计费公平的安全移动数字版权管理方案

黄晓芳[1,2]，赖 欣[3]，马兆丰[1]，杨义先[1]，钮心忻[1]

(1. 北京邮电大学网络与交换技术国家重点实验室信息安全中心 北京 海淀区 100876;
2. 西南科技大学计算机科学与技术学院 四川 绵阳 621000; 3. 西南交通大学信息安全与国家网格计算实验室 成都 610031)

【摘要】在现有移动数字版权管理的研究基础上，结合目前3G无线通信网络给出了一种计费公平的安全移动数字版权管理方案，保证了媒体内容和版权对象的机密性和完整性，防止了版权中心的剽窃；并提出一种无需可信第三方参与的公平支付机制应用在该方案中，降低了协议的实现代价，减少了参与方的交易成本。最后对该方案的安全性进行了分析，证明了该方案的安全性和可靠性。

关 键 词 并发签名； 内容中心； 数字内容； 移动DRM； 版权中心
中图分类号 TP309 **文献标识码** A doi: 10. 3969/j. issn. 1001-0548. 2009. 02. 33

Secure Mobile DRM Solution on Fair Charging

HUANG Xiao-fang[1,2], LAI Xin[3], MA Zhao-feng[1], YANG Yi-xian[1], and NIU Xin-xin[1]

(1. Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications Haidian Beijing 100876; 2. Department of Computer Science, Southwest University of Science and Technology Mianyang Sichuan 621000;
3. Information Security and National Computing Grid Laboratory (IS&NC), Southwest Jiaotong University Chengdu 610031)

Abstract Based on the research of mobile digital rights management (DRM), a charging fair solution of secure mobile DRM for applications in 3G wireless communication networks is proposed. The secure mobile DRM solution guarantees the security and integrity of the digital contents and right objects, and prevents the right issuers cribbing the digital contents. Furthermore, a practical fair payment protocol without TTP is presented and used in this mobile DRM, it leads to cost reductions of protocol implementation and involving exchange. At last, the security analysis and efficiency comparison are presented.

Key words concurrent signature; content issuer; digital content; mobile DRM; right issuer

随着移动通信设备的普及和功能的不断完善，用户们开始频繁地使用移动设备来传输多媒体数据。互联网中面临的数字版权管理问题，又在移动数字媒体出版商身上重演。因此如何对移动数字媒体内容进行版权管理，对其使用与转发进行控制和计费，以保护运营商和内容提供商的利益，成为一个迫切需要解决的问题。针对这一情况，本文在对国内外移动数字版权管理(DRM)的研究基础上，结合目前3G无线通信网络给出一个计费公平的安全移动DRM方案，提出一种新的内容密钥分发机制和应用在移动DRM中的无需可信第三方参与的公平支付协议，证明了该协议满足安全性和公平性要求。最后，通过和其他移动DRM方案进行比较，证明本文提出的移动DRM方案在数字内容的完整性保护、内容密钥的安全分发和支付协议的公平性方面均有突出表现，并且通信和计算代价小，适合移动通信环境。

1 相关工作

近来，Microsoft、LockStream、NDS、InterTrust等公司相继推出了自己的DRM系统，而针对移动通信领域也出现了相应的数字版权管理方案，但大部分方案彼此不兼容。针对这一状况，很多研究组织致力于此项标准的研究，如3GPP、3GPP2、OMA等。其中，OMA制定的移动DRM标准得到了广泛的支持和认同。在OMA DRM v2.0中，文档详细定义了数字内容和版权对象的安全模型，对数字内容以及版权对象给出了保护格式和机制，支持客户端和内容认证中心的双向认证和域版权许可授权[1]。

在学术界，移动DRM也同样受到了广泛的关注。文献[2]提出利用移动网络运营商对移动终端进行认证，并负责版权对象的转发，支付费用加至用户话费清单的交易模式。但在这种交易模式中，由

收稿日期： 2007 ↖ 12 ↖ 25；修回日期：2008 ↖ 10 ↖ 30
基金项目：国家973项目(2007CB311203)；北京市自然科学基金(4062025)
作者简介：黄晓芳(1977 ↖)，女，博士生，主要从事通信安全、移动支付、数字版权管理方面的研究.

