互动视频业务保护技术与应用

ECHNOLOGY AND APPLICATION OF INTERACTIVE VIDEO SERVICE PROTECTION

杨 成 编著

中国传媒大学出版社

互动视频业务保护技术与应用

ECHNOLOGY AND APPLICATION OF INTERACTIVE VIDEO SERVICE PROTECTION

杨 成 编著

中国传媒大学出版社

图书在版编目(CIP)数据

互动视频业务保护技术与应用/杨成编著. —北京:中国传媒大学出版社,2013.12
ISBN 978-7-5657-0892-3

Ⅰ.①互… Ⅱ.①杨… Ⅲ.①视频信号—数字技术—应用—传播媒介—研究
Ⅳ.①G206.2

中国版本图书馆 CIP 数据核字(2014)第 009134 号

互动视频业务保护技术与应用

编　　著　杨　成
责任编辑　王雁来
责任印制　阳金洲
封面制作　泰博瑞国际文化传媒
出 版 人　蔡　翔

出版发行　中国传媒大学出版社
社　　址　北京市朝阳区定福庄东街 1 号　邮编:100024
电　　话　86—10—65450528　65450532　传真:65779405
网　　址　http://www.cucp.com.cn
经　　销　全国新华书店

印　　刷　北京中科印刷有限公司
开　　本　787×1092mm　1/16
印　　张　17.25
版　　次　2014 年 3 月第 1 版　　2014 年 3 月第 1 次印刷

书　　号　978-7-5657-0892-3/G·0892　　定　　价　59.00 元

目录

第1章 概 述

1.1 互动视频业务的安全需求

互动视频业务是一种基于宽带互动电视 iDTV、IPTV 等互动视频系统的实时视频广播与点播业务，采用机顶盒、PC 机以及移动多媒体终端等实时接收和观看。随着对视频内容个性化体验要求的不断提升，互动视频业务已经成为推动数字电视产业发展的重要支撑。同时，互动视频业务通过与相应的互动视频网络、计算机网络、多媒体技术以及通信技术等的有机结合，可以为以家庭电视为代表的主要接收终端提供大量的个性化服务和高清晰度视频节目内容，是实现三网融合的重要途径。

目前，提供互动视频业务的主要途径包括基于 HFC 的 DVB - C 数字电视系统①、基于 IP 的 IPTV 系统②和 OTT - TV 系统③。不论在哪一种系统下，由于互动视频业务所具有的互动性、开放性、泛在性、多样性、灵活性等特点，决定了对媒体内容与业务运营提供灵活高效的安全保护，既是互动视频业务系统不可或缺的重要组成部分，也是理论研究和技术实现的焦点

① Jones G. A. , Defilippis J. M. , Hoffmann H. , Williams E. A. , "Digital Television Station and Network Implementation", *Proceedings of the IEEE*, 2006, Vol. 94, pp. 22 - 36.

② Degrande N. , Laevens K. , De Vleeschauwer D. , Sharpe R. , "Increasing the User Perceived Quality for IPTV Services", *IEEE Communications Magazine*, 2008, Vol. 46, pp. 94 - 100.

③ 罗松：《OTT TV 推动新一轮三网融合的兴起》，《电信网技术》2013 年第 1 期，第 1 - 4 页。

之一。

互动视频业务的重要基础是节目内容的数字化和传输交换的网络化以及宽带互动能力,但也正是因为数字化和网络化,使得对节目内容的保存、篡改、盗版、传播变得异常容易,严重地损害了内容提供商的利益,影响了互动视频业务的健康和有序发展,必须通过相应的技术手段对节目的版权进行保护。数字水印和数字签名等技术的发展为有条件播出和盗版追踪提供了可能。

互动视频业务一般都要实现对节目流(组)的访问控制;也关系到运营商的生存和发展。有条件接收系统(Conditional Access System,CAS)正是为解决这一问题而产生的。CAS 采用数据加密、访问控制、安全的系统体系结构、密码算法以及密钥与用户的安全管理等措施和手段,来达到保证整个互动视频业务传输和运营安全的目的,保护了网络运营商、传输公司和消费者的利益。

在国家层面上,构建高可信网络具有重要的战略意义,正好与互动视频业务的发展形成互补。互动视频业务的发展为高可信网络的建设提供了切实的需求和真实的应用环境,而高可信网络作为网络基础设施,又可以成为互动视频业务可持续发展的重要保障。安全技术是互动视频业务与高可信网络共同的重要支撑。

