摘 要

数字版权管理(DRM)，是指数字化内容在生产、传播、销售、使用过程中知识产权保护与管理的工具。DRM 的目标是运用技术手段遏制盗版，保护数字化内容的知识产权，保证数字化产品市场销售渠道的畅通，保障作者、出版商的利益和用户的合法使用权利。

本文在收集和分析近年来国内外 DRM 文献的基础上，对 DRM 技术体系、功能结构与信息结构、DRM 主要技术原理、DRM 系统模型及 DRM 在电子书版权管理中的应用进行了研究；文章结合椭圆曲线数字签名，提出了一种基于硬件指纹的电子书认证算法；同时本文也将移动代理技术应用于数字版权管理，提出了一种改进的 DRM 系统模型。

随着网络的飞速发展，出现了网络书店等各种形式的电子书网络出版发行方式，为了遏制盗版、非法复制与传播等侵权行为，对于电子书的版权保护变得非常重要。因此，本文最后设计并实现了一个简单的基于 DRM 的电子书在线销售系统，系统使用机器指纹实现用户身份认证及许可证有效性验证，能够有效地实现电子书在线及离线的版权保护。

关键词 数字版权管理，信息安全，移动代理，电子书，椭圆曲线

ABSTRACT

Digital Rights Management (DRM) is the tool that protects and manages the intellectual property of digital content during producing, spreading, selling and using. Its target is to make use of technique means to suppress pirating, to protect the intellectual property of digital product, to ensure the outlet of the market sale expedite of digital products, and to guarantee the benefits of authors, publishers and the legal usage right of the customers.

Based on collecting and analyzing literatures internal and overseas about DRM, the paper studies the technique system, function structure and information structure, main technical theory, and the system model of DRM. The paper also probes into the application of DRM on e-book copyright management. Combining with elliptic curve digital signature, the paper forwards an e-book attestation arithmetic which is based on hardware fingerprint. And then the paper takes the advantage of mobile agent technique and forwards a reformative DRM system model.

With the quick development of network, various forms of e-book publication, such as bookstore, appear on internet. In order to suppress these actions, such as pirating, illegal copying and spreading, it is important to protect copyright of e-books. So, a simple e-book on-line distribution system, which is based on DRM, is finally designed and achieved in this paper. The system uses machine fingerprint to achieve customer identity attestation and license usefulness verification, and thus achieving copyright protection of e-books on-line and off-line efficiently.

KEY WORDS digital rights management, information security, mobile agent, e-book, elliptic curve

原 创 性 声 明

本人声明，所呈交的学位论文是本人在导师指导下进行的研究工作及取得的成果。尽我所知，除论文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得中南大学或其他单位的学位或证明而使用过的材料。与我共同工作的同志对本研究所作的贡献已在论文的致谢语中作了明确的说明。

作者签名：胡秀　　日期：2007年5月27日

关于学位论文使用授权说明

本人了解中南大学有关保留、使用学位论文的规定，即：学校有权保留学位论文，允许学位论文被查阅和借阅；学校可以公布学位论文的全部或部分内容，可以采用复印、缩印或其它手段保存学位论文；学校可根据国家或湖南省有关部门规定送交学位论文。

作者签名：胡秀　导师签名：　日期：2007年5月27日

第一章 绪论

1.1 课题背景

在当今数字化的时代，许多文化产品如音乐、视频和书籍等都开始以数字作为载体。数字文化产品容易保存，便于复制，结合高速发展的网络，可以很方便地实现网上发行，从而缩短发行周期，降低发行成本。但是成也萧何，败也萧何，阻碍数字文化产品发展的最大障碍也正在于此，它的易复制、易传播性同样会被少数非法盗版者利用。在网络发达的今天，可以很容易地将复制后的产品传播到全国甚至全球。因此要使数字文化产品体现出应用的优势，切实有效地保护好数字产品的版权就显得非常重要。

传统上，对数字产品的访问控制只是简单地基于访问控制机制，如注册登陆和付费购买等。这种简单机制无法防止少数用户在购买了产品之后的非法复制和传播。因此，关于数字版权管理[1][2](Digital Rights Management，简称DRM)的研究就应运而生了。

数字版权管理(DRM)是一项涉及到技术、法律和商业各个层面的系统工程，它为数字媒体的商业运作提供了一套完整的实现手段。DRM技术使得版权者不用再耗费大量时间和精力与客户谈判，来确保数字媒体内容能够被合法的使用。DRM将使各个平台的内容提供商们，无论是因特网、流媒体还是交互数字电视，提供更多的内容，并采取更灵活的节目销售方式，同时有效地保护知识产权。

那么什么是DRM呢？

以前数字版权管理主要是利用安全和加密方法来解决非法拷贝问题，即将信息内容的分布锁定和限制在付费用户的范围内。这是第一代DRM系统，它意味着对现实的充分限定和DRM系统功能的扩展；而第二代DRM系统则包括了描述、身份认证、交易、保护、监控和追踪记录对有形和无形资产的各种权利使用形式，其中也包括对权利拥有者之间关系的管理。

DRM不仅仅指版权保护，同时也提供了数字媒体内容的传输、管理和发行等一套完整的解决方案。因此DRM是一个系统概念，它包含数字版权信息使用、受版权保护的数字媒体内容的管理和分发。关于DRM，一个比较正规的说法是“DRM是对有形和无形资产版权和版权所有者关系的定义、辨别、交易、保护、监控和跟踪的手段。”需要强调的一点是，DRM是“权利的数字化管理”，而

不是“数字化权利的管理”，即DRM是管理所有各种权利而不仅仅是管理对数字化内容的许可权。在实际应用中，我们遇到的硬件狗、软件许可证、系列号、机顶盒等都属于DRM的范畴。

DRM 并不玄妙。对创作者来说，建立一张简单的电子表格，在表格里面记录作品的版权信息和所有者，并对这些信息进行跟踪就可以实现最简单的 DRM。当然这个电子表格可以做成 ONLINE 的形式，这样就可以随时在网络上查阅了。对于生产和发行商来说，DRM 系统就复杂多了，它要能够记录、追踪、监控一系列已有和新创作的作品，作品内容本身以数字格式被存储并加密，只有当生产商、发行商、创作者就合同达成一致，结算货款以后才能被解密使用。系统从使用角度来说主要包括内容提供商、内容运营商和内容消费者三个子系统[3]：其中内容提供商部分负责内容的采集、加密以及数据库的创建和管理；而内容运营商部分要实现的功能包括许可证管理、用户管理、计费管理以及发布频道定制；内容消费者部分包括方便实用的播放器、有效方便的购买及支付方式。DRM 运营时其子系统之间的相互协作关系如图 1-1 所示。

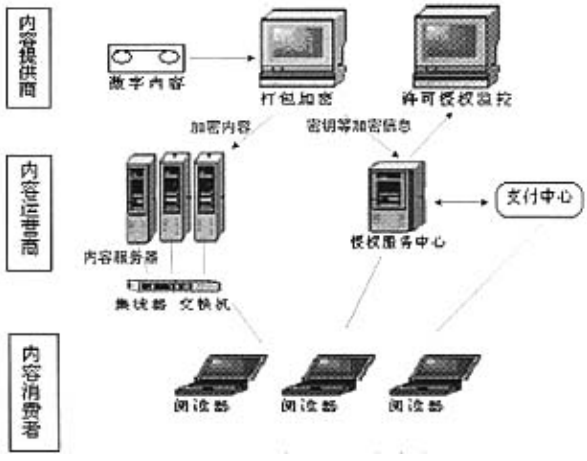


图 1-1 DRM 运营时的协作关系

美国畅销小说作家Stephen King在2000年3月14日发表了一本eBook《Riding the Bullet》，这是第一本只出eBook不出印刷版本的书，也是得益于DRM技术，作家在半个月内获得45万美元的收入。从这几年的网络出版发展看，DRM技术应用于网络出版后，出版eBook的出版社和销售eBook的网站持续增长，DRM技术推动了eBook产业的发展。同时DRM技术也在很大程度上推动了电子商务、流媒体、远程教育、数字电视等各方面的发展。

本课题基于国家自然科学基金项目(编号：60173041)和湖南省自然科学基金项目(编号：02JJY2094)两个科研项目。

1.2 国内外研究现状

目前已经有很多DRM方面的研究项目在不同的领域内开展[4]。IBM公司的Cryptolope就是一个从90年代初期就开始研究的基于超级分发的版权管理系统。一些著名的软件公司已经推出包含DRM技术的产品，比如Adobe公司的Merchant，是和Adobe的Acrobat电子图书阅读器相配合的电子图书交易和版权管理系统；微软公司的Media Rights Server是和微软公司的Media Player相配合使用的流媒体授权系统；原GlassBook公司GlassBook ContentServer(现为Adobe Content Server)是一个专门的电子图书版权管理服务软件，提供电子图书的制作、存储、发布，和Adobe的Acrobat或GlassBook的GlassBook Reader相配合。在国内,DRM也有着巨大的发展空间，如视频点播、付费电影、DRM加密直播、数字媒体文件的预览和付费使用等等，方正Apabi[5]对数字版权管理的各项应用都提出了完整的解决方案。

而在DRM的使用过程中，也不可避免的暴露出一些安全上的缺陷，现今的安全算法，在安全性、严密性方面很多都存在着一定的隐患，最终导致被黑客破解，将加密的内容从DRM中剥离，这直接损害了信息版权所有者和合法经营者的应得利益；另一方面，在互联网这个虚拟的数字空间里，往往无法清晰地识别用户，明确地规划和约束用户对于信息使用的行为。身份认证作为已经日趋成熟的技术，解决了用户合法身份的问题。但是，对于如何约束拥有合法身份的人员合法使用信息而不具备超越权限的行为，却一直没有一个有效的技术手段。

虽然存在着以上的问题，但DRM技术正在不断地发展并被广泛地应用，通过不断改进加密算法，不断地提高设计的合理性、严密性，DRM技术更好地在数字空间里不可伪造地识别用户、授予用户的权利范围权利、规范用户的行为方式来保障数字化信息的所有者和经营者的权利及利益。

数字内容的版权管理是通过两个方面来实现的[3][6]，一是数字版权保护，二是认证计费技术，本文中主要研究数字版权保护技术。

1.2.1 数字版权保护

数字版权保护是实现数字信息产品通过网络销售的前提条件，采用数字版权保护技术可有效地杜绝通过网络和计算机非法复制、拷贝和传送数字信息产品。数字版权保护的软件是一个端到端的系统，实现一个可扩展的平台用来安全地分发数字产品。该系统具有以下特征：

1．通过加密等技术保证数字产品的安全性；

2．未经授权，用户不能通过欺骗或解密的方式在线或离线查看数字内容；

3．授权用户不能将数字内容以未经保护的形式保存或分发；

4．授权用户不能对数字内容进行许可证限制范围之外的操作；

5．授权用户不能将自己的许可证提供给他人使用；

6．实现在线版权保护和下载数字版权保护两种方式；

7．数字内容在流通过程中应该是可计数的；

8．可以控制数字内容的二次传播。

在实现这几个方面保护时，需要用到对称加密技术、非对称加密技术、数字签名和单向Hash函数、数字证书、数字水印、防止篡改以及XML等多种技术。

对用户操作的限制可包括：

1．播放时间限制(播放许可证的生效日期和失效日期)；

2．播放次数限制；

3．许可证和用户使用的硬件环境绑定。

1.2.2 认证计费技术

认证计费技术是一整套数字信息产品计费、认证、收费、报账的用户付款结算系统，只有实现安全可靠、方便快速的付款结算系统才能保证数字信息产品的经营，保证企业与消费者共同的利益。认证计费的主要功能如下：

1．可以自主地、根据不同类型的数字信息产品和不同分类，以及其他一些数字信息产品的属性信息来设定不同的价格体系(收费体系标准)。收费形式包括：免费、月租费、时间卡预付费、按数量购买收费、打包/套餐收费。同时，也可以按带宽、数字产品类型、档次、服务质量等条件设定收费体系；

2．支持对特定时段、特定用户的优惠节目折扣定义(时间段、双休日)，特殊用户折扣定义(点播常客),用户缴费管理(修改用户账户余额、设置用户按月访问的权限)。实现按时段优惠、假日优惠、内容优惠、特定用户群优惠等；

3．用户费用查询、修改功能；

4．建立数字产品的计费、财务、收费系统，并提供相关经营报表。计费财务处理系统包括计费数据的分拣、出账、销账、查询、结算处理等，支持银行托收功能、网上电子商务方式的缴费功能；

5．从认证和数据采集系统获得原始的计费数据，再与用户管理系统结合，对用户信用的控制实时化、个性化，既有效控制欠费，又鼓励用户消费；

6．提供发票管理功能，与内容提供商之间的结算、版权结算等，对客户服务系统提供收费清单接口。

1.3 DRM技术的发展及前景

近年来，正版电子书在国内外的应用越来越普及，网民可以在网上购买电子书，或到数字图书馆借阅电子书；随着iPod等设备的流行，越来越多的网民体验了从网上购买正版音乐的便捷；同时，国内也有不少宽带服务商提供有版权保护的VOD点播节目。虽然这些应用的商业模式各不相同，但都是通过互联网进行数字内容的销售或服务，需要对数字内容的版权进行保护，因此数字版权保护技术及其重要性也被越来越多的人关注和认识。早在2003年10月，IDC的调查分析就显示，DRM是未来最有前景的10大IT技术之一。

现今DRM技术已经在软件、电子书、音乐、影视、安全文档等领域得到了一定应用。随着新需求的产生，DRM有着更为广阔的发展前景，主要体现在以下三个方面：

1．数字内容的共享与转移：支持数字内容共享要求在保护数字内容版权的前提下，允许用户在一定的范围内，在多台设备上共享数字内容，用户不能在超出范围的其他设备上使用受保护的数字内容；支持数字内容的转移需要解决由于设备更换引发的数字内容在设备间的迁移和由于出借、赠送、转卖数字内容引发的数字内容在用户间的转让这两个问题，转移的关键在于实现所有权的真正转移，确保源设备或源用户(暂时或永久)无法使用数字内容，目标设备和用户可以使用数字内容；

2．可信计算平台：在现有的大部分系统中，数字内容的解密使用、使用权利的解析验证由客户端DRM应用程序负责。对PC等通用设备而言，客户端DRM应用程序的运行环境是不安全的。因此，需要采用各种技术手段来确保程序的可信执行；

3．移动DRM：随着移动数据增值业务的迅速发展，内容提供商通过大量下载类业务及MMS等信息类业务传播的音视频和应用软件、游戏等数字内容越来越多，其版权及相关利益必须得到保证。将DRM技术引入移动增值业务，可以确保数字内容在移动网内传播，保证内容提供商的利益。

1.4 论文研究内容及组织结构

本文研究DRM体系结构、基本结构、DRM主要技术原理(加解密及数字签名、唯一标识符技术、信息隐藏与数字水印技术、数字权限描述语言等)、DRM系统模型等，同时研究DRM在电子书版权管理中的应用。最后，本文将探讨在电子图书的数字出版领域中DRM技术的应用，即研究基于DRM的电子书销售系统中

版权保护涉及到的主要技术与解决方案，并设计相关程序。

论文共分为五章，各章内容简介如下：

第一章为绪论，主要介绍了课题的研究背景，分析了国内外数字版权管理技术的研究现状，同时讨论了DRM技术的发展前景；

第二章主要对DRM技术进行了详细地分析和研究，研究了DRM体系构成、基本结构等；研究了DRM在电子书版权管理中的应用，并提出了一种基于椭圆曲线与硬件指纹的电子书认证算法；此外对DRM的系统结构进行了分析，并将移动代理技术应用于DRM系统，提出了一种改进的DRM系统模型；

第三章提出了一种基于DRM的电子书在线销售系统模型的总体设计，并给出了系统的主要流程；

第四章详细介绍了电子书在线销售系统主要技术的实现，本设计主要完成服务器端电子书的加密及许可证文件的生成，并给出了相关程序；

第五章是总结与展望，总结了本文所做的一些工作，指出不足之处，并提出今后的努力方向。

第二章 DRM 技术分析与研究

2.1 DRM 技术体系的基本构成

DRM 技术是一套比较完整的技术体系[7]，从技术上保障数字内容在整个生命周期内的合理使用。DRM 技术应该是一个可信、公平、公正的技术体系，是一种具有认证并无法轻易破坏的平台，它包括一系列相互联系的技术，这些技术经过集成形成相对完整的技术机制，DRM 技术体系的基本构成如图 2-1 所示。

