第 33 卷 第 2 期 计 算 机 工 程 2007 年 1 月
Vol.33 No.2 Computer Engineering January 2007
·开发研究与设计技术· 文章编号：1000—3428(2007)2—0249—03 文献标识码：A 中图分类号：TP393

家庭网络 DRM 与典型 DRM 整合问题的研究

李 敏，刘胜利，陈克非
(上海交通大学电子信息与电气工程学院，上海 200030)

摘 要：对 DRM 和新兴的家庭网络 DRM 进行了概括介绍，通过对比分析探讨了二者之间整合的必要性。对整合所存在的问题进行了研究，提出了一种合理的解决方案。该方案不但可以使得内容和证书在家庭内共享，还可以保证内容提供商的利益并提供控制追踪的能力。对整合方案的可行性进行了讨论，结果表明此方案是完全可行的。

关键词：典型 DRM 系统；家庭网络 DRM 系统；系统整合；数字证书；设备使用链表

Study on the Integration of Home Network DRM and Typical DRM

LI Min, LIU Shengli, CHEN Kefei
(School of Electronics and Electric Engineering, Shanghai Jiaotong University, Shanghai 200030)

【Abstract】This paper introduces the development in DRM and home network DRM. Through the comparison between them, it proves the integration of both kinds of systems is necessary. It proposes a novel solution for the integration. The solution can not only make content and certificates sharable at home but also protect the benefits of content providers and provide the ability to control and trace. It discusses the feasibility of the solution and the results prove it.

【Key words】Typical DRM system; Home DRM system; Integration; Digital certificate; Device using chains

1 概述

随着因特网的普及和数字化技术的进步，数字化音乐、书籍等都能方便地通过网络发布给用户，数字内容提供商一方面期待从网络分发的商业模式中获取利益，另一方面则需要数字版权管理(Digital Right Management，DRM)技术来保护版权。近年来对DRM的研究备受关注，提出了很多相关方案[1]。目前针对DRM的研究主要有两个方向：典型DRM和新兴的家庭网络DRM。

典型 DRM 以单个消费者购买数字产品作为点播单位，采用内容和证书分离的机制。该机制下，证书和设备绑定，所以数字内容只有在购买设备上才能使用。这种绑定模式固然可以保障内容提供商的利益，但对于用户来说却极其不便，比如内容在用户本人的两台设备之间也不能共享。

新兴的家庭网络 DRM 解决了该问题。家庭网络 DRM 进行以家庭为单位的版权管理，用户合法获得的数字内容可以在家庭内联网的各设备之间自由共享，但家庭和家庭之间的内容传播有严格限制。目前掀起了研究热潮的数字家庭，旨在提供设备间的共享和协同工作能力，可见典型 DRM 会限制这种能力，而家庭网络 DRM 却很适合数字家庭环境，因此发展潜力很大。目前有 DVB、TV Anytime、OMA 等组织在积极制定家庭网络内容保护方面的标准。

比较而言，典型DRM技术较成熟，应用较广泛；家庭网络DRM发展潜力大，适用于数字家庭网络。可以推断，在较长时间内这两类技术将共存。但是共存会带来一些问题，典型DRM中证书和设备绑定，证书一旦离开购买设备就不可用，无法实现设备间共享。从已有研究来看，只有文献[6]提出了整合需求，尚无实际方案提出。因此如何在二者之间建立信息转换机制使其能够整合是很重要和迫切的。经过整合，内容就能从典型DRM输出到家庭网络DRM中共享，从而既能保护内容提供商的权益，又能给予用户更多的方便[6]。

2 典型 DRM 系统和家庭网络 DRM 系统的介绍

2.1 典型 DRM 系统

目前存在多种典型DRM解决方案[2]，如Windows Media DRM系统、Helix系统等。对这些系统进行分析可以发现，尽管它们在技术细节上不同，但整个系统框架和处理流程都是相同的，如图 1 所示。