总的来说,互动视频业务对安全技术的需求从总体上可以分为三类:(1)业务安全需求;(2)内容安全需求;(3)监管需求。

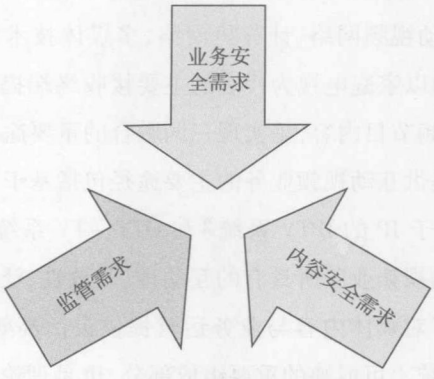

图 1-1 互动视频业务的安全需求

“业务安全需求”主要是指业务提供商和网络运营商在进行业务提供和内容分发时的业务保护、认证授权等。在传统的 DVB 标准中,是采用单向有条件接收系统来解决这个问题的。但是传统的单向有条件接收系统是在广播电视单向传播的条件下提

出的解决方案，存在着带宽占用大、授权时延长、系统复杂、灵活性差、无法跟踪用户状态等问题。对于互动新媒体业务，单向有条件接收技术显然无法适应，也无法充分利用双向网络的优势，更无法适应 DVB/IPTV 双模业务安全的需要。

“内容安全需求”主要是指内容提供商进行内容生产和交易中的内容保护、认证授权等，主要通过数字版权管理技术体系加以解决。数字版权管理体系涉及版权封装、权限管理、盗版追踪、互操作等具体问题及其相应的技术解决方案。互动视频业务中的内容安全主要是针对点播业务与 B2B 业务，需要进行预封装，同时也希望能对盗版追踪提供支持。

“监管需求”主要是指对业务运营商和网络运营商分发的节目、用户终端使用的节目的合法性进行监管，防止非法、“三俗”等内容的流入，阻止对和谐社会和精神文明建设的破坏。目前，监管技术主要是从信号是否异常等传输层面进行监控，同时兼顾内容层面的识别与处理，数字水印技术作为监管的技术储备，已经逐渐引起人们的关注，但是数字水印技术本身的算法鲁棒性等问题成为影响其应用的重要瓶颈。同时，建立数字水印基础设施和基于数字水印的监管体系也是大规模产业化应用的重要问题。

1.2 视频业务保护技术的发展

互动视频业务大规模应用对相应的业务保护系统提出了越来越高的要求，许多技术问题亟待解决。例如，版权保护如何支持互操作，并解决与合理使用之间的矛盾；有条件接收如何适应互动环境，提供支持跨网络、大规模用户的认证授权；如何提供更加灵活的权限控制和更加方便的权利使用方法；如何利用数字水印、模式识别等技术提供盗版鉴别和盗版追踪能力；如何利用先进技术为内容、业务监管提供高效解决方案，保障行业与社会的可持续发展；如何面向云计算提供安全服务与存储能力，解决用户隐私保护、运营利益和政府监管之间的矛盾等，这些都是摆在我们面前的现实需求。

DVB、IPTV 等领域都先后就视频业务保护问题制定了诸如 DVB - CAS①、18Crypt②、OMADRM③ 等技术标准，我国的 ChinaDRM 等组织也围绕着广播电视行业的视音频应用，在节目内容制作编辑、传输分发、数字家庭等多个环节都开展了标准制定

① Digtal Video Broadcasfiy(DVB),“Conditional Access”,www. dvb. org/sfandard

② “FEC62455 ed2.0”,www. iec. ch.

③ “OMA Digital Rigats Manayement v2.2”,www. openmobilealliance. org

工作。①

图 1 - 2 以广电领域为例给出了需求驱动下的电视业务和技术要求的总体变化情况。如何正确把握用户需求，建立起需求驱动的电视业务和高效可靠的业务环境，是行业得以可持续发展的根本。

在数字化发展的初期为了追求节目的高质量，提出了节目数字化的需求，启动了广电系统从节目制作到节目播出、传输和使用的全流程数字化改造进程，在这一时期，业务保护方面广泛应用的主流技术是结构复杂的基于单向广播的有条件接收（DVB - CAS）技术②。