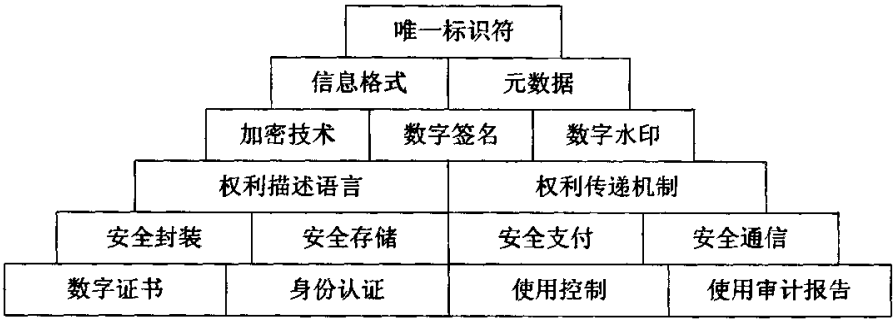


图 2-1 DRM 技术体系的基本构成

1. 唯一标识符：在网络环境下唯一持久地标识数字版权管理中的各个实体；

2. 信息格式：通过开放格式(如 XML、PDF、JPEG、MPEG、CSS 等)支持多种信息内容形态的表示、交换和解析；

3. 元数据：用来支持对数字版权管理中各实体的定义和描述，是保存特定信息的数据段；

4. 加密和签名技术：用来支持对数字内容的加密、防伪造、防抵赖和来源认证以及与此相关的密钥管理；

5. 数字水印技术：是信息隐藏技术的分支，通过将特定的数字内容隐藏地嵌入公开数字内容以实现对数字内容的鉴别，从而发现泄密者或擅自拷贝者；

6. 权利描述语言及权利传递机制：对数字信息交易使用过程涉及的复杂对象及复杂权利进行定义、描述，并以计算机可识别的方式进行标记、传递和检验；

7. 安全封装：负责将多个数字信息对象及其元数据封装到单一文件内或特定物理载体上以便传递，封装过程可能涉及压缩和加密处理；

8. 安全存储：负责整个数字版权管理过程中数据内容的可靠存储；

9. 安全支付和安全通信：主要利用SET(安全电子交易)和SSL(安全套接层)等技术保证数字信息产品的可靠交易和安全传递；

10. 数字证书和身份认证：通过X.509数字证书和PKI(公开密钥基础设施)认证体系来验证双方身份、保障交易或传递的不可抵赖性和可审计性；

11. 使用控制和使用审计报告：在身份验证、权利和义务的规定的基础上实施交易或利用授权，并统计、报告交易或使用的情况。

2.2 DRM基本模型

在设计和实现DRM的过程中，有两类关键体系要考虑，即功能结构、信息结构[8-9]。功能结构是指DRM系统的高层模块和组件；信息结构是指DRM内部实体及其关系的建模。

2.2.1 DRM功能结构

所谓功能结构，是指DRM系统的高层模块和组件，这些组件通过协作能提供产权的端对端管理。如图2-2所示。

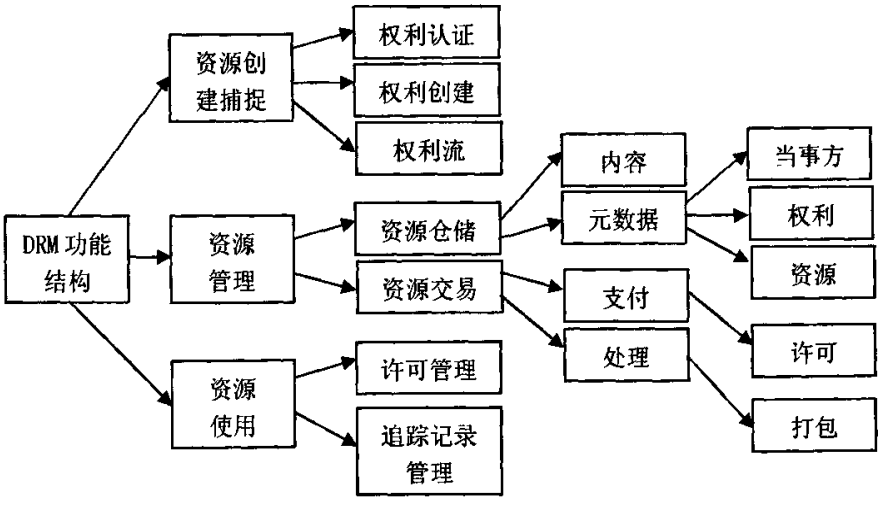


图2-2 DRM系统的功能结构

1. 具有知识产权的资源创建与捕捉模块

这一模块是管理数字信息内容的创建，使其可以比较容易地进行交流和交易。当信息内容被不同的创建者或提供者首次创建(或重新使用以及在权利范围内进行扩展)时，这一模块确保他们的权利，它主要完成以下三个功能：

(1) 产权确认：保证在已有内容基础上创建的资源合乎权利要求；

(2) 产权建立：将产权赋给新内容，如指明产权的所有者和使用许可；

(3) 产权工作流：允许对内容进行一系列的工作流步骤进行产权的审查和/或认可。

2．资源的管理

这一模块用来管理和实现内容的交易，包括从资源创建者那里获取内容，加入到资源管理系统中去。这个模块中的交易系统需要管理描述性元数据及产权元数据(如团体、使用、支付等)。这个模块主要完成两个功能：

(1) 仓储功能：允许对可能是分布式的数据库中的内容的存取与检索，以及对元数据的存储与检索；

(2) 交易功能：将许可赋给拥有内容产权交易协定的团体，包括获得许可的人向产权所有者的付费(如版税支付)，在某些情况下，需要对内容进行一定的处理以满足许可协议的要求，如对信息进行加密或打包处理。

3．资源的使用

这一功能模块用来处理进行内容交易时对内容的使用管理，包括在特定的系统或软件中支持在被交易内容之上定义的一些约束。主要实现两个功能：

(1) 许可权限管理：使内容的使用环境能遵守与内容相关的产权。例如：如果用户只有阅读文档的权限，那么他不能将它打印出来；

(2) 跟踪管理：追踪内容的使用情况。如用户只得到播放一部视频十次的许可，如果每一次都要付费，则这个模块需要与交易系统进行协作，以跟踪使用情况或记录事务。

2.2.2 DRM信息结构

DRM系统的第二个重要结构是信息结构，信息结构是指DRM内部实体及其关系的建模。它覆盖了DRM系统内部各个实体的建模及其相互之间的关系。信息结构主要涉及三个问题:即实体建模、实体的确认与描述、权利声明的表示。

1．实体建模

为DRM中的各个实体与实体之间的联系建立清晰和可扩展的模型是非常重要的，模型的基本原则是要清楚地确定三个核心实体：即用户、数字化信息内容和权利。

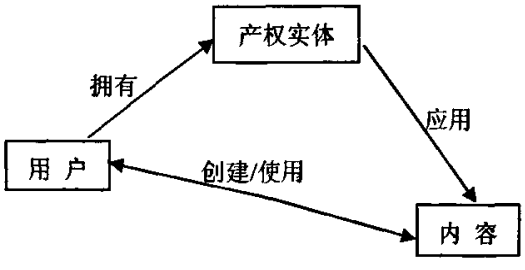


图 2-3 DRM信息结构-实体关系图

其中用户的类型是多样的，既可以是版权持有者，也可以是终端用户；内容则可以是任一集合层次上的任何形式的内容；权利实体是用户和内容之间各种许可、限制和义务的表示。三者的关系如上图 2-3 所示。

下面以内容为例，探讨下实体的具体建模方式。内容建模的基本原则是：内容包含了不同知识阶段(或发展演化阶段)的许多层次，如国际图联(IFLA)将内容确定为作品(Work)、表达(Expression)、体现(Manifestation)和款目(Item)四个层次，在每个层次上，都有不同的权利和权利支持者需要支持。DRM 信息结构的内容建模可以用图 2-4 表示。

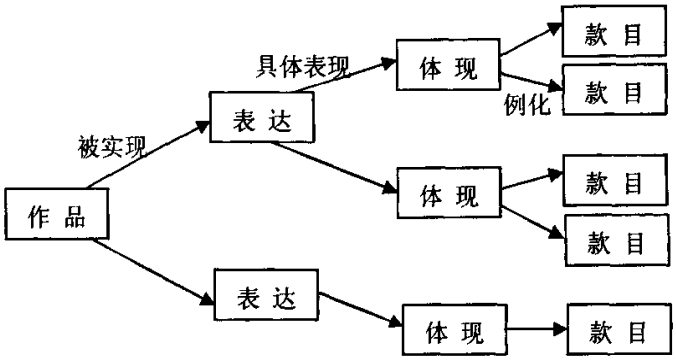


图 2-4 DRM 信息结构的内容模式

其中内容的作品层次是指明确的知识或艺术创造，表达层次是指一件作品的知识或艺术实现，这二者反映了学术性或创造性的内容；内容的体现层次是指一件作品表达的数字化体现，内容的款目层次是指一种体现的单一样本示例，这二者反映了物理或数字形式。比如说：曹雪芹的著作《红楼梦》，其内容、事实、思想、概念描述等属于作品层次；其表达层次则可能包括：曹雪芹的原始文本、原始文本的英译本、**的剧本改编等；而其中“英译本”表达的体现可能包括：X 出版社 2000 年出版的精装本、Y 出版社 1998 年出版的简易本、Z 出版社 2005 年出版的电子图书等；“图书”体现的款目则可以包括：从新华书店购买的精装本，从网上书店购买的数字化文件等。从这里可以看出：这个内容模式的重要一点就是在任何一点上都可以识别出权利拥有者。

2．实体的确认和描述

DRM 系统中的所有实体都需要加以确认和描述。应该通过系统中每个实体的开放标准机制来完成确认工作，无论是实体还是实体的元数据记录都必须是可确认的。开放标准主要有 Uniform Resource Identifiers(URI)和 DOI 等。

3．权利声明的表示

权利这个实体可以从许可、限制、义务和其他与用户和信息内容有关的权利信息等几个方面加以表示。权利实体的重要性在于它代表了一种用来联系权利元数据的语言表达。由于权利表示的复杂性会越来越高，因此也必须对这些表示进

行建模，以便理解这些权利表示之间的联系。权利表示可以由四个部分组成：许可(允许用户做的事情)、限制(对许可的一些制约)、义务(用户所必须做、提供或接受的事情)和权利持有者。权利声明的表示如图2-5所示。

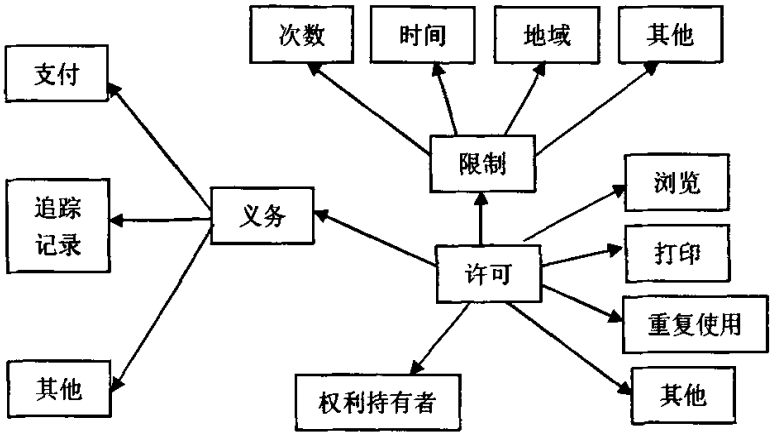


图 2-5 DRM信息结构-权利声明的表示

比如一份权利表示声明："一本电子图书的费用为30元人民币(支付义务)，在一个学期内(时间限制)可以最多被打印(使用许可)10 次(次数限制)，每次打印本书作者(权利持有者)将收到一定比例的提成"。通常如果某种权利在表示中不是很明确，就意味着没有被赋予这项权利。

2.3 DRM的主要技术原理

2.3.1 对称与非对称加密技术

加密的目的是保护信息不被非授权用户获取，加密可分为对称加密和非对称加密两种方式。

1．对称加密技术

对称加密采用了对称密码编码技术，它的特点是文件加密和解密使用相同的密钥，即加密密钥也可以用作解密密钥，这种方法在密码学中叫做对称密钥加密算法(也称块密码)。对称加密算法使用起来简单快捷、密钥较短，且破译困难。

由于在DRM系统中，数字内容跟解密密钥是分开发送的，即使用户将数字内容复制传送给其他人，新用户也无法打开数字内容，除非申请许可证获得解密密钥。而且对称加密算法非常快(相对于公钥算法)，特别适用于对较大的数据流执行加密转换。因此，在DRM系统中，一般采用对称密钥算法来加密数字内容。

常用的对称加密算法有：DES，3DES，RC2。

DES[10]算法的入口参数有三个：Key、Data、Mode。其中Key为8个字节共

64 位，是 DES 算法的工作密钥；Data 也为 8 个字节 64 位，是要被加密或被解密的数据；Mode 为 DES 的工作方式，有两种：加密或解密。DES 算法是这样工作的：在通信网络的两端，双方约定一致的 Key，在通信的源点用 Key 对核心数据进行 DES 加密，然后以密文形式在公共通信网(如电话网)中传输到通信网络的终点，数据到达目的地后，用同样的 Key 对密文进行解密。DES 对称密钥算法用于保密通信如图 2-6 所示。

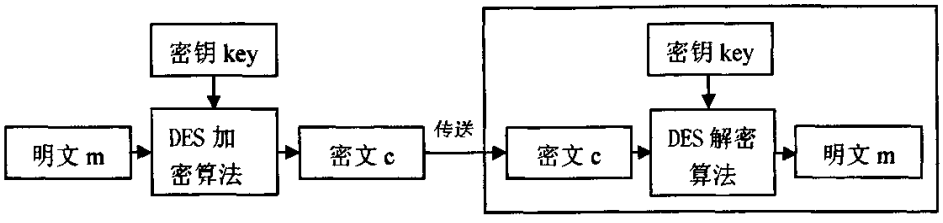


图 2-6 DES 加密机制

2．非对称加密技术

与对称加密算法不同,非对称加密算法需要两个密钥：公开密钥(public key)和私有密钥(private key)。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。

非对称加密算法的保密性比较好，它消除了最终用户交换密钥的需要，同时公钥算法可用于创建数字签名以验证数据发送方的标识，但加密和解密花费时间长、速度慢，因此它不适合于对文件加密而只适用于对少量数据进行加密。非对称加密通常用于加密一个私钥算法将要使用的密钥，传输密钥后，会话的其余部分将使用对称加密。

(1) 非对称密码体制

一个公钥(非对称)密码体制[11]由以下要素构成：

随机参数空间:R(Random)；

秘密密钥空间:PrK(Private Key)；

公开密钥空间:PuK(Public Key)；

明文空间:P(Plaintext)；

密文空间:C(Ciphertext)；

密钥生成算法:KeyGen(Key Generation) R->PrK&PuK；

加密算法:Enc(Encryption) PuK&P->C；

解密算法:Dec(Decryption) PrK&C->P；

对于任意 r∈R，x∈PrK，y∈PuK，m∈P，c∈C，若(x,y)=KeyGen(r),c=Enc(y,m)，则有以下两个条件成立：

① x 容易计算出 y,但是由 y 计算出 x 在计算上是不可行的;

② m=Dec(x,c)。

公钥体制用于保密通信如图 2-7 所示。

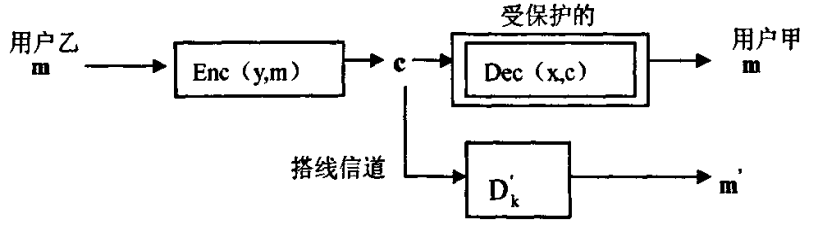


图 2-7 非对称密码算法的加密机制

图中假定用户乙要向用户甲发送机密消息 m。那么甲首先随机选择一个参数 $r\in R$，计算出 $(x,y)=KeyGen(r)$,并将 y 公开，将 x 作为自己的私钥。用户乙从公钥本上查到甲的公开钥 y 对消息 m 加密得到密文 $c=Enc(y,m)$，然后将密文送给用户甲。甲收到后用自己的秘密钥 x 对 c 进行解密变换得到原来的消息

$$m=Dec(x,c)=Dec(x,Enc(y,m))$$

系统的安全保障在于从公开钥 y 和密文 c 要推出明文 m 或解密密钥 x 在计算上是不可能的。“窃听者”只能知道密文 c 和公开密钥 y，但他不能根据 c 和 y 得到解密密钥 x，因而不能计算出明文消息。

(2) RSA 公钥密码体制

RSA[11]是一种常用的非对称加密算法：独立地选取两个大素数 p 和 q，n 为两素数之积即 n=pq，其欧拉函数值为 $\varphi(n)=(p-1)(q-1)$，随机选取密钥指数对 e，d，(其中 $1\le e\le\varphi(n)$ 且 $(\varphi(n),e)=1$)，使得 $ed=1\bmod\varphi(n)$。选取公钥为 e，秘密钥为 d(p,q 不再需要，可以销毁),RSA 体制的明文和密文空间均为 Z_n。

RSA 加解密算法：对于任何明文消息 $m\in Z_n$,加密算法为 $c\equiv m^e \bmod n$

相对应的解密算法为 $m\equiv c^d \bmod n$

RSA 数字签名算法：对于给定的消息 $m\in Z_n$，其数字签名为 $s\equiv m^d \bmod n$

相应的验证算法为：首先计算 $m'\equiv s^e \bmod n$，如果 $m=m'$ 就接受签名，否则拒绝。

RSA 公钥密码算法是目前网络上进行保密通信和数字签名的最有效的安全算法。RSA 算法的安全性基于数论中大素数模 n=pq 分解的困难性，所以，RSA 需采用足够大的整数，因子分解越困难，密码就越难以破译，加密强度就越高。

2.3.2 数字签名技术

签名与加密不同，签名的目的是使消息的接收者确认信息的发送者是谁、信息是否被他人篡改。数字签名[12-14]建立在公钥密码基础之上，采用私钥签名公钥验证的体制。数字签名基本原理[11]如图 2-8 所示。

