一种数字内容借(租)阅模型及其实现框架

钟 勇[1,2] 林冬梅[1] 刘凤玉[2,3]

(佛山科学技术学院信息与教育技术中心 佛山 528000)[1]

(南京理工大学计算机科学与技术博士后流动站 南京 210094)[2]

(南京理工大学计算机科学与技术学院 南京 210094)[3]

摘 要 提出了一种数字内容借(租)阅模型及其实施框架。该模型可实现数字内容的传统借(租)阅模型,也易于产生新的数字内容使用模型,具有较强的灵活性。模型的主要协议及其功能由许可证规则实现,易于借阅策略的更新修改,也使客户端软件代码精简短小,易于高可信验证。说明和示例了模型的协议、实施机制和实施方法,并与相关方法进行了对比。

关键词 借阅模型,数字内容,数字权利管理

中图法分类号 TP309 **文献标识码** A

Digital Content Lending (Renting) Model and its Implementaion Framework

ZHONG Yong[1,2] LIN Dong-mei[1] LIU Feng-yu[2,3]

(Information and Educational Technology Center, Foshan University, Foshan 528000, China)[1]

(Postdoctoral Mobile on Computer Application, Nanjing University of Science and Technology, Nanjing 210094, China)[2]

(School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing 210094, China)[3]

Abstract A lending (renting) model and its implementation framework of digital content were presented. The model not only can implement traditional lending (renting) models, but also can realize many new using models, which brings a strong flexibility to the model. The main protocols and functions of the model were implemented by license rules that make the update of lending policies easier and code shorter, and can satisfy the requirements of high assurance. The protocol, implementation meachnism and method of the model were explained and exampled. Finally, a comparative analysis with current methods was showed.

Keywords Lending model, Digital content, Digital rights management (DRM)

1 引言

随着互联网的发展,数字内容(电子图书、数字音像制品等)通过网络发布给用户。由于数字内容存在易复制、传播等问题,对数字内容的知识产权进行保护,确保数字内容的合法使用和传播的要求,使数字版权管理技术(digital rights management,DRM)正在成为全球许多标准化组织和厂商关注和研究的热点[1]。国际上许多著名计算机公司和研究机构纷纷推出各自的系统和产品,如 Micorsoft WMRM, IBM EMMS, Adobe Content Server, InterTrust DigiBox 和 Apple 的 Itune 等产品[2,3]。

控制数字内容是 DRM 系统的核心策略。DRM 系统不仅需要解决允许谁能访问数字内容的问题,而且要解决之后数字内容如何使用和控制的问题。对于数字内容服务商来讲,一种数字内容服务方式是借(租)阅方式。在传统图书馆的借阅方式中,持有图书证的合法用户可以从图书馆借阅一定数量的图书,在借阅期内可以使用该书,也能转借他人。在借阅期满之后,必须归还图书。租阅方式是一种计时收费方式,数字内容没有借阅期,但按借阅时间收取费用。租阅方式中数字内容也能转租他人,服务商可在该时段向租阅人收取费用或转租费。

对数字内容的借(租)模型特别是实施机制的研究,在 DRM 研究中尚处于空白。原因在于 DRM 系统中,许可证(license)是重要的组成部分,许可证中包含数字资源的使用权限、密钥、元数据等关键信息。权利描述语言(REL)用来构造许可证,描述数字资源或服务的使用权利,是数字权利保护的重要研究课题。目前的权利描述语言主要包括基于 XML 的语言,如 XrML(http://www.xrml.org),ODRL (http://www.ordl.net), MPEG-21 REL, OMA (Open Mobile Alliance) DRM-REL 和 OeBF (Open e-Book Forum) REL 等权利

到稿日期:2008-09-23 返修日期:2008-12-17 本文受中国博士后科学基金(20070421015),广东省自然科学基金(8452800001001086),江苏省博士后科研资助计划(0801045B),佛山市科技发展专项资金(200701002),国家自然科学基金(60673127),国家 863 计划(2007AA01Z404)资助。

钟 勇(1970-),男,博士后,副教授,主要研究方向为信息安全、数据库技术、数字版权保护技术等,E-mail:zhongyong1970@126.com;林冬梅(1969-),女,副教授,主要研究方向为信息安全、数据库技术、数字版权保护技术等;刘凤玉(1943-),女,教授,博士生导师,主要研究方向为网络性能保护和信息安全。

描述语言。基于 XML 的权利描述语言主要研究数字权限的表达，并未说明实施方法和具有正式语义，因而使基于 XML 的 REL 语言的确切含义严重依赖特定理解，并容易产生二义性和不确定性。如近来有学者证明 XrML 和 MPEG REL 等语言的评价(evaluation)算法并不能保证完全的可终止性[4]。缺乏正式语义也使基于 XML 的 REL 语言的安全实施缺乏可信性和形式化分析基础。因而，从总体上，现有的数字权利保护模型缺乏正式的可实施逻辑框架描述。

在提出的分布式使用控制和权利描述语言 LucScript[5] 的基础上，提出了数字内容的借(租)阅模型及其实施框架。该模型的优势在于：易于实现各类传统媒体的借阅和租阅模型，也易于产生新的数字内容使用模型，具有较强的灵活性。并且模型的主要协议及其功能由许可证规则实现，易于更新修改。而客户端软件只需包括许可证解释器等功能，代码精简短小，易于高可信验证。本文对该模型的协议、实施机制和实施方法进行了说明和示例，最后与现行的相关方法进行了比较。