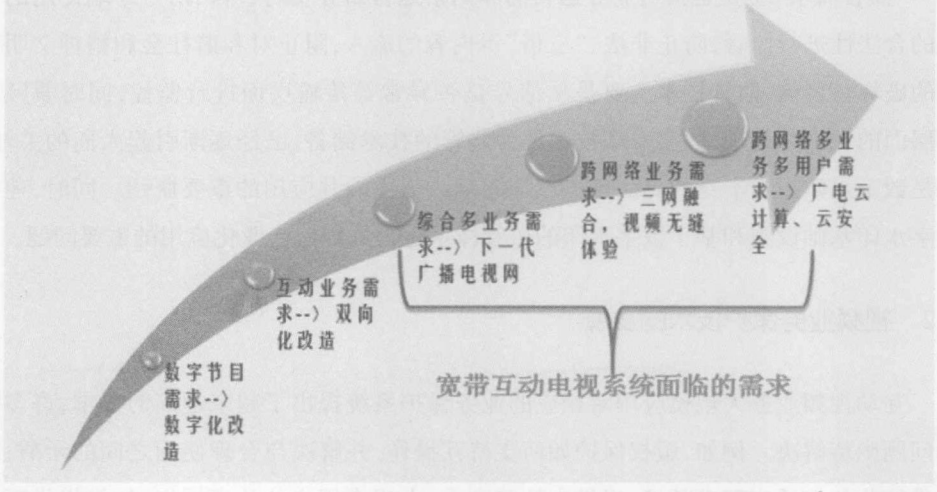

图 1 - 2　需求驱动的电视业务

在第二阶段，为了追求个性化的视频服务，互动业务的需求日益增长，以有线电视为代表的广电网络双向化改造进程随之启动。传统的有线电视单向 HFC 网络，通过技术改造（例如：Cable Modem、IP 网络改造及 EPON + EOC 等）可以变成具有 IP 回传通道的非对称双向宽带网络，从而实现互动电视业务。同时，IPTV 也在悄然崛起。由于它天生就具有的数字化、宽带交互等特征，发展势头非常强劲，更有超越数字电视的趋势；中央电视台、北京人民广播电台和上海文广等传媒巨头都已经开始了 IPTV 的部

① “IPTV 内容分发数字版权管理技术标准”，www. chinadrm. org. cn

② ETR 289：Digital Video Broadcasting（DVB）：Support for use of scrambling and Conditional Access（CA）within digital broadcasting systems，1996

署,中国电信和中国网通也分别依托“互联星空”和“天天在线”网络平台开始建设IPTV,在广东、北京、东北建立了IPTV的试点。① 在国外,尤其是发达的北美和欧洲,基于DVB-C和IPTV的互动电视业务更是得到了较好的发展和普及。

这一阶段的业务保护技术朝着体系化的方向在发展,重点是研发基于双向网络实现的DVB/IPTV双模统一的有条件接收系统,可以放弃针对单向数字电视广播设计的复杂CA技术,采用通用加扰技术,通过认证、授权、加密传输等新的安全管理方式,对用户的接入控制、授权服务进行管理。

当前,随着数字化、双向化的不断深入,也随着社会经济的快速发展,人们对广播电视的观念悄然改变,从“看电视”转变为“用电视”的社会需求逐渐显现。在这一阶段,互动视频业务逐渐成熟,下一代广播电视网络(NGB)的建设也列入了议事日程。针对宽带和互动的需求,NGB规划中提出了构建综合多业务平台的解决思路,在业务保护方面,数字版权管理、盗版追踪等技术也不断演进,成为NGB中不可缺少的重要组成部分。同时,用户对业务体验的需求也不断提升,跨网络业务体验、视频无缝体验、电视电话等引起了业界和公众的共同关注,在这一背景下,割裂的广电、电信、互联网对这些新业务的发展形成了阻碍和制约,于是,三网融合成为关系到国家发展的战略问题,与之相适应的业务保护技术也在朝着跨网络、大规模并行处理的方向发展。

网络规模的不断扩大和互动新业务种类的不断增多,导致了业务承载的负荷和业务管理的复杂性在不断上升,如何为运营商提供更加简便高效的跨网络、多业务、多用户的业务运营支持,也为终端用户提供真正无缝的业务体验,是下一阶段发展的主要任务,为此,业务保护系统将基于广电云计算、云安全的思想,采用分布式技术、虚拟化技术、智能化技术等,构建一个统一的、安全的、灵活的业务运营环境。