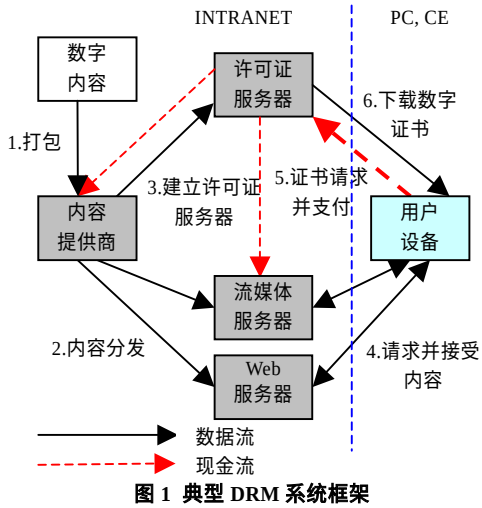

图 1 典型 DRM 系统框架

典型 DRM 系统包括内容提供商、许可证服务器、媒体服务器、用户设备这 4 大组成部分，其功能分别是打包、内容分发、证书购买和播放使用。框架中基本数据流程如下。

基金项目：国家自然科学基金资助项目(60303026)
作者简介：李 敏(1982－)，女，硕士，主研方向：数字版权管理；刘胜利，副教授；陈克非，教授、博导
收稿日期：2006-03-15 **E-mail：**limin@sjtu.edu.cn

(1)打包：内容提供商把数字内容用一个“密码”加密，这个密码存在加了密的证书中。其他信息附加在数字内容文中，例如获得证书的 URL 等。

(2)分发：打包后的内容放在网站、数字内容服务器上供用户下载，或者通过 CD、DVD 分发。

(3)建立许可证服务器：内容提供者建立许可证服务器，以存储特定的权限或证书规则。数字内容和许可证分开存储和分发，使整个系统更易管理。

(4)内容下载：用户设备可以通过不同的途径获取数字内容。典型 DRM 系统允许消费者把受版权保护的数字内容发送给他的朋友们。

(5)许可证请求和购买：设备要播放数字内容，必须先获得证书密钥来解密内容。设备向证书服务器发送请求并支付相应的费用来获得证书。

(6)播放数字内容：为了播放数字内容，消费者需要支持 DRM 的播放器。播放器会根据证书中的规则或权利来播放内容。证书可以包含不同的权限，例如持续时间、使用计数。这里证书和购买设备绑定，不可以传递。

2.2 家庭网络 DRM 系统

目前有不少家庭网络DRM解决方案，如认证域协议[3]、xCP方案[4]、SmartRight[5]等。虽然这些方案采用不同的技术对家庭内设备进行控制，它们的共同点在于引入了适应设备和认证域的概念。适应设备的特点是“自我遵守规则”，在对数字内容进行操作之前会先检查该操作是否违反了使用规则。家庭中拥有的适应设备连接起来组成认证域，用户合法获得的数字内容可以在域中各设备间无缝地流动，但域和域之间的内容传播有严格限制。图 2 显示了认证域的一般框架。

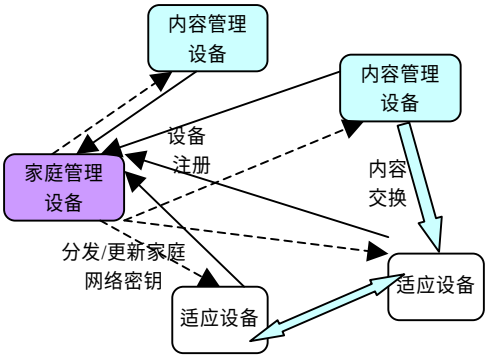

图 2 认证域框架

如图 2 所示，认证域由适应设备组成，一般存在家庭管理设备和内容管理设备。

(1)家庭管理设备负责管理认证域，包括组建域、注册设备到域中、从域中删除设备等；

(2)内容管理设备会引入新内容到域中，一个域可有多台内容管理设备；

(3)每个适应设备都有 CA 颁发的设备证书,标识号 GDL，和一对公私钥；

(4)同一认证域中的设备共享一个家庭网络密钥。认证域中的设备共享一个秘密，为方便叙述，用家庭网络密钥来指代；

(5)设备需要通过认证才能加入域，设备在同一时间内只能属于一个认证域，域设备间要进行内容交互之前也会进行相互认证。通过家庭网络密钥机制，可以标明和限制：某设备属于认证域 A 不属于认证域 B，该设备可以访问取 A 中的内容，但无法访问 B 中的。

3 典型 DRM 系统和家庭网络 DRM 系统整合框架

一般地，典型DRM系统能给内容提供商提供如下功能[7]：

(1)进行数字内容交易，发放证书并且接受支付费用；

(2)设置并跟踪用户对数字内容所进行的操作；

(3)提供额外控制，包括内容使用的次数、使用时间等。

内容提供商希望能够对数字内容进行交易、控制、并且跟踪，这也是典型 DRM 采用绑定机制的主要原因。要实现内容在家庭内共享，仍然要满足这些要求。通过研究，提出了整合框架，如图 3 所示。典型 DRM 系统中包括内容提供商、媒体服务器和许可证服务器；家庭网络 DRM 系统中包括一组适应设备。家庭中可采用任意家庭网络 DRM 方案，内容由内容管理设备从媒体服务器下载，证书需由家庭管理设备向许可证服务器购买。

