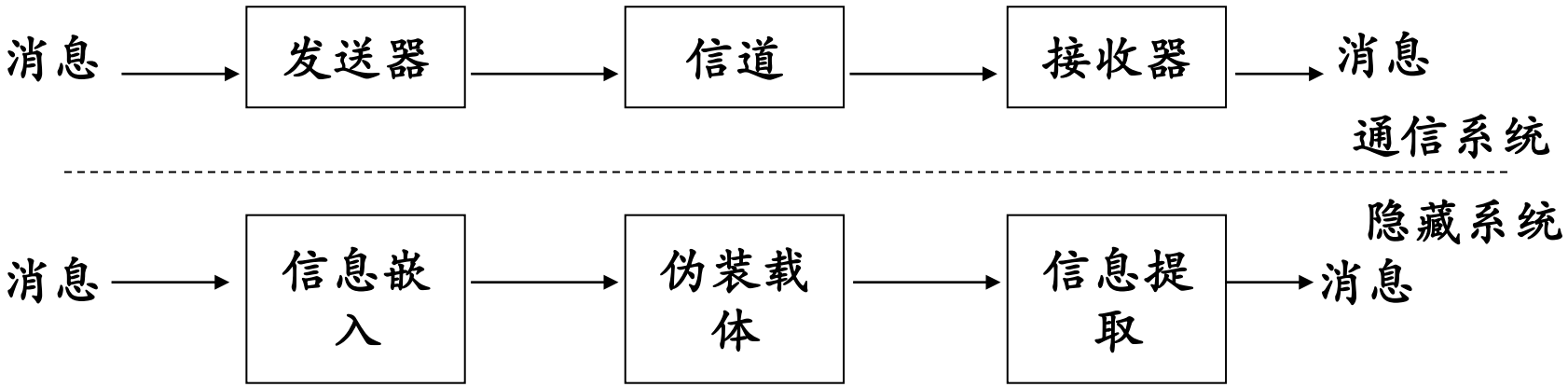
信息隐藏与通信

信息隐藏的通信模型

- 目前对信息隐藏的理论研究还不充分
  - —缺乏像Shannon通信理论这样的理论基础
  - —缺乏对人类感知模型的充分理解
  - —缺乏对信息隐藏方案的有效度量方法等
- 目前一种研究方法是：将信息隐藏过程类比于隐蔽信息的通信过程

隐藏系统与通信系统的比较(1/3)

- 可以将信息隐藏的载体看作通信信道，将待隐藏信息看作需要传递的信号，而信息的嵌入和提取分别看作通信中的调制和解调过程



隐藏系统与通信系统的比较(2/3)

- 目标相同：都是向某种媒介（称为信道）中引入一些信息，然后尽可能可靠地将该信息提取出来
- 约束条件：
  - —通信系统：最大的平均功率或峰值功率约束
  - —隐藏系统：感观约束

隐藏系统与通信系统的比较(3/3)

- 信道干扰
  - —通信系统：主要为传输媒介的干扰，如设备噪声、大气环境干扰等
  - —隐藏系统：不只受到无意的干扰，还受到各种主动攻击
  - —隐藏系统：已知更多的信道信息（载体信号是已知的）

通信模型分类——根据噪声性质分类

- 加性噪声信道模型
  - 设原始图像为I_0，待隐藏信息为W，隐藏后图像为I_1，接收端收到的图像为I_2，待隐藏信息经过特定的处理后加载到图像的空间域或变换域中，用$I_1-I_0=f(W)$表示，图像在信道中受到的处理用$I_2-I_1=P$表示
- 非加性噪声信道模型（几何变换）
  - 但有一些攻击不能用加性噪声表示，如图像的平移、旋转等，这些处理不仅影响象素值，而且还影响数据的位置。
  - 这类攻击信道表示为几何信道，并分为两类：针对整个图像的几何变换，包括平移、旋转、尺度变化和剪切，可以用较少的参数描述；另一类是针对局部的几何变换，如抖动等，需要更多的参数来描述

通信模型分类——按载体对检测器的贡献分类

- 将载体等效为噪声，认为载体未知
  - —将载体图像与信号处理、攻击同等对待。信息提取端将载体、信号处理和攻击都看作信道噪声和干扰
- 利用已知载体的信息
  - —如果将载体内容仅仅视为噪声，则忽略了“信息嵌入端完全知道载体的内容”的事实
  - —把载体内容视为信道边信息
  - —Cox认为这种模型与已知边信息的通信模型很类似
  - —寻找最佳嵌入方案，设计更有效的信息嵌入和提取方法：定义某种距离的度量，在允许干扰范围内，选择载体图像，使得检测概率最大

通信模型分类——按是否考虑主动攻击分类

- 主动攻击的建模难度很大，一些文献只考虑原始载体和某类信号处理对信息隐藏的影响（被动攻击）
- 利用博弈论思想考虑主动攻击的影响

  —把信息隐藏看作信息隐藏者和攻击者之间的博弈过程，定义载体信号嵌入信息前后、受到攻击前后的距离，在这种距离定义条件下，嵌入过程和攻击过程分别受到约束，隐藏容量就是平衡点处的容量值

信息隐藏的应用与演示

信息隐藏的应用(1/2)

- 军事和情报部门
  - —现代化战争的胜负，越来越取决于对信息的掌握和控制权
  - —军事通信中通常使用诸如扩展频谱调制或流星散射传输的技术使得信号很难被敌方检测到或破坏掉
  - —伪装式隐蔽通信正是可以达到不被敌方检测和破坏的目的

信息隐藏的应用(2/2)

- 需要匿名的场合
  - —包括很多合法的行为，如公平的在线选举、个人隐私的安全传递、保护在线自由发言、使用电子现金等
  - —非法的行为，如诽谤、敲诈勒索以及假冒的商业购买行为

信息隐藏检测

- 在信息隐藏技术的应用中，使用者的伦理道德水平并不是很清楚
- 信息隐藏的对立面——隐藏检测技术应运而生

信息隐藏演示实验

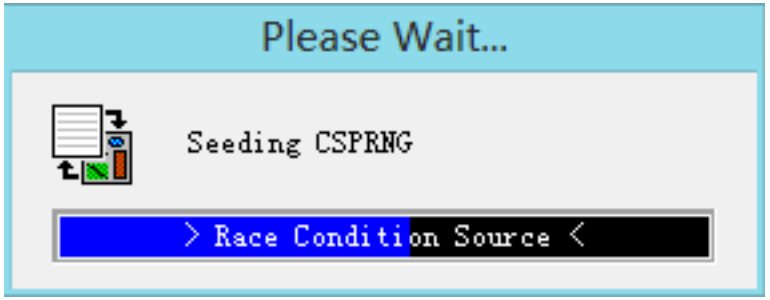
- 图像信息隐藏
  - —利用GIF图片的注释字段
    - http://weibo.com/1651460060/wr0qmmljqv
  - —图像隐写术：openstego
- 视频信息隐藏
  - —openpuff

openpuff

- 专业信息隐藏工具
  - 基于硬件的随机数生成器
  - 可否认信息隐藏
  - 支持链式载体（最大支持256Mb隐藏数据）
  - 载体信息利用率选择
  - 支持16种现代密码学算法
  - 多层数据混淆（支持3个独立口令）
- 独有的安全和混淆特性
- 支持多种载体格式
  - 图片支持 (BMP, JPG, PCX, PNG, TGA)
  - 音频支持 (AIFF, MP3, NEXT/SUN, WAV)
  - 视频支持 (3GP, MP4, MPG, VOB)
  - Flash-Adobe 支持 (FLV, SWF, PDF)
- 绿色便携软件
- 免费软件
  - 核心加密库开源

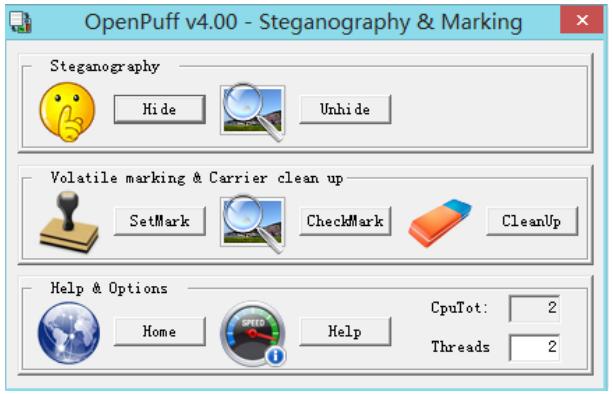
openpuff独有的安全和混淆特性

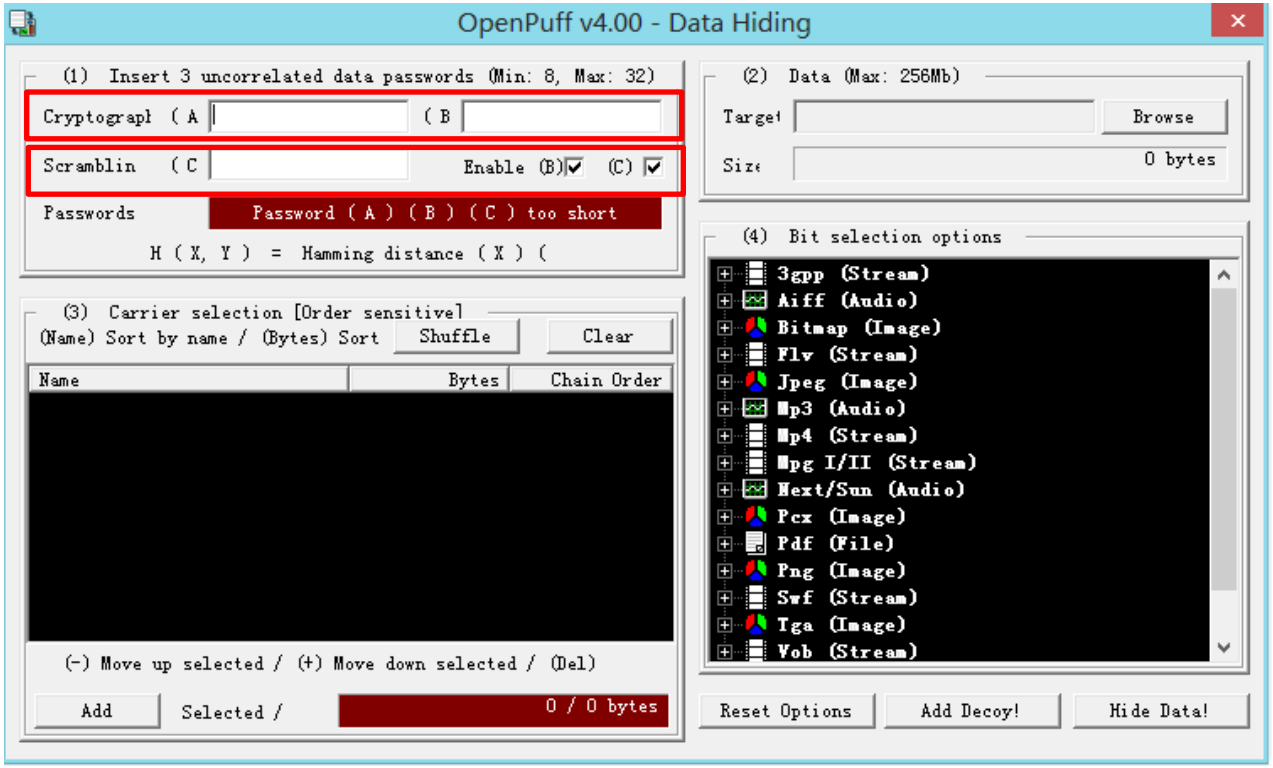
- 隐藏数据在注入信息载体之前，需要经过
  - —加密
    - 二次对称加密（16种候选加密算法、2个独立256bit加密密钥）
  - —扰乱
    - 密文被使用基于第三个独立密钥的CSPRNG产生的随机序列随机分块打乱
  - —白噪声化
    - 扰乱后密文被使用基于独立CSPRNG产生的白噪声序列随机填充
  - —自适应非线性编码
    - 白噪声混入后密文数据与原始信息载体一起被进一步使用非线性编码，对抗信息隐藏检测



openpuff使用截图

- 密码学加密密钥：A、B
- 随机扰乱算法种子值：C





本章内容提要

- 信息隐藏
- **版权管理**

本节内容提要

- 从传统媒体到数字媒体
- 从数据安全到内容安全
- 从条件接收到数字版权管理
- 版权保护系统基本框架
- 版权保护系统关键技术
  - —数字水印与版权保护
  - —媒体指纹与版权保护

从传统媒体到数字媒体

数字化时代——设备

- 报纸/杂志 VS. 电纸书/Kindle
- 卡带机 VS. iPod
- 电视 VS. iTV
- 电话 VS. 智能手机

数字化时代——内容

- 纸质出版物 VS. 电子出版物
- 磁带 VS. MP3
- 胶片 VS. MP4

Everything is connected…

- 从互联网到移动互联网
- 从计算机联网到物联网

—任何数字化设备均可实现联网

– 数字内容的生产和传播不受时空限制

数字时代，移动互联，个性服务，在线生活

模拟时代内容版权的核心在于介质

- 内容版权与内容出版技术
  - —Copyright 副本的权利
- 版权管理 == 介质管理
  - —报纸/图书
  - —磁带/录像带
  - —CD/VCD/DVD
  - —电视频道
    - 条件接收
- 模拟内容复制和分发费时费力并且效果欠佳
- 版权拥有者和用户的价值关系靠纸、塑料和电缆维系

- 数字时代的福音
  - —创建、处理、分发、存储和体验数字内容更加便捷
  - —媒体应用范围迅速扩大
    - 人人都是自媒体（iphone == 录音笔+摄影机+数码相机）
  - —成本降低
    - 载体价值：几乎零成本（免费的云存储）
    - 复制成本：几乎为零（C-V）
    - 分发成本：边际成本逼近零（Web 2.0、微博）