1.3 互动视频业务保护的技术问题

在iDTV、IPTV等互动视频系统的建设发展中,对互动视频业务内容的保护与控制正成为影响互动视频业务得以推广的重要瓶颈。在建立基本的互动视频业务系统后,很多运营商和学者开始考虑如何提供安全、高效、一体化的内容保护、传输保护和访问控制,甚至盗版追踪和内容监控,进而实现对互动视频内容及其业务的保护,实现系统服务的价值,促进产业健康有序发展。

① 李晓明等:《盘点新媒体》,《现代电视技术》2007年第4期,第120-122页。

采用传统的有条件接收技术等视频业务保护系统是运营商首先考虑的解决方案。但是传统的视频业务保护系统建立在单向网络上，为了将控制字、用户的授权信息和管理信息等重要内容安全可靠地传输到客户端，采用了层层设防的基本思想，系统结构复杂，安全性不高，疲于与黑客破解作斗争。

由于传统的广电网属于单向的广播网络，决定了其视频业务保护系统也必然是广播方式。在这种方式下，服务前端不了解客户端的任何状况，无法对客户端的有效性和可靠性进行验证，客户端也无法验证前端的有效性和可靠性，只能被动地接收，这与视频业务保护系统针对用户及其收看行为进行节目收费的初衷存在矛盾。在传统的视频业务保护系统中解决办法是前端对所有用户生成可能需要的安全信息并加以传输，这样做一方面增加了网络负载，浪费了大量的带宽，给用户体验带来了较大的延迟；另一方面又因为大量加密信息的存在，增加了破坏者破解加密体制的可能性，形成潜在的安全隐患。

传统的视频业务保护系统采用了复杂的多重加密作为其密钥管理机制，这样做虽然从理论上说是安全的，但是却增加了实施的难度，并且在系统架构的设计和实现中都存在安全漏洞。实际上每增加一个密钥，对密钥的生成、分发、管理的难度就会有大幅度的提升。破坏者只要破坏其中的任何一个环节，就可以有效地摧毁整个系统，即使是采取多密码算法备份等辅助措施，也无法从根本上解决这个缺陷。

广电网络的双向化，为解决上述问题提供了手段和途径。建立在双向网络基础上的互动视频业务保护系统，可以借鉴传统 Internet 上成熟的安全技术[①]，结合双向广电网自身的特点，提出复杂性低、安全性高的互动视频业务保护技术解决方案。互动视频业务保护系统解决的核心问题是基于 CSA 和高强度加密的信息安全策略，实现在用户访问控制下的认证、授权和计费服务，具体包括业务的传输安全（实时加扰、有条件播出）服务、业务的访问控制（认证、授权）服务、内容安全（加密封装、盗版追踪、内容监控）服务等。

从实际应用中我们可以归纳出诸多方面的安全需求，提供不同的安全服务所需要满足的安全需求也不尽相同，表 1－1 给出了不同的安全服务与面临的安全需求之间的对应关系。

---

① ISO/IEC 10745：1995 Information technology－Open Systems Interconnection－Upper layers security model；GB/T 17902.2－2005 信息技术 安全技术 带附录的数字签名 第 2 部分：基于身份的机制；GB/T 17902.3－2005 信息技术 安全技术 带附录的数字签名 第 3 部分：基于证书的机制；GB/T 16264.8－2005 信息技术 开放系统互连 目录 第 8 部分：公钥和属性证书框架。

表1-1 安全服务与安全需求对应关系

	业务的传输安全	业务的访问控制	内容安全
业务逻辑安全需求	✓	✓	✓
身份认证需求		✓	
访问控制需求		✓	
重复提交控制需求		✓	
保密性需求	✓	✓	✓
完整性需求	✓	✓	✓
可用性需求	✓	✓	✓
不可伪造性需求		✓	✓
不可抵赖性需求		✓	
超级分发控制需求			✓
系统自身安全需求	✓	✓	✓
安全机制的实时性需求	✓	✓	✓
鲁棒性需求	✓		✓
不可感知性需求	✓		✓
信息嵌入容量需求	✓		✓

其中，业务逻辑安全需求、保密性需求、完整性需求、可用性需求、系统自身安全需求是提供各类安全服务所面临的共同基础性需求。业务逻辑安全需求强调软件、脚本等的业务处理逻辑代码和配置不产生漏洞和缺陷；保密性需求、完整性需求在不同的安全服务下有不同的表现形式，传输安全中强调业务传输流的保密性和完整性，访问控制中强调认证和授权信息的保密性和完整性，内容安全中则强调视频内容在加密封装中的保密性和完整性；可用性需求、系统自身安全性需求强调安全服务系统及其网络的可用和软硬件环境的安全。

