



IPTV 超高清视频中的 DRM 技术研究与应用

沈晶歆

(中国电信股份有限公司上海研究院, 上海 200122)

摘 要: 对 OMA、微软、Intertrust、ChinaDRM 等不同 DRM 标准进行特点和差异性比较, 提出 DRM 应用的需求场景, 分析了 DRM 关键技术, 基于业界普遍使用的高安机顶盒对 IPTV 高清视频领域 DRM 保护需求进行架构设计, 创新性地提出了高安机顶盒的硬件信任根、远程下载终端密钥、双重加密的内容密钥, 能够充分利用目前机顶盒生产过程中已有的芯片 OTP 数据烧写流程, 既充分考虑运营中的可实施性, 又保障了 DRM 安全性, 最后制定了 DRM 内容解密的业务流程并给出实施案例。

关键词: DRM; IPTV; UHD

中图分类号: TN915

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018283

Research and application of DRM technology in IPTV UHD video

SHEN Jingxin

Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200122, China

Abstract: The characteristics and differences of different DRM standards such as OMA, Microsoft, Intertrust, and ChinaDRM were compared. The requirements of DRM applications were presented. The key technologies of DRM were analyzed. Based on the high-tech set-top box commonly used in the industry, the architecture of DRM protection in IPTV high-definition video was designed. The hardware trust root of high security set-top box, remote download terminal key, double-encrypted content key and other mechanisms was put forward innovatively. Finally, the business process of decrypting DRM content was formulated and an implementation case was given.

Key words: DRM, IPTV, UHD

1 引言

4K 是新兴的分辨率标准, 其 UHDTV 规格可以达到 3 840 dpi×2 160 dpi, 最高的 Full Aperture 4K 规格更是达到了 4 096 dpi×3 112 dpi。对比现在主流 1080P 的 1 920 dpi×1 080 dpi, 4K 能够提

供 4 倍以上的清晰度。除分辨率外, 全 4K 还需要实现高动态范围 (HDR)、高帧率 (P60)、宽色域、高色深 (10 bit) 等特征。全 4K 技术能向用户提供色彩更丰富、颜色更逼真的宽带视频, 色调变化更细腻, 颜色层次更丰富, 色彩和亮度更接近真实环境, 使得用户体验得到显著提升。

收稿日期: 2018-10-07; 修回日期: 2018-11-14



全 4K 内容在制作时需要更换前端拍摄、制作设备,拍摄成本远高于高清视频。因此,各大内容提供商纷纷把全 4K 内容视为高价值内容,为保护内容权益,各牌照方明确要求电信运营 IPTV 业务时需要对视频内容进行版权保护,希望系统具备严格的内容保护能力,防止被非法盗版播放,内容提供商需要对 DRM 能力进行确认后才能提供全 4K 内容。

2 主要 DRM 标准简介

目前被业界认可的 DRM 标准有 MovieLabs ECP、OMA DRM、InterTrust Marlin、ChinaDRM 等。

(1) MovieLabs ECP

好莱坞六大内容提供商为保护全 4K 内容,联合成立了技术标准公司 MovieLabs,制定了 UHD 内容保护标准《MovieLabs Specification for Enhanced Content Protection》(ECP)。所有好莱坞片商在输出 UHD 片源时,都会要求运营商整体符合 ECP 要求。ECP 主要对数字版权保护技术提出需求,要求在终端上实现基于芯片的硬件级别 DRM 保护,而且算法也要加密,但不提出实现方案。

ECP 对 DRM 的主要需求包括:

- 可信执行环境 (trusted execution environment);
- 安全启动&存储 (secure boot & storage);
- 安全视频路径 (secure video path);
- 输出控制 HDCP 2.2 (output control HDCP 2.2);
- 取证水印 (forensic watermarking);
- 侧信道攻击保护 (side channel attack protection);
- 第三方认证 (3rd party testing and certification)。

(2) OMA DRM

OMA DRM 是 OMA (Open Mobile Alliance,

开放移动联盟)制定的可应用于移动通信终端的 DRM 协议。OMA 组织于 2002 年 9 月发布了 OMA DRM V1.0,于 2006 年 3 月发布了 OMA DRM V2.0。OMA DRM 标准是完全开放的,目前大部分运营商都已经采用或计划采用 OMA DRM 标准。DRM v1.0 标准定义满足 Forward Lock、Combined Delivery、Separate Delivery 方式的基本商用需求;OMA DRM2.0 增加支持下载、流媒体、多媒体等多种业务模式,完善了版权发布者和 DRM 代理之间的授权对象和协议机制、内容和授权协议传送机制、加密和解密默写机制等。