于所有用户下载的版权对象都需要移动网络运营商进行转发，而每次支付都需要可信第三方参与，容易导致可信第三方和移动网络运营商成为系统中的通信瓶颈。而且这种购买方式也只适合交易金额不大的微支付情况。随着移动业务的发展，这种单一的微支付方式已经不再能满足用户和内容提供商的需求。为了满足大宗交易的需求，出现了以电子支票为支付手段的移动DRM系统。文献[3-4]提出的基于智能卡的移动DRM系统，利用防篡改设备作为系统可信基础，电子账户信息存储在智能卡中，利用智能卡和版权中心进行匿名认证和电子支票支付。但是该支付中，没有提供公平支付的保障机制和交易纠纷的解决方法。

在内容密钥(contents encryption key, CEK)的分发方面，文献[5-6]指出当版权中心和内容提供商分属不同的运营商时，版权中心控制内容密钥，容易导致版权中心对保密的数字内容进行剽窃，因此提出了将加密的内容密钥分成两个子密钥，分别嵌入版权对象和数字媒体内容中发送给版权中心和移动终端，以防止版权中心对数字内容的剽窃。但该方案增加了DRM实现的复杂性，而且并不实用，不能从根本上防止数字内容和内容密钥的非法传播问题。

国内多数文献[7-13]对DRM的研究主要集中在数字版权描述语言和数字水印算法的改进方面，对移动DRM方面的研究较少。而本文主要侧重于讨论移动计算领域中的数字版权管理。

2 计费公平的安全移动DRM系统方案

2.1 系统框架

本文提出的计费公平的安全移动DRM系统也采用了OMA DRM的核心思想，该系统架构包含以下功能实体：

移动终端：本文中提到的移动终端，如果没有特别说明，均为移动电话。

DRM代理：下载在移动终端中的代理程序，负责控制数字内容的使用。

内容中心(content issuer, CI)：主要负责对数字媒体内容进行封装，根据移动终端的下载请求，产生内容密钥，利用CEK将数字媒体内容加密封装成DRM的内容格式(drm content format, DCF)，分别将数字内容的使用权限和部分密钥信息发送给版权中心，DCF发送给DRM代理。

版权中心(right issuer, RI)：根据数字内容中心传送的信息，对合法用户产生和分发媒体内容使用的相应的版权对象(right object, RO)，其中定义了数字媒体内容的使用权限和相应的密钥。