数字时代的困境

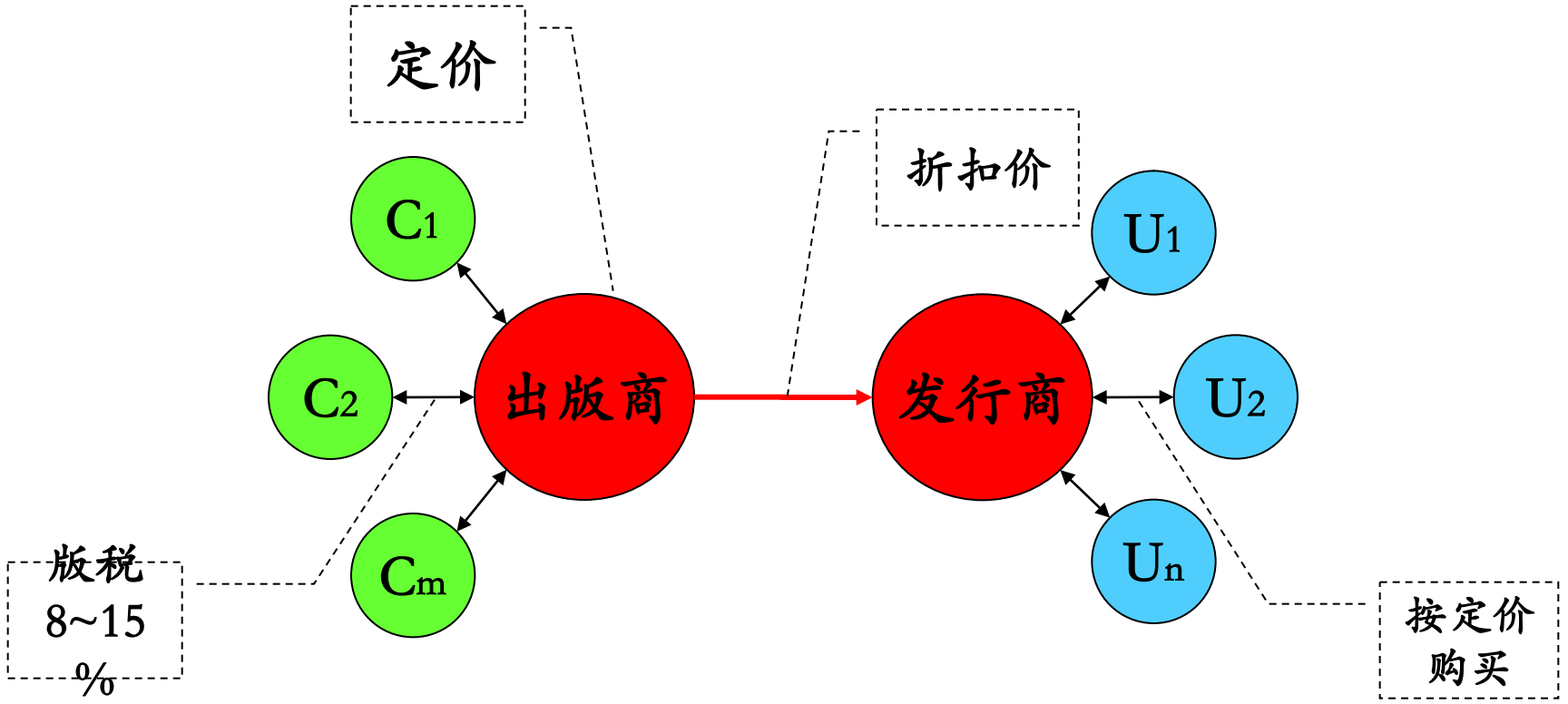
- 内容和介质逐渐无关

—DVD→ U盘 → 视频网站

—（有线、无线）电视→网络电视

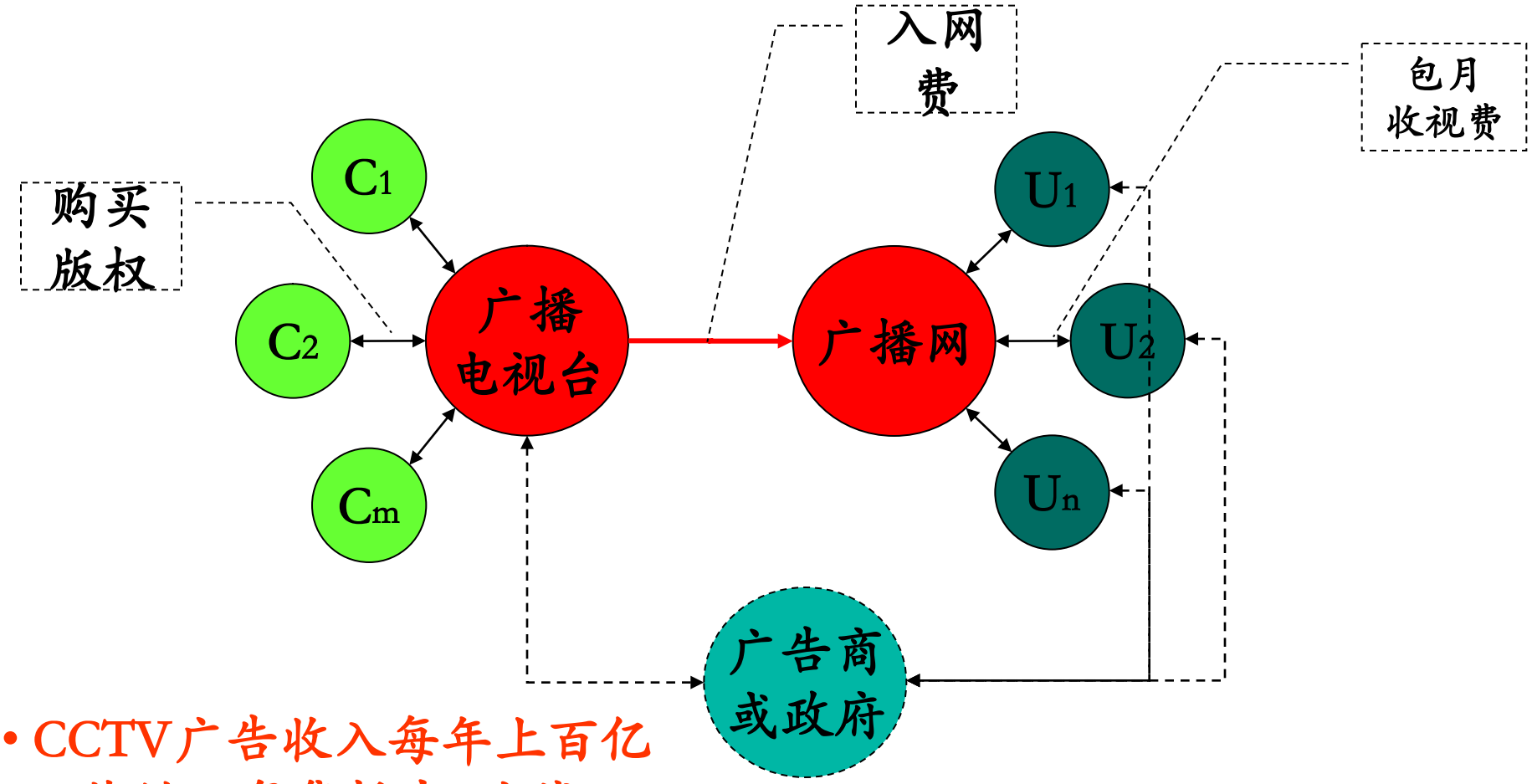
介质无法作为版权控制的手段了

“模拟”媒体：出版业



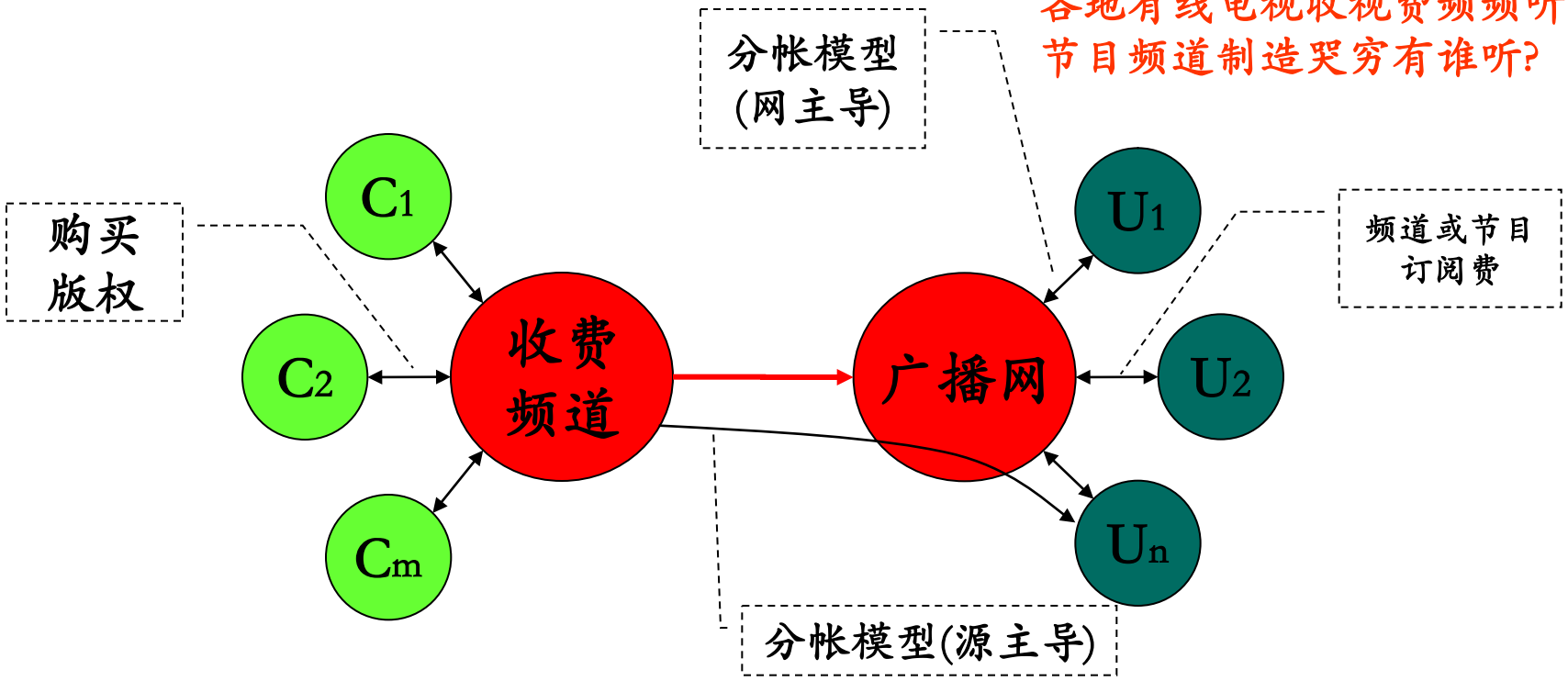
非创意成本：*出版社、印刷厂、运输公司、书店、回收* > 80%

“模拟”媒体：开放广播电视



- CCTV广告收入每年上百亿
- 《蓝猫》每集播出3块钱

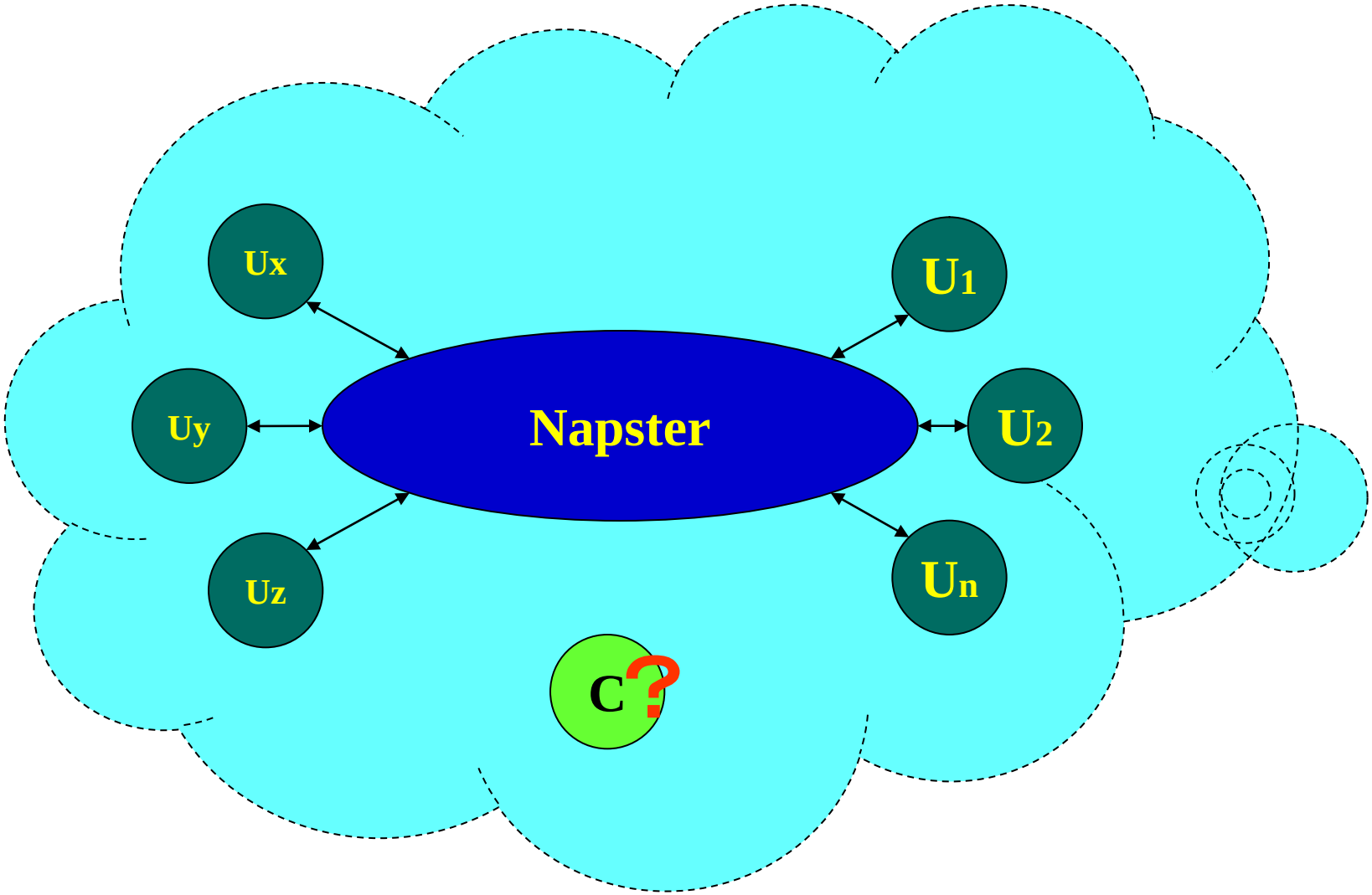
“模拟”媒体：收费广播电视



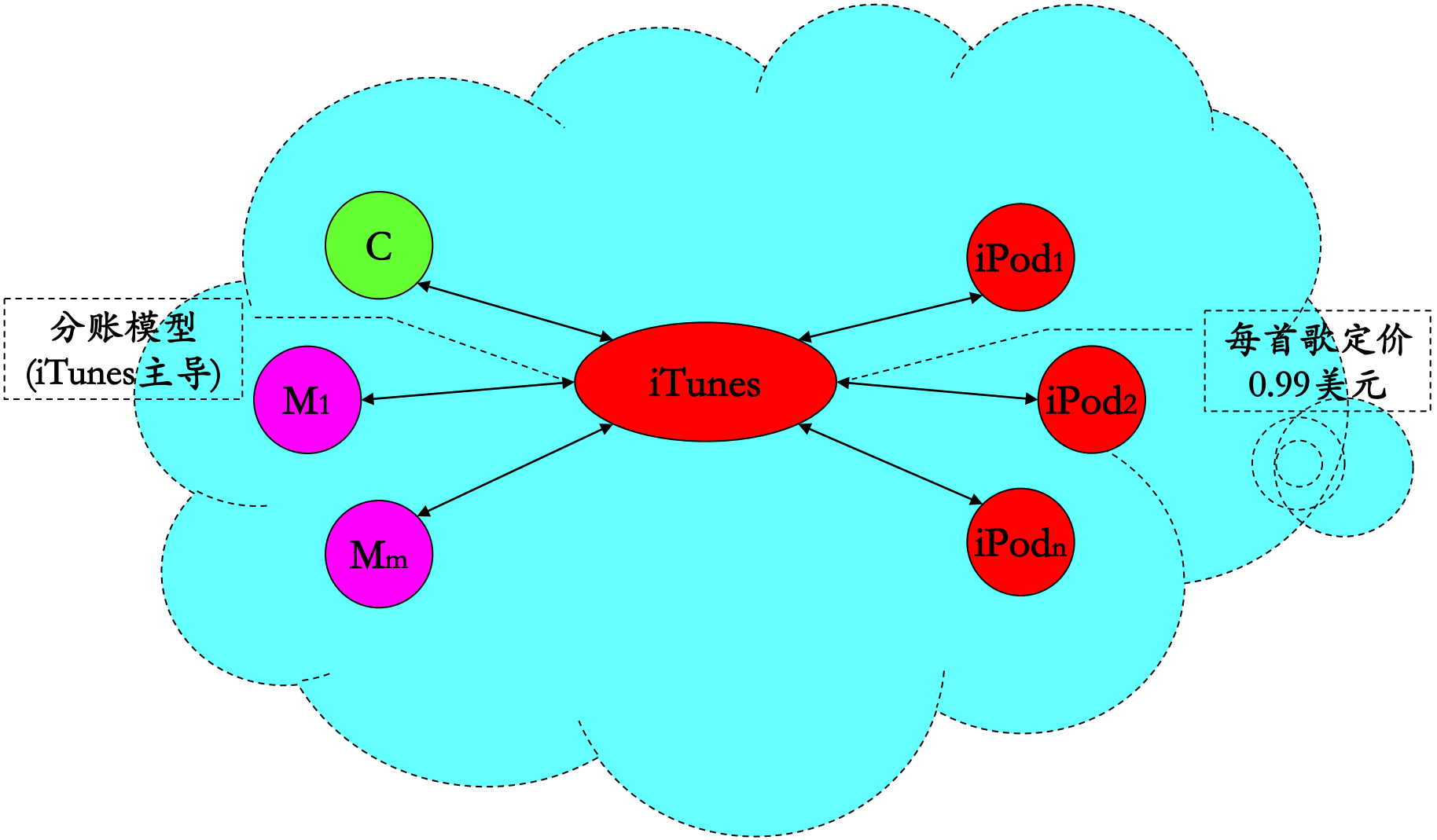
各地有线电视收视费频频听证
节目频道制造哭穷有谁听?

