基于 P2P 模式的数字版权管理系统

陈绪乾[1],孟宪明[1],陈绪鹏[2],王 纬[1]
CHEN Xu-qian[1],MENG Xian-ming[1],CHEN Xu-peng[2],WANG Wei[1]

1.山东水利职业学院 信息工程系,山东 日照 276826
2.山东省曲阜市陵城镇中学 信息教育中心,山东 曲阜 273100
1.Information and Engineering Department,Shandong Water Polytechnic,Rizhao,Shandong 276826,China
2.Information Education Center,Qufu Lingcheng Town Middle School of Shandong Province,Qufu,Shandong 273100,China
E-mail:epchen02@163.com

CHEN Xu-qian,MENG Xian-ming,CHEN Xu-peng,et al.Digit Rights Management system based on P2P.Computer Engineering and Applications,2009,45(24):241-245.

Abstract: A DRM system based on P2P whose certificate and digital production can both transmitted among users is presented to solve the bottle-neck problem of the system.The improvement of the system is to make the digital production transmitted quicker,at the same time,the digital right of the production can be saved in security.The security of the system is given finally.
Key words: Digit Rights Management(DRM);P2P;k-Times Anonymous Authentication(k-TAA);bilinear pairs

摘 要:设计了一个具有 P2P 特性的数字版权管理系统,该系统的证书和数字内容都可以在用户间传送,充分发挥了点对点传输的效率,有效解决了系统瓶颈的问题。使得既能以可观的速度传输数字产品,又能对版权实施有力的保护。最后,对系统的安全性给出了证明。
关键词:数字版权管理;P2P;k 次匿名可验证(k-TAA);双线性对
DOI:10.3778/j.issn.1002-8331.2009.24.073 **文章编号:**1002-8331(2009)24-0241-05 **文献标识码:**A **中图分类号:**TP393

与传统客户/服务器(C/S)模式的网络相比,P2P 网络(P2P network)具有直接、快速、灵活的数字内容传输优势[1-5]。与此同时,P2P 技术的发展也引发了一系列争议,主要集中在它对现有版权体系的巨大冲击以及它带来的信息控制上的困难等方面。1999 年,美国 Napster 版权案的出现成为 P2P 网络构成对数字内容版权侵犯的标志,直到今天,Napster 公司仍然没有摆脱困境。

数字版权管理(Digit Rights Management,DRM)系统[6-7]的出现为保护数字智能财产提供了可能。它灵活管理不同平台(PC、LAPTOP、PDA、手机)不同形式的数字内容(如音视频流、数字书本、图片),严格控制数字内容的分发和使用,阻止非授权访问,限制访问权限,为数字内容提供了持久保护。DRM 的核心是数字证书的管理和使用。用户无需购买数字内容,取而代之的是购买证书来获取访问数字内容的相应权限。受保护的数字内容可以通过客户机服务器系统、超级分发、数字音频/视频广播形式来进行分发。没有经数字证书处理过的内容是一长串无规则的位串。受保护的数字内容和证书通常分别存储,这样可以使受保护的内容在用户中自由分发,证书可以在以后使用的时候再进行请求,这种方式使系统更具灵活性。

然而,传统的 DRM 系统也存在证书和内容服务器过于繁忙的特点。由于证书和数字内容必须在服务器上进行下载或申请,导致系统效率太低下而用户也无法以可观的速度得到需要的数字产品。为了解决这个问题,可以把 P2P 技术的优点渗透到 DRM 系统的设计理念中,这样,既可以解决传统 DRM 系统的传输速度慢,服务器拥挤的缺点,又可以解决 P2P 内容分发模式的版权缺失问题。

