OMA DRM 技术体系研究综述

魏景芝[①] 杨义先[①] 钮心忻[②]
[①](北京邮电大学信息安全中心 北京 100876)
[②](北京邮电大学网络与交换技术国家重点实验室 北京 100876)

摘 要：为了对最新发布的开放移动联盟(OMA)数字版权管理(DRM)标准的技术体系结构有一个系统全面的认识，积极推动我国DRM标准的制定和数字内容保护技术的应用研究，该文在深入研究最新发布的OMA DRM2. 0规范的基础上，对OMA DRM技术体系结构：版权对象获取协议(ROAP)、安全模式、体系结构、内容格式和版权描述语言进行了详细分析，然后从综合角度给出一个系统全面的OMA DRM工作机制：OMA DRM 工作流程和原理，最后，对OMA DRM性能做了详细分析：OMA DRM2. 0和OMA DRM1. 0的主要区别，以及OMA DRM2. 0的尚待改进之处。

关键词：数字版权管理；体系结构；数字内容格式；版权对象获取协议
中图分类号：TP393 **文献标识码**：A **文章编号**：1009-5896(2008)03-0746-06

Overview of Study on the Technical Architecture of OMA DRM

Wei Jing-zhi[①] Yang Yi-xian[①] Niu Xin-xin[②]
[①](*Information Security Center*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)
[②](*State Key Laboratory of Networking and Switching Technology*, *Beijing University of Posts and Elecommunications*, *Beijing* 100876, *China*)

Abstract: In order to have a thorough understanding of the technical architecture of OMA DRM specification, and to actively promote creation of the Chinese DRM standard and application research of digital content protection technology, a systematic approach of OMA DRM is presented. The following functions of the latest release of OMA DRM2.0 are analyzed: rights object acquisition protocol, security model, architecture, content format and rights expression language. Then, these features are synthesized to present a complete working mechanism of OMA DRM: working flow and principle of OMA DRM. Finally, the capabilities of the latest release are analyzed by presenting the main difference between OMA DRM2.0 and OMA DRM1.0, and the limitations of OMA DRM2.0.

Key words: Digital Rights Management(DRM); Architecture; Digital content format; Rights object acquisition protocol

1 引言

随着互联网的日益普及和流媒体压缩技术的不断提高，数字内容(如音视频流、电子书等)能通过网络发布给终端用户。为使这些数字内容的创作、分发和消费在可控方式下进行，确保数字内容的真实性，有效阻止对数字内容的非法使用，真正达到知识产权保护的目的，采用数字版权管理(DRM)技术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]。在目前所有 DRM 技术标准中，开放移动联盟(OMA)制定的 OMA DRM2.0 标准最成熟、参与者最多、影响力最大。2002 年 11 月 OMA 正式发布了 OMA DRM1.0 标准。然后又针对 1.0 版本的不足，于 2006 年 3 月完成并发布了 OMA DRM2.0 标准的批准版：OMA DRM2.0 规范，OMA DRM2.0 内容格式，OMA DRM2.0 版权描述语言，OMA DRM2.0 体系结构和 OMA DRM2.0 需求。目前国内大多数 DRM 方案都是依据 OMA DRM 标准设计的，此外，由广电总局牵头正在制定的 China DRM 标准也借鉴了 OMA DRM 标准，所以对 OMA DRM 标准进行深入研究就显得非常重要。目前在国内已有的 OMA DRM 研究中[2–6]，文献[2]和文献[3]都是基于 OMA DRM1.0 版本，这对想了解最新 OMA DRM 标准的人来说，显然没有参考价值；文献[4–6]是基于 OMA DRM2.0 的候选版本，而非最新正式版本；文献[3–6]都主要针对 OMA DRM 标准中的体系结构部分，但 OMA DRM 标准是由 5 个不同的部分组成，若只针对 OMA DRM 标准的体系结构部分，显然不能完整体现 OMA DRM 标准技术体系；此外，文献[2–6]都是基于 OMA DRM 原文翻译的介绍，缺少对整个 OMA DRM 技术体系的系统性概括和分析。鉴于此，本文针对最新发布的 OMA DRM2.0 标准的批准版本进行了深入研究[7–11]，在综合运用 OMA DRM2.0 规范，OMA DRM2.0 体系结构，OMA DRM2.0

