doi:10.3969/j.issn.1000-436x.2013.10.018

新型通用格式多媒体数字版权管理系统设计与实现

黄勤龙[1,2]，马兆丰[1,2]，莫佳[1,3]，钮心忻[1]，杨义先[1]

（1. 北京邮电大学 信息安全中心，北京 100876；2. 北京国泰信安科技有限公司，北京 100876；
3. 电子科技大学 计算机科学与工程学院，四川 成都 611731）

摘 要：针对多媒体内容的版权保护问题，设计一种新型通用格式多媒体数字版权管理模型，包括内容加密与打包、密钥管理、安全引擎、许可证管理与分发、DRM 客户端和 DRM 管理等功能单元，该模型通过非结构化加密方法，克服了基于内容格式加密方法的局限性，实现对通用格式多媒体内容的保护。另外，采用许可证提取码作为下载许可证的凭证，解决许可证重新发行和转让的问题，并支持细粒度使用控制方式。基于此模型，实现了基于固定与移动融合业务的多媒体数字版权管理系统，并将其运用于数字消费领域，实验结果和实际运行表明该方案不影响多媒体质量，效率及安全性较高，在多媒体内容版权保护方面具有较好的实用性。

关键词：数字版权管理；多媒体版权保护；非结构化加密；许可证书；使用控制

中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2013)10-0153-09

Design and implementation of a novel general format multimedia digital rights management system

HUANG Qin-long[1,2], MA Zhao-feng[1,2], MO Jia[1,3], NIU Xin-xin[1], YANG Yi-xian[1]

(1.Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2.Beijing National Security Science and Technology Co., Ltd, Beijing 100876, China;
3.School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China)

Abstract: Aiming at the copyright protection of multimedia content, a novel general format multimedia digital rights management model was designed which includes encryption and packaging of content, ke nagement, security engine, license management and distribution, DRM client, DRM management and other functional units. This model uses un-structured encryption method which overcomes the limit ions of encryption method based on the content format to sup-port the general format multimedia. In addition, this model uses the license acquisition number as the only certificate to download license to solve the problem of license reissue and transfer, and supports fine-grained control model. Combined with this model, a multimedia digital rights management system was developed based on fixed and mobile converged services which is used in the field of digital consumer. experimental results and practical application show that this scheme with good practice in the copyright protection multimedia content does not affect the multimedia quality, and have high efficiency and safety.

Key words: digital rights management; multimedia rights management; unstructured encryption; license; usage control

1 引言

随着 Internet 技术的快速发展，数字多媒体内容的分发、复制和编辑变得越来越普遍，移动互联网的飞速发展使得多媒体内容的制作、分享和下载越来越简单，由此带来的大量多媒体内容盗链、盗版以及不规范使用行为对数字媒体产业造成巨大的冲击。数字多媒体内容的非法复制和传播损害了

收稿日期：2012-05-17；**修回日期**：2012-10-24

基金项目：国家自然科学基金资助项目（60803157, 90812001, 61272519）；国家标准制定计划基金资助项目（20080200-T-339）；国家质检公益性科研专项基金资助项目（10-126）

Foundation Items: The National Natural Science Foundation of China (60803157, 90812001, 61272519); The National Standard Development Planning (20080200-T-339); The Standardization Public Industry Special Foundation of China (10-126)

版权所有人和内容运营商的合法权益，如何防止数字多媒体内容的非法复制与扩散，保护多媒体内容的版权是数字内容产业发展所面临的关键问题，数字版权管理技术正是为了解决这一关键问题而产生的。

数字版权管理（DRM，digital rights management）是通过数字内容的制作、发行、安全许可和计费等一系列手段防止数字内容的非法误用，确保数字内容在公平、合理、安全许可框架下的条件使用和消费[1]。

2 相关工作

随着DRM技术的应用越来越广泛，学术界和工业界进行了大量的研究和实践[2~11]。

马兆丰等人提出了一种新的支持时空约束的数字版权管理安全许可协议[2]，将内容对象与版权对象相分离，通过内容加密密钥CEK保护数字内容本身，在用户与许可证中心之间采用动态实时密钥协商算法实现双向认证和动态许可申请。

针对P2P网络，Jung-Shian Li等人提出了一个新的端对端音乐内容分发的DRM框架[8]，内容分发的顽健性通过使用基于拉格朗日插值法的网络编码方法来实现，不会对音频质量产生影响，但该框架分发到用户的内容将不受控制。针对IPTV内容，Boseung Kim等人提出了一种采用帧加密的内容保护的方法[9]，该方法使用一种干扰加密方法，即使用散列函数而不是复杂的加密过程，通过改变像素值来重新排列每帧的图像，从而实现简单而又比较有效的IPTV内容保护，然而该方法安全性较低，缺少密钥管理和许可证管理。Yeonjeong Jeong等人提出了一种在不同音频DRM系统之间可以互相转换的方法[10]，目前音频内容受多种DRM系统，每个采用不同的DRM技术，DRM内容也不相同，该方法使得已经受DRM保护的音频内容可以在其他DRM兼容的设备上使用，但该方法适用范围有限。钟勇等人提出了一种面向DRM的责任授权模型及其实施框架[11]，该模型基于分布式时态逻辑和Active-U-Datalog语法规则，具有表达事件驱动、事件驱动和责任补偿等各种责任授权的语义能力，具有良好的可实施性，提高了DRM系统对数据使用控制的灵活性和能力。

