doi:10.3969/j.issn.1000-436x.2014.02.013

云计算环境中支持隐私保护的数字版权保护方案

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

（1. 北京邮电大学 信息安全中心，北京 100876；2. 北京邮电大学 灾备技术国家工程实验室，北京 100876；
3. 北京国泰信安科技有限公司，北京 100086）

摘 要：针对云计算环境中数字内容安全和用户隐私保护的需求，提出了一种云计算环境中支持隐私保护的数字版权保护方案。设计了云计算环境中数字内容版权全生命周期保护和用户隐私保护的框架，包括系统初始化、内容加密、许可授权和内容解密 4 个主要协议；采用基于属性基加密和加法同态加密算法的内容加密密钥保护和分发机制，保证内容加密密钥的安全性；允许用户匿名向云服务提供商订购内容和申请授权，保护用户的隐私，并且防止云服务提供商、授权服务器和密钥服务器等收集用户使用习惯等敏感信息。与现有的云计算环境中数字版权保护方案相比，该方案在保护内容安全和用户隐私的同时，支持灵活的访问控制，并且支持在线和超级分发应用模式，在云计算环境中具有较好的实用性。

关键词：数字版权管理；隐私保护；属性基加密；同态加密；云计算

中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)02-0095-09

Privacy-preserving digital rights management scheme in cloud computing

HUANG Qin-long[1,2,3], MA Zhao-feng[1,2,3], FU Jing-yi[1,2,3], YANG Yi-xian[1,2], NIU Xin-xin[1,2]

(1. Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China;
3. Beijing National Security Science and Technology Co Ltd, Beijing 100086, China)

Abstract: In order to meet the needs of digital content and user privacy protection in cloud computing environment, a privacy-preserving digital rights management (DRM) scheme in cloud computing was proposed. The framework of digital content copyright lifecycle protection and user privacy protection in cloud computing was firstly designed, which includes four protocols: system setup, content encryption, license acquisition and content decryption, and then a content encryption key protection and distribution mechanism based on attribute-based encryption and additively homomorphic encryption was proposed, which ensures the security of content encryption key. In addition, the proposed scheme also allows the users to purchase content and acquire license anonymously from cloud service provider, which protects the user privacy and prevents cloud service provider, license server and key server in the cloud from collecting the user's sensitive information. Compared with existing DRM schemes in cloud computing, the proposed scheme which not only protects the data security and user privacy, but also supports fine-grained access control, and supports online and super-distribution application modes, is more applicable in the copyright protection for cloud computing.

Key words: digital rights management; privacy preserving; attribute-based encryption; homomorphic encryption; cloud computing

收稿日期：2013-07-01；**修回日期**：2013-09-20

基金项目：国家自然科学基金资助项目(60803157, 90812001, 61272519)

Foundation Item: The National Natural Science Foundation of China (60803157, 90812001, 61272519)

1 引言

随着互联网和云计算技术的快速发展和不断普及，云计算在提高使用效率的同时，为数字内容安全与用户隐私保护带来极大的冲击与挑战[1]。数字版权管理（DRM，digital rights management）通过数字内容的加密和安全许可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[2~5]。

云计算以动态的服务计算为主要技术特征，有着较大的灵活性和成本优势。企业能够将内容存储和运营外包给云服务提供商，而不需自己购买设备和维护系统，还能在存储需求变化时灵活地增减云资源的租用。同时，用户也能够方便地通过不同终端接入云服务，使用海量的数字内容。然而，如何保护云环境下数字内容的安全性和合理使用，同时防止云服务提供商挖掘或者泄露用户隐私信息是云计算环境中数字版权保护无法回避的核心问题。

针对云计算环境中数字版权保护的需求，本文提出一种云计算环境中支持隐私保护的数字版权保护方案，实现数字内容版权全生命周期的保护和用户隐私的保护。本文的贡献主要有3个方面。

1) 提出云计算环境中数字内容版权全生命周期保护和用户隐私保护的框架，包括系统初始化、内容加密、许可授权和内容解密4个主要协议，支持云计算环境中细粒度的用户授权和灵活的应用模式。

2) 采用基于属性基加密和加法同态加密算法的内容加密密钥保护和分发机制，保证内容加密密钥的安全性。内容加密密钥由主密钥、授权密钥和辅助密钥三部分组成，其中主密钥使用内容提供商设置的访问策略加密，授权密钥和辅助密钥分别由授权服务器和密钥服务器加密分发给用户，用户只有在其属性满足密文的访问策略并且拥有有效许可证的情况下才能基于加法同态加密算法解密出内容加密密钥。

3) 允许用户匿名向云服务提供商订购内容和申请授权，有效保护用户的隐私，同时防止云服务提供商、授权服务器和密钥服务器等收集用户使用习惯等敏感信息。

2 相关工作

云计算技术带来的大规模在线存储和按需使用的模式，使越来越多的用户选择云计算作为内容的存储平台。然而，数字内容的全生命周期保护包括内容的安全性、内容的合理使用等，是云计算发展和应用中面临的关键问题。在云计算快速发展的推动下，国内外学者在云环境下版权保护方面的研究也在不断深入，并取得不少研究成果，主要集中在内容安全、访问控制和隐私保护等方面[6~15]。

