新闻出版重大科技工程项目管理及相关成果丛书

数字版权保护技术研发工程论文选辑

Selected Edition of Theses on the National DRM R&D Project

中国书籍出版社
China Book Press

编 委 会

《数字版权保护技术研发工程论文选辑》

主　编：魏玉山

副主编：张凤杰　张从龙

统　稿：张凤杰　李　欣

序　言

版权保护，是新闻出版业得以繁荣发展的前提，新闻出版业是版权产业的重要组成部分。信息技术的飞速发展，在给人们带来内容消费便捷的同时，也使侵权盗版变得更加容易。如果任由侵权盗版恣意横行，版权产业链将难以正常运转，内容企业的创新积极性将会下降，经济效益将无法保障，社会效益也将无从实现。

党中央、国务院高度重视版权产业的发展，做出一系列重大部署。政府主管部门不断加强顶层设计，完善相关政策、法律，加大执法力度，并通过实施“项目带动战略”，加强相关技术研发与应用，全面应对信息技术给版权产业带来的冲击。

早在十年前，原新闻出版总署就提出四项新闻出版重大科技工程的建设目标，由国家数字复合出版系统工程提供数字化生产系统，由数字版权保护技术研发工程（简称“版权工程”）提供版权保护与运营的技术保障，由中华字库工程提供用字保障，由国家知识资源数据库工程提供出版业向知识服务转型升级的全面支撑。四大工程先后列入国家“十一五”与“十二五”时期文化发展规划纲要，在国家财政的支持下陆续启动。

版权工程2007年6月启动可行性论证，2010年1月获准立项，2011年7月正式启动，共18个分包、26项课题，建设内容涵盖标准研制、技术研究、系统开发、平台搭建、总体集成、应用示范等多个方面，参与工程研发、集成、管理任务的单位24家。工程总目标是：探索数字环境下的版权保护机制，为出版单位数字化转型提供政府主导的第三方公共服务平台，为数字出版产业发展提供一整套数字版权保护技术解决方案。

在总局新闻出版重大科技工程项目领导小组的直接领导下，重大科技工程项目领导小组办公室积极推进，总体组、工程管控、总集、标准、监理以及各技术研发单位、应用示范单位共同努力，圆满完成了版权工程预定任务，取得了多方面的成果。

一是完成了工程的总体目标，实现了多项技术突破。按照总体设计方案，版权工程研究制定了四类25项工程标准与接口规范，形成了一套数字版权保护技术标准体系，在此基础上，突破传统版权保护技术手段，研发并形成了内容分段控制技术、多硬件绑定技术、富媒体保护技术、数字水印嵌入技术、媒体指纹提取技术、可信交易计数技术等版权保护核心支撑技术；针对移动出版、互联网出版、出版单位自主发行等业务模式，开发了五类版权保护应用系统，完成了五类数字版权保护技术集成应用示范；搭建了数字内容注册与管理、版权保护可信交易数据管理、网络侵权追踪三个公共服务子平台；经过整理与集成，最终形成了综合性的数字版权保护技术管理与服务平台。

二是获得多项知识产权，形成一系列相关成果。在技术研发过程中，版权工程共申请发明专利41项（其中5项已授权），登记软件著作权62件，在国内外媒体上发表论文42

篇。同时，为了解全球范围内相关领域最新的科技创新成果、发展方向和发展趋势，版权工程管控包委托第三方知识产权机构开展了专利检索分析、知识产权规避设计、专利池建设建议方案编制等工作，形成了一系列知识产权相关成果。

三是积累了重大科技工程项目管理的经验。版权工程是原新闻出版总署组织开展的第一个国家重大工程。在此之前，我们对重大科技工程项目管理缺乏经验，在工程的实施过程中，我们一边探索工程的管理体制与管理机制，一边组织工程的研发。通过工程的实施，我们形成了一套比较可行的工程管理体系，形成了包括财务管理、进度管理、质量管理等一批工程管理制度，积累了重大科技工程项目管理的经验。

在版权工程全面完工之际，及时总结工程项目管理经验，认真梳理工程创新成果，并加以展现和传播，具有重要意义。为此，版权工程总体组在总局重大科技工程项目领导小组指导和支持下，对工程标准、已发表论文、专利检索分析成果物进行梳理，对工程过程管理内容与质量控制举措等进行总结，形成系列丛书并予以出版。