工业界目前有多种DRM解决方案，如OMA DRM[12]、Marlin DRM[13]、苹果的FairPlay系统[14]、微软的Media DRM系统[15]和Adobe的Flash Access系统[16]等，推动了DRM的发展和应用，但OMA DRM不支持版权对象[17]的重新发行，FairPlay、Media DRM和Flash Access等均只支持有限的几种格式。

现有针对多媒体内容的DRM系统存在如下一些问题和局限性。

1) 现有基于内容格式加密或者帧结构加密的多媒体DRM系统，其加密过程复杂，内容解密播放时处理性能较低，如Boseung Kim等人[9]提出的一种干扰的帧加密方法，其加密速率比采用AES算法的非结构化加密方法要低。

2) 现有的音视频等多媒体DRM系统，多与音视频的格式相关，一般只支持少数的几种视频格式，如微软的Media DRM[15]只支持WMV、WMA和ASF 3种格式，Adobe的Flash Access[16]只支持FLV和F4V 2种格式，目前，DRM系统未能支持通用格式的多媒体，不同格式之间的多媒体无法统一订购和使用，无法满足不同内容提供商提供的不同多媒体内容保护需求。

3) 现有的多媒体DRM系统存在权利许可无法重新发行或者转让的不足，当权利许可丢失或损坏时，用户无法继续使用版权内容，如OMA DRM，同时用户也不能将自己购买的权利许可转让给他人，如微软的Media DRM和Adobe的Flash Access等。

因此，本文在支持时空约束的数字版权管理安全许可协议[2]的基础上，广泛参考国内外DRM标准和规范，综合考虑现有DRM系统存在的问题以及多媒体内容消费的需求，设计了一种新型通用格式多媒体数字版权管理模型（CPSec media DRM, content protection security），该模型通过非结构化加密方法，不依赖多媒体内容格式，支持通用格式多媒体内容。另外，为了解决许可证重新发行和转让的问题，采用许可证提取码作为下载许可证的凭证，并支持细粒度使用控制[18]方式。

在此模型的基础上，本文实现了基于固定与移动融合（FMC，fixed mobile convergence）[19]业务的多媒体数字版权管理系统，该系统与运营商业务平台结合，综合了内容加密与打包、许可证管理与分发和DRM客户端等重要功能，运营商在运营版权内容的同时，保护内容提供商的权益，同时用户在订购获取内容并下载许可证后可以按需使用内容。

3　CPSec Media DRM 模型技术目标

3.1　支持通用音视频多媒体格式

为了支持不同业务，内容平台包含了大量不同格式的音视频多媒体，包括 H263、H264、MPEG-4、MPEG-2、MP3 和 AC3 等，CPSec Media DRM 设计时同时支持以上通用的音视频格式和未来的新格式，支持不同内容提供商提供的不同格式的版权内容，为 DRM 系统的融合、流通和推广奠定了基础。

3.2　支持许可证重新发行和转让

为了解决许可证丢失无法使用内容和许可证无法转让的问题，CPSec Media DRM 系统设计了随机的许可证提取码，每个许可证对应一个提取码，用户在 DRM 客户端通过许可证提取码下载许可证，并可将许可证提取码转让给其他人，许可证丢失时可以重新通过许可证提取码下载许可证。

3.3　支持细粒度使用控制方式

DRM 许可证描述了用户使用内容时的各项权利，CPSec Media DRM 设计时支持细粒度使用控制方式，包括使用时间、使用次数、用户绑定、设备绑定等，通过不同权利的动态组合满足试用、包月和赠送等使用场景。

4　CPSec Media DRM 模型设计方案

CPSec Media DRM 同消费平台和内容平台等进行业务、内容和用户数据的交互，完成内容的加密与打包，同时向用户提供控制内容使用的许可证。CPSec Media DRM 功能架构如图 1 所示，包括内容加密与打包系统、密钥管理系统、安全引擎系统、许可证管理与分发系统、DRM 客户端和 DRM 管理系统等功能单元。