1) 数字内容安全。内容加密是保护云环境中内容安全的基本手段，JAFARI等人在2011年的ACM DRM 会议上提出支持云存储环境的数据版权保护方案[6]，通过加密用户上传的数字内容，并限制访问者对内容的使用权利，保护内容的安全性。该方案不依赖于可信的云服务提供商，但是不支持细粒度的用户授权。另外，在JAFARI等人的方案中，数据拥有者在为用户授权时，使用用户的公钥加密内容加密密钥，导致用户解密的计算复杂度较高。针对内容加密密钥的保护，WANG等人提出云计算中基于SIM卡的移动版权保护方案CS-DRM[7]，使用对称加密技术加密内容加密密钥。但是，该方案需要通过SIM卡提前协商对称密钥，实用性不高，同时会泄露用户使用内容的习惯。

PETRLIC 也提出云计算环境中支持细粒度授权的版权保护方案[8]，允许内容提供商将加密的内容上传到云服务提供商，并设置使用权限。用户在使用内容时，云服务提供商利用代理重加密技术将内容重加密为用户公钥加密的内容，确保只有该用户才能解密，并且在重加密过程中，云服务提供商也无法知道内容的明文。该方案虽然可以保证内容在云环境中的安全性，但是用户每次使用内容时都需要重加密内容，当用户数量达到一定规模时会带来很大的额外开销。

另外，同态加密也广泛应用于数字内容的安全保护，SAMANTHULA 等人提出了云计算环境中基于代理重加密和同态加密技术的内容安全共享方案[9]。CORENA等人也提出了基于云计算的财务数据安全整合和存储的方案[10]，该方案基于加法同态加密和秘密共享技术实现数据在密文状态下的运算。

2) 内容访问控制。密文的访问控制是云计算环境下加密内容安全使用的关键问题，WU 等人提出了一种云计算环境下基于属性基加密的内容保护方案[11]，以实现灵活的访问控制。洪澄等人在属性基加密的基础上提出一种内容保护和访问控制方案[12]，设计出一种基于秘密共享方案的云端重加密方法，在不损失安全性的前提下将一部分重加密代价转移到

云端，降低权限管理的复杂度，实现密文访问控制。MULLER 等人首次提出基于属性基加密的数字版权保护方案[13]，通过静态规则和动态规则实现版权内容的合理使用。其中，静态规则是通过设置密文的访问策略，实现用户的访问控制，动态规则是将用户允许使用的权限通过许可证分发给用户，实现内容的使用控制。

3) 用户隐私保护。针对云计算环境下用户使用内容时隐私保护的问题，CONRADO 等人最早提出支持隐私保护的版权保护方案[14]，允许用户匿名购买内容和申请授权。但是，该方案基于智能卡实现，缺乏实用性。PERLMAN 等人提出基于匿名现金和盲签名技术的用户隐私保护方案[15]，允许用户匿名使用内容，同时防止云服务提供商跟踪用户的使用行为，但是不支持细粒度的用户授权。在 PERLMAN 等人方案的基础上，PETRLIC 等人提出一种云计算环境中支持灵活用户授权的内容版权保护方案[16]，该方案基于同态加密和秘密共享技术实现云服务器上加密内容的授权管理，结合重加密机制防止云服务器收集用户的敏感数据。然而，该方案同样在用户每次使用内容时都需重加密内容，效率较低。

本文在上述工作成果的基础上，提出适用于云计算环境的数字内容版权全生命周期保护方案，允许内容提供商上传加密内容到云存储环境，采用属性基加密和加法同态加密算法分发内容加密密钥，不仅保护内容的安全性，支持灵活的访问控制，而且允许用户匿名获取内容和授权，同时防止云服务提供商获得用户使用内容的记录。

3　预备知识

3.1　CP-ABE

属性基加密（ABE）最初由 SAHAI 和 WATERS 提出[17]，它以属性为公钥，将密文和用户私钥与属性关联，能够灵活地表示访问策略，当用户的私钥与密文的访问策略相互匹配时，该用户才能解密密文。ABE 包括密钥策略（KP-ABE）以及密文策略（CP- ABE）2 类。其中，CP-ABE 的密文与访问策略关联，更加适合于云计算环境下的访问控制。

CP-ABE 算法包括以下 4 个组成部分。

1) *ABE.Setup*()。生成系统公钥 *PK* 和系统主密钥 *MK*。

2) *ASK* = *ABE.KeyGen*(*AS*, *MK*)。使用用户属性 *AS* 和 *MK* 生成用户的属性私钥 *ASK*。

3) *CT* = *ABE.Encrypt*(*AP*, *M*, *PK*)。使用访问策略 *AP* 和 *PK* 将数据明文 *M* 加密为密文 *CT*。

4) *M* = *ABE.Decrypt*(*ASK*, *CT*)。如果用户的属性 *AS* 满足访问策略 *AP*，使用属性私钥 *ASK* 解密密文 *CT* 得到明文 *M*。