1 研究背景

1.1 传统的 DRM 系统基本架构

图 1 是一个 DRM 系统的最基本流程:首先,内容提供者(Content Provider,CP)先到票据交换中心(Clearing House,

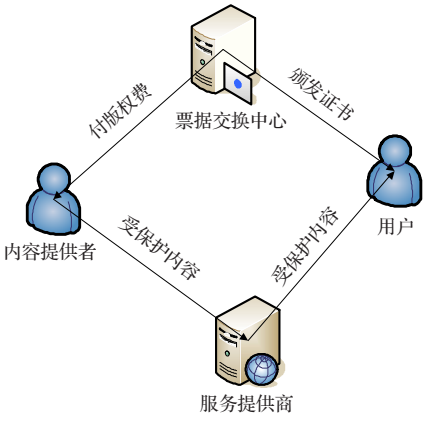

图 1 DRM **系统基本流程**

作者简介:陈绪乾(1978-),男,教师,主要研究方向为计算机网络。
收稿日期:2008-05-05 **修回日期:**2008-08-12

CH)获取版权费,并把数字产品的使用规则告知票据交换中心。然后,内容提供者对提供的内容进行编码,生成 DRM 系统支持格式的内容,并把它传给服务提供商(Service Provider,SP),当用户(User,U)需要使用该受保护内容时,他要到票据交换中心去请求证书,票据交换中心验证了用户的身份后,颁发给用户一个证书,用户利用该证书到服务提供商处提出使用某数字产品的申请,服务提供商验证了 CH 的签名证书后,根据用户对产品的使用要求对用户收费,并把受保护内容传给用户,同时颁发给用户使用该产品的证书。用户利用证书里提供的密钥对该数字产品解密并使用产品。

1.2 P2P 网络介绍

自 1999 年以来,由 Napster 点燃的 P2P 计算模式正在逐渐成为研究和应用的热点。P2P 计算模式的兴起得益于 Internet 的广泛普及、网络带宽的大幅增加以及基于 Internet 端系统计算能力的迅速增强。上述因素促使原先在其他计算模式中被忽视的端系统成为一种宝贵的计算资源。到目前为止,P2P 研究已经涉及非常广泛的方面,主要包括:分布式数据存储、大规模并行计算、即时通讯等。P2P 分布式存储系统的目的就是通过互联网将端系统闲散的网络资源整合起来,实现大规模的文件共享和存储。现有的 P2P 分布式存储系统中比较著名的系统有 Napster、Gnutella、JXTA、Freenet、Chord、CAN、Pastry、Tapestry等。

1.3 k 次匿名可验证证书机制介绍

Teranisi[8]等首次提出了一种具有 k 次匿名可验证的证书方案 k-TAA(k-Times Anonymous Authentication),下面简单介绍该方案的工作原理。

在这个方案里主要包含以下参与者:群组管理员(GM),服务提供者(AP)和用户(U)。该验证机制的实现过程如下:首先,U 如果需要申请 k 次匿名可验证证书,必须向 GM 提出注册请求;GM 验证了 U 的身份后,颁发给 U 一个身份证书,U 在取得该身份证书后也即加入了群组。U 把身份证书提交给 AP,申请获取 AP 提供的服务。AP 在验证了 U 的证书是合法的之后,颁发给 U 一个可多次使用其产品的证书,也即 k 次匿名可验证证书。该证书具有以下特点:用户可使用该证书至多 k 次,在少于 k 次使用该证书的时候,用户的身份都不能被 GM 和 AP 识别,而当用户使用该证书超过 k 次时,用户的真实身份将被揭露出来。

然而,该方案把几乎所有的权限都交给 GM 进行管理,这对于服务提供者明显是不方便和不合理的,Lan Nguyen 和 Rei Safavi-Naini[9]在此基础上对该方案进行改进,提出了一种动态的 k 次匿名可验证证书机制(dynamic k-times anonymous authentication),该方案在原方案基础上增加了 AP 的权限,使其既可以颁发使用证书给用户,也可以撤消用户的使用权限,该机制在理论上进一步改进了原机制。

该文借鉴了该机制的特点,把其运用到数字版权管理系统的设计理念中,希望解决传统 DRM 系统的服务器拥挤、效率低下的问题。

1.4 双线性对理论介绍

双线性对是近几年发展起来的构造密码体制的一个重要工具,目前只能通过对(超)椭圆曲线中的 Weil 对或 Teil 对进行变形而得到。是否存在其他类型的双线性对是密码学的一个公开问题。下面介绍双线性对的一些基本知识:

