申请上海交通大学硕士学位论文

基于属性的加密算法

学　　校：上海交通大学

院　　系：计算机科学与工程系

学科专业：计算机软件与理论

研 究 生：单忆南

导　　师：曹珍富 教授

上海交通大学电子信息与电气工程学院

2009 年 12 月

A Dissertation Submitted to Shanghai Jiao Tong University for the Degree of Master

Attribute-based Encryption Algorithm

Author: Yinan Shan

Advisor: Prof. Zhenfu Cao

Specialty: Computer Science and Engineering

School of Electronic, Information and Electrical Engineering

Shanghai Jiao Tong University

December 2009

上海交通大学

学位论文版权使用授权书

本学位论文作者完全了解学校有关保留、使用学位论文的规定，同意学校保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权上海交通大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

保密□，在____年解密后适用本授权书。

本学位论文属于

不保密□。

（请在以上方框内打“√”）

学位论文作者签名：　　指导教师签名：

日期：　年　月　日　　日期：　年　月　日

上海交通大学

学位论文原创性声明

本人郑重声明：所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已经注明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

学位论文作者签名：

日期：　年　月　日

基于属性的加密算法

摘 要

随着密码学的不断发展，基于属性的密码体系作为基于身份的密码体系的一个扩展，由于其特殊的应用意义以及使用场景的广泛性正在受到越来越多的关注。利用属性的加密体系，系统中的用户的认证以及访问权限不再用单一的身份或者证书进行刻画，每个用户拥有一个属性集合以及属性集对应的密钥集。加密或者解密的过程与一个访问控制结构相关联，我们可以通过对此结构的定义规定解密者应具有的属性结构。

目前基于属性的密码研究已经取得了一系列的进展，无论从加密政策类型的划分：密钥政策和密文政策，基于属性的数字签名方案，较强的安全可证模型的安全证明以及多授权方的基于属性的加密算法都使得基于属性的密码研究向前迈进了一大步。但是基于属性的密码体系仍然存在一些问题需要人们研究和解决，其中包括：提高密码运算效率，比如如何减少配对运算的次数；提高访问控制结构的表达能力，在已有的门限，与门，或门和非门等基础上，如何构造更强大的单调或者非单调表达能力的访问控制结构；设计和构造更多更实际的基于属性密码系统的应用以及应用场景；简化密钥密文关系以及缩小密文空间的规模等等。

本文也将围绕基于属性的密码关注的几个方面进行研究。首先我们对基于属性密码算法的引入，意义以及现有的一些方案和协议进行了整理，并给出了相应的分析和比较。之后介绍了多授权方的基于属性的加密算法和基于属性的数字签名方案。然后我们利用并且扩展了Waters[10]的访问控制结构的构造方式，构造了一个新的多授权方的密文政策的基于属性的加密算法，并给出了基于选择属性密钥集安全模型

的一个证明。

之后我们对于新设计出的多授权方的基于属性的加密算法进行了扩展，将其应用于私密信息提取的应用场景中。结合私密信息提取的特点，设计出一套高效安全的方案。在文章的最后我们利用 SPIR[15]协议对我们的方案又进行了改进，使其获得更高的安全性属性和应用意义。

关键词：基于属性的加密，可证安全，多授权方，私密信息提取, 访问控制结构。

Attribute-based Encryption Algorithm

ABSTRACT

As the development of the Cryptography, attribute-based Encryption, an extension from the Id-based encryption is now drawing more attention from researchers in this community for its specific practicability and scenario. The users in attribute-base encryption system are not described by Identities or certifications any more but a set of attributes. The encryption course or decryption course is related to a so called access structure. We can define the access structure to associate the set of attributes.

Currently, the attribute-based encryption has reached a lot of achievements, such as the policy definition of the attribute-based encryption: ciphertext policy attribute-based encryption and key policy attribute-based encryption; attribute-based digital signature scheme; strong secure proof model applied; and multi-authority attribute-based encryption. These aspects all contribute a lot to the attribute-based encryption. However, there are still some problems involving in these methods, which includes: the improvement of the efficiency of the calculation, how to decrease the calculation times of bilinear pairings; how to improve the express ability of the access structure, how to construct more expressive monotone/non-monotone access structure based on the threshold gate AND gate and OR gate; how to construct more practical attribute-based encryption systems; how to simplify the relations between key and cipheretext; how to decrease the size of the ciphertext space and key space

This article will show the research work based on the questions mentioned in the above. First we will bring in the attribute based encryption and its significant meaning. Then we will introduce the current schemes of the attribute-based encryption and make comparisons. After that, we will also introduce multi-authority attribute-based encryption and attribute-based digital signature. Further, we will show a new constructed multi-authority attribute-based encryption based on the access structure from Waters[10] plan and give a security proof with the adaptive selective set of attributes.

We then extend the newly contrived multi-authority attribute-based encryption and apply it into the private information retrieval scenario. This scheme is practical and efficient. Finally we improve the scheme by using SPIR[15] scheme and make improvement on the security attribute and practicability.

Keywords: attribute-based encryption, multi-authority, provable secure, access structure.

目 录

基于属性的加密算法.....9
摘 要.....9
ABSTRACT.....11
第一章 绪 论.....17
1.1 研究背景.....17
1.2 公钥密码学.....18
1.3 从基于身份到基于属性的加密算法.....20
1.4 论文的组织结构.....22
1.5 本章小结.....22
第二章 预备知识.....23
2.1 数学运算.....23
2.1.1 近世代数基础.....23
2.1.2 双线性配对.....23
2.1.3 拉格朗日插值定理.....23
2.2 安全假设与计算复杂性.....24
2.2.1 安全假设.....24
2.2.2 计算复杂性.....25
2.3 可证安全模型.....25
2.3.1 可证安全基本定义.....25
2.3.2 可证安全模型.....26
2.4 基于属性加密算法的相关定义.....27
2.5 本章小结.....29
第三章 基于属性的加密算法及应用.....31
3.1 模糊匹配的基于身份(Fuzzy IBE)的加密方案.....31
3.2 近年来的基于属性的加密方案.....32
3.2.1 V Goyal 等人的 Fined-Gained KPABE 方案[4].....32
3.2.2 Brent Waters 的 CPABE 方案.....34

3.2.3 现有方案的比较及综述 34
3.3 多授权方的基于属性加密方案 36
3.3.1 基本场景介绍 36
3.3.2 Chase 的开创性方案 36
3.3.3 已有多授权方的基于属性的加密算法的比较 38
3.4 基于属性的签名方案 38
3.4.1 基本应用场景描述 38
3.4.2 D Khader 的基于属性的签名方案 39
3.4.3 已有的基于属性签名方案的比较 40
3.5 基于属性加密算法相关的其它研究 41
3.6 本章小结 42
第四章 基于属性的多授权方加密方案 43
4.1 基于属性的多授权方加密方案内容描述 43
4.1.1 方案参与者描述 43
4.1.2 方案函数描述 43
4.1.3 方案定义和场景描述 44
4.1.4 方案的构造描述 44
4.2 一个基于属性的多授权方加密方案的效率和应用分析 45
4.3 一个基于属性的多授权方加密方案的安全性证明 46
4.3.1 一个基于属性的多授权方加密方案的安全模型 46
4.3.2 一个基于属性的多授权方加密方案的安全证明 47
4.4 本章小结 49
第五章 用于私密信息提取的扩展的属性基加密方案 51
5.1 私密信息提取 51
5.2 用于层次化认证私密信息提取的扩展的属性基加密方案 51
5.2.1 场景描述 51
5.2.2 用于层次化认证私密信息提取的扩展的属性基加密方案函数描述 53
5.2.3 用于层次化认证私密信息提取的扩展的属性基加密方案运行方式描述 54
5.2.4 用于层次化认证私密信息提取的扩展的属性基加密方案构造描述 54
5.2.5 用于层次化认证私密信息提取的扩展的属性基加密方案的效率和安全分析 56

5.3 改进的用于私密信息提取的扩展的属性基加密方案 57
5.3.1 SPIR[28]方案的工作原理 57
5.3.2 改进的用于私密信息提取的扩展的属性基加密方案函数描述 58
5.3.3 改进的用于私密信息提取的扩展的属性基加密方案运行方式描述 58
5.3.4 改进的用于私密信息提取的扩展的属性基加密方案构造描述 59
5.3.5 改进的用于私密信息提取的扩展的属性基加密方案的效率和安全分析 61
5.4 本章小结 63
第六章 总 结 65
6.1 主要结论 65
6.2 研究展望 66
参 考 文 献 69
致 谢 73

第一章 绪 论

1.1 研究背景

随着网络信息技术应用的日渐普及,网络信息安全越来越成为一个倍受关注的课题。一方面，网络信息技术使世界范围的信息交流日益方便快捷，同时给人们带来了更多的商业和科学研究的机会。而在另一方面，一旦网络上传递的重要信息(如国家机密、商业机密或个人隐私等)被截获或篡改，国家、企业或个人将蒙受巨大损失。另外，以非法入侵和非法获利为目的的信息犯罪日益增多，也对网络的安全运行和进一步发展提出了挑战。（例如信息泄漏、信息窃取、数据篡改、数据删添、计算机病毒等）通常利用计算机犯罪很难留下犯罪证据，这也大大刺激了计算机高技术犯罪案件的发生。计算机犯罪率的迅速增加，使各国的计算机系统特别是网络系统面临着很大的威胁，并成为严重的社会问题之一。人们对信息安全的要求越来越强烈，这一迫在眉睫的现实需求成为推动信息安全理论与技术研究的能动力。

通常情况下我们把信息安全定义为机密性、完整性、可用性、可控性和不可抵赖性的综合体服务。

- 机密性：指信息按给定要求不泄漏给非授权的个人、实体或过程，或提供其利用的特性，即杜绝有用信息泄漏给非授权个人或实体，强调有用信息只被授权对象使用的特征。
- 完整性：指信息在传输、交换、存储和处理过程保持非修改、非破坏和非丢失的特性，即保持信息原样性，使信息能正确生成、存储、传输，这是最基本的安全特征。
- 可用性：指网络信息可被授权实体正确访问，并按要求能正常使用或在非正常情况下能恢复使用的特征，即在系统运行时能正确存取所需信息，当系统遭受攻击或破坏时，能迅速恢复并能投入使用。可用性是衡量网络信息系统面向用户的一种安全性能。
- 可控性：指对流通在网络系统中的信息传播及具体内容能够实现有效控制的特性，即网络系统中的任何信息要在一定传输范围和存放空间内可以被控制。除了采用常规的传播站点和传播内容监控这种形式外，最典型的如密码的托管政策，当加密算法交由第三方管理时，必须严格按规定可控执行。

- 不可抵赖性：指通信双方在信息交互过程中，确信参与者本身，以及参与者所提供的信息的真实同一性，即所有参与者都不可能否认或抵赖本人的真实身份，以及提供信息的原样性和完成的操作与承诺。

1.2 公钥密码学

公钥密码学开始于 1976 年由 Diffie 和 Hellman 的一篇文章《密码学的新方向》[1]。在这篇文章中，作者第一次提出了公共钥密的概念，即加密的密钥（公钥）和解密的密钥（私钥）不同，同时从计算的可行度来看，知道一个加密公钥是无法计算出相应的解密私钥的。

公钥密码学又称非对称密码学，是相对于传统的对称密码学而言的一种定义。

对称密码算法，要求通信双方必须事先共享加密和解密的密钥，才能实现保密通信，工作方式如图 1-1 所示。此类密码系统的优点是计算效率高，但随之而来的问题是，双方在实现保密通讯前，需要事先进行秘密的密钥协商，当用户数量大量增加的情况下，密钥的生成、存储以及分发所带来的开销都非常大。

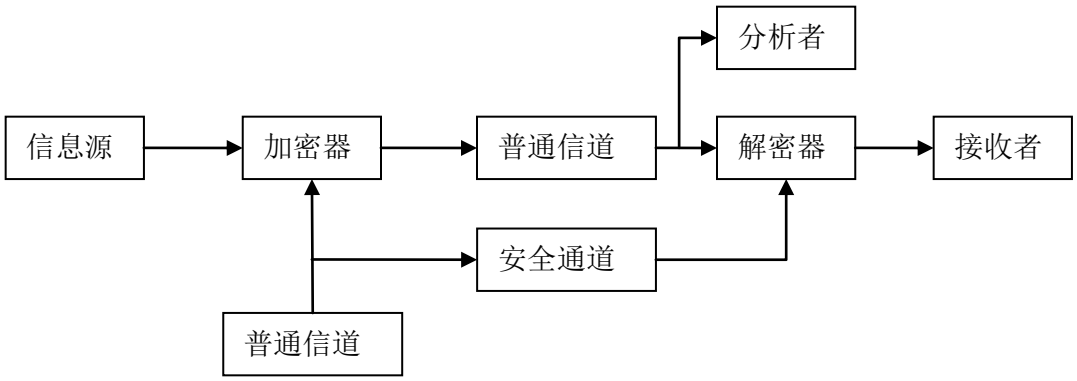

图 1-1 对称密码体系下的 Shannon[43]保密系统

于是公钥密码学与对称密码学相比有了以下几个优点。首先公钥的拥有者可以将公钥作为公开参数公布，而且无须担心解密用的私钥被泄露。对称加密算法因必须使用相同的密钥，往往需要借助可信通道，密码本等方式约定一个共同的密钥，所以当密钥持有者的一方被攻破，这个系统的其它参与方也将是不安全的。其次公钥密码系统解决了对称密码系统中密钥量随用户增加而激增的问题，而且也使得密钥更加容易管理。由公钥密码学技术产生的更多的信息安全保证手段，如密钥分发协议，公平交易，数字签名，密钥协商等也得到了更好的应用和发展。