3.2　加法同态加密

同态加密技术允许用户对加密数据进行直接运算或处理，是实现云计算安全中密文处理和隐私保护的重要基础。同态加密[18]是在 1978 年由 RIVEST 等人提出的，是基于数学难题的计算复杂性理论的密码学技术。2009 年，GENTRY 提出了基于多项式环上理想格的全同态加密算法[19]。2010 年，DIJK 等人提出针对整数加密的全同态加密算法[20]。

基于同态加密算法，可以对加密数据进行运算或处理，而不再需要先进行解密。CASTELLUCCIA 等人提出一种加法同态加密算法[21]，满足如表 1 所示的属性，包括加密算法、解密算法和密文加法，该方案是可证明安全的。

表 1　　**加法同态加密算法**

加密算法	解密算法	密文加法
$c = Enc(m, k, M)=m+k \pmod M$，其中，$M$ 是一个大整数，$m \in [0,M-1], k \in [0,M-1]$。	$Dec(c, k, M)=c-k \pmod M$。	如果 $c1 = Enc(m1, k1, M)$，$c2 = Enc(m2, k2, M)$，其中，$m1+m2 \in [0, M-1]$，则有 $Dec(c1 + c2, k1 + k2, M) = m1+m2$。

4　云计算环境中版权保护需求

1) 灵活性

云计算由于可扩展性和灵活性等特性，能够满足用户对数字内容不断增长的需求，并且支持按需使用的业务模式。因此，云计算环境中的版权保护方案在保证数字内容安全性的前提下应满足灵活的业务需求和细粒度的用户授权，并且支持内容提供商设置灵活的访问控制。同时，云计算为用户提供使用便利，用户可以随时随地使用不同终端访问云服务提供商，购买和租用数字内容。因此，云计算环境中的版权保护方案应支持灵活的应用模式。

2) 安全性

云计算允许内容提供商将内容发布到云存储平台，并快速分发给用户，因此版权保护方案应保证内容的安全性，防止由于云服务系统内部人员失职、外部黑客攻击等引起的数字内容泄露，保护内容提供商的合法权利。同时，为了保证数字内容的合理使用，版权保护方案应确保数字内容只能被授

权用户访问，防止假冒攻击和重放攻击等非授权访问，并且支持许可证的撤销。

3) 隐私保护

用户通过云服务提供商订购内容时，版权保护方案应防止内容提供商和云服务提供商等获取用户身份信息，保证用户的匿名性。另外，云服务提供商在为用户提供内容服务的同时，往往通过网页等技术收集并分析用户的使用记录，为用户精准地推荐相关内容。因此，版权保护方案应防止云服务提供商收集用户的使用记录等敏感信息，保护用户的隐私。

5 方案设计思想

基于 CP-ABE 和加法同态加密算法，本文提出一种半可信云计算环境中支持隐私保护的数字版权全生命周期保护方案，保护版权内容在上传、存储、传输和使用等环节的安全性和合理使用。如图 1 所示，数字版权保护方案涵盖属性机构、内容提供商、密钥服务器、授权服务器、云服务提供商和用户等组成部分。

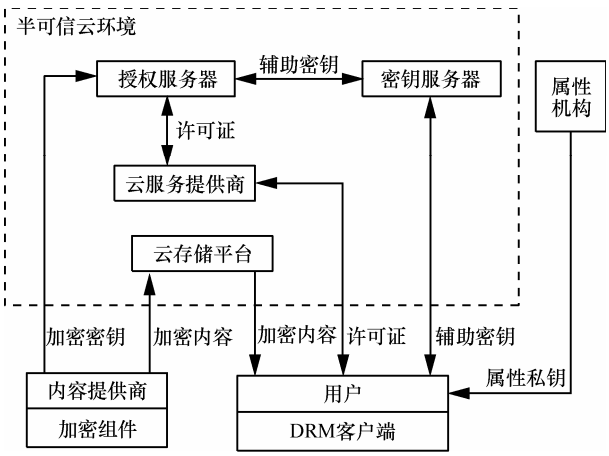

图 1 数字版权保护方案框架

1) 属性机构：属性机构是可信的服务器，为用户分配属性，并生成用户的属性私钥通过安全信道分发给用户。

2) 内容提供商：内容提供商通过加密组件使用随机的主密钥、授权密钥、辅助密钥相加得到内容加密密钥，使用内容加密密钥加密准备上传的数字内容，并将加密后的数字内容发布到云存储平台。同时，内容提供商通过访问策略加密主密钥以实现用户的访问控制。

3) 密钥服务器：密钥服务器接收内容提供商加密的辅助密钥，在申请内容解密时为已授权用户提供辅助密钥。另外，在授权服务器撤销许可证后，密钥服务器拒绝已撤销许可证的内容解密请求。

4) 授权服务器：授权服务器根据云服务提供商的内容订购请求，为用户生成许可证，并通过云服务提供商分发给用户。许可证中包含加密的授权密钥以及时间限制、次数限制等细粒度授权，并使用授权服务器的私钥签名。

