流媒体国际标准化DRM技术动态综述*

□ 李颖 白海燕 王莉 乔晓东 / 中国科学技术信息研究所 北京 100038

摘要：DRM既是内容流通领域的重要技术，也是确保同时满足内容的创作者、提供商、用户等不同角色需求这一复杂流通环境的必要技术。DRM的应用会部分妨碍用户获取内容，但因不当拷贝内容的事件持续发生，提供商针对各种问题被迫实施DRM强化技术。文章首先介绍早期的DRM；通过DVD应用案例概述DRM技术；阐述快速普及的手机移动设备的DRM标准，即OMA DRM；在存储介质的DRM方面，以SD卡为例介绍CPRM技术；有关DRM国际标准化活动，以MPED—21为中心案例，解说IPMP技术；在事实标准化活动案例中，列举业界主导型DRM，即Coral，给出其要点；最后，总结DRM的现状和未来。

关键词：DRM，内容流通，加密方式，DVD，CPRM/CPPM， MPEG—21，REL，IPMP，Coral
DOI：10.3772/j.issn.1673—2286.2010.11.007

序言[1]

DRM（Digital Rights Management的简称，本文称作数字权益管理）目前虽然不被众人所知，但其必要性已被业界认同。术语DRM出现在许多场景，由于持不同视角的人对DRM内容理解各异，还不存在DRM的共通认识。DRM作为各种内容传播体系的关键技术，事实上已被广泛应用，但从独立工具到复杂的认证系统，其中所使用的DRM技术千姿百态，很难定义什么是DRM技术。为使DRM技术明确和具体化，本文对从DRM早期模式到进化中产生的几种典型的DRM系统进行概要说明，利于读者看到有形的DRM，同时也论及DRM的若干问题。DRM依然是发展中的技术，由于其特殊性（保密性），公开的信息并不多。本文尽量列举国际标准化的重要技术，在公开可检索的信息范围之内，对DRM进行通俗的介绍。

1 DRM发展历程及初期DRM

DRM发展历程

DRM技术处理的数字内容一般术语称数字项（digital item，也称数字对象）。DRM的出现是管理者为了限制数字对象被复制次数及复制行为本身而开发的技术。从传播方来看，DRM技术是防止音视频等流媒体内容这类非免费创作物被无端不当使用的技术。通常，原创数字对象以非公开的保密方式加以记录，使其不被普通的软件或硬件技术再生。DRM技术的引入，使内容消费者的复制及再利用有可能变得困难。所以说，DRM技术是一种保护技术。引入了防拷贝技术的内容传播系统有时也被称作DRM，同时，以限制拷贝为目的开发设计的系统技术也称作DRM。

近期开发的DRM系统，在兼容性、互操作性以及标准化等方面有所考虑。另外，在DRM未来发展方向上，开始探索其与数字内容著作相关的价值链（Value chain）、资金链（Money Chain）之间的关联。

初期DRM

DVD 1996年左右开始进入市场，DVD的易处理性和易规模化生产的方式，使其市场发展方面被寄予了极大的关注，与此同步，拷贝控制的市场关心度也在提高。图1显示了以DVD媒体为中心的早期DRM机制。DRM技术在可规模化生产媒体中的正式应用始于DVD，它是构建后继DRM技术基础的实用案例。当时还处于数字与模拟信号VCR（Video Cassette Recorder，磁带录像机）共存的过渡期，在存储媒体环境中，经由模拟信号的拷贝也存在问题，因此引入了禁止DVD内容模拟拷贝的干扰信号Macrovision（即录像噪音信号，也称复制保护信号）[2-3]，如图1所示。

Macrovision是在TV模拟信号AGC（Automatic Gain

* 基金项目：本文系科技部国际科技合作项目“建立中国数字对象唯一标识体系的研究与应用”(项目编号：2007DFA10580)的研究成果之一。

图1 DVD采用的DRM技术和其流程案例*

*目标是保护刻录完成的DVD内容，是版权持有者对数字内容复制方式对策的需求。
→以终端设备厂家为中心，开发内容加密方式CSS（Content Scrambling System，内容加扰系统），引入到DVD。
→基于第三方，设立钥匙键管理机构，考虑模拟信号视频输出的录像禁止。
→在内容中，嵌入Macrovision公司开发的Macrovision信号。

Control，自动增益控制）部分中，嵌入特殊信号，干扰模拟信号录像设备的动作，这一方式被认为是DRM技术的开始。当时出现了模拟信号VRT的拷贝问题，但由于不同代产品间拷贝品质的劣化，著作权问题看似收敛。然而，伴随数字时代的到来，出现了完美无瑕的复制品，录像设备的拷贝问题再度复燃。

数字化早期的民用设备著作权管理技术中，VCR及盒式磁带等所采用的禁止拷贝标志（Flag）是很好的案例，其采取了实现物理上禁止拷贝的措施。之后，内容业界的权利意识提高，开发了采用近乎纯粹的数字数据和程序的控制系统技术，即使拷贝了数字项的数据，也无法视听再生的该数字项的拷贝。