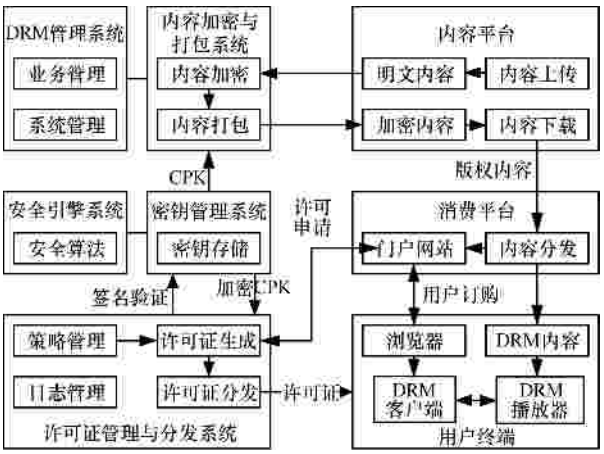

图 1　CPSec Media DRM 模型

1) 内容加密与打包系统

内容加密与打包系统接收内容平台需要进行 DRM 保护的内容，使用密钥管理系统提供的内容加密密钥对内容按照非结构化加密方法进行加密。内容打包系统按照 DRM 系统相关规范对加密后的内容打包，然后将受 DRM 保护的内容传送到内容平台，供用户下载使用。

2) 密钥管理系统

密钥管理系统负责管理 DRM 系统中使用的各种密钥，并维护媒体文件与内容主控密钥的映射关系。内容加密系统从密钥管理系统申请用于加密媒体文件的内容主控密钥；许可证管理与分发系统根据内容标识从密钥管理系统申请对应的内容主控密钥，以加密形式封装到许可证中。

3) 安全引擎系统

安全引擎系统向密钥管理系统提供以下服务：内容及其主控密钥的加解密、许可证的签名与验证、生成内容主控密钥、对指定内容计算散列值。

4) 许可证管理与分发系统

许可证管理与分发系统主要负责许可证的生成、分发和管理，包括许可证生成、许可证分发和许可证策略管理等模块。许可证生成模块接收业务系统的许可证创建请求，根据权利信息为用户创建许可证，同时向密钥管理系统申请相应的内容主控密钥，以密文形式封装到许可证；许可证分发模块实现许可证的分发和下载功能；许可证策略管理模块实现许可证策略的管理功能。

5) DRM 客户端

DRM 客户端执行与媒体文件使用相关的许可和约束，控制用户对媒体文件的使用。用户播放受 DRM 保护的媒体文件时，如果终端没有相应的许可证，媒体播放器会提示用户需要相应的权限才能使用，并通过浏览器将用户重定向到业务系统进行订购，获取许可证下载信息。DRM 客户端获取许可证后，利用内容主控密钥对媒体文件密文进行解密，并根据许可证中的权利信息控制用户对媒体文件的播放及使用。

6) DRM 管理系统

DRM 管理系统负责内容加密情况、许可证分发与使用情况的统计、分析工作。系统管理负责 DRM 系统角色管理、权限管理和工作状态的检测。

4.1 内容加密与打包系统

4.1.1 内容加密与打包格式

在 CPSec Media DRM 中，通用媒体文件加密后打包成 CPSec Media DRM 内容格式（DCF），定义如下。

1) 媒体文件头

媒体文件头长度为 20 字节。其中，预留 4 字节，即(‘CDRM’)；文件类型 4 字节；CPSec DCF 整体标记 4 字节；CPSec DCF 规范版本标识 4 字节；CPSec DCF 兼容性标记 4 字节。图 2 是文件类型、标记、版本与其他媒体文件内容之间的关系。

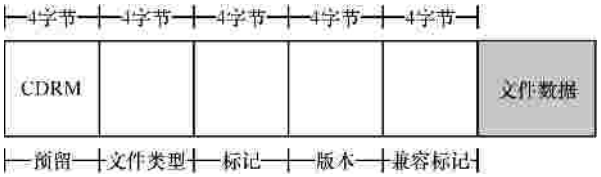

图 2 CPSec DCF 媒体头格式

2) 媒体文件体

图 3 是对媒体文件格式的全面描述。DCF 文件体由若干个 CPSec DCF 容器组成，每个 CPSec DCF 容器只包含一个 DCF 头和一个 DRM 内容对象容器。

图 3 CPSec DCF 整体格式

3) 非结构化内容加密

内容加密与打包系统使用分组加密算法（如使用 CBC 模式或者 CTR 模式的 AES 算法）将不同格式媒体文件按照分块加密，并按照 DCF 整体格式打包。该方法克服了基于内容格式加密方法的局限性，将媒体文件当作整体分块加密，不依赖于多媒体内容的编码格式，因此支持通用格式媒体文件的加密。

4.1.2 内容加密与打包系统工作流程

内容加密与打包系统接收到 DRM 管理系统或内容平台的媒体文件加密请求后，对需要加密的媒体文件按照非结构化加密方法进行加密，同时按照规定的 DCF 对加密后的媒体文件进行打包，内容加密与打包系统参数如表 1 所示。

表 1 内容加密与打包系统参数

参数名称	含义
CP	content provider
CID	content identity
PCD	plain content data
ECD	encrypted content data
ECH	encrypted content hash
DCD	DRM content data
CPK	content provider key
CRK	content random key
CEK	content encryption key
AID	algorithm identity
RID	retrieval identity