令 G_1 和 G_T 分别是阶为素数 p 的加群和乘群,P 为 G_1 的生成元,假设在 G_1 和 G_T 这两个群中求解离散对数都是困难问题。令 $e:G_1\times G_1\rightarrow G_T$ 为满足下列三条性质的双线性对:

(1)双线性性:$e(aP,bQ)=e(P,Q)^{ab}$,对所有的 $P,Q\in G_1$ 和所有的 $a,b\in Z_p^*$。

(2)非退化性:若 $e(P,Q)=1$,$\forall Q\in G_1$,则 $P=\Theta$。

(3)可计算性:存在有效算法可以计算 $e(P,Q)$,对所有 $P,Q\in G_1$。

把满足上述三条性质的双线性映射叫做可容忍的双线性映射,在这样的群 G_1 上,有以下几个密码学问题:

(1)离散对数(DL)问题:给定 $P,Q\in G_1$ 找出整数 n,使得 $Q=nP$,如果这样的 n 存在。

(2)强 Diffie-Hellman 问题(SDH 问题)[10-11]:对给定的(k+1)元组$(P,aP,a^2P,\cdots,a^kP)$,其中 $a\in Z_n^*$ 是未知整数,计算二元组$(b,\frac{1}{a+b}P)$。

(3)判定 Diffie-Hellman(DDH)问题:给定四元组$(P,aP,bP,abP)\in G_1^4$,$\forall a,b,c\in Z_p^*$,判断 $c\equiv ab(\mathrm{mod}\ q)$是否成立。

2 基于 P2P 模式的 DRM 系统的模型描述

基于 P2P 模式的 DRM 系统的设计要求有如下几点,分别进行简单的讨论。

(1)为了达到降低系统服务器压力的要求,数字内容和数字证书最好不要都由服务器进行分发。DRM 系统的服务器分为内容服务器和证书服务器,无论是内容服务器和证书服务器,只要接受了过多用户的签名和传输请求,必然导致系统瓶颈的出现。这也是传统的 C/S 模式带来的弊病。因此,当设计系统时,可以借鉴 P2P 技术来解决这个问题。只要尽量把证书分发和内容分发的任务交给用户去处理,就可以把服务器的压力有效地降低,同时增加用户的传输速度。

(2)当把证书分发和数字内容传输的任务分发给用户后,必须注意版权的跟踪保护,保证非法用户无法使用数字产品。这是 DRM 系统的基本要求,一般而言,把证书分发的职责交给用户是很不安全的行为,因为用户属于非可信方,并不能保证用户不会滥用证书分发的权利,这就要求在系统设计时要充分考虑到整个系统对用户的控制是否牢靠的问题。

(3)合法使用数字产品的用户能被匿名保护。一般的 DRM 系统在设计时没有考虑到用户隐私的保护这一点。通常在颁发证书的时候,没有把用户的身份隐藏起来,使得用户的身份可以被轻易地泄露。而一个用户在合法使用数字产品时,他的身份应该是隐匿的,不应该被公诸于众。

(4)非法使用数字产品的用户应该能被追踪。用户的身份在一般情况下是隐匿的,然而,一旦用户非法使用了数字产品,那么他的身份应该能被系统还原出来,这是出于系统安全性考虑的需要。

(5)系统的安全性必须是能被证明的。系统的安全性应该能在数学上被证明是安全的。

根据以上的系统设计要求,在借鉴了动态 k 次可验证证书原理的基础上,设计了以下的系统模型,下面给出该模型的详细描述:

