# 数字版权管理中数字权利使用控制研究进展

张志勇[1,2] 牛丹梅[1]
(河南科技大学电子信息工程学院 洛阳 471003)[1] (西安交通大学管理学院 西安 710049)[2]

**摘 要** 数字版权管理(Digital Rights Management,DRM)技术是关系到数字内容产业良性、健康发展的关键技术,其中的数字权利使用控制机制能够保障终端用户合法授权地使用数字内容,以及转移分享相应的权利。在分析预防式和反应式两条DRM研究技术路线的基础上,综述了一般意义的DRM系统和移动DRM中数字权利描述语言与使用控制、权利委托与转移、数字权利可信执行与安全终端平台等方面的国内外研究现状和发展动态,分析、比较了代表性的权利描述语言及形式化使用控制模型。最后指出了数字权利使用控制中存在的开放问题和挑战。

**关键词** 数字版权管理,使用控制,权利描述语言,安全模型,可信计算
**中图法分类号** TP309 **文献标识码** A

## Advances on Digital Rights Usage Control in Digital Rights Management

ZHANG Zhi-yong[1,2] NIU Dan-mei[1]
(Electronic Information Engineering College, Henan University of Science and Technology, Luoyang 471003, China)[1]
(School of Management, Xi'an Jiaotong University, Xi' an 710049, China)[2]

**Abstract** Digital Rights Management(DRM) technology is crucial to a prosperous and meaningful development of digital contents industry, thereinto digital rights usage control mechanisms can guarantee that end users access to contents, transfer and share the corresponding rights by an authorized model. Based on an analysis of preventive and reactive DRM research roadmaps, a survey of research advances and progresses was made on Rights Expression Languages (REL) and usage control, rights delegation and transferring, trusted rights execution and secure terminal platform regarding a generic DRM system and Mobile DRM, as well as representative RELs and formalized usage control models were analyzed and compared. Finally, some open issues and challenges on digital rights usage control were addressed.

**Keywords** Digital rights management, Usage control, Rights expression languages, Security model, Trusted computing

## 1 引言

随着通信网络技术与信息技术的飞速发展,下一代高速宽带互联网络以及3G、4G等无线移动通信网络正逐渐从研究试验阶段向大范围部属和应用阶段迈进,用户通过各种接入方式能够更加便利地使用网络资源,即可以在任何时间、任何地点得到所需数字信息和服务。在如此发展态势下,由于数字内容(包括电子书、数字图像、音视频内容、Java类移动应用软件等)具有无损复制、易于分发等重要特性,目前随意批量复制受知识产权法案保护的数字内容产品,并将其通过各类通信网络载体进行非授权分发、传播和滥用的现象普遍存在,由此所引发的一系列数字版权问题日益严峻。数字侵权行为对国家、企事业单位以及个人的数字内容(资产)管理及数字内容产业的良性发展带来严重伤害,同时侵犯了版权所有者的基本权益,挫伤了内容原作者的创作积极性。更为严重的是,随着P2P网络的兴起,近年来大量涌现的用于多媒体内容分享的社交网络(Social Network)服务工具,如YouTube, Myspace, Tudou等,使得用户间可基于宽带互联网和无线移动通信网络搭建虚拟社会化网络,从而更加便捷地传递、分享和使用音视频及电子书等数字内容格式。然而,对于受版权保护的有价数字内容,随意地分享和传播给整个社会文化、经济发展所造成的严重后果又将是不言而喻的。

数字版权管理(Digital Rights Management, DRM)是关系到数字内容产业良性、健康发展的关键问题,也是多学科的研究领域,涉及到DRM安全技术、数字版权法案及其技术实现[1]、DRM经济学[2]、商业模型[3]以及DRM定价(Pricing)策略[4,5]等。从DRM技术上,近年来出现的移动DRM(Mobile DRM)研究,也是面向移动通信网络环境解决受版权保护的数字内容的产生、在移动网络及应用中的分发与传输,以及在移动终端上的安全存储和使用控制等问题,如Mobile IPTV DRM[6],以及个人数字内容及许可权利的转移[7]等。自2007年起,北美和欧盟国家的基于DRM的移动数字内容服务、受版权保护的P2P网络、家庭娱乐网络以及IPTV等同时被列为4类DRM关键应用领域[8]。

到稿日期:2010-04-12 返修日期:2010-08-24 本文受国家自然科学基金项目(61003234,60803150),中国博士后科学基金面上项目(20100471611),河南省重点科技攻关项目(092102210295),河南科技大学科学研究青年基金项目(2008QN010)资助。
**张志勇**(1975-),男,博士后,副教授,CCF高级会员,主要研究方向为数字版权管理、访问控制与可信计算,E-mail:xidianzzy@126.com;**牛丹梅**(1979-),女,硕士,讲师,主要研究方向为信息系统安全与DRM。

## 2 DRM 技术路线

近年来的 DRM 研究有两条技术路线：其一是预防式(Preventive)DRM 技术，主要基于密码学理论与使用控制(Usage Control)技术，研究数字内容的加密保护、安全分发、安全存储、使用控制等；其二是反应式(Reactive)DRM 技术，主要针对用户侵犯数字版权的行为，通过数字水印与生物特征跟踪、鉴别数字内容的版权等。上述两条技术路线主要以内容提供商或数字权利提供方为中心研究数字内容的安全保护和版权管理，从而实现 DRM 系统的核心功能完备性、增强安全性以及基础的互操作性等。这些研究开展得较早，研究工作比较广泛和深入，也较为成熟。