2006-10-30 收到，2007-03-09 改回
北京市自然科学基金(4042025)资助课题

内容格式和 OMA DRM2.0 版权描述语言的基础上，给出了系统全面的 OMA DRM 工作流程和详细的工作原理。本文对初次接触或正在研究 OMA DRM 标准的研究人员来说，不必再花费大量时间研究 OMA DRM 标准就能很快明白 OMA DRM 的整个工作流程和原理；对推动我国数字媒体内容保护的应用研究起到积极作用；对正由中国广播影视数字版权管理标准起草委员会制定的我国自主的 DRM 标准有借鉴意义。

2　OMA DRM 技术体系结构

OMA DRM 标准的 2.0 版本包括 OMA DRM2.0 规范，OMA DRM 体系结构，OMA DRM 内容格式，OMA DRM 版权描述语言，OMA DRM 需求。下面将对 OMA DRM2.0 规范中的版权对象获取协议(ROAP)和安全模式，OMA DRM 体系结构，OMA DRM 内容格式以及 OMA DRM 版权描述语言这 5 大技术体系分别进行分析。

2.1 ROAP(版权对象获取协议)

ROAP 就是版权对象获取协议，是 OMA DRM2.0 规范的主要内容，是用来完成版权发布者(RI)/内容发布者和设备之间的注册、版权对象(RO)获取、入域或离域操作。一个 ROAP 组包含：4 通道注册协议，2 通道 ROAP，1 通道 ROAP，2 通道入域协议和 2 通道离域协议。除 1 通道 ROAP 外，ROAP 组里其它协议都由 ROAP 触发器启动。只有成功执行 4 通道 ROAP 注册协议，建立一个基于设备和 RI 的有效 RI 前后关系后，才能进一步执行 RO 获取、入域或离域操作。

4 通道注册协议是一个完全安全的信息交换和同步交换，用于完成 RI 和设备之间的注册功能。其流程见图 1 中的 4 通道注册协议部分。一般只在第 1 层执行此协议，但当 RI 认为设备的 DRM 时间不准确或在交换、更新信息时，也可执行此协议；2 通道 ROAP 是设备用于获取 RO 的一种协议，它包含设备和 RI 间的相互认证、RO 的完整性保护和发送。其流程见图 1 中的 2 通道 ROAP 部分。只有成功执行一个 4 通道注册协议，在设备中建立一个基于设备和 RI 的有效 RI 前后关系后，才能成功执行此协议；1 通道 ROAP 就是只能从 RI 把 RO 发送给设备(如消息/推)，它是 RI 单方面发起的，不需要设备发送任何信息，实际上它是 2 通道变量的最后一个消息。其流程见图 1 中的 1 通道 ROAP 部分。只有成功执行一个 4 通道注册协议，在设备中建立一个基于设备和 RI 的有效 RI 前后关系后，才能成功执行此协议；2 通道入域协议就是一个设备通过此协议加入一个域，其流程见图 1 中的 2 通道入域协议部分。只有成功执行 4 通道注册协议，在设备中建立一个基于设备和管理着域的 RI 的有效 RI 前后关系后，才能成功执行此协议。入域协议成功完成后，就会在设备中建立一个域前后关系，它含有详细的域钥信息的域安全。设备通过使用一个域前后关系来安装和使用域 RO；2 通道离域协议就是一个设备通过此协议离开一个域，其流程见图 1 中的 2 通道离域协议部分。只有成功执行 4 通道注册协议，在设备中建立一个基于设备和管理着域的 RI 的有效 RI 前后关系后，才能成功执行此协议。

ROAP 工作流程如图 1 所示。

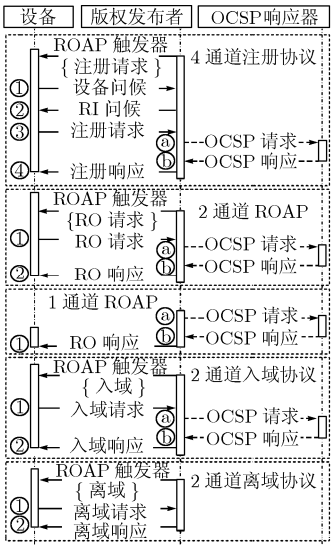

图 1 ROAP 工作流程

(1) RI 产生一个用于注册的 ROAP 触发器给 DRM 代理。

(2) DRM 代理接到 ROAP 触发器后，会尽可能快地启动 ROAP 协议交换。在启动 4 通道注册协议前,DRM 代理必须获得用户同意，除非 ROAP 触发器的<ROAP 统一资源定位>元素的万能域名部分和用户同意列表中的登陆一致，则不需要获得用户同意就能访问 RI。征得用户同意后，DRM 代理向 RI 发送一个包含设备身份(ID)的设备问候消息来启动 4 通道注册协议。RI 通过<设备问候>元素来识别 4 通道 ROAP 注册协议里的 ROAP-设备问候消息，并通过设备 ID 来识别设备。