如图 2 所示,该系统有 4 个参与者:内容服务器,证书服务器,认证服务器和用户。要完成整个系统的一个周期的流程,需

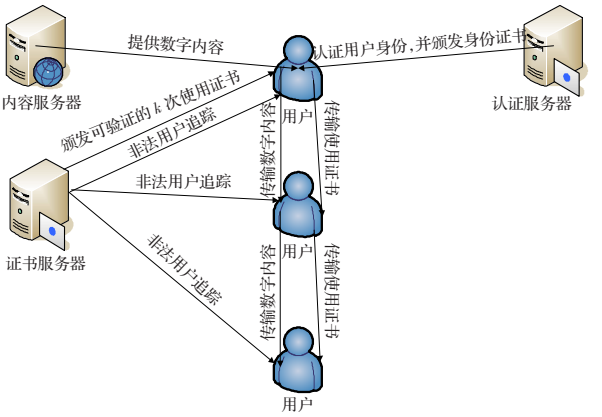

图 2　基于 P2P 模式的 DRM 系统模型图

要执行以下步骤:

(1)用户注册过程

用户(User,U)要使用数字产品,必须先到认证服务器(Authentic Server,AS)进行注册。认证服务器认证了用户的真实身份后,就颁发给用户一个数字证书。

(2)使用证书次数上限声明

CS 在获取了一个新的数字产品后,先对它进行加密,然后公布其产品 ID:D_{ID}, 及一次最多可获取该产品的使用上限 k,并产生该产品的 k 次使用证书。

(3)用户获取使用证书过程

该过程可分为两种情况。

①用户直接向证书服务器(Certificate Server,CS)申请使用证书。用户可向证书服务器直接申请某个数字产品的 k 次使用证书。此时,证书服务器验证用户的身份证书是否合法,如果合法,即向用户颁发 k 次匿名可验证的使用证书,该证书的颁发过程是匿名的,也即是用户在获得该使用证书后,CS 并不知道颁发的证书是颁发给哪个用户。

②用户向某个拥有多次使用证书的用户申请使用证书。那么,拥有多次使用证书的用户可代理证书服务器的功能,验证向他申请使用证书的用户的身份合法性,如合法,便把使用证书发送给该用户。这种从别的用户机器上下载数字证书,以减轻服务器负荷的方法和 P2P 的设计理念是一致的。

另外,在证书服务器颁发使用证书时,会在使用证书里嵌入用户的身份证书,以便对非法用户进行追踪,该身份信息来源于用户的身份证书。

(4)撤消用户使用权限过程

如果用户申请使用的数字产品使用期限已满,或者用户非法使用了数字产品,CS 可以通过该过程撤消用户的使用权限。

(5)用户下载数字产品过程

在获取了使用证书后,用户可以到内容服务器(Content Provider,CP)下载数字产品,或者从其他已经在内容服务器下载了数字产品的用户机器上进行数字产品的下载,这和 P2P 的思想是一致的。当用户要使用数字产品时,用户机器上的客户端程序在和证书服务器的交互中验证用户使用证书的合法性,如果合法,则允许用户进行数字产品的使用。

(6)验证过程

当用户需要使用数字产品时,装在他机器上的 DRM 系统的客户端就在 CS 的协作下验证用户的使用证书是否合法,如果合法,便允许用户使用数字产品,如果用户意图超过使用次数地使用数字产品,则进入用户追踪过程。

(7)非法用户追踪过程

当用户不按服务器要求的次数使用数字产品时,也即用户使用数字产品超过服务器定义的 k 次时,CS 可以很容易地计算出用户的真实身份以对用户实行追踪。

(8)使用证书刷新过程

用户要验证他的使用证书的确为 CS 颁发的,必须在每次验证前及时到 ARC 刷新其使用证书。

3　系统的详细构造过程

3.1　系统初始设置

(1)AS 初始设置

产生安全的双线性对元组(p,G_1,G_T,e,P),其中 $e:G_1\times G_1\rightarrow G_T$是 1.4 节中定义的双线性映射,$p$ 是群 G_1、G_T的阶,P 是群 G_1的一个生成元。AS 选择 P_0,$H\leftarrow G_1$,$\gamma\leftarrow Z_p^*$,令 $P_{pub}=\gamma P$,$\Delta=e(P,P)$。AP 的私钥为 $ask=\gamma$,AP 的公钥为 $gpk=(P,P_{pub},P_0,H,\Delta)$。AP 再初始化一张用户的身份表 LIST, 该表在初始的时候为空,这张表的功能是将来可以用来识别出非法用户的真实身份。