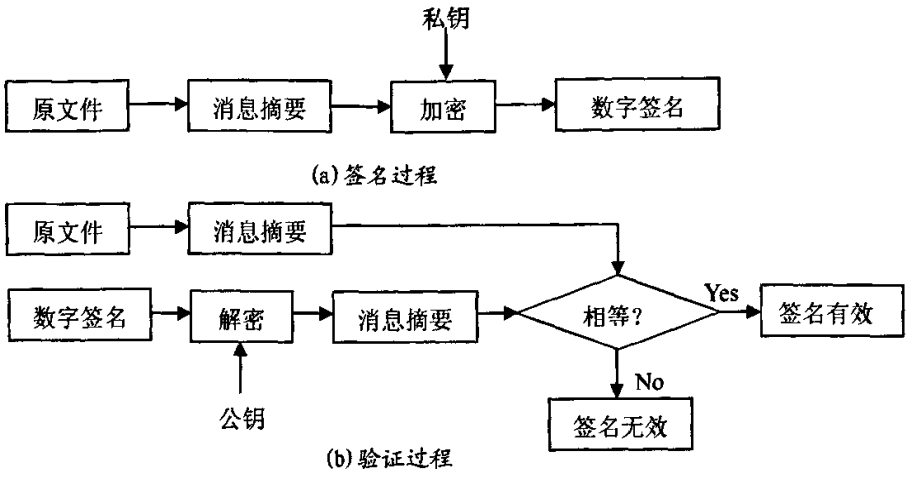


图 2-8 数字签名和验证过程

2.3.3 Hash 运算

1．什么是 Hash 函数

Hash 函数[15](也称杂凑函数)就是把任意长的输入消息串变化成固定长的输出串的一种函数，这个输出串为该消息的杂凑值。Hash 函数主要用于完整性校验和提高数字签名的有效性，一个安全的杂凑函数有以下特点：

(1) 输入长度是任意的；

(2) 输出长度是固定的，根据目前的计算技术应至少取 128bits 长；

(3) 对每一个给定的输入，计算输出即杂凑值是很容易的；

(4) 给定杂凑函数的描述，找到两个不同的输入消息杂凑到同一个值在计算上是不可能的；

(5) Hash 函数的输出并不以可辨别的方式依赖于输入，在任何输入串中单个比特的变化，将会导致输出比特中将近一半的比特发生变化。

2．MD5 信息－摘要算法

MD5 叫信息－摘要算法[16]，是一种 Hash 运算，它可以对任何文件产生一个唯一的 MD5 验证码，每个文件的 MD5 码就如同每个人的指纹一样，都是不同的。MD5 是一种不可逆的字符串变换算法。

(1) MD5 的典型应用

MD5 的典型应用是对一段 Message(字节串)产生 fingerprint(指纹)，以防止被“篡改”。比如：你写一段话在 readme.txt 文件中，并对这个文件产生一个 MD5 的值并记录在案，然后你将文件传给别人，别人对文件有任何修改你都可以通过重新计算 MD5 来发现，如果再有一个第三方的认证机构，用 MD5 还可以防止文件作者的“抵赖”，这就是所谓的数字签名应用。

MD5 还广泛用于加密和解密技术上。比如在 unix 系统中用户的密码就是以 MD5(或其它类似的算法)经加密后存储在文件系统中。当用户登录的时候，系统把用户输入的密码计算成 MD5 值，然后再去和保存在文件系统中的 MD5 值进行比较，进而确定输入的密码是否正确。这样系统在并不知道用户密码的明码的情况下就可以确定用户登录系统的合法性。

(2) MD5 算法简介

对 MD5 算法简要的叙述可以为：MD5 以 512 位分组(在信息后面填充一个 1 和多个 0，使其字节长度对 512 求余的结果等于 448，然后，在这个结果后面附加一个以 64 位二进制表示的填充前信息长度，经过这两步的处理，使得最终信息长度为 512 的整数倍)来处理输入的信息，且每一分组又被划分为 16 个 32 位子分组，经过了一系列的处理后，算法的输出由 4 个 32 位分组组成，将这 4 个 32 位分组级联后将产生一个 128 位散列值。

2.3.4 信息隐藏及数字水印技术

1．信息隐藏

信息隐藏[17]主要研究如何将某一机密信息秘密隐藏于另一公开的信息中，然后通过公开信息的传输来传递机密信息。可能的监测者或非法拦截者难以从公开信息中判断机密信息是否存在，难以截获机密信息。信息隐藏技术主要由下述两部分组成：

(1) 信息嵌入算法，利用密钥来实现秘密信息的隐藏；

(2) 隐蔽信息监测/提取算法(检测器)，利用密钥从隐蔽载体中检测/恢复出秘密信息。在密钥未知的前提下，第三者很难从隐蔽载体中得到、删除甚至发现秘密信息。

2．数字水印技术

数字水印[18-21]是信息隐藏研究领域一个重要的分支，该技术是通过在原始数据中嵌入秘密信息—水印(watermark)来证实该数据的所有权。这种被嵌入的水印可以是一段文字、标识、序列号等，而且这种水印通常是不可见或不可察的，它与原始数据(图象、音频、视频数据)紧密结合并隐藏其中，能够抵抗应用过程中的各种破坏，如数字信号处理技术，包括噪声、滤波和有损压缩等。

数字水印技术并不能阻止盗版活动的发生，但它可以判别对象是否受到保护，监视被保护数据的传播、真伪鉴别和非法拷贝、解决版权纠纷并为法庭提供证据。典型的数字水印系统模型如图 2-9 所示。图中(a)为通用水印信号嵌入模型，其功能是完成将水印信号加入到原始数据中；图(b)是通用水印信号检测模型，用以判断某一数据中是否含有指定的水印信号。

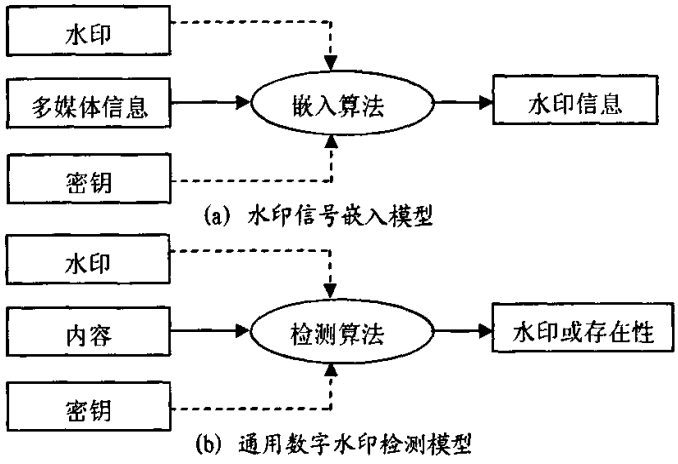


图 2-9 典型的数字水印系统模型

2.3.5 DRM 数字权限描述语言

数字权限描述语言[22](Digital Right Expression Language, DREL)用以指定给予用户(以及中间层实体，如发行商和图书馆)的许可集，以及可以行使这些许可的条件和义务。也就是说，数字权限描述语言准确定义和描述了谁拥有什么数字信息产品的什么权限，按照什么协议和交易方式将哪些权限在哪些范围授予给谁。这些信息必须用标准的、开放的和计算机可识别的方式描述和标记，DRM系统才能自动进行相应的记录、识别和解析，并据此进行权限控制。数字权限描述语言主要有XrML、MPEG-21 REL、ODRL等。

1．XrML—可扩展权限标记语言

XrML[23]是美国施乐公司帕拉阿图研究中心开发的一种有关对数字产品内容的使用权利、费用和条件以及有关适合电子出版形式的描述和标识语言。它是一种基于XML的语言，以简单和容易理解的方式，给出使用权利的基本概念定义，提供不同环境和不同应用的信用系统的要求，被用来标记数字产品的有关内容。此外，XrML还提供了有关的语义标签和元数据。

XrML可以应用于单篇作品或作品集，它规定了作品不同内容的有关使用权利，并加上其有关的元信息，包括是谁发布的、发布时间和向谁发布，以及数字签名等。

2．MPEG-21 REL(MPEG-21 的第五部分-数字权限描述语言)

MPEG-21 REL指明了对于一个数字资源(内容、服务等)来说，谁可以使用资源，他们可以使用的权限，以及行使资源所拥有的权限所需的条件或约束。MPEG-21 REL由核心集，标准扩展集和多媒体扩展集三部分组成：核心部分规定了一些基本元素的语义，定义了授权时所需的模式机制、变量机制以及授权算法；标准扩展部分定义了对所有数字资源都适用的权限、条件或约束；多媒体扩

展则定义了多媒体特定的一些权限、条款、条件或约束，扩展增强了核心的功能与适用性。第三方组织可以在此之上再定义适用于自己领域的扩展。MPEG-21 REL的体系结构如图2-10所示。

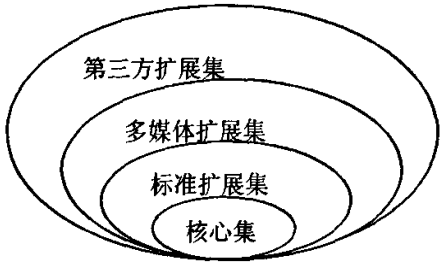


图 2-10 MPEG-21-REL 的体系结构

3．ODRL(开放的数字权限语言)

ODRL是DRM研究领域描述针对内容权限的语言，它旨在提供灵活地、可互操作的机制，以支持在出版、发行和消费电子出版物、数字媒体、音频、电影、计算机软件和其他数字资源时实现无障碍和创新的使用。它以XML作为语法，包括一组核心语法，这组核心语法包括权限持有者和对资源进行许可使用的表示。ODRL基于一种权限表达扩展模型，它包括大量核心实体以及实体间的关系。ODRL基础模型由三个核心实体组成，如图2-11所示。

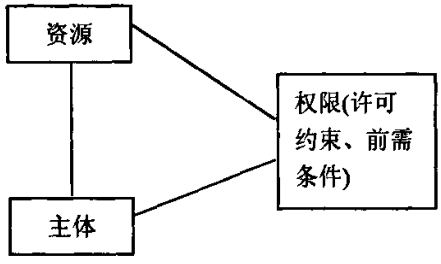


图 2-11 ODRL 的基本概念

(1) 资源：包括实物和数字化内容。一个资源必须被唯一认证，它可能由很多子部分组成，也可能有其他不同形式，也可能被加密以保证安全发布；

(2) 权限：包括许可，许可又包括约束、前需和条件。许可是在资源上被许可的实际用法或行为。约束是对许可的限制(如最多播放5次视频)。前需是为了执行而必须要完成的义务(如你每一次播放视频时，都要付5元)。条件指明例外，即如果例外为真，则许可过期，需要重新协商(比如信用卡过期，则所有的许可都不能播放视频)；

(3) 主体：包括终端用户和权限持有者。主体可以是人、组织或指定的角色。终端用户通常是资源的消费者,权限持有者通常是在资源的创建、生产和分发中扮演重要角色的团体，在资源和资源的许可上能断言的某种形式的拥有者。

2.3.6 唯一标识符技术

1．标识系统的组成

网络环境中的数字对象独立于应用协议和应用系统，往往存放于不同的数字资源库，需要通过唯一标识符予以一个唯一的标记。一般来讲一个标识系统由以下部分组成：

(1) 命名域：代表一定的标识系统，在该系统内遵循统一的命名规则和程序；

(2) 唯一标识符：在特定命名域内按一定规则给予数字对象的唯一和永久的名字，即URI的统一资源名；

(3) 命名机构：按照一定规则和权限管理命名过程的机构；

(4) 命名登记机构：存储命名登记数据的系统；

(5) 地址解析系统：负责将对象的唯一标识符转换成相应的物理存放地址。

2．数字对象标识符(DOI)

DOI[24-27](Digital Object Identifiers)是DOI系统中的唯一标识符，DOI系统是CNRI(美国国家研究推进机构)根据AAP(美国出版协会)的要求定制开发的系统，它是Handle系统在出版行业的应用,力图建立因特网环境下知识产权管理和保护的解决方案。DOI系统主要由标号体制、元数据、解析系统和政策框架四部分组成，本文简单介绍下DOI系统的标号体制与解析原理。

(1) DOI的标号体制

标号体制主要定义DOI唯一标识符的语法和语义问题，如图2-12所示。

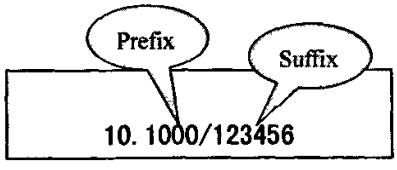


图2-12 DOI标识符的语法定义

DOI唯一标识符由前缀和后缀两个部分组成，前缀和后缀由“/”分隔。其中前缀是由DOI命名机构分配的号码，后缀是注册DOI机构的组织或个人对数字对象定义的本地标识符。一般DOI的注册者都通过在后缀中融入现有的唯一标识符如ISSN、ISBN或其他标识符来达到向下兼容。DOI的前缀又可以分为两个部分，两者用“.”分隔，其中“10”是一个常量字符，表示DOI是Handle系统的一个具体应用。前缀的后半部分由数字组成的字符串是IDE登记机构分配给DOI注册者的号码，如10.1045/april99-van_de_somepel-ptl。其中10为DOI系统的服务标识，1045是DLIB杂志注册后活动的机构代码，april99-van_de_somepel-ptl是DLIB杂志内部的记录号。

(2) DOI 解析过程

解析系统负责将用户提交的 DOI 唯一标识符解析成其他有用的信息，例如将 www.las.ac.cn 解析为对应的 IP 159.226.100.8，从而获得 DOI 标识的实体的网上地址。

DOI 的解析原理是这样的：在一个数字对象发布或发布前，出版商赋予其一个唯一和永久的标识符，并将标识符和数字对象的地址信息嵌入 DOI 系统。当用户查询某一 DOI 标识的数字化对象时，系统就在其数据库中查找该 DOI，然后将与 DOI 相关的数字对象的信息返回。如果数字对象变更名称或移动位置，其所有权人负有更新数据的权利，以确保解析结果的正确。比如每一篇文章都有唯一的 DOI 标识,每一个 DOI 对应一个 URL,出版机构将论文的元数据和 DOI 存放在数据库中，当用户点击引文时,检索系统将请求发送到数据库中,由系统解析器对其进行解析,找到对应 URL，然后将参数转发到相应的电子期刊系统中，找到原文。

一个 DOI 可以解析为任何其他的信息，比如多个 URL、其他的 DOI 或者能够标识实体特征的元数据。DOI 的解析结果可以被进一步处理或供用户选择处理。早期的解析是将一个 DOI 标识符解析成一个 URL，目前 DOI 的解析逐渐趋向一对多解析，即一个 DOI 对应多个数字化对象，并且根据预设的要求或使用权限自动引导用户访问一个或多个相关对象(服务)。其解析过程如图 2-13 所示。

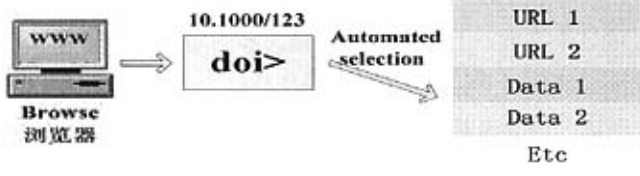


图 2-13 一对多解析示意图

2.4 DRM 技术的特点

所有的 DRM 应用都是基于“信息记录”的[2]。记录里面包括了合法版权所有者的情况和基本版权信息。这些情况或信息是通过元数据(Metadata)、版权管理信息(Rights Management Information，简称 RMI)或数字对象标识符(Digital Object Identifiers，简称 DOI)来实现的。

2.4.1 元数据(Metadata)

元数据[28-29]是保存特定信息的数据段，它是一种描述数据本身基本特征和属性的数据，又称为“数据的数据”。从本质上来说，元数据是一种数据结构标准，它提供了一种框架体系和方法来描述、表征数字化信息的基本特征，并通过一套

通用的编码规则，将来源各异的数字化资源归纳到一个统一的体系中。

1．元数据结构

一个Metadata格式由多层次的结构予以定义：

(1) 内容结构(Content Structure)：内容结构定义Metadata的构成元素，可包括：描述性元素、技术性元素、管理性元素、结构性元素(例如与编码语言、命名空间、数据单元等的链接)。

(2) 句法结构(Syntax Structure)：句法结构定义Metadata格式结构及其描述方式，例如元素的分区分段组织、元素选取使用规则、元素描述方法、元素结构描述方法、结构语句描述语言等。有时，句法结构需要指出元数据是否与所描述的数据对象捆绑在一起、或作为单独数据存在但以一定形式与数据对象链接，还可能描述与定义标准、DTD结构和命名空间等的链接方式。

(3) 语义结构(Semantic Structure)：语义结构定义Metadata元素的具体描述方法。例如描述元素时所采用的标准、最佳实践或自定义的描述要求。

2．元数据编码语言

编码语言指对元数据元素和结构进行定义和描述的具体语法和语义规则，即定义描述语言(DDL)。随着元数据格式的增多和互操作的要求，人们开始采用一些标准的DDL来描述元数据，其中以XML(可扩展的标记语言)最有潜力。

3．元数据互操作性

由于不同的领域甚至同一领域往往存在多个元数据格式，当在用不同元数据格式描述的资源体系之间进行检索、资源描述和利用时，就存在元数据的互操作性问题(Interoperability)。解决元数据互操作性的一种思路是建立一个标准的资源描述框架，用这个框架来描述所有元数据格式，那么只要一个系统能够解析这个标准描述框架，就能解读相应的Metadata格式。实际上，XML就能起着这样的作用。XML通过其标准的DTD定义方式，允许所有能够解读XML语句的系统辨识用XML_DTD定义的Metadata格式，从而解决对不同格式的释读问题。

2.4.2 个性化和颗粒性

个性化是指根据用户要求，对作品大小、格式、内容进行剪裁，同时打上可见的个人水印。比如说，一个教学课件包括了许多书籍和杂志的文章，并会注明哪段来自于哪本书的哪个章节、作者是谁等等。这样读者就可以很方便地查找原始素材。因此只要做法得当，个性化是个非常有效的方式。