数字版权管理涉及数字内容及其权利从生成、分发、传输到使用和传播的全生命周期内存在的内容保护、使用控制和版权追踪等问题[9,10]。在预防式(Preventive)DRM 技术中，主要基于密码学理论与使用控制(Usage Control)技术，研究数字内容的安全分发、安全存储、授权使用以及知识产权(IP)保护[11]。其中，数字内容保护主要涉及广播加密[12-14]、密钥管理与秘密共享[15]、数字权利使用控制则涵盖数字权利语言描述[16]、DRM 使用控制[17]以及用户终端可信计算环境[18,19]、内容使用策略的可信执行[20]等问题。对于反应式(Reactive)DRM 技术，主要针对用户侵犯数字版权的行为，通过数字水印来跟踪、鉴别数字内容的版权[21]等，包括研究数字水印鲁棒性和认证方案的改进[22,23]、基于 EXIF(EXchangeable Image File) 格式元数据的数字图像水印[24]、硬件辅助多媒体水印[25]、适合于多用户、多许可的数字水印算法[26]以及基于生物特征的侵权跟踪与认证[27]、数字媒体保护[28]和叛逆者追踪(Traitor Tracing)[29]等问题。随着 DRM 技术的深入研究和工业界相关标准与规范的建立，近年来 DRM 技术也涌现出诸多应用领域和实例，如面向电子商务的 DRM 系统[30]、面向企业环境的 E-DRM[31]以及端到端的 DRM(E2E DRM)安全框架[32]等。

此外，鉴于 DRM 研究的基础背景是一个完整的数字内容价值链生态系统(DRM Ecosystem)，包含安全、信任和风险等诸多方面，并支撑内容获取和内容分享两个一般应用场景(如图 1 所示)，我们针对 DRM 安全策略选取[33,34,58]和数字内容/权利分享场景下 DRM 安全策略风险评估[35,84]等问题，提出了以安全-效用(Security-Utility)为中心的 DRM 多方信任框架，并通过建立 DRM 可组合安全策略的效用分析理论及博弈论选取方法，使得 DRM Ecosystem 多方能够合理地选取和部署效用最优的安全策略。

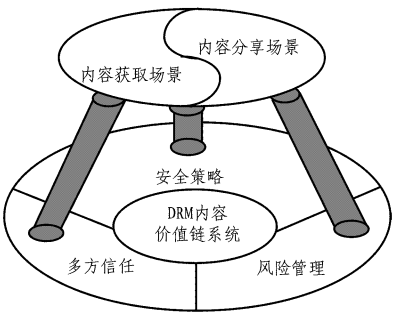


图 1 DRM 内容价值链系统及其应用场景

## 3 数字权利描述语言与使用控制

### 3.1 DRM REL

数字权利描述语言(Rights Expression Language，REL)主要用来面向权利提供方(如 RI 等)规范和描述用户对数字内容的授权使用策略，其中主要包括使用权限、条件和约束规则[36,37]。现有代表性的 REL，例如 XrML[38]、ODRL[39]和 MPEG-21[40]，主要是通过引入新的 XML 标签(Tag)来实现。XML 作为 REL 的源语言，具有灵活性、机器可理解性、用户可读性以及较强的描述能力。作为权利描述语言，语义的无二义性是本质问题。如何基于 REL 正确地描述被购买内容的使用权利，并确保权利之间无冲突，是值得考虑的。因此，近年来 REL 研究工作也集中在形式化的 REL 描述，例如 XrML 和 ODRL 的形式化被提出[41,42]，ISO MPEG-21 REL 标准中也实现了形式化描述，从而保障语义的正确性和无二义性[40]。Jamkhedkar 则提出了一个数字权利的形式化核心模型作为 REL 的基础，并给出与 CC(Creative Commons) License，XrML，ODRL 3 种 REL 的映射关系[43]。此外，文献[44]针对 OMA REL 缺少形式化语义的不足，采用可执行的代数描述语言 CafeOBJ 给出了 OMA REL 的形式化语法，进一步的目标是实现自动化工具和许可集的行为检测。

基于逻辑的形式化方法作为一个简单的基础方法，被用于完成 REL 形式化和推理工作，实现较强的权利管理描述功能性。Llic 是一个精确且严格的 REL 语言，提供了许可相关的多种性质，并能够描述内容消费者动作(Action)，这些动作在一定的环境和前提条件下能够被授权或禁止[45]。Halpern 采用一阶逻辑，提出了一个更有表达性、语义和语法更加清晰和准确的形式化语言 Lithium，用于描述使用控制策略，并最终给出了 XrML，ODRL 和 Lithium 间的映射翻译[46]。

Chong 等人[47]提出了现有基于 XML 的权利描述语言所存在的主要缺陷，例如复杂和难于理解的语法、缺少形式化的语义等等，然后分析了 REL 中的基本组件和相互关系，并提出了一种形式化的 REL，LicenseScript。它是一种以许可为中心、基于多集合重写(Multiset Rewriting)特性和纯 Prolog 编程的逻辑语言，不仅能够捕捉到许可授权的动态特征，也可以用来描述许可的静态条件等，从而提供一组精确的、显式的形式化授权语义集。

基于内容价值链的全生命周期和版权规则的考虑，García 提出了一个基于本体(Ontology)和规则(Rule)的价值链动态特征建模方法，其中包括基于 Ontology X 的创建模型(Creation Model)和权利模型(Rights Model)，以及系统的形式化描述，从而有助于数字版权保护系统的开发[48,49]。Sheppard 探讨了 XML-REL 与虚拟机程序的翻译问题，提出了 REC(Rights Expression Compiler)概念，并将其用于经典 REL 语义的形式化定义和一致性准确的翻译[50]。关于数字权利的验证，Sachana 实现了一个有效的 Lincese 验证方法[51,52]。

关于 REL 设计准则，Jamkhedkar 等人提出了一个 DRM 开放层次框架和现有 REL 存在的问题，归纳总结了满足各层次互操作性的 REL 设计准则，最终给出一个满足该准则的原型系统实现[53]。Wang 等人[54]针对现有的 REL 和访问控制

