第35卷 第20期 计 算 机 工 程 2009年10月
Vol.35 No.20 Computer Engineering October 2009
·博士论文· 文章编号：1000—3428(2009)20—0020—03 文献标识码：A 中图分类号：TP311

支持权利二次交易的数字版权保护模型

邓子健[1]，来学嘉[1,2]，何大可[1]
(1. 西南交通大学信息安全与国家计算网格实验室，成都 610031；2. 上海交通大学计算机科学与工程系，上海 200240)

摘 要：提出一种新的支持权利二次交易的数字版权模型。该模型第一次将用户经济利益纳入数字内容产业链中，平衡了数字内容发行商和用户两者的经济利益，激励用户使用正版数字内容。利用基于身份的公钥系统和重加密方案设计新协议，给出该模型的一种实现，并分析了该模型的安全性和经济利益。

关键词：数字版权保护；权利二次交易；信息安全

Digital Rights Management Model to Resell Right

DENG Zi-jian[1], LAI Xue-jia[1,2], HE Da-ke[1]
(1. Laboratory of Information Security and National Computing Grid, Southwest Jiaotong University, Chengdu 610031;
2. Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200240)

【Abstract】 This paper gives a new Digital Rights Management(DRM) model to resell right. The model brings the consumer's economic interests into the industrial chain, balances the interests between content provider and user, and incites the consumer to play legal content. A new protocol using Identity Based Encryption(IBE) and re-encryption scheme to implement this model is designed. Security and economic interests of this model are analyzed.

【Key words】 Digital Rights Management(DRM); right resell; information security

目前的数子版权保护(Digital Rights Management, DRM)研究主要涉及技术[1]、法律 2 个角度，很少有研究关注于经济利益平衡。忽略了用户的利益，使得用户的参与度不高。因此，有必要将技术、法律和经济三者综合考虑。本文在现有的终端平台下，提出一种新的 DRM 模型，在基于角色的方案中，该模型包括 5 部分角色：权利出让者，权利购买者，交易服务器，内容提供商，版权提供商。其目的是支持用户二次买卖其所购买的数字证书，平衡数字内容产业链中各方的经济利益，让用户更灵活地使用所购买的数字内容。

1 相关工作

目前数字版权系统中存在以下问题：用户购买音频文件后，购买的次数为 N_1 次，使用 N_2 次之后，用户打算放弃继续使用其后的 $N_3(N_3=N_1-N_2)$次，但当前的 DRM 系统不支持权利买卖，因此，用户只能选择继续使用该音频文件或者将其转赠给第三方。从经济角度来看，用户损失了 N_3 次音乐费用，同时违背了数字内容是可以买卖的电子商品原则。

文献[2-3]提出了用户所购买的数字内容在 Domain 中共享的方案。在该方案下，用户可以通过自己所拥有的 Device 共享音乐，但是无法出售自己购买的数字内容。

文献[4]提出可以用于权力买卖的 DRM 方案。该方案的安全性依赖于终端安全，用户在其自身终端对所出售的数字内容进行解密操作，其安全性的要求超出了当前 DRM 方案中 DRM Agent[2]的安全能力，可行性不高。

2 模型细节

2.1 模型工作流程

假设权利出让者 *A* 通过内容提供商(CI)和版权提供商(RI)获得了数字内容 CO 和相应的版权证书 RO[2]。*A* 想将购买的数字内容的版权证书售出，并组建一个群 $Group_A$，交易服务器会对其分发一对基于身份的公私钥，在 Group 建立后，*A* 可以在该 Group 有效期内，出售其拥有的数字内容。购买 *A* 的数字内容的买家 *B* 先加入该 Group，并从交易服务器处获得一对临时的基于身份的公私钥用于和 *A* 交易。在用户 *A* 和用户 *B* 协商后，交易服务器分割数字证书，经过用户 *B* 确认支付后，交易结束。

在基于角色的系统中，存在买卖管理服务器，管理 Group，可以由 RI 来承担，也可以由 CI 来承担，本文假设由 RI 来承担。

本文符号约定：PK_U / SK_U 分别表示用户 *U* 平台上 DRM Agent 的公钥/私钥，用于用户 *U* 和服务器通信使用。ID_U 表示基于用户 *U* 身份的公钥，d_U 表示基于用户 *U* 身份的私钥，该公私钥对用于用户 *A* 和用户 *B* 协商时通信使用，出现纠纷时，可以作为证据提交给交易服务器。$E_K(C)$ 表示用密钥 *K* 对内容 *C* 加密，$Sig_U(C)$ 表示用户 *U* 对内容 *C* 的签名。S_U 表示用户 *U* 的终端平台的状态信息，R_U 表示其他用户对 *A* 的评论信息，V_D 表示基于身份的公私钥有效期，一般对于组建 Group 的用户 *A* 该 V_D 较长，而对于加入 Group 的用户 *B*，V_D 较短。*A* 表示出售权利的用户 *A*，*B* 表示购买权利的用户 *B*，*R* 表示 RI。