颗粒性是用来描述DRM系统对信息的细分能力。一个目标信息能够细分到多小的模块，这些模块又如何被其他创作者和制作人使用来创作新作品？颗粒性使得创作开发人员能高效低成本地选择、组合新的或已有的视音频、平面素材用

来创作新的作品。比如说，一个教师要创作一个课件，他购买了一本参考书的一章或一页，又购买了10秒的一段录像，然后他利用购买来的这些东西创作了自己的新电子课件。如果所有这一切由DRM系统提供，那么就需要DRM系统既要把老师需要的内容正确的发送出去，同时又要以预先设定的方式赋予这些内容必要的权限，以保证其版权。

2.4.3 DRM系统的兼容性

在商业环境中，创作者、生产商、发行商需要互相沟通。制作人和使用者需要频繁地在不同场合使用不同来源、不同格式的作品资源，这就需要DRM系统具有较强的兼容性。在系统兼容性方面开发的工作包括：数字对象标示符 DOI和版权表述语言(Rights Expression Languages)，其中版权表述语言是为了表述使用数字内容的法律条款，现在有很多形式的表述语言，这些语言具有通用性，可以被用在网站、文本文件、图片、音乐、PDF文档和流媒体中。这些表述语言中比较有名的是Open Digital Rights Language Initiative(ODRL)和Extensible Rights Makeup Language(XrML)。

2.4.4 易用性

要使DRM系统能够被采纳，必须使合法用户能够轻松方便地使用这个系统，嵌入在元数据中的技术控制手段不能让用户觉得别扭，同时还需要帮助合法消费者能够快捷地访问自己需要的内容，而不用再填写额外的表格。在大多数情况下，除非用户企图访问未授权的内容，否则他们一般不会感觉到DRM系统的存在。虽然用户的访问受到了控制，但对合法的用户而言，DRM应该是透明的。

2.4.5 付费系统

DRM能够提供的付费方式有好几种。因特网上最普遍的付费方式是用信用卡来付费，不过使用信用卡需缴纳高额的银行手续费，甚至有时手续费比所购买的商品价值还高。由于网上单次交易额通常不会很大，因此DRM需要开发新的付费方式来应对大量的小额交易，哪怕只有几毛钱。

1．预付费

预付费，也称订阅服务。用户需要在信用卡上预先缴纳一笔费用，用户享受服务一直到卡上的钱用完为止。然后用户需要继续缴纳费用。预付费系统容易维护，成本低廉,它的缺点是用户不知道卡上的钱什么时候用完；另一个缺点是预

付费系统一般是按照用户使用时间或信息量来收费，销售商无法将营业收入与用户浏览过的内容联系起来，除非系统详细记录了这方面的信息。

2．累计付费

顾客每次访问系统所产生的费用被累计起来，只有达到一定额度时才被要求付费。也就是先享受服务，然后付费。这与信用卡消费的观念是一致的。这种方式的缺点是对那些偶尔使用系统的顾客来说，通常会无限期的拖延付费。

3．付费中心

付费中心采取集中化管理来处理所有销售商的预付费和累计付费账单，这样就避免了顾客需要向多家销售商缴费带来的烦恼，同时也可以有效处理大量的小额交易。付费中心可以将顾客在不同地方、不同形式的消费，包括累计消费、预付费、甚至超市购物费用累计起来并通知，用户在适当的时候一次性缴纳。这样就避免了多次小额付费产生附加的运营成本。

4．电子货币

电子货币是以金融电子化网络为基础，以商用电子化机具和各类交易卡为媒介，以电子计算机技术和通信技术为手段，以电子数据(二进制数据)形式存储在银行的计算机系统中，并通过计算机网络系统以电子信息传递形式实现流通和支付功能的货币。现阶段电子货币的使用通常以银行卡(磁卡、智能卡)为媒体。电子货币通常在专用网络上传输，通过POS、ATM机器进行处理。

建立电子货币系统，可以大大减少银行信用卡系统高额的运行成本，带给顾客更多实惠，虽然在理论上，已经有好几种电子货币系统可行，但还没有一个成功的商业范例。对于它的发展，我们拭目以待。

2.5 基于移动代理的DRM系统模型

2.5.1 DRM系统模型

DRM系统[30]主要的组成实体包括有：数字产品内容提供商(Content Provider)、DRM服务器(DRM Server)、用户客户端(Consumer Client)。

内容提供商将原有的数字产品进行压缩加密形成DRM系统支持的媒体文件格式，并在数字内容中嵌入完整性数字水印，然后将处理后的数字内容分发给用户，受保护的数字内容可以通过在线或离线的方式分别进行分发；此外，内容提供商还负责把加密的密钥交给DRM服务器。

DRM服务器负责管理用户的许可证。具体操作包括为用户定制数字产品许可证、验证用户身份、为合法用户提供解密密钥。

用户客户端软件需要进行的工作有：验证用户许可证有效性、验证用户是否有正

确的解密密钥，在安全的机制下解密数字产品，对数字内容进行播放和使用。

2.5.2 移动代理技术

移动代理[31-33](Mobile Agent)是一种能够携带代码、数据及执行状态在网络中根据既定的路线在主机间迁移并能够在新的位置从断点处继续执行的程序。它是一种功能相对独立的可执行程序，可以自主地在异构的网络上按照一定的规则移动，寻找合适的计算资源、信息资源，代表用户完成特定的任务，并返回相关结果。

在具体实现中，用户或代理中心向网络中发出一个(或多个)移动代理，该代理依据用户预定义的路线或由代理自己确定的节点路线在网络中漫游，并动态地收集资源或与各服务器交互计算以完成任务。最终，移动代理回到用户或代理控制中心，并带回收集的数据或交互结果。

1．移动代理系统的组成

一般情况下，一个Mobile Agent系统至少应该包含Mobile Agent和Mobile Agent Server两部分。Mobile Agent通过Mobile Agent server实现其在网络上的移动和相应动作；而Mobile Agent server为Mobile Agent 的移动和执行提供必要的执行环境以及相应的安全管理和服务调用等功能或服务。目前，已应用于实际中的典型移动代理平台有IBM的Aglets等。

2．移动代理的特点

(1) 移动性：移动代理可以在运行期间直接进行主机间的迁移，即可以从一个节点采集所需要的数据后，不终止进程而直接迁移到另一个节点继续运行，保留了原来的进程的数据段；

(2) 智能性及低网络数据流量：移动代理可以实时对所采集到的数据进行过滤，将关键数据提出，而不需像传统的代理体系那样，将各个主机的所有数据都汇集到一个中央服务器中进行处理，然后再向相关的代理转发，减少了网络负荷；

(3) 协作性：相同代理之间可以实现相互协作，一旦有代理失效，其他代理可以弥补转移到该代理的主机进行失效弥补，此外，异种代理之间也可以进行互补性合作，多个不同功能的代理协作完成共同目标；

(4) 跨平台性：移动代理通常采用与平台无关的语言，这样的程序可以跨平台运行；同时一般的移动代理体系都建立了与移动代理相配套的平台无关的通信协议，通过这些协议，代理之间无须建立直接的通信连接。

2.5.3 基于移动代理技术的DRM系统模型

1．基于移动代理的DRM系统框架

改进的基于移动代理的DRM系统框架包含三个实体：数字产品内容提供商(Content Provider)、DRM服务器(DRM Server)、用户客户端(Consumer Client)。

在基于移动代理技术的DRM系统中设计了两种移动代理，一种“用户移动代理”，称为Agent，主要完成内容的安全传输；一种“数字水印代理”，实现水印跟踪及检测，因此改进的系统增加了新的功能，其结构模型如图2-14所示。

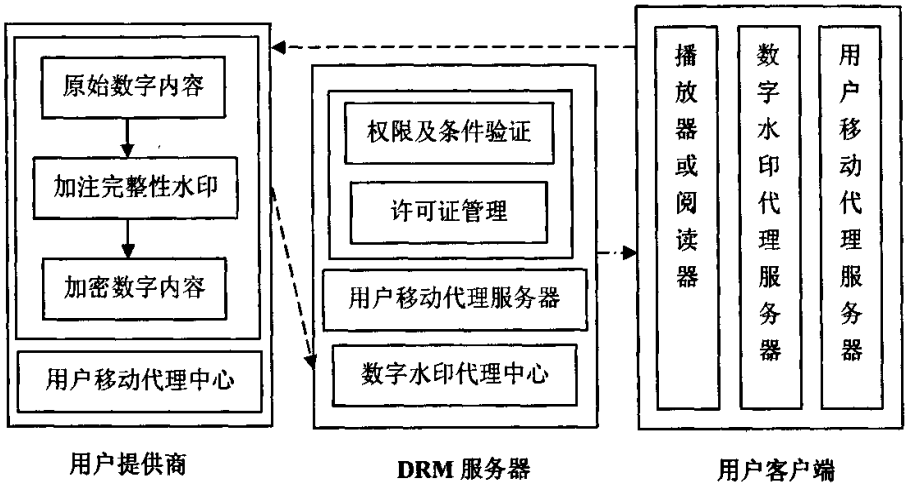


图2-14 基于移动代理的DRM系统模型

(1) 用户提供商部分：新增了用户移动代理中心，移动代理中心负责派遣Agent，收集处理Agent返回的报告信息、产生代理的路由策略以及根据代理的返回结果生成对数字内容的控制策略等；

(2) DRM服务器部分：新增了用户移动代理服务器和数字水印代理中心。用户移动代理服务器为移动代理的移动与执行提供环境，并为其提供相应的安全管理及服务调用；水印代理中心产生水印代理以实现数字水印的跟踪与检测；

(3) 用户客户端部分：新增了数字水印代理服务器与用户移动代理服务器，为相应移动代理的执行提供环境及安全管理。

2．基于移动代理技术的DRM系统工作流程

在基于移动代理技术的DRM系统中，其主要工作流程是这样的：

(1) 首先假设内容提供商、DRM服务器、用户的公私钥分别为(y_1,x_1),(y_2,x_2),(y_3,x_3),enc为加密算法，dec为解密算法。当用户选择好要购买的数字内容时，用户与内容提供商之间首先要达成某种协议m，协议中规定用户对数字内容的使用权限、期限及相关的条件等，同时协议上还可存储一些相关的信息，

如数字内容的版权信息、内容的描述、支付条款、费用、用户及内容提供商的身份信息等，用户对协议以自己的私钥签名 sig(m)=enc(x_3,m),而内容提供商对协议加密 C=enc(y_1,m),加密后的协议 C 构成“用户移动代理”的一部分，然后内容提供商的移动代理中心派遣“用户移动代理”，称为 Agent；

(2) Agent 携带用户已签名的协议 sig(m)等信息，从内容提供商处携带受保护的数字内容移动到 DRM 服务器，DRM 服务器首先验证用户签名的有效性，dec(y_3,sig(m))=dec(y_3,enc(x_3,m))=m,然后验证用户使用权限及期限的有效性。若验证通过，DRM 服务器则生成许可证 L(包括用户使用权限、期限、条件及数字内容的解密密钥)，将许可证 L 与受保护的数字内容一起打包形成打包文件 m_1，同时 DRM 服务器对许可证进行 hash 运算，得到一个 hash 值 h，服务器对打包文件 m_1 和 h 签名 sig(m_1+h)=enc(x_2,m_1+h),构成 Agent 的一部分，同时在代理中嵌入完整性数字水印以防止终端用户篡改使用权限。此时数字水印代理中心派遣出“水印代理”，称为 watermark Agent；

(3) Agent 携带服务器的签名 sig(m_1+h)迁移到用户客户端，客户端先验证许可证有效性：第一步：验证签名 dec(sig(m_1+h))=dec(y_2,enc(x_2,m_1+h))= m_1+h；第二步：提取许可证 L，将其进行与 DRM 服务器一样的 hash 运算，得到 h_1，若 h_1=h，则许可证有效，客户端提取解密密钥，按照规定的权限控制用户对内容的使用。

3．数字水印代理的工作流程

数字水印代理主要完成的工作有：从水印代理中心移动到用户主机，寻找用户主机上需要检测的文件，从需要检测的文件中抽测水印并检测，恢复出水印并读出水印中嵌入的信息，如版权所有者、拷贝次数等，并和代理自身携带的水印版权策略相比较，判断是否相等，如果相等则返回报告给代理中心，不相等则说明有侵权行为，水印代理根据侵权情节的严重性给予主机警告或直接删除文件等处分，接着代理向代理中心以 Email 形式发送报告。最后水印代理自我复制，并根据代理中心的路由策略确定下个主机的地址，由水印服务器向该主机发送代理复制品，继续完成网络中的水印跟踪与检测任务。水印代理也可根据需要由一台主机移动到另外的主机。

每个代理通常带有版权拥有者一个或多个密钥来检测与版权者相关的水印。一个代理中心可以分派多个代理,各个代理完成不同版权者或不同作者的水印检测任务,这由水印代理所携带的密钥决定。水印代理的工作流程如图 2-15 所示。

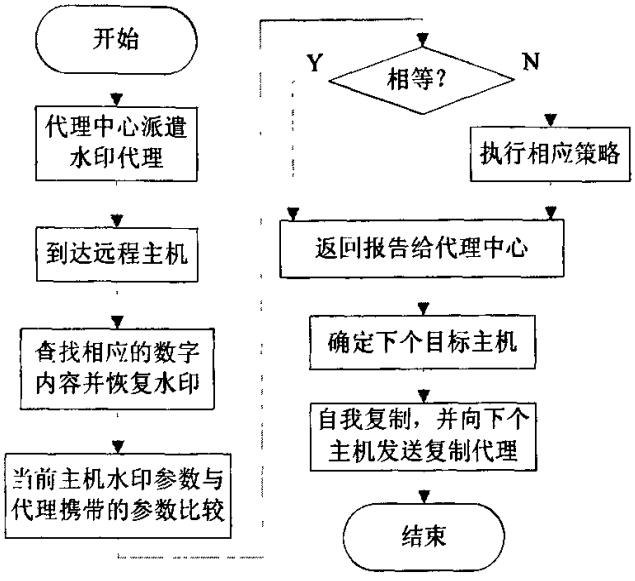


图 2-15 水印代理工作流程

4. 系统使用移动代理的优点

系统中利用移动代理可以在运行期间直接进行主机间的自主迁移特性，可减少 DRM 各个实体之间协商的时间，并可避免实体与实体间的直接接触，加速了处理过程。

系统将许可证和数字内容一起构成代理的一部分，并在代理中嵌入完整性数字水印，完成客户端的验证及数字内容的使用等工作，简化了工作流程，也给用户带来了很大的方便；同时系统使用水印代理跟踪，能及时有效地发现用户的侵权行为。

2.6 DRM 在 eBook 版权管理中的应用

数字版权管理技术已广泛应用于电子图书[34-35]、数字图书馆[36-38]、软件保护、远程教育、电子文档[39]、流媒体、数字电视[40-42]、移动增值业务[43-44]等领域。本节介绍 DRM 在 eBook 版权管理中的应用。电子书的 DRM 系统可以分为两类应用：一类是通过网上的书店直接面向读者销售，如国外的 Amazon 网站、eReader 网站，国内的中文电子书网、易文网等；另一类是通过数字图书馆，给读者提供借阅的服务，如国外的 netLibrary、国内的方正 Apabi 系统。

首先，eBook 是 electronic book 的缩写，可直译为电子图书。通常来说，eBook 有两个层面的含义[45]。其一，它是网络时代的新生产物，是以互联网为流通渠道、以数字内容为流通媒介、以网上支付为主要交换手段的一种崭新的信息传播方式，是基于网络为基础的图书的出版和发行方式；其二，eBook 是专用硬件阅

读器的简称。如国外最早推出的 Soft Book 和 Rocket Book。

2.6.1 基于 DRM 的 eBook 管理系统

基于 DRM 的 eBook 管理系统在结构上采用的是 C/S 模式[46]，如图 2-16 所示。服务器端是 DRM 服务器，主要负责权益的创建管理和 eBook 内容的加密；客户端是 eBook 阅读器，主要完成 eBook 内容的解密、相关权限的验证和内容的解析展示。用户的权限在 DRM 服务器端被加密包装，以授权证书的形式下载到客户端。授权证书的内容由用户的权限描述和相关电子书的解密密钥组成，并被加密封装。在客户端，eBook 阅读器对证书解密，验证其中的用户权限是否合法，如果合法，则对电子书进行解密，用户才能阅读。

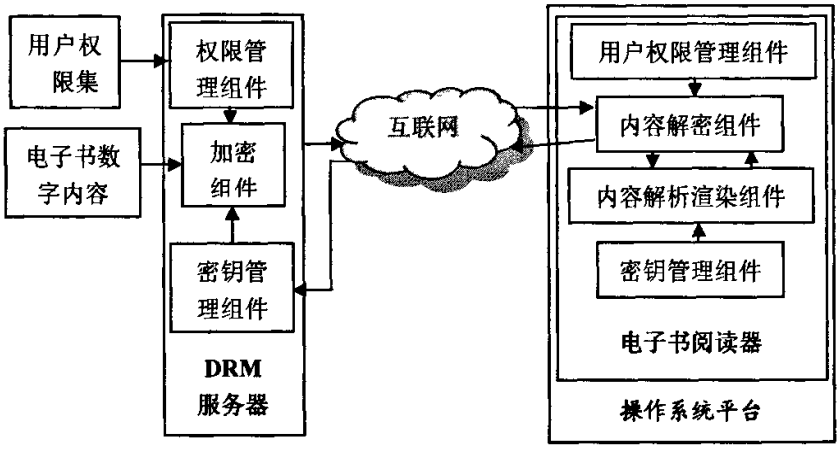


图 2-16 基于 DRM 的 eBook 管理框架

2.6.2 eBook 阅读器的实现

目前，国内和国外开发的电子书阅读器种类比较多，国内比较有影响的有超星阅读器和北大方正的 Apabi[5]，国外的有 Adobe 公司的 eBook Reader，Microsoft 公司的 Microsoft Reader。