2 LucScript 权利描述语言

基于 XML 的 REL 语言难以满足 DRM 系统对开放性、灵活性、可扩展性以及支持各类使用权利描述的要求[6]，缺乏实施语义。逻辑语言由于具有表达力、灵活性和语义完整性的优势，近年来，基于逻辑的 REL 语言的研究受到重视，但现存逻辑语言存在一些问题，如 LicenseScript 语言[6] 规则的不统一性、权限管理的不开放，缺乏表达授权决策持续性和数字内容实时动态使用控制等语义能力。LucScript(Logic-based Usage Control License Script)权利描述语言是提出的基于逻辑框架的新型数字权利管理语言，该语言基于 Active-U-Datalog[7] 逻辑语言，其具有触发功能的授权机制，起源于前期提出的使用控制授权框架 LUC[8]，具有较强表达力、灵活性和开放式权限管理能力等。

Active-U-Datalog 是一种结合主动规则、具有可更新能力的 Datalog 程序，其谓词原子包括表示插入和删除的更新原子 $\pm p(t_1,t_2,\cdots,t_n)$。通过 Active-U-Datalog 的主动规则，权利描述语言能描述环境条件变化产生的自适应规则，具有表达授权决策持续性和授权主客体属性可变性(mutability)下进行实时动态使用控制的能力。

LucScript 语言中许可证 *lic* 是四元组 $\{D, IDB, AR, BV\}$，其中 D 是许可证所保护的数字内容的唯一识别符，IDB 是内涵规则集，AR 是触发规则集，BV 是表示为 *name*≡*value* 形式的属性绑定形式。称 $P=IDB\cup AR\cup BV$ 为许可证程序部分。许可证表示成 $lic(D,\Delta)$，其中 Δ 是许可证程序标识符。图 1 是许可证示例。

```
(1) License //许可证示例
(2) (e_film_star_war, //许可证数字媒体标识
(3)     { play(D)← counter(n),n≥1,update_counter();
(4)       update_counter()←counter(n),n = n1 +1,-counter
          (n),+counter (n1);}, //IDB
(5)     { -total_counter(n),+total_counter(m)←total_counter
          (n),m=n+1,+play_a(D) },//AR,
(6)     { counter≡50;total_counter≡'0';version≡'11.6.1';expire
          ≡'07/12/31';type≡'use' }, //BV
(7) )
```

图 1　使用许可证示例

图 1 中语句(2)说明该许可证管理的数字媒体标识。语句(3)－(4)是 *IDB* 部分，语句(3)说明只有当计数器不小于 1 时才能播放该媒体并使用语句(4)进行计数器更新。语句(4)将计数器的值减 1，其中 $-counter(n)$ 删除计数器的当前值，$+counter(n_1)$ 插入新的计数值。语句(5)是主动规则，该规则在用户进入播放状态时触发(由 $+play\_a(D)$ 更新谓词触发)，将总计数值 *total_count* 加 1，其中 $-total\_counter(n)$ 删除现在的总计数值，$+total\_counter(m)$ 插入加 1 后的计数值。通过该触发规则，许可证可记录用户的总使用次数。语句(6)是许可证外延绑定部分，如 *counter* 谓词说明该许可证允许播放媒体 50 次。

LucScript 许可证使用逻辑程序调用谓词进行交互和更新。逻辑程序调用谓词(如表 1 所列)是提出的一种处理逻辑事务的特殊谓词。设事务 T，Δ 是许可证程序 $P=IDB\cup EDB\cup AR$ 的标识符，程序调用谓词包括表 1 的两类谓词。

表 1　调用谓词

谓词形式	谓词的使用
call(T) (Ⅰ型)	确定调用该谓词的逻辑程序是否可满足 T，如果 T 是可满足的且引发的更新是一致的，谓词返回 true，否则返回 false
call(□,(T)) (Ⅱ型)	确定逻辑程序 Δ 是否可满足 T，如果可满足且 T 引发的更新对程序 Δ 来说是一致的，谓词返回 true，否则返回 false

实际上，加入调用程序标识符，Ⅰ型调用谓词也能用Ⅱ型调用谓词表示。增加调用语义后，许可证具有自拆分能力。如假定在图 1 的许可证中增加下列 *IDB* 规则：

$$clone(lic(D,\Delta))\leftarrow create(lic(D,\Delta)),call(\Delta,(+IDB(r))),IDB(r) \quad (1)$$

其中 $create(lic(D,\Delta))$ 创建许可证 $lic(D,\Delta)$；$IDB(r)$ 是许可证结构谓词，代表许可证中的 *IDB* 规则；$call(\Delta,(+IDB(r)))$ 是Ⅱ型调用谓词，在程序 Δ 中执行 $+IDB(r)$ 插入。整个规则创建临时许可证 $lic(D,\Delta)$ 并将图 1 许可证的 *IDB* 规则全部插入到该临时许可证中。通过这种方法，可以拆分和创建新的许可证。

3 传统图书馆借阅模型的实现

本文获取数字内容和使用许可证的方式采用 LucScript 数字内容权利保护和迁移协议方式①，将用户的使用许可证与设备绑定的方式来限制数字内容的使用。LucScript 数字权利保护和迁移机制如图 2 所示，该机制实体主要包括内容提供商、清算中心和客户端 3 部分，其中内容提供商使用内容服务器提供数字内容，清算中心提供许可证管理和数字内容购买等功能，其中最主要的是版权服务器(含许可证生成器)，客户端最主要的结构是版权控制器。简单起见，只考虑了内容服务器(CS)、版权服务器(RS)和版权控制器(A)之间的协议关系作为三类实体的代表。

