学校编码：10384　　分类号_____密级_____
学号：200328006　　UDC _____

厦门大学

硕士学位论文

基于公钥密码算法的无状态广播加密方案的研究与应用

The Research and Implementation of Stateless Broadcast Encryption Scheme Based on Public Key Cryptography

陈昭智

指导教师姓名：郑建德 教授

专　业　名　称：计算机应用技术

论文提交日期：2006 年 5 月

论文答辩时间：2006 年　月

学位授予日期：2006 年　月

答辩委员会主席：_____

评　　阅　　人：_____

2006 年 5 月

厦门大学学位论文原创性声明

兹呈交的学位论文，是本人在导师指导下独立完成的研究成果。本人在论文写作中参考的其他个人或集体的研究成果，均在文中以明确方式标明。本人依法享有和承担由此论文产生的权利和责任。

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人完全了解厦门大学有关保留、使用学位论文的规定。厦门大学有权保留并向国家主管部门或其指定机构送交论文的纸质版和电子版，有权将学位论文用于非赢利目的的少量复制并允许论文进入学校图书馆被查阅，有权将学位论文的内容编入有关数据库进行检索，有权将学位论文的标题和摘要汇编出版。保密的学位论文在解密后适用本规定。

本学位论文属于

1、保密（　），在　　年解密后适用本授权书。

2、不保密（　）

（请在以上相应括号内打“√”）

作者签名：　　日期：　　年　月　日

导师签名：　　日期：　　年　月　日

摘 要

随着 Internet 的发展，多媒体信息越来越丰富，同时多媒体信息也不可避免地面临着版权保护的问题，迫切需要多媒体数字版权管理系统(DRM)来保障版权拥有者的合法权益。

基于无状态的广播加密算法能够非常直观地构建 DRM 系统。但目前应用较广的广播加密方案中用户持有的密钥为对称密钥，密钥发布中心、消息发布中心和用户持有同一对称密钥，其导致了用户密钥的安全性问题，并且多个消息发布方不能采用同一用户的同一密钥。公钥密码体制的引入可解决上述问题，但是一般公钥密码体制只能应用于广播加密中的 CS 方案，而效率更高的 SD 和 LSD 方案则需要使用基于身份的 HIBE 的加密方案。

本文首先利用基于 X509 证书的广播加密的完全子树(CS)方案设计并实现了一个灵活、安全的视频数字版权管理系统。

本文同时利用基于 Weil 配对性质的 HIBE 算法，利用子集覆盖框架下的完全子树(CS)方法构造了一种基于身份的广播加密方案。该方案使用用户的身份作为加密的公共密钥，因此无需单独的公钥/证书发布系统。同时该算法利用 HIBE 中的层次密钥算法，使得用户所需的私钥存储空间从 $\log N$ 减少到 1。本文同时对该方案的安全性、效率和动态可扩展性进行了讨论和分析。

本文同时将最新的恒定密文长度 HIBE 方案中的密钥生成方法和加解密方法进行改造，使之能够应用于广播加密中的子集差分(SD)方案中，并对其进行安全性分析。

关键字： 广播加密，子集覆盖，完全子树，子集差分，HIBE，数字版权管理

Abstract

With the success of the Internet, Multimedia applications and compression technology make great improvements. The security issue of Multimedia becomes more and more important. The digital rights management (DRM) is a good framework to solve the security problem and protect the copyright of multimedia.

The stateless Broadcast Encryption scheme can be directly designed to build a DRM system.Most of the Broadcast Encryption schemes for stateless receivers are designed to work in symmetric key setting. Key Distribution Center, Message Distribution Center and Client User all have to keep the same symmetric keys, which leads to the problem of key compromise. Building a public key broadcast encryption scheme is a good solution to this problem. However, the common public key schemes are fit only for Complete Subtree method in Broadcast Encryption. The more elegant SD/LSD methods using public key scheme will result in an enormous public key and very large storage for every user. The Hierarchical Identity-Based Encryption can reduce the public size and user's storage when it is used in SD/LSD methods.