模型作了详细比较，提出了一系列的 REL 设计准则，其中包括语法与语义的无二义性，以及支持商业模型的较强的描述能力。按照所提出的准则，REL 形式化方法对于数字权利描述是至关重要的。此外，Rafi 在 MPEG-21 REL 中引入“角色”的概念，增强了原有语言的表达性[55]。文献[56]中也给出了在一个在线音视频网站的 DRM 系统中基于角色的访问控制(RBAC)，此外强制访问控制(MAC)在 DRM 领域也可以得以应用[57]。

表 1 给出了代表性的 REL 及形式化使用控制模型在数字权利使用控制中典型特性的比较。符号“○”，“×”和“—”分别表示具备、不具备或不适合某特性。

表 1　数字权利描述语言与形式化模型的使用控制特性比较

| 数字权利使用控制 | 规范的数字权利描述语言 | | | | 形式化的 REL 与使用控制模型 | | | |
|---|---|---|---|---|---|---|---|---|
| | XrML | ODRL | OMA | MPEG-21 | License-Script | LiREL | $UCON_{ABC}$ | $UCON_D$ |
| “否定”权利 | — | ○ | — | — | — | × | × | × |
| 约束与义务 | ○ | ○ | × | × | ○ | ○ | ○ | ○ |
| 版权实现 | × | × | × | — | ○ | × | — | × |
| 权利管理 | × | × | × | × | ○ | — | ○ | ○ |
| 形式化方法 | ○ | ○ | — | 集合描述 | 多集合重写 Prolog 逻辑 | 集合描述 | 集合描述一阶逻辑 | 集合描述一阶逻辑 |
| 权利可转移 | ○ | ○ | × | ○ | ○ | ○ | × | ○ |

### 3.2　DRM 授权管理与使用控制

随着商业模型的扩充和新的数字权利的提出，现有的 REL 描述功能及语义在不断地扩展、完善并且被精确地详细地描述。但是，Jamkhedkar 等人[16]对此提出了一个关键问题——“REL 膨胀”。由于现有的 REL 针对一些具体的 DRM 应用场景，并且不能合理、有效地描述权利管理，因此新的 DRM 商业模型特征被不断引入 REL，造成了 REL 核心语义被不断扩展，以支持新的商业模型中的权利管理需求。这个问题的出现主要是由于缺少权利管理和权利描述的分离，导致 REL 变得复杂，难于理解和操作。为此，在层次性 DRM 系统[59]中曾提出一种基于核心语义描述和权利管理分离的 DRM 服务框架。该框架具有两个优势：一是在不改变内核语义的基础上通过引入新的协议来实现扩展权利管理的能力；二是用户的终端设备仅仅需要支持简单的核心语义，而复杂的权利管理功能被放置在服务器端处理。然而，作为一个总体概念模型，它并未考虑授权使用控制中的可信性问题；其次，针对数字权利管理、许可分享、用户认证等关键技术，目前仍缺少具体的实现机制和安全协议。

值得注意的是，最近由有关 REL 和 DRM 权利(许可)管理的研究得出，数字权利使用也可以被看作内容分发、传播和使用过程中一种特殊的、持续的访问控制机制。这明显不同于传统的访问控制方法，因为传统的访问控制机制主要集中在实体授权和资源访问前的合法权利判定，例如自主访问控制 DAC、强制访问控制 MAC 和基于角色的访问控制 RBAC 等 3 种重要的访问控制策略及相关模型。Arnab 等人[60]提出了用于 DRM 应用、无控制边界的持续访问控制方法和 Licensing REL(简称 LiREL)。在 LiREL 中，重点描述内容(权利)提供商和购买者之间的合同和契约性质，并形式化了 DRM 价值链中各方所具有的约束、义务和约定等特征，同时定义了包含有权利委托性质的访问控制规则和策略。

Usage Control(简称 UCON)是一种可用于 DRM 应用的基础的访问控制框架[61]，它融合了授权(Authorization)、义务(oBligation)和条件(Condition)等 3 个基本组件，也被称为 UCONABC。该框架在 Sandhu 等人的研究下被看作下一代访问控制架构，具有持续的访问控制特征，并且易于描述资源使用过程中实体属性的动态变化。在 UCONABC 中，属性的变化通常体现在权利实施前、后以及作用过程中，同时结合 3 个基本组件，构成了 UCON 模型家族，如图 2 所示。值得注意的是，该框架能够较好地实现 3 大访问控制策略，并已得到形式化的证明。Pretschner 则给出了使用控制在可应用性、实现及非功能性质等 3 方面的系统分类[17]。文献[62]中提到权利管理和内容保护成为目前 DRM 系统的关键脆弱点，为此提出了一个 4 层安全模型，包括信任层、权利管理层、权利实施层和内容保护层等。Nair 和 Andrew S. Tanenbaum 等人基于 $UCON_{ABC}$ 提出了一个支持 DRM 的 Trishul-UCON 框架，并实现了它基于 JVM 中间件的跨应用 DRM 策略[63]。

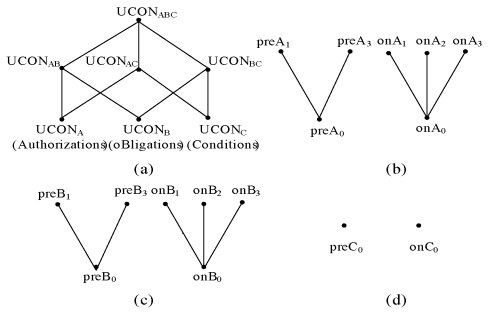


图 2　UCON 模型家族

在 DRM 使用控制的时空扩展方面，文献[64]在传统的权利使用控制中增加了“位置约束”，用于实现移动终端设备随位置动态变化而实施的敏感资源访问控制。Muhlbauer 利用 MPEG-21 REL 和 IPMP 组件，联合支持 HTTP-HELD 协议的可信位置信息服务器，实现了非瞬时(Non-instantaneous)播放使用控制，还对非瞬时访问控制系统和技术进行了有效分类。马兆丰、杨义先和钮心忻等人也提出了支持时间-空间约束特征的 Lincese 可信分发安全管理及协议 CPSec DRM，它可以实现在线和离线两种模式的版权二次分发[65]。于爱民和冯登国等人提出了基于 TPM 的 DRM 框架 TB-DRM，用于保障数字许可在全生命周期内的安全性和新鲜性[19]。