2 DRM技术[4-15]

IT行业，即PC环境下，采用PC Bus（总线）进行认证，而DVD媒体（记录介质）的DRM应用也有其实用化的合理考虑，以下介绍各种媒体中DRM的机制。

2.1 面向媒体的DRM技术

媒体业界所适用的DRM关键技术如图2所示，按视频和音频领域顺序排列。这里简要介绍必要的DRM关键技术的功能和特征。

如图2所示，适用音视频领域的DRM技术大体分为电子水印及加密和认证。电子水印技术专注内容，是在内容分发渠道跟踪中直接嵌入所需信息的技术。

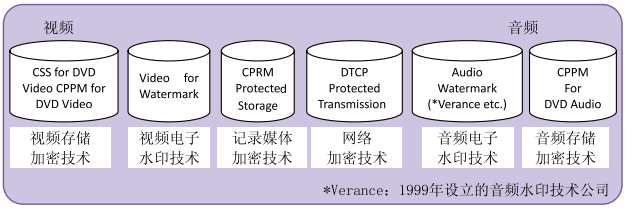

图2 视频和音频储存媒体所用DRM技术案例*

*DRM技术的特征：
① 分为加密和电子水印技术
② 可适用模拟和数字信号两类的内容保护
③ 满足来自内容持有者需求的规范化技术，SDMI（Secure Digital Music Initiative，安全数字音乐倡议）等

由于内容的保密性，电子水印信息的嵌入场所、嵌入信息，及技术内容的细节不公开。电子水印的信号信息，由于直接嵌入内容中，对原内容而言为噪音。在噪音不被感知的前提下，确保嵌入的信息量是嵌入技术的重点，它不是DRM的系统技术，被视为个别的DRM关键技术。图2的CSS（Content Scrambling System，内容加扰系统）、CPPM（Content Protection for Prerecorded Media，预录制媒体内容保护）、CPRM（Content Protection for Removable Media，移动媒体内容保护）、DTCP（Digital Transmission Content Protection，数字传输内容保护）等为DRM加密和认证技术的实例。

在DVD等规模生产的存储媒体中，如图3所示进行著作权保护。图3是CPRM方式的拷贝控制案例。控制系统的核心课题是内容分发、媒体、终端设备等企业之间达成一致的加密方式和解密钥匙键管理、设备间的相互认证。以下各节就CSS、CPPM、CPRM及DTCP进行概要阐述。

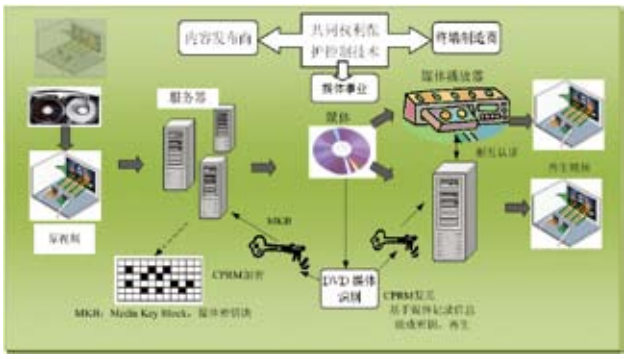

图3 DVD媒体著作权保护处理概要

2.2 DVD的CSS

DVD1996年出现，它不仅是视频的专用盘，也是可处理大容量数字数据的主流存储媒体。1996年，DVD业界成立了内容保护工作组CPTWG（Copy Protection Technical Working Group，拷贝防护技术工作组）。CPTWG决定在以DVD内容保护为目的DRM方面采用CSS 40bit编码。它的机制是在内容认证（盘片内容加密）和设备认证、PC上，进一步结合总线认证的方式。内容认证是加密内容复原时所必须的解码密钥在第三方机构管理下、发布许可的方式，设备认证是采用被授予的密钥进行解码，总线认证是通过PC总线进行DVD驱动器和设备驱动器及MPEG解码器之间相互认证的方式。这种CSS方式基于内容加密，是将DRM技术应用于规模化生产媒体上的先行尝试。

1999年，发生了CSS的密钥（解密盘片钥匙）被第三方破解、破解方式被公布于网上的事件，造成了DVD业界的困惑。这一事件也引发了提高DRM系统安全性的争论。历经了这一被破解事件，CSS方式短期之内就把其主角地位让给了其他方式。

2.3 CPPM/CPRM

作为可刻录型DVD的DRM，有CPRM/CPPM加密系统，基本为上述CSS方式的改良。CPRM适用于可刻录型DVD（DVD-RAM、DVD-R等）、CPPM适用于刻录完成的再生专用DVD的DRM。CPRM和CPPM共通采用C2（Cryptomeria Cipher）密码。C2的钥匙键长为56bit，为64bit的块（Block）加密方式。

CPPM、CPRM钥匙键管理技术采用因播放器而异的设备键，基于MKB（Media Key Block，媒体密钥块）处理，生成媒体固有的56bit媒体钥匙键的方式。CPPM中，利用预先保密分配的设备钥匙键，处理MKB，生成媒体钥匙键（图4），MKB处理在本来应当保密的设备键一旦被公开时，就将再生设备无效化。也就是说，对已经公开钥匙键，变更为不能复原的MKB，持续DVD的生产，其后的DVD就不能再生。所以，内容被再度保护。实际DVD媒体中记录内容管理信息如图5所示。图5的CPPM利用设备键、MKB、Album ID（专辑ID）3种信息，CPRM利用设备键、MKB、媒体ID、加密标题（title）键4类信息。两种盘片的信息记录场所也相同，CPRM的加密标题键被记录在记录区域。