Based on the stateless broadcast encryption scheme with Complete-Subtree method using the X509 certificate, this paper discusses the design of a secure Multimedia system and implements a scalable, flexible and more robust DRM system for Multimedia.

And we designed an ID-based broadcast encryption scheme using the latest HIBE algorithm based Weil Pairings and the complete subtree method under the subset cover framework. In this scheme, user's ID is used as public key for encryption. So the Public Key/Certificates Distribution System is not necessary. And the number of private keys which users have to keep can be reduced from O(*logN*) to O(*1*), because of the key hierarchical generation in HIBE algorithm. Finally the cryptanalysis and the discussion of efficiency and dynamic extensibility are given as well.

And We bring the latest and efficient HIBE scheme, which has the constant size cipher text, to SD method and demonstrate the modified HIBE scheme which makes

the key generation and decryption more efficient. The cryptanalysis of the scheme is given as well.

Key Words: broadcast encryption; subset-cover; complete subtree; subset difference; hierarchical identity-based encryption; digital rights management

目 录

Contents

第一章　绪论

1. 研究背景

随着信息化的加快发展，网络和个人计算机已经成为人们日常工作生活必不可少的工具之一。通过网络和计算机，人们可以进行相互通信或者获取自己所需的信息资源。同时，人们也越来越依赖于网络和计算机。一些企业的工作需要在网络和计算机上进行，现代城市中大多数人的生活都离不开计算机和网络。随着宽带的快速发展，诸如远程教学、视频会议、视频点播、网络游戏等新兴的网络应用越来越受到人们的关注。这些应用都涉及到“一对多”或者“多对多”的多播网络通信。

近几年随着宽带网络的建设和 Internet 的普及,出现了一类新兴业务,如宽带数字付费电视、数字广播、Internet 组播、广播电子赠券及电子宣传材料等,这类业务的共同特点是:广播性,前向信道数据率高,反向信道或者不存在、或者数据率很低;安全性,只有被授权用户(付费用户) 才可以接收信息。这类业务被统称为加密广播业务。

广播加密提供了一种在非安全的信道中以便捷的方式来分发数字信息给用户的方法。广播加密中的一种常见且应用广泛的情形是：加密消息的客户接收端是无状态的装置。即消息接收装置无法保存过去的所有传输并以此改变自身的状态。其解密操作必须基于当前的传输以及自身的原始配置。这种情况的主要应用有：受版权保护的 CD 和 DVD，卫星接收装置（GPS 或卫星电视），数字付费电视等。因此，设计能够应用于无状态接收装置的广播加密方案尤为重要。

自从 Fiat 和 Naor 在[1]中引入广播加密的问题以来，广播加密得到了广泛的研究。Naor D，Naor M 和 Lotspiech J[2]提出了能够应用于无状态接收装置的广播加密方案。他们提出了一种通用的“子集-覆盖”(Subset-Cover)框架，该框架能够高效的应用于这种无状态的广播加密方案。在文献[2]中，他们给出了基于该框架的两种实现方法：完备子树(Complete Subtree)方法，简称 CS 方法；以及更高效的子集差分(Subset Difference)方法，简称 SD 方法。基于该框架下的进一步研究成果包括 Halevy 和 Shamir[3]的 Layered SD 方案和 Goodrich，Sun 和 Tamassia[4]的 Stratified SD 方案，把子集差分的方案进一步完善，降低了通信开销。

目前应用较广的广播加密方案中用户持有的密钥为对称密钥，密钥发布中心、消息发布中心和用户持有同一对称密钥，其导致了用户密钥的安全性问题，并且多个消息发布方不能采用同一用户的同一密钥。公钥密码体制的引入可解决上述问题，由密钥发布中心发布的用户私钥由用户保存，而消息发布中心只使用用户的公钥进行加密，消息的发布过程不会有泄露用户私钥的可能性。