第一个公钥密码方案 RSA[2]由 Rivest, Shamir 和 Adleman 三人于 1978 年提出，利用大整数分解难题假设进行构造，对之后的公钥密码学发展影响重大。至今仍作

为标准的加密算法，应用于各种安全体系中，只是密钥长度已经增加了很大规模，已经达到 1024 位。由 RSA 衍生出的各种签名，认证更促进了密码学的其它领域的发展。

公钥密码学虽然解决了很多对称密码系统中出现的问题，但也存在很多需要改进的地方。例如，在公钥密码系统中，用户的公钥是某个集合上的一个随机比特串，加密者如何正确选取与信息获取者对应的公钥，即将公钥和目标的身份绑定起来是一个重要而有意义的问题。为了解决这个问题，Kohnfelder[31]在 1978 年提出了基于证书的加密算法的概念，一个合法的公钥证书中包含了持有者身份信息，公钥参数，以及可信第三方对整个信息的一个数字签名。

所谓数字签名就是附加在数据单元上的一些数据,或是对数据单元所作的密码变换。这种数据或变换允许数据单元的接收者用以确认数据单元的来源和数据单元的 完整性并保护数据,防止被人(例如接收者)进行伪造。它是对电子形式的消息进行签名的一种方法, 一个签名消息能在一个通信网络中传输。基于公钥密码体制和私钥密码体制都可以获得数字签名,目前应用叫广泛的主要是基于公钥密码体制的数字签名。

数字签名的应用过程是，数据源发送方使用自己的私钥对数据校验和或其他与数据内容有关的变量进行加密处理，完成对数据的合法“签名”，数据接收方则利用对 方的公钥来解读收到的“数字签名”，并将解读结果用于对数据完整性的检验，以确认签名的合法性。数字签名技术是在网络系统虚拟环境中确认身份的重要技术，完全可以代替现实过程中的“亲笔签字”，在技术和法律上有保证。

密钥协商协议与加密、数字签名，被认为是最基本的 3 个密码原语（Cryptographic Primitive）。密钥协商协议允许两个或者两个以上的用户在由敌手完全控制的开放式网络环境下通过交换信息，协商完成一个共享的密钥。这一密钥将用于这些用户之间的后续安全通信。因此，安全密钥协商协议是更加复杂的高层协议的最基本模块。最早提出密钥协商的也正是文章[1]给出的 Diffie-Hellman 密钥协商协议。

如果一个密钥协商协议能够允许一组用户在开放式网络环境下协商达成一个共享密钥，并确保只有指定的用户有可能获得这一共享密钥。这样的性质叫做隐式密钥认证（Implicit key authentication）[28,29]，进一步，这样的密钥协商协议叫做认证密钥协商协议。另外，如果该协议还能够确保指定的用户确实拥有了某个共享密钥，这样的属性叫做显式密钥认证（Explicit key authentication），提供显式密钥认证的密钥协商协议叫做带密钥确认（Key confirmation）的认证密钥协商协议。近 20 年以来，多种多样的安全属性被发现是一个安全的密钥协商协议所必需达到的。人们

开发了不同的方法来研究如何获得这些安全属性。密钥抽取函数、消息认证码（MAC）、数字签名方案等等，是认证密钥协商协议的基本工具。这些协议分为两大类：证书基协议与身份基协议。在证书基密钥协商协议中，通信的双方需要获得对方的长期公钥，而这样的公钥是经过公钥证书中心 CA 认证过的，因此证书基公钥在使用的过程中，不可避免的牵涉到 CA 数字签名的验证，这大大增加了用户的计算负荷。而在身份基密钥协商协议中，用户的公钥是一些例如姓名、家庭住址或者电子邮件等身份信息，这样的公钥在使用时，不需要验证它的真实性。

另外，由于公钥密码学大多数是基于复杂的数学计算，效率与对称密码学相比有一定的劣势，于是很多公钥密码和对称密码结合的体系相应诞生。例如，利用密钥协商协议使得参与的双方或多方获得临时的统一的密钥，再通过对称加密进行大规模的数据传输。

1.3 从基于身份到基于属性的加密算法

在 1984 年，Shamir[4]提出了基于身份的加密方案。其中，用户的身份信息就相当于用户的公共密钥。同时有一个所有用户信任的私钥生成者（PKG），有时也称为密钥生成中心（KGC），它提供用户相应的私钥。Shamir 在基于证书的公钥基础设施提出了一个实际的身份基签名方案并且要求基于身份的加密方案来简化密钥管理过程。

Shamir 在文献 [4] 中提出了一个基于整数分解的身份基数字签名方案，于是如何找到一个安全实用的身份基加密方案成为研究者关注的问题。在此之后，Boneh 和 Franklin 利用椭圆曲线上的双线性配对首次提出了一个基于身份的加密方案[5]，Cocks[7]利用二次剩余理论构造了一个安全的基于身份的加密方案，并由 Boneh 在 2007 年对此方案进行了改进。

传统的访问控制系统中，消息以明文的形式存储于服务器。当用户需要获得这些消息时，将自己的认证消息发给控制器，控制器通过认证确认了用户的合法使用性就可以将相应的被询问信息发送给用户。但是这个方案存在如下几个问题，首先，以明文的形式存储于服务器是不安全的，一旦攻击者直接可以拿到服务器的控制权限，所有的消息也就被泄露了。其次，当控制器经验证后把信息传递给用户的时候需要其它的手段保证传输不被窃听。针对以上问题，通过公钥密码系统和基于身份的加密手段，我们就可以使安全性大大提高。但是大部分的基于身份的密码系统，如方案[30-34]都应用了双线性配对技术，于是也引入了一个基于身份密码体系的效率改进的问题。

因此公钥密码学应用于访问控制系统的方案构造为，每个用户有一对公私玥对，消息是以用户的公钥加密的形式存储于服务器中，服务器只简单响应用户的询问需求，并回复对应的密文，只有具有相应私钥的用户才可以解密。

在基于身份的密码学体系中，通信模式往往是一对一的，即加密方和解密方都是唯一的，这里所叙述的一对一同时也包括签名和认证的双方。所以加密者必须知道解密者的身份，而验证者必须知道签名者的身份。这样的通讯模式在实际的系统中很多局限性。例如，当加密方想要将一个信息让目标的一群人得以分享，以现在的系统只能针对每一个人的私钥进行加密，将不同的机密结果在公共信道传送至对应的人群。在这种情况下用已有的方案进行操作，无论是在效率上还是实际应用都是难以让人满意的，因此一种基于访问控制的思想和身份基加密相结合的方案被提出。

一个典型的利用基于身份加密技术解决这类问题的方案就是基于身份的广播加密。在广播加密的过程中，可以被解密的身份集合被涵盖在密文中，于是只有解密者是广播加密密文的目的接收者时，用户才可以解密。

在这种思路的提示下，一种表达能力更强大的访问控制方案被提出。在系统中的每个用户并不是由 ID 以及对应的私钥确定唯一的身份。每个用户是由一组属性进行刻画的，而每个属性对应于一个或者一组密钥。这里的属性一般就是指系统所关心的一些特质，例如，职位，所属部门，工作时间等等。明文通过一种加密方式讲访问控制信息与对应的属性结合起来得到密文。当解密者拥有了符合这个访问结构的密钥时，才可解密。

回到最开始的场景，当某用户想将一个信息发送给一个团体时，例如产品部的的所有经理，他可以将这样一个访问控制结构（经理 AND 产品部）结合所包含的属性对明文进行加密。解密者只有同时拥有这两种属性的私钥时才可以解密获得明文信息。这样加密过程只需要进行一次，而密文的传输也可以以广播的形式传送出去，同时，与之前介绍的基于身份的广播加密相比，加密者不需要知道具体有哪些人满足这样的条件。

基于属性的加密方法与一般的基于身份的加密算法相比，使用了可以包含与或非，以及门限能力的表达式，使得密文可以被多个用户共享，同时提高了系统的效率。

在基于属性的加密方法给我们带了很多好处的同时，他也存在着几个方面的问题，首先就是如何提高表达式的表达能力，不同的方案具备的表达能力是不相同的。能表达的属性组合越多，系统的实用性更高。其次就是如何避免共谋攻击，当具有不同属性的用户共享密钥之后，要保证他们共享之前如果没有人可以解开这个密文

则合谋之后仍然没有办法解开密文。关于这一点可以将发放给每个人一组密钥绑定一个秘密信息，但这样也同时引入了密钥扩张的问题。再其次就是如何将基于属性的加密应用于更多的场景。本文将围绕以上几个问题进行研究，分析比较已有方案和应用，提出安全性、应用性更好的方案并给出研究结论和证明。

1.4 论文的组织结构

本文的章节结构安排如下：

第二章主要介绍了需要的一些数学知识，主要是针对近世代数的一些知识的介绍。之后简单介绍了密码学的一些重要的安全假设和安全模型，在章节最后还给出了基于属性加密的一些公共定义。

第三章先从模糊匹配的基于身份的加密方案谈起，整理比较了近年来的几个方案以及应用并且给出了多授权方的基于属性的加密方案以及基于属性的数字签名等相关研究。

第四章给出了一个可证安全的多授权方的基于属性的加密方案，并给出了对方案的分析和跟已有方案的比较，详细描述了方案的场景，定义，构造和证明等内容。

第五章将第四章给出的这个方案进行了扩展并应用于另一个私钥提取的场景。为了获得更好的安全性，之后我们又给出了一个改进的方案，并对方案的安全性，实用性和效率进行了分析和比较。

第六章对全文进行了总结，并提出了基于属性的加密算法中需要进一步研究的问题。

1.5 本章小结

本章首先介绍了信息安全应用的背景以及公钥密码学在信息安全中起到的作用。之后从公钥密码学的一个方向，基于身份的加密方案进一步提出了基于属性的加密算法。在最后的小节介绍了整篇文章的结构。

第二章 预备知识

2.1 数学运算

2.1.1 近世代数基础

定义 2.1(群)：设 G 是一个非空集合，若在 G 上定义一个二元运算“·”满足：

- 结合律：对任何的$a,b,c \in G$,有$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- 单位元：存在单位元 e 使得对于任何$a \in G$有$a \cdot e = e \cdot a = a$
- 逆元：对任何$a \epsilon G$，都有逆元a^{-1}使得$a^{-1} \cdot a = a \cdot a^{-1} = e$

定义 2.2（阶）：群 G 中的元素的个数叫做群的阶，用|G|表示。如果|G|是悠闲地，那么称 G 为有限群。

定义 2.3（阿贝尔群）：若对于任何$a,b,c \in G$,有$(a \cdot b) \cdot c = a \cdot (b \cdot c)$, 若 G 是有限的，那么称 G 为可换群。

定义 2.4（循环群）：若存在一个元素 g,使得对于任何$a \in G$都存在一个整数 i ∈ Z,满足$a = g^i$,则称 G 为一个循环群，其中，g 成为 G 的生成元。

2.1.2 双线性配对

设有一个 q 阶（q 为素数）加法循环群 G_1,P 为 G_1 的生成元。G_2 为一个相同素数 q 阶的乘法循环群。我们假定在 G_1 和 G_2 上的离散对数问题(DLP)是难的。双线性配对 e：$G_1 \times G_1 \rightarrow G_2$ 具有以下三个性质：

（1） 双线性：

$e(P_1+P_2,Q_1)=e(P_1,Q_1)e(P_2,Q_1)$

$e(P_1,Q_1+Q_2)=e(P_1,Q_1)e(P_1,Q_2)$

其中 P_1,P_2,Q_1,Q_2 均属于 G_1

（2）非退化性：存在 P，Q 属于 G_1 使得 $e(P,Q) \neq 1$

（3）可计算性：对所有的 P，Q 属于 G_1 存在一个高效的算法可以计算 $e(P,Q)$

2.1.3 拉格朗日插值定理

设 q 是一个素数 $f(x)$是一个 k 阶的多项式；设 $j_0,...j_k$ 是 Z_q 上的不同元素。设 $f_0=f_{j_0},...,f_k=f_{j_k}$ 利用拉格朗日插值定理，我们可以将多项式 $f(x)$表示城

$$f(x)\overset{\Delta}{=}\sum_{t=0}^{k}(f_t\cdot\lambda_t(x))$$

其中

$$\lambda_t(x)\overset{\Delta}{=}\prod_{0\le i\ne t\le k}\frac{j_i-x}{i_i-i_t},t=0,...,k$$

为拉格朗日系数。

2.2 安全假设与计算复杂性

2.2.1 安全假设

定义 2.5（离散对数问题）:令 G 表示一个 q 阶的群，g 是其生成元。离散对数问题即给定随机元素$y\in G$,求元素$x\in Z_p$满足 $y=g^x$。

定义 2.6（计算 Diffie-Hellman 问题 CDHP）: 令 G 表示一个 q 阶的群，g 是其生成元。计算 Diffie-Hellman 问题是给定三元组(g,g^a,g^b),计算 g^{ab}。

定义 2.7（判定 Diffie-Hellman 问题 DDHP）：令 G 表示一个 q 阶的群，g 是其生成元。判定 Diffie-Hellman 问题是给定三元组(g^a,g^b,g^c)判断 g^c 是否等于 g^{ab}。

定义 2.8（双线性 Diffie-Hellman 问题 BDH）：对于群 G_1,G_2，g 是 G_1 的生成元，e 为双线性配对运算，则 BDH 问题是给定（g,g^a,g^b,g^c）计算 $e(g,g)^{abc}$

定义 2.9（判定双线性 Diffie-Hellman 问题 DBDH）：对于群 G_1,G_2，g 是 G_1 的生成元，e 为双线性配对运算，给定（g,g^a,g^b,g^c,Z）判断等式 $e(g,g)^{abc}=Z$ 是否成立。