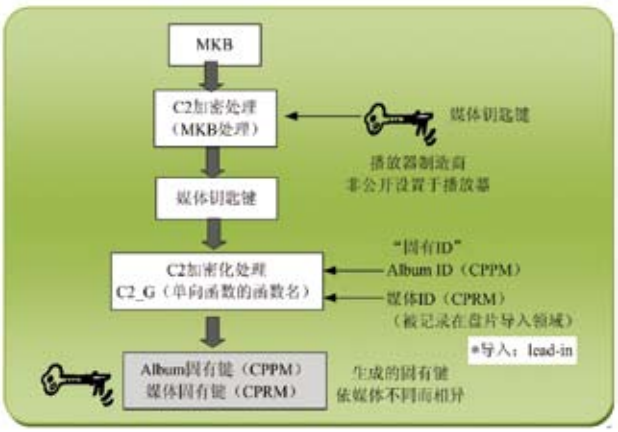

图4 基于MKB的CPPM/CPRM的钥匙键管理方法

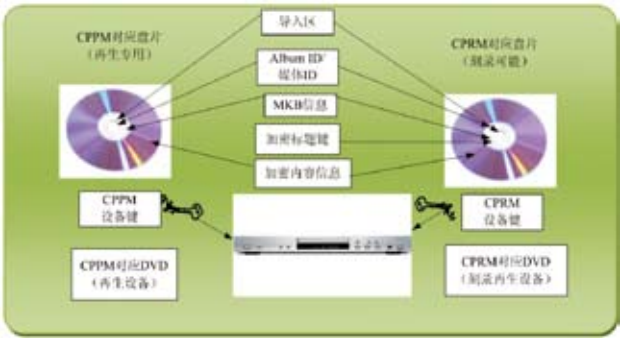

图5 CPPM/CPRM的内容管理信息记录区域

MKB是认证机构管理生成的钥匙键管理信息，数据量最大为3MByte，如图5所示，它被记录在DVD内容管理信息区域。MKB本来是保密、不应公开的设备键，当因某种原因被披露之际，即刻写入无效的播放器信息，其后被记录的刻录完成设备就不可再生。

CPPM中，利用设备键通过C2加密解码MKB信息，得到结果采用album ID进行C2加密处理，内容加密，得到解码键。MKB由专门认证机构提供，记录在图5的数据区域（导入的外栏）。Album ID基于每张DVD，著作权持有者按照规定进行设定，记录在导入区域。

CPRM中，用设备键、C2加密处理MKB，得到的结果进一步用媒体ID来进行C2加密处理，利用其结果，依据title加密被自动设定的title键及解码。与CPPM同样，即使初期设定的MKB被不同的设备键C2加密处理，也可得到同一媒体键。

与CPPM同样，在CPRM中，MKB信息被记录在DVD内侧的导入区域。媒体ID依据规则，盘片制造者

对每张盘片记录不同数据。被加密title键被记录在盘片的数据区域。图4表示了以上钥匙键管理信息的处理流程。

CPPM/CPRM中，MKB是许可管理控制信息源，对无许可的设备具有无效化的功能。

2.4 通用存储媒体的DRM

在通用存储设备中，保存数字数据的存储设备正在普及。存储设备便于数据保存、传输，作为简易的数据传输设备，急速渗透于PC用户为中心的利用群体之中，特别是SD卡及USB类型的存储容量达到了GByte的数量级，与磁带及盘片媒体匹配的记录容量，应用范围进一步扩大。由此产生了利用存储媒体记录视频及音乐等内容的应用，像DVD那样的预录制商品成为可能。但是，由于这类存储设备的价格与内容价值对比不可忽视，直接将内容记录到存储设备，作为录制完成的商品形态，还没有得到普及。

图6显示了SD卡（full规范）的存储图（Map）。这一非强制（option）规格已经考虑到了未来的扩展，在一部分的通用存储设备中，实现了著作权管理保护的机制。另外，目前普及的SD卡具备了著作权保护管理机制（CPRM），也与著作权保护标准对应。

保密区域是存储每张卡介质固有键的区域，拒绝来自主设备（Host）的访问及篡改。系统区域是读出专用的信息存储区，储存进行加密处理的MKB。保护区域是认证设备可访问的信息存储区，只有用户区域是可利用的存储区。记录媒体固有的媒体ID在记录介质的不可写入替代区域记录媒体信息，基于媒体ID获得被计算出的媒体固有键，用媒体固有键对内容进行C2加密处理后记录。媒体ID掌控在管理机构之下，以确保其唯一性。

2.5 SD卡的CPRM

图7为SD卡著作权保护方式的说明图。图7的应用场景为通过网络下载内容的案例，显示了CPRM的机制。内容通过网络被下载到PC终端的HD（Hard Disk，硬盘）上，发布的内容通常进行了加密，这是CPRM控制系统框架的外侧处理。在图7的下部，模式化地显示了被下载内容的流程。也就是说，图7PC中的SD卡遵循CPRM的处理，被相互认证，进入管理流程的框架。