5) 云服务提供商：云服务提供商向用户提供内容服务，用户通过云服务提供商购买内容提供商的内容并获取许可证，在此过程中云服务提供商不能获取明文内容、用户隐私和敏感信息。

6) 用户：用户获取加密的内容后，通过云服务提供商向授权服务器申请许可证，在使用内容时向密钥服务器申请辅助密钥。用户设备上的可信 DRM 客户端首先利用属性私钥解密出主密钥，然后基于加法同态加密算法解密出授权密钥与辅助密钥的和，再与主密钥相加得到内容加密密钥并解密明文内容。DRM 客户端在执行内容使用权利约束的同时，保护内容加密密钥和明文内容不被窃取或者转存。

下面介绍数字版权全生命周期保护中系统初始化、内容加密、许可授权和内容解密 4 个主要的协议。文中用到的符号定义如表 2 所示。

表 2 相关符号定义

符号	含义
SP, *U*	云服务提供商，用户
S, *K*	授权服务器，密钥服务器
PK, *MK*	系统公钥/主密钥
AS	用户属性
AP	访问策略
ASK	属性私钥
CID	内容标识
PCD, *ECD*	明文内容，加密内容
CMK, *LK*, *AK*	主密钥，授权密钥，辅助密钥
CEK	内容加密密钥
UK	用户的随机密钥
HK	同态密钥
LIC	用户许可证
T	时间戳
Enc(), *Dec*()	加密/解密运算
Sig()	私钥签名运算

5.1　系统初始化协议

系统初始化时，属性机构定义系统属性为 $A=\{a_1,a_2,a_3,\cdots,a_n\}$，公开发布系统公钥 PK，并秘密保存系统主密钥 MK。

用户注册时，根据用户的属性 AS 为用户生成属性私钥 ASK，并通过安全信道发送给用户秘密保存。

$$ASK = ABE.KeyGen(AS, MK)$$

5.2　内容加密协议

在内容加密阶段，内容提供商的加密组件生成随机的 CEK，再使用 CEK 基于对称加密算法加密内容提供商上传的内容。

Step1　内容提供商的加密组件随机生成长度为 l 的 CMK、LK 和 AK，并相加得到 CEK。

$CEK = CMK + LK + AK \in [0, M-1]$，其中 $M \geqslant 2^{l+1}$

Step2　加密组件使用 CEK 加密 PCD，并把加密结果 ECD 发布到云存储平台。

$$ECD = Enc(CEK, PCD)$$

Step3　内容提供商设置该内容的访问策略 AP，加密组件基于 CP-ABE 算法使用 AP 加密 CMK，使用授权服务器的公钥 PK_S 加密 LK，并将结果一并发送给授权服务器，同时使用密钥服务器的公钥 PK_K 加密 AK 发送给密钥服务器。

$$CP \rightarrow S: ABE.Enc(AP, CMK, PK) \,||\, Enc(PK_S, LK)$$

$$CP \rightarrow K: Enc(PK_K, AK)$$

5.3　许可授权协议

用户通过云服务提供商订购内容后，云服务提供商向授权服务器申请 LIC，授权服务器根据用户的订购权限生成 LIC，并通过云服务提供商分发给用户。许可授权协议时序如图 2 所示。

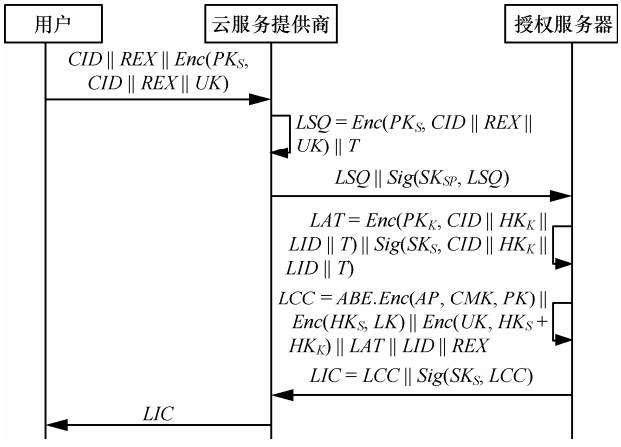

图 2　许可授权协议时序

Step1　用户随机生成密钥 UK，向云服务提供商提交内容订购请求，包括 CID、用户使用权限 REX 和许可授权请求 LAQ。其中，LAQ 包括 CID、REX 和 UK，并使用 PK_S 加密。