(3) 为响应 ROAP-设备问候消息，RI 向设备返回一个包含 RI ID 的 4 通道 ROAP 注册协议中的的第 2 个消息：ROAP-RI 问候消息。设备上的 DRM 代理必须用<RI ID>元素验证它和 RI 之间有一个有效的 RI 前后关系，并用它识别 RI。

(4) 设备向 RI 发送一个由<注册请求>元素指示的 4 通道 ROAP 注册协议中的第 3 个消息：ROAP-注册请求消息。

(5) 协议注册期间，RI 为了得到自己的证书，可随时执行一个基于实时的在线证书状态协议(OCSP)请求，再把返回的 OCSP 响应提供给设备；若 RI 认为设备的 DRM 时间不准确，则 RI 要执行一个基于实时的 OCSP 请求；若设备是一个不支持 DRM 时间的未连接设备，则协议注册期间，

RI 为了得到自己的证书，必须执行一个基于实时的 OCSP 请求。

(6) RI 向设备发送一个由<注册响应>元素指示的 4 通道 ROAP 注册协议中的最后消息：ROAP-注册响应消息。若 ROAP-注册请求消息发送成功，则设备再访问 RI 时，可用<ROAP 统一资源定位>元素来发送 ROAP 请求。成功完成协议注册后，就在设备中建立一个 RI 前后关系。

(7) RI 产生一个用于 RO 请求的 ROAP 触发器给 DRM 代理。

(8) 设备通过<ROAP 统一资源定位>元素向 RI 发送一个由<RO 请求>元素指示的 2 通道 ROAP 中的第 1 个消息：ROAP-RO 请求消息。

(9) RO 请求期间，RI 为了得到自己的证书，可随时执行一个基于实时的 OCSP 请求，然后把返回的 OCSP 响应提供给设备；若 RI 认为设备的 DRM 时间不准确，则 RI 要执行一个基于实时的 OCSP 请求；若设备是一个不支持 DRM 时间的未连接设备，则 RO 请求期间，RI 为了得到自己的证书，必须执行一个基于实时的 OCSP 请求。

(10) RI 向设备发送一个由<RO 响应>元素指示的 2 通道 ROAP 中的第 2 个消息或 1 通道 ROAP 中的唯一一个消息：ROAP-RO 响应消息，它携带着受保护的 RO。

(11) RI 产生一个用于入域的 ROAP 触发器给 DRM 代理。

(12) 设备向 RI 发送给一个由<入域请求>元素指示的 2 通道入域协议中的第一个消息：ROAP-入域请求消息。

(13) 入域请求期间，RI 为了得到自己的证书，可随时执行一个基于实时的 OCSP 请求，然后把返回的 OCSP 响应提供给设备；若 RI 认为设备的 DRM 时间不准确，则 RI 要执行一个基于实时的 OCSP 请求；若设备是一个不支持 DRM 时间的未连接设备，则入域请求期间，RI 为了得到自己的证书，必须执行一个基于实时的 OCSP 请求。

(14) RI 向设备发送一个由<入域响应>元素指示的 2 通道入域协议中的第 2 个消息：ROAP-入域响应消息。

(15) RI 产生一个用于离域的 ROAP 触发器给 DRM 代理。

(16) 设备向 RI 发送一个由<离域请求>元素指示的 2 通道离域协议中的第 1 个消息：ROAP-离域请求消息。

(17) 为了从域中删除设备，RI 向设备发送一个由<离域响应>元素指示的 2 通道离域协议中的 ROAP-离域响应消息。

2.2 安全模式分析

(1) 信任模式：OMA DRM 信任模式是基于公钥基础设施(PKI)的。若 RI 核实过 DRM 代理证书且该证书没有被吊销，则 RI 就信任 DRM 代理；若 DRM 代理核实过 RI 的证书，且该证书没有被吊销，则信任 RI。

(2) 机密性：通过对内容加密和对携带内容密钥(CEK)的 RO 加密绑定，确保了只有经过认证和授权的 DRM 代理才能访问受保护内容，未经授权方不能访问 DRM 内容。