在欧美国家，eBook 的发展正在逐步走向规范化。在 eBook 格式统一标准方面，虽然目前尚没有能够形成统一的格式，PDF、OEB、HTML 等 eBook 格式都有相应的市场，但 OEB 的建立为格式统一提供了可能。OEB 是美国商业部、标准技术院等十几家公司机构为了统一文件格式、规范发展电子书市场而推出的一种行业标准。我国的北大方正已经正式加入 OEB 组织，成为其正式成员之一。OEB 的文档结构格式[27]如图 2-17 所示。

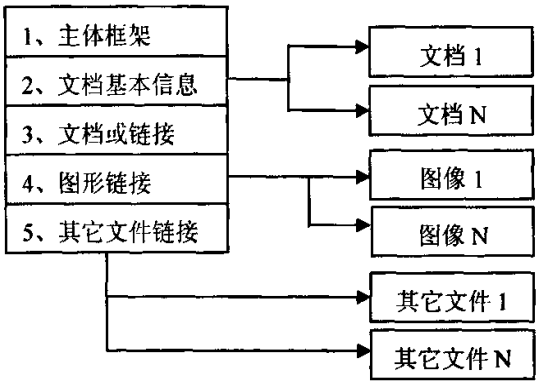


图 2-17 OEB 文档结构格式

因此在电子书阅读器的格式上，一般采用国际上通用标准 OEB 规范 1.1 作为电子书的内容格式标准。由于 OEB 格式包含的文件是以链接的形式存在，比较分散，如图 2-17 所示。于是把这些文件进行编码合并到一起，形成一个统一的文件，这样不仅便于进行存储压缩，而且更有利于实现版权保护。

而在显示技术上采用了子像素技术，它通过将单个像素能量扩展到邻近像素的方法，来弥补显示设备能力不足而对图像显示造成的粗糙，从而给读者在阅读上提供一种舒适的感觉；在功能上，电子书阅读器可以选择拷贝文件、对段落进行标记、放大和缩小字体；在安全认证上，Apabi、Adobe 和 Microsoft 都采用电子书认证证书的方式来保护电子书的安全，通过电子认证证书把电子书和用户身份信息、用户权益相绑定，安全性高得多。

电子书阅读器的内部功能框图[46]如图 2-18 所示。密钥管理组件用来生成本机的机器硬件指纹；证书管理组件完成证书验证、计算解密密钥和解密用户权益集；用户权益管理组件用来验证用户权益的合法性并确保其得到贯彻；内容解密、解析组件用来解密电子书内容并进行语法解析；内容渲染引擎用来将解析后的电子内容显示到输出设备上。

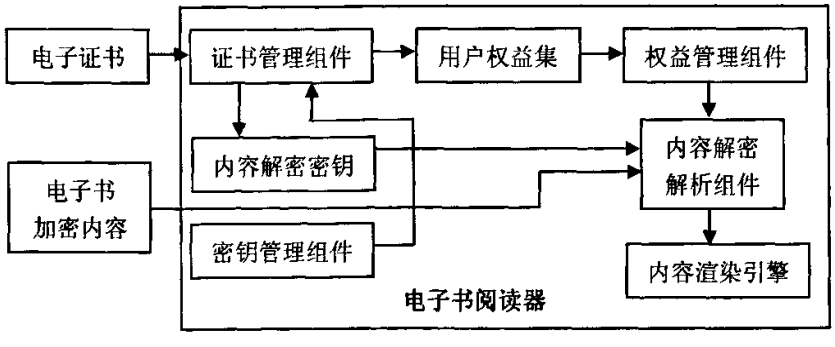


图 2-18 电子书阅读器内部结构

将DRM技术与电子书阅读器相结合，可以从技术上解决制约电子书发展的两大瓶颈问题：数字版权保护困难与数字化内容阅读的不方便，预示着电子书出版发行市场将走向成熟。

2.6.3 基于椭圆曲线与机器指纹的电子书认证算法

对于eBook的DRM系统，电子书内容的提供商要将数字内容传送到一个不能保证安全的用户环境。为了能在这种不可信任的环境下保证数字内容的安全，DRM系统只能依靠在客户端用户环境下运行的组件(即电子书阅读器)来实现。该组件将确保数字内容拥有者的权益得到保障，并使得用户所赋予的权利得以充分实现。电子书阅读器不仅仅用来显示电子书，而且还通过电子认证证书保障电子书的安全和用户权益的实现。

eBook的DRM系统提供给每个用户的电子书都有相应的电子证书[46]。电子证书由数字签名和用户权益信息组成。数字签名用来验证电子证书的合法性。电子书的内容和用户权益信息都被加密保存。

目前采用的电子书认证算法都基于RSA数字签名，但RSA密钥大，运算速度相对较慢，而椭圆曲线数字签名[47-49]具有密钥小、参数规模小、运算速度快及安全性高的特点，同时结合机器硬件指纹，可以唯一地标示用户主机，具有更高的安全性。

1．参数设置

(1) F(q),E,P,l,h.其中F(q)是有限域，E是F(q)上的椭圆曲线，P是E上的一个有理点，称为基点。P的阶为l(l为素数)，H是一个单向*hash*函数；

(2) 系统有一个私钥$x_0 \in \{1,2,...l-1\}$，公钥是$P_0 = x_0 P$；

(3) hkey是客户机的机器硬件指纹，它由客户机的CPU序列号、主板信息、硬盘序列号、网卡序列号等硬件信息组成，是一个长度约为300多位的大整数；

(4) m是用户的身份信息，b是电子书的序列号，它们都是一个32位整数。

2．生成电子证书数字签名的基本算法

(1) 电子书阅读器将hkey、m、b提交到DRM服务器，服务器计算：

$$ID = H(hkey, m, b) \qquad \text{公式(2-1)}$$

ID就是电子证书的标识号，这个标识号是用户身份和机器硬件信息、电子书序列号的绑定，且是唯一的。

(2) 服务器随机选择一个整数$k \in \{1,2,...l-1\}$，计算$kP = (x,y)$，然后计算：

$$r = x \bmod l \qquad \text{公式(2-2)}$$

$$s = k^{-1}(ID + rx_0) \bmod l \qquad \text{公式(2-3)}$$

则(r,s)就是电子证书的签名。

3．验证签名

在客户机端，电子书阅读器将本机的 hkey 以及用户信息 m、电子书序列号 b 做如下运算：$ID_1 = H(hkey,m,b)$,并计算：

$$u = s^{-1} ID_1 \bmod l \qquad \text{公式(2-4)}$$

$$v = s^{-1} r \bmod l \qquad \text{公式(2-5)}$$

然后计算：$(x_1, y_1) = uP + vP_0 = s^{-1} ID_1 P + s^{-1} r P_0 = s^{-1}(ID_1 P + r P_0)$

由于 $s^{-1} = k(ID + rx_0)^{-1} \bmod l$，$P_0 = x_0 P$ 所以上式变为：

$$(x_1, y_1) = k(ID + rx_0)^{-1}(ID_1 P + rx_0 P) = kP(ID + rx_0)^{-1}(ID_1 + rx_0)$$

这样只有当 $ID = ID_1$ 时，才满足 $(x_1, y_1) = kP = (x, y)$ 公式(2-6)

这样 $r_1 = x_1 \bmod n = r$ 公式(2-7)

从而证实了该签名的有效性，也就证明了该电子证书签名确实是由本机硬件信息产生的。

由于电子书的认证与机器的硬件指纹相关，当电子证书被拷贝到其他机器上，就会验证失败，这就有效防止了电子书的非法复制与二次传播。

4．方案安全性分析

(1) 椭圆曲线的离散对数问题

椭圆曲线离散对数问题ECDLP是指:给定有限域上 F(q) 的椭圆曲线 E，设 $P = kG, G \in E(F_q)$,由给定的 P 和 G 确定出 k。有限域上椭圆曲线的离散对数问题是比有限域上的离散对数问题困难得多的问题。

(2) 安全性分析

在本方案中，攻击者要由 $P_0 = x_0 P$ 求解私钥 x_0 时，要面临着椭圆曲线上的离散对数问题；攻击者要想从签名信息中求解出随机数 k，也同样面临着椭圆曲线的离散对数问题。因此，该方案具有很高的安全性。

2.7 本章小结

DRM技术是现在和今后的研究热点，本章主要对DRM技术及其特点进行了分析和研究；然后介绍了DRM的系统模型，并结合移动代理技术，提出了一种改进的DRM系统模型；最后详细介绍了DRM技术在电子书版权管理中的应用，并提出了一种结合椭圆曲线与机器硬件指纹的电子书认证算法。

第三章 基于DRM的电子书在线销售系统的总体设计

3.1 系统方案设计

3.1.1 引言

20世纪90年代以来，数字化技术的飞速发展，使得大量的书籍资料转化为电子书的形式成为可能，而网络技术的发展也为电子书的发展起了巨大的推动作用，它使得电子书的复制和传播变得越来越方便和迅速，但同时也带来相应的版权问题。无论是网络书店还是在数字图书馆系统的建设过程中，都需要解决以下两个问题[46]：

1．如何将电子书安全地交到客户手中；

2．如何防止客户得到的电子书被非法(未经授权)的复制和传播。

3.1.2 系统设计目标

电子书在线销售系统将DRM技术引入电子书的加密管理及用户身份验证，是为了实现电子书的版权保护，以保护出版商、创作者等各方面的权益。本系统设计一个简单的电子书在线销售系统，主要实现以下几个功能：

1．对电子书内容打包加密

本系统中，版权商(或版权拥有者)首先将电子书打包，然后采用DES加密算法加密打包过的电子书，并存放在服务器中；

2．RSA加密字符串

当用户购书的款项已经到位后，版权者使用RSA加密由DES解密密钥(即电子书内容密钥)、电子书的使用权限与期限构成的字符串，并将密文存放在数据库中；

3．获取客户机的机器指纹

机器指纹由客户机的硬盘序列号和网卡号组成，用来唯一标示客户机，实现身份验证。用户订购一本电子书时，首先获得该书的序列号，然后使用自己的账号(新用户先注册)登录成功后进行获取本机机器密码的操作，此时服务器自动获取客户端本机的MAC地址，同时客户端提示用户是否下载ActiveX插件来获取本

机硬盘序列号，如果客户选择是，则服务器通过ActiveX插件自动获取本机硬盘序列号，并将硬盘序列号与MAC地址一起做hash运算形成机器指纹存放在数据库中；当版权者收到用户购书的款项后，用户就有了下载该电子书的权限，此时系统自行计算用户机器的机器指纹，并与之前存在数据库中的机器指纹相比较，如果相等，则证实该用户身份合法，可以下载电子书，不相等，则不能下载，以确保电子书只能在客户本机上下载；

4．生成 XML 格式的许可证文件

当用户有了下载电子书的权限时，服务器即自动生成XML格式的许可证文件(包含RSA加密的电子书解密密钥、用户设置的使用电子书的权限及期限)；

5．许可证有效性验证

当电子书及许可证书被下载到本地后，服务器首先对许可证进行椭圆曲线数字签名，具体算法见2.6.3，并将其传到客户端，客户端先验证签名的有效性，若有效，再判断许可证是否有效。

许可证验证由电子书阅读器内置软件完成，它同样使用机器指纹在客户端验证许可证的有效性，以确保用户只能在本机阅读该电子书，这样即使把电子书与许可证文件传递给其他任何一台机器，由于不能通过机器指纹的验证，也无法阅读，除非重新付费申请许可证，这样就能保障该电子书离线后的版权不受到侵犯；

6．使用移动代理跟踪用户对电子书的使用情况

当用户购买并下载电子书后，服务器派遣移动代理到用户主机，监测用户电子书的使用情况，判断其是否有擅自拷贝、修改等侵权行为，并能根据不同程度的侵权行为执行相应的策略。

3.2 系统的工作模式

系统采用 B/S 开发模式，可以使得运行维护比较简便，能实现不同的人员，从不同地点，以不同的接入方式(比如 LAN, WAN, Internet/Intranet 等)访问和操作共同的数据。它的优势在于用户的工作界面是通过 IE 浏览器来实现的，用户界面完全通过 WWW 浏览器实现，一部分事务逻辑在前端(Browser)实现，但是主要事务逻辑在服务器端(Server)实现，形成所谓 3-tier 结构，如图 3-1 所示。

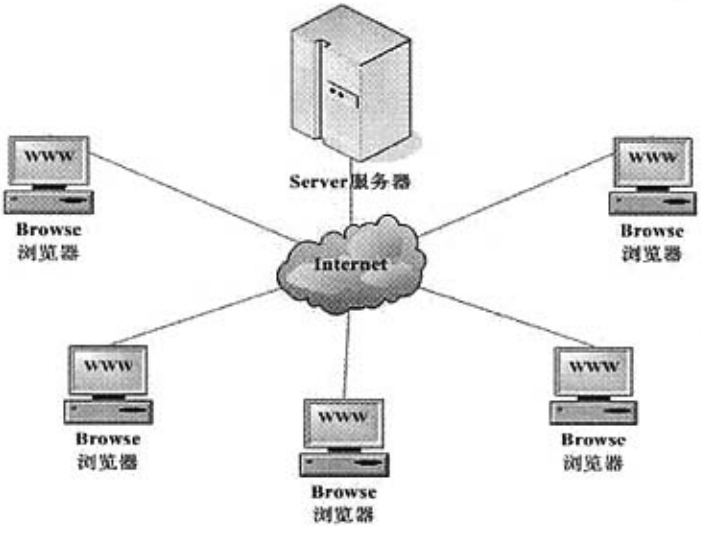


图 3-1 浏览器/服务器模式图

3.3 系统开发工具及运行环境

本系统既可以运行在局域网环境中，也可以运行在广域网环境下，其客户部分可运行在通用的PC上，服务器部分可运行在通用的中高档PC服务器上。

操作系统：

客户端：Windows 2000，Windows XP及以上操作系统；

服务器：Windows 2000 Server。

数据库系统：

客户端：不需要数据库；

服务器：SQL Server 2000

开发环境：Microsoft Visual Studio .Net 2003

3.4 系统总体设计

基于DRM的电子书在线销售系统分为服务器端与客户端。服务器端的主要任务是对电子书进行打包、加密，发布电子书的基本信息，发送许可证、发送加密的电子书；客户端的主要任务是验证许可证，识别并打开加密的电子书，并控制用户按照规定的权限使用电子书。在本系统中主要实现服务器端的设计，并给出了客户端许可证的有效性验证流程，同时系统提出了使用移动代理实现跟踪电子书使用情况的方案，该方案有待进一步研究。

3.4.1 服务器端工作流程

服务器端的流程是首先对电子书进行打包加密，上传至本地服务器，然后将电子书信息发布到门户网站，供用户选择购买。用户选择好要购买的电子书并付费，当版权者收到购书的款项，系统就通过机器指纹验证用户身份的合法性，若用户身份合法，则服务器根据用户的购买权限和使用期限生成XML格式的许可证，此时用户可下载电子书及许可证；若用户身份不合法，则提示其没有权限下载电子书及许可证。其工作流程如图3-2所示。

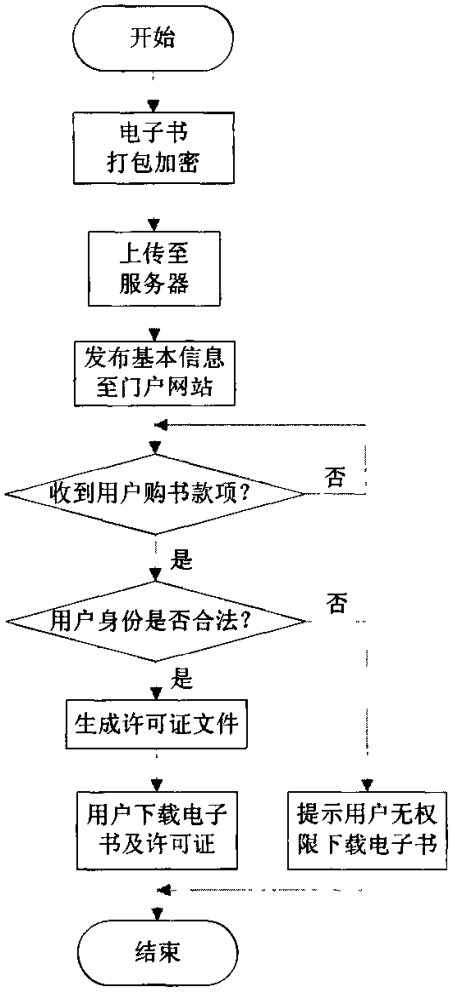


图 3-2 服务器端工作流程图

3.4.2 用户购书流程

用户购买电子书的流程是这样的：

1．用户登录门户网站，选择自己需要的电子书；

2．用户设置好使用权限及使用期限后，点击订购此书，提示订购成功后，获得此次订购交易的序列号；

3．如果是新用户，则用户输入序列号后，再输入姓名、密码、Email 等信息进行注册，注册完后登录，如果是已有账号的用户可直接登录；

4．用户登录成功后，在列表中选择自己要买的书购入，然后用户进行获取本机机器密码的操作，获得本机的机器指纹，并存入数据库中。此时用户还没有下载电子书的权限，用户需及时将购书的款项汇给版权者；

5．用户登录门户网站，若版权者已收到用户的购书款项，则用户可进行下载操作，此时系统自动计算机器指纹，并与数据库中的机器指纹相比较，相等则证明该用户身份合法，这时用户才能将电子书与许可证下载到本机上；否则，提示用户无权限下载电子书及许可证。