OMA DRM 规范主要分为 3 个部分:对被保护媒体的数字内容格式 (digital content format, DCF) 的规范、对版权描述语言 (rights expression language, REL) 的规范和对内容下载方式的规范。

(3) InterTrust Marlin

Marlin DRM 是一个开放的数字版权管理标准,由 Intertrust 和索尼、松下、飞利浦、三星 4 家一线消费电子公司在 2005 年制定,其宗旨是为实现能够相互兼容的 DRM 系统,开发规定了 DRM 核心技术,确保基于 Marlin 的 DRM 技术具有相互兼容性。Marlin 标准包括 1 个核心系统的标准和 3 个传输系统标准,核心标准定义了 Marlin 的实现原理,传输标准定义了对于某一特定类型的传输信道 (如宽带、广播或移动等) 的附加需求以及公共域标准、IPTV 技术标准和物理媒体传输系统技术标准。

(4) ChinaDRM

ChinaDRM 论坛由中央电视台牵头,联合清华大学、国家广播电视总局广播科学研究院等几十家单位成立,宗旨是制定中国广播影视数字版权管理技术标准。2014 年发布《GY/T 277 互联网电视数字版权管理技术规范》,该标准面向互联网电视业务应用定义了内容封装格式、权利描述与授权、权利获取协议和信任与安全体系等数字版权管理基础格式、技术机制和方法,其中内

容封装格式定义了受保护内容在数字版权保护系统中的基本呈现形式,包括内容标识、加密信息及获取许可证必须的信息;权利描述与授权定义了描述数字版权管理系统权利的方法和向内容使用方进行使用授权的技术机制;权利获取协议定义了 DRM 服务端和 DRM 代理进行安全通信和传递许可证的技术方法;信任与安全体系定义了基于 PKI 系统的信任技术机制,包括内容保密性、身份鉴别和数据完整性。采用该标准定义的基础格式、技术机制和方法,能够构造一个端到端的互联网电视数字版权管理系统,对互联网电视内容进行有效的数字版权管理。2017 年,好莱坞 MovieLabs 和 ChinaDRM 已经签署了法务认可协定,发布数字版权保护联合声明,在国内共同推广 ChinaDRM 标准。目前 ChinaDRM 实验室与 FOX 签署数字版权保护战略合作框架协议。

上述标准中,MovieLabs ECP 从业务层面对 DRM 提出需求,这些需求已获得内容提供商、DRM 方案解决商和视频运营商的普遍认可,事实上常常作为制定具体技术标准的需求来源使用;OMA DRM 作为一个定义较为松散的协议,主要定义数字内容格式和版权描述语言,目前没有获得大规模商用;ChinaDRM 协议是国内目前主推的 DRM 标准。2014 年 5 月 6 日,国家新闻出版广电总局批准 GY/T277—2014《互联网电视数字版权管理技术规范》为中华人民共和国广播电影电视推荐性行业标准,在和好莱坞 MovieLabs 签订法务认可协定后,近年来在国内推广力度不断增强,使用 ChinaDRM 标准能够帮助 IPTV 运营商避免冗长的法务谈判,缩短内容获取时间;Marlin 虽然是开放标准,但是使用时需要向标准制定者缴纳一定的专利费,因此主要用在索尼、松下、飞利浦和三星生产的数码设备中,在国内 IPTV 视频领域并没有实现规模应用。

3 DRM 关键技术

DRM 的关键技术包括认证技术、加密技术、数字水印技术、防篡改硬件模块和智能卡技术。

(1) 认证技术

对视频播放和存储媒质,如数字电视机、机顶盒、PC、硬盘、存储卡等设备分配 PKI 公钥证书,通过公钥证书在通信或视频播放前进行身份认证、设备认证以及权限分配等功能。

(2) 加解密技术

使用对称/非对称密码、分组密码和流密码等各种密码算法来保护数字内容的安全以及实现必要的认证。

(3) 数字水印技术

利用头端水印、终端水印等各种数字水印算法来保护数字内容的完整性和版权信息等内容,同时为相关版权纠纷的判决提供证据。

(4) 防篡改硬件模块和智能卡技术

通过相关的硬件技术使得所有水印、加/解密等运算只能在安全模块中进行。

4 基于高安机顶盒的 DRM 系统架构

数据显示,2017 年我国 4K 电视机产量达到 3 300 万台,占全球 4K 电视机总量的 42%;4K 电视机国内销量占比近 60%,远高于 35%的全球平均水平;超高清机顶盒销量占比超过 54%,三大电信运营商全面普及 4K 机顶盒。