(3) 认证：在 OMA DRM 的 4 通道注册协议，2 通道 ROAP 和 2 通道入域协议里，通过对实时或时间戳进行数字签名完成 RI 和 DRM 代理间的相互认证；在 1 通道 ROAP 里，通过对时间戳进行数字签名完成对 RI 的认证，但不能向 RI 认证 DRM 代理；在 2 通道离域协议里，通过对时间戳进行数字签名完成 RI 对 DRM 代理的认证，但不能向 DRM 代理认证 RI。

(4) 数据完整性保护：通过对 ROAP 和 RO 进行数字签名完成数据的完整性保护，防止对数据进行未经授权的修改。

(5) 密钥确认：通过受保护密钥和发送方 ID 上的消息访问控制(MAC)来完成密钥确认，用受保护密钥的一部分作为 MAC 密钥。密钥确认确保能够接收含有受保护密钥的信息。

(6) 重放保护：时间戳提供了重放保护。

2.3 OMA DRM 体系结构

OMA DRM2.0 采用独立的功能体系结构，如图 2 所示。

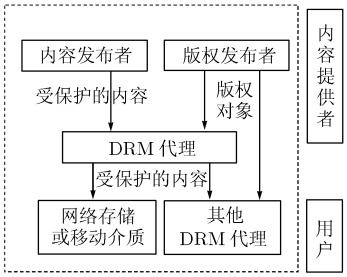

图 2 功能结构

内容发布者发送 DRM 内容，RI 产生一个 XML 文档的 RO 来控制 DRM 内容的使用。OMA DRM 让 DRM 内容和 RO 进行逻辑分离。可以分别或同时请求/发送 DRM 内容和 RO。例如，用户选择一个内容并付费，然后在同一个交易中接收 DRM 内容和 RO。若以后 RO 过期，用户无需再次下载 DRM 内容，只需获取一个新的 RO 即可。DRM 代理是一个设备上的实体，它对一个设备的信任成分进行具体化，只有 DRM 代理才能访问 RO，它强制执行设备上的许可限制，并控制对 DRM 内容的访问等。用户必须通过 DRM 代理才能获取 RO。

2.4 OMA DRM 内容格式

DRM 内容格式有数字版权管理内容格式(DCF)和打包的数字版权管理内容格式(PDCF)两种。DCF 是具有扩充功能的对象结构文件，主要用于离散内容，它是 OMA DRM 中的通用格式；PDCF 称为打包的 DCF，主要用于连续内容，它是 ISO 基本媒体文件格式支持加密媒体路径的一个实例。这两种格式类型共享一些数据结构，且都遵循 ISO 箱扩

展机制，定义了若干容器箱，分别保存与 DRM 相关的描述信息(如内容标识、加密算法、RI 地址等)和加密后的媒体对象数据。

(1) DCF 文件格式　DCF 结构见图 3。(a) DCF 文件结构：DCF 文件的开头是长度为 20bit 的 DCF 文件头(含有商标号和版本域的文件类型箱)；接着是第 1 个 OMA DRM 容器箱：必须包含一个 DCF 头箱和一个受保护的内容箱；DCF 头箱是偏移 OMA DRM 容器箱开头 20bit 的第 1 个箱：包含普通头箱和用户数据箱；在 DRM 内容箱后面，是 OMA DRM 定义的扩充部分：其它 OMA DRM 容器箱和易变 DRM 信息箱；易变 DRM 信息箱又包含交易跟踪箱和版权对象箱；(b) OMA DRM 容器箱：禁止把 OMA DRM 容器箱嵌入在别的数据类型里面，它必须出现在最高层，必须支持长 64bit 的域值为 1 的域，必须用大域值表示箱容量，必须在 DCF 文件里至少出现一次，必须在其头部有唯一一个内容 ID，必须在每个容器箱中有不同的的媒体类型，必须把第 1 个容器的媒体类型默认为 DCF 内容的媒体类型，必须用 DCF 头箱中的内容类型域指示内容对象的原始 MIME(多目的网络邮件扩展)媒体类型，必须在 DRM 内容箱的内容对象箱中包含数据长度域和数据字节；(c) 普通头箱：必须出现在 DCF 头箱中，必须把普通头版本的版本值设为 0。它包含如何解密已加密内容的加密方法域，如何填充密文最后部分的填充方案域，规定明文初始长度的明文长度域，规定内容 ID 值必须大于零的内容 ID 长度域，指示域值长度的 RI 统一资源定位长度域，指示域值长度的原文头长度域，含有全球唯一的内容对象标识符的内容 ID 域，定义 RI 统一资源定位的 RI 统一资源定位域；(d) 用户数据箱：包含描述内容对象名称的标题箱，描述内容对象的描述箱，含拷贝宣言的拷贝箱，描述内容对象作者的作者箱。