LucScript 数字内容权利保护和迁移协议依靠版权控制器产生客户端的设备标识(设备许可证)并发送到服务端，由服务端将使用许可证与设备许可证绑定再发回客户端的方式

① LucScript 技术报告 3：http://www.fosu.edu.cn/zhongyong/LucReport3.pdf(专利受理号：200810027787.5)

绑定用户机器。假定3类实体内容服务器、版权服务器和版权控制器均是安全可信的。数字内容付费收据 γ[9]是数字内容购买(会员)凭证,是安全防篡改的,只有购买数字内容的用户才可以从清算中心获得相应的付费收据,而 γ 的格式、γ 的安全发放、γ 的有效性检验不在本文考虑范围(更倾向于将 γ 与用户的电子证书联系起来)。LucScript 易于实现各类传统的借阅和租阅模型,也易于产生新的数字内容使用模型。

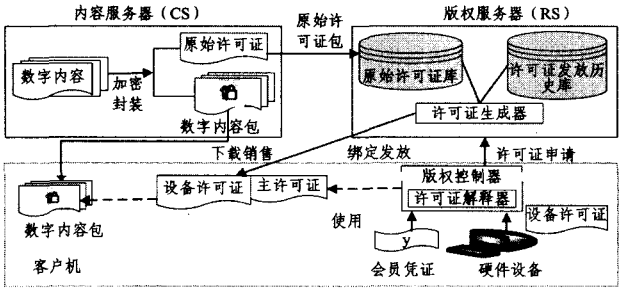

图2 LucScript 数字内容保护和迁移机制

3.1 主要实现步骤

图书馆借阅方法一般采取会员制,会员经注册后获得图书证。按会员类别不同,图书借阅有相应借阅期和数额限制。用户在超出借阅期未归还图书后,每天按一定金额进行处罚。用户也可以将图书转借他人,转借他人后,自己就无法使用该书。

LucScript 体系实现传统图书馆借阅模型的方法如下:

(1) 用户(付费)成为会员后,获得会员付费收据 γ,服务端设立用户账户,记录用户的可用金额。

(2) 用户在客户端下载加密的数字内容并安装版权控制器。通过版权控制器产生客户机的设备许可证 Dic_u 发送到版权服务器。

(3) 版权服务器收到设备许可证并验证用户合法性后,产生用户主许可证 Lic_u,并在 Lic_u 中设置借阅规则,然后与 Dic_u 绑定加密后发送回版权控制器。

(4) 版权控制器在收到主许可证后可按许可证的规定使用数字内容。当用户需要将数字内容转借他人使用时,称该用户为转借人,转借对象为借阅人,按下列步骤操作:

① 借阅人在借阅机安装版权控制器和下载加密的数字内容。

② 借阅人通过版权控制器产生借阅机的设备许可证 DIC_J 并输入借阅密码 J,版权控制器通过密钥生成函数 $K_J=G(H(J))$[②]生成会话密钥 K_J 加密 DIC_J。

③ 借阅人通过版权控制器导出加密后的 DIC_J 并通过网络发送或通过移动介质拷贝到转借人的客户机,再通过任何的可信途径将借阅密码 J 传送给转借人。

④ 转借人将借阅密码 J 输入到版权控制器,还原会话密钥 K_J 并解密 DIC_J,然后调用主许可证的借阅规则,产生借阅许可证 LIC_J,主许可证在产生借阅许可证的同时将处于暂时失效状态。

⑤ 转借人的版权控制器将 LIC_J 和 DIC_J 绑定并使用 K_J 加密后发回或拷贝到借阅人的客户机,然后导入版权控制器使用。

⑥ 借阅人要归还数字内容时,首先输入借阅密码 J,版权控制器通过密钥生成函数 $K_J=G(H(J))$ 生成 K_J 加密 LIC_J 后导出,并通过网络发送或通过移动介质拷贝到转借人的客户机。在 LIC_J 导出的同时,版权控制器将 LIC_J 删除,从而借阅人不能再使用数字内容。

⑦ 借阅人的版权控制器将加密后的 LIC_J 导入并使用 K_J 解密后,调用主许可证归还规则,该规则验证 LIC_J 后恢复主许可证的使用。

(5) 用户在使用完毕后将主许可证返回服务端并删除主许可证。服务端在收到主许可证后,将相应的数字内容标记为已还并修改相关的记录。

(6) 用户超出借阅期未还,服务端按照借阅规则每天从用户账户中扣除罚金,直到用户归还或许可证过了有效期。

3.2 数字内容借阅和归还协议(协议 E)

借阅模型在数字内容封装、主许可证获取和数字内容的使用等方面均使用 LucScript 数字内容保护和迁移协议中的相应协议。主许可证的归还采用协议 B 的许可证请求包的方式,不同之处在于归还许可证请求包中包含的是主许可证而不是设备许可证。

本文在该协议基础上增加数字内容借阅和归还协议(协议 E),符号约定如表2所列。

表2 协议所使用的符号约定

	符号	意义
1	A	版权控制器
2	D,Did	数字内容及其标识符
3	LRB	加密后的许可证借阅请求包
4	LLB	加密后的许可证借阅包
5	RRB	加密后的许可证归还请求包
6	Dic_i,Lic_i	许可证,i表示产生许可证的对象
7	$\{\cdots\}_K$	使用密钥加密后的信息
8	H(…)	单向 Hash 函数
9	G(…)	对称密钥生成函数,单射
10	γ	会员(付费)凭证