(2)CS 初始设置

CS 选择 $Q\leftarrow G_1$,$s\leftarrow Z_p^*$,Υ,$\Lambda\leftarrow G_T$,令 $Q_{pub}=sQ$,CS 的私钥为 $csk=s$, 其公钥为 $cpk=(Q,Q_{pub},\Lambda,\Upsilon,H)$,CS 维护一张验证表 LOG,该验证表是追踪非法用户时需要用的,并初始化一个累计值 $V_0\leftarrow G_1$,该值当 CS 允许或撤消某用户使用其数字产品的权利时被更新;CS 还维护一张公共存档的表 ARC,该表里的每一项都是一个四元组,该四元组的第一个值为申请了 CS 的数字产品使用证书或被撤消使用证书的某用户的公钥的一部分,第二个值为该用户是被允许(1)还是被撤消(0)使用数字产品的权利,第三个值即为累计值 V。

3.2　用户注册过程

某用户要想使用数字产品,必须先向 AS 注册,该注册过程如下:

(1)用户 U_i选择 x',$r\leftarrow Z_p^*$,并发送一个承诺 $C'=x'P+rH$ 给 AS。

(2)AS 发送 y,$y'\leftarrow Z_p^*$给 U_i。

(3)U_i 计算 $x=y+x'y'$,$r'=y'r$ 和$(C,\beta)=(xP,\Delta^x)$,并把(i,β)加到 LIST 里去。然后 U_i把(C,β)和一个知识证明 $Proof_1=PK\{(x,r'):C=xP\wedge yP+y'C'-C=r'H\}$发送给 AS。

(4)AS 验证(i,β)的确被加到 LIST 里,并验证是否有 $\beta=e(C,P)$以及知识证明 $Proof_1$是否正确,如果上述验证通过,AS 产生 $a\leftarrow Z_p^*$,计算 $S=\frac{1}{\gamma+a}(C+P_0)$,然后把$(S,a)$发送给 U_i。

(5)U_i验证 $e(S,aP+P_{pub})\stackrel{?}{=}e(C+P_0,P)$,如果成立,那么 U_i的私钥为 $usk=x$,其公钥为 $upk=(a,S,C,\beta)$。

这里,用户私钥的选取必须通过用户和 AS 的协作后才能产生,AS 虽然参与了私钥的产生过程,然而并不知道用户私钥的实际值。这样处理的好处是可以使用户的私钥具有充分的随机性,降低非法用户破解系统的风险。

3.3　用户获取使用证书过程

U_i如果想使用某个数字产品,他可以向 CS 或者其他已获得某个数字产品多次使用权的用户申请使用证书。在申请到 k 次的使用证书后,他还需要初始化一个 v 值,该值表示他已经

使用了该证书的次数。该值初始为0,每当用户使用了一次使用证书,该值就被累加1。

(1)如果用户向CS申请使用证书,那么他必须向CS发送他的公钥(a,S,C,β)以及他需要使用的数字产品的ID和需要使用的次数(D_{ID},k),CS验证了用户公钥的合法性后,将用以下方法颁发某个数字产品的k次使用证书。

假设CS的ARC已经有j个元组并假设第j个元组的累计值为V_j。CS计算一个新的累计值$V_{j+1}=(s+a)V_j$,并把$(a,1,V_{j+1})$加到ARC里去。然后,CS计算k个证书$(\theta_j,\theta_j')=H_{G_T\times G_T}(D_{ID},k,j)$ $(j=1,\cdots,k)$并把其传给用户。用户可以计算自己的使用证书$mak=(j+1,W)$,其中$W=V_j$。

(2)用户U_i向已获得多次使用权的用户U_j申请使用证书的步骤比较简明,他可以以任意方式向U_j出示自己的身份证明,U_j根据U_i要求的使用次数n把n个未使用过的证书传给U_i,并把v值加上n,同时记录下U_i的身份及获取的使用证书的编号,以便将来如果U_i滥用使用证书时可以进行追踪即可。