$$LAQ = Enc(PK_S, CID \,||\, REX \,||\, UK)$$

$$U \rightarrow SP: CID \,||\, REX \,||\, LAQ$$

Step2　云服务提供商处理用户的内容订购请求后，向授权服务器提交许可生成请求 LSQ 和签名。其中，LSQ 包括 LAQ 和 T 等。

$$LSQ = LAQ \,||\, T$$

$$SP \rightarrow S: LSQ \,||\, Sig(SK_{SP}, LSQ)$$

Step3　授权服务器收到许可生成请求 LSQ 和签名后，验证 LSQ 的签名是否正确，并验证 T 是否有效。验证通过后，授权服务器首先使用 SK_S 解密出 CID、REX 和 UK。其次，授权服务器根据 CID 随机生成长度为 l 的 HK_S 和 HK_K（满足 $HK_S + HK_K \in [0, M-1]$，其中每个内容的 HK_K 均相同）。根据许可证权利描述为用户生成 LIC 并返回给云服务提供商。LIC 中包括 AP 加密的 CMK、HK_S 加密的 LK、许可授权凭证 LAT 和许可证标识 LID 等，并使用 SK_S 签名。

$$LAT = Enc(PK_K, CID \,||\, HK_K \,||\, LID \,||\, T) \,||\, Sig(SK_S, CID \,||\, HK_K \,||\, LID \,||\, T)$$

$$LCC = ABE.Enc(AP, CMK, PK) \,||\, Enc(HK_S, LK) \,||\, Enc(UK, HK_S + HK_K) \,||\, LAT \,||\, LID \,||\, REX$$

$$S \rightarrow SP: LIC = LCC \,||\, Sig(SK_S, LCC)$$

Step4　云服务提供商将 LIC 发送给用户，用户使用 PK_S 验证 LIC 的完整性，并保存 LIC。

5.4　内容解密协议

用户使用内容时，将已申请的 LIC 中的 LAT 发送给密钥服务器请求 AK。用户获取 AK 后，基于加法同态加密算法解密出 LK 与 AK 的和。内容解密协议时序如图 3 所示。

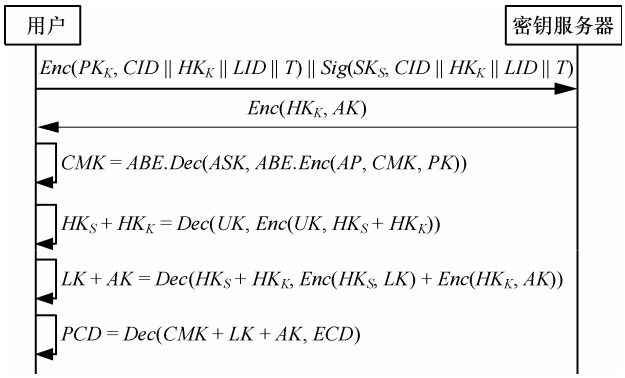

图 3　内容解密协议时序

Step1 用户使用内容时首先判断 *LIC* 是否存在，若 *LIC* 存在并且有效时，用户从 *LIC* 提取出 *LAT* 发给密钥服务器申请 *AK*。

$U \rightarrow K$: $Enc(PK_K, CID \| HK_K \| LID \| T) \| Sig(SK_S, CID \| HK_K \| LID \| T)$

Step2 密钥服务器收到 *LAT* 后，使用 PK_S 验证 *LAT* 的完整性，并使用 SK_K 解密出 *CID* 和 HK_K。然后，密钥服务器使用 SK_K 解密出该内容的 *AK*，并使用 HK_K 加密 *AK* 后，将 $Enc(HK_K, AK)$返回给用户。

$$K \rightarrow U: Enc(HK_K, AK)$$

Step3 用户使用 *ASK* 从 *LIC* 中解密出 *CMK*。

$$CMK = ABE.Dec(ASK, ABE.Enc(AP, CMK, PK))$$

Step4 用户使用 *UK* 从 *LIC* 中解密出 $HK_S + HK_K$。

$$HK_S + HK_K = Dec(UK, Enc(UK, HK_S + HK_K))$$

Step5 基于加法同态加密算法，用户使用(HK_S+HK_K)解密出$(LK + AK)$。

$$LK + AK = Dec(HK_S + HK_K, Enc(HK_S, LK) + Enc(HK_K, AK))$$

Step6 用户使用 *CEK* 解密 *ECD*，并按照 *LIC* 中的 *REX* 执行权利约束。

$$PCD = Dec(CMK + LK + AK, ECD)$$

6 方案应用模式

1) 云在线应用模式

云计算将大量计算资源、存储资源与内容资源通过网络连接在一起，推动了在线应用和在线内容服务的快速发展。本文方案支持云环境下数字内容在线使用场景下灵活的版权控制，例如在线播放多媒体内容、在线阅读电子书等。用户通过安装在终端的 DRM 客户端向授权服务器在线申请许可证，获取许可证后实时解密在线传输的加密内容流，并按照许可证中规定的权利进行使用控制。通过方案中的隐私保护方法，用户不仅可以享受云计算带来的在线数字内容服务，而且无需担心隐私和敏感记录的泄露。

2) 云超级分发应用模式

云计算通过 CDN 等技术消除网络运营商之间的互通瓶颈，将数字内容分发到离用户最近的网络节点，为用户提供更快的内容超级分发服务。本文方案支持许可证与内容独立分发的模式，加密的数字内容可以在用户之间或者用户的不同终端设备之间进行超级分发。用户使用加密内容时，需要通过云服务提供商向授权服务器申请许可证。本文方案不仅满足云环境中数字内容分发和共享的需求，而且保护用户使用内容过程中的隐私。