LucScript 数字内容保护和迁移协议中的数字内容权限迁移协议(协议 D)完成单个用户在不同设备版权控制器($A_1\rightarrow A_2$)之间权利转移过程,因而假定这些设备间可拥有共同的付费收据 γ 来产生会话密钥。本文的借阅模型需要将数字内容转借给不同的借阅人,因而使用共享借阅密钥的方法来产生会话密钥。协议 E 的主要步骤如下:

(1)A_2(借阅人版权控制器)产生借阅机设备许可证 Dic_{A2},输入借阅密钥 J,产生会话密钥 $K_J=G(H(J))$,并利用 K_J 生成许可证借阅请求包 LRB,发送或拷贝到 A_1,$LRB=\{Did,(Dic_{A2})K_L,(H(\{Did,(Dic_{A2})K_L\}))K_L\}$,并将密钥 J 通过安全渠道传给 A_1。

(2)A_1 从 LRB 包中分析出 Did 并查找是否存在使用许可证 Lic_{A1}。如不存在,则拒绝请求,否则利用 J 产生 $K_J=G(H(J))$并解密 LRB 包,进行完整性验证。如果未通过,则拒绝,否则 A_1 执行 Lic_{A1} 的借阅规则,产生借阅许可证 Lic_{A2} 并与 Dic_{A2} 绑定。借阅规则也使主许可证失效。

(3)A_1 构成借阅许可证包 $LLB=(Did,(Lic_{A2},Dic_{A2})K_L,(H(\{Did,(Lic_{A2},Dic_{A2})K_L\}))K_L)$发送或拷贝到 A_2。

(4)A_2 在收到 LLB 后用密钥 K_L 解密 LLB 包并进行完

② $G()$是单射的对称密钥生成函数,$H()$是单向 hash 函数。除版权控制器,用户应无法从 J 推出 K_J。具体方法不属本文范围。

整性验证。如果未通过检查，则拒绝 LLB，否则解密，得到 Lic_{A2} 和 Dic_{A2}。将 Lic_{A2} 和 Dic_{A2} 导入并使用 K_L 重新加密、保存、管理和使用。

(5)A_2 要归还借阅数字内容。输入借阅密钥 J，产生会话密钥 $K_J=G(H(J))$，并利用 K_J 生成许可证归还包 RRB 发送或拷贝到 A_1，$RRB=\{Did,(Lic_{A2})K_L,(H(\{Did,(Lic_{A2})K_L\}))K_L\}$，$A_2$ 在发送 RRB 包的同时删除 Lic_{A2}。

(6)A_1 利用 J 产生 $K_J=G(H(J))$并解密 RRB 包，进行完整性验证。如果未通过，则拒绝，否则 A_1 执行 Lic_{A1} 的归还规则，恢复主许可证的功能。

定理 1 数字内容借阅和归还协议(协议 E)是安全的，并能保证数字内容不被滥用，数字内容只能被单个用户使用。

证明：

(1) 协议在 A_1 和 A_2 之间传输信息是安全保密的。协议 E 在 A_1 和 A_2 之间的信息交流均使用共享借阅密钥 J 产生的会话密钥 $K_J=G(H(J))$加密。只有知道共享借阅密钥的版权控制器才能够解密和加密相应交流信息。

(2) 第三方无法重演(*replay*)使用 A_1 和 A_2 之间交流的信息。由于借阅许可证绑定 A_2 的设备，第三方即使导入借阅许可证也无法使用。

(3) 数字内容只能被单个用户使用。在第 2 步产生借阅许可证后，主许可证将被暂停使用，直到第 6 步借阅许可证被归还，在此期间只能被借阅人使用。而借阅人归还借阅许可证后不能再使用数字内容，保证了数字内容只能被单个用户使用。

(4) 转借人和借阅人无法滥用权限。转借人和借阅人虽然知道共享借阅密钥 J，但只有通过控制器才能产生会话密钥 K_J，转借人和借阅人本身无法得知 K_J 并解密和修改交流的信息。转借人同时只能产生 1 次的借阅证，无法将数字内容同时借阅给多人。同理，借阅人将共享借阅密钥泄露给多个人也无法获取多个借阅许可证。即使共享借阅密钥 J 的泄露也不会给本协议安全产生影响。

3.3 具体实现方法示例

由于版权控制器安装在不可信的客户端环境，为了达到高可信和可验证目的，版权控制器除包含 LucScript 解释器和可信存储等代码外，其代码应尽量短小。因而，在实现方法上，协议 E 的主要功能均由许可证和许可池的管理许可证规则来实现。该方法也具有较高的灵活性，易于借阅策略的修改和更新。

假定用户 A 成为会员后，获得会员(付费)收据 γ。服务端设立用户账户，记录用户可用金额。A 在客户机安装版权控制器并下载加密后的数字内容 D。然后按照数字许可证申请协议(协议 B)产生图 3 所示设备许可证并生成许可证请求包发往版权服务器。该设备许可证绑定客户机的 3 类设备：硬盘序列号、网卡 MAC 地址、主板序列号。

```
(1)  License
(2)    (client_A,//D
(3)    { }, //IDB
(4)    { }, //AR,
(5)    { id=='12345';type='device' harddisk=='1294-4373';mac
       =='00-11-11-3B-E3-BA', mainboard='UY2H 601XXXXX'
       },//BV
(6)  )
```