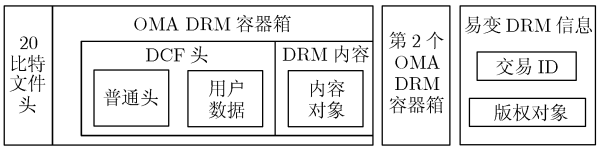

图 3 DCF 结构

(2) PDCF 文件格式　PDCF 结构见图 4。PDCF 格式可用于下载机制或流传输机制中的媒体内容，OMA DRM 不要求设备必须支持 PDCF 格式。通过把保护计划信息箱放进视频路径里，同时把 OMA DRM 标识符规范为密钥管理系统，就可保护 PDCF 里的所有路径。在 PDCF 文件里，计划信息箱就是 OMA DRM 密钥管理系统箱，所以 PDCF 必须支持用于密钥管理系统的 OMA DRM。由于播放设备要用头信息来解密 PDCF 内容，所以加密 PDCF 内容时，不管 OMA DRM 普通头箱中的加密方法域是否为空，都要把 OMA DRM 访问单元的头信息加进处理访问单元。

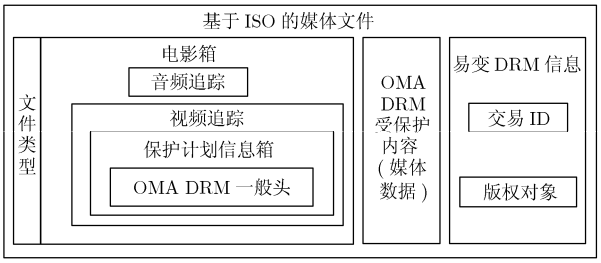

图 4　PDCF 结构

2.5 OMA DRM 版权描述语言

OMA DRM2.0版权描述语言是在开放的数字版权描述语言(ODRL)的基础上，对RO进行了语法和语义的定义。而ODRL缺少语义的定义，所以OMA DRM2.0版权描述语言又对ODRL的使用提供补充说明。OMA DRM2.0版权描述语言以XML方式定义了对OMA DRM 内容的各种访问许可(如播放、显示、拷贝、保存)和限制(如次数、时段、质量)。

3　OMA DRM 工作机制

针对图5中的OMA DRM工作流程，其工作原理具体如下：

(1) 由内容提供者制作原始的DRM内容。

(2) 内容提供者采用对称加密算法AES，使用128bit的CEK对DRM内容加密并打包来保护DRM内容免遭未经授权的访问；对于内容格式为DCF的离散媒体内容，是在一个内容容器内，把其内部结构作为一个完全未知对象进行加密保护并打包的；对于内容格式为PDCF的连续媒体内容，是在一个单独的格式类型里对连续媒体内容进行加密保护。

(3) 内容提供者把打包加密的内容传给内容分发者，由内容分发者发送DRM内容。

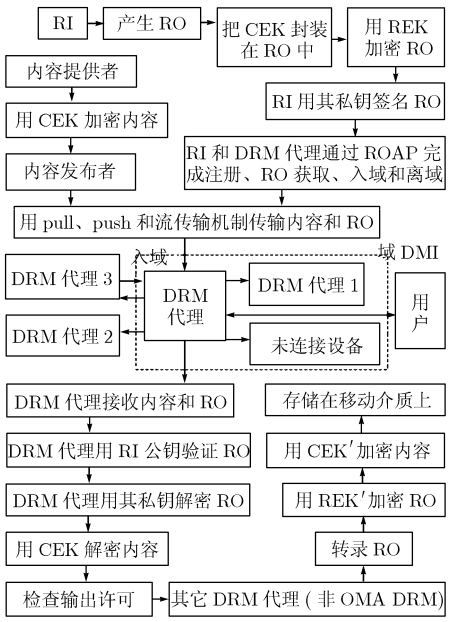

图 5 OMA DRM 工作流程

(4) 由RI给DRM内容分配许可限制。

(5) RI用DRM代理能够识别的版权描述语言产生相应的RO。RO是个XML文档，它由许可限制以及嵌入在RO中的其它信息(如版权信息)和CEK组成。通过规定和内容相关的许可限制来控制DRM内容的使用。一个RO可以和许多条DRM内容联系起来。只有获得和内容相关的RO，才能使用DRM内容。