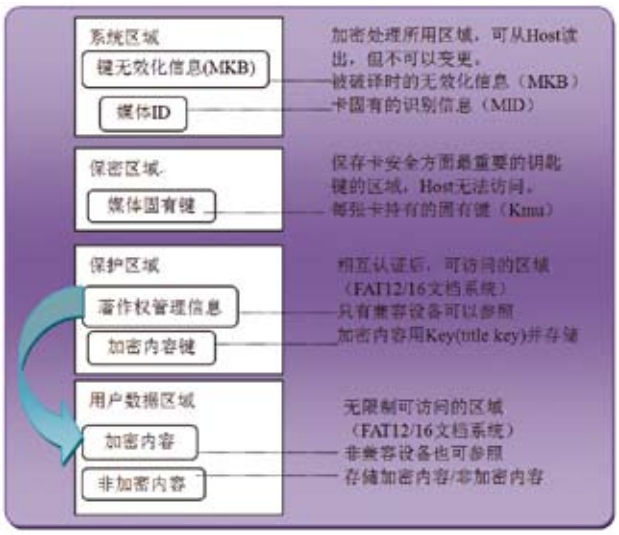

图6 SD卡存储图（Memory Map）

另一方面，PC机下载的内容被C2加密处理，存储保管在SD卡中。SD卡和播放器用CPRM框架相互认证，播放器解码C2加密，再生内容。以下①－④为SD卡的内容获取步骤：

① 在MKB处理中，图7的PC以及播放器被分配了设备键。SD卡中的系统区域记录了MKB。用此设备建处理MKB，可获得媒体键。

② 媒体ID和媒体固有键，由于被记录在SD卡的保密区域，利用步骤①的MKB处理得到的媒体键获取媒体固有键。

③ 利用得到的媒体固有键，进行SD卡和设备的相互认证。

④ 利用得到的媒体固有键，在SD卡保护区，存储加密的标题键和其他内容保护相关信息。另外，用

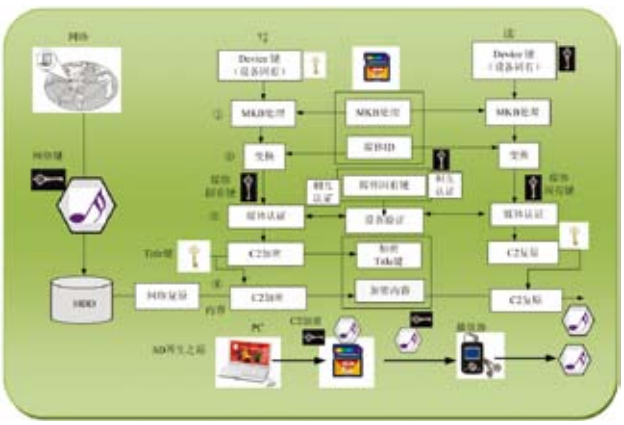

图7 SD卡著作权保护方式

标题键在数据区域存储C2加密的内容。

有关复原处理，在读出（read）侧的设备内进行上述①－④的处理，得到明文（非加密）的内容。这一连的CPRM处理中，上述“相互认证”针对每一处理，重新产生随机数，执行MKB，写入到上述①中的保护区域，因为相互认证的结果，共有之际被变换，用会话键（Session key）加密，所以可以安全地传输。SD卡的用户区域中存储的内容数据可以传送到其他媒体，标题键为每种媒体用固有键加密，为不可复原的机制。

2.6 移动终端的DRM与OMA DRM

2.6.1 OMA DRM v.1.0

移动通讯系统的移动终端是目前生活的必需品，其应用多种多样。手机的功能除双向式电话外，也是通过网络从外部获得必要信息的信息收集工具，利用的基本功能是信息下载，特别是收费内容下载被恒常利用。与PC终端不同，在早期手机受限的信号接收条件下，获得内容的质与量、存储及再利用都是受限的。而进化后的今天，已经达到了PC水平。其结果带来了移动终端的内容下载和其利用方面需要规范和标准，被迫解决国际性的标准化问题。

2002年7月，通讯机构及终端设备制造者共同成立了国际标准化团体OMA（Open Mobile Alliance，开放移动联盟），作为OMA标准，制定了面向简易内容的标准v.1.0，2004年接着推出了较高价内容下载规范v.2.0，图8表示了基于OMA的DRM功能的案例，显示了v.1.0标准的内容，基于WAP（Wireless Application Protocol，无线应用协议）3种内容接收下载方式的应用场景，各自添加了定义、制定了规范。图8中：

① 转发锁定（Forward Lock）（必须），非加密内容转发输出的锁定方式。下载在终端内的内容输出被锁定。也就是说，该类内容被附加了转发锁定的标识信息。接收此信息的手机终端装置启动输出锁定功能，终端的输出信号被禁止。

② 组合发送（Combined Delivery）（可选），内容和其权益管理信息同时下载的方式。接收此信息的手机终端，除输出锁定之外，控制内容的视听条件。例如，可以限制内容的1次视听。

③ 分离发送（Separate Delivery）（可选），内容和其权益管理信息分离下载的方式，内容被加密。内容权益管理信息包含加密的解码信息。内容输出不被锁定，可以存储转发内容。也可以采取另行购入权益控制信息来视听内容的消费模式，这一发布方式也称作“超级分发”。