图 3 设备许可证示例

版权服务器在验证用户的合法性后，产生如图 4 所示的使用许可证，并生成许可证包发送回 A 的客户机。

```
(1)  License
(2)  (e_film_star_war, //D
(3)    { valid()←date(d1),expire(d2),d1≤d2,status('using');
(4)      play()←device(lic(dev,Δ)),call(Δ,(permit())),valid();
(5)      clone(lic(D,Δ))←create(lic(D,Δ)),insert(lic(D,Δ)),de-
         vice(lic(dev,Δ')),call(Δ',(permit()));
(6)      insert(lic(D,Δ))←call(Δ,(+IDB(r))),IDB(r),head(r,
         'valid');
(7)      insert(lic(D,Δ))←call(Δ,(+IDB(r))),IDB(r),head(r,
         'play');
(8)      insert(lic(D,Δ))←call(Δ,(+BV(name,value))),BV
         (name,value),name()'device',name()'borrow';
(9)      insert(lic(D,Δ))←call(Δ,(+borrow(TRUE)));
(10)     lend(lic(dev,D'),lic(D,Δ))←clone(lic(D,Δ)),call(Δ,
         (+device(lic(dev,D')))),status('using'),-status('u-
         sing'),+status('lending');
(11)     return(lic(D,Δ)←call(Δ,(id(i1),borrow(TRUE))),id
         (i2),i1 = i2,status('lending'),-status('lending'),+
         status('using')
       },//IDB
(12)   { },//AR,
(13)   { id=='12346';device=lic(client_A Δclient_A);type='use';
       borrow = FALSE; lendtime = '2008/08/31'; expire =
       '2008/12/31';status='using'},//BV
(14)  )
```

图 4 包含借阅规则的主许可证

图 4 所示的 *device* 谓词(第 13 行)绑定主许可证的设备许可证，*lendtime* 绑定用户的借阅期，*expire* 绑定许可证自身的有效期。在 *IDB* 规则中，第 3 行规则说明许可证在有效期内(注：非借阅期)且状态是'*using*'的时候才是有效的。第 4 规则说明在使用数字内容前必须验证设备的正确性且许可证是有效的才能使用。第 5 行规则说明生成新许可证规则，该规则说明生成新许可证之前必须验证设备的正确性(通过 *call*(Δ',(*permit*()))调用谓词查看设备许可证的 *permit*() 规则是否可满足)，谓词 *create*(*lic*(*D*,Δ))创建许可证结构。第 6、7 行规则分别将主许可证中规则头为 *valid* 和 *play* 的规则(第 3、4 行规则)复制到新许可证中。第 8 行规则将许可证的 *BV* 复制到新许可证中，但绑定设备的 *device* 谓词和 *borrow* 标志谓词不复制。第 9 行规则将新许可证的 *borrow* 标志设置为 TRUE。第 10 行规则是借阅规则，该规则头包含设备许可证并与新许可证绑定(由 *call*(Δ,(+*device*(*lic*(*dev*,Δ'))))调用谓词执行)，该规则也说明只能在主许可证状态为'*using*'的时候才能借阅(防止重复借阅)，借阅数字内容的时候产生新的许可证并将主许可证状态设置为'*lending*'。第 11 行规则是数字内容归还规则，该规则说明如果归还的许可证与主许可证的序列号相同且是借阅许可证(*borrow*(*TRUE*))，将主许可证的状态设置为'*using*'。

A 的版权控制器在验证主许可证的合法性后按照许可池规则导入主许可证，假定 A 的许可池管理规则如图 5 所示。

```
(1)  License //许可证示例
(2)  (lpool, //许可池唯一标识
(3)    {……;
```

```
        * * * * * * * * * * 接口规则 * * * * * * * * * *
(4)     encrypt_interface(e)←Is_LRB(e),input(J),GHash(J,
        Key),deLRB(Key,lic(Dev,Δ)),default_interface((lic
        (Dev,Δ)));
(5)     encrypt_interface(e)←Is_RRB(e),input(J),GHash(J,
        Key),deRRB(Key,lic(D,Δ)),default_interface((lic(D,
        Δ)));
(6)     default_interface((lic(D,Δ)))←+lic(D,Δ),call(Δ,(type
        ('use'),borrow(FALSE)));
(7)     default_interface((lic(D,Δ)))←call(Δ,(type('use'),bor-
        row(TRUE),id(i1))),lic(D,Δ'),call(Δ',(id(i2),+sta-
        tus('using'),-status('lending'))),i1=i2;
(8)     default_interface((lic(Dev,Δ)))←call(Δ,(type('de-
        vice')),assign_interface((lend(lic(Dev,Δ),lic(D,
        Δ'))),lic(D,Δ")),make_LLB(lic(D,Δ'));
        * * * * * * * * * * 接口规则 * * * * * * * * * *
(9)     make_LLB(lic(D,Δ))←input(J),GHash(J,Key),LLB
        (Key,lic(D,Δ)),
    }, //IDB
(10)  { }, //AR,触发规则
(11)  { id='12347';type='pool';algorithm='first' }, //BV
(12)  )
```