内容加密与打包系统工作流程如图 4 所示。

step1 内容加密与打包引擎获取内容主控密钥 CPK 及内容辅助密钥 CRK，安全引擎产生内容加密密钥 CEK，该密钥用于加密媒体内容

$$CEK = E_{CPK}(CRK)$$

step2 内容加密与打包引擎获取加密和打包参数，包括 AID 和 RID 等。

step3 内容加密与打包引擎对 CP 提供的原始媒体文件进行加密，并计算加密内容散列值 ECH。

$$ECD = E_{CEK}(PCD, AID, RID)$$

$$ECH = Hash(ECD)$$

step4 内容加密与打包引擎对加密后的数据按照规定的 DCF 进行打包，DCD 即是受 DRM 保护的媒体内容。

$$DCD = \{CID \parallel CRK \parallel ECD\}$$

step5 所有加密打包过程的参数都保存到数据库中，加密打包后的内容 DCD 提供用户使用。

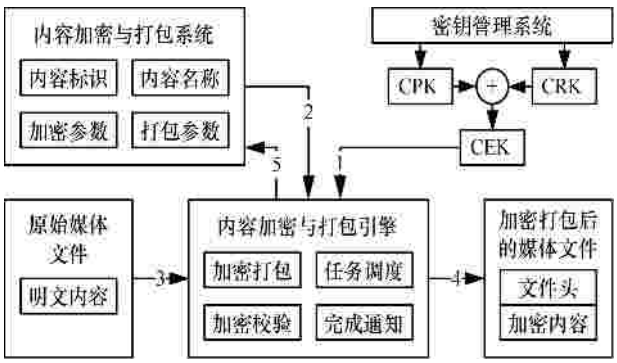

图 4 内容加密与打包系统工作流程

4.2 密钥管理系统

密钥管理系统负责内容主控密钥 CPK 的生

成和管理、加密后内容散列值 ECH 的存储和管理等，包括密钥生成、密钥分发、密钥存储和密钥更新等。

密钥管理系统参数如表 2 所示。

表 2　密钥管理系统参数

参数名称	含义
MK	master key
EPK	encrypted provider key
UEK	user encryption key
PRK	private key
PUK	public key

step1　密钥管理系统产生内容主控密钥 CPK，并使用密钥保护 MK 加密存储在数据库中

$$EPK = E_{MK}(CPK)$$

step2　接受内容加密与打包系统的请求，使用密钥保护密钥 MK 解密存储在数据库中加密的内容主控密钥 EPK，返回内容主控密钥 CPK

$$CPK = D_{MK}(EPK)$$

step3　接受许可证管理与分发系统的请求，返回使用用户的公钥 PUK 加密的内容主控密钥 CPK 得到的 UEK 和内容散列值 ECH

$$CPK = D_{MK}(EPK)$$
$$UEK = E_{PUK}(CPK)$$

4.3　安全引擎系统

安全引擎系统为密钥管理系统提供安全计算，主要包括对称加密算法、公钥算法和散列算法等，并支持证书的操作。

4.4　许可证管理与分发系统

许可证管理与分发系统主要包括许可证生成和分发等功能。

1) 许可证生成

许可证生成模块负责根据从业务平台接收的订购信息和用户许可证请求信息生成许可证。

2) 许可证分发

许可证分发模块接收和响应 DRM 客户端的许可证下载请求，将相应的许可证分发到 DRM 客户端。

4.4.1　许可证生成流程

许可证管理与分发系统负责根据从业务平台接收的订购信息，包括用户标识、内容标识以及权限信息等，生成许可证，并返回给业务平台。许可证管理与分发系统参数如表 3 所示。

表 3　许可证管理与分发系统参数

参数名称	含义
UID	user identity
DID	device identity
REX	rights expression
LCQ	license request
LQS	license request signature
LCC	license content
LCS	license signature
LIC	license

许可证管理与分发系统流程如图 5 所示。

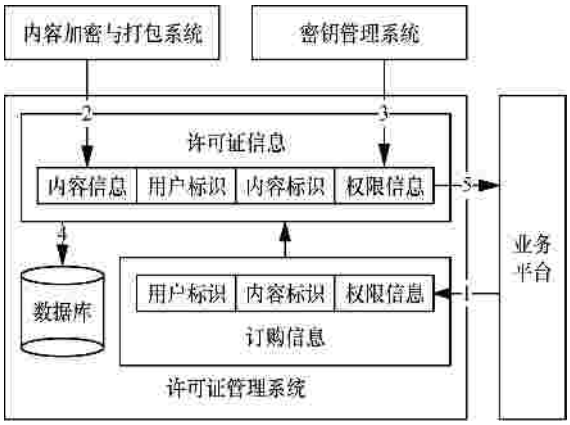

图 5　许可证生成流程

step1　业务平台处理用户的订购请求，将订购信息（包括用户标识 UID、内容标识 CID 和权限信息 REX 等）发送到许可证管理与分发系统，许可证管理与分发系统创建该许可证信息。

step2　许可证管理与分发系统根据订购信息中的内容标识从内容加密与打包系统中查询加密内容信息，并保存到许可证信息中。

step3　许可证管理与分发系统将完整的权限信息保存到许可证数据库。

step4　许可证管理与分发系统将许可证下载信息返回给业务平台，业务平台将许可证下载信息返回给用户浏览器，供用户下载许可证。

4.4.2　许可证分发流程

许可证分发模块接收 DRM 客户端的许可证下载请求，包含设备标识 DID、用户的公钥证书及下载请求签名信息，并将上述信息发送到许可证生成模块，许可证生成模块将最终的许可证内容返回到许可证分发模块，许可证分发模块将许可证分发到 DRM 客户端，如图 6 所示。