(6) RI必须在RO中对内容密钥进行封装。

(7) RI利用版权密钥(REK)，也就是DRM代理的私钥加密RO，通过把RO和指定的一个或一组DRM代理加密绑定，确保只有指定的设备才能访问RO，进而访问DRM内容。

(8) RI 采用数字签名和 MAC 来确保交换信息的完整性和真实性，并用 RSA-PSS [PKCS-1] 作为默认签名方案。(a) RI 根据 DCF HASH 计算程序产生一个 DCF 的加密 HASH 值，再把它插进 RO 中来确保 DRM 的完整性：对 DRM DCF 的任何改动都会使 RO 中的 HASH 值自动无效。终端中的 DRM 代理接收到全部的 DRM 内容后，就在 DCF 上计算 HASH 值，并与相应 RO 中携带的 HASH 值比较，两者相同表示该 DRM 内容未在传输过程中被修改。若不一致，则 DRM 代理必须禁止解密和使用 DCF；(b) 为保证 RO 的可靠性和传输完整性，RI 向 DRM 代理发送 RO 前，先用其私钥对 RO 进行数字签名。DRM 代理对收到的 RO 用 RI 的公钥验证其数字签名，从而确认该 RO 是否来自该 RI 且在传输过程中未被修改。

(9) DRM代理必须通过ROAP完成和RI间的注册、RO获取、入域或离域操作。

(10) 由于DRM内容和RO既是独立实体，又在逻辑上彼此联系，所以可用传输机制pull(http pull，OMA下载)，push(WAP push，MMS)或流分别发送DRM内容和RO，或者在ROAP-RO响应消息里用上述传输机制同时发送它们，或者通过使用RO箱把受保护的RO当作二进制数据插进DCF或PDCF里，用上述传输机制同时发送它们。所以DRM内容和RO有分别发送、组合发送和超分发3种发送方式。

(11) 用户只能通过DRM代理才能访问内容。

(12) DRM代理：其功能是当使用DRM内容时，执行RO里的许可规范，保护和处理有关系统安全的秘密和密钥，并防止未经授权者使用内容。所有DRM代理都有一个唯一的公/私钥对和一个证书。证书包括附加信息，如制造商，设备类型，软件版本，序列号等。证书允许内容发布者和RI能安全地认证一个DRM代理。

(13) DRM 代理，DRM 代理 1 和未连接设备构成了一个由 RI 创建、管理和执行的域 DM1。域 DM1 中的所有设备不需要来回连接 RI，就可共享此域中的全部 DRM 代理上的离线的 DRM 内容。为了提供安全的时间资源，作为连接设备(具有广域网连通性的 OMA DRM 便携设备)的 DRM 代理和 DRM 代理 1 必须支持 DRM 时间，但是未连接设备(不具有广域网连通性的 OMA DRM 便携设备)由于容量有限，可不用支持 DRM 时间。连接设备和未连接设备都必须支持 OMA DRM 且都属于同一个域。DRM 代理通过网络连通性确保未连接设备能加入域 DM1。域 DM1 的工作原理如下：(a) DRM 代理和 DRM 代理 1 连接到 RI，通过 4 通道注册协议完成注册后，再通过 2 通道 ROAP 入域协议加入域 DM1；(b) DRM 代理通过网络连到内容发布者端口，以 DCF 格式下载 DRM 内容。再从 RI 那儿购买用于 DCF 的域 RO，然后把下载的 DCF 和域 RO 保存在本地设备上。为确保其它设备一旦收到 DCF，就能访问此内容，DRM 代理把域 RO 嵌入在 DCF 里；(c) DRM 代理向 DRM 代理 1 发送 DCF 及其相关的域 RO，由于 DRM 代理 1 也是域 DM1 的成员，故 DRM 代理 1 无需连到 RI 就能立即使用其上的内容和版权；(d) 作为连接设备的 DRM 代理使用 OBEX(对象交换协议)上的 ROAP 传输机制把内容发给未连接设备；(e) DRM 代理也想把内容发送给 DRM 代理 2，但由于 DRM 代理 2 不是域 DM1 的成员，不能使用此内容。为了能使用内容，用户选择连到 RI 或加入域 DM1 来获取访问内容的版权。对于前者，DRM 代理必须使用超分发机制把内容发送给 DRM 代理 2；对于后者，DRM 代理 2 必须通过 2 通道 ROAP 入域协议向 RI 发送一个 2 通道 ROAP-入域请求消息申请入域。若 RI 批准 DRM 代理 2 入域，则向 DRM 代理 2 返回一个 2 通道 ROAP-入域响应消息。若入域后的 DRM 代理 2 想离开域 DM1，则必须通过 2 通道 ROAP 离域协议向 RI 发送一个 2 通道 ROAP-离域请求消息申请离域。RI 接到离域请求消息后向 DRM 代理 2 返回一个 2 通道 ROAP-离域响应消息。