央视高清频道年收入才一百多万

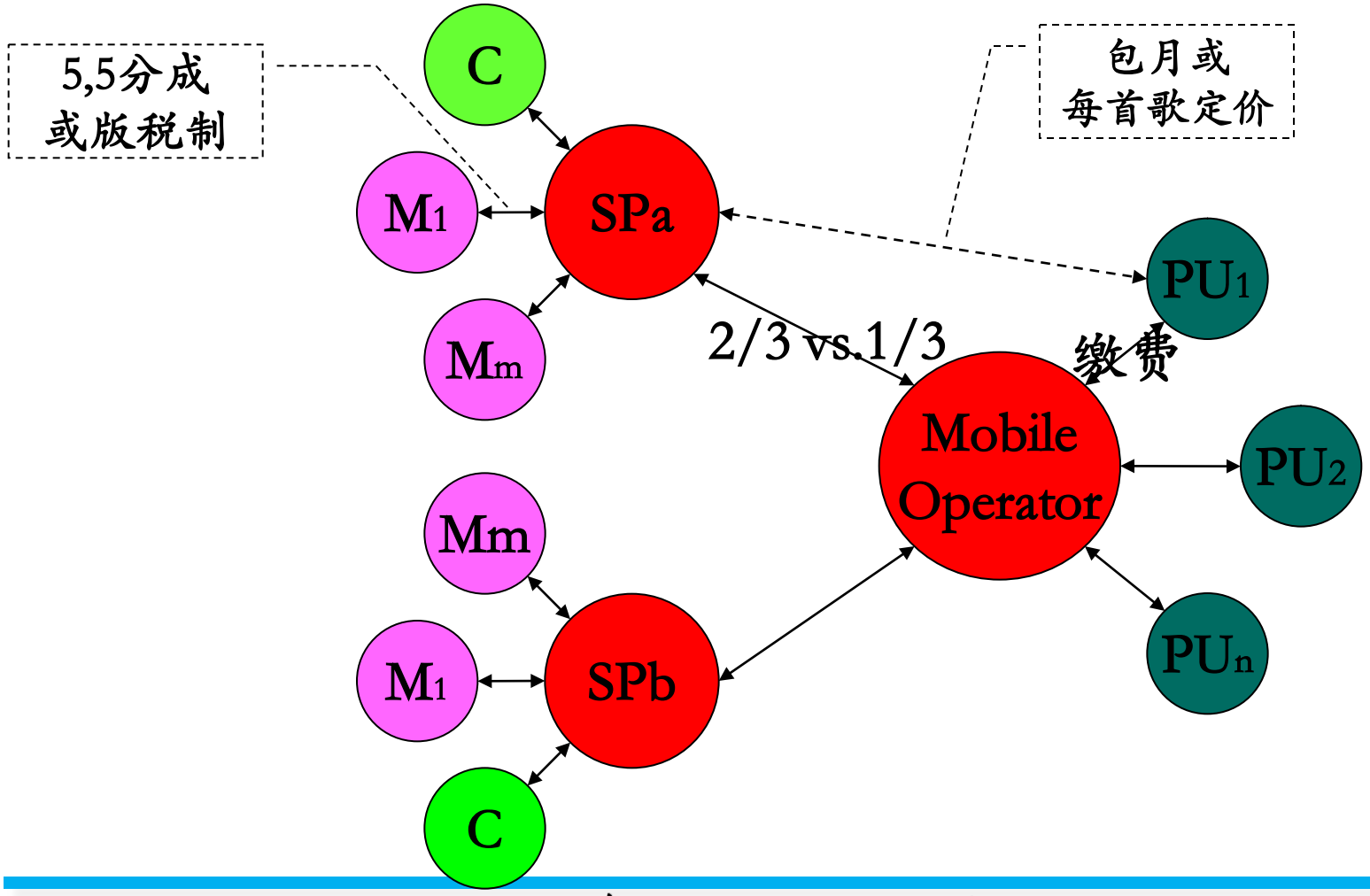
数字媒体： Napster——数字音乐P2P分享



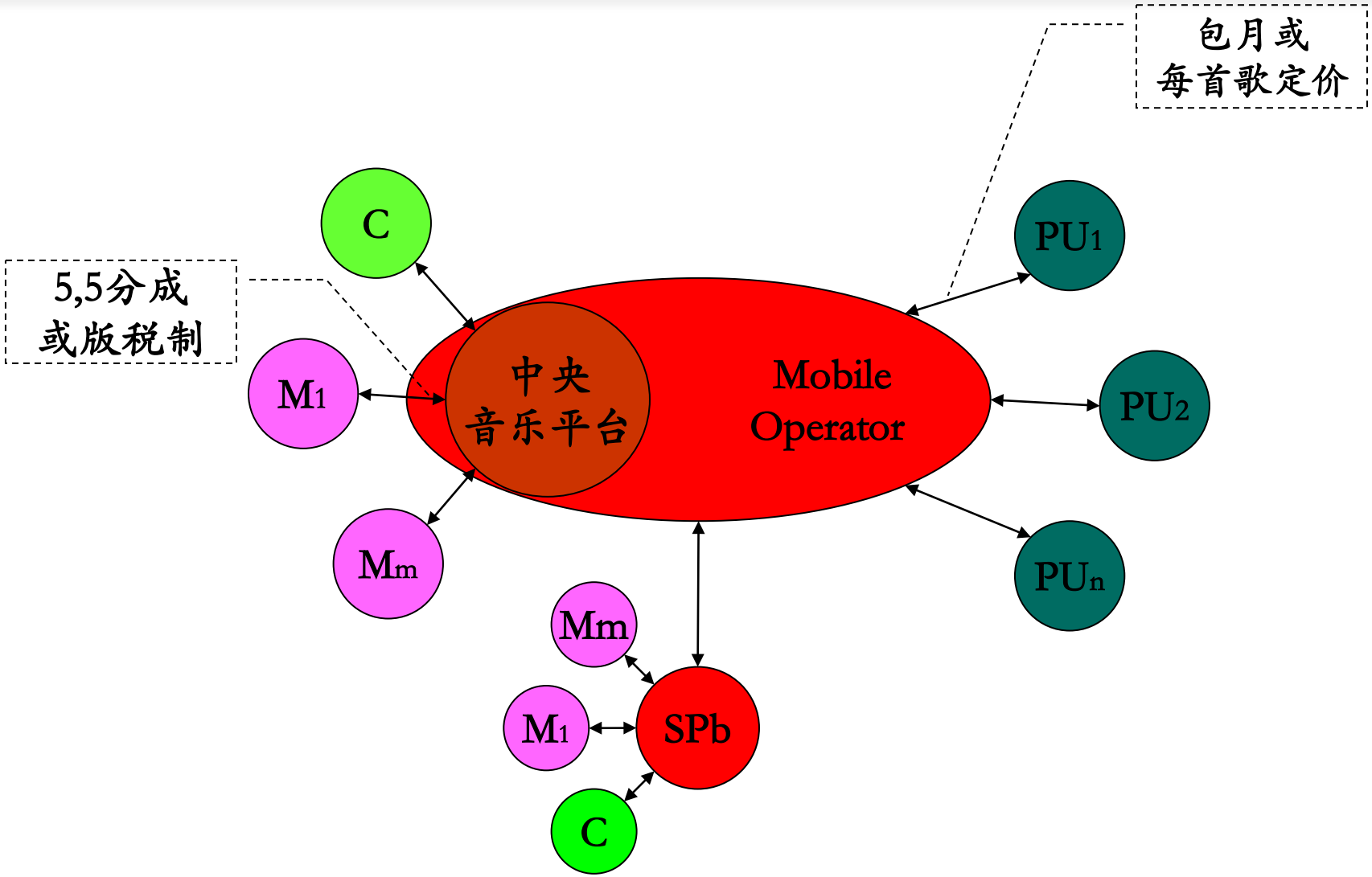
数字媒体：Apple



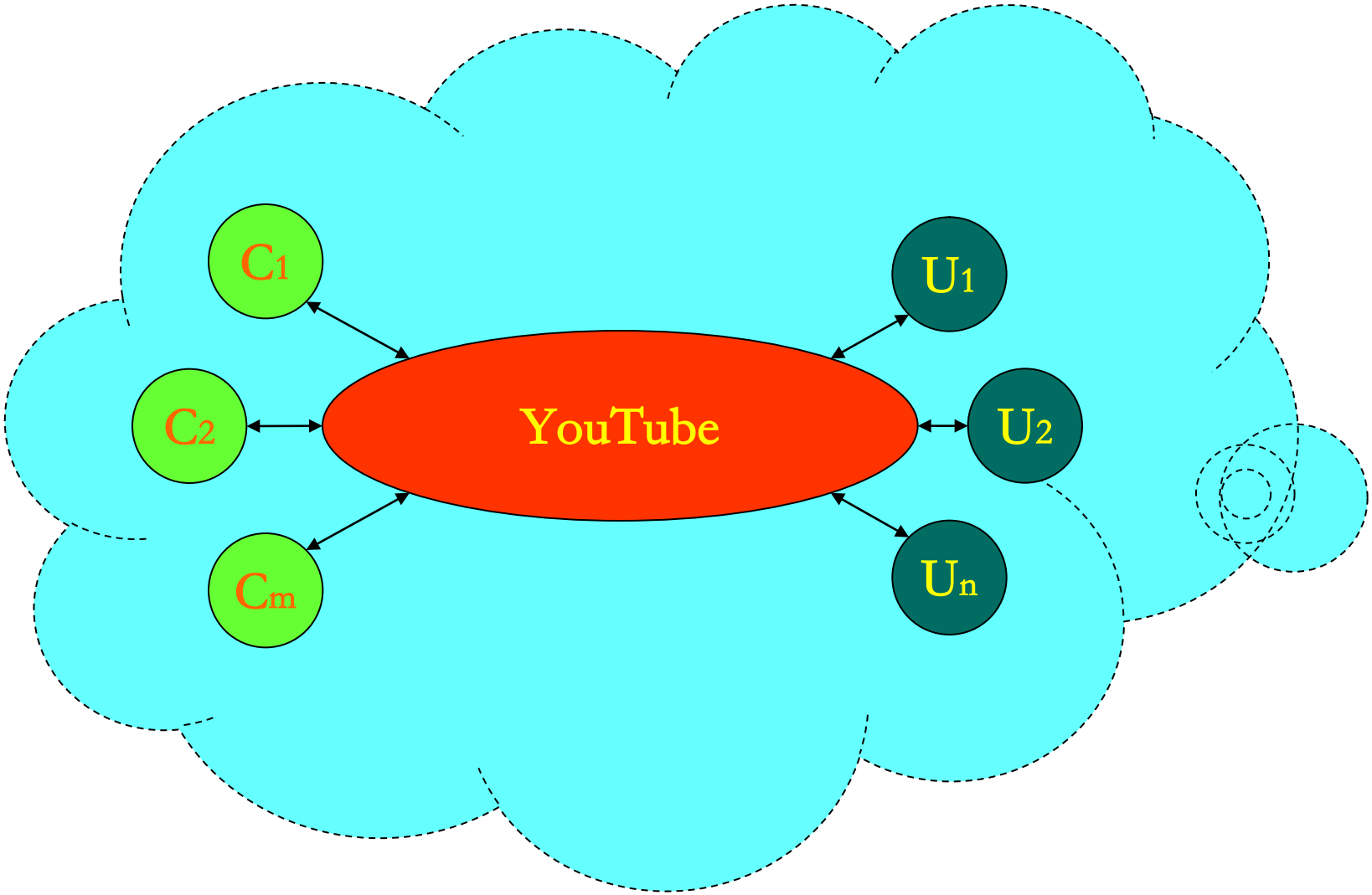
数字媒体：移动音乐(SP模式)



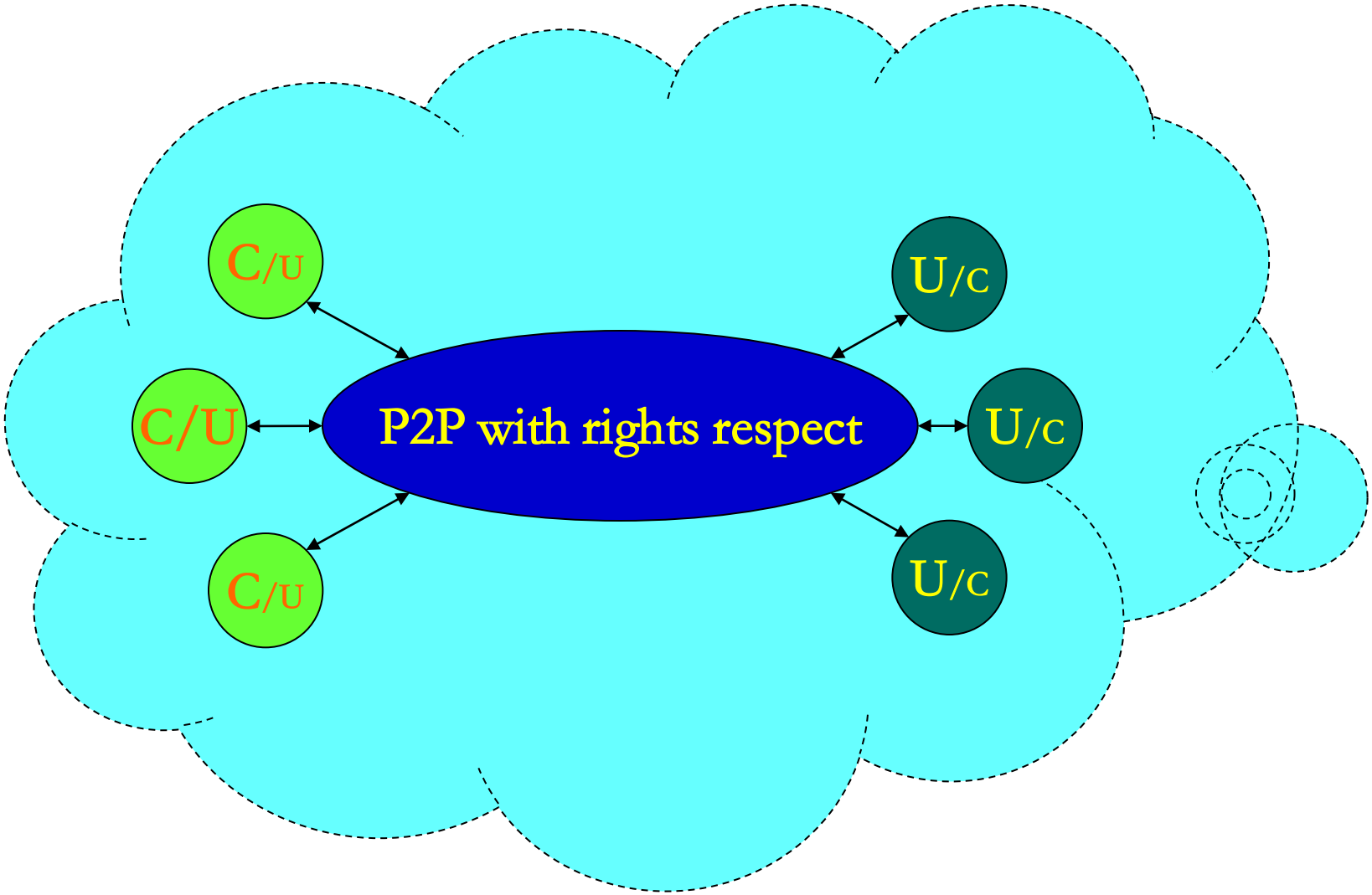
数字媒体：移动音乐(运营商主导)



数字媒体：YouTube



数字媒体 over 互联网



当前新媒体

- 特点：
  - —创作：由大量的个人或团队拍摄创作的音视频或其他形式的多媒体作品
  - —传播：通过互联网进行全球性共享和快速传播
  - —使用：任何人都可以通过互联网从海量媒体中即时选择自己喜欢的内容进行欣赏
- 打破模拟媒体的束缚：
  - —创作群体小、传播渠道固定、用户使用方式受限

未来新媒体

- 特点：
  - —交互：固定音视频节目与互动场景的有机结合，更有利于用户介入
  - —分发：节目一旦制作完成，可以自动通过Web、IPTV和Mobile等多种渠道分发
  - —版权：尊重创作、改编、分发、使用等主体之间形成明晰的版权和权益关系
- 建设数字媒体新价值链
  - —在网络化数字空间中建设新的共生价值链

从数据安全到内容安全

数字时代对信息安全的要求

	前数字时代	数字时代
机密性	机密内容不可解读	隐私内容不可解读
完整性	精确检测内容是否被篡改（哪怕是1bit改动都不允许）	“内容”不可篡改，但“数据”可能允许压缩修改
可用性	业务连续性	业务连续性
认证	识别数据访问的主体	内容生产者认证、内容传播者认证、内容分发者认证、内容消费者认证等
授权	主体对客体的访问能力限制，强调集中、权威授权，例如：PKI机制、Oauth协议等	分散、人人可授权，例如：内容生产者对传播者的授权、内容生产者对消费者的授权等
审计（不可抵赖）	日志系统，重点监控访问行为	数字内容版权管理，重点是审计机制如何嵌入到数字内容的整个生命周期
隐私	行为和实体人之间的不可关联性，例如：匿名通信、匿名投票等	内容和实体人之间的不可关联性

内容安全的概念

- 信息
  - —客观概念，强调细节
    - 信息熵、比特、字节
- 内容
  - —主观概念，强调轮廓
    - 一首李白的唐诗、一部信息安全题材的电视剧
- 信息编码不同、信息存储容量不同，但内容可以相同
  - —H.264编码、AVI格式封装、700MB