但是若一般公钥密码体制应用于上述广播加密方案中，消息发布方需要持有大量的用户的公钥，在 SD 方法实现中所需的公钥持有量更加庞大。基于身份的公钥密码体制能够很好地解决公钥量庞大的问题，用户的公钥可以直接根据用户的身份名称(如姓名，身份证号，邮件地址等)得到。一般的基于身份的公钥加密算法能够直接应用于 CS 方法中，但要在更高效的 SD 和 LSD 方法中使用，则须使用分层结构的基于身份的公钥加密算法(Hierarchical Identity Based Encryption)，简称 HIBE。

HIBE 中每一层中 ID 对应的私钥可以由上一层父节点生成或者其任意祖先节点生成，这一性质刚好符合子集差分方案中对密钥链生成规则的要求，只要对现有的 HIBE 进行改造就可以应用于广播加密的子集差分方案中。

目前已有的基于 Weil 配对的 HIBE 主要有[7]，[9]，[10]。在文献[7]和文献[10]中的 HIBE 方案，用户的持有密钥长度随着自身所处层次的增加而增加，同时密文的长度也随之增加。而在文献[9]的方案中，密钥同样随着层次的增加而减少，而密文的长度能够保持恒定不变，同时该方案较前两种方案计算量更少，效率更高。在广播加密方案中，每个用户需要持有若干密钥，同时发布的加密消息中是由多个身份公钥加密的多段密文组成。在现有的三种 HIBE 方案中，由于[9]的方案具有的密文长度恒定、计算效率高的优点，非常适用于广播加密方案中的 SD 方法。

Dodis 和 Fazio 在[5]中提出了在 HIBE 方案下将 SD 和 LSD 方法转化为公钥体制的基本方法，并在附录中引述了文献[7]中的 HIBE 算法。文献[9]中也提出了恒密文长度的 HIBE 方案可以应用于广播加密中的 SD 方案。但在现有的文献中都没有具体的 HIBE 在广播加密 SD 方法中应用的实现方案，以及效率讨论与安全性的证明。

本文利用[9]中的 HIBE 算法的思想，构造了一种基于 Weil 配对性质的快速

广播加密算法。该算法的特点是：

(1)消息发布方只需知道用户二叉树的结构(或构造规则)和 O(logN)个必要的系统参数就可以进行广播加密，减少了繁杂的用户公钥查询和发布的过程。

(2)同时每个用户只需持有一个主密钥和 logN 个密钥生成参数。其中的主密钥需要以安全的方式存储，而 logN 个密钥生成参数可以存放在公共存储区域，并不会对系统安全性产生影响。而一般的基于对称密钥的方案和基于公钥的方案都需要在安全存储区中存放至少 logN 个密钥。这样可以减少安全保存区的容量要求，如小型智能卡、电子钥匙等安全保存区容量有限的应用环境，减少用户端硬件的成本。

本文提出了将[9]中的 HIBE 在广播加密 SD 方法中应用的实现方案。在该方案中对用户持有的密钥生成方法进行优化，进一步减少用户所需的存储空间，并构造快速解密密钥的生成方法，使得在由父密钥生成子密钥解密更加快捷。本文同时提出广播加密方案的安全攻击模型，并给出了在该种安全攻击模型下的安全性证明。

2. 研究目标与内容

2.1. 研究目标：

1. 将新的恒定密文长度 HIBE 方案中的密钥生成方法和加解密方法进行改造，使之能够应用于广播加密中的 SD 方案中，并进行相关的优化和安全性分析
2. 将现有的几种可应用于广播加密 SD 方案的基于身份的公钥密码算法进行横向比较，
3. 设计一套基于公钥密码算法的广播加密 CS 方案的原形系统

2.2. 研究内容：

1. 改造现有恒密文长度的 HIBE 方案的密钥生成算法以及加解密算法，构造在广播加密 SD 方案使用的基于身份的公钥密码算法
2. 对构造的方案进行相关的安全性分析
3. 使用现有的公钥密码算法实现广播加密的 CS 方案，利用构建的原形系统演示基于公钥的密码算法应用在广播加密中的一些特性和优势