(14) 由于 DRM 代理 3 不是域 DM1 成员，所以 DRM 代理必须通过超分发机制把 DCF 发送给 DRM 代理 3。

(15) 为了能在那些不支持 OMA DRM 但支持其它一些 DRM 机制的设备上使用 DRM 内容， RI 可以限制内容只能输出到指定的其它 DRM 系统，所以下载的内容和版权就要和目标 DRM 系统兼容。把 DRM 内容和 RO 输出给其它 DRM(非 OMA DRM)系统时，授权保护机制如下：(a) 把受保护的内容和 RO 发送给可信的 OMA DRM 代理后，DRM 代理依据受保护的 RO 中描述的许可和限制来消费受保护的内容。消费内容时，OMA DRM 代理用自己的私钥解密受保护的 RO，然后从已解密的 RO 中获取 CEK，进而用 CEK 解密受保护的内容；(b) 输出时，DRM 代理检查 RO 中描述的许可：RI 是否允许把内容输出到目标 DRM 系统；内容类型是否正确；使用规则是否和目标 DRM 系统兼容。DRM 代理通过当用户想下载输出内容时收到的来自 RI 的通知，就能确知受保护的内容和 RO 都适合目标 DRM 系统；(c) RDM 代理把原始内容和使用规则发送给其它 DRM 代理；(d) 为保持和源版权对象的一致性，其它 DRM 代理要依据由 RI 和其它 DRM 系统定义的专门规则，把兼容的版权转录到其它 DRM RO 里；(e) 其它 DRM 代理自己生成新的 CEK′(其它 DRM 系统的内容密钥)，并用此密钥加密内容，用 REK′(其它 DRM 系统的版权密钥)加密包含 CEK′ 的转录的 RO；(f) 其它 DRM 代理和移动介质通过相互认证

确保双方的可靠性，认证通过后，根据其它 DRM 系统的规范格式在移动介质上保存加密的内容和 RO；(g) 用户可从设备上取出移动介质，插进兼容其它 DRM 系统的设备，就能欣赏内容。

4 OMA DRM 性能分析

4.1 OMA DRM2.0 和 1.0 的比较

OMA DRM 1.0 技术主要用于内容的保护，OMA DRM 2.0 技术在完全兼容 DRM 1.0 技术的基础上，对 DRM 规范做了大量改进，主要加强了通信和密钥的保护。它是针对功能更强大的终端设备设计的，这些终端设备拥有较多的内存和强大的处理能力，能播放高质量的音视频内容，能将受保护的内容发送给其他 DRM 设备或存储备份。OMA DRM 1.0 和 OMA DRM 2.0 技术的主要区别如下：

(1) OMA DRM1.0：(a)安全度较低：它假定用户终端本身是受信任的，在内容密钥的安全传输及 DRM 内容防篡改方面存在不足；(b)没有获得安全音乐分销曲目的广泛认同；(c)基于移动特定技术；(d)不支持流；(e)不支持针对超级分发的即时预览；(f)不支持多重设备拥有。

(2) OMA DRM2.0：(a)OMA DRM 的实现是基于 PKI 体系的高安全级别：从 RI 到每个用户终端都必须具备自己的数字证书，对内容密钥、版权密钥的生成和传输都有明确规定，对如何抗重放攻击、防止版权内容的篡改也做出了明确规定；(b)采用内容管理授权管理员(CMLA)信任模型；(c)并非基于一些移动特定技术支持 PC 和家用设备；(d)支持分组包媒体；(e)DCF 的普通内容头内，含有支持即时预览功能的预览头；(f)引入域的概念，支持跨多种设备的内容消费，通过域密钥将许可证和受保护内容同整个域绑定，而不是只绑定到一个设备上。允许用户共享同一用户域内所有设备中的离线受保护内容，通过域密钥的更新和管理，实现域内设备的增删和域更新。