7 方案分析

7.1 正确性分析

已知 $HK_S + HK_K \in [0, M-1]$，$LK + AK \in [0, M-1]$，M 是一个大整数。

基于 CASTELLUCCIA 等人提出的加法同态加密算法[21]可以得出

$$Enc(HK_S, LK) + Enc(HK_K, AK) = Enc(HK_S + HK_K, LK + AK)$$

则由上述等式，可得

$$(LK + AK) = Dec(HK_S + HK_K, Enc(HK_S, LK) + Enc(HK_K, AK))$$

由 $CEK = CMK + LK + AK$，用户可以正确解密内容。

7.2 安全性分析

定理 1 用户只有满足访问策略并获取有效的许可证后才能解密内容。

加密服务器使用 *CEK* 加密数字内容，用户只有获取 *CEK* 才能解密内容。用户通过云服务提供商向授权服务器申请 *LIC*，*LIC* 中包含 *AP* 加密的 *CMK*、HK_S 加密的 *LK*、$Enc(UK, HK_S + HK_K)$和 *LAT* 等。在使用加密内容时，用户将 *LIC* 中的 *LAT* 发送给密钥服务器，密钥服务器验证有效后，返回 $Enc(HK_K, AK)$给用户，用户然后使用属性私钥 *ASK* 解密出 *CMK*，再基于加法同态加密算法解密出 *CEK*。因此，用户只有满足属性结构并获取有效的许可证后才能解密内容。另外，撤销的用户由于无法通过密钥服务器获取加密的 *AK*，因此也无法解密内容。

定理 2 云服务提供商、授权服务器和密钥服务器均无法获得内容加密密钥。

在许可授权阶段，由于 *CMK* 使用 *AP* 加密，因此云服务提供商和授权服务器均无法获得 *CEK*。在内容解密阶段，密钥服务器可以根据 $Enc(PK_K, AK)$ 解密出 *AK*，但是无法获得 *CMK* 和 *LK*，因此也无法获得 *CEK*。另外，如果攻击者试图伪造 *LAT*，随机生成 HK_K'并发送 $Enc(PK_K, CID \| HK_K' \| T) \| Sig(SK_S', CID \| HK_K' \| T)$给密钥服务器。密钥服务器使用 PK_S 验证签名 $Sig(SK_S', CID \| HK_K' \| T)$不通过，攻击者无法获取 *AK*。因此，云服务提供商也不能

联合攻击者获得 *CEK*。

定理 3　攻击者不能重放云服务提供商的许可生成请求。

在许可授权阶段，云服务器提供商向授权服务器提交许可生成请求。攻击者试图重放许可生成请求，发送 $LSQ' \| Sig(SK_{SP}, LSQ')$给授权服务器。授权服务器验证 *LSQ'*的签名正确，然后使用 SK_S 解密 $LAQ \| T'$得到 *LAQ* 和时间戳 *T'*等，但是验证时间戳 *T'*与授权服务器时间不符。因此，攻击者无法通过重放攻击获取授权服务器颁发的许可证。

7.3　隐私保护分析

1) 匿名性

用户在内容订购时，生成随机的 *UK* 向授权服务器申请授权，云服务提供商和授权服务器无法获取用户的身份信息。用户在使用内容时向密钥服务器提交的 *LAT* 也不包含用户的身份信息。因此，本文方案能够保证用户的匿名性，防止泄露用户的身份信息。

2) 敏感记录保护

用户向云服务提供商订购内容时，随机生成密钥 *UK* 封装在许可授权请求中发送给云服务提供商。由于每次订购时 *UK* 都不相同，因此云服务提供商无法将该内容订购请求与特定的匿名用户联系起来，也无法收集匿名用户的内容订购记录。同时，许可授权申请中每次的时间戳 *T* 都不相同，因此授权服务器也无法统计特定匿名用户的授权记录。

用户在使用内容时，向密钥服务器提交 *LAT*，由于 HK_K 是随机生成的，并且每个内容的 HK_K 均相同，因此密钥服务器也无法分析用户的内容使用习惯。

通过以上分析，本文方案能够有效防止用户敏感记录的泄露和分析。

7.4　实验分析

1) 实验环境

下面将设计实验对本文方案的性能进行分析。实验环境是 Ubuntu 12.10 虚拟机（Intel Core i5 2.53 GHz，分配 2 GB 内存）。实验的编码实现基于 cpabe 库[22]，对称加密算法使用 128 bit AES 算法。

2) 实验结果

针对不同内容大小和属性个数的情况进行加密和解密实验，图 4 展示了访问策略中属性个数为 8 的情况下加密和解密时间开销与内容大小的对比关系，图 5 展示了解密时间开销与访问策略中属性个数的对比关系。实验结果可以看出，加密和解密的时间开销与内容大小和访问策略中属性个数成线性关系，加密 10 M 大小的内容所需的时间小于 1 s，解密时间也远小于加密时间，因此，本文所提方案在内容加密和解密操作的时间开销方面具有优势。