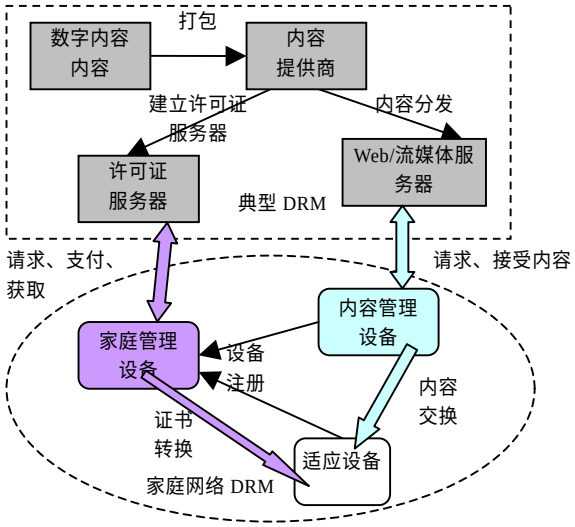

图 3 整合框架

4 一种适合于典型/家庭网络 DRM 系统的整合方案

在系统整合框架的基础上，通过采用链表机制，提出了一种整合方案。该方案增加证书的转换机制，使内容可以在家庭内部共享。

通过研究，发现在典型 DRM 系统中采用的是证书和内容分开的机制，分发商本身就允许内容可以随意复制而不做控制，由此对于 DRM 系统之间的内容的请求/获取问题上可以不作考虑，而重点在于证书的请求/获取问题的研究。而对于如何界定设备是否属于家庭、设备之间是否有权共享内容等交互认证都是属于家庭网络 DRM 系统的控制范围。因此只从证书结构、证书请求/获取过程等方面进行设计和分析，从而实现内容在两个系统之间的无缝转移。

4.1 证书结构

数字证书不再和管理设备绑定，而是在家庭网络 DRM 允许情况下在家庭内共享。有两种获取内容证书的方式：家庭管理设备向许可证服务器请求并购买；拥有可用证书的家庭设备转换生成给其他设备使用。

图 4 是证书的数据结构。证书分为两部分：传统证书和设备使用链表。

(1)传统证书是管理设备向许可证服务器购买后获得的，即典型 DRM 中所使用的证书。它一般包括数字

内容信息、购买设备和分发者信息、内容加密密码、颁发日期、使用规则、以及家庭共享或单个设备购买的标示等，最后许可证服务器对证书进行签名。因有签名，传统证书自

购买后就不得修改。

(2）设备使用链表记录着传递该证书的设备信息。此链表表示证书可以转移给家庭内其他设备使用，同时会记录内容使用情况。

证书的第 1 部分保留了传统证书结构，可以在典型 DRM 系统中通用；根据证书标识和设备链表，可以区分是不是可在家庭内共享。在证书上标识出当前可用设备，保证同一时间只能有一个设备拥有可用证书，即一旦设备把内容证书转化给其他设备使用，它就不能再使用该证书来播放内容。这样播放器才能根据证书来识别设备权限，能更好地限制和统计用户所购买播放次数、时间等权限。链表最后还加入基于密码的消息验证码（MAC），防止恶意设备删除或其他不可预知操作。

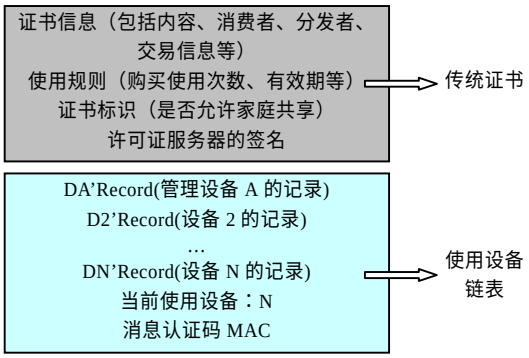

图 4 证书结构

4.2 证书请求/获取过程

4.2.1 许可证服务器->家庭管理设备

当家庭内需要播放数字内容 C，又没有 C 的可用证书时，可以通过管理设备进行购买。购买流程如下：

(1)管理设备以家庭名义向许可证服务器发出请求，购买家庭可共享的证书。

(2)许可证服务器验证其管理设备权限和设备证书，并根据支付情况发送设备证书、内容密码 CK 以及认证码 AK。证书中标识为家庭共享，并在设备链表中加入家庭管理备的记录。