4.2 OMA DRM2.0 的不足

在 OMA DRM 体系中，采用分别发送方式发送受保护的 DCF 和 RO 是一个巨大创新，能使内容适用于很多应用场景，因而得到广大厂商支持。但是该体系目前尚存在以下不足：(1)由于受保护的 DCF 和版权对象被分开存放，当版权对象丢失或损坏时，用户就无法继续使用已付费内容，因而影响使用已购买的内容。(2)OMA DRM 采取把 RO 和指定的一个或一组设备相绑定的机制，来确保只有授权用户才能访问内容和 RO。此机制给用户带来很大不便：(a)用户只能在特定的设备上使用已购买的 DRM 内容，而不能带到异地使用；(b)由于 RO 和用户设备已绑定，用户不能升级自己的设备(如计算机)；(c)用户不能将自己购买的 RO 转让给别人；(d)攻击者可通过盗用用户计算机，非法使用数字产品。

5 结束语

DRM技术是信息时代保护数字版权的最新技术，其广泛应用不仅能有效保护数字内容所有者的利益，也将促进整个数字内容消费体系的有序化和可管理化。考虑到文献[2–4]的不足，本文在深入研究最新发布的OMA DRM2.0批准版的基础上，详细分析了OMA DRM技术体系结构，从综合角度出发，给出了一个系统全面的OMA DRM工作流程和原理。本文的分析和研究必将对推动我国数字媒体内容保护的应用研究起到积极作用，并对中国广播影视数字版权管理标准起草委员会正在制定的我国自主的DRM标准有借鉴意义。

参 考 文 献

[1] National Institute of Standards and Technology. MD 20899-8951-2002. A Quick-reference List of Organizations and Standards for Digital Rights Management[S]. 2002.

[2] 姜楠，王键. OMA DRM 和 OMA 下载[J].计算机安全, 2005, (4): 15–54.
Jiang Nan and Wang Jian. OMA DRM and OMA download[J]. *Coputer Security*, 2005,(4): 15–54.

[3] 李学伟，王磊. OMA DRM 体系介绍[J]. 世界宽带网络, 2005, (9): 9–13.
Li Xue-wei and Wang Lei. OMA DRM architecture introduction[J]. *International Broadband Network*, 2005, (9): 9–13.

[4] 王美华，范科峰，王占武. OMA DRM 体系结构分析[J].网络安全技术及应用, 2006, (5): 76–79.
Wang Mei-hua, Fan Ke-feng, and Wang Zhan-wu. Analysis on the OMA DRM architecture[J]. *Network Security Technology and Application*, 2006, (5): 76–79.

[5] 范科峰，赵新华. OMA DRM 技术与标准研究[J]. 信息技术与标准化, 2006, (7): 16–20.
Fan Ke-feng and Zhao Xin-hua. Investigation on OMA DRM technology and standard[J]. *Information Technology and Standard*, 2006, (7): 16–20.

[6] 王力生，曹南洋，梅岩. OMA DRM 体系结构的研究[J]. 网络安全技术及应用, 2006,(7): 71–83.
Wang Li-sheng, Cao Nan-yang, and Mei Yan. Research of OMA DRM architecture[J]. *Network Security Technology and Application*, 2006, (7): 71–83.

[7] Open Mobile Alliance. OMA-TS-DRM-DRM-V2_0-20060303-A. OMA DRM Specification Approved Version2. 0[S]. 2006.

[8] Open Mobile Alliance. OMA-AD-DRM-V2_0-20060303 -A. OMA DRM Architecture Approved Version 2.0[S]. 2006.

[9] Open Mobile Alliance.OMA-TS-DRM-DCF-V2_0-20060303-A. OMA DRM Content Format Approved Version 2.0[S]. 2006.

[10] Open Mobile Alliance. OMA-TS-DRM-REL-V2_0-2006 0303 -A. OMA DRM Rights Expressin Language Approved Version 2.0[S]. 2006.

[11] Open Mobile Alliance. OMA-RD-DRM-V2_0-20060303-A.OMA DRM Requirements Approved Version 2.0[S]. 2006.

魏景芝：　女，1975年生，博士生，研究方向为密码学、网络攻防、DRM.

杨义先：　女，1962年生，教授，博士生导师，研究方向为密码学、信息安全.

钮心忻：　女，1964年生，教授，博士生导师，研究方向为密码学、信息安全.