内容安全技术的内涵

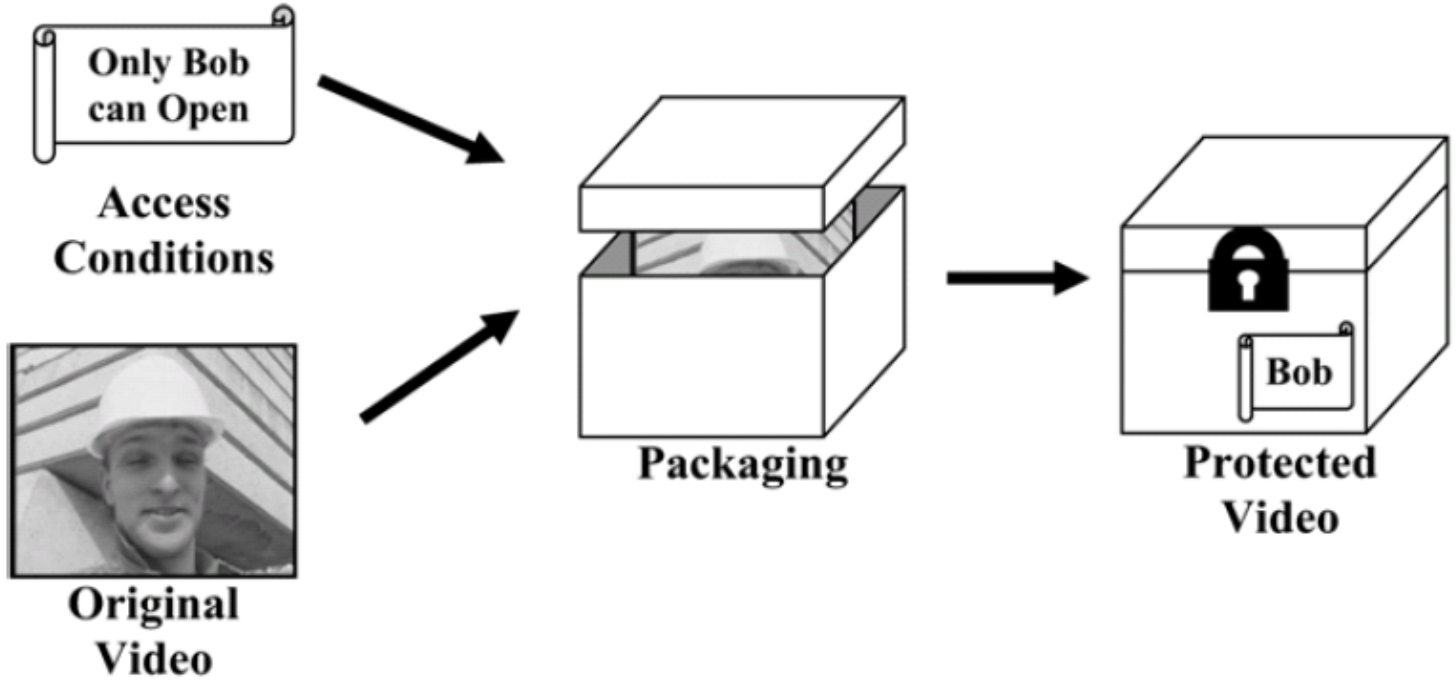
- 广义内容安全

  —数字版权保护、数字水印、多媒体加密、多媒体取证、内容认证、内容过滤与监控、垃圾邮件防范、舆情控制、信息泄漏防范等

- 狭义内容安全

  —内容过滤与监控、数字版权保护等

加密保护内容


Only Bob can Open
Access Conditions
Original Video
Packaging
Bob
Protected Video

Media protected		Secure delivery of content	Device authentication	Association of digital rights	Licensed technology	System renewability
Prerecorded media	Video on DVD-ROM	encryption	Mutual between DVD drive and PC	metadata	CSS [8]	Device revocation
	Audio on DVD-ROM	encryption	Mutual between DVD drive and PC	metadata	CPPM [35]	Device revocation
		watermarking	n/a	watermark	4C/Verance Watermark [36]	n/a
	Video or audio on DVD-R/RW/RAM	encryption	Mutual between DVD drive and PC	metadata	CPRM [37]	Device revocation
	Video on digital tape	encryption	n/a	metadata	High Definition Copy Protection [38]	Device revocation
Digital interface	IEEE 1394	encryption	Mutual between source and sink	metadata	DTCP [39]	Device revocation
	Digital Visual Interface (DVI)	encryption	Mutual between source and sink	metadata	HDCP [40]	Device revocation
	NRSS interface	encryption	Mutual between host and removable security device	metadata	Open standards [41]–[43]	Service revocation
Broadcast	Satellite	encryption	None	metadata	Conditional access system [44], [45]	Smartcard revocation
	Terrestrial	encryption	None	metadata	Conditional access system [45]	Smartcard revocation
Cable transmission		encryption	None	metadata	Conditional access system [46]	Smartcard revocation
Internet	Unicast	encryption	Receiver	metadata	DRM [47], [48]	Software update
	Multicast (A few watermarking schemes have been proposed for multicast data [49])	encryption	Sender and receiver (depends on the authentication type)	metadata	Group key management [49]	tbd

DVDCCA（CSS）

- DVD Copy Control Association
  —DVD内容控制协会(内容加扰系统)
- Content Scramble System (CSS)：一套加扰方案
- **目的：防止内容复制**
- 技术手段：
  —内容（盘片）需要得到授权
  —播放机需要得到授权
  —上述两个授权配合才能回放受保护的内容，从而防止节目的随意复制
- 安全核心：加扰算法和万能钥匙
- 1999年被破解
- DeCSS：一套在互联网上公开的解扰工具

版权管理－ 工业应用

- CE:
  - CAS (Conditional Access System) for DTV broadcasting
  - CSS (Content Scramble System) for DVD
  - SDMI (Secure Digital Music Initiative) for MP3 player
  - DTCP (Digital Transmission Content Protection)
  - CPRM (Content Protection for Removable Media)
  - SVP (Secure Video Processor)
  - HDCP (High Bandwidth Digital Content Protection)
  - AACS (Advanced Access Content System) for NG-DVD
- IT DRM solution:
  - Intertrust, ContentGuard etc
  - Apple DRM for iPod and iTunes (and Real Helix)
  - Microsoft Media DRM
  - Sun Microsystems DReaM: open source and royalty-free
- CE: cooperate under the flag of interoperability
  - Coral Consortium: the end of 2004
  - Marlin Joint Development Association: start of 2005

版权管理 – 标准

- MPEG IPMP
  - MPEG-2 CAS interface to IPMP(Part11)
  - MPEG-4 IPMP (Part 13)
  - MPEG-21 IPMP
- OMA (Open Mobile Alliance)
  - 2002, for mobile service
  - OMA DRM 1.0 ,June 2004
  - OMA DRM 2.0 ,Sep. 2005
  - CMLA (Content Management Licensing Administrator)
- DMP (Digital Media Project)
  - DMM, Sep.,2003, Leonardo Chiariglione
  - Target: Interoperable DRM Platform
  - Phase I specifications (for Portable Audio and Video Devices, PAVs)
  - Phase II specifications (for Stationary Audio and Video Devices, SAVs)
  - Phase II TRUs (Traditional Rights Usage)
- AVS DRM:
  - Core Profile
  - IPTV Profile, Broadcasting Profile, Adaptive Profile (OMA,DMP,IPMP etc.)

从条件接收到数字版权管理

专业术语

- 控制字 CW(Control Word)
- 授权控制消息 ECM(Entitled Control Message)
- 授权管理消息 EMM(Entitled Management Message)
- 加扰/解扰（Scrambling/Unscrambling）
- 加密/解密（Encryption/Decryption）

条件接收原理（1/8）

数字电视可以只让付费的用户能够收看到相应的节目。这就是“条件接收”！

如果一个网络是双向单播网络，那么本身就已经能达到条件接收的效果。

如果一个网络是双向广播网络，那么可以使用鉴权认证的方式实现条件接收。

但由于当前的多数广电网络都是单向网络，这就要依靠授权的方式实现“条件接收”。

注：鉴权认证是终端与局端双向交互、动态获取密码；授权是不需申请，局端直接将你有权观看的节目的密钥发给你。

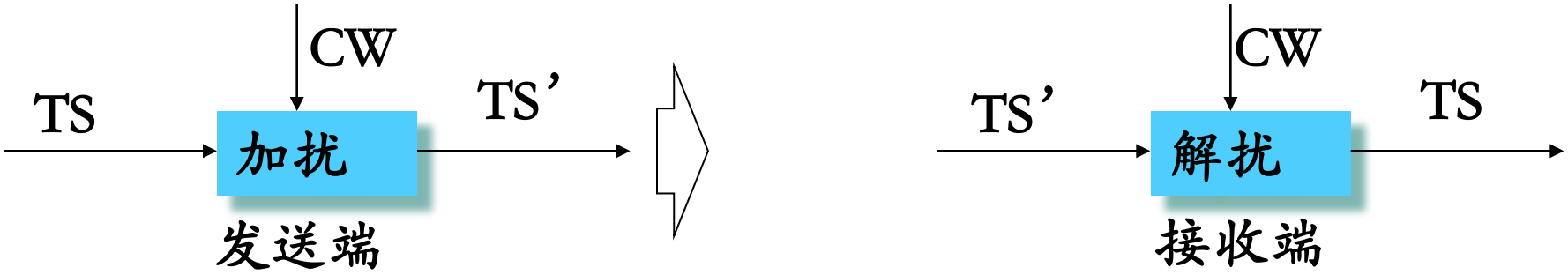
条件接收原理（2/8）

- 为什么要引入 条件接收系统 Conditional Access System
  - ——数字电视的运营需要进行有效收费
    - 保证交费用户能正常收看电视节目的同时，限制非法用户的盗看
    - 需要一个身份识别系统
  - ——数字电视网络仍采用模拟电视的HFC网络
    - HFC是一个单向网络，用户无法向广电提供身份信息

- 为什么现在的网络较多的是单向网络?
  - 当前数字电视系统大多数是利用了之前已有的模拟电视的同轴电缆网络进行播放，该原有的网络是单向的网络，如果要改造成双向的，有技术上及资金投入上的难度。

条件接收原理（3/8）

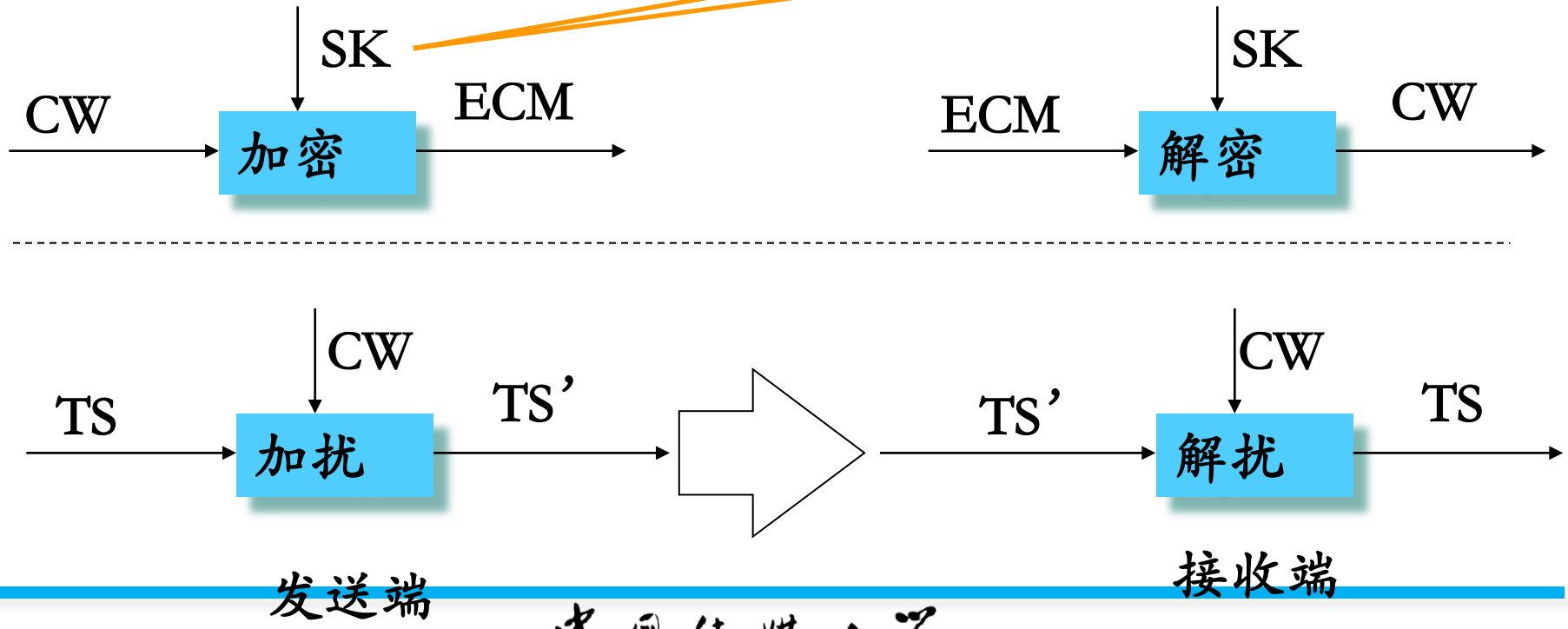
- 第一层：码流加扰
  - —加扰过程是在发送端用一个伪随机序列（CW，Control Word）对复用后的TS流进行实时扰乱控制，使用加扰序列控制对打包的图像信号进行扰乱。
  - —接收端必须获得CW，再次对码流进行位运算才能将码流还原
  - —只有授权用户才能获取CW，才能对码流进行解扰
  - —CW如果明文传输，则很容易被破解，因此提出需要对CW进行加密，在码流中传送的是密文信息。
  - —如何保密传输CW？如何使只有授权用户才能获取CW呢？



条件接收原理（4/8）

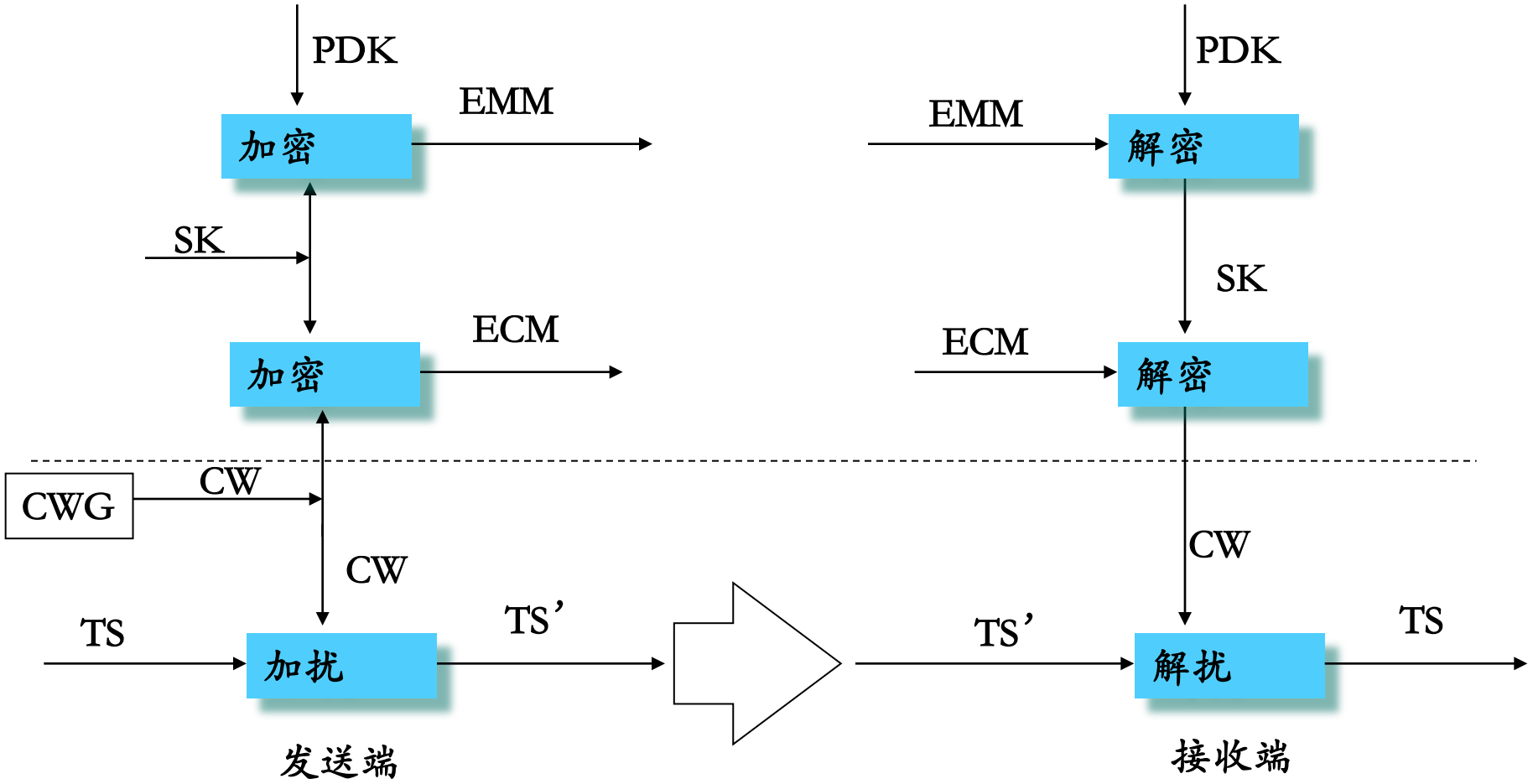
- 第二层：访问控制（CW加密）
  - —发送端：采用SK（加密密钥）对CW进行加密，传输加密后的数据（ECM）
  - —接收端：必须先获取SK，然后运用SK对ECM进行解密，得到CW
  - —如何保证只有授权用户才能得到SK?