版权工程时间跨度较长，参与单位较多，人员变动较大，相关成果物本身专业性、技术性非常强，整理、汇编起来非常不易；再加上丛书编写人员时间、精力有限，该套丛书在材料选取、内容校正、综合分析等方面肯定会存在不足。但瑕不掩瑜，本套丛书的出版，无疑可以为新闻出版行业类似项目的开展以及数字版权保护技术领域相关研究提供重要的经验借鉴和资料参考。

期望新闻出版行业以及社会各界以本套丛书的出版为契机，更加关注数字版权保护技术的研发与应用，共同推动版权工程成果的落地转化，利用高新技术手段，破解版权保护难题，为创新发展保驾护航，促进社会主义先进文化的大发展、大繁荣！

孙寿山

2016 年 12 月 12 日

出版说明

数字版权保护技术研发工程（简称版权工程）是列入国家“十一五”与“十二五”时期文化发展规划纲要的重大科技专项，是国家新闻出版广电总局新闻出版重大科技项目之一，是推进新闻出版业转型升级、实现持续发展、构建新兴业态的重要保障。在总局重大科技工程项目领导小组的直接领导下，总局重大科技工程项目领导小组办公室积极推进，总体组、工程管控、总集、标准、监理以及各分包研发单位、应用示范单位通力协作，攻坚克难，共同完成各项既定任务，取得了丰硕成果。

2016 年 12 月 2 日，版权工程召开整体验收会并顺利通过专家验收，验收专家对工程成果及工程管理和工程研发各方给予高度评价，一致认为版权工程立项定位明确，管理思路清晰，工作过程扎实、成果效果显著。

作为总局率先完成的新闻出版重大科技项目，数字版权保护技术研发工程除向行业及社会提供一套技术成果外，还将研发过程中产生的研究论文、专利检索分析报告、工程标准以及过程管理文档等汇编成书，供业界参考。这本身也是工程取得的另一形式的成果。

本套丛书共四部、七册，基本情况如下：

1.《数字版权保护技术研发工程过程管理与质量控制》：在介绍工程基本情况基础上，重点介绍了工程过程管理、质量控制的主要内容与方法，以及知识产权管理、软件测评管理等专项管理的“软技能”。此外，还有工程项目管理各阶段文档编写的要求（附模板）以及工程研发成果简要情况；

2.《数字版权保护技术研发工程论文选辑》：在工程研发过程中，各分包在中外媒体上公开发表的相关论文 42 篇。综合考虑论文质量及作者意愿，总体组分为“安全技术研究”、“相关算法研究”、“其他相关研究”三辑，选编了 28 篇论文成果结集出版；

3.《数字版权保护技术研发工程专利检索与分析》：以第三方知识产权公司专利检索分析成果为基础，从工程 72 个技术检索主题中选取了 55 个技术检索主题进行重点介绍。这些技术主题涉及“多硬件环境相关技术”、“加密认证相关技术”、“数字水印相关技术”、“内容比对相关技术”、“内容访问控制相关技术”、“其他相关技术”等六大方面。由于篇幅较大，分为上、下两册出版；

4.《数字版权保护技术研发工程标准汇编》：以工程研究制定的标准成果为基础，系统介绍了工程管理类标准、基础类标准、数据类标准以及工程接口协议类标准等四类 26 项标准。由于篇幅较大，分为上、中、下三册出版。

丛书出版是工程成果转化的形式之一。版权工程既定的研究建设任务虽已基本结束，但后续推广应用工作才刚刚开始。只有工程成果得到广泛应用，众多工程参与者的付出才

得到切实回报，工程成果的价值才能得以真正显现。此刻我们所要吹响的绝非船到码头车到站的“熄灯号”，而是动员各有关方面不忘初心、继续前进的“集结号”。

让我们继续努力，共同推动版权工程成果的落地转化，为新闻出版业数字化转型升级提供有力支撑，为传统出版与新兴出版融合发展提供有力支撑！

张毅君

2016 年 12 月 9 日

前　言

为应对信息技术飞速进步带来的挑战，促进新闻出版业态转型融合发展，国家新闻出版广电总局（原新闻出版总署）从产业需求出发，集众智力顶层设计，提出了数字复合出版系统工程、数字版权保护技术研发工程（简称版权工程）、中华字库工程、知识资源数据库工程等四项重大科技工程的建设目标并被先后列入国家“十一五”与“十二五”时期文化发展规划纲要。根据国家规划的分工部署于2007年开始可行性研究论证和相关立项工作；2011年，在国家财政的大力支持下，版权工程、中华字库工程率先启动研发。