此外，业务的访问控制还面临身份认证、访问控制、重复提交控制、不可伪造、不可抵赖等安全需求；业务的传输安全还面临传输流加扰封装、有条件播出的实时性以及有条件播出合法性水印的鲁棒性、不可感知性、信息嵌入容量等需求；内容安全还面临视频内容高效封装、内容监控的实时性以及视频内容盗版的超级分发控制、版权和指纹水印的鲁棒性、不可感知性、信息嵌入容量等需求。

通过对上述安全需求的全面满足，互动视频业务保护系统便能够实现各项数字电视广播业务的授权管理和接收控制。其中，信任模式主流的身份认证技术包括两类，

即基于 PKI(Public Key Infrastructure)的认证和基于 IBE(Identity Based Encryption)的认证。PKI 认证需要认证中心的支持,由认证中心将其生成的身份证书与用户的信息绑定,并且身份认证过程也需要认证中心的参与,认证中心作为可信的第三方给出身份确认的证明。IBE 认证是采用被认证方公开的标识,如 URL,作为初始值,通过双线形映射函数得到公钥,来认证由被认证方的私钥加密的数据签名。IBE 认证过程中不需要第三方认证中心的支持,也不需要身份证书的传递过程,系统得到了简化,安全性也得到了提高。PKI 和 IBE 两种认证技术可以根据不同的应用场景来进行选择。

另外,互动视频业务保护系统是一个综合性的系统,系统的研发与建设与传统的有条件接收系统类似,将涉及多种技术,包括系统管理技术、网络技术、加解扰技术、加解密技术、数字编解码技术、数字复用技术、接收技术、智能卡技术等,同时也将涉及用户管理、节目管理、收费管理等信息管理应用技术。①

基于双向网络实现的 iDTV、IPTV 互动视频业务保护系统,可以放弃针对单向数字电视广播设计的复杂 CA 技术,采用通用加扰技术,通过认证、授权、加密传输密钥等新的加密和管理方式,对用户的接入控制、授权服务及有条件接收进行管理,从而实现对业务、内容进行安全保护的目标。

① 关亚林等:《数字有线电视前端系统组成》,第八届国际广播电视技术讨论会(ISBT'2003),2003 年。

第2章
互动视频业务保护模型

2.1 单向有条件接收系统

传统的视频业务保护主要是指数字电视广播标准①②③的条件接收技术及其系统(CAS:Conditional Access System),它适合于有线数字电视应用场景下的单向认证授权。只有得到授权的用户才可以正常地访问这些受保护的业务数据。

CAS在单向广播环境中,将业务流与业务流密钥分别通过两类不同的安全逻辑通道进行广播传输(复用),不同的终端用户占用不同的安全逻辑通道,并由终端完成对业务流的访问控制。

在实际中,为了提高系统的安全性,往往采用更加复杂的变换,如CSA④(Common Scramble Algorithm)和AES(Advanced Encryption Standard)等。

---

① GY/Z 175-2001,《数字电视广播条件接收系统规范》,中华人民共和国广播电影电视行业标准化指导性技术文件。

② ITU-R Rec. BT.810:Conditional Access Broadcasting Security in the System by Interacting with Receiver Systems,1992.9.

③ H. Shirazi, J. Cosmas, D. Cutts, "Mobile Integrated Conditional Access System", IEEE International Symposium on Consumer Electronics-ISCE08,2008, pp. 1-4.

④ Jones G. A., Defilippis J. M., Hoffmann H., Williams E. A., "Digital Television Station and Network Implementation", *Proceedings of the IEEE*,2006, Vol. 94, pp. 22-36.

单向有条件接收系统虽然一定程度上解决了单向广播环境中业务安全传输和用户使用控制问题，但是，其技术体系依然存在不完善的地方，比如加密系统的安全性问题，用户认证授权的安全性问题，对业务环境的适应性问题、核心算法的标准化问题等。

2.2 数字版权管理系统

数字版权保护，即所谓的 DRM（Digital Rights Management），就是采取包括信息安全技术手段在内的系统解决方案，在保证合法的、具有权限的用户对数字信息（如数字图像、音频、视频等）正常使用的同时，保护数字信息创作者和拥有者的版权，根据版权信息使其获得合法收益，在版权受到侵害时能够鉴别数字信息的版权归属及版权信息的真伪，并确定盗版数字作品的来源。① DRM 一般都采用安全容器②的方式对内容进行封装，利用权限描述语言③对权限加以规范化说明。