(3)所有信息通过管理设备的公钥加密后传送。管理设备的播放器验证证书后使用 CK 播放内容；或者转换给其他设备使用。

4.2.2 拥有可用证书的设备->同一家庭内适应设备

当适应设备 D2 需要播放内容 C，并且家庭内设备 D1 拥有 C 的可用证书。

(1)D1 和 D2 相互认证是否属于同一认证域（属于家庭网络 DRM 的范围）。

(2)D1 把证书转换给 D2：D1 必须为当前可用设备，否则无权转换。D1 在设备使用链表中加入 D2 记录，每条使用设备记录包括：

D2'Record={证书转换者（D1），证书接受者(D2)，时间戳(转换时间)，D1 签名}。

(3)D1 把当前使用设备修改为 D2，并修改消息验证码：MAC=H(D'Record+…+D1'Record+D2'Record+AK)；H()是哈希函数，AK 是共享的认证码。

此后 D1 不是当前可用设备，不能再使用内容 C。

(4)D1 使用家庭网络密钥加密 CK 和 AK，发送给设备 D2。

(5)D2 收到证书后使用家庭网络密钥解密。D2 首先会验证传统证书完整性，并通过 MAC 检查设备链表的完整性，以及它是否为当前使用设备，检验完成后播放器才会解密内容并使用。

4.3 整合方案性能分析

通过系统整合并增加设备使用链表后，既能实现内容共享，又能满足内容提供商对于内容交易、跟踪、控制的需求。

(1)不改变典型 DRM 系统框架和原有证书结构，许可证服务器仍按照原有方式进行交易、设置访问条件和接收支付费用。

(2)设备使用链表记录着所有拥有过该证书的设备信息，内容提供商可以据此跟踪内容的使用情况。链表的存储空间和有效性检验时间都会随着链表长度的增加而线性增加，但对于一般家庭环境而言，设备不会太多，设备还是有能力来支持整合方案。

(3)当前使用设备标识保证了同时只有一个设备拥有可用证书，播放器可以按照原有方式对证书内限定的播放次数、时间等进行控制，这满足了内容提供商对于使用次数、时间等额外控制的需求，许可证服务器可以根据用户支付金额来限定播放次数、时间等。

(4)不改变原有许可证服务器所提供的证书结构，设备既可以单独购买内容证书，也可以作为认证域设备获取证书，增加了整合后系统的灵活性。

(5)认证域内可以使用任意的家庭网络 DRM 协议来控制设备和内容。

(6)设备只要通过家庭管理设备的认证，就可以获取内容证书。这样可以真正地方便用户共享，链表最后还加入 MAC 防止篡改。

通过分析可以看出，整合方案没有改变原有典型 DRM 系统和家庭网络 DRM 系统结构，也不局限于特定的系统，具有较好的通用性。整合方案中为用户增加了购买模式，购买后的证书通过标识位和设备链表来区分，用户可以灵活的选择以单个设备或者家庭的模式来购买证书。整合后的系统不仅可以为内容提供商提供原有功能，包括证书购买交易、设置内容证书、控制内容的使用、跟踪用户对内容使用等；还提供给用户足够的便利，只要用户家庭中使用采用家庭网络 DRM 方案，用它来保障家庭设备的认证和识别，内容证书即可以在家庭内部共享。

5 小结和未来展望

典型 DRM 系统和家庭网络 DRM 系统分别采用不同的框架，由此必须建立一套系统整合机制，数字内容才能在两种系统之间无缝传输。本文针对此问题作了深入分析并提出了解决方案。方案中取消证书和设备的绑定，增加了用户对于证书的购买模式，用户设备既可以以单个设备作为购买单位，也可以以家庭作为购买单位。方案中添加设备使用链表记录证书转移情况，从而提供了内容使用的追踪能力。通过整合可以在保证版权不受侵害的条件下，给用户提供共享便利性。今后，我们还会对各类典型/家庭网络 DRM 方案进行研究，通过对整合方案进行改进，使其可以适用于新系统。

致谢：感谢项目组成员俞峰琳、王晓芸等提供资料。

参考文献

1 Lyon G A. 500-241 2002 A Quick-reference List of Organizations and Standards for Digital Rights Management[S]. NIST Special Publication.

(下转第 254 页)