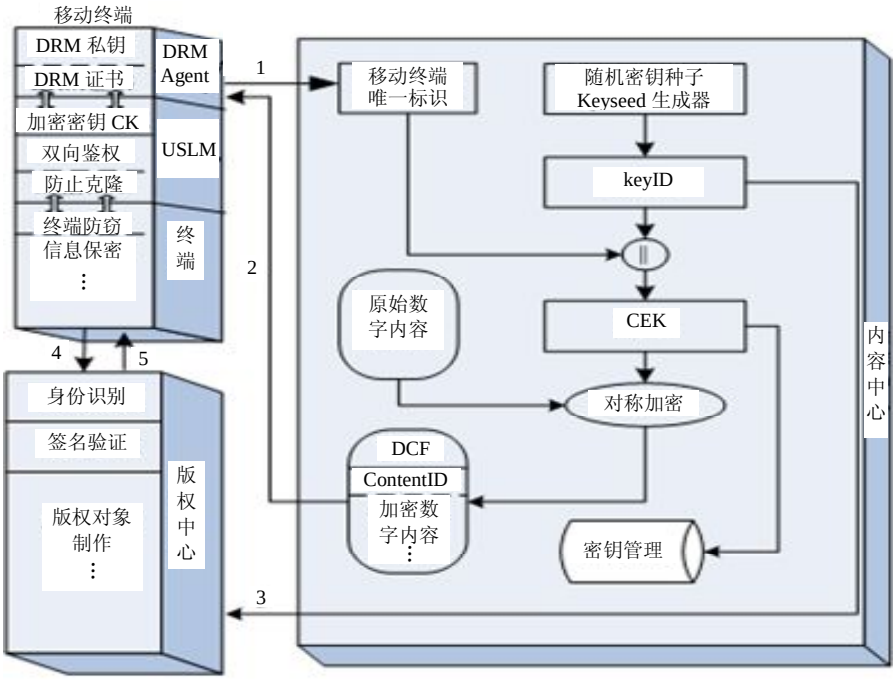

图1　安全的移动DRM系统架构

系统架构的核心思想还是采用OMA DRM中内容与版权相分离的思想，首先用户通过移动终端的DRM代理向数字内容中心发出下载请求，数字内容中心根据DRM代理发出的下载请求，对数字媒体内容加密打包转换成DCF格式，然后将其发送给DRM代理，同时把相应的内容使用权限、解密密钥等信

息发送给版权中心。DRM代理收到DCF后，根据DCF中包含的版权中心的地址，向版权中心提出下载请求，通过身份认证后，下载对应的版权对象。由于版权对象用相应的DRM代理的公钥加密，所以只有指定的DRM代理才能解密版权对象，从而恢复出加密的数字媒体内容。本文系统架构如图1所示。

本文与OMA标准的不同在于以下两个方面的改进：

(1) 内容密钥的安全分发：为了防止版权中拥有每个DRM内容的完整的密钥，该方案中，内容密钥由两部分组成，一部分由内容中心保密管理的密钥种子KeyID，另一部分为DRM代理产生的随机数组成，该随机数是基于USIM的密钥种子在每次请求下载时产生的，而这部分密钥信息不需用发送给版权中心，这样，既保证了只有经过授权的移动终端才能解密购买的数字内容，同时防止了版权中心掌握内容密钥后，对数字内容的剽窃。

(2) 数字版权对象的公平交换：在RO的申请下载和获取过程中，设计了安全公平的交换协议，完善了OMA DRM规范中支付机制的缺憾。

在支付阶段，本文系统在并发签名体制的基础上，提出一种无需可信第三方参与的公平的移动支付方式，保证了参与各方的利益。并发签名(concurrent signatures)体制[14]的基本思想是发起者掌握一个秘密信息keystone，按照协议双方各自产生一个签名，在keystone公开以前，两份签名的签名主体信息对任意第三方都是模糊的，一旦keystone公开，签名和签名者的身份绑定。而且，相比文献[15]提出的基于并发签名，由商户掌握keystone的支付协议，本文协议更加注重于保证客户的利益，让客户在电子交易中不再处于劣势，客户具有可否认签名的权利，而内容提供商只有部分可否认性，一旦客户出示keystone，内容提供商不能抵赖签名，而且客户在交易前中断协议不会有隐私泄漏的风险。如果内容提供商掌握keystone，则有可能出现恶意的内容提供商，他们只收集客户的消费依据，而不提供实质性的数字内容，用户发送模糊签名后，内容提供商并不发送有效的版权对象，而是将keystone和用户的签名绑定给予任意的第三方，收集客户的消费情况。

本文重点对该方案的价格协商子协议和移动支付子协议做详细的描述和分析。

2.2 协议描述

2.2.1 记号和符号

本文方案中参与的实体包括：移动终端的DRM代理(统称为客户C)、内容中心CI和版权中心RI，协议将使用到的基本标识符如表1所示。

表1 基本标识符

A→B:X	A给B发送消息X
X_A	A的公钥
x_A	A的私钥
ID_A	A的身份标识
check	用户的电子支票
E(check,k)	利用k对电子支票加密
l	会话标识符
Sig_A (m)	A对消息m的普通签名
∇_A (m)	A对消息m的并发签名
H(m)	对消息m用Hash函数取摘要值
$m\|\|n$	消息m和消息n的级联