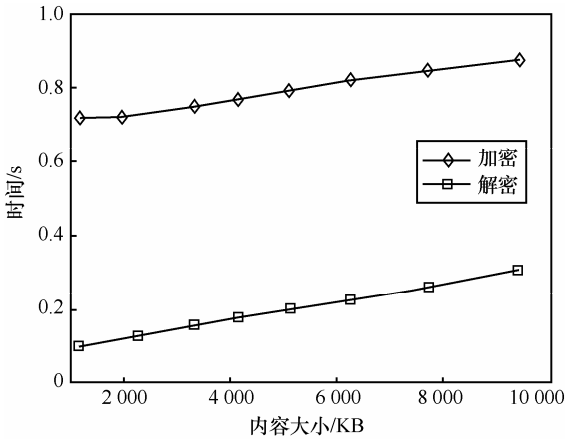

图 4　内容加密和解密时间开销与内容大小的关系

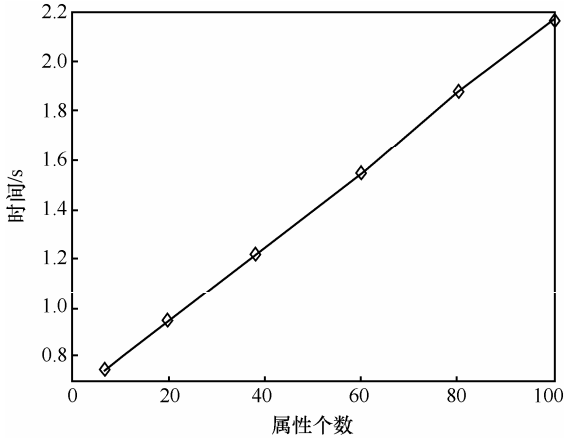

图 5　内容解密时间开销与属性个数的关系

7.5　与其他方案的比较

本文方案使用对称加密算法加密内容，保护内容的安全性，支持许可证的细粒度用户授权，如是否允许播放、时间限制和次数限制等，同时支持在线和超级分发应用模式。通过引入 CP-ABE 和加法同态加密机制分发内容加密密钥，保证内容加密密钥的安全性。另外，本文在保证用户匿名性的同时，能够防止用户敏感记录的泄露和分析。本文方案与现有的云计算环境中内容保护方案对比分析的结果如表 3 所示。

与文献[6,7]相比，本文方案支持细粒度的用户

表 3　云计算环境中内容保护方案功能对比分析

方案	内容加密	内容加密密钥保护	内容重加密	细粒度授权	许可证分发	用户匿名	敏感记录保护	在线模式	超级分发模式
文献[6]	对称加密	公钥加密	不需要	不支持	独立分发	不支持	不支持	不支持	支持
文献[7]	对称加密	对称加密	不需要	不支持	独立分发	不支持	不支持	不支持	支持
文献[12]	对称加密	属性基加密	不需要	支持	独立分发	支持	不支持	支持	不支持
文献[13]	对称加密	属性基加密	不需要	支持	独立分发	支持	不支持	支持	支持
文献[16]	加法加密	加法同态加密	需要	支持	独立分发	支持	支持	支持	不支持
本文	对称加密	属性基加密和加法同态加密	不需要	支持	独立分发	支持	支持	支持	支持

授权，同时允许用户匿名使用云计算环境中的版权保护服务，保护用户敏感记录。与文献[16]相比，本文方案使用对称加密算法加密内容，安全性更高，并且在使用内容时不需要重新加密内容，效率更高，同时也支持超级分发模式。与文献[12,13]相比，本文方案支持对用户敏感记录等隐私的保护。

8　结束语

针对云计算环境中数字版权保护的需求，本文提出一种云计算环境中支持隐私保护的数字版权保护方案。首先，提出云计算环境中数字内容版权全生命周期保护和用户隐私保护的框架，描述了数字内容版权全生命周期中系统初始化、内容加密、许可授权和内容解密 4 个主要的协议。其次，本文提出基于属性基加密和加法同态加密算法的内容加密密钥保护和分发机制，保证内容加密密钥的安全性。内容加密密钥由主密钥、授权密钥和辅助密钥组成，分别独立加密分发到用户。用户在其属性满足密文的访问策略并且拥有有效许可证的情况下，可以首先解密出主密钥，然后基于加法同态加密算法解密出授权密钥与辅助密钥的和，最后得到内容加密密钥。同时，本文允许用户匿名向云服务提供商订购内容和申请授权，有效保护用户的隐私，防止云服务提供商、授权服务器和密钥服务器等收集匿名用户使用习惯等敏感信息。此外，本文支持云计算环境中灵活的业务模式和许可证的细粒度授权，支持在线和超级分发应用模式。

安全性、隐私保护和实验分析表明，与现有的云计算环境中数字版权保护方案相比，本文方案灵活性及安全性较高，能够有效保护用户的隐私，支持灵活的访问控制，在云计算环境中具有较好的实用性。

参考文献：

[1] 冯登国, 张敏, 张妍等. 云计算安全研究[J]. 软件学报, 2011, 22(1): 71-83.
FENG D G, ZHANG M, ZHANG Y, *et al*. Study on cloud computing security[J]. Journal of Software, 2011, 22(1):71-83.