## 4　数字权利分享与转移

合法地分享所购买的数字内容及数字权利，有助于一个完整的 DRM 系统及其价值链的延伸和扩展。提出或扩展一个 REL，使得它能够描述权利的转移/委托等功能性，是必要的。目前，OMA 在其 REL 规范中并没有给出与数字权利转移相关的形式化的语法/语义描述，使得采用 OMA DRM 规范的系统难于实现内容分享机制，以及无法描述数字转移相关的前提条件、约束等特征[66]。虽然其他 REL，例如 ODRL 和 XrML 能够描述一些可转移权利，比如 ODRL 中的 Sell，Lend，Give 等，以及 XrML 中的 Delegation，但这些规范只能粗粒度地描述权利转移/委托。在一般的商业模型中，更需要一种细粒度的权利描述语言。我们针对面向 DRM 应用的访

问控制框架 Usage Control 提出了一种具有委托(转授权)基本特征、形式化的 $UCON_D$ 模型及其基于委托证书 DC(Delegation Certificate)的实现,该模型是对 $UCON_{ABC}$ 框架在委托机制上的必要补充,从而进一步完善、丰富了 Ravi Sandhu 提出的 $UCON_{ABC}$ 框架[67]。此外,基于 $UCON_D$ 模型,我们提出了一种细粒度的 DRM 数字权利转移安全策略,并结合可信计算为数字权利分享提出了新的细粒度权利转移安全策略[68],以及可信分发与执行[69]等。其中,基于可扩展的 ODRL 语言对数字权利对象及其可转移权利的描述如图 3 和图 4 所示。

```
<o-ex:rights
  xmlns:delegate ="http://www.mispb.com/rbac/transfer-dd">
  <o-ex:context>
    <o-dd:uid>RightsObjectID</o-dd:uid>
  </o-ex:context>
  <o-ex:agreement>
    <o-ex:asset>
      <o-ex:context>
        <o-dd:uid>ContentID</o-dd:uid>
      </o-ex:context>
    </o-ex:asset>
  <o-ex:permission>
    <o-dd:basicPermission>
      <o-ex:constraint>
        count_constraint OR datatime _constraint OR...
      </o-ex:constraint>
    </o-dd:basicPermission>
    <transfer:transferPermission>
      <o-dd:basicPermission>
        <o-ex:permissionConstraint>
          count_constraint OR datatime _constraint OR...
        </o-ex:permissionConstraint>
        <o-ex:transferConstraint>
          transferDepth OR transferCardinality OR
          transferTimelimit
        </o-ex:transferConstraint>
      </o-dd:basicPermission/>
    </transfer:transferPermission>
  </o-ex:permission>
</o-ex:agreement>
</o-ex:rights>
```

图 3　基于扩展 ODRL 的权利对象描述

```
<o-ex:rights
   xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
   xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
   xmlns:delegate ="http://www.mispb.com/rbac/transfer-dd">
<o-ex:context>
   <o-dd:uid>TranferableRightsObjectID</o-dd:uid>
</o-ex:context>
<o-ex:agreement>
   <o-ex:asset>
     <o-ex:context>
       <o-dd:uid>ContentID</o-dd:uid>
     </o-ex:context>
   </o-ex:asset>
<o-ex:permission>
   <o-dd:basicPermission_1>
     <o-ex:constraint>
       <o-dd:count>count_constraint_1</o-dd:count>
       <o-dd:datetime>datatime_constraint _1</o-dd:datetime>
         …
     </o-ex:constraint>
   </o-dd:basicPermission_1>
   <o-dd:basicPermission_2>
       basicPermisson_2 constraint
   </o-dd:basicPermission_2>
   <transfer:transferPermission>
       transferPermisson_1
   </transfer:transferPermission>
</o-ex:permission>
</o-ex:agreement>
</o-ex:rights>
```

图 4　基于扩展 ODRL 的可转移权利对象描述

在数字内容(权利)共享的实现机制方面,由于 OMA RI 在为用户许可授权时,通常采用内容-许可-设备(用户)绑定的方式,使得数字内容的共享使用受到了较强的限制。Digital Video Broadcasting 联盟最初为了便于内容在不同设备上的共享使用,首先提出了“授权域(Authorized Domain)”概念[70],随后 OMA DRM 方案也在多个版本中使用了这一概念[71],并实现了 RI 对域的统一管理,包括创建和撤销域、用户设备的加入与退出域等,域内设备之间可以共享内容和数字权利,但由此增加了 RI 的负担,并成为授权域的瓶颈;此后,OMA DRM 在后续版本中通过引入域管理器对此进行了改进。目前,DRM 数字内容共享研究侧重于家庭网络域[72]和个人娱乐域(Personal Entertainment Domain)[73]。文献[74]给出了一个 DRM 授权域的安全架构及其安全协议,但它不支持 RO 的转移和内容共享;为此,文献[72]在家庭网络域 DRM 中进行了改进,在引入本地域管理器(Local Domain Manager)的基础上,代替 RI 实施域成员设备的许可分发和共享,同时通过被委托 RO(Delegated RO)和代理证书(Proxy Certificate)实现了数字权利委托与共享。然而 LDS 的引入增加了系统开销和被攻击的对象,并且数字内容的共享机制仅限于家庭网络。如何将其推广至广域网络,需要做进一步的考虑。