第二章　广播加密算法

1. 算法简介

本章首先介绍在组播中应用较广的逻辑密钥层 LKH(logical key hierarchy)密钥管理方案。在该方案中，用户需要保持在线的状态，以便当系统的用户退出时组密钥管理中心能够实时地更新剩于用户的密钥。

当用户一般处于不在线的状态时，系统是无法更新个用户的密钥的。因此有 LKH 方案衍生出了用户是无状态时(Stateless，即用户无法更新自身的密钥)的密钥管理方案，子集覆盖 Subset-Cover 方案。

本章将逐一介绍 Subset-Cover 方案的框架，以及在该框架下的两种实现方法：完全子树(Complete-Subtree)和子集差分(Subset-Difference)。

2. LKH

文献[12,13]各自提出了倒置树(rooted-tree)式的逻辑密钥层次 LKH(logical key hierarchy).它们以及由此派生出来的一系列方案统称为树型(tree-based)密钥管理[14]。

逻辑层次树技术中，密钥由密钥服务器产生，组控制器管理的密钥及相关密钥都用维数为 d 的树来表示，根节点表示组会话密钥，每一个叶子节点表示一个成员密钥，中间结点密钥用于保护组会话密钥的分发，没有实际的物理实体，成员通过组会话密钥进行加密通信，组控制器负责对组密钥进行集中管理。

图-1 是一棵逻辑层次树的示意图，为了便于描述，我们以平衡二叉树（逻辑层次树对此并不要求）为例，讨论成员加入和退出时的密钥更新过程。

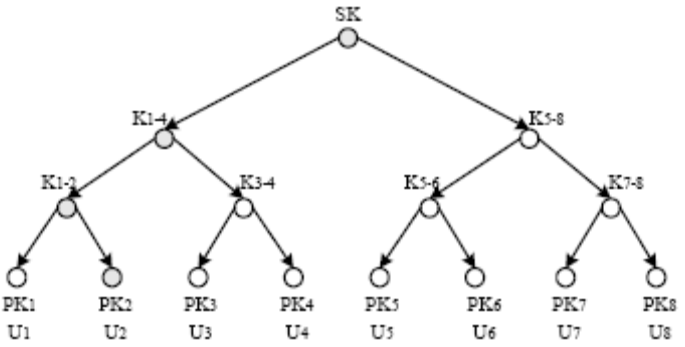

图-1 逻辑层次树

每个成员需要存储从叶子节点到根节点经过的所有密钥，例如成员 $U2$ 拥有

的密钥有{PK_2、$K_{1\text{-}2}$、$K_{1\text{-}4}$、SK}；组控制器端需要存储整棵密钥树所有节点的密钥。

当成员向组控制器申请加入多播组时，组控制器首先验证成员的身份，确认后为该成员产生新的成员节点并产生密钥 PK_i 作为该成员的私有密钥，通过单播分发给该成员。为了实现向前访问控制，组控制器需要产生新组会话密钥 $SK(r+1)$，用该成员的 PK_i 加密再传送给该成员，成员获得组会话密钥 $SK(r+1)$ 后就可以解密组通信数据；同时组控制器通过旧的组会话密钥 SK 加密分发新组密钥 $SK(r+1)$，完成剩下成员的新组会话密钥的更新。

成员退出时，需更新其所在路径与其他成员共享的密钥，以实现向后访问控制。例如在图-1 中，成员 U_2 退出时，密钥更新过程如下(其中$\{K'\}_K$ 表示用 K 加密 K')：

(1)$K_{1\text{-}2}(r)$更新为 $K_{1\text{-}2}(r+1)$，$\{K_{1\text{-}2}(r+1)\}_{PK1}$ 发送给成员 U_1；