基金项目：国家自然科学基金资助项目(60573032)；华为科技基金资助项目(YJCB2007048IN)
作者简介：邓子健(1982－)，男，博士研究生，主研方向：P2P 数字版权系统；来学嘉、何大可，教授、博士生导师
收稿日期：2009-03-07 **E-mail：**zijian.deng@gmail.com

2.2 Group 的概念

从版权控制的角度以及公平交易的角度考虑，本文首次提出了买卖 Group 的概念，对于一个出售自己所购买的版权的用户 A，系统中存在一个属于 A 的 Group(用 $Group_A$ 表示)。购买 A 的数字商品的用户都必须先加入该 Group，Group 的概念类似于 OMA 中的 Domain，但是与 Domian 所不同的是，Domain 中的实体是平等的，任何实体均可以使用 Domain 内的数字内容，实体加入 Domain 后，一段时间是稳定的，退出 Domain 需要通知 RI；Group 中的实体不是平等的，以该 Group 中的卖家为中心，数字内容在 Group 中是买卖的关系，不是共享关系，在买卖结束后，买方就退出 Group，退出过程不需要 RI 参与。

2.3 Group 的组建

用户 A 向 R 申请组建一个 Group，协议如下：

Step1 A->R: $E_{P_R}(S_A \| A \| Sig_A(S_A \| A))$

A 向 R 发送 Create Group Request，该请求包括用户 A 平台上 DRM Agent 的状态信息 S_A 及用户标识 A。

Step2 R->A: $E_{P_A}(d_A \| V_D \| Sig_R(d_A \| V_D))$

R 通过 S_A 验证 A 上 DRM Agent 的软件状态信息，并且查看该平台是否安全，验证通过后，生成基于 A 身份的私钥。如果验证通过，R 生成组建 Group 所需要的信息。R 向 A 发送 Create Group Response，该响应包括基于用户 A 身份的私钥 d_A，该 Group 的有效期 V_D，超过 V_D 后，该 Group 自动注销。

2.4 Group 的加入

创建及加入组的示意图如图 1 所示。

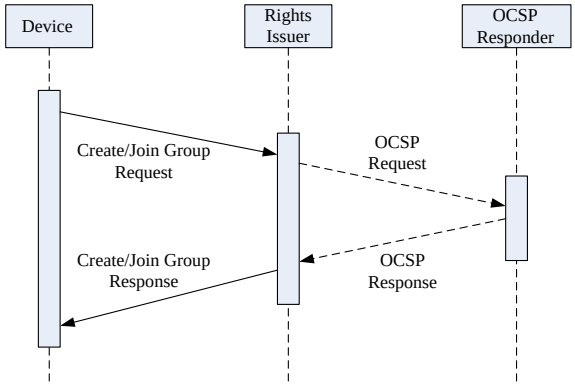

图 1　创建/加入组示意图

当用户 B 对用户 A 所出售的数字内容感兴趣时，B 加入 $Group_A$，该协议如下：

Step1 B->R: $E_{P_R}(S_B \| B \| G_A \| Sig_B(S_B \| B \| G_A))$

B 向 R 发送 Join GroupRequst，其中包括 S_B 用户 B 平台的 DRM Agent 状态信息、用户 B 的标识 B、加入的群 G_A。

Step2 R->B: $E_{P_B}(d_B \| V_D \| R_A) \| Sig_R(d_B \| V_D \| R_A)$

R 查看 B 的状态信息，同时验证 A 是否被吊销，验证通过后，生成基于身份的私钥 D(用户名+时间+群名)和该密钥有效期 V_D，默认值为 1 天。

2.5 协商

协商过程使用基于身份的公私钥对通信，协商完毕后，用户 A 将 $E_{d_A}(N_1 \| N_3 \| B \| C \| T)$ 发送至 R，用户 B 将 $E_{d_B}(N_3 \| A \| C \| T)$ 发送至 R。其中，$E_{d_A}(N_1 \| N_3 \| B \| C \| T)$ 中的 N_1 代表 A 现有的版权证书中剩余的次数；N_3 表示将要转让的次数；B 代表将要转让给组中的用户名；C 表示转让费用；T 表示时间戳。$E_{d_B}(N_3 \| A \| C \| T)$ 中的 N_3 表示 B 需要购买的次数；A 表示 B 需要购买的用户的标识；C 表示购买的费用；T 表示时间戳。R 收到买卖双发发送的信息后，比较两者中的协商信息，如果以上通过，则 R 触发版权交易协议执行。