2.2.2 价格协商子协议

在该协议中，C发出下载请求，其中包括价格和使用权限等信息。CI收到C的请求后，验证用户是否合法，验证成功后，则将价格信息进行核对。如果价格符合，则发送价格确认信息和提供服务的品质保证等信息。详细协议步骤如下：

(1) C→CI：OI,ID_C, l, Sig_C(H(OI|| l))

(2) CI→C：OIRes, TID, l, Sig_{CI}(H(OIRes|| TID|| l))

其中，OI是订购信息，包括C要购买的数字内容的标识、价格和使用权限等；ID_C是C的身份标识；Sig_C(H(COI||1))，是用DRM代理的私钥进行签名。CI首先验证C的身份，通过后，则对OI中的信息进行确认，如果数字产品的标识、价格和使用权限等信息与CI公布的一致，则CI发送OIRes响应客户的订购请求，OIRes中包括数字产品的标识、价格和使用权限，以及CI对相关服务或产品的品质承诺等。TID为交易标识信息，包括交易时间和日期等。

2.2.3 支付子协议

C和CI协商好数字内容相关的交易信息后，开始执行支付协议。在协议中，对于银行支票的信息，采用并发签名算法进行签名。该协议前提是，C需要在银行建立一个账户，并申请电子支票业务，下载证书和签名程序到移动设备上。

文献[14]提出的并发签名定义中，包括以下4个算法阶段：

(1) 参数建立。

消息空间M、keystone空间K：M=K={0,1}*、密钥映射空间F=Z_q^*，以及函数KGEN：$K \rightarrow F$。随机选择2个大素数p、q，满足$q|(p-1)$，q阶生成元$g \in Z_p$，散列函数$H_{1,2}$：{0,1} $\rightarrow Z_q$，x_i和y_i分别为私钥和

公钥，且$y_i = g^{x_i} \bmod p$。

(2) 并发签名算法。

一个并发签名算法Csig对于输入$<y_i,y_j,x_i,f,m>$，y_i、y_j是公钥且$y_i \neq y_j$，x_i是相应y_i的私钥，$f=H_2(k)$，$k \in K$，$m \in M$，随机数$\Leftrightarrow \in Z_q$，计算$h= H_1((g^{\Leftrightarrow} y_j^f \bmod p)||m)$，$h'=(h \nwarrow f) \bmod q$，$c=(\Leftrightarrow \nwarrow h' x_i) \bmod q$，输出关于$m$的签名 $\bigtriangledown = <c, h', f>$。

(3) 验证算法。

算法AVERIFY，输入$<\bigtriangledown, y_i, y_j, m>$，如果：

$$h' + f \equiv (H_1((g^c y_i^{h'} y_j^f \bmod p)||m)) \bmod q$$

则签名正确，否则输出拒绝。

(4) 鉴别算法。

算法VERIFY(k,S)，输入$<k,S>$，$k \in K$，$S = <\bigtriangledown, y_i, y_j, m>$。首先运行验证算法是否成立，如果不成立则中止；否则将$H_2(k)$和h'、f的值分别比较。如果$H_2(k)=f$，则i为签名者；如果$H_2(k)= h'$，则j为签名者。

支付协议详细步骤如下：

(1) C→CI：E(check,k), TID, f, X_C ,X_{CI} , $\bigtriangledown_C$, l

C选择一个随机数k，计算$f = H_2(k)$，根据协商好的价格填写好电子支票，根据并发签名算法，用f对$H(E(\text{check},k)||\text{TID}||f||X_C\ ||X_{CI}||l)$进行并发签名，生成$\bigtriangledown_C$发送给CI。

(2) CI→C：DCF, m_{CI}, $\bigtriangledown_{CI}$, X_C , X_{CI} , l

CI收到C的信息后，首先用验证算法AVERIFY验证签名的有效性，如果无效则中止协议；否则将用对称密钥CEK加密后的数字内容打包成DCF格式发送给C，并利用收到的散列函数值f，用相同的签名算法对消息m_{CI}签名后发送给C。其中，$m_{CI}= H(\text{DCF}||\text{TRI}_{RO}||f||\text{TID}||X_C||X_{CI}||l)$，$\text{TRI}_{RO}$是触发C到相应的版权中心下载版权对象，包括版权中心的地址、版权对象的标识等。