Barhoush 等人[75]提出了数字内容安全多播的 11 项安全需求,并针对这些需求,详细分析了现有代表性的 DRM 商用系统所存在的相关特征和不足,以及改进的方向。文献[76]为改进现有的数字权利分发过程中许可配置受限的问题,给出了一个 OPA(Onion Policy Administration) DRM 模型,该模型使内容创建者和分发者都可以配置许可,并且具有可追踪性,有效地提高了数字权利分享的效率和安全性。Bhatt 等人[7]在 Motorola E680i 智能移动终端上实现了个人化 DRM (Personal DRM)原型系统,使终端用户可自主地设置数字许可(License),并且灵活地在设备间转移许可,达到保护个人数字内容的目标。此外,Lee 提出了一个基于设备间内容使用时间的二次分发方案及其安全协议,它是对数字权利中时间要素分享的一次有益尝试,拓宽了数字权利分享研究的视野[77]。冯雪和汤帜等人提出了一个 DRM 许可分享方案,该方案基于遍历加密(Ergodic Encryption)和机器认证技术的许可获取与分享机制,减轻了传统依赖授权域的成本负担[78]。

## 5　安全终端平台与数字权利可信执行

用户终端的安全平台是保障有价的数字内容按照内容提供商/版权所有者所描述的数字权利安全、可控、可信赖执行的基础,数字权利的可信执行将直接影响到 DRM Ecosystem 信任关系的建立。随着近年来可信计算技术的发展,学术界已开始研究它在 DRM 领域的基础应用。基于可信计算中的关键技术,如远程证明、Seal 技术等,以及完整的可信终端平台体系,研究 DRM 内容使用策略的可信分发、安全存储和 DRM Controller 可信执行。文献[79]综述性地探讨了可信计算的进展及其基本特征,并阐述了基于可信计算技术的可信移动 DRM 健壮性实现,主要包括设备密钥的安全存储、基于 Seal 的内容分发与访问等。文献[80]中较为详细地阐述了基于 TCG 规范的移动终端平台架构,指出了移动终端平台所需的基本 TPM 指令和函数,并从终端保护、移动代码安全等角度讨论了移动代码授权问题,以及基于远程证明的移动终端平台验证和 DRM 内容保护。文献[81]也给出了一个概念性的可信移动平台体系架构。文献[82]从 DRM Controller 平台环境的角度,探讨了现有的 OS 不能有效地支持可信计算中的远程证明和 Seal 技术,目前开放终端平台上的主流 OS 及其访问控制模型无法保护对解密后数字内容的直接访问和输出,并探讨了许可策略的可信实施[83],以及需进一步构建基于虚拟机技术的隔离执行环境、实施参考监控器(Reference Monitor)概念并加强强制访问控制模型的实现等。

关于可信终端计算环境,除了 TCG 不断完善的可信计算总体框架和最佳设计准则之外[85,86],还有欧洲开放可信计算(Open TC)组织和我国可信计算联盟等所提出的可信 PC 体系架构,以及一系列的面向可信移动终端体系的标准和规范。NTT DoCoMo,IBM 和 Intel 于 2004 年底提出的可信移动平

台规范(包括软硬件和协议3个子规范)是最早的移动终端可信性研究的参考规范[87]。目前,TCG移动电话工作组(MPWG)在移动可信模块MTM(Mobile Trusted Module)规范[88]和可信移动参考架构[89]中分别定义和规范适用于移动终端平台和应用环境的可信模块指令集和数据结构,以及基于MTM在移动终端建立信任根。此外,TCG MPWG还提出了面向可信移动终端基于域隔离机制的应用引擎执行环境,从而提高引擎执行和数据访问的安全性[89]。此外,TCG MPWG在用例分析中也明确表示支持健壮性DRM系统实现[90]。由国际知名移动运营商,如AT&T,Hutchison 3G,T-Mobile等联合发起的开放移动终端平台(Open Mobile Terminal Platform,简称OMTP)论坛,目前也开始关注于可信的移动终端平台环境和移动应用(Mobile Application)类数字内容的安全等领域[91]。通过文献[92]中提出的一个基于TPM和具有隐私保护的SITDRM实现可信终端的方案看出,DRM与可信计算技术是融合的、互补的。结合Xen虚拟技术及架构,通过支持第三方远程证明协议AP2RA,可实现对用户终端平台关键部件(如DRM控制器等)的远程验证,确保数字权利的可信执行[69]。

**结束语** 现有DRM研究主要有两条互补的技术路线:其一主要是从数字媒体内容的密码学安全保护与数字权利使用控制的角度展开研究,其二是从数字内容侵权的追踪、数字水印鉴别与认定等进行研究。然而,近年来出现了从DRM Ecosystem视角对数字版权进行管理的研究工作。随着DRM Ecosystem的发展和日臻完善,数字内容/权利分享成为日益凸现的一个基本需求[93]。因此,数字权利使用控制目前存在以下开放问题与挑战:

(1)数字权利分享从一般授权域(如数字家庭网络或个人娱乐域)延伸到广泛的用户社会网络域后,内容提供商将面临着由数字权利分享、转移和扩散所造成的不可控和滥用等安全风险。探索DRM权利在用户社会网络中的传播机理,并有效地控制其安全风险,成为亟待解决的关键问题。

(2)数字权利使用控制和转移过程中,结合可信计算技术及其终端平台(包括PC、移动终端等)标准规范,研究具有互操作性的数字权利可信分发和转移,保障数字权利的分享在多样性终端系统或网路平台上互联互通。

(3)综合化、跨网络(授权)域的数字权利转移与使用控制认证平台,为内容提供商保障数字权利可控的分享和传播,防止非授权使用和权利滥用,进而集中式控制和降低权利传播过程中的安全风险,实现普遍意义上的DRM数字权利安全、可控的分发和传播奠定了基础,从而促进数字内容产业的良性、健康发展。