定义 2.10（判定 q 双线性 Diffie-Hellman 问题 q-BDHE）: 令 G 表示一个 q 阶的群，g 是其生成元。判定 q 双线性 Diffie-Hellman 问题是对于随机选取的$a,s\in Z_p$对于给定的参数

$$y=\left(g,g^a,\dots,g^{a^q},,g^{a^{q+2}},\dots,g^{a^{2q}},g^s\right),T$$

判断等式

$$T=e(g,g)^{a^{q+1}s}$$

是否成立

2.2.2 计算复杂性

定义 2.11（函数平凡上界）：对于两个函数 *f(x)*和 *g(x)*,若存在一个常数 c 和一个正整数 x_c 满足对于所有的 $x>x_c$ 都有$0 \le f(x) \le c \cdot g(x)$则 *f(x)*是个 *g(x)*的一个平凡上界，即$f(l) = O(g(l))$。

定义 2.12（可忽略函数）：对于任意的多项式 *p(x)*，总存在一个自然数 *N* 使对于所有的 *x>N* 都有$f(x) < \frac{1}{p(x)}$则称 *f(x)*为可忽略函数。反之，则称 *f(x)*为不可忽略函数

定义 2.13（多项式时间算法）：若一个算法的运行最差时间是 $O(l^c)$，其中 *l* 是输入的规模，*c* 是一个常数，则称此算法为多项式算法。反之，则称其为一个非多项式时间的算法。

2.3 可证安全模型

2.3.1 可证安全基本定义

定义 2.14(哈希函数)：哈希函数通常为一个确定的函数，它将任意长度的比特串映射到固定长度的比特串。对于哈希函数 $H:\{0.1\}^* \rightarrow \{0,1\}^n$,即将任意长度映射到 *n* 长度的比特串，它需要满足以下的安全性质：

- 散列性：对于任意的输入 *x*，输出地哈希值 *H(x)*应当在区间$[0,2^n]$中均匀分布的二进制窜在计算上不可区分。
- 单向性：已知一个哈希值 *h*,找出一个输出串 *x* 使得 *H(x)=h*,在计算上是不可行的。
- 有效性：给定一个输入串 *x*，哈希值 *H(x)*的计算可以在关于 *x* 的长度规模的多项式时间内完成。
- 抗强碰撞性：找出两个不同的输入 *x* 和 *y*,使得 *H(x)=H(y)*，在计算上是不可进行的。
- 抗弱碰撞性：给定一个输入 *x*，找出两一个不同的输入 *y*，使得 *H(x)=H(y)* 在计算上是不可行的。

常用的哈希函数有 MD5[35],SHA[36]等。

定义 2.15(随机预言机及模型)：对于哈希函数 H:{0,1}*→{0,1}^{n},如果满足均匀性，确定性和有效性，则称这个哈希函数为随机预言机。利用随机预言机进行密码体制安全证明的方法被称为随机语言模型。

随机预言机模型用于证明密码体制的安全时，往往被作为一个随机函数使用。在体制开始设计的时候，系统中的各个角色共享随机预言机，并利用随机预言机完成设定和初始操作。对于随机预言模型下证明安全的函数，我们则认为在现实中可以使用较安全的哈希函数代替随机预言机。

定义 2.16(标准模型)：标准模型是相对于随机语言模型而言，不需要使用随机预言机假设的安全模型。

与随机预言模型相比，标准模型不能借助随机数生成机制来产生一些假设。在描述安全证明时，模拟者需要模拟一切真实的环境，包括现实中的哈希函数的使用。使得欺骗攻击者对模拟的环境进行攻击操作。在密码体系安全证明的过程中，最后我们总是将其归约到一个假设难的问题上去，如 BDH，CDH 问题等等。如果攻击者对模拟的环境可以进行成功的攻击，则可以以不可忽略的概率解决或判定这些难的问题，这与密码学的基本假设是矛盾的，从而使密码体系的安全得到证明。

2.3.2 可证安全模型

定义 2.17（公钥加密方案），一个公钥加密方案一般由以下四个算法组成。

- 系统初始化(Setup)：这是一个概率算法，以一个安全参数作为输入，一般是以 1^{k} 的形势输入，k 是与安全的强度规模相关。输出系统的系统公钥和公共参数 PK。
- 密钥抽取（KeyGen）：这是一个概率算法，输入为系统公钥和公共参数 PK,输出为一组公私密钥对，我们经常用 pk,sk 分别代表公钥和私钥。
- 加密（Enc）：加密算法同样为一个概率算法，输入为一个消息 m,系统公共参数 PK，某个接收者的公钥 pk,输出为密文 CT。
- 解密(Dec)：解密为一个确定性算法，输入为密文 CT 用户私钥 sk 输出为明文 m 或者终止符⊥。

定义 2.18(选择明文攻击安全 IND-CPA)。对于挑战者 C 和攻击者 A 之间的一个游戏包含以下几个部分

- 系统建立阶段：挑战者 C 选择一个安全参数 k，运行系统初始化算法(Setup)和密钥抽取(KeyGen)算法，并想攻击者 A 提供生成的系统公钥及公共参数

PK 以及公钥 *pk*。但对于私钥 *sk*，挑战者并不向攻击者 A 提供而是自行保留。

- 挑战：攻击者 A 向挑战者提供两个长度相等的信息 m_0,m_1,挑战者 C 随机选取其中一个设为 m_t 并生成挑战密文 $C'=Enc(pk,m_t)$。并将挑战密文交与挑战者。
- 输出，如果攻击者 A 对于 m_t 给出一个猜测 $t'=t$ 或者 $t'\neq t$。如果攻击者 A 给出了正确的猜测则我们称攻击者赢得了游戏。

对于这样的一个游戏我们称之为选择明文攻击(IND-CPA)游戏，对于攻击者赢得游戏的概率我们定义为：

$$Adv_A(k) = |Pr[t' = t] - \frac{1}{2}|$$

如果对于任何的 IND-CAP 攻击者，在这个游戏中的赢得游戏的概率都是可以忽略的（定义 2.6）,我们称这个 PKE 方案是 IND-CPA 安全的。

定义 2.19（选择密文攻击 IND-CCA）。对于挑战者 C 和攻击者 A 之间的一个游戏包含以下几个部分

- 系统建立阶段：挑战者 C 选择一个安全参数 k，运行系统初始化算法(Setup)和密钥抽取(KeyGen)算法，并想攻击者 A 提供生成的系统公钥及公共参数 *PK* 以及公钥 *pk*。但对于私钥 *sk*，挑战者并不向攻击者 A 提供而是自行保留。
- 挑战前查讯阶段：攻击者 A 可以一次或者多次的向挑战者 C 提出解密查询，挑战者 C 利用私钥 *sk*，将查询密文 CT_i 对应的明文 m_i 提供给攻击者。
- 挑战：攻击者 A 向挑战者提供两个长度相等的信息 m_0,m_1,挑战者 C 随机选取其中一个设为 m_t 并生成挑战密文 $C'=Enc(pk,m_t)$。并将挑战密文交与挑战者。
- 挑战后查询阶段：同挑战前查询阶段，但攻击者不可以询问被挑战的密文。
- 输出：如果攻击者 A 对于 m_t 给出一个猜测 *t=0* 或者 *t=1*。如果攻击者 A 给出了正确的猜测则我们称攻击者赢得了游戏。

如果对于任何的 IND-CCP 攻击者，在这个游戏中的赢得游戏的概率都是可以忽略的（定义 2.6）,我们称这个 PKE 方案是 IND-CCA 安全的。

2.4 基于属性加密算法的相关定义

定义 2.20(门限，Threshold)：一个门限是一个逻辑运算单元，它具有一个阀值 *K* 和 *num* 个输入($K \leq num$)，每一个输入只有 1/0 两种状态。当状态为 1 的输入数大于等于 *K* 时，门限将输出 1，否则则输出 0。对于特殊的门限，例如 *K=1* 则是对应的或门（OR Gate），当 *K=num* 时则是对应于与门(AND Gate)。示例如图 2.1 图 2.2，图 2.3 所示。

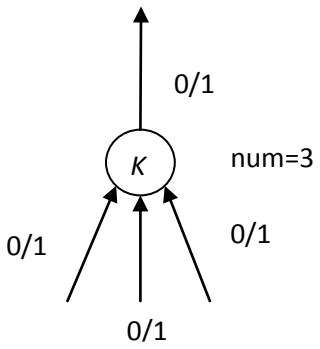

图 2.1 输入为 3 的门限

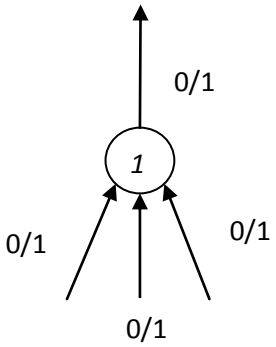

图 2.2 输入为 3 的与门

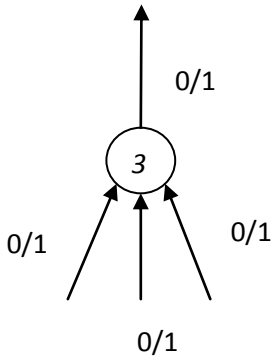

图 2.3 输入为 3 的或门

定义 2.21(访问树，Access Tree)：访问树用于表达一个控制访问结构。每一个树的非叶子结点都是一个门限，而叶子结点则与某属性绑定。对于叶子结点 *x*,函数 *att(x)*则返回叶子结点相对应的属性。对于任意节点 *x*,函数 *index(x)*则返回该节点的索引。如图 2.4 所示

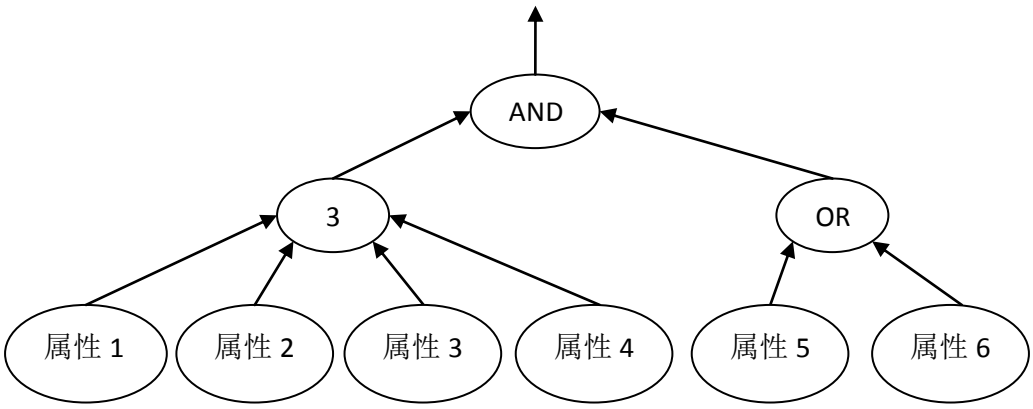

图 2.4 访问控制树

定义 2.22(线性秘密分享方案，Linear Secret-Sharing schemes): 如果对于一个集合 *P*,集合中的每一个元素所获得的分享部分可以形成一个 Z_p 上的向量。存在一个 *l* 行 *n* 列的分享生成矩阵 *M*,使得对于所有的 *i=1,...,l*,矩阵 *M* 的第 *i* 行代表集合中的一个元素，并且我们可以通过函数$\rho(i)$找到对应的元素。对于这样一个向量

$v=(s,r_2,\ldots,r_n)$,其中 s 是一个 Z_p 上的需要被分享的秘密，$r_2,\ldots,r_n$ 都是在 Z_p 上随机选取的。则 Mv 得到的向量是这 l 个元素所分享的信息，其中$(MV)_i$属于元素$\rho(i)$。

由文章[9]可知元素分享的信息具有秘密恢复的属性，即对于某个集合 S 是由矩阵 M 决定的可以恢复出秘密的集合。则对于$I \subset \{1,2,\ldots,l\}, I = \{i:\rho(i) \in S\}$存在这样的常量集合$\{\omega_i \epsilon Z_p\}_{i\in I}$使得对于秘密 s 的有效分享λ_i信息有

$$\sum_{i\in I} \omega_i \lambda_i = s$$

这些常量的集合可以根据矩阵 M 在多项式的时间内获得。

2.5 本章小结

本章主要介绍了公钥密码学属性加密相关的一些预备知识，首先介绍一些数学的定义和运算，大部分公钥密码学的运算都是基于抽象代数的。之后我们又分别介绍了安全假设和可证安全模型以及安全属性的证明方式。在最后一节给出了关于基于属性的一些相关定义。

第三章 基于属性的加密算法及应用

3.1 模糊匹配的基于身份(Fuzzy IBE)的加密方案

模糊匹配的基于属性的加密方案[3]由 Amit Sahai 和 Brent Waters 于 2005 年发表于欧洲密码学会议。在这篇文章中结合实际的解释了属性的概念。并通过给出的方案进一步的引伸出基于生物属性的模糊匹配的应用场景。

这篇论文基于的场景可以描述如下，首先系统通过一个密钥抽取算法对一个集合的属性（设为ω'）生成对应的公私钥对，之后对明文 M 进行加密。当解密者拥有的属性私钥集合ω满足ω和ω'的交集的大小大于某个系统设定值 d 则，解密者可以解密获得明文。

简要的协议描述如下:

- 基本定义：设 G_1 是一个以素数 p 为阶的双线性群，g 是其生成元，$e: G_1 \times G_1 \to G_2$为一个双线性配对运算。

$$\Delta_{i,S}(X) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$$

  为拉格朗日参数，S 是一个在Z_p的集合。所有的属性集合为 U,而所有属性都与Z_p^*中的元素关联。

- 初始设置：对于一个集合的属性，为其随机选择Z_p上的t_i作为属性的私钥，并公布属性对应的公钥为

$$\{T_1 = g^{t_1}, \cdots, T_{|U|} = g^{t_{|U|}}\}$$

  而系统的公钥为$Y = e(g,g)^y$，系统的管理密钥为$\{t_1, \cdots, t_{|U|}\}, y$。

- 密钥抽取：对于一组属性集合$\omega \subseteq U$,随机选择一个 *d-1* 维的多项式 *q(x)*使得 *q(0)=y*。这样对于用户的私钥 D_i, $i \in \omega$对应于 T_i有$D_i = g^{\frac{q(i)}{t_i}}$。

  - 加密算法：对于集合ω'和明文$M \in G_2$选择随机值 *s*,加密后的结果为

$$E = (\omega', E' = MY^s, \{E_i = T_i^s\}_{i \in \omega'})。$$

- 解密算法：对于集合ω如果$|\omega \cap \omega'| \geq d$则选则任意属于两个集合交集的 d 个元素，利用拉格朗日差值定理，可得

$$E' / \sum_{i \in S} (e(D_i, E_i))^{\Delta_{i,S}(0)} = M$$

模糊匹配的基于身份的加密算法为基于属性的加密算法提供了一个雏形，成功的将刻画身份的 ID 分解成为了例如性别，年龄，工作单位的集合。并提出，对基于生物特征，如血型，基因而抽取相应的属性密钥对身份的访问控制和认证的方式和设想，为基于属性的加密算法的发展奠定了基础。

3.2 近年来的基于属性的加密方案

从模糊匹配的基于身份的加密算法开始，基于属性的密钥引起了越来越多人的重视，首先由 VGoyal 等人于 CCS06[4]的会议上提出了一个有控制结构的基于属性的加密方案，同时将基于属性的加密算法进行了划分，分为密文政策的属性基加密算法（CPABE）和密钥政策的属性基加密算法（KPABE）,并对这两种基于属性的加密方法进行了比较和分析，并指出[4]作者提出的是一个密钥政策的属性基加密。之后 Cheung,L 等人通过给出固定大小的访问控制表达树在 CCS07[5]上给出了一个密文政策的属性基加密方案，同时对于控制结构的表达能力进行了改善。在改善的同时也引入了一些新的问题，比如密钥扩张和可证安全的问题。围绕这些问题，V Goyal[6]等人，R Ostrovsky[7]等人以及 Brent Waters[8]等人都做出了一些让人瞩目的贡献。本节以 Vipul[4]等人和 Waters[8]的方案为例对基于属性的密码进行描述，在最后会对这些协议进行一个全面的总结和分析。

3.2.1 V Goyal 等人的 Fined-Gained KPABE 方案[4]

在这篇文章的方案中，作者提出了表达能力更强的控制结构（Access structure）。通过一种树状的结构，可以提供包括与（AND）或(OR)以及门限（Threshold）的操作。这些操作大大增强了加密系统中对访问控制能力控制的灵活性。

这篇文章的另一个突出贡献就是提出了对基于属性的加密算法的一种划分，即密文政策和密钥政策。密文政策是指加密系统中，密文对应于一个访问结构而密钥对应一个属性集合，解密者当且仅当拥有的属性集合中的属性能够满足此访问结构才可获得明文。这种设计可以较好的应用与现实的场景，即加密者可以自由的选择对属性的控制，而解密者只经过一次属性密钥分发的过程即可对他被授权解密的信息进行解密。而密钥政策就是指密钥对应于一个访问结构而密文对应于一个属性集合，解密者当且仅当拥有的属性集合中的属性能够满足此访问结构时才可解密。这

种场景比较适合增加新用户或新增加用户访问权限对特定的静态的数据的访问。我们可以将属性集合和密文存储在一个服务器上，新增加的用户或新增加用户权限时，只需要针对对应的属性进行分发即可。

这篇文章设计的协议是上述划分中的密钥政策的基于属性的加密方案。

- 基本定义：访问树（Access Tree 参见定义 2.21)；门限(threshold gate 参见定义 2.20); 设 G_1 是一个以素数 p 为阶的双线性群，g 是其生成元，$e: G_1 \times G_1 \to G_2$为一个双线性配对运算。

$$\Delta_{i,S}(X) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$$

为拉格朗日参数，S 是一个在Z_p的集合。所有的属性集合为 U,而所有属性都与Z_p^*中的元素关联。

- 初始设置：对于一个集合的属性，为其随机选择Z_p上的t_i作为属性的私钥，并公布属性对应的公钥为

$$\{T_1 = g^{t_1}, \cdots, T_{|U|} = g^{t_{|U|}}\}$$

而系统的公钥为$Y = e(g,g)^y$，系统的管理密钥为$\{t_1, \cdots, t_{|U|}\}, y$。

- 加密算法：对于集合ω'和明文$M \in G_2$选择随机值 s,加密后的结果为

$$E = (\omega', E' = MY^s, \{E_i = T_i^s\}_{i \epsilon \omega'})$$

- 密钥抽取：对于每一个访问树中的非叶子节点 x,选择一个多项式 $q(x)$,使得它的度为这个节点的阀值少一，即$d_x = k_x - 1$；对于根节点 r 则选择 $q_r(0)=y$，而对于其它非叶子结点，使得 $q_x(0)=q_{parent}(index(x))$;针对于叶子结点的抽取的密钥为

$$K_x = g^{\frac{q_x(0)}{t_i}}, i = att(x)$$

- 解密算法：对于所有的用户拥有的属性对应的叶子叶结点计算

$$D_x = e(k_x, E_i) = e(g,g)^{s \cdot q_x(0)}$$

对于非叶子结点利用它的子节点的返回值，由下至上的进行递归运算，

$$F_x = \sum_{z \in S_x} F_z^{\Delta_{i,S_x'}(0)} = e(g,g)^{s \cdot q_x(0)}$$

其中 $i=index(z), S'_x=\{index(z): z \in S_x\}$。最后可以通过拉格朗日差值定理得到$e(g,g)^{sy}$,故$M = E'/e(g,g)^{sy}$。

3.2.2 Brent Waters 的 CPABE 方案

在这篇文章的方案中，作者提出了一个标准模型下可证安全的 CPABE 方案，并且将对控制结构的描述提出了一种新的方式，通过利用线性秘密分享的方案(LSSS)来决定哪些子集属于授权集合哪些属性的集合不是授权集合。基于这种方案的属性基的加密打破了原来众多方案只能使用拉格朗日差值定理进行构造的模式，无论在表述能力上还是安全证明上都有很大的贡献。

- 基本定义：对于一个属性的集合，如果它满足了对应的控制结构，我们则称其为一个授权集；对于所有的授权集所组成的集合我们称之为授权集集合，同时也代表了这一类属性基加密算法的控制结构，我们定义为Γ。对于线性分享方案 LSSS（定义 2.21），对于授权集合中的元素即对应于属性，每一个矩阵 M 对应于这些授权集集合Γ。即对于授权集合中的元素，可以通过他们的分享恢复出秘密。
- 初始设置：G_1 是一个以素数 p 为阶的双线性群，g 是其生成元，$e: G_1 \times G_1 \to G_2$为一个双线性配对运算。随机的我们可以在 Z_p 上选取 a 和α。选择哈希函数$H: \{0，1\}^* \to G_1$。
- 加密算法：对于明文 m 选择随机向量 $v=(s,r_2,\ldots,r_n)$,则$\lambda_i = v \cdot M_i$,密文为

$$CT = (C = me(g,g)^{\alpha s}, C' = g^s, C_1 = g^{a\lambda_1} H\big(\rho(1)\big)^{-s}, \ldots, C_l = g^{a\lambda_l} H(\rho(l))^{-s}$$

- 密钥抽取：对于某一属性的集合 S，在 Z_p 上随机选取 t，则密钥为

$$K = (K_0 = g^{\alpha} g^{at}, L = g^t, \{K_x = H(x)^t\}_{x \in S})。$$

- 解密算法：对于密文 CT 和线性分享的结构对应的矩阵(M,ρ),满足控制访问结构的属性集合 S 对应的密钥 K，以及线性密钥分享方案对应的常量集合 $\{\omega_i\}$，则解密的运算首先计算

$$e(C', K_0)/(\prod_{i \in I}(e(C_i, L)e(D_i, K_{\rho(i)}))^{\omega_i} = e(g,g)^{\alpha s}。$$

之后可以从 C 中分离出明文 m。

3.2.3 现有方案的比较及综述

本节前面几个部分重点介绍了两种基于属性的加密算法。先对这些协议进行一个综合的评价。

表 3-1 现有属性基加密算法的总结与比较

协议	贡献	效率分析	安全证明	不足
V Goyal [4]	• KPABE 方案 • 提出了 CPABE 和 KPABE 的划分 • 提出了访问控制树的概念 • 提供了门限作为逻辑单元的表达能力	加密：1 次双线性运算 解密：访问控制数的节点个数次双线性运算	选择模型，IND-CPA; 基于 BDH 假设	安全证明基于的模型不够强。 在 Chase[10]的方案中给出了对此方案共谋攻击的方式。
Chueng L[5]	• CPABE 方案 • 引入了非属性的概念 • 安全模型较强	加密：0 次双线性运算 解密：属性空间维度次双线性运算。	非适应性 IND-CPA。选择身份模型	密钥的空间与属性空间相比扩展了三倍
V Goyal[6]	• CPABE 方案 • 属性可以一对多的映射与访问控制树中的结点。	加密：0 次双线性运算 解密：属性空间维度次双线性运算。	非适应性 IND-CPA 选择树模型	树的大小受到限制，每次解密都需要对全部属性解密。
R Ostrovsky, B Waters[10]	• KPABE 方案 • 非单调的访问控制结构 • 提供非属性	加密：0 次双线性运算 解密：每个属性需要 2 或者 3 次的双线性运算，	基于 BDH 问题的选择集合模型。非适应性的 IND-CAP	解密效率较低
B Waters[8]	• CPABE 方案 • 安全模型强 • 利用 LSSS 方案中的矩阵描述访问结构	加密：0 次双线性运算 解密：需要参与用算的属性的个数次双线新配对运算	基于 BDH 问题的选择身份模型，非适应性的 IND-CPA	非属性的扩展较困难

由表 3-1 可以看出，近年来的研究主要是围绕着以下几个问题开展。首先就是更强的表达能力，从文章[4]引入树形的访问控制结构，到文章[5]中扩展到了访问控制结构中包含非门的属性，再到之后的非单调的属性结构以及利用 LSSS 协议刻画的控制结构，基于属性的加密算法的表达能力在不同的方面有着不同的改进。其次就是协议的安全模型证明，上述的安全证明也在基于不同假设和不同模型下力争给出更安全实用的安全证明。效率问题也是非常重要的一个方面，尽管目前为止对此关注的较少，但由于基于属性加密的算法的解密通常需要多次的双线性配对运算，故在目前的实际应用中基于属性的加密效率还是相对低的，所以改进解密时的配对运算次数对于基于属性的加密算法的应用也有很大的意义。

3.3 多授权方的基于属性加密方案

3.3.1 基本场景介绍

多授权方的基于属性的加密方案最先由 Chase 于文章[10]提出。所谓多授权方的基于属性的加密是指用户的属性私钥不再由唯一的中心授权方授权，而是由各个不同的授权方分别发送。这一改进在现实中是有很大积极意义的。考虑这样一个场景，学校作为一个授权方可能会发给用户一些属性，例如，年级，学号，专业，班级，三好学生等等。但是某个游泳俱乐部可能发给这个用户的属性为，俱乐部 ID,加入时间，俱乐部成员有效期，俱乐部金卡会员。对于这样的一些系统我们可以分别建立两个基于属性的加密方案。但如果可以更多的组织集合起来使用一个加密系统，无论是对于效率，安全性还是建立成本都是有很大意义的。但就如此例所示，如果由一个中心可以对所有属性进行授权将是十分不安全的。无论是将游泳俱乐部的授权给学校还是将学校的授权给俱乐部都是不切实际的。Chase 的方案对于基于属性的加密方案有了很大的促进意义，之后很多人也围绕这方面展开研究。在此将 Chase 的方案简单整理如下：

3.3.2 Chase 的开创性方案

- 基本定义：设 G_1 是一个以素数 p 为阶的双线性群，g 是其生成元，$e: G_1 \times G_1 \rightarrow G_2$ 为一个双线性配对运算。对于所有的用户，他们在拥有属性的同时还拥有一个统一的身份区分信息，*GID*。
- 初始设置：随机选择 $y_1, y_2, \ldots, y_k$ 作为 k 个授权方的私钥，使得

$$y_0 = \sum_{k=1}^{K} y_k$$

系统的公共密钥为 $Y=e(g,g)^{y_0}$

- 授权方密钥抽取：授权方 k 随机生成其拥有授权权限的属性基 A_k 对应的属性私钥集$\{t_{k,i}\}$并且公布所有的属性公钥$\{T_{k,i}=g^{t_{k,i}}\}$。
- 用户属性私钥抽取:授权方对用于用户 u 随机选择一个指数为 d_k-1 的多项式 p 使得 $p(0)=y_k$。则该授权方授权给用户的属性私钥集为

$$\{D_{k,i} = g^{\frac{p(i)}{t_{k,i}}}\}_{i\in A_k}$$

- 加密方法：对于属性集合ω'和明文$M \in G_2$选择随机值 s,加密后的结果为

$$E = (\omega', E' = MY_0{}^s, \{E_{k,i} = T_{k,i}^s\}_{i\epsilon\omega'})。$$

- 解密方法：对于每一个授权方 k，用户选择加密信息中使用的该授权方的属性交集中的 d_k 个并通过拉格朗日插值定理得到$Y_k^s = e(g,g)^{p(0)s} = e(g,g)^{y_k^s}$, 将每一个授权方的密钥进行组合可以得到$\prod_{k=1}^{K} Y_k^s = Y_0^s$则可以获得明文 $m=E/Y_0^s$。