3.4 撤消用户使用权限过程

假设CS由于某种原因需要撤消用户U_i的使用证书,U_i的公钥为(a,S,C,β),又假设CS的ARC已经有j个元组且第j个元组的累计值为V_j,CS计算$V_{j+1}=1/(s+a)V_j$,并把元组$(a,0,V_{j+1})$加到ARC中即可。

3.5 用户验证过程

假设用户U_i的私钥为x,他想利用申请到的证书使用数字产品。那么可以通过以下步骤进行:

(1)用户机器上的客户端先把v值加1,并检查是否有$v>k$,如是,发送$\perp$给CS并停止该验证过程。如否,用户运行3.7节的使用证书刷新程序来刷新其使用证书,并发送该数字产品的ID。

(2)CS产生随机数$l\leftarrow Z_p^*$并把其发送给U_i。

(3)U_i用他收到的第v个使用证书(θ_v,θ'_v)计算标签$(\Gamma,\Gamma')=(\theta_v^x,(\Delta^l\theta'_v)^x)$,并把$(\Gamma,\Gamma',v)$以及一个知识证明$Proof_2$传给CS,该知识证明的详细验证方法请参考文献[9]。

$$Proof_2=PK\{(v,a,S,x):\Gamma=\theta_v^x\wedge\Gamma'=(\Delta^v\theta'_v)^x\wedge e(S,aP+P_{pub})=e(xP+P_0,P)\wedge e(W,aQ+Q_{pub})=e(V,Q)\}$$

(4)如果上面的知识证明是合法的并且Γ和CS维护的LOG表里的所有第v个使用证书的Γ都不相同,就把(Γ,Γ',v)加入到LOG表中,并允许用户使用数字产品,否则,拒绝用户使用并终止该过程。

3.6 非法用户追踪过程

非法用户如果试图使用数字产品超过允许的次数,假设他请求验证时的参数为(Γ,Γ',v),他的ID将会被恢复出来。具体实现步骤如下:

(1)CS查找LOG里的每一个元组,看是否有一个元组(K,K',v')满足$\Gamma=K$并且$v\neq v'$。

(2)如果找到该元组,CS计算$\beta=(\Gamma'/K')^{1/(v-v')}=\Delta^x$。这样,再查AS维护的LIST表,就可以把用户对应的i值查出来,也就实现了非法用户的身份追踪。

3.7 使用证书刷新过程

假设CS的ARC有n个四元组,用户U_i的公钥为(a,S,C,β),其使用证书为(j,W_j),那么,他用如下方法计算一个新的使用证书:

For$(k=j+1;k++;k<=n)$ do
取ARC的第k个元组(u,b,V_k)
if$(b=1)$ then $W_k=V_{k-1}+(u-a)W_{k-1}$
else $W_k=(1/(u-a))(W_{k-1}-V_k)$
end for;
return(n,W_n)

4 系统的安全性分析

4.1 系统的正确性

系统的正确性是指,合法使用该系统的用户都能正常地使用数字产品。这可以分为三部分证明:

(1)在用户注册过程中,如果用户合法进行注册,那么以下式子成立:$e(S,aP+P_{pub})=e(C+P_0,P)$。

证明 $\because S=\frac{1}{\gamma+a}(C+P_0),P_{pub}=\gamma P$

$$\therefore e(S,aP+P_{pub})=e(\frac{1}{\gamma+a}(C+P_0),(a+\gamma)P)=e(C+P_0,P)$$

(2)在用户合法地申请使用证书后,那么以下式子成立:$e(W,aQ+Q_{pub})=e(V,Q)$。

证明 由3.3、3.4节知道,在用户获得使用证书的时候,CS把其累积值初始化为$V_{j+1}=(s+a)V_j$,以下证明,用户可以在ARC中获取到一个以下的三元组(u,b,V_k),如果$b=1$,那么$V_k=(s+u)V_{k-1}$,如果$b=0$,那么$V_{k-1}=(s+u)V_k$。