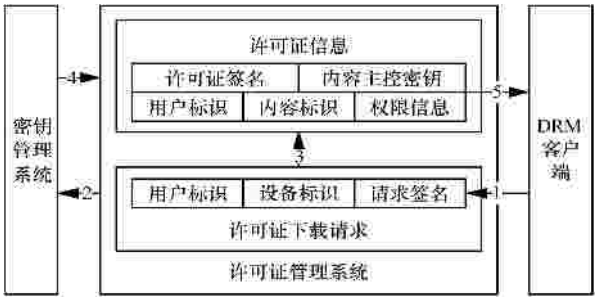

图 6 许可证分发流程

step1 许可证管理与分发系统收到 DRM 客户端发起的许可证下载请求，包含许可证下载信息 URL，用户标识 UID，设备标识 DID、用户的公钥 PUK 及下载请求签名信息 LQS 等

$$LCQ = \{URL \| UID \| DID \| PUK \| LQS\}$$

step2 许可证管理与分发系统将用户的公钥及下载请求签名信息发送到密钥管理服务器请求验证下载请求和用户身份

$$LQS' = D_{PUK}(URL \| UID \| DID)$$

验证以下等式是否成立

$$LQS' = LQS$$

step3 许可证管理与分发系统根据下载请求查找到内容标识 CID 和许可证信息，然后将内容标识 CID 发送给密钥管理服务器，获得密钥管理服务器返回的经过加密后的内容主控密钥 UEK 和内容散列值 ECH。

step4 许可证管理与分发系统将权限信息 REX 基于许可证权利描述语言生成待签名的许可证 LCC

$$LCC = \{CID \| UEK \| ECH \| REX \| UID \| DID\}$$

step5 许可证管理与分发系统将待签名的许可证发送给密钥管理服务器请求签名得到 LCS

$$LCS = E_{PRK}(LCC)$$

step6 许可证管理与分发系统在得到密钥管理服务器返回的签名信息 LCS 后，生成最终的许可证文件 LIC

$$LIC = \{LCC \| LCS\}$$

4.5 DRM 客户端

DRM 客户端负责管理包括加密媒体解析和解密、安全引擎调用、许可证下载和管理、客户端管理等。

DRM 客户端的基本工作流程包括：许可证下载和媒体文件解密播放等。

1) 许可证下载

用户订购完成后获取许可证下载信息，通过许可证下载代理模块完成许可证的下载。用户也可以在 DRM 客户端管理提供的许可证下载界面上输入许可证提取码，发起许可证下载请求。

如图 7 所示，在下载许可证之前，客户端需要向许可证管理与分发服务器提供用户的公钥，在这里，用户的公私钥对由客户端产生和维护。许可证管理与分发服务器和密钥管理服务器协作完成许可证的封装，并把许可证下发到客户端。

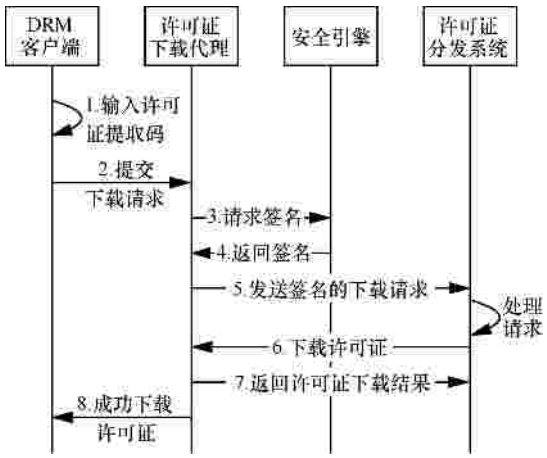

图 7 DRM 客户端下载许可证时序

2) 媒体文件解密播放

DRM 客户端获取许可证后，使用 DRM 播放器按照许可证描述播放内容，时序如图 8 所示。

DRM 客户端使用许可证管理与分发服务器的公钥来验证许可证签名，许可证和设备的绑定是通过用户的公钥加密内容主控密钥 UEK 和用户设备标识 DID 实现，在判断绑定关系正确后，DRM 客户端使用用户的私钥从许可证解密出内容主控密钥 CPK，然后和 DRM 头中的内容辅助密钥 CRK 导出 CEK

$$CPK = D_{PRK}(UEK)$$

$$CEK = E_{CPK}(CRK)$$

DRM 客户端使用 CEK 调用安全引擎解密受保护的媒体内容 ECD，将待播放的明文数据 PCD 交给播放器进行播放

$$PCD = D_{CEK}(ECD, AID, RID)$$

5 CPSec Media DRM 系统实现方案

5.1 内容加密与打包系统

内容加密与打包系统以任务的形式提供服务，

支持单个和批量任务的提交，系统后台自动伺服对内容按照指定参数进行加密和打包，任务完成后通知用户和系统。系统支持高、较高、一般、较低、低等 5 个优先级，管理员可根据内容要求动态调整任务优先级。