[2] 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 rights management[J]. Chinese Journal of Computers, 2005, 28(12):957-968.

[3] 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]. Journal on Communications, 2008, 29(10):153-164.

[4] ZHANG Z Y, PEI Q Q, YANG L, *et al*. Establishing multi-party trust architecture for DRM by using game-theoretic analysis of security policies[J]. Chinese Journal of Electronics, 2009, 18(3):519-524.

[5] QIU Q, TANG Z, LI F, *et al*. A personal DRM scheme based on social trust[J]. Chinese Journal of Electronics, 2012, 21(4):719-724.

[6] JAFARI M, SAFAVI-NAINI R, SHEPPARD N P. A rights management approach to protection of privacy in a cloud of electronic health records[A]. Proceedings of the 11th Annual ACM Workshop on Digital Rights Management[C]. Chicago, USA, 2011.23-29.

[7] WANG C K, ZOU P, LIU Z, *et al*. CS-DRM: a cloud-based SIM DRM scheme for mobile internet[J]. Eurasip Journal on Wireless Communications and Networking, 2011, 2011:1-30.

[8] PETRLIC R. Proxy re-encryption in a privacy-preserving cloud computing DRM scheme[A]. Proceedings of the 4th International Symposium on Cyberspace Safety and Security, CSS 2012[C]. Melbourne, Australia, 2012.194-211.

[9] SAMANTHULA B K, HOWSER G., ELMEHDWI Y, *et al*. An efficient and secure data sharing framework using homomorphic encryption in the cloud[A]. Proceedings of the 1st International Workshop on Cloud Intelligence[C]. Istanbul, Turkey, 2012.1-8.

[10] CORENA J C, OHTSUKI T. Secure and fast aggregation of financial data in cloud-based expense tracking applications[J]. Journal of Network and Systems Management, 2012, 20(4):534-560.

[11] WU Y D, WEI Z, DENG R H. Attribute-based access to scalable media in cloud-assisted content sharing networks[J]. IEEE Transactions on Multimedia, 2013, 15(4):778-788.

[12] 洪澄, 张敏, 冯登国. 面向云存储的高效动态密文访问控制方法[J]. 通信学报, 2011, 32(7):125-132.
HONG C, ZHANG M, FENG D G. Achieving efficient dynamic cryptographic access control in cloud storage[J]. Journal on Communications, 2011, 32(7):125-132.

[13] MULLER S, KATZENBEISSER S. A new DRM architecture with strong enforcement[A]. Proceedings of the 5th International Conference on Availability, Reliability, and Security, ARES 2010[C]. Krakow, Poland, 2010.397-403.

[14] CONRADO C, PETKOVIC M, JONKER W. Privacy-preserving digital rights management[A]. Proceedings of the Secure Data Management 2004[C]. Toronto, Canada, 2004.83-99.

[15] PERLMAN R, KAUFMAN C, PERLNER R. Privacy-preserving DRM[A]. Proceedings of the 9th Symposium on Identity and Trust on the Internet, IDtrust 2010[C]. New York, USA, 2010.69-83.

[16] PETRLIC R, SORGE C. Privacy-preserving DRM for cloud computing[A]. Proceedings of 26th IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2012[C]. Fukuoka, Japan, 2012.1286-1291.

[17] SAHAI A, WATERS B. Fuzzy identity-based encryption[A]. Proceedings of EUROCRYPT 2005[C]. Aarhus, Denmark, 2005.457-473.

[18] RIVEST R, SHARMIR A, DERTOUZONS M. On Data Banks and Privacy Homomorphisms[M]. Orlando: Academic Press, 1978.

[19] GENTRY C. Fully homomorphic encryption using ideal lattices[A]. Proceedings of the 41st Annual ACM Symposium on Theory of Computing[C]. New York, USA, 2009.169-178.

[20] DIJK M, GENTRY C, HALEVI S, *et al*. Fully homomorphic encryption over the integers[A]. Proceedings of Advances in Cryptology-Eurocrypt 2010[C]. Riviera, France, 2010.24-43.

[21] CASTELLUCCIA C, MYKLETUN E, TSUDIK G. Efficient aggregation of encrypted data in wireless sensor networks[A]. Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services[C]. San Diego, USA, 2005. 109-117.

[22] BETHENCOURT J, SAHAI A, WATERS B. Advanced crypto software collection[EB/OL]. http://acsc.cs.utexas.edu/cpabe/.

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，北京邮电大学讲师，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。

傅镜艺（1990-），女，重庆人，北京邮电大学硕士生，主要研究方向为数字版权管理、数字内容安全。

杨义先（1961-），男，四川盐厅人，北京邮电大学教授、博士生导师，主要研究方向为密码学、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，主要研究方向为数字水印、信息隐藏、隐写分析。