其工作流程图如图 3-3 所示。

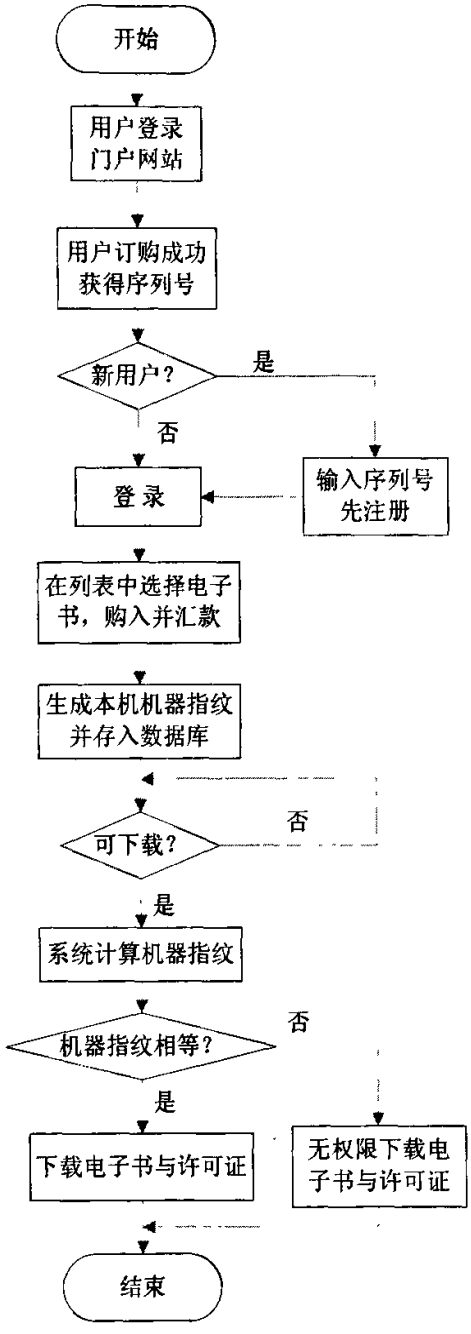


图 3-3 用户购书流程图

3.4.3 基于椭圆曲线及机器指纹的许可证有效性验证流程

当电子书及许可证被下载至客户机后，客户端在打开电子书时需先验证许可证的有效性。客户端的许可证验证的流程如图 3-4 所示。其中，客户端第一次运行的时候生成空的许可证文件 Licence.dat 和签名文件 Signature.dat，Licence.dat

用于存放下载下来的XML许可证，而Signature.dat用于存放服务器对许可证形成的数字签名(签名基于椭圆曲线与机器指纹)。

1．客户端在阅读电子书时，首先打开Licence.dat查找对应电子书的许可证是否存在；

2．若许可证存在，则打开Signature.dat，提取出签名字符串；

3．验证签名，判断签名是否有效；

4．若签名有效，则说明该许可证是合法的，此时解析许可证，判断其使用期限是否在有效的时间范围内，从而判断许可证的有效性；

5．若许可证有效，则可提取电子书内容的解密密钥，解密、打开并按照规定的权限阅读该电子书。

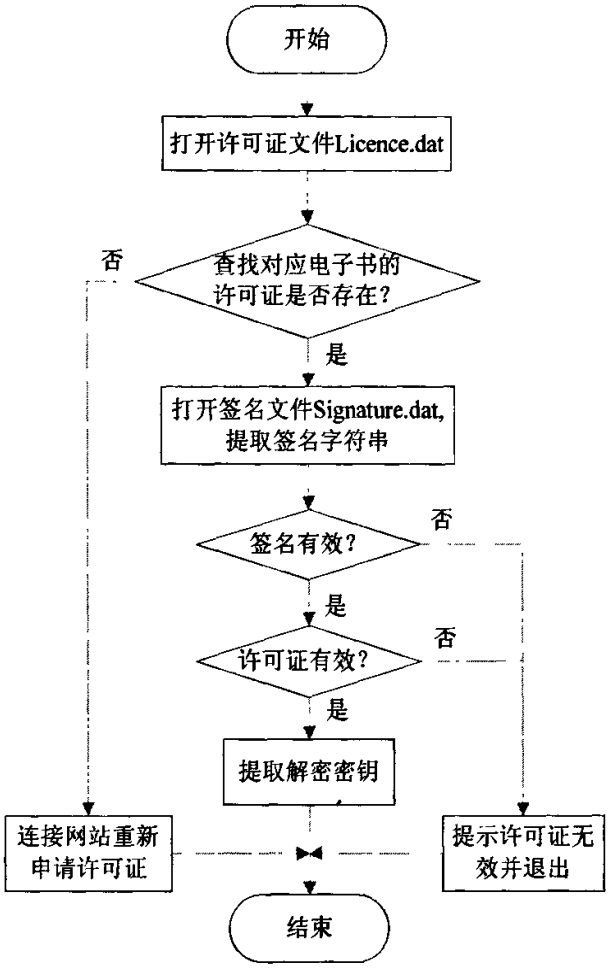


图 3-4　许可证验证流程

3.4.4 基于移动代理的使用权限跟踪流程

系统可使用移动代理实现对电子书使用情况的跟踪，代理主要跟踪监测电子

书的使用权限，及时发现用户的侵权行为，并执行相应策略，其工作流程图如图3-5所示。

1．首先服务器派遣移动代理到用户主机；

2．用户每次打开电子书，代理即开始监测用户的使用情况；

3．移动代理将用户使用情况与自身携带数据相比较，判断其是否有侵权行为；如果没有，则继续监测用户；如果发现用户有非法拷贝、修改、复制等侵权行为，则代理根据服务器提供的策略对主机进行相应的处理。

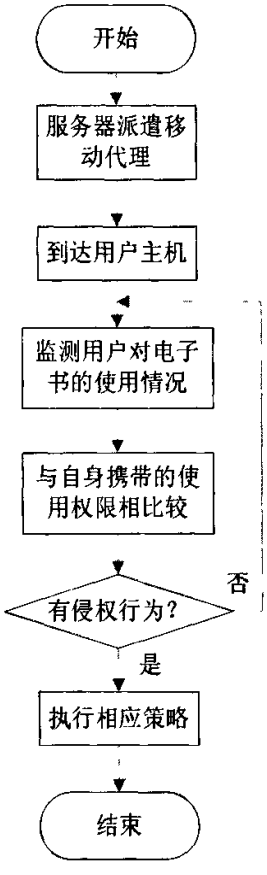


图 3-5　移动代理工作流程

3.5 数据库表结构

本系统采用SQL Server 2000作为数据库服务器，数据库中有下面几个表：

1．用户信息表U-USERINFO

用户信息表用来登记用户基本信息以及相应的购买记录。其中购买序列号LONGID对应用户一次的购买记录，是唯一的，它由电子书的ISDN号的hash 值+购买电子书的时间+8位随机数组成；而机器密码MACHCODE是指将用户的硬盘序列号与MAC地址组成的字符串进行hash运算后所产生的hash值。

表 3-1 U-USERINFO 表

字段名称	类型	说明	示例
NAME	Vchar	用户姓名	hf
PWD	Vchar	用户密码	111
LONGID	Vchar	购买序列号	73a861e51228b59820070116014838375QW3FVMQ1
EMAIL	Vchar	电子邮箱	hufang8209@yahoo.com.cn
LOGINTIME	Vchar	注册时间	2007-01-16
MACHCODE	Vchar	机器密码	cfa1f6efee52339c9cf42feafb0e0d12

2. 电子书登记表 U-BOOKDETAIL

电子书登记表用来登记每本电子书的详细信息，同时也包含了该电子书的 DES 加/解密密钥(密钥随机生成)以及打包加密后的电子书的文件名(文件名中加入时间标志以区分不同时间上传至服务器的电子书)。

表 3-2 U-BOOKDETAIL 表

字段名称	类型	说明	示例
LONGID	Vchar	购买序列号	73a861e51228b59820070116014838375QW3FVMQ1
ISDN	Vchar	电子书的 ISDN	7-81094-730-3
BOOKNAME	Vchar	书名	亲密接触 ASP.NET
BOOKFROM	Vchar	出版社	清华大学出版社
BOOKDATE	Vchar	电子书上传日期	2000-01-12
BOOKFILE	Vchar	加密后的电子书名	20070118105843453.rar
DESKEY	Vchar	DES 加/解密密钥	N73KPIOP

3. 购书记录表 U-BOOKBUY

购书记录表用来登记用户的购书信息，其中包括用户设置的阅读权限(在这里，只设置了只读、可打印、可打印(可读))和使用期限，通过 ISDN 跟 U-BOOKDETAIL 表关联、LONGID 跟 U-USERINFO 关联，对应一次唯一的购买记录。

表 3-3 U-BOOKBUY

字段名称	类型	说明	示例
ISDN	Vchar	电子书的 ISDN	7-81094-730-3
PRI	Vchar	使用期限	三月
DAT	Vchar	使用权限	可打印(可读)
LONGID	Vchar	购买序列号	73a861e51228b598200701160201203 59H7SISRRJ

4. 表 U-BYTE

表 U-BYTE 包含两个字段：LONGID 和 BYTECRY。其中 LONGID 对应一次购买记录，而经 RSA 加密的字符串，以字节形式存放在 Image 类型的 BYTECRY 字段里，且此字段在数据库中是不可见的。

表 3-4 U-BYTE

字段名称	类型	说明	示例
LONGID	Vchar	购买序列号	73a861e51228b5982007011602012 0359H7SISRRJ
BYTECRY	image	RSA 加密密文	

3.6 本章小结

本章主要介绍了基于 DRM 的电子书在线销售系统的总体设计，分析了其设计目标、设计模式、运行环境及主要的工作流程，并给出了数据库中的表结构。本系统中主要实现电子书在线销售过程中版权保护的关键技术，其中包括加密、签名、硬盘绑定(机器指纹)、hash 运算等，在下一章中，将详细介绍各种关键技术的实现原理及过程。

第四章 一个简单的基于DRM的电子书在线销售系统的实现

本系统主要设计并实现一个简单的电子书在线销售系统，并引入DRM技术以实现电子书的数字版权管理。本章主要介绍系统中实现的关键技术，其中包括DES对称加密技术、RSA非对称加密及数字签名、MD5运算、ActiveX技术等。

系统总体可分为2个子系统：电子书销售管理子系统和版权管理子系统。其中电子书销售管理子系统主要实现对用户信息进行录入、对电子书打包加密以及发布电子书基本信息等功能；而版权管理子系统主要实现许可证文件的生成、发放与管理、用户身份认证、权限跟踪管理等功能。

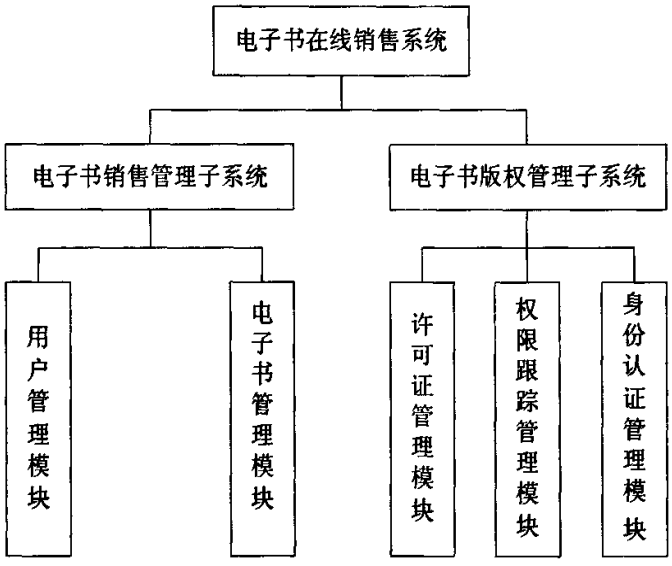


图 4-1 电子书在线销售系统模块图

4.1 电子书管理模块

系统管理员首先将电子书打包，然后采用DES加密，并将加密后的电子书上传至本地服务器，然后在数据库中录入电子书的基本信息，再将电子书基本信息发布至门户网站以供用户浏览并选择购买。

4.1.1 电子书的加密及录入

在加密电子书之前，首先使用 winrar 将电子书打包，才能加密。加密后，再输入电子书的 ISDN、书名、出版社、出版日期等信息，进行上传。将加密后的电子书传至服务器，并将电子书的基本信息存入数据库的表 U-BOOKDETAIL 中，然后发布至门户网站，电子书的加密及录入界面如图 4-2 所示。

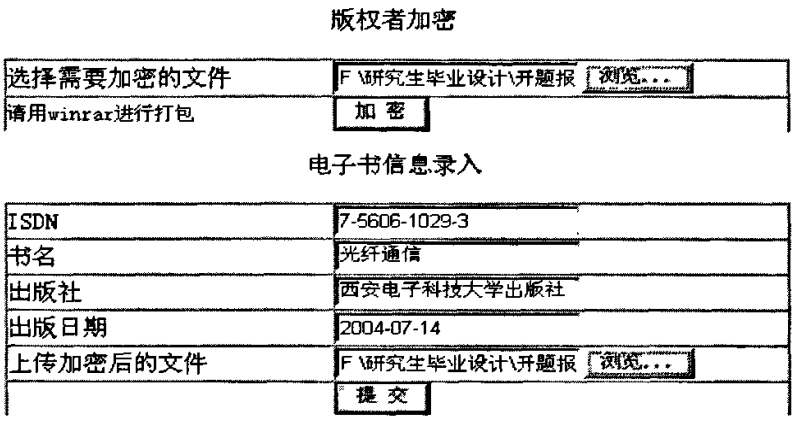


图 4-2 电子书加密及录入界面

4.1.2 DES 加密电子书内容

DES 是一种对称密钥算法，也就是说加密密钥和解密密钥是一样的，DES 密钥为 8 位，一般用来加密比较大的数据。这里采用 C#实现 DES 加密和解密，系统采用.NET Framework 提供的对称加密 DESCryptoServiceProvider 类来实现对电子书内容的加密操作。

1．DES 八位随机密钥的产生

DES 的八位密钥是随机生成的，这里调用了 GetRandom(int length)函数，用于生成随机数，length 指生成随机数的长度，其代码如下：

```
public static string GetRandom(int length)
    {
        string result = "";
        string include = "ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789";
//随机数在26个字母及10个阿拉伯数字中产生
        Random random = new Random();
        for (int i = 0; i < length; i++)
        {
            result += include[random.Next(0, 35)].ToString();
        }
        return result;
    }
```

2．DES 加密内容的实现

DES 加密调用 DesEncrypt()函数，其中参数 m_InFilePath 指文件的输入路径，m_OutFilePath 指文件的输出路径，strEncrKey 指加密密钥。对文件进行 DES 加密的主要代码段如下：

(1) 将 DES 加密密钥及初始化向量转换为字节形式：

```
byte[] byKey=null;
byKey=System.Text.Encoding.UTF8.GetBytes(strEncrKey.Substring(0,8));
byte[] IV= {0x12, 0x34, 0x56, 0x78, 0x90, 0xAB, 0xCD, 0xEF};
```

(2) 指明文件的输入和输出路径：

```
FileStream fin = new FileStream(m_InFilePath, FileMode.Open, FileAccess.Read);
FileStream fout = new FileStream(m_OutFilePath, FileMode.OpenOrCreate,
FileAccess.Write);
```

(3) 为读写数据创建临时变量，并创建 DES 算法的加密类：

```
fout.SetLength(0);                  //创建变量来读和写
byte[] bin = new byte[100];         //以字节数组作为加密的中间存储器
long rdlen = 0;                     //设置总共的写入字节数
long totlen = fin.Length;           //设置加密文件的总长
int len;                            //设置一次写入的字节数
DES des = new DESCryptoServiceProvider();  //创建 DES 加密类
```

(4) 使用类 DESCryptoServiceProvider 的 CreateEncryptor 方法创建一个加密转换接口，参数 byKey 为 DES 密钥，IV 为初始化向量，并创建 CryptoStream 对象将数据流连接到加密转换的流：

```
CryptoStream encStream = new CryptoStream(fout, des.CreateEncryptor(byKey,
IV), CryptoStreamMode.Write);
```

(5) 读取输入文件，加密并输出，然后关闭所有的流文件：

```
while(rdlen < totlen)
    {
        len = fin.Read(bin, 0, 100);
        encStream.Write(bin, 0, len);
        rdlen = rdlen + len;
    }
        encStream.Close();
        fout.Close();
        fin.Close();
```

4.2 用户管理模块

在用户管理模块中，主要实现用户的账号管理及用户购书的整个流程管理。用户注册登录门户网站，浏览各类电子书的基本信息，选购自己所需要的电子书。用户在选购电子书时，将获得电子书序列号，记录此次交易，同时系统将计算机器指纹，存入数据库中。

4.2.1 电子书查询及订购

用户打开门户网站，可浏览或查询自己所需要的书籍进行选购，用户查询电子书的界面如图 4-3 所示。用户可输入书名或 ISDN 号等进行查询，点击购买按钮，即进入订购页面。

图 4-3 电子书查询界面

如图 4-4 所示，在订购页面里，用户设置好对该电子书的阅读权限(本设计只设置了只读、可打印和可打印(可读)三种权限)和使用期限(本设计简单设置为一个月、三个月、一季或一年)，点击订购此书，系统将出现“订购成功，您的订购序列号是*********”的提示框，点击确定，将获得此次交易的序列号，如73a861e51228b59820070129041954078EUVZGTGP。序列号由电子书的 ISDN 的 MD5 值+购书的时间+8 位随机数组成，标示唯一的购买记录(可区分不同用户在同一时段买同一本书)，如图 4-5 所示。