图 5　许可池管理许可证

许可池使用接口机制提交事务。为了处理借阅协议,在许可池中增加处理加密协议包的接口 *encrypt_interface(e)*。加密的借阅协议包首先由版权控制器提交接口 *encrypt_interface(e)* 。第 4 行规则说明当协议包提交到接口时 *encrypt_interface(e)*,判断该包如果是许可证借阅请求包(*Is_LRB(e)*),则输入借阅密码(*input(J)*)并产生会话密钥(*GHash(J,Key)*),然后解密该包并判断完整性(*deLRB(Key,lic(Dev,Δ))*)。如果成立,则将解密得到的设备许可证提交缺省接口(*default_interface((lic(Dev,Δ))))*。第 5 行规则处理许可证归还请求包,处理过程类似于规则 4。第 6 行规则是缺省(管理)接口规则,说明当提交的是使用许可证且非借阅许可证时,许可池将该许可证插入许可池中。第 7 行规则说明当提交的是借阅许可证时,许可证将与该借阅许可证 *id* 号相同的主许可证状态设置为'*using*',也即恢复该主许可证的有效性。第 8 行规则说明当提交的是设备许可证时,缺省接口将引发指定接口 *assign_interface* 由用户指定许可证 *lic(D,Δ")*,并将事务(*lend(lic(Dev,Δ),lic(D,Δ'))*)提交该许可证执行,即执行该许可证的借阅规则并产生借阅许可证 *lic(D,Δ')*,然后将借阅许可证封装成许可证借阅包(*make_LLB(lic(D,Δ'))*)。第 9 行规则是许可证借阅包封装规则,输入借阅密码(*input(J)*)并产生会话密钥(*GHash(J,Key)*)后,加密形成借阅包(*LLB(Key,lic(Dev,Δ))*)。

当 *A* 欲将数字内容转借给 *B* 使用时,首先由 *B* 的版权控制器产生设备许可证并在输入借阅密钥加密后发送或拷贝到 *A*。*A* 在输入借阅密钥解密后,将 *B* 的设备许可证提交到缺省接口(即许可证到达所提交的管理接口③),然后执行图 3 的第 6 行规则,并在用户指定主许可证后执行该许可证的借阅规则,将产生如图 6 所示的借阅许可证并设置主许可证状态为'lending',导致主许可证暂停使用。

```
(1)  License
(2)  (e_film_star_war, //D
(3)    { valid()←date(d1),expire(d2),d1≤d2,status('using');
(4)      play()←device(lic(dev,Δ)),call(Δ,(permit())),valid();
       }, //IDB
(5)    { }, //AR,
(6)    { id≡'12346';device≡lic(client_B,Δclient_B);type≡'use';
       borrow≡TRUE';lendtime≡'2008/08/31';expire≡
       '2008/12/31';status≡'using'}, //BV
(7)  )
```

图 6　借阅许可证

A 将许可证借阅包发送或拷贝到 *B*,*B* 输入借阅密钥并解密后将借阅许可证导入许可池使用。*B* 的许可池管理许可证图 7 所示。

```
(1)  License //许可证示例
(2)  (lpool, //许可池唯一标识
(3)    {……;
       * * * * * * * * * * 接口规则 * * * * * * * * * *
(4)    encrypt_interface(e)←Is_LLB(e),input(J),GHash(J,
       Key),deLLB(Key,lic(D,Δ)),default_interface((lic(D,
       Δ)));
(5)    default_interface((lic(D,Δ)))←+lic(D,Δ),call(Δ,(type
       ('use')));
* * * * * * * * * * 接口规则 * * * * * * * * * *
(6)    borrow()←get_device((lic(Dev,Δ)),make_LRB(lic(Dev,
       Δ));
(7)    make_LRB(lic(D,Δ))←input(J),GHash(J,Key),LRB
       (Key,lic(D,Δ));
(8)    return()←input(lic(D,Δ)),make_RRB(lic(Dev,Δ)),-lic
       (D,Δ);
(9)    make_RRB(lic(D,Δ))←input(J),GHash(J,Key),RRB
       (Key,lic(D,Δ));
    }, //IDB
(10)  { }, //AR,触发规则
(11)  { id≡'12347';type≡'pool';algorithm≡'first' }, //BV
(12)  )
```

图 7　借阅人的许可池管理许可证

图 7 所示的第 4 行规则说明当协议包提交到接口时 *encrypt_interface(e)*,判断该包如果是许可证借阅许可证包,则输入借阅密码产生会话密钥后解密该包并判断完整性,然后将解密的借阅许可证提交缺省接口。第 5 行规则是缺省(管理)接口规则,说明当提交的是使用许可证时,许可池将该许可证插入许可池中。第 6 行规则是借阅规则,该规则产生设备许可证后将该许可证封装成借阅许可证请求包。第 7 行规则是许可证借阅请求包封装规则。第 8 行规则是归还规则,该规则在用户指定归还的许可证后产生归还许可证请求包,并将该包从许可池中删除。第 9 行规则是归还许可证请求包封装规则。

许可证借阅包发送或拷贝到 *B* 以后,首先提交到 *encrypt_*

③ 参见技术报告 2:http://www.fosu.edu.cn/zhongyong/LucReport2.pdf

*interface(e)*解密后再提交到缺省接口(第5行),缺省接口将借阅许可证插入许可池使用。在使用完毕后,*B*调用管理许可证的第8行*return*规则产生*RRB*包后删除借阅许可证。

4 租赁模型的实现

4.1 租赁模型

租赁模型由服务商将数字内容以按时段收费的方式出租给用户或代理商,代理商可以将数字内容继续出租给用户使用,收取相应的租金。除许可证规则不同外,租赁模型使用和借阅模型相同的协议和体系。

4.1.1 直接租赁模型

(1) 用户(付费)成为会员后,获得会员付费收据 γ,服务端设立用户账户,记录用户的可用金额。

(2) 用户在客户端下载加密的数字内容并安装版权控制器。通过版权控制器产生客户机的设备许可证 Dic_u 发送到版权服务器。

(3) 版权服务器收到设备许可证并验证用户合法性后,产生用户主许可证 Lic_u,并在 Lic_u 中设置租赁规则,然后与 Dic_u 绑定加密后发送回版权控制器。