SK与产品一一对应



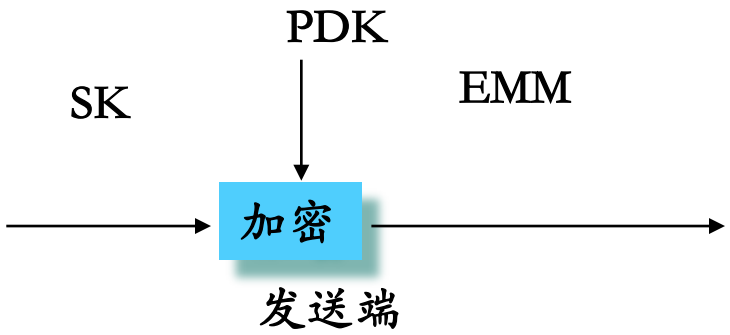
条件接收原理（5/8）

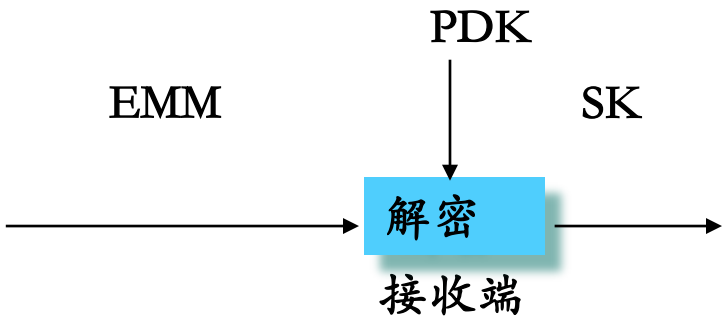
- 第三层：授权管理（SK加密）



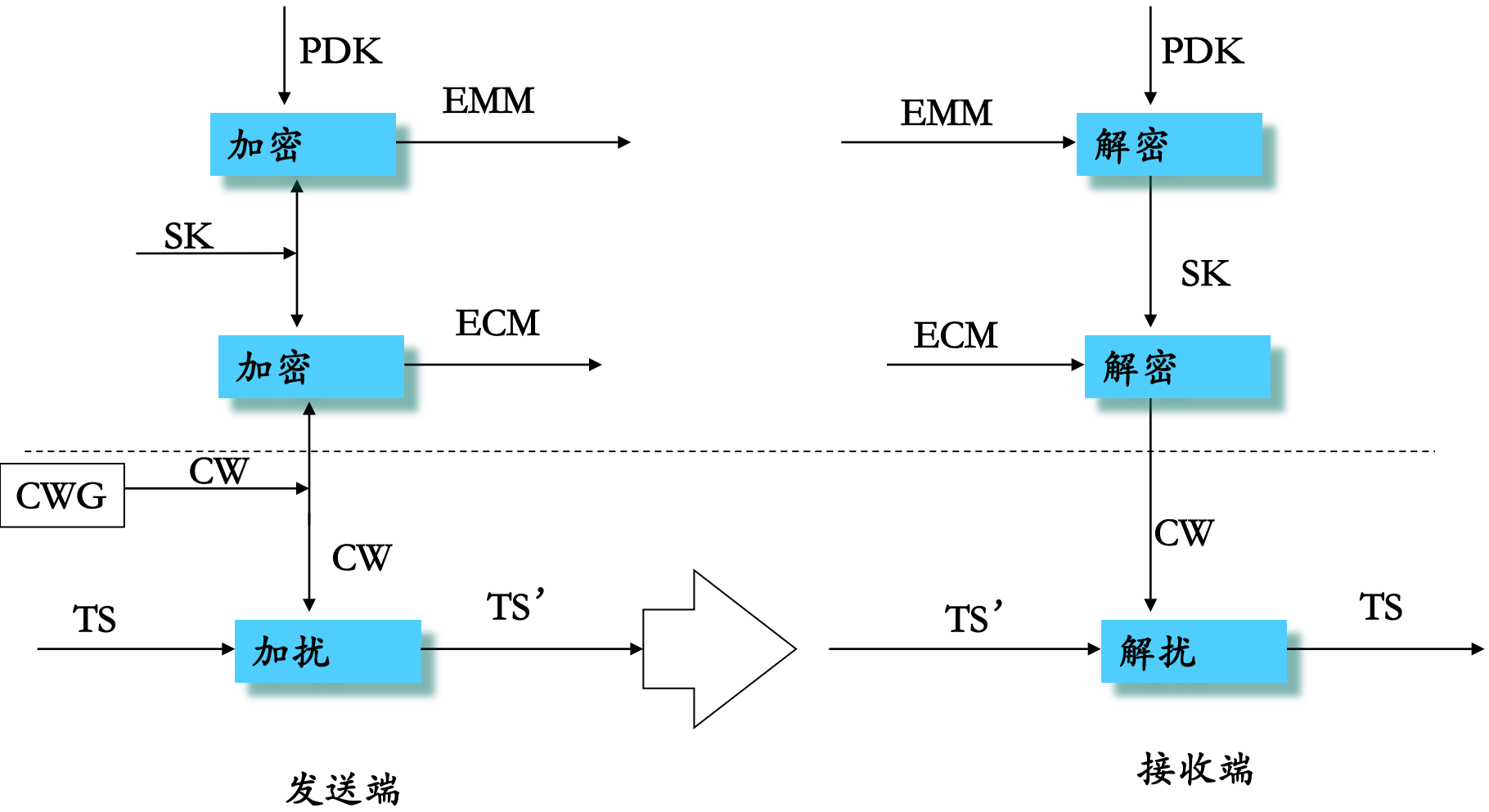
条件接收原理（6/8）

- **第三层：授权管理（SK加密）**
- 每一授权用户将获得一张IC卡，在卡内保存有一个或多个PDK（个人密钥），在发送端运用PDK对SK进行加密，生成数据以EMM的形式打包进码流中。这样保证只有拥用该PDK的用户才能解密得到SK。

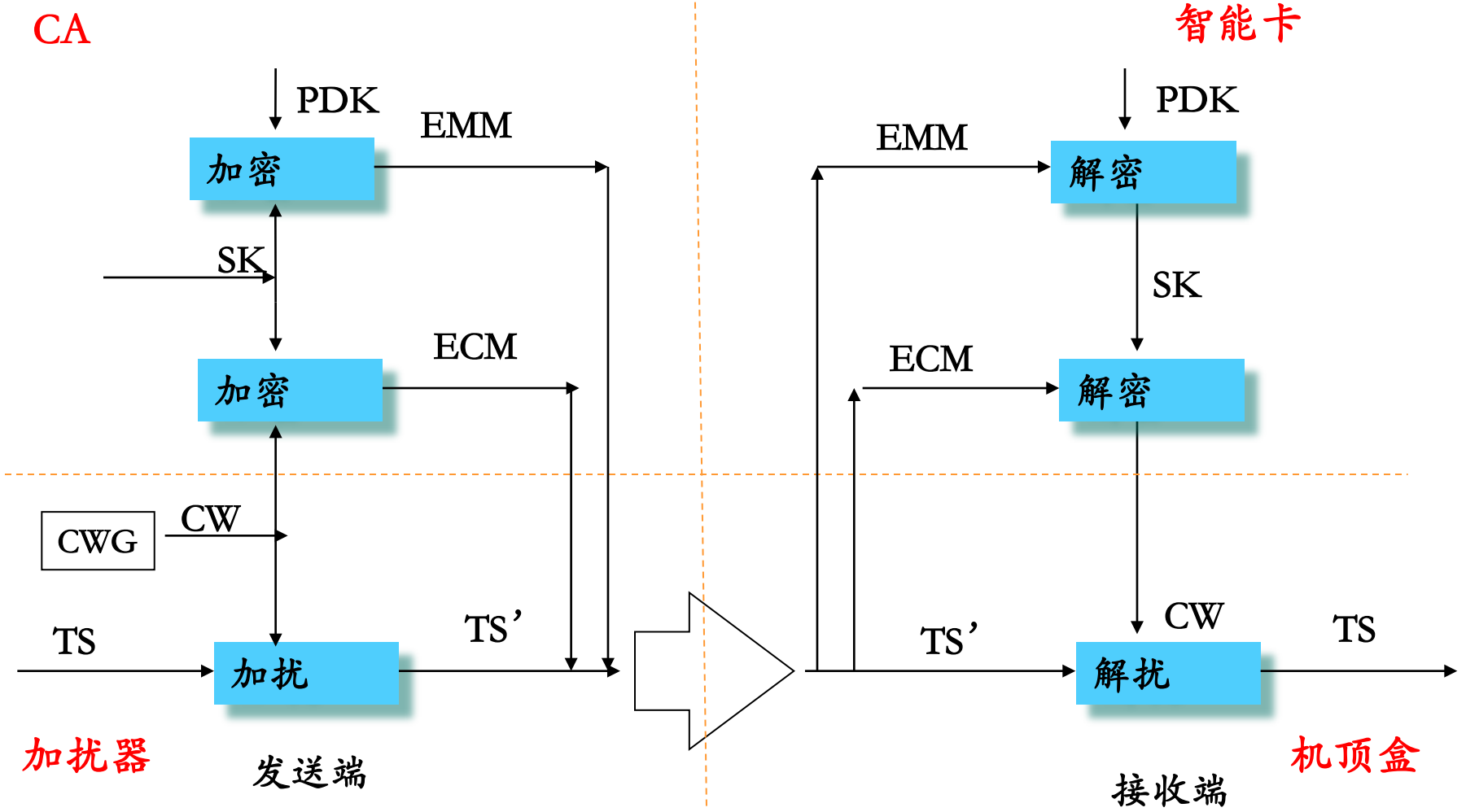




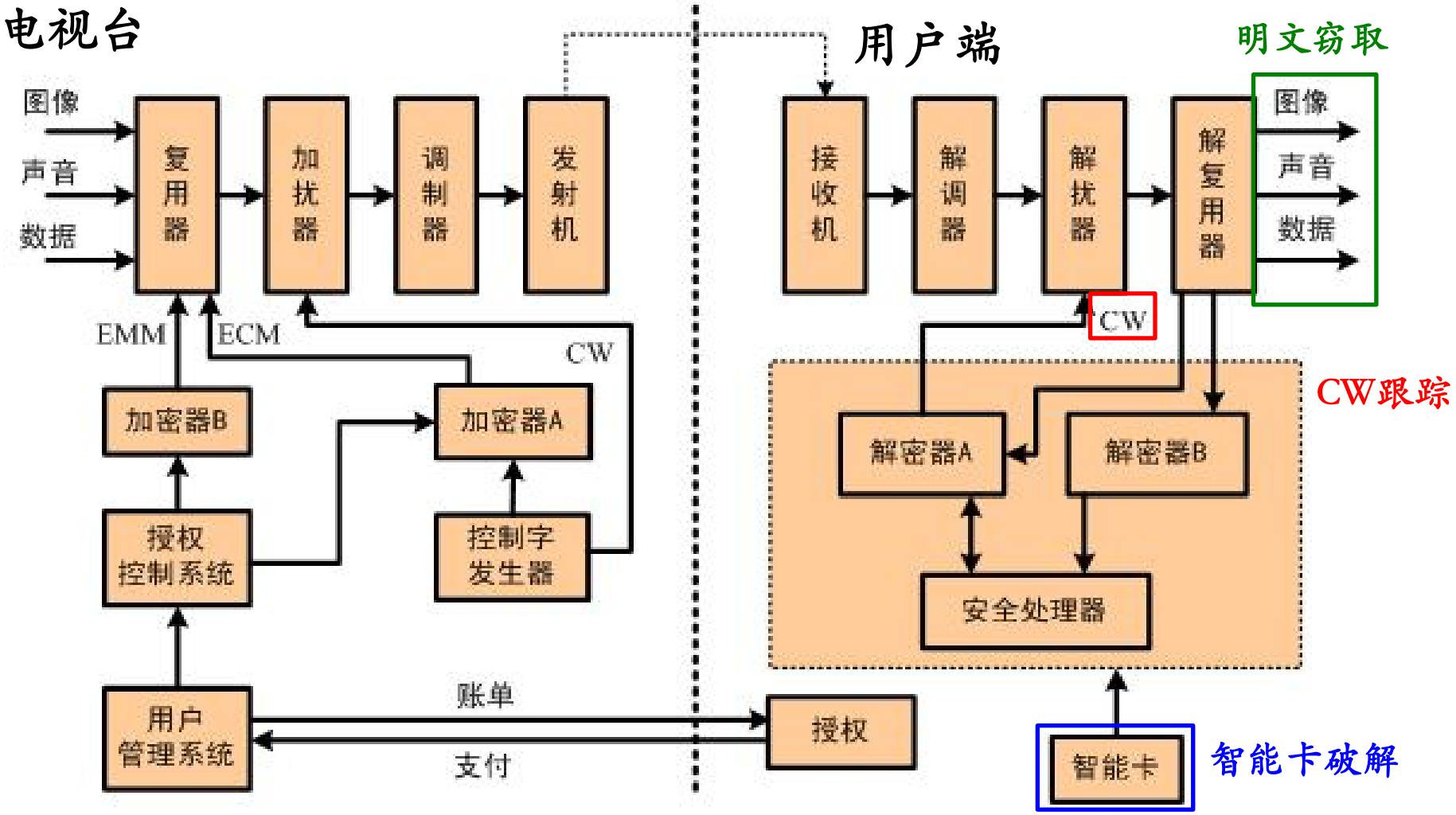
条件接收原理（7/8）


PDK
EMM
加密
SK
ECM
加密
CWG
CW
CW
TS
加扰
TS’
发送端
PDK
EMM
解密
SK
ECM
解密
CW
TS’
解扰
TS
接收端

条件接收原理（8/8）

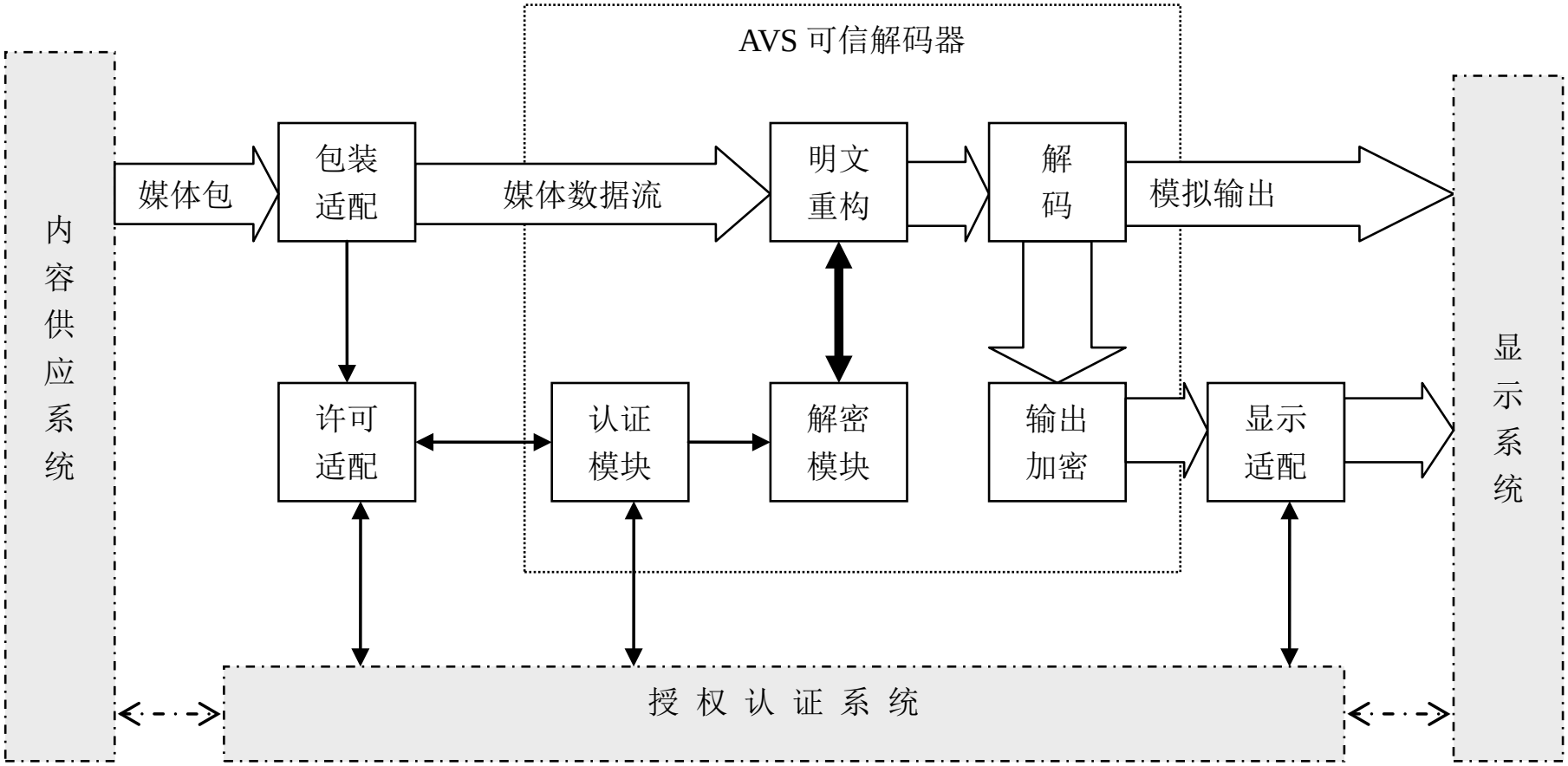

CA
智能卡
PDK
EMM
加密
SK
ECM
加密
CWG
CW
TS
加扰
TS’
加扰器
发送端
EMM
PDK
解密
SK
ECM
解密
TS’
CW
TS
解扰
机顶盒
接收端