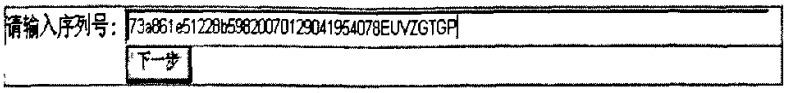
图 4-4 电子书订购界面

图 4-5 获取订购序列号界面

4.2.2 用户注册及登录

用户获得购书的序列号后，如果是新用户，则首先输入序列号注册用户账号，然后登录，如果是已有账户的用户则直接进行登录，用户注册界面如图 4-6 所示。

请输入购买序列号,进行注册



用户注册

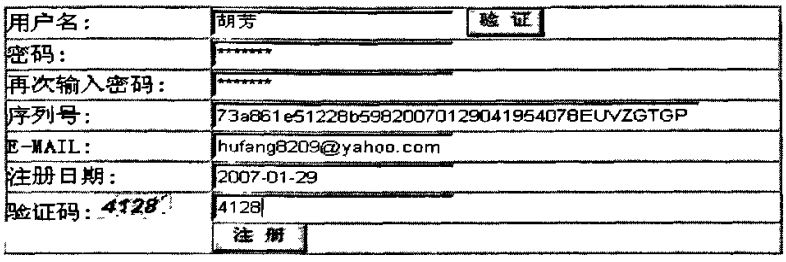


图 4-6 用户注册界面

4.2.3 用户购买 eBook

用户注册成功后，登录门户网站，此时用户可看到以往的购书清单，点击购入新书，输入之前获得的序列号，清单中将出现此次购买的新书，用户点击机器密码，在系统提示下生成机器密码(用于之后下载电子书时的身份认证)，此时用户可看到该书对应的“下载”按钮呈灰色，说明用户此时还没有权限下载该电子书，只有当网络书店收到购书的汇款并完成用户身份认证(将在后文详细介绍)后，用户才可下载，至此用户才完成购书的全过程。

图 4-7 用户购书界面(a)

图 4-7 用户购书界面(b)

如图 4-7(b)所示，书编号为 7-5606-1027-2 的电子书为此次购买的书籍，点击机器密码按钮，系统提示获取机器密码成功后，即可获取本机硬盘序列号与

MAC 地址，如图 4-8 所示。同时系统自行根据硬盘序列号与 MAC 地址计算机器指纹存入数据库中，用户可查看本机硬盘序列号及 MAC 地址，此时用户即可汇款给网络书店。

图 4-8 获取硬盘序列号及 MAC 地址界面

4.3 RSA 加密权限及密钥字符串

4.3.1 用户购书情况查询

用户购书的时候设置了该电子书的阅读权限及使用期限，服务器将该电子书的阅读权限和使用期限以及 DES 解密密钥组成的字符串进行 RSA 加密，加密后的密文以字节形式存放在数据库中，而 RSA 加密的密钥对则以 XML 格式存放。如图4-9所示，系统管理员在用户列表中可以查看每个用户的购书清单，如图4-10所示为用户名为“胡芳”的购书清单，当网络书店收到该用户汇来书编号为7-5606-1027-2 的款项后，即可点击加密按钮进行 RSA 加密操作，点击详情可以查看该电子书的基本信息：ISDN、书名、出版社、出版日期。

图 4-9 用户列表界面

书编号	阅读权限	阅读期限		详细
7-5606-1029-3	可打印(可读)	三月	加密	详情
7-5606-1028-1	只读	一季	加密	详情
7-5606-1027-2	可打印(可读)	一年	加密	详情
1				

图 4-10 某用户购书清单界面

4.3.2 RSA 加密字符串

由于 RSA 加密算法使用两个非常大的素数来产生公钥和私钥，因此其运算速度比较慢，通常用于加密字符串，本设计中采用 RSA 加密由电子书的解密密钥、电子书的使用权限和使用期限所构成的字符串。系统采用.NET Framework 提供的公钥加密算法类 RSACryptoServiceProvider 来实现。

RSA 加密：密钥以 XML 形式保存，加密后的内容以字节形式保存在表 U-BYTE 的 image 字段里，其主要的代码段如下：

1．获取需要加密的字符串 strCry，即唯一序列号对应的电子书对应的 DES 密钥及对该电子书的阅读权限和使用期限：

```
int i =e.Item.ItemIndex;
string strSel = "select DESKEY from U_BOOKDETAIL where LONGID
='"+DataGrid1.Items[i].Cells[0].Text+"'";
DataSet ds=new DataSet();
SqlDataAdapter MyAdapter = new SqlDataAdapter(strSel,MyConn);
MyAdapter.Fill(ds);
string strCry = ds.Tables[0].Rows[0][0].ToString()+"-"
    +DataGrid1.Items[i].Cells[1].Text+"-"+DataGrid1.Items[i].Cells[2].Text;
```

2．初始化RSA,然后保存密钥至XML文件：

```
RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
string PPKeyXml=rsa.ToXmlString(true);        //以XML的格式保存私钥
string PKeyXml=rsa.ToXmlString(false);        //以XML的格式保存公钥
```

3．导入公钥，加密字符串：

```
RSAParameters rsaParamsExcludePrivate=rsa.ExportParameters(false);
rsa.ImportParameters(rsaParamsExcludePrivate);          //导入公钥
byte[] DataToEncrypt = System.Text.Encoding.Default.GetBytes(strCry);
byte[] EncryptedData=rsa.Encrypt(DataToEncrypt,false); //公钥加密
```

最后，加密后的密文以字节形式存入表U-BYTE的image字段。

而对于RSA解密，则首先从XML文件中读取密钥，再读出字节格式的密文，最后使用私钥对密文解密。解密是加密的逆过程，代码不再赘述。

4.4 硬盘序列号的获取

4.4.1 ActiveX插件技术

1．ActiveX插件定义

根据微软权威的软件开发指南MSDN(Microsoft Developer Network)的定义，ActiveX插件以前也叫做OLE控件或OCX控件，它是一些软件组件或对象，可以将其插入到WEB网页或其它应用程序中。

2．ActiveX插件特点

在因特网上，ActiveX插件软件的特点是：一般软件需要用户单独下载然后执行安装，而ActiveX插件是当用户浏览到特定网页时，IE浏览器即可自动下载并提示用户安装。 ActiveX插件安装的一个前提是必须经过用户的同意及确认。

3．浏览器如何保证ActiveX插件的安全性

当通过Internet发行软件时，软件的安全性是一个非常引人注意的问题，对于ActiveX插件的安装显然涉及到一个安全性问题，IE浏览器通过以下的方式来保证ActiveX插件的安全：

(1) ActiveX使用了两个补充性的策略：安全级别和证明，来追求进一步的软件安全性；

(2) Microsoft提供了一套工具，可以用它来增加ActiveX对象的安全性；通过Microsoft的验证代码工具，可以对ActiveX插件进行签名，这告诉用户你的

确是控件的作者而且没有他人篡改过这个控件。为了使用验证代码工具对组件进行签名，必须从证书授权机构获得一个数字证书，证书包含表明特定软件程序是正版的信息，这确保了其他程序不能再使用原程序的标识。证书还记录了颁发日期，当您试图下载软件时，Internet Explorer 会验证证书中的信息，以及当前日期是否在证书的截止日期之前。如果在下载时该信息不是最新的和有效的，Internet Explorer 将显示一个警告；

(3) 在 IE 默认的安全级别中，ActiveX 插件安装之前，用户可以根据自己对软件发行商和软件本身的信任程度，选择决定是否继续安装和运行此软件。

4.4.2 发布 GetDiskKeyNo 控件获取硬盘序列号

本系统中引用名为 GetDiskKeyNo 的 ActiveX 插件获取硬盘序列号，该控件能够读取用户登录所用微机的硬盘序列号并进行加密后随表单信息一同传送至服务器，与服务器数据库内的值相比较，用户名、密码、序列号都符合，则验证通过，从而限制了一个合法用户只能在一台客户机上登录，防止了信息资源流失。由于 WEB 服务器端获取本机的硬盘序列号会受到安全方面的限制，客户端脚本(如 JavaScirpt)是无法有权限获取本机的硬盘序列号的，而服务器端的 C#更是无法实现获取本地硬盘序列号的功能。因此需要使用 getdiskkeyno.ocx 的 ActiveX 插件，该控件的作用是使用户下载到本机上，提取出本地的硬盘序列号将其编码后以一定的格式输出。

具体实现：该 ActiveX 插件存放在服务器端，并且在需要使用该控件的页面中使用以下代码调用该 ActiveX 插件：

1．将已生成的 GetDiskKeyNo 控件拷贝到 Web 服务器的一个目录下，本设计是拷贝至 DRM\Drm\getmachinecode 下；

2. 在 Web 服务器中 DRM\Drm\getmachinecode 文件夹中建立 Login.asp 登录页面引用该控件，源码摘要如下：

```
<OBJECT id="GetDiskKey"
codeBase="http://192.168.1.86/getdiskkeyno.ocx#version=1,0,0,17" height="6"
width="6" classid="clsid:CBF07105-2110-11D5-BBD1-00A0C99041D3"
VIEWASTEXT> </OBJECT>
```

以上 Codebase 的值是分发控件的路径、控件名和控件版本号。

使用之前，需设置客户机 IE 浏览器的安全特性，在“可信站点”中加入发布控件站点的 URL 地址，并允许启用该站点的 ActiveX 控件，否则浏览器将拒绝执行 GetDiskKeyNo 控件程序。安全站点设置界面如图 4-11 所示。

图 4-11 安全站点设置界面

用户在设置了安全站点后，访问需要调用ActiveX插件的页面时，作为可信任站点会出现友好提示是否调用该ActiveX插件,即需要经过本地用户的同意后才可以下载该控件。

经过用户的同意后，则下载该 ActiveX 插件到本地，自动获取硬盘序列号。硬盘序列号在 Login.asp 页面通过以下代码获得：

```
//得到硬盘序列号的值:
<script language="VBScript">
  sub tj_onclick()
    a=document.t1.smw.value
    document.t1.getdiskkey.sm=a
    document.t1.smw.value=document.t1.getdiskkey.keyno
  end sub
</script>
```

4.5 机器指纹

机器指纹即本地机器密码，机器指纹由本机硬盘序列号及网卡号经 MD5 运算得到。在 4-2-3 节用户购书过程中需点击机器密码以生成本机机器指纹存入数据库，机器指纹的作用主要是为了实现用户身份验证和许可证有效性验证。

4.5.1 获取 MAC 地址

在使用 ActiveX 插件获取本机硬盘序列号的同时，系统自行获取本机网卡

号。系统引用 Iphlpapi.dll Windows IP 辅助 API 应用程序接口，inet_addr()函数通过引用该 DLL 来使用。ws2_32.dll 是 Windows Sockets 应用程序接口，用于支持 Internet 和网络应用程序，SendARP 函数通过引用该 DLL 来使用。

函数说明：inet_addr()用来将参数 cp 所指的网络地址字符串转成网络所使用的二进制的数字。网络地址字符串是以数字和点组成的字符串，如 192.168.0.236 返回值 ：成功则返回对应的网络二进制的数字，失败返回-1；SendARP 函数用以获取指定 IP 的网卡 MAC 地址。

```
[DllImport("Iphlpapi.dll")]
private static extern int SendARP(Int32 dest,Int32 host,ref Int64 mac,ref Int32
length);
[DllImport("Ws2_32.dll")]
private static extern Int32 inet_addr(string ip);
```

1．获取网卡号的主要代码段：

```
string userip=Request.UserHostAddress;                    //获取远程客户端地址
Int32 ldest = inet_addr(userip);                          //将IP地址转换成二进制
Int64 macinfo = new Int64();
Int32 len = 6;
int res = SendARP(ldest,0, ref macinfo, ref len); //得到二进制数值的网卡号
string mac_src=macinfo.ToString("X");
string mac_dest="";
```

2．将 16 进制的 MAC 地址以"-"连接的形式显示, 如"00-0C-76-11-7C-EC"

```
for(int i=0;i<11;i++)
{
    if (0 == (i % 2))
        {
            if ( i == 10 )
                {
                    mac_dest = mac_dest.Insert(0,mac_src.Substring(i,2));
                }
                else
                {
                    mac_dest ="-" + mac_dest.Insert(0,mac_src.Substring(i,2));
                }
        }
}
```

4.5.2 计算机器指纹

MD5 为单向不可逆的 hash 运算，这样即使数据库管理员得到密文，也没办法还原成明文。本设计采用 MD5 计算用户机器指纹，即对硬盘序列号与 MAC 地址加密，用于唯一标示用户 PC 机，具体实现代码是这样的：

```
lblMachinehash.Text = System.Web.Security.FormsAuthentication.
HashPasswordForStoringInConfigFile(lblMachinehash.Text.Trim(),
"MD5").ToLower().ToString();
// lblMachinehash.Text.Trim()中为硬盘序列号与MAC地址字符串
```

4.5.3 用户身份验证

前面说到，当网络书店收到用户的款项时，用户登录网站，可点击下载按钮，此时系统将自动计算本机机器指纹，并与之前用户订购电子书时存入数据库的机器指纹相比较，如果相等，则提示“本地机器码验证成功，可以下载”，此时系统生成该电子书的许可证，用户即可下载电子书及许可证文件。若不相等，则表示用户身份不合法，系统给出验证失败，不能下载的提示。如图 4-12 所示。也就是说，用户只能在同一台机器上订购及下载电子书，这样即使用户名及密码被盗取，如果不能使用同一台机器，窃取者也不能下载该电子书，从而实现了电子书在线销售的版权保护。

图 4-12　机器指纹验证成功界面

4.6 许可证文件及其有效性验证

4.6.1 XML(可扩展标识语言)

XML 是一套定义语义标记的规则，这些标记将文档分成许多部件并对这些部件加以标识。它也是元标记语言，即定义了用于定义其他与特定领域有关的、语义的、结构化的标记语言的句法语言。

XML 是一种类似于 HTML 的语言，它被设计用来描述数据，而 HTML 是用于如何显示数据的。在 HTML 中所有的标志(tags)和文档结构都是预先定义好了的，我们只有权利使用那些标准的 HTML 标志，而 XML 允许我们自定义自己的标志和自己的文档结构，它能够用来将数据保存到文件和数据库中去。

下面给出一个简单的 XML 文档例子：

```
<? xml version="1.0"?>
<note>
<to>Tove</to>
<from>Jani</from>
<heading>Reminder</heading>
<body>Don't forget me this weekend!</body>
</note>
```

文档的第一行：一个应该包含的 XML 申明,它定义了 XML 文档的版本号。在这个例子中表示文档将使用 XML1.0 的规范：

<? xml version="1.0"?>

下一行定义了文档里面的第一个元素(element)根元素：

<note>

再下面定义了根元素的四个子元素(分别是 to, from, heading,和 body)：

<to>Tove</to>
<from>Jani</from>
<heading>Reminder</heading>
<body>Don't forget me this weekend!</body>

最后一行定义了根元素的结束标志：

</note>

所有的 XML 元素都必须要有一个结束标志。文档意为 Jani 提醒 Tove 不要忘了两人本周末的约定。

4.6.2 XmlTextWriter 对象

随着 XML 的普及以及在动态 WEB 应用程序中大量应用，如何通过.NET 创建，删除，修改 XML 文件变的越来越重要了。很多 ASP 的开发者，当他需要程序输出 XML 文件的时候，通常都是用 Response.Write()方法输出 XML 文档。

使用 Response.Write()的方式来输出 XML 文档，并不是一种那么好的方法，首先，我们用这种方法输出字符以组成 XML 文件的时候，我们会很担心输出的这些字符是不是符合 XML 规范，不符合 XML 规范的 XML 文档将不能得到正确完整的显示，如：<,>,&,"",和'这些符号，当它们在 XML 文件里的出现的时候，我们必须手工查找这些不合规范的字符；再次，当我们需要输出的是一个包含很多名字空间，属性和元素的 XML 文件的时候，使用 Response.Write()方法所必须的代码将会变得冗长以及可读性差。

.NET FrameWork 提供了一个特别为创建 XML 文件使用的类--System.Xml.XmlTextWriter,使用这个类来创建 XML 文件，并不需要担心输出是否符合 XML 规范的问题，同时代码将会变得非常简洁。

使用 XmlTextWriter 对象创建 XML 文件，需要在类构造器中指定文件的类型，而且编码类型必须是 System.Text.Encoding，如：System.Text.Encoding.ASCII, System.Text.Encoding.Unicode 及 System.Text.Encoding.UTF8，在 XmlTextWriter 类构造器指定为何种类型，在输出 XML 文件将以那种流文件形式输出。

XmlTextWriter 对象包含了很多可用于在创建 XML 文件时添加元素和属性到 XML 文件里的方法，见表 4-1。

表 4-1 XmlTextWriter 对象说明

方法名称	说明
WriteStartDocument()	创建第一行代码，用来指定该文件是 XML 文件以及设置它的编码类型
WriteStartElement(string)	在 XML 文件中创建新元素
WriteElementString(name,text_value)	创建一个只有字符的元素
WriteEndElement()	作为一个新元素的结尾；
WriteEndDocument()	XML 文件创建完后使用该方法结束
Close()	关闭所有的文本流，把创建的 XML 文件输出到指定位置

4.6.3 使用 XmlTextWriter 对象生成许可证书

本设计使用 XmlTextWriter 对象生成 XML 格式的许可证书，并将许可证书保存在相应的位置，许可证中包含用户对电子书的阅读权限和使用期限以及该电子书的 DES 解密密钥。首先导入 System.Xml 和 System.Text 命名空间，然后在 Page_Load 事件中创建一个 XmlTextWriter 对象实例，并且指定创建的 XML 文件保存为 Licence.xml 文件和它的编码类型为 UTF8(a translation of 16-bit unicode encoding into 8-bits)。主要代码如下：