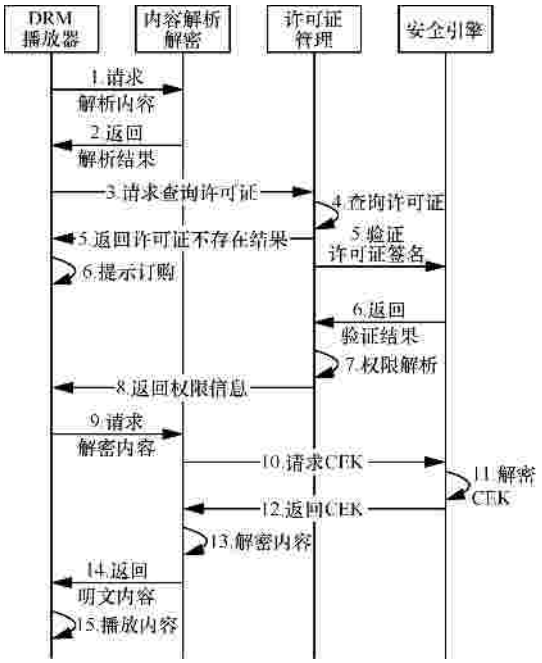

图 8　DRM 媒体解密播放时序

5.2　密钥管理系统

密钥管理系统采用 3 层密钥管理模型，其中第一层负责媒体内容加密，采用分组密码算法；第二层负责内容密钥保护，所用密钥称为内容主控密钥，采用分组密码算法；第三层负责将内容主控密钥分发给授权用户，采用非对称算法。

5.3　安全引擎系统

安全引擎系统基于 OpenSSL 算法库，提供相关加解密算法，支持对称加密算法、非对称加密算法、散列算法和 X.509 证书操作等，实现公私钥对的生成、数字签名、身份认证、散列值计算、解密内容主控密钥 CMK 等功能。

5.4　许可证管理与分发系统

许可证管理与分发系统负责根据从业务平台接收的订购信息，生成许可证提取码，并返回给业务平台，用户获取许可证提取码后在终端输入许可证提取码下载许可证，系统根据许可证提取码分发许可证到客户端。

CPSec Media DRM 系统定义的权利表达语言 REL（rights expression language）规定的是基于 ODRL[20]控制 DRM 内容使用权利的语法和语义，即权利表达语言是用于规范定义权利对象的语法和语义，包括基础模版、协议模版、背景模版、许可模版、约束模版、继承模版和安全模版，约束模板包括的细粒度使用控制如表 4 所示。

表 4　许可证约束模板中细粒度使用控制

元素	描述
count	计次元素规定一个许可对 DRM 内容可授权使用的次数
timed-count	定时计次元素可视为增加了一个可选择的定时器属性的计次元素
datetime	日期时间元素定义时间的范围，对包含的许可分别表示时间的限制
start	开始元素规定开始的时间或日期
end	结束元素规定结束的时间或日期
interval	间隔时间元素规定许可能够在 DRM 内容上执行的时间周期
accumulated	累计时间元素规定权利作用于 DRM 内容的累计时间的最大值
individual	个体元素规定与 DRM 内容所绑定的个体
system	系统元素规定 DRM 内容和权利对象可以输出到的目标系统

5.5　DRM 客户端

DRM 客户端包括加密文件解析解密、安全引擎、许可证下载代理、许可证管理、本地许可证库、客户端管理、播放器插件和浏览器插件等单元。

6　CPSec Media DRM 实验结果分析

通过实验对比 CPSec Media DRM 系统加密的性能，同时对比原始内容和受 DRM 保护后的内容播放的资源占用等性能，验证本文方案的性能和实时性。

6.1　实验 1

比较 CPSec Media DRM 系统采用的非结构化加密和帧加密的加密性能。实验数据选取水平分辨率分别为 320 p、480 p、720 p 和 1 080 p 的不同媒体，实验环境为 IBM X3650 服务器，非结构化加密算法采用 AES 算法。

实验过程中分别对上述 4 组 DRM 媒体进行加密处理，并统计其加密时间。

实验中本文的非结构化加密结果和文献[9]的帧加密进行了对比测试，结果如表 5 所示。实验结果表显示非结构化加密平均速度为 10 Mbit/s，而帧加密平均速度为 8.4 Mbit/s。与帧加密相比，非结构