## 参 考 文 献


[1] Hinkes E M. Access Controls in the Digital Era and the Fair Use/First Sale Doctrines[J]. Santa Clara Computer and High-Technology Law Journal,2007,23(4):685-726

[2] Kiema I. Commercial Piracy and Intellectual Property Policy[J]. Journal of Economic Behavior & Organization, 2008, 68(1): 304-318

[3] Regner T, Barria J A, Pitt J V, et al. An Artist Life Cycle Model for Digital Media Content:Strategies for the Light Web and the Dark Web[J]. Electronic Commerce Research and Applications, 2009,8(6):334-342

[4] Lesk M,Stytz M R,Trope R L. Digital Rights Management and Individualized Pricing[J]. IEEE Security & Privacy,2008,6(3): 76-79

[5] Li Y M,Lin C H. Pricing schemes for digital content with DRM mechanisms[J]. Decision Support Systems, 2009, 47(4): 528-539

[6] Nishimoto Y, Imaizumi H, Mita N. Integrated Digital Rights Management for Mobile IPTV Using Broadcasting and Communications[J]. IEEE Transactions on Broadcasting,2009,55(2): 419-424

[7] Bhatt S,Sion R,Carbunar B. A Personal Mobile DRM Manager for Smartphones[J]. Computers & Security,2009,28(6):327-340

[8] Rosenblatt B. DRM, Law and Technology: an American Perspective [J]. Online Information Review,2007,31(1):73-84

[9] 俞银燕,汤帜. 数字版权保护技术研究综述[J]. 计算机学报,2006,28(12):1957-1968

[10] 范科峰,莫玮,曹山,等. 数字版权管理技术及应用研究进展[J]. 电子学报,2007,35(6):1139-1147

[11] Fan Y C,Shen J H. DFT-based SoC/VLSI IP Protection and Digital Rights Management Platform[J]. IEEE Transactions on Instrumentation and Measurement,2009,58(6):2026-2033

[12] Ak M,Kaya K,Selcuk A A. Optimal Subset-Difference Broadcast Encryption with Free Riders[J]. Information Sciences, 2009,179(20):3673-3684

[13] Hou S H,Uehara T,Satoh T,et al. Integrating Fingerprint with Cryptosystem for Internet-based Live Pay-TV System[J]. Security and Communication Networks,2008,1(6):461-472

[14] Lian S. Secure Video Distribution Scheme Based on Partial Encryption[J]. International Journal of Imaging Systems and Technology,2009,19(3):227-235

[15] Fazio N. On Cryptographic Techniques for Digital Rights Management[D]. New York:New York University,2006

[16] Jamkhedkar P, Heileman G, Ortiz I. The Problem with Rights Expression Languages[C]// Proc. of 2006 ACM Workshop on Digital Rights Management. New York:ACM Press,2006:59-67

[17] Pretschner A,Hilty M,Schütz F,et al. Usage Control Enforcement:Present and Future[J]. IEEE Security & Privacy,2008,6(4):44-53

[18] Stamm S,Sheppard N P,Reihaneh S N. Implementing Trusted Terminals with a TPM and SITDRM[J]. Electronic Notes in Theoretical Computer Science,2008,197(1):73-85

[19] Yu A M,Feng D G,Liu R. TBDRM:A TPM-Based Secure DRM Architecture[C]// Proc. of 2009 International Conference on Computational Science and Engineering. Washington DC: IEEE Press,2009:671-677

[20] Gasmi Y,Sadeghi A R,Stewin P,et al. Flexible and Secure Enterprise Rights Management based on Trusted Virtual Domains [C]// Proc. of the 3rd ACM Workshop on Scalable Trusted Computing. New York:ACM Press,2008:71-80

[21] Thomas T,Emmanuel S,Subramanyam A V,et al. Joint Watermarking Scheme for Multiparty Multilevel DRM Architecture [J]. IEEE Transactions on Information Forensics and Security, 2009,4(4):758-767

[22] Singhal N,Lee Y Y,Kim C S,et al. Robust image watermarking

using local Zernike moments[J]. Journal of Visual Communication and Image Representation,2009,20(6):408-419

[23] Phan R C. Tampering with a Watermarking-based Image Authentication Scheme[J]. Pattern Recognition, 2008, 41(11): 3493-3496

[24] Huang H C, Fang W C. Metadata-based Image Watermarking for Copyright Protection[J]. Simulation Modelling Practice and Theory,2010,18(4):436-445

[25] Kougianos E,Mohanty S P,Mahapatra R N. Hardware assisted watermarking for multimedia[J]. Computers and Electrical Engineering,2009,35(2):339-358

[26] Poon H T,Miriand A,Zhao J Y. An Improved Watermarking Technique for Multi-user,Multi-right Environments[J]. Multimedia Tools and Applications,2009,42(2):161-181

[27] Koster P,Jonker W. Digital Rights Management[EB/OL]. http://www. springerlink. com/ index/v317 858416435v64. pdf

[28] 骆伟祺,黄继武,丘国平. 鲁棒的区域复制图像篡改检测技术[J]. 计算机学报,2007,30(11):1998-2007

[29] Jin H X,Lotspiech J,Nelson M,et al. Adaptive Traitor Tracing for Large Anonymous Attack[C]// Proc. of 2008 ACM Workshop on DRM. New York:ACM Press,2008:29-38

[30] Banerjee S,Karforma S. A Prototype Design for DRM based Credit Card Transaction in E-Commerce[J]. ACM Ubiquity, 2008,9(18):1-9

[31] Chen C L. A Secure and Traceable E-DRM System based on Mobile Device[J]. Expert Systems with Applications,2008,35(3):878-886

[32] Hidalgo A,Albors J,Lopez V. Design and Development Challenges for an E2E DRM Content Business Integration Platform[J]. International Journal of Information Management,2009,29(5): 389-396