(3) C→RI：$E(k||\ m_{CI}||\ \bigtriangledown_{CI}||\text{TID}||\ l, X_{RI})$

C将收到的M签名，经过同样的验证算法验证后，将其和k用RI的公钥加密后发送给RI。

(4) RI→CI：$E(k||l, X_{CI})$

RI→C：$E(\text{RO}||\ l, k)$

RI用VERIFY对k进行鉴别，如果有效则CI和C对各自的签名都得到绑定。RI首先检查CI的签名，如果证实CI的签名，并且TID中时间有效，则将k用CI的公钥加密后发送给CI，CI利用k解密得到check信息，然后连同C的签名发送给银行，进行转账或取款；同时，根据签名内容将相应的版权对象RO用k对称加密后发送给C，这样既验证了C的身份，同时也减少了计算量。

在协议中，C只需存储为本次交易产生的k和CI的签名，存储信息少，不会占用移动存储的空间；而且整个交易过程中，只有5条信息的交互，减少了无线网络的通信开销。该协议不需要额外地解决争端的子协议或是其他可信第三方的参与，因为客户要想享用购买的电子产品，则必须公开k，而一旦k公开，则CI就可以获得电子支票，并且联合客户的签名获得应有的酬劳。如果C不公开k，那么CI也可以否认自己的签名，版权中心无法鉴别CI的签名，则会拒绝C的要求，不会发送版权对象给C，这样客户和内容提供商都没有损失。

2.3 安全性分析

(1) 数字内容及版权的机密性和完整性。

首先CI对保护的数字内容采用对称加密算法进行加密，加密后，数字内容转化为DCF格式供下载。数字内容的密钥由两部分组成：一个是内容中心自己提供的密钥种子；另一个由DRM代理产生的随机数组成，该随机数是基于USIM的密钥种子在每次请求下载时产生的，这样防止了任何一方对内容的剽窃或联合欺骗，保证最后只有被授权的移动终端才能解密相应的数字内容。

(2) 支付的公平性。

本文提出的支付协议利用并发签名机制达到公平支付的目的，而且不需要可信第三方的参与。作为协议的发起方，客户C掌握着是否释放以及何时释放秘密信息k的权利。看起来协议并不公平，因为如果客户不释放k，则内容提供商CI无法将支票和客户的签名绑定，得不到相应的支付款；但是客户也得不到相应的版权对象，无法解密下载的数字内容，因此双方无损失。而且在现实生活中，很少有客户下载了数字内容而不愿去购得版权对象的，因为加密的数字内容对客户来说，是没有用的。所以对于客户来说，具有完成交易的需求。

在电子交易中，通常客户是作为弱势群体，商户往往掌握了交易的控制权，但是在本文协议中，利用客户掌握k，使得在完成交易前，客户具备一定的优势，如果客户发现延时过长或是内容提供商有欺诈嫌疑，则可以中断交易，并且否认自己的签名。同时，版权中心没有正确的k，因此也无法验证CI的签名，所以不会发送相应的版权对象给客户。双方无损失，保证了协议的公平性。

(3) 可追究性和抗抵赖。

在价格协商子协议中，内容提供商和客户都利用自己的私钥对协商好的价格和服务进行了签名，

因此$Sig_C(H(OI||l))$和$Sig_{CI}(H(OIRes||TID||l))$可以作为当数字内容的价格和付款金额出现不一致时的会话证据，出示给第三方仲裁，这个阶段的协议有CA参与，但并不影响在支付协议中提出的无需可信第三方参与的性质。

支付协议阶段的不可否认的证据在协议执行到步骤(3)时才产生， 当客户公开keystone以后，则发方非否认证据(evidence-of-origin, EOO)和收方非否认证据(evidence-of-receipt, EOR)分别为：

$$EOO=\nabla_C=Sig_C(H(E(check,k)||TID||f||X_C||X_{CI}||l))$$

$$EOR=\nabla_{CI}=Sig_{CI}(H(DCF||TRI_{RO}||f||TID||X_C||X_{CI}||l))$$

利用文献[16]提出的方法对本文的公平支付协议的可追究性和公平性进行形式化分析，可得到：

(1) CI can prove (C claims (check||TID))