化加密速度平均高出 15%~20%，并且非结构化加密速度符合线性关系，而帧加密随着媒体内容大小和帧数量的不断增多，其速度呈逐渐降低趋势。

表 5 非结构化加密结果

内容分辨率	内容大小/MB	加密时间/s		加密速度/(Mbit·s^{-1})	
		本文	文献[9]	本文	文献[9]
320 p	109	11.0	12.6	9.91	8.65
480 p	157	15.9	18.2	9.87	8.63
720 p	321	32.2	38.3	9.97	8.38
1 080 p	648	63.9	80.5	10.14	8.05

与非结构化加密相比，帧加密需要耗费时间在多媒体内容帧结构的解析上，并且帧加密后的媒体依然能够播放，只不过画面出现错乱，而非结构化加密方法将媒体结构信息等全部加密，用户无法播放加密后的媒体，安全性较高。

实验结果表明非结构化加密方法有着较高的加密效率和较好的实用性，并且能够支持不同格式和大小的多媒体内容的加密处理。

6.2 实验 2

比较 CPSec Media DRM 系统播放的性能。实验数据选取水平分辨率分别为 320 p、480 p、720 p 和 1 080 p 的同一媒体，实验环境 CPU 主频大小为双核 2.2 GHz，内存大小为 2 GB。

实验过程中分别对上述 4 组 DRM 视频进行下载播放，并统计其 CPU 平均占用率。

实验中 CPU 平均占用率如图 9 所示。实验结果表显示多媒体比特率越高，受 DRM 保护的多媒体播放时 CPU 平均占用率比原始媒体播放时高出越多。

总体来看，DRM 保护的媒体使用时资源占用平均高出 3%~5%，在不影响多媒体质量的前提下，保持着较低的资源占用，能够支持不同硬件性能的终端。

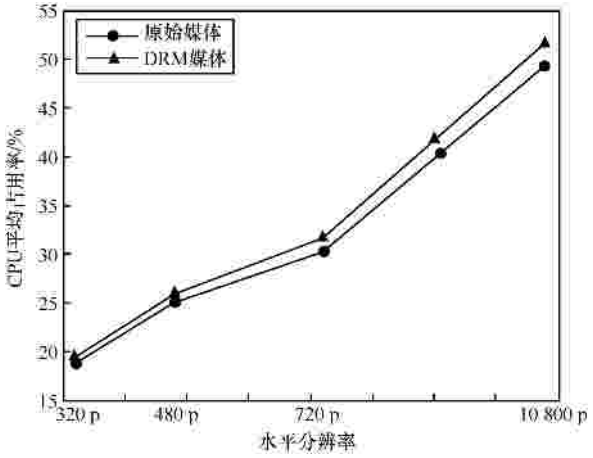

图 9 资源占用实验结果对比

7 CPSec Media DRM 对比分析

目前，主流的多媒体 DRM 方案包括 OMA DRM 2.0、Adobe Flash Access 和微软 Media DRM 等，CPSec Media DRM 在支持的媒体格式、内容加密方法、支持的终端平台、许可证重新发行、许可证转让、许可证用户绑定、许可证设备绑定和许可证离线使用等方面与这些方案的对比分析如表 6 所示。本文所提的方案支持通用媒体格式，许可证支持重新发行、转让、用户绑定、设备绑定和离线使用。

针对 DRM 的攻击主要包括协议中的客户端和服务器之间缺乏相互认证，转储内容加密密钥或未加密的内容等，本文所提的方案中媒体内容使用内容加密密钥加密，保证内容的安全性，许可证下载时客户端和服务器之间使用 HTTPS 加密协议，保证下载申请和许可证的安全性，同时下载申请使用用户的私钥签名，提供给服务器认证用户身份，下载的许可证使用服务器的私钥签名，保证许可证的完整性，许可证中的内容密钥使用用户的公钥加密，保证内容加密密钥的安全性。

表 6 多媒体 DRM 对比分析

对比特性	CPSec Media DRM	OMA DRM 2.0	Adobe Flash Access	微软 Media DRM
支持的媒体格式	通用媒体格式	移动媒体格式	FLV 和 F4V	WMV、WMA 和 ASF
内容加密方法	非结构化加密	非结构化加密	结构加密	结构加密
支持的终端平台	PC 终端、移动终端和机顶盒终端等	移动终端	PC 终端、移动终端和机顶盒终端等	PC 终端和移动终端等
许可证重新发行	支持	不支持	支持	支持
许可证转让	支持	不支持	不支持	不支持
许可证用户绑定	支持	支持	支持	不支持
许可证设备绑定	支持	支持	不支持	不支持
许可证离线使用	支持	支持	支持	不支持

目前，多媒体内容逐渐成为互联网主流，为了适应多媒体技术和移动终端的快速发展，本方案下一步重点研究许可证的离线分发和用户域的支持。

8　结束语

本文提出一种新型通用格式多媒体数字版权管理的模型，该模型通过非结构化加密方法以支持通用多媒体格式，支持不同内容提供商提供的不同类型的版权内容。同时，本模型实现中引入了许可证提取码的概念，用户通过许可证提取码下载许可证，解决许可证重新发行和转让的问题，满足试用、赠送等复杂的使用场景。

与现有的多媒体 DRM 方案相比，本文提出的 CPSec Media DRM 方案，支持通用多媒体格式，支持许可证的重新发行和转让，并且支持细粒度使用控制方式，效率及安全性较高，具有较好的实用性。

参考文献：

[1] WIPO - world intellectual property organization[EB/OL]. http:　ww. wipo.int.