在 Chase 的方案中，Chase 应用了一个中心授权方，这个中心授权方为所有授权方产生每一方所控制的属性私钥。授权方根据掌握的属性授权方为用户生成用户的属性私钥。但是同时也带来一个问题，及中心授权方还是权力过大，可以为任何人生成本属于某一授权方的属性密钥。尽管 Chase 在文章 [10] 提出了一个改进方案，但由于效率较低，也并不实用。之后多授权方的基于属性的加密体制由于其应用背景也备受关注。

与单一授权方的基于属性的加密相比，除了效率，表达能力以及密钥空间扩张等问题，多授权方的基于属性的加密还需要考虑如何去掉可信中心或者中心授权方的问题，另外如何保证各授权方产生属性的算法独立而且不互相影响也是非常重要的。在此方面 Huang Lin[12]等人提出了以一种无中心授权方的多授权方，但存在的问题亦为引入过多的高时间复杂度的运算使得算法的效率很低。之后由 V Bozovic[13]等人又提出了一个具有所谓的"忠实却又好奇"（honest but curious）的可信中心的多授权方基于属性的加密算法。这个方案里提出的忠实却又好奇的可信中心是一种相对 Chase[10]方案中较弱的假设，即可信中心会按照自己的自责行事，例如生成密钥，分发密钥等等，但是可信中心也可能会想要对一些密文进行解密。这个方案的安全性是说明这样的中心是无法得到明文的，即可信中心的权利受限。但是这个方案也因引入了很大的密钥空间扩张以及安全模型不够强等问题需要更多的

改进和研究。Ibraimi[14]等人也提出了一个可代理的基于属性密钥，并提到了如何利用他们的方案扩展到多授权方的基于属性的加密算法。

3.3.3 已有多授权方的基于属性的加密算法的比较

对已有的多授权方的基于属性的加密算法进行一个简单的总结如表 3.2 所示：

表 3-2 现有多授权方的属性基加密算法的总结与比较

方案	贡献	不足
Chase[10]	• 提出了多授权方的基于属性加密的概念 • 每个授权中心可以自行生成属性私钥	• 所有人的身份用 GID 表示
Huang Lin[12]	• 不需要可信中心	• 运算效率低
V Bozovic[13]	• 定义了一个能力弱的可信中心，无能力参与解密 • 加密解密不需要所有的授权方参与	• 密钥空间扩张 • 使用 GID 表示身份
Ibraimi[14]	• 提出了基于属性加密的代理方案。 • 提供层次的多授权方的基于属性加密 • 用户密钥可以收回。	• 每份密钥有多个部分构成，分发复杂

3.4 基于属性的签名方案

3.4.1 基本应用场景描述

在基于属性的加密方案备受关注的同时，一些以基于属性加密思想为核心的技术与应用场景被设计出来并加以改进与研究。在这些方案中，有一定现实意义的是基于属性的签名和认证方案。近年来，基于属性的签名方案主要有 D Khader 的群上的签名方案[16][17]，J Li[19]等人的环上的签名方案，以及 H Maji[20]等人提出的方案。D Khader 还利用基于属性的签名构造了一个基于属性的认证算法[18]。

这些算法基本上都是基于这样一个共同的场景。当你需要一个签名或对某一类人进行认证时，往往我们并不要求签名方是固定的一个人，我们希望某一个能代表这一团体的某个人来签名，例如，我们希望从学生会出示一份证明，学生会主席的

签名当然是有效的，但是学生会副主席的签名也是能说明问题的，另外，工作两年以上的学生会成员的签名我们也认为是可信任的。对于这样的场景，我们可以利用基于属性的密码的思想，定义一个访问控制结构，签名人利用自己的属性按照这个控制访问结构进行签名，认证者可以容易的判断这个签名是否具有这样的属性。当然我们可以只用简单的对每一个属性进行认证的方法而不必附加所谓的控制访问结构，例如，同样是前面所述的场景，我们可以要求对方证明是学生会主席，或者是副主席，以及利用工作两年属性密钥和学生会成员属性密钥分别对其进行签名，这样似乎也可以达到我们场景所要达到的目的，但是相比之下，基于属性的签名应该还应该可以使验证者无法区分用户的签名到底来自那一种，从而隐藏签名者的身份而使得获得签名者依然可以得到认证。接下来我们将对较早的一个 D Khader[16]的一个方案进行一个简单的介绍，之后会给出一个对所有方案的比较。

3.4.2 D Khader 的基于属性的签名方案

- 基本定义：设 G_1,G_2 分别是一个以素数 p 为阶的双线性群，g_1，g_2 分别是其生成元，$e: G_1 \times G_2 \to G_T$为一个双线性配对运算。$S$ 是一个在Z_p的集合。所有的属性集合为 U,而所有属性都与Z_p^*中的元素关联。选择哈希函数 $H: \{0，1\}^* \to G_1$。选择$h \in G_1, e_1, e_2 \in Z_p$s,设定$gmsk = \{e_1,e_2\}$,设 u,v 为 G_1-中的元素，并使得

  $$u^{e_1} = v^{e_2} = h, \omega = g_2{}^{\gamma}$$

  其中γ，ω作为系统私钥保留，其它参数公布。
- 属性密钥抽取：对于每一个属性，随机选择 $t_i, i \in U$作为属性的私钥，并计算g^{t_i}作为属性的公钥。
- 根据访问控制结构生成验证公钥：对于访问控制结构上的每一个节点，设其阈值为 k，选择一个度为 $k-1$ 的多项式 $q(x)$,使得 $q_{root}(0)=\gamma$。$Q_{node}(0)= q_{parent}(index(node))$;公布关于此访问结构的验证公钥为：

  $$gpk = \{D_{leaf_i} = g_2^{\frac{q_{leafi}(0)}{t_{leafi}}}, h_j = h^{t_j}\}$$

- 签名者私钥抽取：对未签名者 j 随机选择 Z_p 上的值 x_j 就属性 i 生成对应的签名私钥为：

  $$T_{i,j} = g_1{}^{x_j/(\gamma + t_i)}$$

- 签名算法：随机在 Z_p 选择α, β, rnd并计算

$$C_1=u^{\alpha}, C_2 = v^{\beta}, C_3 = A_i h^{\alpha+\beta}, CT_j = (T_{i,j}\, {h_j}^{\alpha+\beta})^{rnd}$$

设$\delta_1 = t_i\alpha, \delta_2 = t_i\beta$。继续在 Z_p 上随机选取$r_\alpha, r_\beta, r_x, r_{\delta_1}, r_{\delta_2}$并计算

$$\mathrm{R_1 = u^{r_\alpha}, R_2 = v^{r_\beta}, R_3 = e(C_3, g_2)^{r_x} e(h, \omega)^{-r_\alpha - r_\beta}}$$

$$\mathrm{R_4 = {C_1}^{r_x} u^{-r_{\delta_1}}, R_5 = {C_2}^{r_x} v^{-r_{\delta_2}}}$$

令 c=H(M,C_1,C_2,C_3,R_1,R_2,R_3,R_4,R_5)。计算辅值：

$$\mathrm{s_\alpha = (r_\alpha + c\alpha), s_\beta = (r_\beta + c\beta), s_x = (r_x + cx)}$$

$$\mathrm{s_{r_{\delta_1}} = \left(r_{r_{\delta_1}} + c r_{\delta_1}\right),\ s_{r_{\delta_2}} = \left(r_{r_{\delta_2}} + c r_{\delta_2}\right)}$$

则最后的签名为

$$\mathrm{\sigma = \{C_1, C_2, C_3, c, CT_1, CT_\gamma, s_\alpha, s_\beta, s_x, s_{r_{\delta_1}}, s_{r_{\delta_2}}\}}$$

- 验证算法：当签名属性的集合满足访问控制结构的每一个节点时，我们计算

$$e\left(CT_{leftfj}, D_{leafj}\right), F_\rho = e\left(A_i h^{\alpha+\beta}, g_2^{rnd}\right)^{q_\sigma(0)}, {R'}_1 = u^{s_\alpha} {C_1}^{-c}, {R'}_2$$

$$= u^{s_\beta} {C_2}^{-c}, R'_3 = u^{s_\beta} {C_2}^{-c} R'_4 = u^{s_{r_{\delta_1}}} {C_2}^{-r_{\delta_1}} R'_5 = u^{s_{r_{\delta_1}}} {C_2}^{-r_{\delta_2}}$$

判断 c 是否等于 $H(M,C_1,C_2,C_3,R'_1,R'_2,R'_3,R'_4,R'_5)$。

3.4.3 已有的基于属性签名方案的比较

对已有的多的基于属性的签名方案进行一个简单的总结如表 3.3 所示：

表 3-3 现有多授权方的属性基加密算法的总结与比较

协议	贡献	效率分析	安全证明	不足
D Khader[16]	• 提出了基于属性签名方案的应用场景 • 提供了一个扩展函数	签名：属性规模成线性关系 $O(\|s\|)$次配对运算 验证：访问控制结构的门限个数 n 次配对运算	启发式证明	• 效率偏低 • 无强安全模型证明
D Khader[17]	• 增加了属性回收的机制	签名： $O(\|s\|)$次配对运算 验证： n 次配对运	启发式证明	• 效率与方案[16]相比稍有提高，但仍不实

		算		际 • 无强安全模型证明
J Li[19]	• 提出了多授权方的基于属性的签名方案	签名： *O(|s|)*次配对运算 验证： *n* 次配对运算	启发式证明	• 效率偏低 • 无强安全模型证明
D Khader[18]	• 授权方的基于属性的签名方案	签名： *O(|s|)*次配对运算 验证： *n* 次配对运算	启发式证明	• 效率偏低 • 无强安全模型证明
H Maji[20]	• 环中的用户互相拥有的属性与签名情况可以隐藏	签名： *6d* 次配对运算 验证： *6d* 次配对运算	一般的全模型启发式证明	• 效率偏低 • 无强安全模型证明

从表中我们可以看出，在目前的基于属性的签名方案仍存在着以下几个问题使得基于属性的签名的研究没有非常大的突破，第一就是效率的问题，如果签名和认证的方案都是以与属性集合的规模呈线性关系次数的配对运算为代价的，这将使协议的应用性大打折扣。第二就是单一的访问控制结构问题，在基于属性的加密方案中，我们已经可以看到越来越多的表达能力强的访问控制结构被提出并给予完善的证明。目前的基于属性的签名方案还是大多基于最开始的 Vopul[10]给出的访问控制结构树的形式进行构造。第三就是目前这些协议都还没有一个好的安全模型的证明，所以在实际应用中，无法对安全的程度进行保证。

3.5 基于属性加密算法相关的其它研究

其他的与基于属性的加密算法相关的研究也无非利用基于属性加密算法的特点进行一些安全相关的研究，或者就是对现有基于属性加密算法的一些能力的扩充，

如验证，代理，回收等等。其中包括由 T qiang[40]提出的可验证的属性基加密和 Chueng L[41]等人提出的抗共谋攻击的用于群密钥控制的基于属性的加密。

3.6 本章小结

本章主要了总结了基于属性的加密算法以及相关一些领域。首先介绍了基于属性的加密算法的引入 Fuzzy IBE 以及几个典型的基于属性的加密算法。之后介绍了多授权方的基于属性的加密算法。最后简单了介绍了基于属性的数字签名算法以及一些简单的应用。

第四章 一个基于属性的多授权方加密方案

在第三章我们已经比较了几种现有的基于属性的多授权方加密方案，并介绍了多授权方加密方案的思想和一些方案。介于多授权方基于属性加密的方案比一般的方案有更加广泛的应用背景，在本章中我们将提出一个新的方案。这个方案的控制访问结构继承了 Waters[8]的方案，与已有的多授权方基于属性的加密方案相比在安全，效率和实际应用等几个方面都有了很好的改进。

4.1 一个基于属性的多授权方加密方案内容描述

4.1.1 方案参与者描述

在我们系统中主要有 *n* 个用户，*t* 个授权方，和 *1* 个可信第三方三个方面组成。每一个授权方控制一个集合的属性密钥的颁发。可信第三方负责生成系统参数，并为每一个用户生成一个密钥。我们的方案继承了 chase[10]方案中的一些定义，每一个用户可以从授权方的到属性密钥，而本身同样有一个 *GID* 作为身份的区分。可信第三方为用户生成的密钥也是基于 *GID* 的。

4.1.2 方案函数描述

方案中主要包括以下几个函数：

- 建立函数：由可信第三方运行，输入为系统安全参数 1^k,输出为系统公钥和每一个用户的私钥。
- 授权方属性密钥生成函数：由每个授权方运行，输入参数为系统公钥和特定属性，输出为属性的公私钥对。
- 用户属性密钥生成函数：由每个授权方运行，输入参数为系统公钥，属性私钥，属性和用户统一身份 *GID*，输出为颁发给用户的特定属性的密钥。
- 加密函数：由加密用户运行，输入参数为属性的访问控制结构，系统公钥，明文。输出为密文。
- 解密函数：由解密用户运行，输入参数为用户拥有的属性密钥集合，系统公钥，用户私钥，和密文；输出为明文。