(2)$K_{1\text{-}4}(r)$ 更新为 $K_{1\text{-}4}(r+1)$，$\{K_{1\text{-}4}(r+1)\}_{K1-2(r+1)}$、$\{K_{1\text{-}4}(r+1)\}_{K3\text{-}4(r)}$发送给成员 $U1$、 $U3$ 和 $U4$；

(3)$SK(r)$ 更新为 $SK(r+1)$， $\{SK(r+1)\}_{K1-4(r+1)}$、$\{SK(r+1)\}_{K5\text{-}8(r+1)}$发送给成员 $U1$,$U3$,… ,$U8$。

在一棵维数为 d, 树深为 $h+1$ 的逻辑层次树，它的组成员最多可以有 $N=d^h$ 个，成员端的密钥存储量 $C_{GM}=h+1$，组控制器端的密钥存储量 $C_{GC}=(d^{h+1}-1)/(d-1)$。在 LKH 中，删除一个成员时密钥更新所需要的网络流量为 $T=d^h+1$ 。

3. Subset Cover 框架

子集覆盖框架(Subset-Cover)的基本思想是：将所有的 N 个用户作为叶子节点并组织成一棵完全二叉树（如图-2）。根据这个用户树，系统调用 Subset 算法对用户进行集合的划分，每个用户属于若干个集合。当有 R 个用户被系统撤销时，调用 Cover 算法对 N\R 个用户进行划分，划分出若干个互不相交的集合，这些集合的并集覆盖了所有的合法用户。

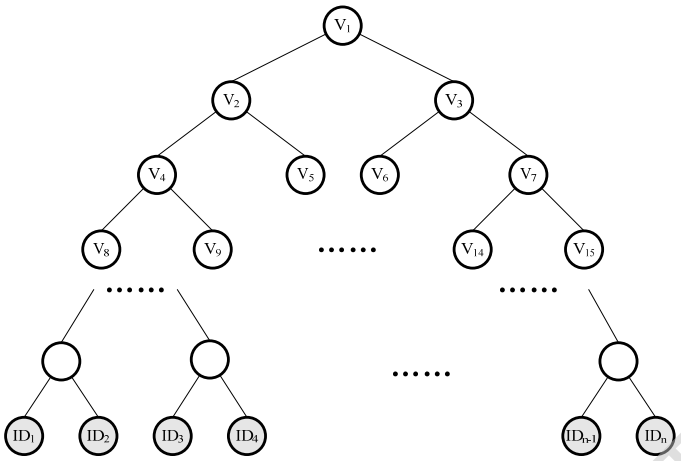

图-2 由所有用户组成的完全二叉树，最下层的叶子节点代表各个用户

3.1. 子集覆盖 Subset-Cover 框架概述

Setup 步骤：该方法就是将所有的用户作为叶子节点并组织成一棵完全二叉树。为这棵树的每个节点分配一个密钥。对于一个有 N 个用户的系统来说，需要生成 2N-1 个密钥。从另一个角度来看，每个树中的节点代表一个集合，该集合包含所有该节点的后代叶节点所代表的用户。

分发步骤：对于每个该系统的用户，以安全保密的方式分发给该用户所在节点及其所有祖先节点所对应的密钥。就是说该用户持有其所属所有集合对应的密钥。

广播步骤：

子集划分：首先获得已撤销的用户列表，调用 Cover 算法对除去撤销用户了的合法用户进行子集划分。划分结果即每个合法用户属于且仅属于这其中的某一个集合。

加密：欲对传输用的 SessionKey 制作加密消息头，用所划分集合所对应的密钥分别对 SessionKey 进行加密，同时用 SessionKey 对消息进行加密。

解密步骤：

每个合法用户接受到加密消息以及消息头之后，在消息头中寻找到用自身所属集合的密钥加密的 SessionKey 数据，使用自身持有的某一个密钥对其进行解密后即可获得 SessionKey，并对加密的消息进行解密获得消息。

使用该种方法的具体实现方式有：完备子树，子集差分以及 Layered 子集差