[2] 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.
MA Z F, FAN K F, CHEN M, *et al*. Trusted digital rights management protocol supporting for time and space constraint[J].　urnal of Communicartions, 2008, 29(10):153-164.

[3] 庄超. 一种新型的 Internet 内容版权保护的计算机制[J]. 计算机学报, 2000,23(10):1088-1091.
ZHUANG C. A new computing mechanism for Internet content copyright protection[J]. Chinese Journal of Computers, 2000,23(10): 1088-1091.

[4] 谭建龙，庄超，白硕. 一种实用的 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):1119-1203.
TAN J L, ZHUANG C, BAI S. Design and implementation of a practical Internet content copyright protection system[J]. Journal of Computer Research and Development, 2001,38(10):1119-1203.

[5] 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):957-968.
YU Y Y, TANG Z. A survey of the research on digital ri hts management[J]. Chinese Journal of Computers, 2005,28(12):957-968.

[6] 马兆丰，冯博琴. 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.
MA Z F, FENG B Q. Secure authentication protocol for t ted copyright management based on dynamic license[J]. Journal f Software, 2004,15(1):131-140.

[7] 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.
FAN K F, MO W, CAO S, *et al*. Advances in digital rights management technology and application[J]. Acta Electronica Sinica, 2007,35(6):1139-1147.

[8] LI J S, HSIEH C J, HUNG C F. A novel DRM framework for peer-to-peer music content delivery[J]. Journal of Systems and Software, 2010,83(10):1689-1700.

[9] KIM B, CHOI J, KIM J, *et al*. A study on frame encryption for protecting IPTV contents[A]. Advanced Communication Technology (ICACT)[C]. 2011. 1484-1488.

[10] JEONG Y, KIM J, YOON K. Consumer electronics[A]. Audio DRM Conversion between Different DRM Content Formats[C]. 2008. 1-2.

[11] 钟勇，秦小麟，刘凤玉. 一种面向 DRM 的责任授权模型及其实施框架[J]. 软件学报, 2010,21(8):2059-2069.
ZHONG Y, QIN X L, LIU F Y. Obligation authorization model and its implementation framework for DRM[J]. Journal of Software, 2010, 21(8):2059-2069.

[12] OMA DRM[EB/OL]. http://www.openmobilealliance.org.

[13] Marlin DRM[EB/OL]. http://www.marlin-community.com.

[14] Apple Inc. Thoughts on music[EB/OL]. http://www.apple.com/ hotnews/ thoughtsonmusic.

[15] Microsoft media rights server. microsoft corp[EB/OL]. http://www.microsoft.com/windows/windowsmedia/drm/default.aspx.

[16] Adobe flash access[EB/OL]. http://www.adobe.com/products/adobeaccess. html.

[17] 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.
WEI J Z, YANG Y X, NIU X X. Overview of study on the technical architecture of OMA DRM[J]. Journal of Electronics & Information Technology, 2008,30(3):746-751.

[18] SANDHU R, PARK J. Usage control: a vision for next generation access control[A]. Proc of the MMM-ACNS-2003[C]. Heidelberg: Springer-Verlag, 2003. 17-31.

[19] WONG C C, LOW A L Y, HIEW P L. Fixed-mobile convergence: creating values with appropriate business models[A]. Information and Communication Technologies, ICTTA '06, 2nd[C]. 2006. 17-22.

[20] ODRL: open digital rights language[EB/OL]. http://www.odrl.net.

作者简介：

黄勤龙（1988-），男，江西新余人，北京邮电大学博士生，主要研究方向为数字版权管理、数字内容安全、网络安全。

马兆丰（1974-），男，甘肃镇原人，博士，北京邮电大学教师，主要研究方向为数字版权管理、数字内容安全、计算机网络安全。

莫佳（1977-），男，四川广元人，电子科技大学博士生，主要研究方向为数字水印、信息隐藏、数字内容安全、计算机网络与信息安全。

钮心忻（1963-），女，浙江湖州人，北京邮电大学教授、博士生导师，北京邮电大学信息安全中心副主任，主要研究方向为数字水印、信息隐藏、隐写分析。

杨义先（1961-），男，四川盐厅人，北京邮电大学教授、博士生导师，北京邮电大学信息安全中心主任，长江学者特聘教授，主要研究方向为密码学、计算机网络与信息安全。