4.1.3 方案定义和场景描述

属性的全集定义为 U，每个授权方在系统的建立期被指定可以对一个集合的属性进行授权，每个授权方所能授权的属性集合互不相交，可信第三方运行建立函数并公布系统密钥 PK，之后为每一个用户生成对应于 GID 的用户私钥 Key_{GID} 并分发给用户。授权方运行授权方属性密钥生成函数产生该授权方所被指定授权的属性集合 I 的公私钥对$\{(PK_i,SK_i)\}$并把属性的公钥信息通过公开信道公布出去。之后用户 u 可以向不同的授权方申请不同属性的密钥，授权方进认定后同意对用户 u 授权属性 i 的密钥时运行用户属性密钥生成函数并将密钥颁发给用户。加密者根据访问控制结构Γ生成 LSSS[9]方案对应的矩阵 M，运行加密函数并对需要加密的明文 m 进行加密生成密文 CT。解密者当且仅当拥有满足控制访问结构的属性密钥时才可以在运行解密函数后获得明文 m。

4.1.4 方案的构造描述

- 建立函数：该函数首先选择一个双线性群，G_1 是一个以素数 p 为阶的双线性群，g 是其生成元，$e: G_1 \times G_1 \to G_2$ 为一个双线性配对运算。在 Z_p 上随机选择α, a,并选择作为随机预言机的哈希函数$H(x): \{0,1\}^* \to G_1$，算法产生的系统公共密钥为

$$PK = (g, e(g,g)^{\alpha}, g^{a}, H, e, G_1, G_2)$$

  之后为每个用户根据用户的 GID 生成用户私钥

$$Key_{GID} = g^{\alpha} H(GID)^{a}$$

- 授权方属性密钥生成函数：授权方从 Z_p 中随机选取 t_i 作为属性 i 的私钥。并且计算该属性的公钥$PK_i = g^{t_i}$，并且将该属性通过公开信道发布出去。在此我们对于属性 i 定义它的公私钥对为（SK_i，PK_i）。
- 用户属性密钥生成函数：对于用户 GID 和目标属性 i,用户的该属性密钥对应为

$$Key_{GID,i} = H(GID)^{t_i}$$

- 加密函数：设Γ为对应于 LSSS 协议的访问控制结构(M, ρ)。这里的函数ρ将矩阵 M 中的行与属性相关联。并且函数ρ为到内映射。设 M 的行为 l,列数为 n。该算法首先选择一个随机的向量 $v=(s,y_2,\ldots,y_n)$。对于 j 从 1 开始到 l 计算$\lambda_i = v \cdot M_i$，其中 M_i 是指矩阵 M 的第 i 行。对于明文 m 则密文为

$$CT_{\Gamma,m} = (C = m \cdot e(g,g)^{\alpha s}, C' = g^s, C_1 = g^{a\lambda_1} g^{-t_1 s}, \ldots, C_l = g^{a\lambda_l} g^{-t_l s})$$

其中$g^{-t_1 s}$的计算可以由$(PK_i)^{-s}$得到

- 解密函数：设属性集合$\mathcal{A}$满足控制结构Γ，并且有集合$I = \{i: \rho(i) \in \mathcal{A}\} = \{1,2,\ldots,l\}$。对应于 LSSS 协议，我们可以知道在多项式时间内找到常量的集合$\{\omega_i | i \in I\}$使得$\sum_{i\in I} \lambda_i \omega_i = s$。则解密算法计算

$$\frac{e(C', Key_{GID})}{\prod_{i\in I}(e(C_i, H(GID))e(Key_{GID,i}, C'))^{\omega_i}}$$

$$= \frac{e(g^s, g^{\alpha} H(GID)^a)}{\prod_{i\in I}(e(g^{a\lambda_i} g^{-t_i s}, H(GID))e(H(GID)^{t_i}, g^s))^{\omega_i}}$$

$$= \frac{e(g^s, g^{\alpha} H(GID)^a)}{\prod_{i\in I}(e(g, H(GID)))^{a\lambda_i \omega_i}}$$

$$= e(g,g)^{\alpha s}$$

之后算法通过计算

$$m = C / e(g,g)^{\alpha s}$$

获得明文。

4.2 一个基于属性的多授权方加密方案的效率和应用分析

我们给出的这个基于属性的多授权方加密方案，在加密的过程中不需要配对计算，所有的运算均限于群上的指数运算和加法运算。设参与加密的属性个数为 *l*，则共进行群的指数运算 *2l+1* 次，群的加法运算共 *l+1* 次。在解密的过程中，设参解密的属性个数为 *l'*则，配对计算公进行了 2*l'+1* 次，群上的指数运算共 *l* 次,群上的加法运算一次。与 Chase 的方案[10]相比，效率上有了很大的提高。

其次在安全模型上我们将给出一个基于标准模型的方案，这与已有的协议相比都有很大的改进。目前的很多多授权方的属性加密算法所基于的安全模型都相对较弱，对于标准模型的方案更是难以构造。方案的具体证明我们将在下一节给出。

在基于属性的加密算法中，对于属性的防控控制结构的表达能力也是为人们所关注的。在 Chase 的方案[10]中，仅能达到对每一个授权中心所控制的属性集合门限控制。其它的几个多授权方的基于属性的加密算法在表达能力上也很有限，只有 V Bozovic[13]的方案可以经过扩展，转化成为含有多个与门和或门的访问控制结构。而我们给出的方案中因为是利用 LSSS 的矩阵 *M* 来刻画访问控制结构，则此控制结构可以用集合的包含关系来刻画,其表达能力与 Waters[8]的方案相同。

我们的协议在实际应用上也有较大的优势。首先由于是密文政策的基于属性的加密，使得密钥不必针对密文的访问控制结构分发。只需要一次分发，之后用户不必每次针对不同的密文需要不存不同的密钥，针对不同的密文只需要利用可以满足访问控制结构的属性密钥集合就可以进行解密。在系统的运行过程中，每一个授权方可以独立的选择属性的私钥，这样当某一个授权方需要更改对某一属性的授权时，只需要选择不同的私钥并将对应的公钥重新发布，之后对授权用户新颁发相应的授权属性密钥即可。这样的应用场景非常广泛，例如会员的制度往往是有有效期的。每到新的一年，授权方可以更换一次会员这个属性的管理私钥，再向新一年的会员进行授权。

在我们的方案中虽然还是有一个可信的中心为每一个用户产生一个系统私钥，但由于每一个授权方的属性私钥是可以动态生成的，故如果对于一个静态的环境，我们可以在可信中心选择好系统参数后，为指定的一个大小的用户集合生成对应的系统私钥，之后由于本加密方案中之后不需要控制密钥参与加密解密的过程，所以可以将可信中心的运作停止，即在系统建立之后，使得可信中心不再参与系统的其它操作。这样的场景也是经常可以见到的，例如一个有用户上限的信息传递部门。

另外我们给出的这个多授权方的基于属性的加密，在构造上将哈希函数作为身份信息映射的工具与无论是属性密钥还是用户系统私钥相绑定，这样的构造有好的扩展性。只要将身份信息转换为其他一些认证信息，或者是其它一些认证信息的结合体，例如身份信息与时间标签的结合体，则我们可以应用于更多的场景。

4.3 一个基于属性的多授权方加密方案的安全性证明

4.3.1 一个基于属性的多授权方加密方案的安全模型

我们为基于属性的多授权方加密方案定义 IND-CCA 的安全模型如下：假设有这样一个游戏

- 系统建立阶段：挑战者 C 选择一个安全参数 k，运行系统初始化算法(Setup)和密钥抽取(KeyGen)算法，并想攻击者 A 提供生成的系统公钥及公共参数 PK 以及公钥Key_{GID}。
- 挑战前查讯阶段:对于攻击者 A，可以对每一个授权 i 方询问属性集合 $S_{i,1},\ldots,S_{i,q}$ 的属性私钥。
- 挑战阶段：攻击者 A 向挑战者提供两个长度相等的信息 m_0，m_1 并提供被挑战的访问控制结构Γ^*。我们要求这个访问控制结构Γ^*不满足之前攻击者

进行的所有询问。挑战者 C 随机选取其中一个设为 m_t 并生成挑战密文 C^*=Enc(Key_{GID},m_t)。并将挑战密文交与挑战者。

- 挑战后查讯阶段:对于攻击者 A，可以对每一个授权 i 方询问属性集合 $S_{i,1},\ldots,S_{i,q}$ 的属性私钥。但询问的属性集合不能满足访问控制结构Γ^*
- 输出：如果攻击者 A 对于 m_t 给出一个猜测 t=0 或者 t=1。如果攻击者 A 给出了正确的猜测则我们称攻击者赢得游戏的概率都是可以忽略的，

如果在这个游戏中我们定义攻击者赢得游戏的概率为

$$Adv_A(k) = |Pr[t' = t] - \frac{1}{2}|$$

如果次概率是多项式时间计算可以忽略的，则我们的方案是安全的。

4.3.2 一个基于属性的多授权方加密方案的安全证明

首先我们假设决定性的 q-BDHE 假设成立，那么则不存在一个攻击者可以选择性的破坏我们的系统。即$Adv_A(k)$是可以忽略的。挑战者 C 开始一个由上面定义的游戏，并按照如下的方式进行：

- 系统建立阶段：挑战者选择 q-BDHE 的参数

$$y = \left(g, g^s, g^a, \ldots, g^{a^q}, , g^{a^{q+2}}, \ldots, g^{a^{2q}}\right)$$

和猜测 T 并选择一个挑战的访问控制结构Γ=(M^*,ρ^*)。挑战者随机选择一个 α'并令$\alpha = \alpha' + a^{1+q}$这个选择在之后也会作为我们把问题规约到 q-BDHE 假设的一个构造。于是有

$$e(g,g)^{\alpha} = e\left(g^a, g^{a^q}\right)e(g,g)^{\alpha'}$$

对于攻击者的 GID，我们首先要为其生成系统私钥，$Key_{GID} = g^{\alpha}H(GID)^a$。首先选择一个向量$\omega = (\omega_1, \ldots, \omega_{n^*}) \in Z_p{}^n$，其中$\omega_1 = -1$并且使得攻击者可能获得的最大属性集 S 中的所有属性 i 有$\omega \cdot M_i = 0$。我们于是让挑战者选择一个随机数 r 并定义

$$H(GID) = g^{r+\omega_1 a^q + \omega_2 a^{q-1} + \cdots + \omega_n a}$$

于是

$$Key_{GID} = g^{\alpha'}H(GID)^a = g^{\alpha}H(GID)^a$$

在此将我们埋入的规约因子消除。

接下来我们为属性的授权方生成属性公私钥对。对于任意的属性 i 我们选择其私钥 t_i 如下：

$$SK_i = z_x + aM^*_{i,1} + a^2M^*_{i,2} + \cdots + a^{n^*}M^*_{i,n^*}$$

对应的属性的公钥为

$$PK_i = g^{z_x + aM^*_{i,1} + a^2M^*_{i,2} + \cdots + a^{n^*}M^*_{i,n^*}}$$

- 挑战前查讯阶段:对于攻击者提出的查询的属性，只要攻击者的查询不能满足当前挑战的访问控制结构，我们就将对应用户 *GID* 的属性私钥

$$Key_{GID,i} = H(GID)^{t_i}$$

颁发给攻击者。由于在系统建立阶段我们对于向量$\omega = (\omega_1, \ldots, \omega_{n^*}) \in Z_p^{\,n}$定义其$\omega \cdot M_i = 0$则在计算$H(GID)^{t_i}$的时候我们可以消掉对应的项$g^{a^{q+1}}$。这也是我们基于的假设所无法给出的项，只有这样我们才可以继续进行我们模拟游戏。于是有

$$Key_{GID,i} = (g^{r+\omega_1 a^{q-1}+\omega_2 a^{q-2}+\cdots+\omega_n})^{z_x + aM^*_{i,1} + a^2M^*_{i,2} + \cdots + a^{n^*}M^*_{i,n^*}}$$
$$= g^{z_x} \prod_{j=1\ldots n} (g^r \prod_{k=1,\ldots,n^*} (g^{a^{q+1+j-k}})^{\omega_k})^{M_{i,j}}$$

- 挑战阶段：攻击者 A 向挑战者提供两个长度相等的信息 *m0*，*m1* 并提供被挑战的访问控制结构Γ^*。对于

$$C = m \cdot \mathrm{e(g,g)}^{\alpha s} = \mathrm{m \cdot T \cdot e}\left(\mathrm{g^s, g^{\alpha'}}\right), \mathrm{C'} = \mathrm{g^s}$$

我们可以直接利用 q-BDHE 构造出来。之后的属性 *i* 相关密文$C_i = g^{a\lambda_i} g^{-t_i s}$我们需要消除$g^{a^{q+1}}$这个因子。于是我们随机选择$\mathrm{s}, y'_2, \ldots, y'_n \in Z_p$并选择

$$v = \left(s, sa + y'_2, sa^2 + y'_3, \ldots, sa^{n^*-1} y'_n\right) \in Z_p$$

于是$\lambda_i = v \cdot M_i$则

$$C_i = g^{a\lambda_i} g^{-t_i s} = (\prod_{j=1,\ldots,n} (g^a)^{M_{i,j} y'_j})^{(g^s)^{-z_{\rho^*(i)}}}$$

- 挑战后查讯阶段: 对于攻击者 A，可以对每一个授权 *i* 方询问属性集合 $S_{i,1}, \ldots, S_{i,q}$ 的属性私钥。但询问的属性集合不能满足访问控制结构Γ^*。具体的模拟过程同挑战前查讯阶段
- 输出：如果攻击者 A 对于 m_t 给出一个猜测 t=0 或者 t=1。如果攻击者 A 给出了正确的猜测则我们称攻击者赢得游戏的概率都是不可以忽略的，由于