数字电视CA系统工作流程

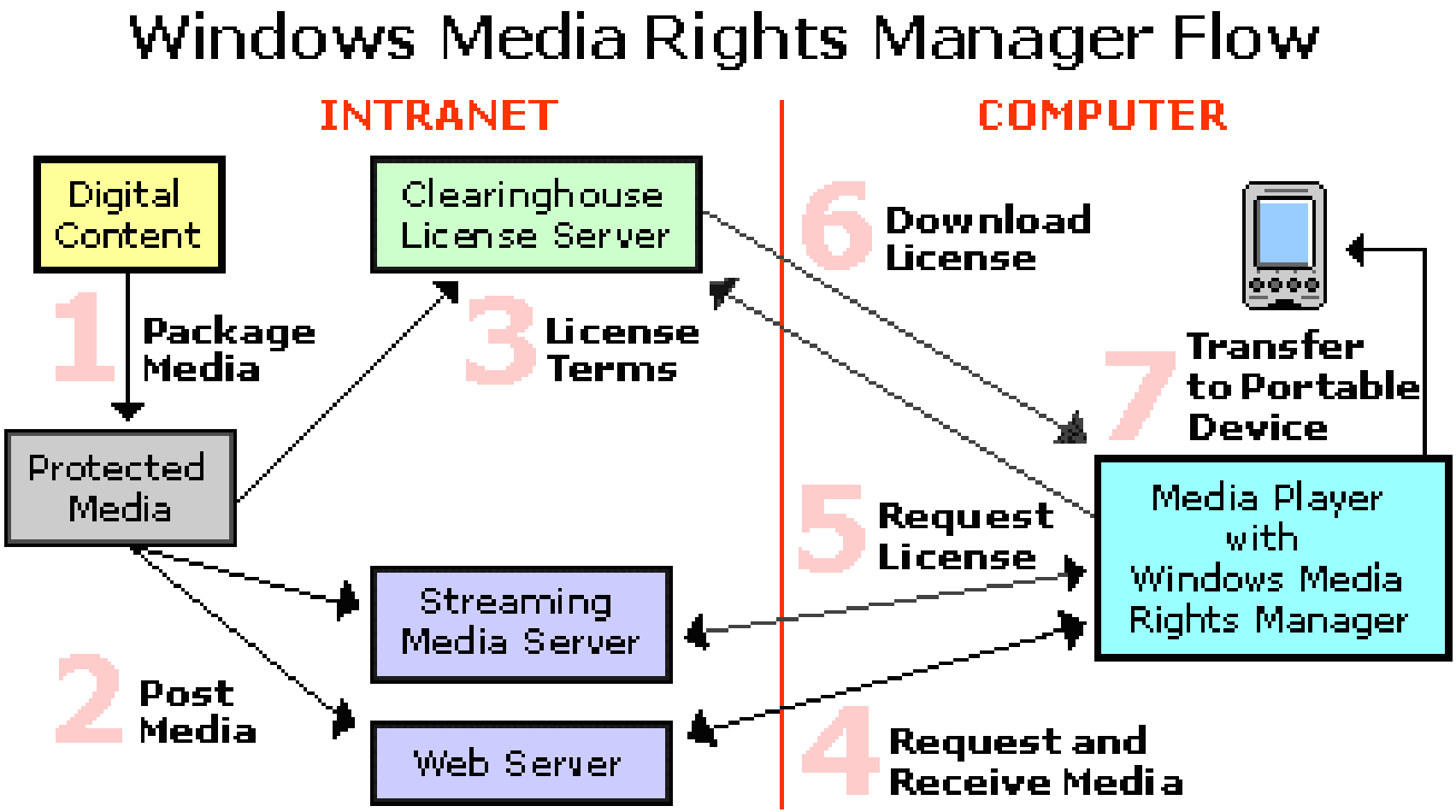


版权保护系统基本框架

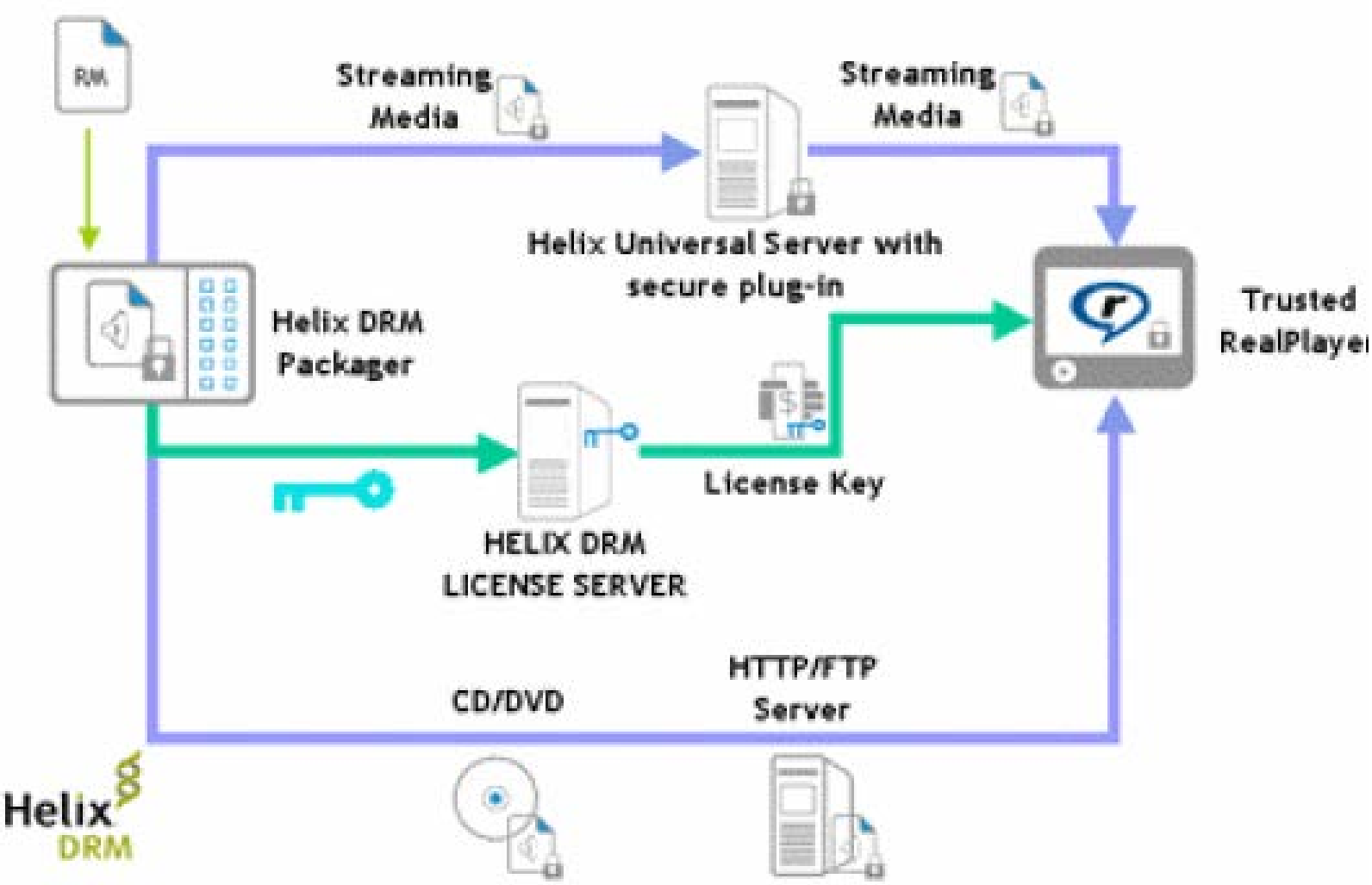
AVS DRM系统模型


AVS 可信解码器
内容供应系统
媒体包
包装适配
媒体数据流
明文重构
解码
模拟输出
显示系统
许可适配
认证模块
解密模块
输出加密
显示适配
授权认证系统

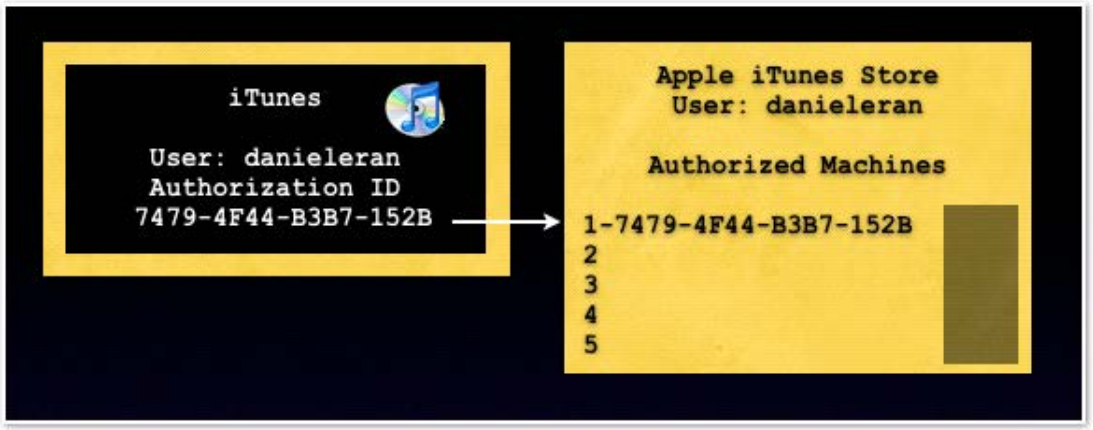
Microsoft DRM in Windows world

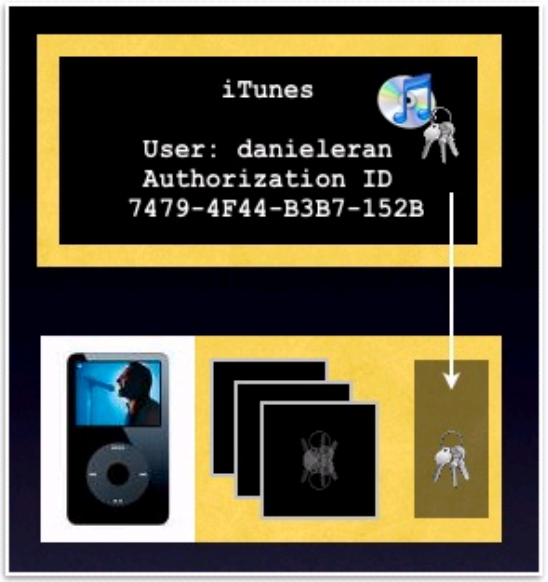


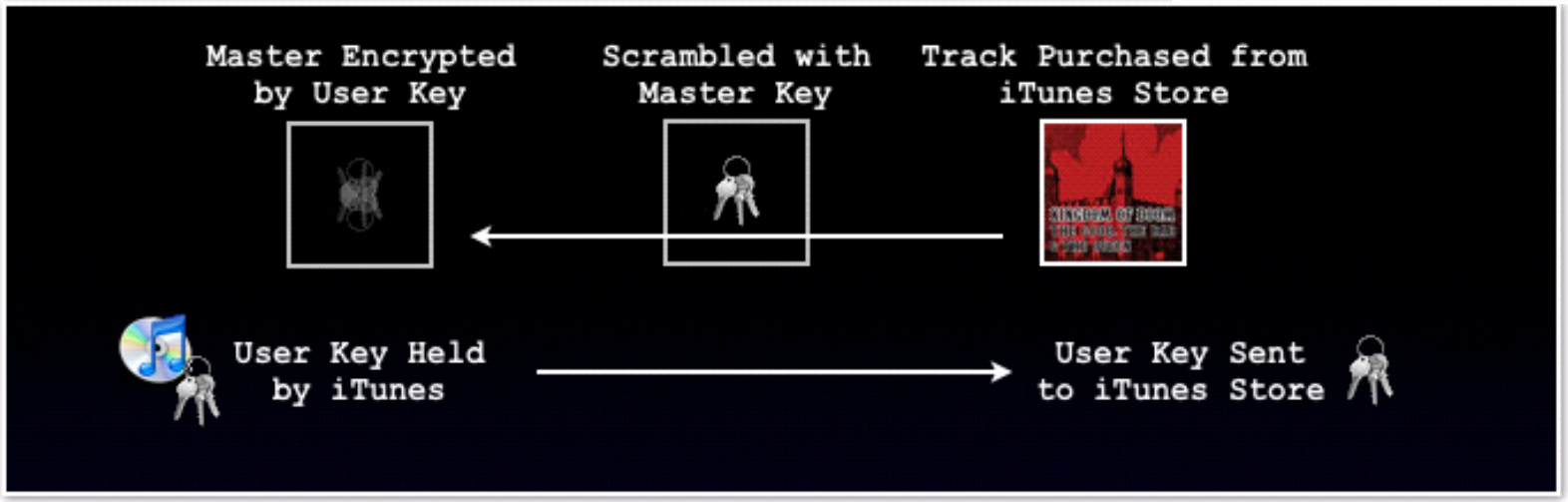
RealNetworks Helix



Apple FairPlay

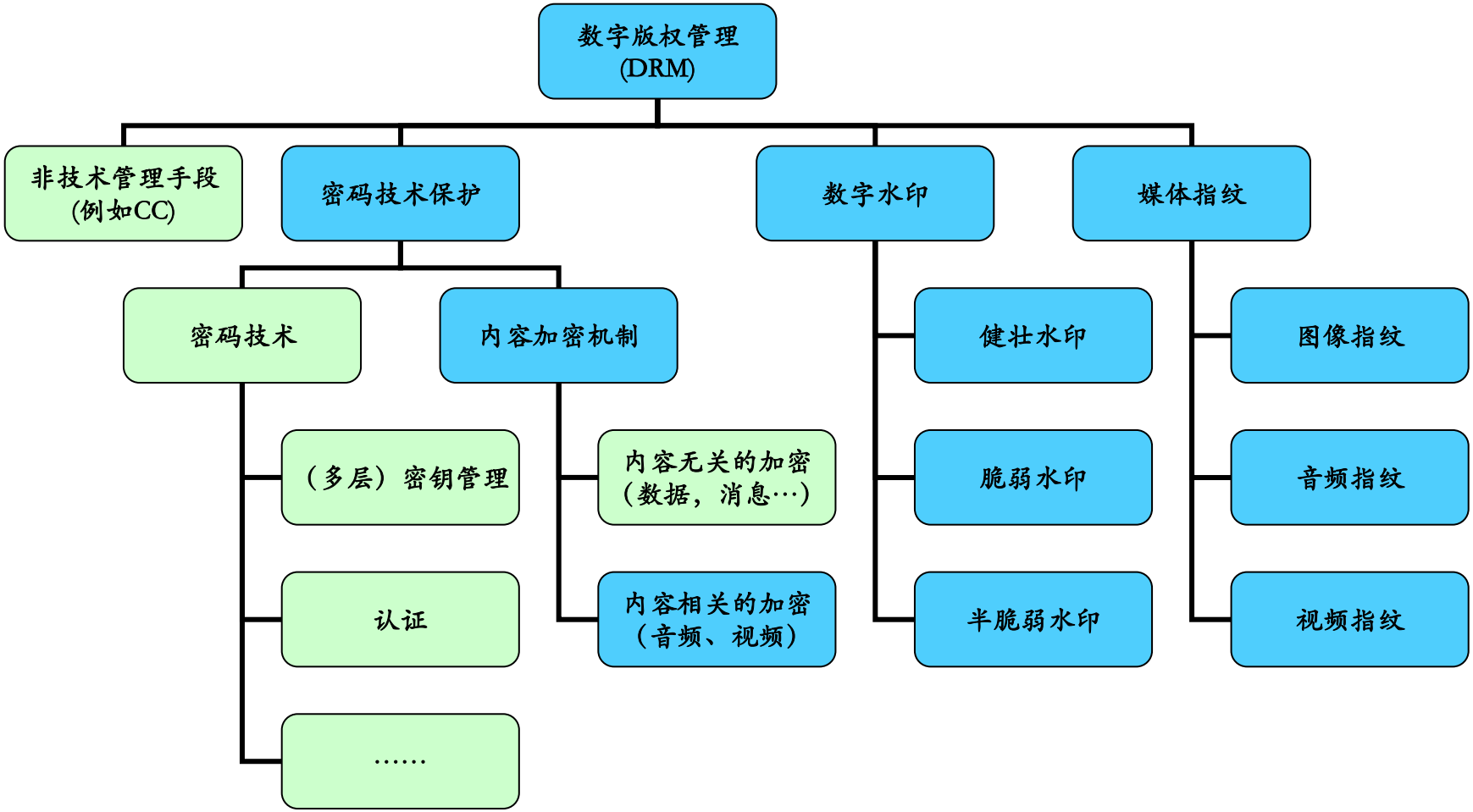






版权保护系统关键技术

数字版权管理的三条技术路线



creative commons 知识共享

- 吉尔是一位初露头角的摄影师，她把自己的作品选集放在网络上。或许有朝一日，她会向复制她的作品的收费。但是现在，她正试图建立声誉，所以希望他人复制她的作品越多越好。她最得意的作品是一些关于摩天大楼的黑白照片。
- 杰克正使用自己新的家用电脑制作一部关于纽约市的数字电影，他想在影片中放进一张帝国大厦的定格照片，但是他上次在纽约的时候却忘了拍这样的照片。他在网 络上搜寻“帝国大厦”，找到了一批网站，其中有些有照片。但他不确定这些照片是否享有著作权。他用了一个搜索引擎寻找没有著作权标识的作品，但是他知道，有些作品即使没有著作权标识，仍有可能受到著作权法的保护。他担心如果自己用了这些在网络上找到的照片，然后把自己的影片放到网络上，这些照片的拍摄者看 到这部影片后，会感到不满并对他提起诉讼。
- 知识共享组织希望能够帮助杰克和吉尔更加容易地在网络上找到对方，开展他们想进行的创意合作。我们建立一种网络应用模式，让吉尔可以用之（技术上称为“许可协议”）公告，只要标明她是原摄影者，任何人都可以复制她的照片。这样的许可协议条件必须是“可直接为电脑处理”的。换言之，借助于搜索引擎等电脑应用程序，就可以判定吉尔的照片的著作权授权条件，而杰克就得以搜寻在知识共享许可协议下获得授权，复制并在网上发布的帝国大厦的照片。他将会找到吉尔的照 片，而且知道吉尔允许他将这些照片放进自己的影片中。

creative commons 知识共享

Step 1: Choose Conditions

Publishing under a Creative Commons license is easy. First, choose the conditions that you want to apply to your work.