版权工程是首个完成研发的新闻出版重大科技工程。在总局重大科技工程项目领导小组的直接领导、重大科技工程项目领导小组办公室的积极推进下，版权工程总体组、管控、总集、标准、监理与其他各研发参与方协同努力，圆满完成了版权工程预定的建设任务，取得了多方面的重要技术成果。其中，已发表论文体现了相关技术领域研发的重点和难点，是该工程创新性的重要标志。

按照项目合同书的约定，版权工程共有9个分包、10家项目承担单位涉及论文发表任务，拟发表论文数量为38篇。截至2016年6月，经过工程总体组审核与确认，已公开发表的相关论文总计42篇，版权工程论文发表任务超额完成。

在工程全面完工之际，版权工程总体组在总局新闻出版重大科技工程项目领导小组的指导和支持下，通过征询论文作者意见，将已发表的工程论文成果进行梳理并结集汇编成册，作为“新闻出版重大科技工程项目管理及相关成果丛书”之一予以出版，旨在展现版权工程技术创新成果，加强与业界分享及交流，同时为数字版权保护技术领域相关研究提供参照和借鉴。

本书共收录版权工程论文28篇，其中11篇以英文形式在国外媒体上发表。根据这些论文研究主题的相关性，版权工程总体组将其归结为三个大类，每个大类一辑，编作三辑出版。其中：

第一辑“安全技术研究”共收录相关论文12篇；

第二辑“相关算法研究”共收录相关论文8篇；

第三辑“其他相关研究”共收录相关论文8篇。

由于论文数量较多，涉及的作者较多，本书不再集中列示各位作者姓名，而是按照各分包提交的论文成果署名情况，分署于相应的论文之中。

借此机会，谨对版权工程的顺利完工表示祝贺，对版权工程各参与单位、全体参与人员包括本书所收录及未收录的所有论文的作者一并表示敬意！

谢俊旗

2016年11月28日

目 录

第一辑

安全技术研究

云计算环境中支持隐私保护的数字版权保护方案*

黄勤龙　马兆丰　傅镜艺　杨义先　钮心忻

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（digital rights management，DBM）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3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。

---

* 本文选自《通信学报》，第35卷第2期，2014年2月，第95－103页

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 ACMDRM 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* O。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
$c = Enc(m,k,M) = m + k(\mathrm{mod}\ M)$，其中，$M$ 是一个大整数，$m \in [0,M-1]$，$k \in [0,M-1]$。	$Dec(c,k,M) = c - k(\mathrm{mod}\ M)$。	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。

（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。

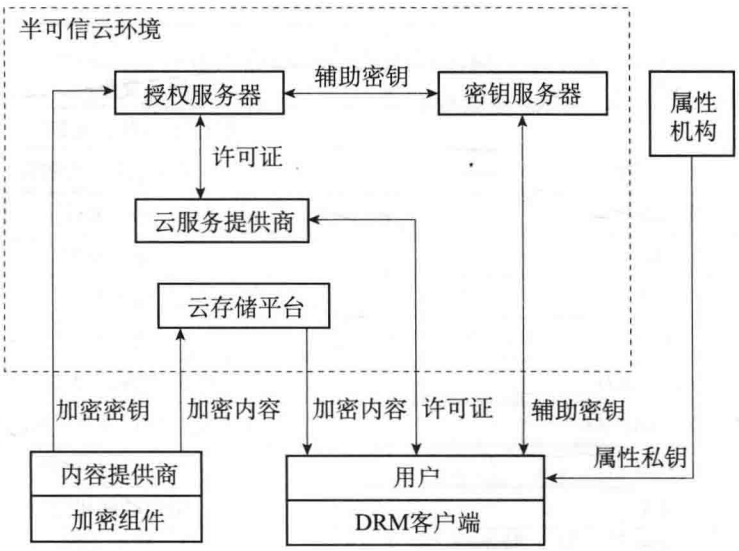

图 1　数字版权保护方案框架

（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。