1．创建一个新的 XML 实例：

```
XmlTextWriter writer = new      XmlTextWriter(Server.MapPath("../xml/"+
(string)Session["longid"]+"Licence.xml"), Encoding.UTF8);
    writer.WriteStartDocument(); //创建第一行代码，指定该文件是 XML 文件
    writer.WriteStartElement("body");                    //写入根元素
    writer.WriteElementString("title", "XML-Licence");  //加入子元素
    writer.WriteEndElement();//关闭根元素，并书写结束标签
    writer.Close();              //将XML写入文件并且关闭XmlTextWriter
```

2．读取空的 XML 文件：

```
string pathToXmlDoc = Server.MapPath("../xml/"+
                    (string)Session["longid"]+"Licence.xml");
XmlDocument xmlDoc = new XmlDocument();
xmlDoc.Load(pathToXmlDoc);
```

3．创建各个节点：ID、权限、期限、解密密钥并保存至XML中：

```
XmlNode root=xmlDoc.SelectSingleNode("body");//查找<body>
XmlElement xe1=xmlDoc.CreateElement("log");  //创建一个<log>节点
XmlElement xesub1=xmlDoc.CreateElement("id");       //ID
    xesub1.InnerText="ID";       //设置文本节点
    xe1.AppendChild(xesub1);  //添加到<log>节点中
XmlElement xesub2=xmlDoc.CreateElement("LONGID"); //电子书序列号
    xesub2.InnerText=RIGHT;
    xe1.AppendChild(xesub2);
 XmlElement xesub3=xmlDoc.CreateElement("RIGHT"); //权限
    xesub3.InnerText=RIGHT;
    xe1.AppendChild(xesub3);
XmlElement xesub4=xmlDoc.CreateElement("DATE"); //期限
    xesub4.InnerText=DATE;
    xe1.AppendChild(xesub4);
XmlElement xesub5=xmlDoc.CreateElement("DESKEY"); //密钥
    xesub5.InnerText=DESKEY;
    xe1.AppendChild(xesub5);
root.AppendChild(xe1);       //添加到<body>节点中
xmlDoc.Save(Server.MapPath("../xml/"+(string)Session["longid"]+"Licence.xml"))
;//保存到指定位置
```

4.6.4 许可证文档

下面为针对某电子书的购买记录生成的许可证文档，该许可证版本号为1.0，其编码类型为 utf-8,该许可证表明电子书的使用期限为一个月，用户只能阅读该书而不能打印。

```
<?xml version="1.0" encoding="utf-8"?>
<body>
  <title>XML-Licence</title>
  <log>
    <id>ID</id>
    <longid>73a861e51228b59820070116014838375QW3FVMQ1</longid >
    <RIGHT>只读</RIGHT>                    //阅读权限
    <DATE>一月</DATE>                      //使用期限
    <DESKEY>5JBLBOW7</DESKEY> //密钥
  </log>
</body>
```

4.6.5 基于椭圆曲线与机器指纹的许可证验证

当电子书及许可证文件被下载到本地后，服务器即对该许可证文件进行签名，其签名的主要算法在 2.6.3 节已详细介绍，在这里不再赘述，所不同的是，在本系统中，首先由服务器从数据库中取得客户主机的机器指纹(在这里，机器指纹包括硬盘序列号及网卡号)、用户的身份信息、电子书的序列号，将其进行 hash 运算，得到客户主机的唯一标识 ID，然后服务器使用椭圆曲线私钥对 ID 签名，并将签名传至客户主机，存在 Signature.dat 中；

每次打开电子书时，电子书阅读器先验证签名，通过验证后再判断其使用期限是否在有效的时间范围内，从而判断许可证的有效性，若有效才能得到解密密钥。由于许可证的签名是和客户机器指纹相绑定的，故电子书只能在一台电脑上阅读，即使将电子书与许可证同时传递给另一台机器，由于签名不能通过验证，也无法阅读电子书，这样便有效地实现了电子书离线的版权保护。

4.6.6 基于移动代理的电子书使用权限的跟踪

当电子书被下载到本地后，可以使用移动代理实现对电子书使用情况的跟踪。本系统拟采用的移动代理系统是 IBM 公司的 Aglets,代理完成的工作就是跟踪电子书的使用情况，并将跟踪情况返回给服务器，然后执行相应策略。

Aglet 移动代理生命周期内的事件及触发方法如表 4-2 所示。

表 4-2 Aglet 事件和方法

事件	方法	
	事件发生时	事件发生后
创建		onCreation()
克隆	onCloning()	onClone()
派遣	onDispatching()	onArrival()
召回	onReverting()	onArrival()
释放	onDisposing()	
挂起	onDeactivating()	
唤醒		onActivation()

当用户将电子书与许可证下载到 PC 机后，网络书店即根据用户的 IP 地址向用户发送移动代理，代理中携带有用户对该电子书的使用权限和对电子书不同程度侵权行为的相应策略，代理到达主机后，首先查找到该电子书，用户每次打开电子书，就检查用户对电子书的使用情况，一旦发现用户有非法使用等侵权行为，即根据自身携带的执行策略向主机发出警告或直接删除电子书，然后向服务器返回结果。

由于移动代理运行在一个不安全的网络环境，其自身的安全性得不到完整的保障，移动代理技术仍处于进一步更完善的研究中，因此系统使用水印代理实现用户对数字内容使用的跟踪有待进一步研究与探讨。

4.7 本章小结

本章主要给出了基于 DRM 的电子书在线销售系统服务器端关键技术的实现：对电子书内容打包后进行 DES 加密，对 DES 密钥及电子书的使用权限、期限进行 RSA 加密，同时对电子书生成 XML 格式的许可证。本设计引用名为 GetDiskKeyNo 的 ActiveX 插件获取本机硬盘序列号，并结合网卡号进行 MD5 运算形成机器指纹，以实现用户在购买电子书时的身份认证，同时用于客户端阅读电子书时的许可证有效性验证，这样就能有效地保护电子书的版权不受到侵犯，维护出版商、销售商及用户的共同权益，同时对于用户对电子书使用情况的跟踪，系统给出了一个使用移动代理的思路。

第五章 总结与展望

5.1 工作总结

数字版权管理技术(DRM)已广泛应用于电子图书、数字图书馆、流媒体、数字电视等领域。本文作者结合硬盘绑定技术提取机器指纹，提出了一个基于DRM的电子书在线销售系统的简单模型，实现了其中使用的关键技术，以实现电子书在线购买和离线使用的版权保护，本论文完成的主要工作如下：

1．简单讨论了数字版权管理技术的概念、发展历史、国内外DRM的研究现状及DRM的前景；

2．对DRM的技术体系、DRM功能结构与信息结构、DRM主要技术原理、DRM技术的特点、DRM系统模型等进行了研究，并结合移动代理技术提出了一个改进的DRM系统模型框架；另外文章介绍了DRM在eBook的数字版权管理中的应用，介绍了电子书阅读器的内部结构、使用原理，并提出了一种改进的基于椭圆曲线的电子书认证算法；

3．本文以ASP.NET为开发平台，实现了一个简单的基于DRM的电子书在线销售系统，系统分为电子书销售管理子系统和电子书版权管理子系统：其中电子书销售管理子系统包括用户管理模块和电子书管理模块，而电子书管理子系统则包括许可证管理模块、身份认证模块和权限跟踪管理模块。系统主要实现的功能有：DES对称加密、RSA非对称加密及数字签名、开发ActiveX插件以获取硬盘序列号并结合MAC地址进行MD5运算生成机器指纹、使用.NET FrameWork提供的XmlTextWriter对象创建XML格式的许可证文件等，并提出了系统实现移动代理的方案。

5.2 工作展望

随着数字版权管理技术的进一步深入的研究，产生了很多不同的解决方案，这些解决方案都仅仅在某一程度上实现了版权保护，而在认证计费技术上却有待更进一步的完善。

同时，数字版权管理技术本身也面临着很多安全性的挑战，首先DRM技术是一种立足于操作级控制的技术[50]，在信息安全领域中，DRM所能对付的只能

是其中一部分隐患，而对于如病毒入侵、黑客破坏等恶性手段并不能提供完整的应对措施。因此，DRM 产品通常需要与杀毒软件、防火墙等针对其他安全层面的安全软件进行配合；其次，安全防范手段本身就是一把双刃剑，在保证安全的同时，往往会带来使用上的不便，因此，今后的 DRM 产品将偏重于灵活性、易用性并能提供良好的嵌入集成机制。

数字版权管理技术包括许多技术手段：数据加密、数字签名、数字水印等等，在今后的发展中，这些技术本身的安全性、实用性也将得到更进一步的提高，人们将提出更快捷、更实用、更安全的加密及签名算法，而数字水印及信息隐藏技术也需要得到进一步的完善。

移动代理技术是一项很有发展前景的技术，目前对该技术研究的主要问题在于其安全性不能得到有效地保障，将移动代理技术应用于数字版权管理系统中，将使得系统的运行更为方便、快捷，同时也能解决一些诸如对数字内容的跟踪记录、水印检测跟踪等问题，因此研究移动代理技术的安全性，并将该技术应用在 DRM 系统是今后研究的方向。

最后，本文只实现了简单的电子书销售系统，要研究开发出真正成熟的系统、使之产品化，具有商业价值，还需要不断的努力。

参考文献

[1] 程巍，龚黎云，高传善. 数字版权管理的相关安全技术和实现方案. 微型电脑应用，2004，20(2)：9~11

[2] 陈江涛. 数字版权管理(DRM)技术与应用. 现代电视技术，2004，9：72~76

[3] 张建明，文学军. 数字版权管理系统的原理与应用. 现代图书情报技术，2004，107(2)：13~17

[4] 张长安，柏丽娜. DRM 技术及其在数字图书馆中的应用. 现代图书情报技术，2003，100(3)：83~85

[5] Apabi Digital Right Management System. http://www.apabi.com

[6] 肖文斌. 数字版权管理(DRM)系统的研究、设计与实现—专有文件管理系统客户端：[硕士学位论文]. 成都：四川大学，2005

[7] 张勇. 数字版权管理(DRM)系统的研究、设计与实现—DRM技术研究和专有文件管理系统设计：[硕士学位论文]. 成都：四川大学，2005

[8] 张福学. 数字版权管理系统的功能和信息结构分析. 情报技术，2002，6：26~27

[9] Renato Iannella. Digital Rights Management(DRM) Architectures. D-Lib Magazine, 2001, 6: 6~7

[10] MaoW 著，王继林等译. 现代密码学理论与实践. 北京：电子工业出版社，2004

[11] 罗丽平. 有序多重数字签名的研究与应用：[硕士学位论文]. 长沙：中南大学，2006

[12] Harn L. New digital signature scheme based on discrete logarithm. Electron Lett, 1994, 30(5): 2025~2026

[13] Harn L And Xu Y. On the design of generalized ELGamal type digtal signature schemes based on the discrete logarithm. Electron Lett, 1994,30(24): 2025~2026

[14] Harn L, iesler T. New digital signature based on discrete logarithm. Electronics Letters, 1994, 30(5): 396~398

[15] R.Anderson, Invited lecture. Fourth Annual Conference on Computer and Communication Security. ACM, 1997.1~7

[16] MD5 的算法与实现. http://blog.csdn.net/ jimmy_w/archive/2006/10/14/

1334403.aspx

[17] Bender.W, Gruhl.D, MorimotoNetal. Techniques for data hiding. IBM System Journal, 1996, 35(3&4): 313~316

[18] 沈海波. 数字水印技术在 DRM 中的应用. 湖北教育学院学报，2004，21(5)：25~27

[19] Hartung F, Ramme F. Digital rights management and watermarking of multimedia content for m-commerce application. IEEE Comunications Magazine, 2000, 11(8): 78~84

[20] Stanley R.M.Oliveira, Mario A. Nascimento, Osmar R.Zaiane. Digital Watermarking. Status, Limitation and Prospects, January 2002

[21] S.H. Kwok, S.C. Cheung, K.C. Wong, K.F. Tsang. Integration of digital rights management into the Internet Open Trading Protocol. Decision Support Systems, 2002, (34): 413~ 425

[22] 王爱华，孙世兵，朱本军. 数字权限描述语言及其比较研究. 开放教育研究，2005，11(4)：77~81

[23] 黄晓斌，黄少宽. 数字化版权管理与 XRML. 图书情报知识，2003，8：48~50

[24] 毛军. DOI系统中参考文献链接技术框架. 北京：中国科学院国家科学数字图书馆，2002. 8~12

[25] 金松. 数字对象唯一标识符解析机制研究报告. 北京：中国科学院国家科学数字图书馆，2003

[26] International DOI Foudation. The DOI handbook version2.0.0 Febrary 2002, DOI Official Website URL: http:// www.doi.org

[27] DOI Handbook Version 2.1.0, April 2002. The comprehensive guide to the DOI System, http://www.doi.org/hb.html

[28] 李文峰，刘雪涛，贾月琴. 基于元数据标准的标准资源库建设研究. 中国标准化，2000，4： 24~25

[29] EBX Working Group. The electronic book exchange system(EBX)version 0.8. July 2000

[30] 沈海波. 一种基于移动代理的数字版权管理系统框架. 湖北教育学院学报，2005，22(2)：23~25

[31] Sycara, K.Decker, K.Pannu. Distributed Intelligent Agents. IEEE Expert, December 1996: 36~45

[32] Lange D B, Oshima M. Seven good reasons for mobil agents.

Communications of the ACM, 1999, 42(3): 88~8

[33] Pagurek B, White T. Mobile agents for network management. IEEE Communications Surveys, 1998, 48(1): 1~8

[34] 孙非. Web 网上电子书店的分析与实现. 信息技术，2005，6：65~67

[35] 长安，于会萍，刘宇胜. 基于 DRM 技术的电子书在线出版销售模式的构建. 现代图书情报技术，2004，106(1)：61~63

[36] 赵继海. DRM 技术的发展及其对数字图书馆的影响. 大学图书馆学报，2002，1：14~16

[37] 张长安，柏丽娜. DRM 技术及其在数字图书馆中的应用. 现代图书情报技术，2003，3：83~85

[38] 曹虹. 数字图书馆建设中版权管理研究. 情报杂志，2003，10：15~18

[39] 蔡皖东，田广利，段琪，任建奇. 基于 DRM 的电子文档保护设计与实现. 微电子学与计算机，2005，22(7)：161~164

[40] 范科峰，赵新华. 数字版权管理技术的研究现状及在数字电视系统中的应用. 标准与技术追踪，2005，6：21~25

[41] 关于 IPTV 标准进展情况及问题分析. 广电行业：网络电视. http://info.broadcast.hc360.com/2006/11/08135795512.shtml

[42] IPTV 技术标准研究的进展. http://www.sy.ln.cn/sycnc/view.php?id=4923

[43] 叶云，吴畏. 移动数字版权管理的应用. 现代电信技术，2004，1(1)：5~7

[44] 王政宏. 移动数字版权管理技术. 电信网技术，2004，2(2)：14~18

[45] 周勃. EBOOK 数字之花悄然开放. 数字时代，2002，1：53~55

[46] 邓珂，邢春晓，周立柱. 数字版权管理中eBook安全机制研究. 计算机科学，2004，31(4)：89~91

[47] 卢鹏菲，詹雄泉，洪景新. 基于椭圆曲线的有序多重数字签名方案. 厦门大学学报(自然科学版)，2005，44(5)：341~343

[48] 施荣华，胡芳. 一种基于椭圆曲线的有序多重数字签名方案. 计算机工程与应用，2006，42(25)：153~154

[49] Blake, Seroussi G, Smart N. Elliptic Curves in Cryptography. Cambridge, United Kingdom: Cambridge University Press, 1999

[50] Qiong Liu. Digital Rights Management for Content Distribution. Information Security Workshop 2003(AISW2003), Conferences in Research and Practice in Information Technology, Vol, 2

致 谢

本文是在导师施荣华教授的悉心指导下完成的，在攻读硕士学位的三年时间里，他以自己深厚的理论造诣、丰富的实践经验和对前沿科学敏锐的洞察能力，为我的研究工作提供了有力的指导和帮助。导师严谨的治学态度、渊博的知识、活跃的学术思想、执着的科研精神及高尚的做人原则，所有这一切都将成为我受益终生的宝贵财富!在此，学生谨向导师表示衷心的感谢!

感谢王国才、刘卫国、梁建武、肖大光和王果平老师在论文完成过程中给予的指导和建议，你们的帮助和鼓励，使我的论文能顺利完成。

感谢我的师兄弟们，尤其是杨政宇、周成、罗俊、胡斌、胥磊、周玉、康晶、鲍骏骏、李娟。正是由于你们的帮助和支持，我才能克服一个一个的困难和疑惑，直至本文的顺利完成。

感谢我的爸爸妈妈，焉得谖草，言树之背，养育之恩，无以回报，你们永远健康快乐是我最大的心愿。

感谢我的母校-中南大学，学业就要告一段落了，带着梦想，带着这里赋予我的一切品质，就要踏入社会，在今后的生活、工作中，我都将积极进取、乐观向上。

感谢信息科学与工程学院的所有老师，七年来的谆谆教导，我铭记在心。

最后我要衷心感谢所有评审老师，你们辛苦了！

攻读学位期间主要的研究成果

一、发表论文情况：

施荣华，胡芳. 一种基于椭圆曲线的有序多重数字签名方案. 计算机工程与应用，2006，42(25)：153～154

二、科研情况：

[1] 参加湖南省科技厅《企业技术开发》杂志社网络投稿评审系统的开发，负责调研、系统需求分析，并负责完成专家远程审稿模块、作者查稿及投稿模块；

[2] 参加湖南省雨花区《地方国防动员系统》的开发，负责调研、系统需求分析工作，并负责完成其中人民防空子系统的开发工作。