OMA定义了上述基于移动信息终端的内容下载方式，向各国有关团体发布。

OMA是相对早期实用化DRM系统的典型案例，作为移动终端的DRM雏形，其后的DRM系统中实用案例较多。

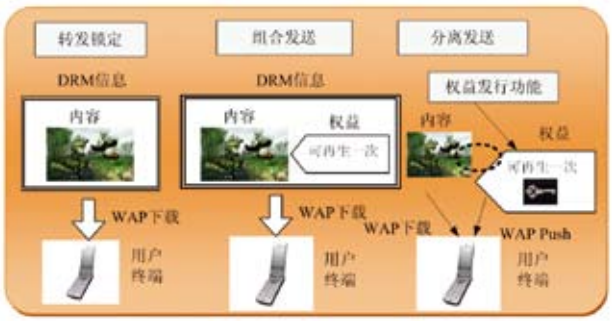

图8 基于OMA DRM v.1.0的DRM功能

2.6.2 OMA DRM v.2.0

OMA DRM v.1.0是以下载铃声等比较廉价内容为目的而进行的条件设定，如图8所示，内容本身不被加密。在此，为了满足在下载音乐及视频等高额内容时，需要更加强化的DRM这一业界的需求，制定了OMA DRM v.2.0。OMA DRM v.2.0是以早期手机服务为前提的v.1.0的扩展，力图支持移动以外的终端，并与其他方式的DRM协作等，进行了功能扩展和安全强化。为此，它与v.1.0不兼容，其主要扩展功能如下：

① 内容权益信息中描述使用控制信息的扩展

② 可与移动终端以外的设备共同使用内容

③ 增加域（domain）功能，可用播放器专用设备再生

④ 预览功能的增加

⑤ 支持流媒体发布的接收

⑥ 可向其他DRM（CPRM等）转移权益信息

上述OMA DRM v.2.0中，内容获取的步骤如图9所示。图9中，内容的下载按照①→③→④的顺序进行。

① 终端A从发行者之处下载加密内容。

② 内容发行者和权益发行者不同时，实行内容键

的共有。

③ 终端A依据内容利用目的获取权益信息和钥匙键。所用协议ROAP（Rights Object Acquisition Protocol，权益对象获取协议）另行规定。

另外，OMA DRM v.2.0中，支持多个终端的内容利用，域以外的终端需要预先取得权益。④内容的转发时也采用ROAP。

基于域功能，可在多个终端之间共有内容。此时，权益发行者持有在域内共有可能的权益信息，域的加入及脱离控制可以通过ROAP消息进行。ROAP中除了终端和权益发行者之间的消息外，提供用PKI（Public Key Infrastructure，公钥基础设施）终端和权益者的相互认证等功能。

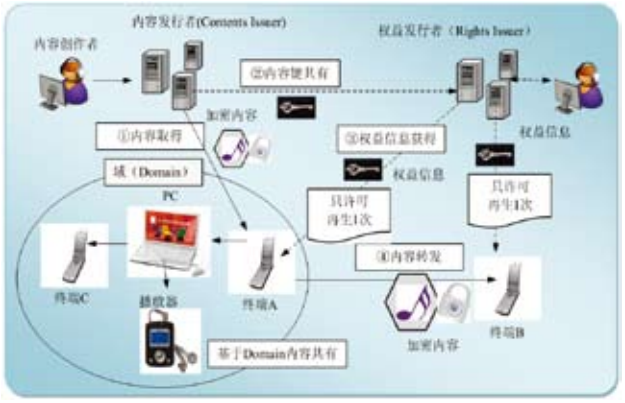

图9 OMA DRM v.2.0的功能

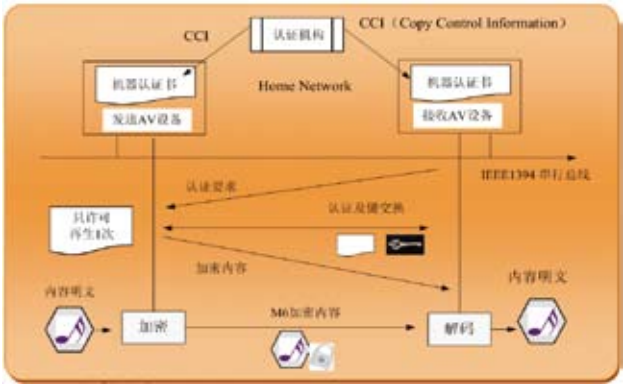

图10 DTCP的系统概念

2.7 传输网络的DRM

高品质AV设备的网络连接标准中，比较有历史的是IEEE1394。IEEE1394开始于1986年IEEE串行总线的标准化工作，通过1994年TA（Trade Association，行业协会）的设立开始致力于普及活动。它已超出了仅为串行总线的功能，与数字设备和数字TV连接构成了网络。基于IEEE1394的数字AV网络上，作为DRM功能的标准有DTCP。DTCP外部认证机构DTLA（Digital Transmission Licensing Administrator，数字传输许可管理者）是具有发行设备证明书的设备之间构成网络，进行键交换，将加密内容在设备间传输的机制。