对超高清机顶盒,目前主流硬件普遍支持在芯片中内置安全启动和防刷机机制,可以大幅降低 DRM 部署难度和成本。基于高安机顶盒且满足 ChinaDRM 标准的 IPTV DRM 系统的结构如图 1 所示。

DRM 系统由加密模块、内容密钥管理模块、内容许可证管理模块、DRM 初始化模块、系统管理模块及终端机顶盒 DRM Agent 模块组成。

DRM 加密模块负责节目内容的密钥生成和

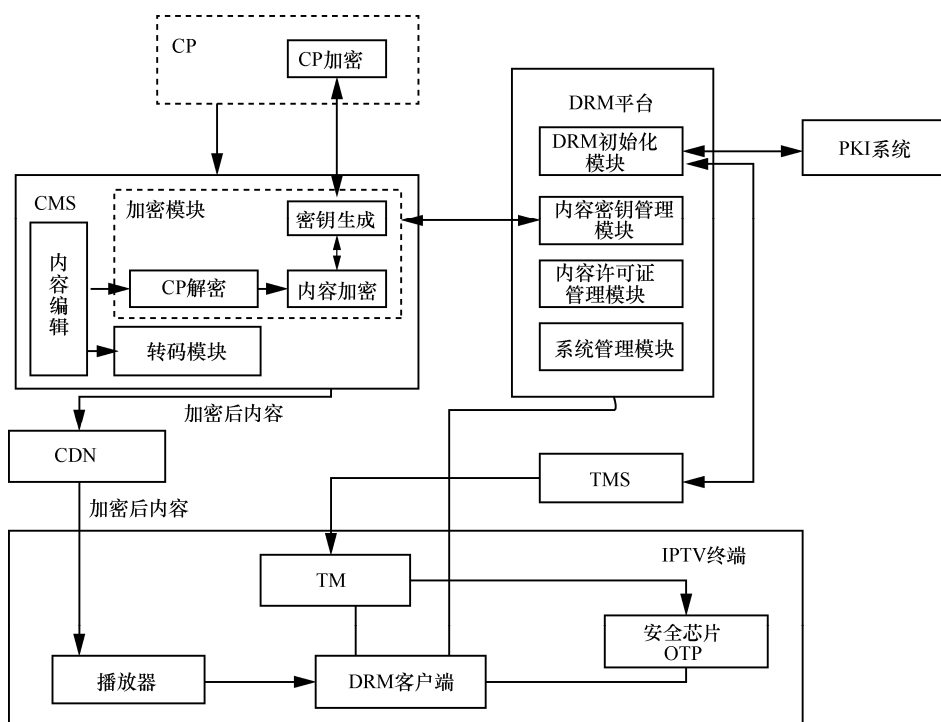


图1 基于高安机顶盒的DRM系统结构示意图

加密功能，内容密钥管理模块负责对内容密钥统一管理，支持和DRM内容加密模块对接，DRM初始化模块完成终端证书和终端密钥的管理并下发终端，内容证书管理模块负责生成内容许可证并下发终端，系统管理模块负责DRM系统的操作和维护。

终端机顶盒DRM Agent是DRM的核心模块，支持终端认证、内容授权及内容解密功能等功能，分为DRM客户端TA和DRM客户端CA两部分，分别运行在安全和非安全执行环境中。

终端管理程序TM实现开机终端身份验证，为DRM提供可信的安全基础。

5 基于高安机顶盒的DRM方案创新性

DRM实施的难点在于对信任根、终端密钥、内容密钥提出了严格的安全要求，信任根必须预置在终端芯片中且必须有防篡改功能，终端密钥和内容密钥既要保障安全性又要具备可操作性。本方案基于智能机顶盒的高安芯片基础，

创新性地提出了以下机制，保障了DRM方案的顺利实施。

(1) 基于高安机顶盒OTP数据的硬件信任根
本方案创新性地使用了高安机顶盒出厂时烧写在OTP数据中的SN(serial number)、RSA公钥作为硬件信任根，每个终端具备唯一的SN和RSA公钥，且不能被非法篡改。开机时，系统生成会话级公钥Kspub并用RSA私钥签名后通过安全接口下发给终端，终端使用RSA公钥验签后获得会话级公钥Kspub，用Kspub对挑战字计算结果和终端证书加密密钥等参数进行加密后发送给系统，系统使用会话级私钥Kspri解密后对挑战字计算结果进行验证。这样就在每次开机启动时进行了双向认证，即终端对服务器进行认证和服务器对终端进行认证。本方案充分利用高安机顶盒的OTP数据作为硬件信任根，避免了重新生成硬件信任根的繁琐操作，可利用目前已有的芯片OTP烧写数据流程实现硬件信任根录入，为DRM实施扫除了关键性障碍。