[33] Zhang Z Y,Pei Q Q,Ma J F,et al. Cooperative and Non-cooperative Game-theoretic Analyses of Adoptions of Security Policies for DRM [C]// Proc. of 2009 IEEE Consumer Communications & Networking Conference. Washington DC:IEEE Press,2009: 1-5

[34] Zhang Z Y,Pei Q Q,Yang L,et al. Establishing Multi-party Trust Architecture for DRM by Using Game-Theoretic Analyses and Simulations of Adoptions of Security Policies[J]. Chinese Journal of Electronics,2009,18(3):19-524

[35] Zhang Z Y,Lian S G,Pei Q Q. Fuzzy Risk Assessments on Security Policies for Digital Rights Management[J]. Neural Network World,2010,20(3):265-284

[36] Zhang Z Y,Pei Q Q,Yang L,et al. Security and Trust of Digital Rights Management:A Survey[J]. International Journal of Network Security,2009,9(3):247-263

[37] Barlas C. Digital Rights Expression Languages[J]. JISC Technology and Standards Watch,2006

[38] eXtensible rights Markup Language(XrML) 2.0 Specification [S]. ContentGuard Inc,2001

[39] Open Digital Rights Language(ODRL) version 1.1[EB/OL]. http://www.w3.org/TR/odrl,2002

[40] Information technology—Multimedia framework Part 5:Rights Expression Language[S]. ISO/IEC 21000-5,2004

[41] Halpern J, Weissman V. A formal foundation for XrML[J]. Journal of the ACM,2008,55(1):4-45

[42] Pucella R,Weissman V. A Formal Foundation for ODRL[C]// Proc. of IEEE Workshop on Issues in the Theory of Security. Washington DC:IEEE Press,2004

[43] Jamkhedkar P, Heileman G. A Formal Conceptual Model for Rights[C]//Proc. of 2008 ACM Workshop on DRM. New York:ACM Press,2008:29-38

[44] Triantafyllou N,Ouranos I,Stefaneas P. Algebraic Specification for OMA REL licenses[C]// Proc. of 2009 IEEE International Conference on Wireless and Mobile Computing,Networking and Communications. Washington DC:IEEE Press,2009:376-381

[45] Pucella R, Weissman V. A Logic for Reasoning About Digital Rights [C]// Proc. of 2002 IEEE Workshop on Computer Security Foundations. Washington DC:IEEE Press,2002:282-294

[46] Halpern J Y, Welssman V. Using First-order Logic to Reason About Policies[J]. ACM Transactions on Information and Systems Security,2008,11(4):1-41

[47] Chong C N. Experiments in rights control expression and enforcement[D]. Enschede:University of Twente,2005

[48] García R,Gil R. Content Value Chains Modeling Using a Copyright Ontology[J]. Information Systems,2010,35(4):483-495

[49] García R,Gil R. Copyright Licenses Reasoning an OWL-DL Ontology[J]. Law,Ontologies and the Semantic Web,2009,188: 145-162

[50] Sheppard N P,Reihaneh S N. On the Operational Semantics of Rights Expression Languages[C]// Proc. of 2009 ACM Workshop on DRM. New York:ACM Press,2009:17-27

[51] Sachana A, Emmanuela S, Dasa A, et al. Privacy Preserving Multiparty Multilevel DRM Architecture[C]// Proc. of IEEE Consumer Communications and Networking Conference. Washington DC:IEEE Press,2009:1-5

[52] Sachana A, Emmanuela S, Kankanhalli M S. Efficient License Validation in MPML DRM Architecture[C]// Proc. of 2009 ACM Workshop on DRM. New York:ACM Press,2009:73-82

[53] Jamkhedkar P,Heileman G. Digital Rights Management Architectures[J]. Computers and Electrical Engineering,2009,35(2): 376-394

[54] Wang X. Design Principles and Issues of Rights Expression Languages for Digital Rights Management[EB/OL]. http://www.contentguard.com/drmwhitepapers/Design_principles_and_issues_of_ REL _for_DRM. pdf,2005

[55] Rafi M, Eleuldj M, Guennoun Z. Improvement of MPEG-21 Right Expression Language[C]// Proc. of 2009 IEEE/ACS International Conference on Computer Systems and Applications. Washington DC:IEEE Press,2009:997-1004

[56] Tsai D R,Chen W Y,Liang C H,et al. Role-based Access Control of Digital Right Management[C]// Proc. of 2009 Fifth International Joint Conference on INC,IMS and IDC. Washington DC:IEEE Computer Society Press,2009:1131-1134

[57] Caelli W J. Modernising MAC:New Forms for Mandatory Access Control in an Era of DRM[C]//IFIP International Federation for Information Processing. Heidelberg:Springer Verlag, 2007:433-442

[58] Zhang Z Y,Pu J X,Wu Q T,et al. Fuzzy Utility-Factor Assessments and Swarm Simulations on DRM Security Policies[C]// Proc. of 2009 International Conference on Computer and Communications Security. Washington DC:IEEE Computer Society

Press,2009:55-59

[59] Jamkhedkar P, Heileman G. DRM as a Layered System[C]// Proc. of 2004 ACM Workshop on Digital Rights Management. New York:ACM Press,2004:11-21

[60] Arnab A, Hutchison A. Persistent Access Control: A Formal Model for DRM[C]// Proc. of 2007 ACM Workshop on Digital Rights Management. New York:ACM Press,2007:41-53

[61] Park J, Sandhu R. The UCONABC Usage Control Model[J]. ACM Transactions on Information and System Security, 2004 (1):128-174

[62] Diehl E. A Four-layer Model for Security of Digital Rights Management[C]// Proc. of 2008 ACM Workshop on DRM. New York:ACM Press,2008:19-27