根据使用证书刷新过程的定义,当ARC上的三元组(u',b',V_k')中的$b'=1$时用户将令$V_k=V_k+(u'-u)V_{k-1}=(u+s)V_{k-1}+(u'-u)V_{k-1}=(s+u')V_{k-1}$,此时ARC中的最后一个元组必然是表示该用户获得使用证书的元组,因此$u'=u$,从而$V_k=(s+u)V_{k-1}$。

同理可以证明当$b=0$时有$V_{k-1}=(s+u)V_k$。

4.2 合法使用该系统的用户具有匿名性

用户身份信息的保密主要依靠用户私钥x的保密。排除掉用户私钥的人为丢失的因素,要从系统的算法体系中直接获取用户的私钥,就必须从元组$(\Gamma,\Gamma')=(\theta_v^x,(\Delta^l\theta'_v)^x)$中着手。首先从$\Gamma=\theta_v^x$中无法得出用户的私钥$x$,如果可以得出,也即可以破解离散对数问题,这在目前是不可能的;另外,要从$\Gamma'=(\Delta^l\theta'_v)^x$中得到$\Delta^x$的值也是不可能的,根据文[9]中的结论,就必须能破解判定Diffie-Hellman问题,而该问题目前没有多项式时间内解法,因此,用户的匿名性在用户合理使用数字产品时是安全的。

4.3 用户不能模仿AS、CS颁发证书

首先,根据文献[12],用户如果能模仿AS颁发证书,那么,意味着该用户可以破解q重计算Diffie-Hellman问题,而由1.4节知道,q重强Diffie-Hellman问题在目前尚无多项式时间的解法,因此,用户不能模仿AS颁发证书。

另外,CS在给用户颁发证书时嵌入了自己的私钥s,如果用户要模仿其签名,必须知道CS的私钥,而这就需要破解离散对数问题,这同样是不可能的。

因此,用户无法模仿AS、CS颁发证书。

4.4 数字产品不能非法使用

用户无法模仿 AS、CS 颁发证书,而如果要使用数字产品,必须有证书的支持,因此数字产品不能被用户非法使用。

另外,用户即使申请到合法证书,如果超过申请数目地使用数字产品,必将被恢复真实身份而被追究责任,因此,数字产品不会被非法使用。

5 结论

在参考了 k 次匿名可验证机制模型的前提下,将其思想运用到数字版权管理系统的设计理念中,设计了一个具有 P2P 特性的数字版权管理系统。该系统的证书和数字内容都可以在用户间传送,充分发挥了点对点传输的效率,有效解决了系统瓶颈的问题。使得该系统既能以可观的速度传输数字产品,又能对版权实施有力的保护。最后,对系统的安全性给出了证明。

参考文献:

[1] Stoica I,Morris R,Karger D,et al.Chord:A scalable peer to peer lookup service for Internet applications[C]//Proceedings of SIGCOMM 2001,Aug 2001.

[2] Ratnasamy S,Francis P,Handley M,et al.Scalable content addressable network[C]//Proceedings of SIG2COMM 2001,Aug 2001.

[3] Napster.http://www.napster.com.

[4] Gnutella.http://gnutella.wego.com.

[5] FreeNet.http://freenet.sourceforge.net.

[6] Smith M L.Digital rights management and protecting the digital media value chain[C]//Proceedings of the 3rd International Conference of Mobile and Ubiquitous Multimedia.Maryland:ACM Press,2004:187-191.

[7] Morir,Kawaharam.Super distribution:The concept and the architecture[J].Transactions of the IEICE,1990,73(7).

[8] Teranisi I,Furukawa J,Sako K.K-times anonymous authentication[C]//LNCS 3329:ASIACRYPT 2004.[S.l.]:Springer-Verlag,2004:308-322.

[9] Nguyen L,Safavi-Naini R.Dynamic k-times anonymous authentication[C]//LNCS 3531:Applied Cryptography and Network Security Conference (ACNS) 2005.[S.l.]:Springer-Verlag,2005:318-333.