(4) 版权控制器在收到主许可证后可按许可证的规定使用数字内容。

(5) 用户在使用完毕后将主许可证返回服务端并删除主许可证,服务端在收到主许可证后将相应的数字内容标记为已还并修改相关的记录。

(6) 服务端按照租赁规则从用户账户中扣除租金,直到用户归还或许可证失效。

直接租用模型除收费方式不同外,其他类似于借阅数字内容的正常使用模型。

4.1.2 代理租赁模型

(1) 用户(付费)成为会员后,获得会员付费收据 γ,服务端设立用户账户,记录用户的可用金额。

(2) 用户在客户端下载加密的数字内容并安装版权控制器。通过版权控制器产生客户机的设备许可证 Dic_u 发送到版权服务器。

(3) 版权服务器收到设备许可证并验证用户合法性后,产生用户主许可证 Lic_u,并在 Lic_u 中设置代理租赁规则,然后与 Dic_u 绑定加密后发送回版权控制器,并按照租赁规则在服务端收取用户的一定费用或逐日计费。

(4) 用户从服务端下载电子钱包许可证(使用类似于获取用户主许可证的方法)。

(5) 当用户需要将数字内容转租他人使用时,称该用户为转借(租)人,借(租)阅对象为借(租)阅人,按下列步骤操作:

① 借阅人在借阅机安装版权控制器和下载加密的数字内容。

② 借阅人通过版权控制器产生借阅机的设备许可证 DIC_J 并输入借阅密码 J(由转借人产生并传送给租用人),版权控制器通过密钥生成函数 $K_J=G(H(J))$ 生成会话密钥 K_J 加密 DIC_J。

③ 借阅人通过版权控制器导出加密后的 DIC_J 并通过网络发送或通过移动介质拷贝到转租人的客户机。

④ 转借人输入借阅密码 J 到版权控制器还原会话密钥 K_J 并解密 DIC_J,然后调用主许可证的租赁规则如设置租用时间等产生租赁(借阅)许可证 LIC_J,版权控制器在产生租赁许可证的同时将按照租赁规则收取费用,转借人可按自己的二级租赁规则或双方约定收取费用。

⑤ 转借人的版权控制器将 LIC_J 和 DIC_J 绑定并使用 K_J 加密后发回或拷贝到借阅人的客户机并导入版权控制器使用。

4.2 具体实现方法示例

以代理租赁模型为例。假定用户 A 成为会员后,获得会员(付费)收据 γ,服务端设立用户账户记录用户,可用金额。A 在客户机安装版权控制器并下载加密后的数字内容 D。然后按照数字许可证申请协议(协议 B)产生设备许可证并生成许可证请求包发往版权服务器。

版权服务器在验证用户的合法性后,产生如图8所示的包含租赁规则的使用许可证并生成许可证包发送回 A 的客户机。

```
(1)  License
(2)  (e_film_star_war, //D
(3)    { valid()←date(d1),expire(d2),d1≤d2;
(4)      play()←device(lic(dev,Δ)),call(Δ,(permit())),valid();
(5)      clone(lic(D,Δ))←create(lic(D,Δ)),insert(lic(D,Δ)),de-
         vice(lic(dev,Δ')),call(Δ',(permit()));
(6)      insert(lic(D,Δ))←call(Δ,(+IDB(r))),IDB(r),head(r,
         'valid');
(7)      insert(lic(D,Δ))←call(Δ,(+IDB(r))),IDB(r),head(r,
         'play');
(8)      insert(lic(D,Δ))←call(Δ,(+BV(name,value))),BV
         (name,value),name()'device',name()'borrow',name()
         'expire';
(9)      insert(lic(D,Δ))←call(Δ,(+borrow(TRUE)));
(10)     lend(lic(dev,Δ'),lic(D,Δ))←clone(lic(D,Δ)),call(Δ,
         (+device(lic(dev,Δ')))),input(date),call(Δ,(+expire
         (d))),pay(date);
(11)     pay(date)←date(d1),n= d1−date,rent(m),money=n
         *m,getpool(lic(wallet,Δ)),call(Δ,(spend(money)));
       },//IDB
(12)   { },//AR,
(13)   { id='12346';device≡lic(client_A Δclient_A);type='use';
         borrow≡FALSE;rent≡0.5;expire≡'2008/12/31';},//
         BV
(14)  )
```

图8 包含租赁规则的主许可证

图8所示的*device*谓词(第13行)绑定主许可证的设备许可证,*rent*绑定每日租金,*expire*绑定许可证自身的有效期。第3行规则说明许可证在有效期内才是有效的。第4规则说明在使用数字内容前必须验证设备的正确性且许可证是有效的才能使用。第5行规则说明生成新许可证规则,该规则说明生成新许可证之前必须验证设备的正确性(通过*call*(Δ',(*permit*()))调用谓词查看设备许可证的*permit*()规则是否可满足),谓词*create*(*lic*(*D*,Δ))创建许可证结构。第6、7行规则分别将主许可证中规则头为*valid*和*play*的规则(第3、4行规则)复制到新许可证中。第8行规则将许可证的*BV*复制到新许可证中,但绑定设备的*device*谓词、*borrow*标

志谓词和 *expire* 谓词不复制。第 9 行规则将新许可证的 *borrow* 标志设置为 TRUE。第 10 行规则是租赁规则，该规则头包含设备许可证并与新产生的借阅许可证绑定(由 *call*(Δ,(+*device*(*lic*(*dev*,Δ'))))调用谓词执行)，该规则也说明需要借阅许可证需要设置有效期(*input*(*date*)谓词)并收取租赁费用。第 11 行规则是付费规则，该规则说明按照借阅许可证的出租日期扣除租用费用。