2.6 证书分割协议的运行

证书转让协议示意图如图 2 所示。

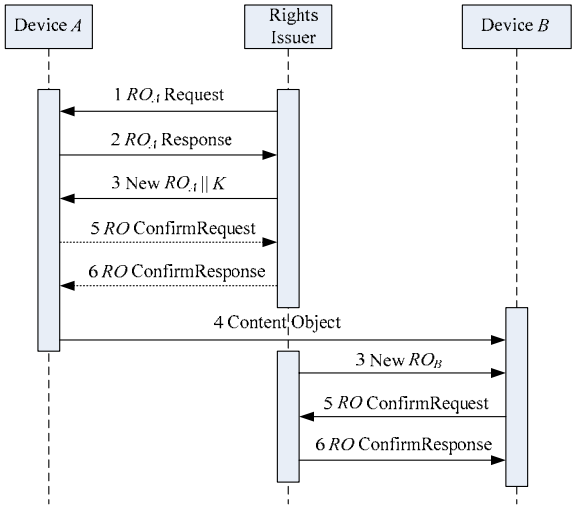

图 2　证书转让协议示意图

运行证书分割的协议如下：

Step1 R->A: *Request* RO_A

R 向卖家 A 的 DRM Agent 请求发送当前的版权证书 RO_A、当前平台状态 S_A 等信息。

Step2 A->R: $E_{P_R}(RO_A \| S_A \| Sig_A(RO_A \| S_A))$

卖家 A 的 DRM Agent 将当前数字证书 RO_A、DRM Agent 状态信息 S_A 发送给 R。当 R 收到来自卖家 A 的 RO_A 后，首先验证该 RO_A 是否有效，然后检查当前 DRM Agent 的状态值 S_A 是否有效。以上验证通过后，R 将 RO_A 按照 2.5 节中双方协商的要求进行分割，分割过程如图 3 所示。其中的 Root RO 代表原 RO，Leaf RO 代表分割后的 RO。

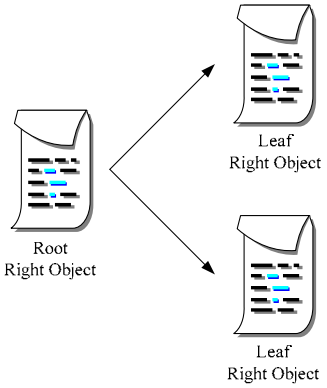

图 3　证书分割过程

在该分割协议下完成全分割和部分分割 2 种操作。全分割是指新的 RO 全部继承原 RO，部分分割是指将原 RO 分割为 2 个独立的 RO。全分割可以作为部分分割的一个子集，在该子集中，分割后的一个证书的使用次数是 0 次。在 2 种分割情况下，使用重加密[5]方案，生成的 Leaf RO 中的内容加密密钥不同于 Root RO 证书中的内容加密密钥，具体见 Step4。

Step3

(1)R->A: $E_{P_A}(RO_A \| K_2 \| Sig_R(RO_A \| K_2))$

RO_A Response，R 将新生成的 RO_A 和内容加密密钥 K_2 发送给 DRM Agent A。

(2)R->B: $E_{P_A}(RO_B \| Sig_R(RO_B))$

RO_B Response，R 将新生成的 RO_B 发送给 DRM Agent B。

Step4 A->B: $E_{ID_B}(E_{K_2}(E_{K_1}(C)) \| T \| Sig_A(E_{K_2}(E_{K_1}(C)) \| T))$

DRM Agent A 用在 Step3 中收到的 K_2 加密存储在本地上的数字内容，该数字内容以密文形式存储：$E_{K_2}(E_{K_1}(C))$。加密后将 $E_{K_2}(E_{K_1}(C))$ 发送给用户 B，用户 B 中的 DRM Agent 可以根据 RO_B 中的内容解密密钥 K_3，对其解密使用 $E_{K_2}(E_{K_1}(C)) = E_{K3}(C)$。

Step5

(1)A->R: RO_A *ConfirmRequest*;

A 检查所获得的新 RO 后，确认；否则，发送 Error 信息。

(2)B->R: RO_B *ConfrimRequest*;

B 检查所获得的新 RO 后，确认并发送支付信息；否则，发送 Error 信息。

Step6

(1)R->A: RO_A *ConfirmResponse*;