构造，我们可以根据攻击者 A 的猜测判断$T = e(g,g)^{a^{q+1}}$是否成立。这样

我们利用这个游戏可以以不可忽略的概率判定 q-BDHE 问题

基于我们最开始的假设，证毕。

4.4 本章小结

本章介绍了一个新的多授权方的基于属性的加密算法。分别从应用场景，工作方式，函数定义，构造等方面对方案进行了详细的描述和讲解。在本章的最后给出了一个选择属性集合的安全模型下的证明。

第五章 用于私密信息提取的扩展的属性基加密方案

私密信息提取（private information retrieval）也是信息安全应用的一个重要方面，本章将利用在前一章中给出的多授权方的基于属性的加密方案，结合私密信息提取的应用场景，给出一个完整的应用方案。之后利用 SPIR[]协议对提出的这个方案进行改进，从而获得安全性上的一些提高。

5.1 私密信息提取

私密信息获取是指用户向服务器申请特定的数据，这些数据都存储在服务器的一些数据库中。在提取的过程中，服务器并不知道用户所申请的数据。同时要保证用户不会获得他询问的数据之外的数据。这样的场景设计有着实际的意义，在系统中总是会有用户希望获得未被授权访问的数据，而用户在访问自己的某些数据时还希望可以不被其他人知道。

一个最简单的私密信息提取方案即将整个数据库根据用户的需求进行加密，然后将整个数据库发送给用户，用户仅能够利用自己生成需要的一些参数进行解密。但这样的方法，如 BENNY CHOR[24]的方案往往效率比较低。E. Kushilevitz[21]等人提出的方案对这个问题进行了很好的解决。在这个方案中询问的过程是可由多项式时间达到的。

对于私密信息的提取还有很多研究的方向，D.Asonov[23]曾对私密信息的提取给出过一个系统的分析。例如 Beimel[22]等人就对具体的服务器的工作场景和稳定性进行了深入的研究，并通过预先计算和备份的机制给出了一些能保证服务器工作稳定性的方案。

另外一个重要的研究方向就是应用场景更加实例化，通过使用授权，认证，签名都手段和方法来达到私密信息提取的一个过程。例如 Mohamed Layouni[25][26]则提出了多方认证的私密信息获取的方式，我们在他方案的基础上利用基于属性加密的特点，将授权的关系引入层次的结构关系进而增强协议的实用性。

5.2 用于层次化认证私密信息提取的扩展的属性基加密方案

5.2.1 场景描述

首先在我们的协议中分别有四种类型的参与者：系统初始者 *I*，发送者 *S*，接收者 *R* 和授权方$\{A_i\}$。系统的初始者负责系统的建立并将参数分发以及公布。发送者是数据的拥有者，他将根据接收者的要求做出相应的回应并发送给接收者，即扮演了服务器的角色。所以在我们场景中，发送者与系统初始者都是唯一的。接收者相当于一般系统的用户，在一次查询过程中因为他是最终数据的获得者，故成为接收者。一般的用户我们仍然给予一个统一的 ID 作为身份的区分:GID。授权者是数据的真正拥有者，在我们的场景中他们不但可以是一个组群，同样可以是一个有层次的结构。

在现实中，一个关键的数据往往不是由一个用户拥有的而是由一个组群的用户拥有的，例如某公司的年利润统计数据。这个数据往往是不会多所有人公开的，但是作为影响公司生产计划的决定因素之一，我们必须保证这个数据被需要授予访问权限的人能够顺利获取。所以如果只有一个授权方显然是不切实际的。更进一步的，在很多组群中，如公司，授权方的能力也是有可能不同的，如果我们单单以能够授权和不能够授权来区分这个组群，将会使我们的具体应用非常受限制。例如，如果规定所有的经理级别的用户都有授权的权限，则可能由于人数很少，在某个用户应该可以访问关键数据时，无法及时找到授权人给予授权而无法访问。但如果给予更多人授权的权力则可能会出现关键数据的管理不善，更多的人具有授权功能，则泄露关键信息的可能就越大。

我们针对这种情况，利用基于属性加密的访问控制结构，可以很好的解决这个问题。有能力授权的用户不再仅仅通过有能力或没有能力进行授权，我们对授权的过程可以进行利用一个表达式来刻画。例如我们希望刻画这样一种授权，对于某个数据，如公司年度利润统计数据，如果经理允许访问，或者数据分析部门的两名成员授权，或者公司任意四名成员授权，则这个用户可以访问，用授权控制树描述如

图 6-1 所示。

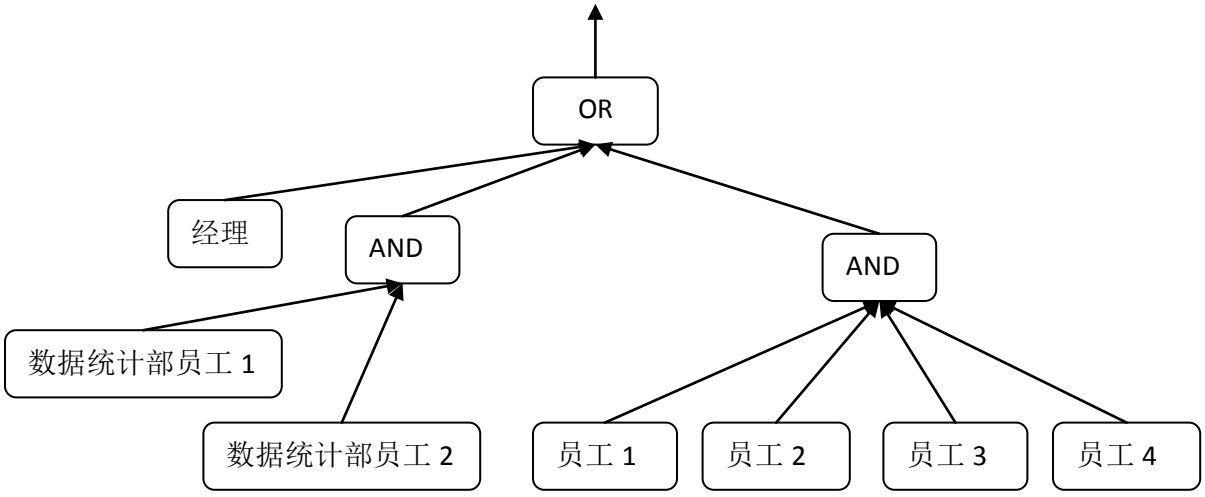

图 6-1 层次的认证结构

在我们的协议中，每一个授权者则对应于基于属性加密算法的属性，授权的过程我们采用了 D Boneh[26]等人提出的短签名方案。所以每一个授权方则相当于我们在前一章给出的多授权的基于属性的加密方案中的一个授权方。授权方进行签名的授权信息就当于之前一个授权方对用户某属性颁发的密钥。

5.2.2 用于层次化认证私密信息提取的扩展的属性基加密方案函数描述

- 公共信息生成函数 Com：输入为安全参数 1^k，输出为一个系统公钥 *PK* 和一个系统控制密钥 *MK*。*PK* 中定义了所有的系统参数如群的选择哈希函数和双线性配对。
- 初始化函数 Init：输入为系统公钥 *PK*, 系统控制密钥 *MK*,和用户统一身份集合{*GID*}输出为用户的私钥$\{Key_{GID}\}$。
- 授权方私钥生成函数 KG：输入为系统公钥 *PK*，输出为认证方 *A* 的公私钥对（PK_A,SK_A）。我们定义对于认证方 A_i的公私钥对为(PK_{A_i}, SK_{A_i})。
- 加密算法 Enc：输入为系统公钥 *PK*，控制访问结构Γ，认证方集合$\{A_i\}$的公共私钥集和加密数据 *d*。输出为密文CT_Γ。
- 签名（授权）算法 Sig：输入为系统公钥 *PK*，认证方 A_i的私钥SK_{A_i}和用户的统一身份 *GID* 输出为签名认证信息Sig_{GID,A_i}
- 签名（授权）验证算法 Ver: 输入为系统公钥 *PK*, 认证方 A_i的私钥PK_{A_i}，用户的统一身份 *GID* 和签名认证信息Sig_{GID,A_i}输出为“有效”和“无效”的符号。

- 解密算法 Dec：输入为系统公钥 PK,包含控制访问结构Γ的密文CT_Γ,一个可以满足控制访问结构的授权者集合$\{A_i\}$的公钥集合$\{PK_{A_i}\}$和由这个集合为用户 GID 颁发的授权集合$\{Sig_{GID,A_i}\}$。输出为数据 d 或者终止符号⊥。

5.2.3 用于层次化认证私密信息提取的扩展的属性基加密方案运行方式描述

首先由初始者运行公共信息生成函数 Com,将产生的公共密钥 PK 发布，之后保存 MK 并为所有的用户针对 GID 产生私钥。用户作为接收者向发送者提出数据申请，接收者从数据库中取出数据 d 并根据该数据的访问控制限制利用加密函数 Enc 对数据加密，并将密文CT_Γ返还接收者。接收者可以同时向一些授权者发送对数据访问请求，授权者如果同意授权则运行授权算法 Sig,用自己的认证私钥对用户的身份进行一次签名，并将签名结果返还给用户。当且仅当给予用户授权的的授权者集合$\{A_i\}$ 满足了访问控制结构时，我们用户利用授权签名集合$\{Sig_{GID,A_i}\}$才可以解开秘文获得明文数据信息，具体的协议运行方式如图 6-2 所示。

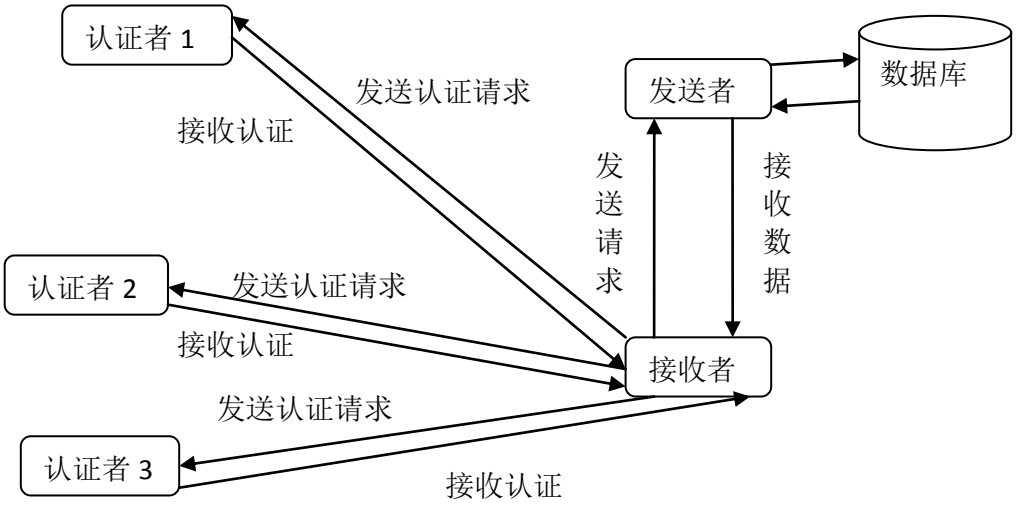

图 6-2 方案运行方式描述图

5.2.4 用于层次化认证私密信息提取的扩展的属性基加密方案构造描述

- 公共信息生成函数 Com：G_1是一个以素数 p 为阶的双线性群，g 是其生成元，$e: G_1 \times G_1 \to G_2$为一个双线性配对运算。随机的我们可以在 Z_p 上选取 a 和α。选择哈希函数$H: \{0，1\}^* \to G_1$。公布的系统参数为

$$PK = (g, e(g,g)^{\alpha}, g^{a}, H, e, G_1, G_2)$$

系统的控制密钥为：

$$MK = (g^{\alpha}, a)$$

- 初始化函数 Init：输入系统公钥 *PK*, 系统控制密钥 *MK*,和用户统一身份 *GID*,输出的密钥为

$$Key_{GID} = g^{\alpha} H(GID)^{a}$$

- 授权方私钥生成函数 KG：授权方 A_i随机的选择$t_i \in Z_p$作为自己的认证私钥SK_{A_i}，并公布自己的公钥为$PK_{A_i} = g^{t_i}$。
- 加密算法 Enc：输入为系统公钥 PK，控制访问结构Γ，认证方集合{Ai}的公共私钥集和加密数据 d，设控制访问结构Γ可以由 LSSS 方案中的(*M*,*ρ*）表达。函数*ρ*在本协议中将矩阵 *M* 中的行与授权方相关联。矩阵 *M* 是一个$l \times n$的矩阵。该算法首先选择一个随机的向量 *v*=(*s*,y_2, …,y_n)。对于 *j* 从 1 开始到 *l* 计算$\lambda_i = v \cdot M_i$，其中 M_i是指矩阵 *M* 的第 *i* 行。对于私密数据 *d* 则密文为

$$CT_{\Gamma,m} = (C = d \cdot e(g,g)^{\alpha s}, C' = g^{s}, C_1 = g^{a\lambda_1} g^{-t_1 s}, \dots, C_l = g^{a\lambda_l} g^{-t_l s})$$