当 A 欲将数字内容转借给 B 使用时，首先从服务端下载电子钱包许可证。假定电子钱包许可证如图 9 所示，其中 *integrity* 绑定许可证的完整性检验值，*seqno* 是该电子钱包的序列号。第(3)行规则装入钱币数，第(4)行规则减少钱币数。

```
(1)  License(
(2)    wallet, //电子钱包标识
(3)  { load(n)←money(n1), n2=n1+n, −money(n1), +money
       (n2);
(4)    spend(n)←money(n1), n2=n1−n, n2≥0, −money(n1),
       +money(n2); }, //IDB
(5)  {}, //AR
(6)  { seqno='123456'; money=1500; type='wallet'; integrity
       =H(lic(wallet,Δ))}, //BV
(7)  )
```

图 9　电子钱包许可证示例

A 的许可池管理许可证类似于借阅模型中的管理许可证，在此不再重复。B 的版权控制器产生设备许可证并在输入借阅密钥加密后发送或拷贝到 A，A 在输入借阅密钥解密后将 B 的设备许可证提交到缺省接口后最终执行图 8 许可证的租赁规则(第 10 行)，将产生如图 10 所示的借阅许可证并导致 A 的电子钱包许可证被扣除租赁费用。

```
(1)  License
(2)  (e_film_star_war, //D
(3)    { valid()←date(d1), expire(d2), d1≤d2, status('using');
(4)      play()←device(lic(dev,Δ)), call(Δ,(permit())), valid
         (); }, //IDB
(5)    { }, //AR,
(6)    { id='12346'; device=lic(client_B, Δclient_B); type=
         'use'; borrow=TRUE; expire='2008/06/31'; }, //
         BV
(7)  )
```

图 10　租赁(借阅)许可证

A 在收取 B 的费用后(以双方协商的任意方式收取)，将许可证借阅包发送或拷贝到 B，B 在输入借阅密钥并解密后将借阅许可证导入许可池使用。租赁模型以时间作为借阅许可证使用期限限制，不需要归还。

结束语　与现存的硬件绑定方法相比，本方法的优势在于许可证本身具有自生成能力，通过服务端设定的许可证生成(借阅)规则，转借人的客户端能够自行产生借阅许可证并绑定借阅人的客户机器，从而既能实现转借人对数字内容的自行借阅，数字内容的版权又能得到保护。现有的相关硬件绑定方法，如 Microsoft WMRM、Adobe Content Server、中科院计算所的 ICCP[10] 和马兆丰等人的 CPSec[11]、北京大学计算所俞银燕等的具有硬件适应性的 HACP 体系[9]等，均不具备客户端的许可证自生成能力，无法实现本文的借(租)阅模型。

与现有的基于逻辑的相关权限描述语言相比，LicenseScript 语言通过使用 Prolog 程序作为许可证的表达语言，并通过多集重写(multiset rewriting)的方式实现许可证更新，是迄今为止最具表达力和灵活性的 REL 语言。但 LicenseScript 语言使用过程性的 Prolog 程序，使许可证的规则顺序影响许可证的运行结果，无法增量更新和生成许可证，无法表达本文的模型。另外，LicenseScript 管理许可证的多集重写方式的表达能力有限，无法实现类似于本文通过许可池对许可证的统一管理方式，无法直接在许可证规则中实现本文的借阅协议机制，缺乏本文在借阅策略上的灵活性和适应性。

下一步将对 LucScript 框架审计机制、权限维护和追踪、责任(obligation)授权等问题进行研究。

参 考 文 献

[1] 魏景芝，杨义先，钮心忻. OMA DRM 技术体系研究综述[J]. 电子与信息学报，2008，30(3)：746-751

[2] 俞银燕，汤帜. 数字版权保护技术研究综述[J]. 计算机学报，2005，28(12)：1962-1968

[3] 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

[4] Becker M Y，Fournet C，Gordon A D. Design and Semantics of a Decentralized Authorization Language [A]// 20th IEEE Computer Security Foundations Symposium [C]. 2007：3-15

[5] Zhong Y，Zhu Z，Lin D M，et al. A Method of Fair Use in Digital Rights Management [A]//Proc. of the 10th International Conference on Asian Digital Libraries [C]. LNCS 4822，Hanoi，Vietnam，2007：160-164

[6] Chong C N，Corin R. et al. LicenseScript：a novel digital rights language and its semantics [A]// Proc. of the 3rd International Conference on Web Delivering of Music [C]. Los Alamitos，California：IEEE Computer Society，2003：122-129

[7] Bertino E，Catania B，Gori R. Active-U-Datalog：integrating active rules in a logical update Language [J]. Lecture Notes in Computer Science，1998：107-133

[8] 钟勇，秦小麟，郑吉平，等. 一种灵活的使用控制授权语言框架[J]. 计算机学报，2006，29(8)：1408-1418

[9] 俞银燕，汤帜. 一种具有硬件适应性的数字内容版权保护机制[J]. 北京大学学报，2005，41(5)：800-808

[10] 谭建龙，庄超，白硕. 一种实用 Internet 内容版权保护系统的设计与实现[J]. 计算机研究与发展，2001，38(10)：1199-1203

[11] 马兆丰，冯博琴，宋擒豹，等. 基于动态许可证的信任版权安全认证协议[J]. 软件学报，2004，15(1)：131-140