(2) C can prove (CI claims (H(DCF) $||TRI_{RO}||$TID))

因此支付子协议满足可追究性目标，只要keystone一公开，参与各方不能抵赖自己的签名。

2.4 效率比较

将本文提出的移动数字版权管理方案和文献[2]提出的利用移动网络运营商作为版权对象转发者的解决方案(MNOFee)及文献[4]中提出的应用智能卡等可信设备的数字版权管理系统方案(CardDRM)进行比较，结果如表2所示。

表2 与其他支付协议的比较

		MNOFee	CardPay	本文系统
数字内容的完整性		有	有	有
内容密钥分发的安全性		不安全	不安全	安全
可追究性和抗抵赖性		有	无	有
支付协议	公平性	有	无	有
	公平性的基础	在线TTP	/	无
	公钥加密次数	3	3	2
	公钥解密次数	3	3	2
	对称密钥加解密次数	1	1	2
	产生签名的个数	4	2	2
	需要鉴别的签名个数	4	2	2
	交换的消息条数	7	6	5

从表2可以看出，本文方案比其他移动DRM系统具有明显的优势，计算和通信的代价都比较低，适合移动通信环境。而且基于智能卡的CardDRM需要强假设条件，可信基础是建立在智能卡可信并且防篡改基础上的，这种将整个系统的安全性建立在某个参与方或实体的可信基础上，在理论上是不安全的，在实际中也是不实用的。而本文方案的支付协议是在没有强假设条件下，也无需可信第三方的介入，仍然保证了安全公平的支付要求。因此，本文提出的移动版权管理方案满足安全性要求，而且所需的计算和通信开销都比较小。

3 结 论

本文在现有移动DRM及其标准的研究基础上，结合目前3G无线通信网络给出一个安全的移动数字版权管理方案，提出将内容密钥分为两部分分发，保证只有授权的用户才能拥有完整的内容密钥。同时设计了应用在移动DRM中的无需可信第三方参与的公平支付协议，并对协议进行安全性分析和证明。通过和其他移动DRM系统在安全性和效率等方面进行比较，证明该方案系统在数字内容的完整性保护，内容密钥的安全分发和支付协议的公平性方面均有突出表现，并且通信和计算代价小，适合移动网络环境。

参 考 文 献

[1] OMAForum.OMA-TS-DRM-DRM-V2_0-20050915-C [EB/OL]. (2005-9-15)[2007-6-5]. http: //www.openmobilealliance.org

[2] SORIANO M, FLAKE S, TACKEN J, et al. Mobile digital rights management: Security requirements and copy detection mechanisms[C]//Proceedings of Sixteenth International Workshop on Database and Expert Systems Applications. Copenhagen, Denmark: IEEE Press, 2006: 251-256.

[3] ATALLAH M J, LI J. Enhanced smart-card based license management[C]//IEEE International Conference on E-Commerce. California: IEEE Press, 2003, 111-119.

[4] SUN Hung-min, HUNG Chi-fu, CHEN Chien-ming. An improved digital rights management system based on smart cards[C]// Digital EcoSystems and Technologies Conference.DEST'07. Cairns: Inaugural IEEE-IES, 2007: 308-313.

[5] JEONG Y, YOON K, RYOU J. A trusted key management scheme for digital rights management[J] ETRI J, 2005, 27(1): 114-117.

[6] 郑 宇. 4G无线网络安全若干关键技术研究[D]. 成都: 西南交通大学, 2006.
ZHENG Yu. Research on some key security issues of 4th generation wireless networks[D]. Chengdu: Southwest Jiaotong University, 2006.

[7] 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 Yin-yan, TANG Zhi. A survey of the research on digital rights management[J]. Chinese Journal of Computers, 2005, 28(12): 957-968.

(下转第308页)