(2) 在线下载终端密钥

终端密钥包括终端的私钥、证书。终端证书中包含公钥及其证书链，终端证书采用 X.509 V3 格式。终端首次开机认证成功后启动终端私钥、证书的下载过程。系统使用终端开机时生成的终端密钥并随挑战字计算结果一起发送给系统的终端证书加密密钥，对终端证书和私钥进行加密并发送给终端，终端获取后解密得到终端私钥和证书，并保存在 TEE 中。如终端请求播放加密内容前，终端检测到未获得终端私钥、证书，或终端私钥、证书失效，则重新启动终端私钥、证书的在线下载过程。本方案可以使用远程下载方式获得终端证书和密钥，不需要在出厂前把终端证书和私钥录入终端，能够节省大量时间，缩短终端上线流程，保障了终端能够顺利启动 DRM 过程。

(3) 双重加密的内容密钥

内容密钥用于加密内容。内容密钥保存在内容许可证中，随内容许可证一起发送给终端。内

容密钥使用 RSAES-KEM-KWS 算法进行加密。用户在 EPG 门户上点击了加密内容的连接后，系统生成临时密钥，用该临时密钥加密内容密钥，用终端公钥加密临时密钥，将加密后的临时密钥、加密后的内容密钥封装在许可证中发送给 DRM 客户端。终端获取到许可证后，用终端私钥解密出临时密钥，用解密出的临时密钥解密出内容密钥，用内容密钥解密内容，实现内容的解码播放。