IEEE1394对应的DTCP，相互认证及键交换作为1394安全命令的扩展，是置于链接层上位层的阶层化方式。1394的内容中，有CCI（Copy Control Information，拷贝控制信息），遵循这一CCI进行内容的交易处理。DTCP的基本原理如图10所示，从信息发送侧到信息接收侧，进行基于CCI的EMI（Encryption Mode Indicator，加密模式指示）的传送、设备间的认证和键交换。这里的认证中，有基于公开键密码的完全认证和基于共通键密码的有限制认证。

AV设备的网络中，存在多个体系，其中，以设备为基础的特性化网络团体是DLNA（Digital Living Network Alliance，数字生活网络联盟）。DLNA中，有多数IT业者的加盟，制定网络构成及传送方式的指导大纲。特点是没有引入新技术的风险，采用现有广泛利用的标准化技术。DLNA的核心是在UPnP（Universal Plug and Play，通用即插即用）中继承了已规定的plug and play的思想，DNLA的DRM定义了连接保护[16]。

3 DRM的标准和互操作[17-19]

DRM从其出现就作为垂直统合的技术而发展，所以，基于标准的互操作及通用规范还谈不上成熟。例如，在手机提供商之间不保证完全互操作，手机音乐播放器各厂家系统间无互操作性。当然从DRM特性上没有必要确保兼容性及互操作性，然而基于用户立场，厂家间的兼容性及提供商间的互操作性，可促进DRM的功能及价格竞争，对系统发展不可欠缺。

在多个国际标准化团体中，也有从标准的概念设计到推进的完整案例。较知名的案例有经过各阶段论证的ISO/IEC（MPEG），以及定义概念化标准模式、决定互操作性和兼容性方面必要技术和术语定义的标准化模式DMP（Digital Media Project，数字媒体计划）案例。除此之外，也有单一公司或多个公司垄断性提出的、但实质为通用的DRM，并正在普及的案例。以

下概要介绍MPEG-21和Coral两个案例。

3.1 MPEG-21

自2000年左右，在ISO/IEC、JTC-1、SC29/GW11（MPEG）有关AV信号符号的标准工作告一段落之后，开始了符号化内容的流通环境相关标准化活动，代表其方向性和应用案例是ISO/IEC2000系列，为内容流通相关的系列标准，目前大部分已经完成了标准化作业。

MPEG-21考虑到数字项的各个服务提供商及终端相异的现状，构建了超越这些差异实现内容自由流通的概念模式，并将遵循这一概念模式的各要素作为组成部分（Part）分别进行标准化。第一阶段完成的MPEG-21如图11所示，其构成复杂，均为内容流通模式中必要的关键技术。

图11的各个Part中与DRM直接关联的是IPMP（Intellectual Property Management and Protection，知识产权的管理和保护）和REL（Rights Expression Language，权益描述语言）。

REL是通用的权益描述语言，描述与许可相关的通用项目，比如“谁发行权益”、“谁以及怎样管理控制什么”等权利许可信息。在内容流通的各个阶段中，需要可适用的语言，作为具有扩展性和阶层化的描述语言，在MPEG中，以XrML（eXtensible rights Markup Language，可扩展权益标记语言）为基础进行描述。值得注意的是，商业目的利用XrML时，需要特定专利权人的许可。

IPMP是与DRM技术直接相关的MPEG-21的一部分。内容流通体系通常依据提供商的业务被垂直统合，像CATV及手机一样，专用终端由提供商提供，所以标准化的实现有难度。目前，不同的提供商之间，或者用户终端DRM之间几乎没有互操作性。垂直统合系统间互操作性也并非必须，为此，创作者需要面向特定提供商提供内容。另外，在提供商新规参与业务方面也有壁垒，内容创作者也同样，需要针对特定的提供商采取不同的应对。