[10] Gupta N,Srivastav V,Bhatia Wyglinski M P S.Middleware-an effort towards making mobile application platform independent[C]//International Conference on IEEE Systems and Networks Communication ICSNC'06,2006:1-6.

[11] Mitsunari S,Sakai R,Kasahara M.A new traitor tracing[J].IEICE Trans,2002,E85-A(2):481-484.

[12] Boneh D,Boyen X.Short signatures without random Oracles[C]//LNCS 3027:EUROCRYPT 2004.[S.l.]:Springer-Verlag,2004:56-73.

(上接 164 页)

[3] Stauffer C,Grimson W.Adaptive background mixture models for real time tracking[C]//Proceedings of IEEE International Conference on Computer Vision and Pattern Recognition,Fort Collins,Colorado,USA,1999:246-252.

[4] Shimada A,Arita D.Dynamic control of adaptive mixture-of-Gaussians background model[C]//Proceedings of the IEEE International Conference on Video and Signal Based Surveillance,2006(8):1079-1085.

[5] Luo X Z,Suchendra M.Nonparametric background modeling using the condensation algorithm[C]//Proceedings of the IEEE International Conference on Video and Signal Based Surveillance(AVSS'06),2006:751-767.

[6] Ben-Akiva M,Harries N.Nonlinear Kalman filtering algorithms for on-line calibration of dynamic traffic assignment models[J].IEEE Transactions on Intelligent Transportation System,2007,8(4):661-670.

[7] Rider C,Munkelt O,Kirchner H.Adaptive background estimation and foreground detection using Kalman-filtering[C]//Proceedings of International Conf on Recent Advances in Mechatronics,ICRAM'95,Istanbul,Turkey,1995:193-199.

(上接 197 页)

物资配送的车辆调度优化问题。该问题是一类较难求解的组合优化问题,而且具有很强的现实应用背景,可产生极其可观的经济效益,因而也是一个很值得深入研究的问题。

主要在以下几个方面进行了探索与研究:

(1)研究实际车辆调度问题的模式化。根据典型的问题约束与目标,将实际应用环境下的车辆调度工作运用数学模型进行描述,归纳为可求解的标准 VSP 问题。

(2)应用数学方法对于多物资储备中心同时供应救灾物资的问题,进行简化处理,依据点到点之间的距离,进行了由多到单的问题简化工作。

(3)研究实用的优化算法。主要研究了免疫算法,它的搜索过程具有非确定性,具有避免陷入局部最优以收敛于全局最优(或次优)的能力。

5.2 进一步的工作

今后的工作将从如下几方面入手:

(1)由于实际情况的不同,车辆调度问题的模型构造与算法选择会有很大区别。研究实际车辆调度问题的模式化时,应根据实际情况和操作经验而不断充实与完善。

(2)各种优化算法均有其利弊,在实际应用中,算法的研究与应用需要进行合理改进,以提高解决问题的效率。该文只涉及到非满载问题,满载问题也应该适当考虑。

参考文献:

[1] 冯旭东,率帅.抓好应急物流配送的几项对策[J].中国物流与采购,2003,23(3):31-34.

[2] 赵林度.城市重大危险源应急物流网络研究[J].东南大学学报:哲学社会科学版,2007,9(1):27-29.

[3] 王旭坪,傅克俊,胡祥培.应急物流系统及其快速反应机制研究[J].中国软科学,2005,6:127-131.

[4] 缪成,吴启迪,许维胜.应急物流的差异分析与体系构建[J].商业时代,2008,8:18-19.

[5] 王磊,潘进,焦李成.免疫算法[J].电子学报,2000,28(7):74-78.

[6] Kim J,Bentley P J.Immune memory and gene library evolution in the dynamical clonal selection algorithm[J].Journal of Genetic Programming and Evolvable Machines,2004,5(4):361-391.

[7] Lim A,Wang Fan.Multi-depots vehicle routing problem:A one-stage approach[J].IEEE Transactions on Automation Science and Engineering,2005,2(4):397-402.

[8] 张斌.应急物流配送车辆调度优化研究[D].大连:大连海事大学,2006.