Attribution. You let people copy, distribute, display, perform, and remix your copyrighted work, as long as they give you credit the way you request. All CC licenses contain this property.

Non-Commercial. You let people copy, distribute, display, perform, and remix your work for non-commercial purposes only. If they want to use your work for commercial purposes, they must contact you for permission.

Share Alike. You let people create remixes and derivative works based on your creative work, as long as they only distribute them under the same Creative Commons license that your original work was published under.

No Derivative Works. You let people copy, distribute, display, and perform only verbatim copies of your work — not make derivative works based on it. If they want to alter, transform, build upon, or remix your work, they must contact you for permission.

Step 2: Get a License

Based on your choices, we'll give you a license that clearly indicates how other people may use your creative work.

- **Attribution**
- **Attribution — Share Alike**
- **Attribution — No Derivatives**
- **Attribution — Non-Commercial**
- **Attribution — Non-Commercial — Share Alike**
- **Attribution — Non-Commercial — No Derivatives**

密码技术保护的局限性

- 数字悬崖（或者购买，或者什么也看不到，翻阅也不行？）
- 割裂市场或DRM垄断（多内容提供商 vs. 多个用户）
- 多用户/设备共享同一内容问题（家庭朋友之间）
- 合理使用问题（数字鸿沟--翻阅，图书馆借阅）
- 媒体引用问题（黑盒之间相互引用、链接？）
- 版权期限问题（版权到期还是加密状态？）
- 数字考古问题（后代看到的是一个个黑盒子）

版权管理的非技术关键因素

- 2006年3月，法国议会下院通过一系列版权法修订案，其中一条要求DRM系统之间必须能够互操作，从而使得消费者能够在不同设备上播放内容并能够复制个人拷贝。
- 2006年6月，此法案几经争议、修改，由法国议会上院批准通过。
- 这个法案标志着DRM领域讨论多时的互操作问题已经从技术层面上升到社会层面，互操作已经成为DRM技术研究和产品开发面临的最重要的问题之一。

数字媒体宣言

- 2003年7月，面对数字媒体商业模型浮现的迫切性，以MPEG大会主席Leonardo为首的科学家发起一个《数字媒体宣言（Digital Media Manifesto）》的运动，宣言认为：

(1)数字媒体处于进退维谷的僵局阶段，导致发展速度减缓；

(2)数字版权管理技术（DRM）能够打破僵局的；

(3)为了不使目前错综复杂的DRM问题乱上加乱，DRM必须可互操作；

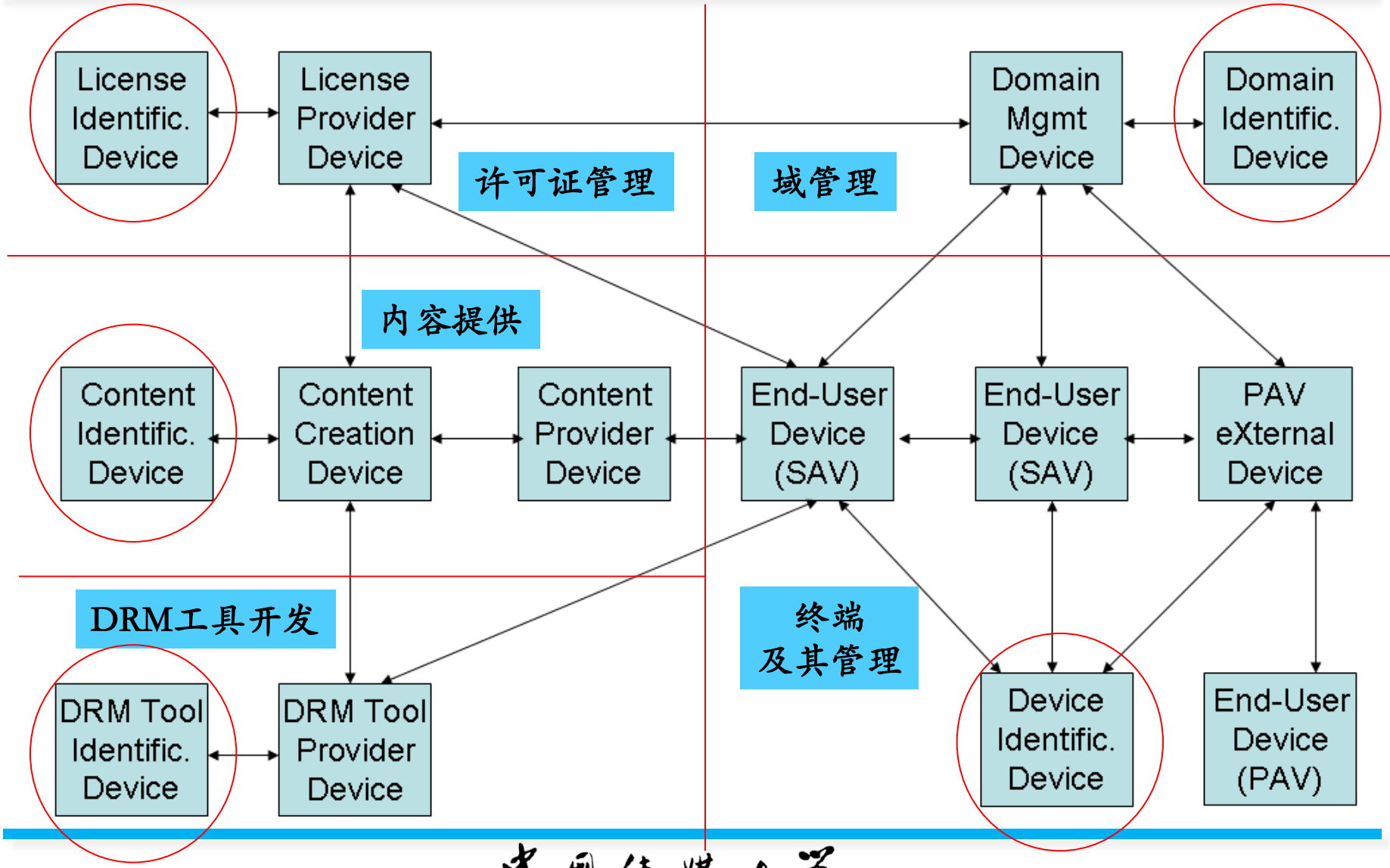
(4)DRM的互操作需要标准支持；

(5)DRM需要应用于整个“媒体价值链”；

(6)DRM影响个人、团体和社会使用内容的方式；

(7)需要消除影响数字媒体商业模型的其它瓶颈。

DRM产业链的主要角色



数字水印与版权保护

数字水印的定义

- 数字水印是永久镶嵌在其他数据（宿主数据）中具有可鉴别性的数字信号或模式，并且不影响宿主数据的可用性

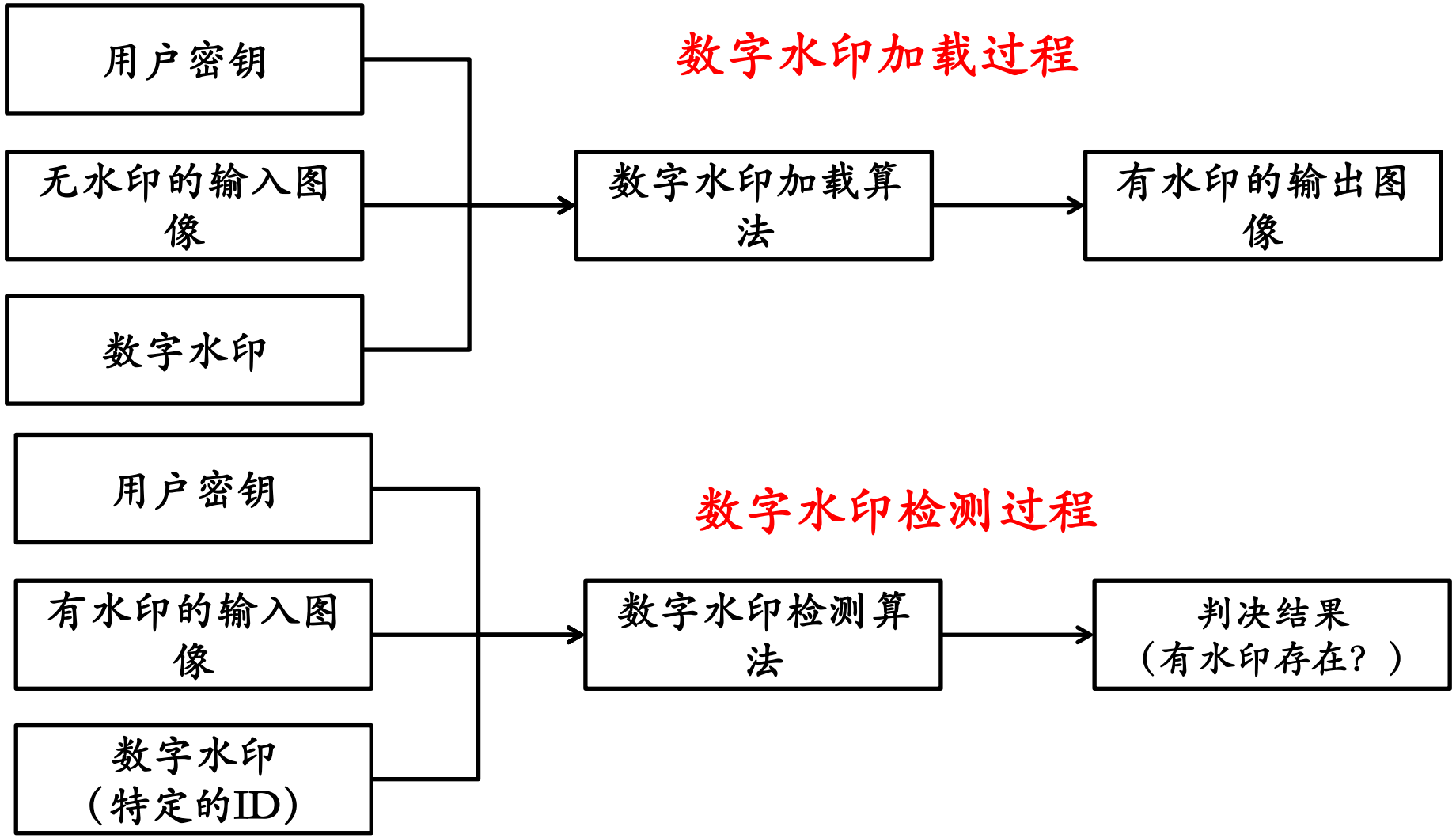
数字水印

- 用于版权保护的数字水印：将版权所有者的信息，嵌入在要保护的数字多媒体作品中，从而防止其他团体对该作品宣称拥有版权
- 用于盗版跟踪的数字指纹：同一个作品被不同用户买去，售出时不仅嵌入了版权所有者信息，而且还嵌入了购买者信息，如果市场上发现盗版，可以识别盗版者
- 用于拷贝保护的数字水印：水印与作品的使用工具相结合（如软硬件播放器等），使得盗版的作品无法使用

数字水印的特点

- 不可感知性
  - —从感观上和统计上都不可感知
- 稳健性
  - —数字水印应该难以被擦除，任何试图完全破坏水印的努力将对载体的质量产生严重破坏
  - —好的水印算法应该对信号处理、几何变形、恶意攻击等具有稳健性

数字水印加载和检测流程



数字水印的应用

- 版权保护：表明对数字产品的所有权
- 数字指纹：用于防止数字产品被非法复制和散发
- 认证和完整性校验：验证数字内容未被修改或假冒
- 内容标识和隐藏标识：多媒体内容检索
- 使用控制：控制复制次数
- 内容保护：保护内容不被滥用

数字水印的研究方向

- 理论

  —数字水印模型、隐藏容量、抗攻击性能等

- 算法

  —研究具有更高性能的水印算法

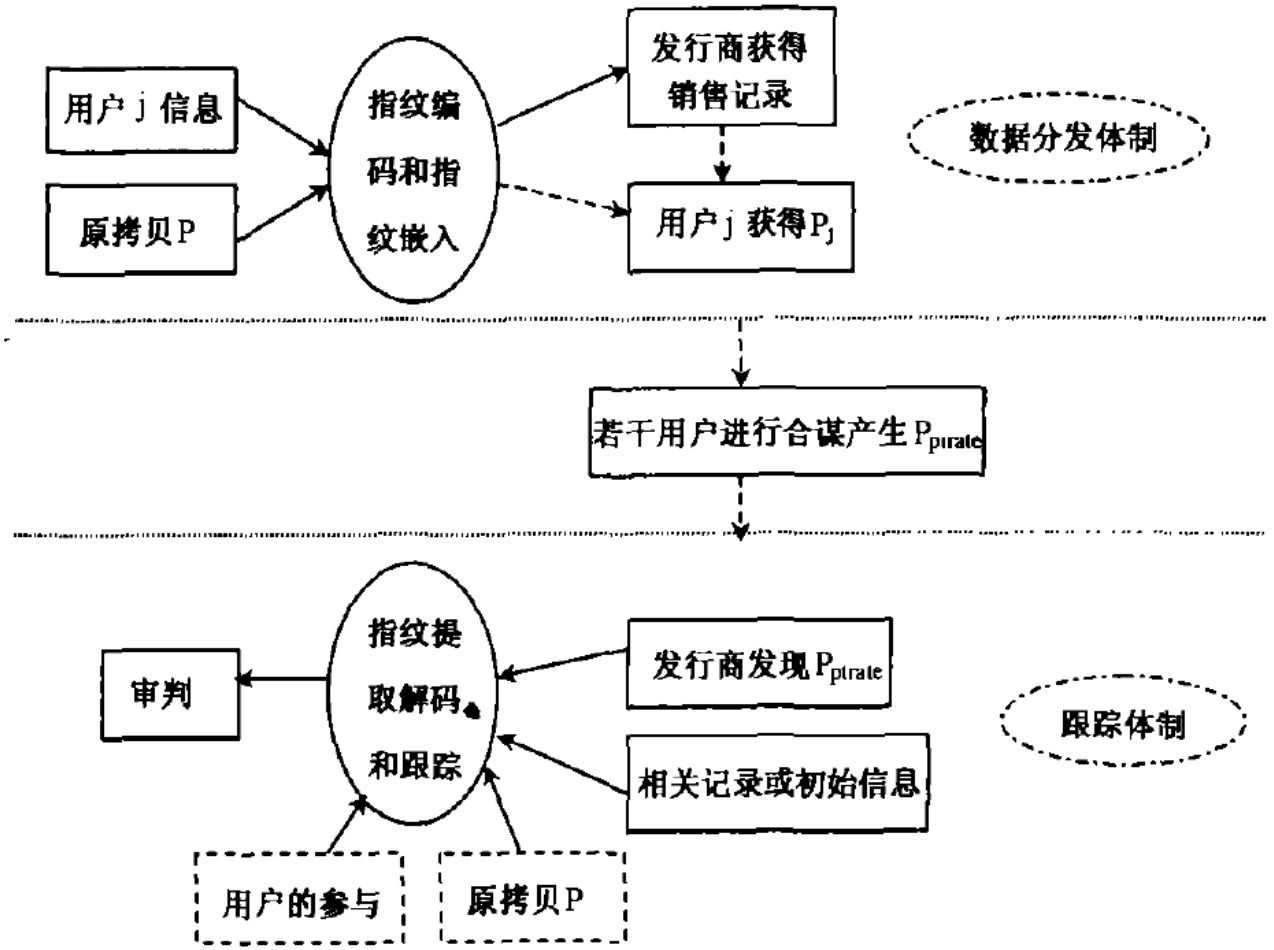
- 标准

  —真正起到数字版权管理的作用，还需要完善一系列的标准和协议

数字水印： 存在的问题

- 嵌入内容拥有者相关的信息：这是我的！
  - —嵌入Logo：贴上我的招牌！
  - —嵌入唯一性信息（例如签名）：证明是我的！
- 嵌入方式：公开或保密
- 鉴定方式：公开或零知识协议
- 面临的问题
  - —抗变换能力有强有弱
  - —抗擦除能力未能过关

数字指纹：嵌入用户信息


用户 j 信息
原拷贝P
指纹编码和指纹嵌入
发行商获得销售记录
用户 j 获得 P_j
数据分发体制
若干用户进行合谋产生 P_{pirate}
指纹提取解码和跟踪
审判
发行商发现 P_{ptrate}
相关记录或初始信息
跟踪体制
用户的参与
原拷贝P

加法的误区

- 加密——当成数据对待
  - —依赖密码技术，继承其优点和缺点
  - —未考虑数字媒体的特点
  - —黑盒子对合理使用和数字考古
- 加水印
  - —健壮水印——拥有者信息，抗擦除能力一直未过关
  - —脆弱水印——发现是否有人动过，而视频适当变化是应用允许的
- 加指纹
  - —记录谁用过，以便进行反向跟踪

加法的误区

- 要支持加法，必须有安全基础设施支持
  - —真安全吗?
  - —谁买单？消费设备成本的增加
  - —升级问题
- 模拟漏洞
  - —一旦得到视频内容，则进入模拟空间，上述数字保护手段将有效

“加法”悖论：只在“加法”范围内有效

- 加密：
  - —加密前的内容?
  - —解密后的内容?
- 加数字水印：
  - —还未加水印的原始内容?
  - —擦除水印后的内容?
- 加数字指纹：
  - —指纹加载之前的内容
  - —指纹抹除或共谋破坏后的内容

数字版权的“非技术公理”

- 媒体版权权属证明不是技术问题，或者说从根本上不靠技术解决
  - —直接的办法是一旦创建，就有公认的中立机构注册登记
  - —对于公开发行的内容来说，数字水印是绕了弯路的办法，不去登记内容而嵌入水印，证明靠水印，可是非版权拥有者也叠加水印的情况下，只有出示未加水印的原始内容才能说明权属
- 密码技术保护内容是本末倒置：内容拥有者和合法消费者支付密码技术设施等额外费用，盗版者透过模拟漏洞不用额外成本消费内容

未点明的事实

- 谁为版权保护技术和设备付费？消费者为什么要付这个钱
- 侵犯合理使用，必然引起反弹
- 模拟世界不会消失，媒体最终是人可感知的，“模拟漏洞”必然存在，数字保护技术是有边界的
- 网络空间是公共空间，在公共空间散发只授予个人使用权的内容是非法的!