[63] Nair S K, Tanenbaum A S, Gheorghe G, et al. Enforcing DRM Policies Across Applications[C]// Proc. of 2008 ACM Workshop on DRM. New York:ACM Press,2008:87-94

[64] Muhlbauer A, Reihaneh S N, Salim F, et al. Location constraints in digital rights management[J]. Computer Communications, 2008,31(6):1173-1180

[65] 马兆丰,范科峰,陈铭,等. 支持时空约束的可信数字版权管理安全许可协议[J]. 通信学报,2008,29(10):153-164

[66] DRM Rights Expression Language Candidate Version 2. 1[S]. Open Mobile Alliance,2007

[67] Zhang Z Y, Yang L, Pei Q Q, et al. Research on Usage Control Model with Delegation Characteristics Based on OM-AM Methodology[C]// Proc. of IFIP International Conference on Network and Parallel Computing. Washington DC:IEEE Computer Society Press,2007:238-243

[68] Zhang Z Y, Pei Q Q, Ma J F, et al. A Fine-grained Digital Rights Transfer Policy and Trusted Distribution and Enforcement[C]// Proc. of International Conference on Computational Intelligence and Security. Washington DC: IEEE Computer Society Press, 2008:457-462

[69] Zhang Z Y, Pei Q Q, Ma J F, et al. Implementing Trustworthy Dissemination of Digital Contents by Using a Third Party Attestation Proxy-Enabling Remote Attestation Model[C]// Proc. of 2008 International Conference on MultiMedia and Information Technology. Washington DC: IEEE Computer Society Press, 2008:322-325

[70] Hibbert C. A copy protection and content management system from the DVB[EB/OL]. The DVB Consortium. http://www.dvb.org/ documents/newsletters/DVB-SCENE-05-Copy Protection Article.pdf,2005

[71] DRM Architecture Candidate Version 2. 1[S]. Open Mobile Alliance,2007

[72] Kim H, Lee Y, Chung B, et al. Digital Rights Management with Right Delegation for Home Networks[C]// LNCS 4296. Heidelberg:Springer Verlag,2006:233-245

[73] Koster P, Kamperman F, Lenoir P, et al. Identity-based DRM: Personal Entertainment Domain[C]// LNCS 4300. Heidelberg: Springer Verlag,2005:104-122

[74] Popescu B C, Crispo B, Kampermanf F, et al. A DRM Security Architecture for Home Networks[C]// Proc. of 4th ACM Workshop on Digital Rights Management. New York: ACM Press,2004:1-10

[75] Barhoush M, Atwood J W. Requirements for enforcing digital rights management in multicast content distribution[J]. Telecommunication Systems,2009

[76] Sans T, Cuppens F, Nora C B. OPA: Onion Policy Administration Model-Another Approach to Manage Rights in DRM[C]// Proc. of 2007 IFIP International Federation for Information Processing. Heidelberg:Springer Verlag,2007:349-360

[77] Lee S, Kim J, Hong S J. Redistributing Time-based Rights Between Consumer Devices for Content Sharing in DRM System [J]. International Journal of Information Security,2009,8(4): 263-273

[78] Feng X, Tang Z, Yu Y Y. An Efficient Contents Sharing Method for DRM[C]// Proc. of 2009 Consumer Communications and Networking Conference. Washington DC:IEEE Press,2009:1-5

[79] Gallery E, Mitchell C J. Trusted Mobile Platforms[C]// LNCS 4677. Heidelberg:Springer Verlag,2007:282-323

[80] Gallery E. Authorisation Issues for Mobile Code in Mobile Systems[D]. London:Royal Holloway,University of London,2007

[81] Zheng Y. A Conceptual Architecture of a Trusted Mobile Environment[C]// Proc. of the Second International Workshop on Security,Privacy and Trust in Pervasive and Ubiquitous Computing. Washington DC:IEEE Press,2006:75-81

[82] Reid J F, Caelli W J. DRM, Trusted Computing and Operating System Architecture[C]// Proc. of 2005 Australasian Information Security Workshop. Washington DC: IEEE Press, 2005: 127-136

[83] Kuhn U, Kursawe K, Lucks S. Secure Data Management in Trusted Computing[C]// LNCS 3659. Heidelberg: Springer Verlag,2005:324-338

[84] 张志勇,叶传奇,范科峰,等. DRM 安全策略的模糊层次分析法效用评估及选取[J]. 通信学报,2009,30(10A):126-131

[85] TCG Specification Architecture Overview Revision 1. 4[EB/OL]. https://www.trustedcomputinggroup.org,Aug. 2007

[86] TCG Design, Implementation, and Usage Principles[EB/OL]. https://www.trustedcomputinggroup.org,Apr. 2009

[87] Trusted Mobile Platform-Hardware Architecture Description, Software Architecture Description, Protocol Specification Document[EB/OL]. NTT DoCoMo, IBM, Intel Corporation, Oct. 2007

[88] TCG MPWG Mobile Trusted Module Specification V1. 0[EB/OL]. https://www.trustedcomputinggroup.org,June 2008

[89] TCG MPWG Mobile Reference Architecture[EB/OL]. https://www.trustedcomputinggroup.org,June 2008

[90] Mobile Phone Work Group Selected Use Case Analysis Specification Version 1. 0[EB/OL]. https://www.trustedcomputinggroup,Jan. 2009

[91] Application Security Framework[EB/OL]. http://www.omtp.org/pdf/ar- chived _ papers/OMTP _ Application _ Security _ Framework_v2_0.pdf,OMTP,Sep. 2007

[92] Stamm S, Sheppard N P, Safavi N R. Implementing Trusted Terminals with a TPM and SITDRM[J]. Electronic Notes in Theoretical Computer Science,2008,197(1):73-85

[93] Zhang Z Y. Security, Trust and Risk in Digital Rights Management Ecosystem[C]// Proc. of 2010 International Conference on High Performance Computing & Simulation. Washington DC: IEEE Press,2010