即使如此，假如设计通用的用户终端，还需要安装相当于不同提供商个数的DRM。另外，DRM常常为攻击的对象，必要时需要随时更新。

遵循MPEG标准的压缩视频和音频信号（digital item，数字项）被多重化为基于MPEG-TS（Transport

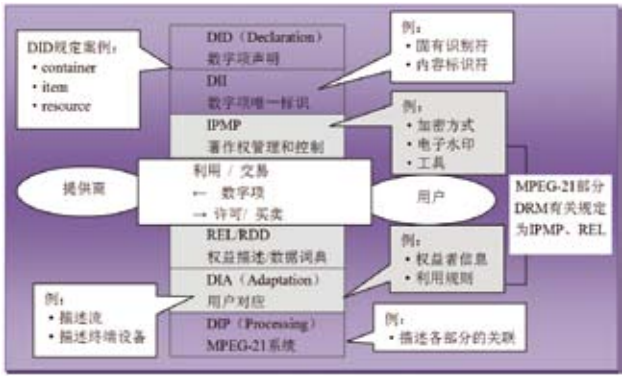

图11 MPEG-21标准的构成要素和其功能*

*通知用户终端多重化传输内容的权益管理控制方式，消息规范和消息解释所必要的管理控制技术。

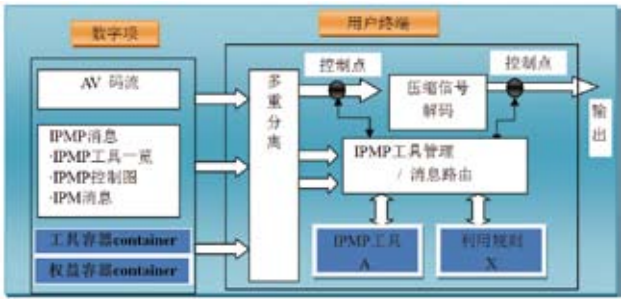

图12 基于MPEG IPMP标准的终端工作说明图*

* IPMP工具决定下载在终端上实施的终端规范。

Stream，传输流）系统码流后传输。系统码流的头部（Head）中有存储码流控制信号的盒（box），可存储IPMP信息。图12中显示了MPEG码流多重传输IPMP消息（Message）的分离、解释、控制工作流的概念图。IPMP标准的特征部分是图12中涂色框部分，IPMP工具没有在终端实施时，外部（例如URL参照加载）也可实施。另外，工具管理把复原部控制点作为动作点，也具有控制解码的输入及输出过程的功能。

基于IPMP的实现，不仅可以实现通用性的解码，也可以具有终端互操作性及提供商间的互操作性，进一步，IPMP工具的更新也可以自动进行。

图13显示了实现具体IPMP的MPEG解码终端。IPMP标准可适用于MPEG-2/4/21。其中，图13显示了适用于MPEG-2的解码器。图13中，被解码的码流被映射为MPEG-TS之后多重传输。其TS头标中的PSI存储部中，存储IPMP信息，转发到解码器，解码器中，解析PSI消息，抽出必要的消息，用控制点进行解码处理的控制。

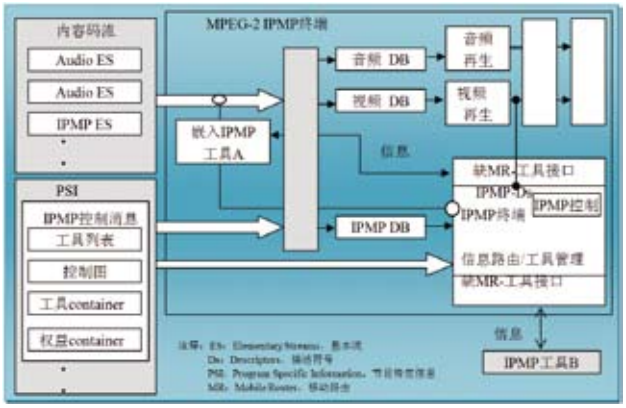

图13 MPEG-2解码器IPMP部分实施案例

3.2 Coral Consortium

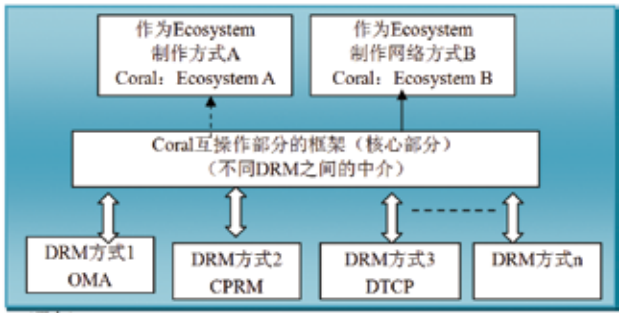

图14 Coral平台*

*特性：Coral国际、公开、自愿参与的标准；Coral不提供DRM系统，而提供框架；
Coral通过domain（home network）保护CE（消费电子）设备；Coral独立处理多个DRM，为兼容性的中介

DRM互操作性在DRM系统相同时可以实现、系统不同的时需要一些方法解决。为了在有多个服务器、域不同情况下，也确保互操作性，需要DRM的主要播放器、具有影响力的系统商之间的合作。系统DRM有关的基础专利权人和有号召力的机构发出了可互操作性平台的倡议，通过这种平台的中介，将第三方的DRM加载于互操作table（表）中，这一DRM体系的方案就是Coral。Coral的成员是依据一定的条件加入联盟，并接受许可。图14表示了Coral联盟提供的平台的概要。其核心部分是进行一种变换处理，通过变换，可实现不同DRM间的共有。Coral的基础是通过称作token的中介标记，统一识别不同的DRM许可。Coral基本架构是采用称作节点（node）的块（block）及设备的集合体进行定义。在此基础上，各节点通过Coral接口可以进行各种信息交换。

也就是说，像被定义的单元系统，也像插件模块一样，可以运作DRM。原来各DRM规范不需要变更，易于参加，要进入了Coral联盟影响力之下，必须得到许可。由于有影响的基础系统事业者及IT行业的参加，所以Coral发展方向受到瞩目。

4 DRM的现状与未来

DRM作为内容流通不可缺少的技术，自早期模式开始一直被屡屡论及。同时也有完全不同立场的意见。近年，国际有影响力的音乐传播事业者发表了“DRM Free”（无DRM限制）音乐传播，在相关业界激起了千层浪。虽说只是一部分事业者，但启动DRM Free的音乐传播，它与过去的商务模式味道稍有不同。以前被特定DRM坚实保护的内容，可以安心地在网络传播，受到了提供商好评。然而，针对希望内容更广泛地传给用户的创作者，以及用户的“只有来自特定DRM事业者的许可设备方能再生内容”的不满声音，很难说DRM技术及系统等受到了创作者及消费者的全面欢迎。另外，加密与破解加密“明争暗斗”，没有停止。