媒体指纹与版权保护

互联网的启示与假设

- 假设前提：
  - —越来越多的公共空间将网络化
  - —在公共空间传播未授权内容是非法的，法律约束
  - —在私人空间的共享使用属于合理使用
- 存在的问题
  - —未网络化的公共空间→合理使用，减少数字鸿沟
- 媒体版权保护
  - —准确监测在公共空间中是否有非法内容传播
  - —通过网络在公共空间进行媒体追踪

走减法路线，学习模拟时代

- 从媒体中抽取关键内容进行保护，非关键内容保持不变

- 从媒体中抽取独特的不变特征作为标识，用于版权监管

媒体指纹

- 媒体指纹（mediaprint）是我们造的一个概念，是从图像、视频、音频等媒体内容中提取的、能够唯一标识该内容的一个表征
- 同类概念：指纹（fingerprint）、声纹(voiceprint)是标识个人身份的独特生物特征一样
- 同义概念：X fingerprint, perception hash（感官Hash）, visual signature（视觉指纹）
- 实例：auralprint(音纹)、documentprint, sourcecodeprint、dataprint

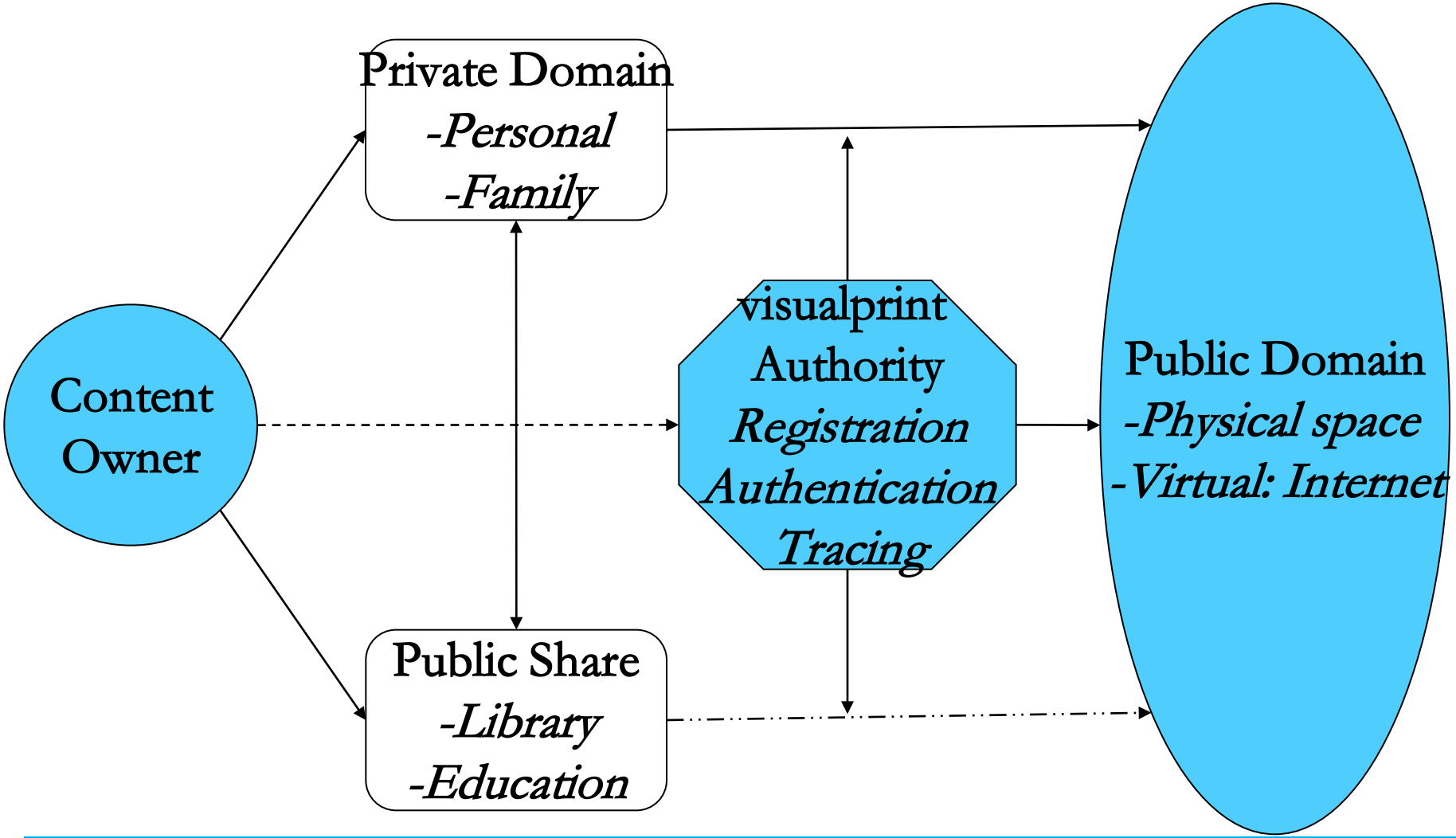
媒体指纹的两个基本特性

- 视纹对同一媒体的不同变化(失真)具有唯一性，对不同视频的具有强区分性
  - —健壮性，即对同一个媒体内容的多种变形（例如不同压缩编码格式、模数转换、尺寸变化等）具有不变性
  - —独特性，按照同一方法从不同媒体内容中抽取的视纹应该不同

相互矛盾的要求

- 唯一性：应尽可能提取出所有不变特征，以降低冲突概率
- 稳定性：抵抗各种变化的不变特征是有限的
- 合理的边界：不变特征是那些一旦改变就会对内容的实际使用（感知）带来不可挽回的影响

数字网络空间中的版权管理



应用逻辑：密码DRM vs. 媒体指纹

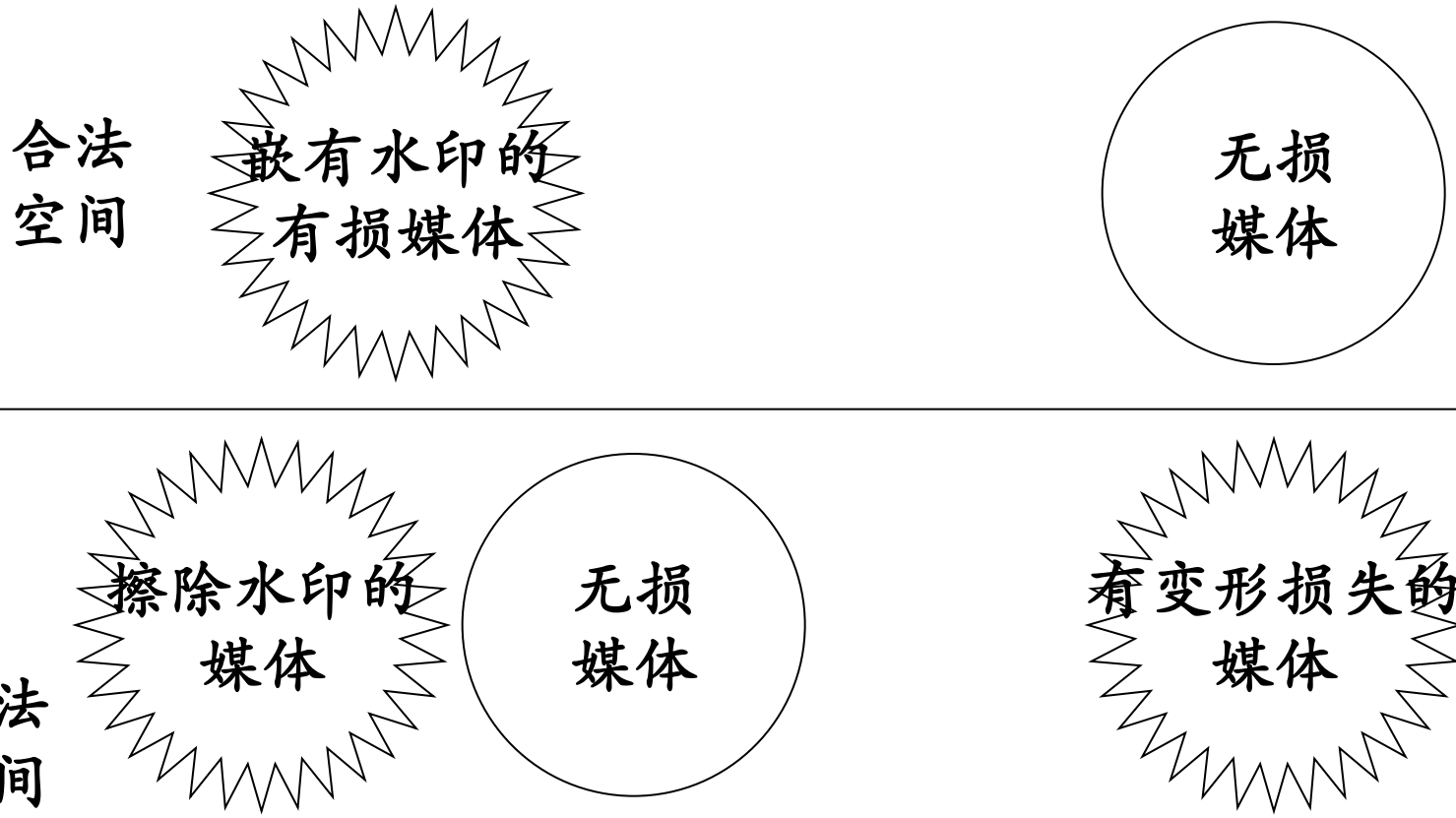
密码技术DRM需要合法用户
为版权保护支持安全成本

（防君子不防小人）

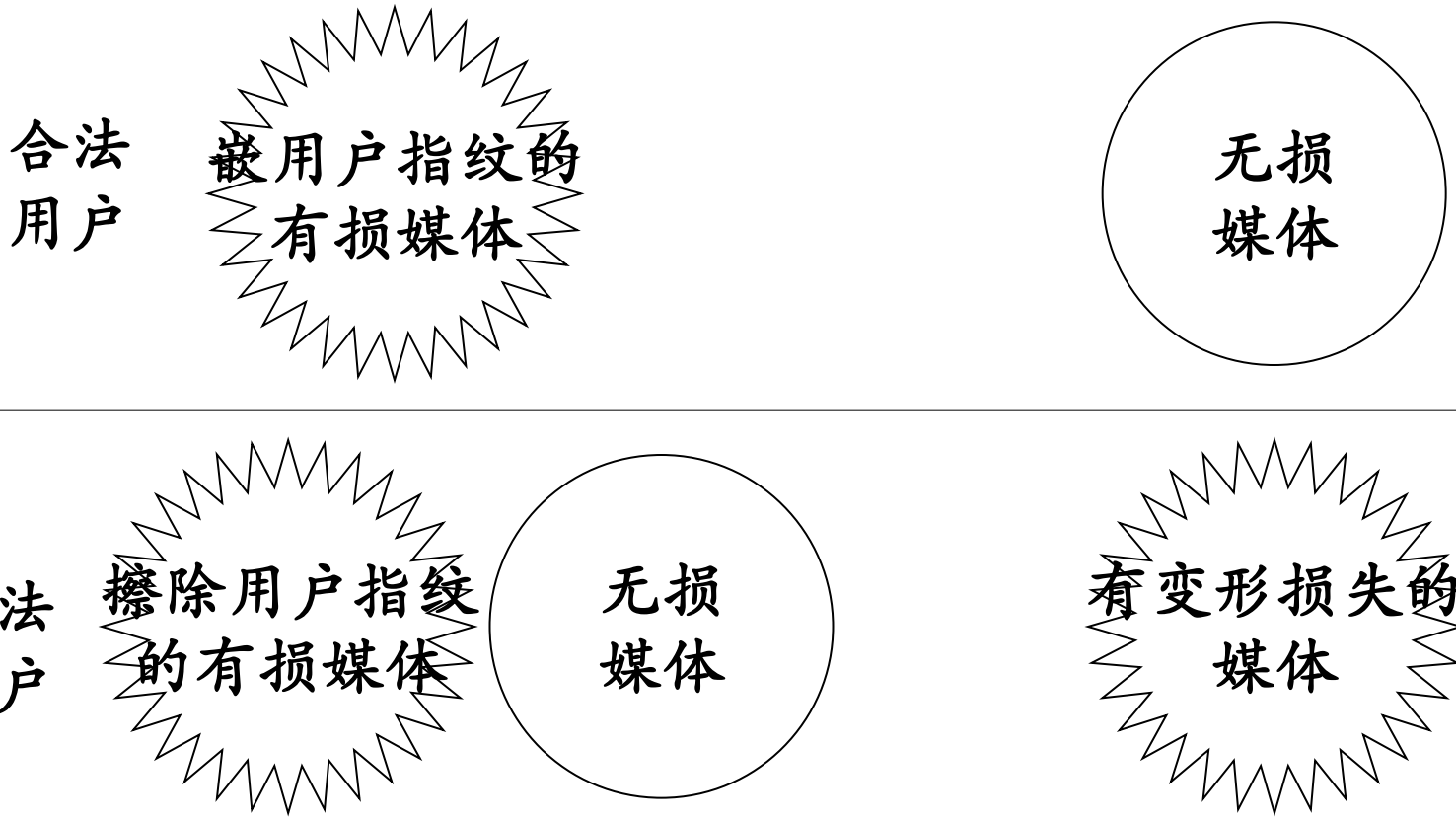
媒体指纹逼迫非法用户
为逃避监管支付成本

(警察抓小偷)

应用逻辑：数字水印 vs 媒体指纹



应用逻辑：数字指纹 vs. 媒体指纹



三类应用，同一需求

- 盗版节目监测：一个受版权法保护的电影或音乐并编码成不同格式在网络上传播，或者在电影院中用个人摄像机翻拍后重新压缩后发行，或者其中的片断被剪辑后在视频网站上共享，发现、过滤这些盗版变体节目是实现数字版权保护所必需的；
- 非法节目封堵：色情、暴力、反动节目的网络传播已经成为社会公害，如何监测、拦截、封堵这些节目在互联网上的传播已经成为网络时代必须解决的社会问题；
- 副本检测发现（duplicate detection）：在一个海量多媒体管理系统（包括互联网）存在一个节目的多个副本，其格式、尺寸等具体形态不同但是内容相同，如果能够将内容相同的多个副本识别出来，则能通过音视频的身份标识建立语义链接，支持节目跟踪、信息组织、自动标注、媒体搜索等应用。

音频指纹

- 定义(Audio Fingerprinting)
  - —也被称为Audio Hash或者Audio Identification
  - —它是通过某种算法提取音频资源中的不变性特征作为该音频的标识符
- 基本特性
  - —健壮性（robustness）
  - —可靠性（reliability）
  - —尺度大小（size）
  - —颗粒度（ granularity）
  - —搜索速度（search speed）
  - —可升级性（scalability）

图像指纹

- 基于局部特征的图像指纹
  - —当前图像指纹算法都基于全局特征，对几何变换的鲁棒性很差
  - —局部特征更加与人类视线集中在图像显著点的原理吻合，对纵横比改变、剪切、嵌入、组合等几何变换，效果很好
- 基于SIFT的图像指纹算法
  - ∞根据SIFT特征生成图像指纹，利用SIFT特征的高区分性和稳定性，来生成满足条件的图像指纹
  - ∞根据仿射变换的重要性质—面积比恒定(Area Ratio Invariance), 设计了匹配算法，使得指纹算法对于图像的仿射变化，如纵横比改变等能保持较好鲁棒性
- *SIFT在对象检测识别中的应用及高速比对算法*

版权管理小结

- 顺应数字媒体广泛传播的现状和趋势，不开历史倒车，音乐和电影已经收不回瓶子中
- 可管理——媒体标识：任何系统可管理的基本条件是管理对象有身份、可标识媒体指纹是解决这一问题的可能出路
- 互操作——技术是为内容服务的，不应束缚媒体，而应更好地解放媒体，互操作是数字版权的必由之路
- 疏之道——“君子版权”：提供购买数字使用权的简便方法，让守法消费者和尊重作者的用户自愿付费
- 堵之道——警察抓小偷：受版权保护的内容不允许在公共空间非法传播，有害内容和非法内容需要拦截
- 恢复内容的传播本性，支持合理使用：私有空间、图书馆、低收入人群等合理使用

参考文献

1. 数字媒体宣言 http://manifesto.chiariglione.org/dmm.php
2. 北大信息科学技术学院《视频编码与理解》数字媒体安全与版权管理技术 黄铁军 2009.05.06