(2)R->B: RO_B *ConfirmResponse*。

2.7 支付协议

当 B 收到自己所购买的版权文件后，确认并支付。在该系统中，R 会对每笔交易收取一定的版权费用，详细的分析见经济利益分析。

3 模型分析

3.1 经济利益分析

假设用户 A 购买了一段音频，花费是 C_1，次数是 N_1。在使用了 N_2 次后，用户 A 还剩下 N_3 次可以使用(N_1=N_2+N_3)，A 想将 N_3 次出售，出售价格是 C_2。用户 B 选择从 A 处购买 N_3 次，假设花费为 C_2，其中 A 获得 C_2 中的 n%，剩下的为 R 获得的版权费用。在系统出售了 N_1 次后，三者的利益是：音乐播放次数为 N_1，R 获得的利益是 $C_1+C_2 \times n\%(>C_1)$，A 付出的价值为 $C_1-C_2 \times (1-n\%)$，B 付出的价值为 C_2。在该方式下，三者的利益在不破坏对方利益的前提下都得到了最大化。

3.2 安全性分析

内容安全：每个平台的数字内容都用不同的内容密钥加密，在二次分发模式和文献下，被分发的数字内容和原分发平台上的数字内容都使用同一内容密钥加密，在大规模分发的情况下，一旦某个平台上的内容密钥被泄露，其他平台的数字内容都有被泄露的危险。在 DRM Agent A 对数字内容加密的过程中，K2 并不是解密密钥，K2 所加密的数字内容也是密文，因此，即使到 K2，数字内容安全仍然不受影响。而且该协议并没有增加对 DRM Agent 的安全要求，兼容现有的 DRM Agent。

交易欺骗：在交易过程中可能存在 2 种欺骗，即证书欺骗和内容欺骗。证书欺骗是指交易后的证书中的信息和双方协商的证书中的信息不符，在本方案中，在协商提交给 R 后，R 会发现双方信息不符，证书的分割由 R 执行，因此，不会出现证书欺骗。内容欺骗是指在证书转让协议 Step4 中，用户 A 发送给用户 B 的内容和所使用的数字内容不符，用户 B 在收到内容后，将对其验证。如果在协商过程中不服，则在证书转让协议的 Step5 中，B 将发送 Error 信息给 R，并提供相应的证据给 R。

4 结束语

本文在 DRM 中提出了一种新的 DRM 模型，在不损害双方利益的前提下，该模型平衡了数字内容发行商利益和用户利益，并首次将用户纳入数字内容利益链中。本文设计了新的协议以作为该模型的一种具体实现，能够在保证数字内容安全和交易公平的前提下，使得用户在购买了数字内容后将其成功转让，该协议兼容现有的 OMA 标准。从模型分析可以看出，在保障内容安全的前提下，该模型中用户购买数字内容并将其再次出售后，数字内容提供者、权利出售者、权利购买者的经济利益没有受到损失。

参考文献

[1] Abbadi I M, Mitchell C J. Digital Rights Management Using a Mobile Phone[C]//Proc. of the 9th International Conference on Electronic Commerce. Minneapolis, USA: [s. n.], 2007: 185-194.

[2] Open Mobile Alliance[DB/OL]. (2008-03-21). http://www.openmobilealliance.org.

[3] Abbadi I. Digital Asset Protection in Personal Private Networks[C]//Proc. of the 8th International Symposium on Systems and Information Security. Sao Paulo, Brazil: [s. n.], 2006: 185-194.

[4] Nair S K, Posescu B C. Enabling DRM-preserving Digital Content Redistribution[C]//Proc. of the 7th International Conference on E-commerce Technology. [S. l.]: IEEE Press, 2005: 151-158.

[5] Canetti R, Hohenberger S. Chosen-ciphertext Secure Proxy Re-encryption[C]//Proc. of the 14th ACM Conference on Computer and Communications Security. Alexandria, Virginia, USA: [s. n.], 2007: 185-194.

编辑　顾逸斐

~~~~~~

(上接第 19 页)

Proc. of International Colloquium on Computing, Communication, Control, and Management. Sanya, China: IEEE CS Press, 2009.

[5] Chappell D. .NET 大局观[M]. 2 版. 荣　耀, 译. 北京: 电子工业出版社, 2006.

[6] 荣　耀, 李　昕. 企业级 AJAX 框架设计与实现[J]. 南京师范大学学报: 工程技术版, 2007, 7(3): 64-69.

[7] Rumbaugh J, Jacobson I, Booch G. UML 参考手册[M]. 姚淑珍, 唐发根, 译. 北京: 机械工业出版社, 2001.

[8] Gamma E, Helm R, Johnson R, et al. 设计模式: 可复用面向对象软件的基础[M]. 李英军, 译. 北京: 机械工业出版社, 2000.

编辑　任吉慧
~~~~~~