不正当拷贝是社会的恶习，基于用户性恶的说法就失去了大多数善良用户，这一事态从商务整体来看，不得不说是负面因素。个人行为的拷贝任由用户，有关禁止拷贝方式，可以继续探索其他形式的DRM技术。确保用户终端的互操作性及创作者自由至少应当是DRM的目标，这一方面，最近出现了可以期待的态势。

5 结语

DRM的技术开发依然处于发展阶段，今后还会出现对应各种应用的DRM。从DRM技术特性看，系统与商业的一部分直接关联，DRM具有保密性，公开部分的信息有限。在内容流通的价值链中，流通模式的抽象、术语的定义、价值链的定义、继续逻辑验证其流程、资金链的模式等诸多方面，都可以看到标准化的活动。

本文在调研国际标准DRM项目中，面向标准实用案例，以通用存储媒体和手机为中心，概要介绍了目前急速普及的DRM技术。由于版面所限，以及DRM自身的复杂性，本文的介绍与阐述不可能充分，仅供读者参考，并期待DRM意识得到进一步的普及与强化。

参考文献

[1] 安田浩安,小暮拓世. DRMの技术动向[J]. 电子情报通信学会誌,2008,91(3):225-236.
[2] Macrovision [EB/OL]. [2010-10-05]. http://www.rovicorp.com/.
[3] Macrovision [EB/OL]. [2010-10-05]. http://www.worldlingo.com/ma/enwiki/zh_cn/Macrovision/.
[4] 加藤拓. DVD-Audioにおけるコンテンツ保护技术[J]. 东芝レビュー,2001,56(7):54-57.
[5] 加藤拓. コンテンツ保护アーキテクチャ[J]. 东芝レビュー,2003(6):8-11.
[6] 馆林诚. DVD著作权保护技术[J]. 映像情报メディア学会誌,2002(4):550-551.
[7]刘广山. 几种高清光盘的日内容保护系统[J]. 音响技术,2009,7(4):63-65.
[8]范科峰. 数字版权保护领域标准化工作思路[J]. 信息技术和标准化,2008(7):29-32.
[9]谢俊,陈明,李晓明. 流媒体版权管理系统的研究与实践[J]. 计算机应用与软件,2009(7):23-25.
[10] RipGuard-Protecting DVD Content (Rovi, Corporation) [EB/OL]. [2010-10-05]. http://www.rovicorp.com/default.htm.
[11] 魏景芝,杨义先,钮心怡. OMA DRM技术体系研究综述[J]. 电子与信息学报,2008(3):746-751.
[12] 脱立恒,等. 基本OMA DRM的域管理方案研究[J]. 微计算机应用,2010(3):22-29.
[13]Open Mobile Alliance [EB/OL]. [2010-10-05]. http://www.openmobilealliance.org/.
[14] OMA White Paper [R]. The Broadcast Services BOF,2004.
[15] [EB/OL]. http://www.medialab.sonera.fi/workspace/MobileDRMWhitePaper.pdf.
[16] DLNA [EB/OL]. [2010-10-05]. http://www.dlna.org/home.
[17]Rightscom Ltd. The MPEG-21 Rights Expression Language-A White Paper 2003 [R/OL]. [2010-10-05]. http://www.rightscom.com/Portals/0/whitepaper_MPEG21-RELCB.pdf.
[18]Coral consortium [EB/OL]. [2010-10-05]. http://www.coral-interop.org/.
[19] 李颖,郭晓峰,等. 以权益描述语言REL为核心的DRM技术进展研究[J]. 图书情报工作,2008(11):11-15.

作者简介

李颖，博士，信息系统专业。相关研究课题：基于XML的数字出版、基于DOI的文献链接和DRM系统等。通讯地址：北京市海淀区复兴路15号 中国科学技术信息研究所信息技术支持中心 100038。E-mail: liying@istic.ac.cn
白海燕，硕士，中国科学技术信息研究所副研究馆员。通讯地址同上。E-mail: baihy@istic.ac.cn
王莉，硕士，中国科学技术信息研究所高级工程师。通讯地址同上。E-mail: wangli@istic.ac.cn
乔晓东，硕士，中国科学技术信息研究所研究员。研究方向：信息服务和信息资源管理。通讯地址同上。E-mail: qiaox@istic.ac.cn

Technology Trend of Standardized DRM on Streaming Media

Li Ying, Bai Haiyan, Wang Li, Qiao Xiaodong / Institute of Scientific and Technical Information of China, Beijing, 100038

Abstract: DRM is an important technology in content distribution and a mandatory technology to ensure to meet the needs of content creators, providers, users under the current content circulation. The application of DRM technology prevents users accessing contents. But with continuing occurrences of illegal copies of contents, providers are forced to strengthen implementation of DRM technology according to a variety of cases. This article describes the earliest DRM, overviews DRM technology by the DVD business; describes rapid spread of standardized DRM in mobile phones, OMA DRM; on storage media DRM, gives CPRM for SD Card as an example. On the current international standardization activities, gives MPED-21and explains the IPMP technology; as de facto standard in industry-oriented DRM, gives Coral, explains its main points; finally, gives current situation and trends of DRM.

Keywords: DRM, DVD, Content distribution, Encryption, MPEG-21, REL, CPRM/CPPM, IPMP, Coral

（收稿日期：2010-10-07）