版权保护是技术手段与非技术手段的结合。在我国有专门的版权保护执法机构和相应的法律法规，同时社会道德建设也从另一方面强调提高大众的版权意识，形成自觉拒绝盗版的社会风气。法律对知识产权保护进行规范，技术在不断发展的过程中使知识产权的保护得以实现并逐渐完善，管理定义了知识产权信息的内容，并与技术密切结合形成实际中的版权保护方案。采用密码学、数字水印等在内的信息安全技术为数字化信息的版权执法和权益维护提供支持和手段，并可作为司法鉴别的依据。随着盗版的猖獗和人们版权保护意识的增强，为在互联网上传播的数字作品提供强有力的版权保护与管理机制成为目前的当务之急。

版权保护是对数字作品作者的署名权、社会及经济利益的保护。通过版权保护将数字作品与其作者或拥有者绑定在一起，如通过安全容器将作者版权信息与数字作品进行加密封装，或将标识作者版权信息的序列号以数字水印的形式嵌入到数字作品中，并通过媒体桥④建立与作者的联系。任何人获得数字作品，也同时显式或隐式地获得了其作者或拥有者的信息。如果对数字作品的使用超出了合理使用的范围，根据版

① 王永淀等：《媒体安全监控》，中国传媒大学出版社 2007 年版。

② O. Sibert, D. Bernstein, D. V. Wie. "The Digibox: A Self - protecting Container for Information Commerce", Proceedings of the 1st USENIX Workshop on Electronic Commerce, 1995. 7

③ ODRL, http://www. w3. org/TR/2002/NOTE - odrl - 20020919, 2002. 9

④ Digimarc, www. digimarc. com/products/mediabridge/default. asp, 2004. 5

权法规和作者要求，就应向作者交纳版权使用费。

版权保护同时也包括权限管理或访问控制。受版权保护的数字作品其传播和使用也是受保护的，任何希望使用数字作品的用户（个人或团体），首先应征得数字作品作者或拥有者的许可，这种许可可以是口头的、书面的或使用权限描述语言[①]描述的数字化权限。权限可以是免费的也可以是有价的，它给出了用户拥有的对某数字作品的能力描述，如DVD的一个权限描述中允许用户在其家庭网络中任意复制、观看某一数字节目，但不允许将该节目拷贝或转发给家庭网络之外的设备上。

版权保护所保护的作者版权信息和用户的权限信息具有可验证性，任何时候都不会产生含糊的不一致的版权归属结论，也不会错误地理解用户的权限。数字作品的作者既可以在需要的时候声明自己对数字作品的拥有权，也不能抵赖或伪造其对某数字作品的拥有权。对于用户的权限，在用户端必须提供合理的机制对其进行解释，并依据解释结果控制用户对数字作品的使用和传播，同时应提供对权限的安全存储和管理，阻止未经授权的访问和篡改。

版权保护提供对盗版追踪的支持。为了最大限度地打击盗版，数字作品在传播过程中应为其用户添加唯一的用户标识，并将该标识与用户获得的数字作品采用数字水印等方式绑定在一起。一旦发生盗版，数字作品的作者或版权执法机构就可以根据与盗版数字作品绑定的用户标识追踪到盗版的源头，进一步提起司法诉讼，并进行相应的处罚。该用户标识同样应具有可验证性，任何人不能伪造、篡改、抵赖和去除。

DRM提供了一种可操作、可控制的方式来保障内容的可用性、保护作者的权益。《数字版权管理技术及应用研究进展》[②]一文中提到，数字版权管理价值链的组成包括：(1)内容创作者；(2)版权拥有者和管理机构；(3)内容代理和发行商；(4)注册与认证；(5)数字版权管理方案提供商；(6)支撑信息系统提供商；(7)内容仓储管理；(8)应用开发者；(9)存储和传输服务、运营；(10)网络服务提供商；(11)接入服务提供商；(12)硬件终端设备制造；(13)软件终端开发。DRM对内容从制作、编辑、存储、分发、使用的全生存期实施完整保护，只有被授权的用户才能够访问受保护的内容。

---

① ODRL, http://www.w3.org/TR/2002/NOTE-odrl-20020919, 2002.9

② 范科峰、莫玮、曹山、赵新华、裴庆祺：《数字版权管理技术及应用研究进展》，《电子学报》2007年第6期。