6 DRM 解密流程

基于高安机顶盒的 DRM 解密流程示意图如图 2 所示。

(1) 用户点击 EPG 门户 DRM 加密内容链接，播放器启动播放。

(2) 播放器检测节目内容的 DRM 标识位，判断加密状态。

(3) 若节目内容为 DRM 加密内容，播放器向 DRM 客户端 CA 模块发起播放请求，并将节目

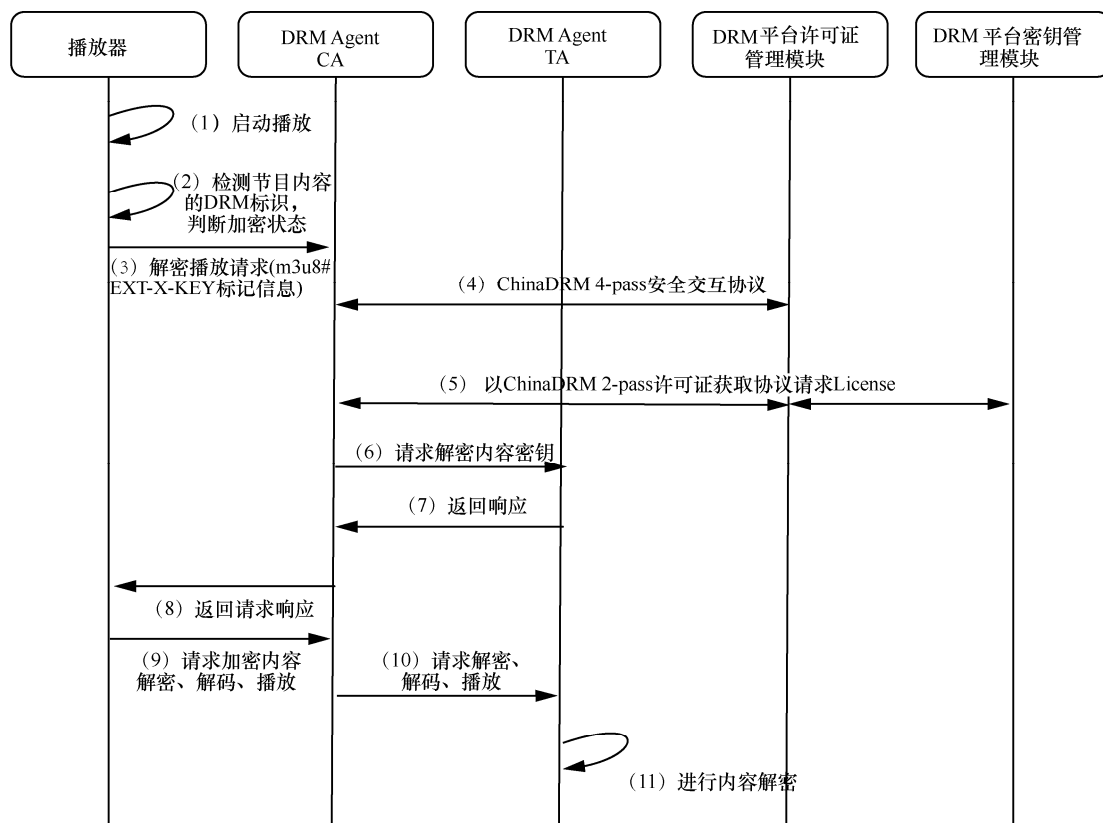


图2 基于高安机顶盒的DRM解密流程示意图



的 m3u8#EXT-X-KEY 标记信息发送到 DRM 客户端 CA 模块;若节目内容为非 DRM 节目,则直接播放该内容。

(4) DRM 客户端 CA 启动 ChinaDRM 4-pass 交互流程,向 DRM 系统请求进行交互,DRM 系统许可证管理模块完成签名校验和 4-pass 交互。

(5) DRM 客户端 CA 根据 URI 地址(标记于 m3u8 索引文件 #EXT-X-KEY 字段中)以 ChinaDRM 标准要求的 2-pass 许可证获取协议向内容许可证管理模块请求 License。DRM 系统的内容许可证管理模块对 2-pass 请求进行验签和证书合法性校验后,向 DRM 系统内容密钥管理模块请求内容密钥,加密及签名后封装在内容许可证中,下发给机顶盒。

(6) DRM 客户端 CA 模块对内容许可证进行验签后,把加密后的内容密钥发送给 DRM 客户端 TA 模块,请求解密内容密钥。

(7) DRM 客户端 TA 模块缓存解密后的内容密钥,向 DRM 客户端 CA 模块返回内容密钥获取成功的响应信息。

(8) DRM 客户端 CA 模块向播放器返回内容密钥获取成功的响应信息。

(9) 播放器服务向 DRM 客户端 CA 模块请求对内容进行解密、解码、播放。

(10) DRM 客户端 CA 模块向 DRM 客户端 TA 模块请求解密、解码、播放。

(11) DRM 客户端 TA 模块使用内容密钥对内容进行解密后播放。

本方案可为使用智能高安机顶盒的 IPTV 运营商提供既易于实施又能够严格保护超高清内容的 DRM 方案,例如中国电信、中国联通定制的高安机顶盒都能够很方便地部署该方案,目前该方案已在部分省进行部署,用来和好莱坞六大 CP 谈判获取超高清 4K 内容。

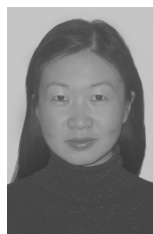
7 结束语

本文提出基于超高清高安机顶盒的硬件基础、遵循 ChinaDRM 标准的 IPTV DRM 系统设计,既能充分利用现有的高安机顶盒的安全启动和防刷机机制,在可行执行环境(TEE)下运行硬件级别的 DRM 客户端 TA 模块,实现解密、解扰、解复、播放、安全路径、安全存储等功能,又能契合国内外 DRM 发展趋势,帮助 IPTV 运营商避免冗长的法务谈判,缩短内容获取时间,为顺利引入国内外高质量全 4K 内容打下坚实的基础。

参考文献:

- [1] 荆雷,曹程. IPTV 业务中数字版权管理技术的应用前景[J]. 邮电设计技术, 2011(2).
JING L, CAO C. The application prospects of DRM for IPTV service[J]. Designing Techniques of Posts and Telecommunications, 2011(2).
- [2] 张志勇. 互融 DRM: 数字版权管理的新进展[J]. 网络安全技术与应用, 2013(10).
ZHANG Z Y. Inter-integration DRM: new developments in digital rights management[J]. Network Security Technology & Application, 2013(10).
- [3] 李劲松,梁春平,付二喜. 基于流媒体视角下的 DRM 技术探析[J]. 科技与创新, 2016(1).
LI J S, LIANG C P, FU E X. Analysis of DRM technology based on streaming media perspective[J]. Science and Technology & Innovation, 2016(1).
- [4] 罗传飞,施唯佳,肖晴. VBR 视频在 IPTV 点播业务中的应用[J]. 电信科学, 2014, 30(5): 3-9.
LUO C F, SHI W J, XIAO Q. Application of variable bit rate video in IPTV on demand service[J]. Telecommunication Science, 2014, 30(5): 3-9.

[作者简介]



沈晶歆(1974-),女,中国电信股份有限公司上海研究院高级工程师,主要研究方向为超高清视频。