其中$g^{-t_1 s}$的计算可以由$(PK_{A_i})^{-s}$得到。

- 签名（授权）算法 Sig：输入为系统公钥 PK，认证方 Ai 的私钥SK_{A_i}和用户的统一身份 *GID* 输出为签名认证信息

$$Sig_{GID,A_i} = H(GID)^{t_i}$$

- 签名（授权）验证算法 Ver: 输入为系统公钥 PK, 认证方 Ai 的私钥PK_{A_i}，用户的统一身份 *GID* 和签名认证信息Sig_{GID,A_i}。验证的过称为判断表达式

$$e\left(Sig_{GID,A_i}, g\right) = e(H(GID), (PK_{A_i}))$$

- 解密算法 Dec：输入为系统公钥 PK,包含控制访问结构*Γ*的密文CT_{Γ},一个可以满足控制访问结构的授权者集合{Ai}的公钥集合{PK_{A_i}}和由这个集合为用户 *GID* 颁发的授权集合{Sig_{GID,A_i}}。并且有集合$I = \{i : \rho(i) \in \{A_i\}\} = \{1,2,\dots,l\}$。对应于 LSSS 协议，我们可以知道在多项式时间内找到常量的集合$\{\omega_i | i \in I\}$使得$\sum_{i \in I} \lambda_i \omega_i = s$。则解密算法计算

$$\frac{e(C', Key_{GID})}{\prod_{i \in I} (e\left(C_i, H(GID)\right) e(Key_{GID,i}, C'))^{\omega_i}}$$

$$= \frac{e(g^s, g^\alpha H(GID)^a)}{\prod_{i\in I}(e(g^{a\lambda_i} g^{-t_i s}, H(GID))e(H(GID)^{t_i}, g^s))^{\omega_i}}$$

$$= \frac{e(g^s, g^\alpha H(GID)^a)}{\prod_{i\in I}(e(g, H(GID)))^{a\lambda_i\omega_i}}$$

$$= e(g,g)^{\alpha s}$$

之后算法通过计算

$$d = \frac{C}{e(g,g)^{\alpha s}}$$

获得私密数据信息。

5.2.5 用于层次化认证私密信息提取的扩展的属性基加密方案的效率和安全分析

我们给出的用于层次化认证的私密信息提取的扩展的属性基加密方案，在加密的过程中不需要配对计算，所有的运算均限于群上的指数运算和加法运算。设参与加密的属性个数为 l，则总共进行群的指数运算 2l+1 次，群的加法运算共 l+1 次。在解密的过程中，设参解密的属性个数为 l'则，配对计算公进行了 2l'+1 次，群上的指数运算共 l 次,群上的加法运算一次。在签名的过程中不需要进行配对计算，只需要 1 次群上的指数运算。在验证签名的过程中需要进行一次配对计算。

在我们的方案中我们达到了一下几个方面的安全性

- 数据安全性：接收者在没有得到足够授权的时候无法解开密文获得关键数据。这一点由于我们的协议可以简单的规约为第四章的多授权方的基于属性的加密，我们可以认为不存在不可忽略的多项式时间可以攻破我们的方案。
- 发送者安全性：即接收者不可以获得他没有授权的数据信息。这一点与数据安全性相近，但在我们的协议中由于发送者每次只发送一条信息，固自然地可以达到。
- 认证者安全性：认证者的安全是指认证者之间并不需要通过通讯等手段同步一些信息再加以认证，同时，认证者之间并不知道是否其它认证者已经对接收者进行了认证，亦即每个认证者的认证过程都是相互独立的。这一点在我们协议中由于是对多授权方基于属性加密的一个扩展，每个认证者即相当于一个只授权一个属性的授权方，所以彼此是相互独立的。无论是个人的私钥生成还是认证过程都可以是相对独立的完成的。
- 接收者的认证可验证性：接收者接到认证后可以凭借检验函数判断这个认证是否为一个有效的认证信息。只有在信息有效地情况下，接收者才可以

利用认证进行解密。由于我们采用了 D Boneh[26]的短签名方案作为我们对接收者发放认证的方式，固可将关于签名的安全性我们可以规约到 CDH 问题。

- 抗共谋攻击：对于基于属性的加密方案，一种很常见的攻击方式即共谋攻击。共谋攻击是指：几个攻击者，每个人都不能对特定的消息进行解密，因为每一方拥有的属性密钥都不满足控制结构，如果他们将属性密钥的集合拼合起来满足了访问控制结构并能够进行解密，我们则称这几个攻击者进行了一次共谋攻击。在我们的方案中每一个有效的信息，例如接收者的公钥，认证等等都与身份信息 GID 唯一的绑定在一起。在解密的过程中我们可以由公式

$$\frac{e(C', Key_{GID})}{\prod_{i\in I}(e(C_i, H(GID))e(Key_{GID,i}, C'))^{\omega_i}}$$

看出，每一个参与解密的项都与用户的身份信息 GID 相关。

在这个方案中，我们虽然很好的解决了有层次结构的授权人群的授权认证过程。但是也存在几个问题，首先接收者的隐私没有得到保证，即发送者知道接收者询问的数据信息。其次，我们对数据的前向安全没有能够提供保障的机制。

前项安全性是指当当前的一些实体或者用户的私钥已经被破解，对于之前的询问和加密过程的信息仍不会有影响。我们的系统由于仅包含单一的身份信息，当用户的私钥以及认证信息被获取后则可以对以前的由发送者发送来的密文信息进行解密。针对以上几个方面的不足，我们在下一节对我们的协议进行了改进。

5.3 改进的用于私密信息提取的扩展的属性基加密方案

5.3.1 SPIR[28]方案的工作原理

SPIR[28]方案是一个经典的私密信息提取的方案。它在保证接收者的私有安全性的同时，还可以提供发送者的私有安全性，即发送者虽然将这个数据库进行加密发送给接收者，但是接收者只能提取他查询的内容，而不能得到其他的信息。SPIR 协议使用的数据库是单一索引的数据库。

在这里我们可以将 SPIR 方案作为一个实现了私密信息抽取的一个黑盒函数。SPIR 的方案运行过程可以简单描述为：用户 *u* 首选选择一个希望选择的数据项，并根据数据项在数据库中的索引 *index* 通过自己的私密生成一个查询 *Q*,然后将这个查询 *Q* 发送给接收者，接收者将数据库中每一项根据 *Q* 和这一项在数据库的 *index*

进行加密。并将加密后的整个数据库 *R* 返回给用户用户根据自己选择的 *index* 和私密运行抽取函数则可以从 *R* 中抽取用户询问的信息。具体流程如图 6-3 所示

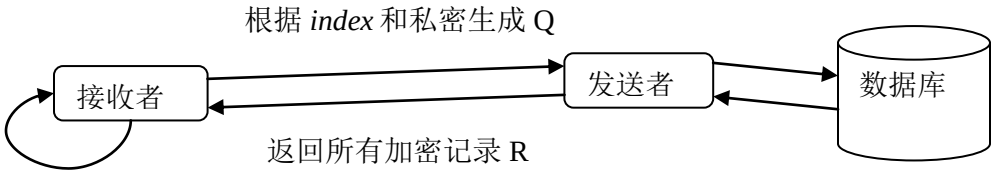

图 6-3 SPIR 协议工作方式描述

5.3.2 改进的用于私密信息提取的扩展的属性基加密方案函数描述

- 公共信息生成函数 Com：输入为安全参数 k，输出为一个系统公钥 *PK*。*PK* 中定义了所有的系统参数如群的选择哈希函数和双线性配对。
- 授权方私钥生成函数 *KG*：输入为系统公钥 *PK*，输出为认证方 A 的公私钥对（PK_A,SK_A）。我们定义对于认证方 A_i 的公私钥对为(PK_{A_i}, SK_{A_i})。
- 加密算法 Enc：输入为系统公钥 PK，控制访问结构Γ，认证方集合$\{A_i\}$的公共私钥集和加密数据 d 和临时认证信息 m。输出为密文CT_Γ。
- 签名（授权）算法 Sig：输入为系统公钥 *PK*，认证方 A_i 的私钥SK_{A_i}，临时认证信息 m 和用户的统一身份 *GID* 输出为签名认证信息Sig_{GID,A_i}
- 签名（授权）验证算法 Ver: 输入为系统公钥 *PK*, 认证方 A_i 的私钥PK_{A_i}，用户的统一身份 *GID*，临时认证信息 m 和签名认证信息Sig_{GID,A_i}输出为“有效”和“无效”的符号。
- 解密算法 Dec：输入为系统公钥 *PK*,包含控制访问结构Γ的密文CT_Γ,一个可以满足控制访问结构的授权者集合$\{A_i\}$的公钥集合$\{PK_{A_i}\}$，临时认证信息 m 和由这个集合为用户 *GID* 颁发的授权集合$\{Sig_{GID,A_i}\}$。输出为数据 d 或者终止符号⊥。

5.3.3 改进的用于私密信息提取的扩展的属性基加密方案运行方式描述

首先由初始者运行公共信息生成函数 Com,将产生的公共密钥 PK 发布。用户作为接收者向发送者提出数据申请 m'这个申请 m'是由两部分组成，一个是申请的

政策，例如时间戳和一些其它的系统设定，另一个是用户身份 *GID*, 即 *m'=Policy || GID*。接收者从数据库中对每一项数据 d_j 针对于它的索引 j 新生成一个请求信息 *m=m'||index* 并根据该数据的访问控制限制利用加密函数 Enc 对数据加密，并将对应于整个数据库的密文$\{CT_\Gamma\}$返还接收者。接收者可以同时向一些授权者发送对数据访问请求 m，授权者如果看过 policy 等内容后同意授权则运行授权算法 Sig,用自己的认证私钥对用户的身份进行一次签名，并将签名结果返还给用户。当且仅当给予用户授权的的授权者集合$\{A_i\}$ 满足了访问控制结构时，接收者利用授权签名集合 $\{Sig_{GID,A_i}\}$ 才可以解开秘文获得明文数据信息。

我们利用 SPIR 协议主要代替了我们前一节协议中接受者和发送者之间的直接传递则新的工作方式图如图 6-4 所示：

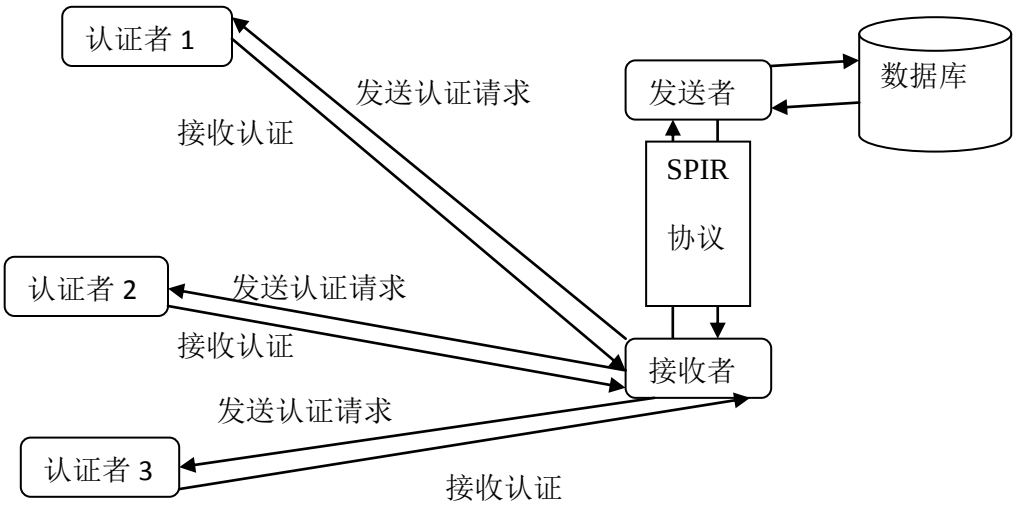

图 6-4 方案运行方式描述图

5.3.4 改进的用于私密信息提取的扩展的属性基加密方案构造描述

- 公共信息生成函数 Com：G_1 是一个以素数 p 为阶的双线性群，g 是其生成元，$e: G_1 \times G_1 \to G_2$为一个双线性配对运算。随机的我们可以在 Z_p 上选取 a。选择哈希函数$H: \{0，1\}^* \to G_1$。公布的系统参数为

$$PK = (g, g^a, H, e, G_1, G_2)$$

- 初始化函数 Init：输入系统公钥 *PK*, 系统控制密钥 *MK*,和用户统一身份 *GID*,输出的密钥为

$$Key_{GID} = g^{\alpha} H(GID)^{a}$$

- 授权方私钥生成函数 KG：授权方 A_i 随机的选择$t_i \in Z_p$作为自己的认证私钥SK_{A_i}，并公布自己的公钥为$PK_{A_i} = g^{t_i}$。
- 加密算法 Enc：输入为系统公钥 PK，控制访问结构Γ，认证方集合{Ai}的公共私钥集,请求信息

$$m=Policy||GID||index$$

和加密数据 d，设控制访问结构Γ可以由 LSSS 方案中的(M,ρ)表达。函数ρ在本协议中将矩阵 M 中的行与授权方相关联。矩阵 M 是一个 $l\times n$的矩阵。该算法首先选择一个随机的向量 $v=(s,y_2,\ldots,y_n)$。对于 j 从 1 开始到 l 计算

$$\lambda_i = v \cdot M_i$$

其中 M_i 是指矩阵 M 的第 i 行。对于私密数据 d 则密文为

$$CT_{\Gamma,m} = (C = d \cdot e\big(g, H(m)\big)^{\alpha s}, C' = g^{s},$$

$$C_1 = e(g^{a\lambda_1} g^{-t_1 s}, H(m)), \ldots, C_l = e(g^{a\lambda_l} g^{-t_l s}, H(m))$$

其中$g^{-t_1 s}$的计算可以由$(PK_{A_i})^{-s}$得到。

- 签名（授权）算法 Sig：输入为系统公钥 PK，认证方 Ai 的私钥SK_{A_i}, 和请求信息 *m=Policy||GID||index* 输出为签名认证信息

$$Sig_{m,A_i} = H(m)^{t_i}$$

- 签名（授权）验证算法 Ver: 输入为系统公钥 PK, 认证方 Ai 的私钥PK_{A_i}，请求信息 *m=Policy||GID||index*,和签名认证信息Sig_{m,A_i}。验证的过称为判断表达式

$$e\big(Sig_{m,A_i}, g\big) = e(H(m), (PK_{A_i}))$$

- 解密算法 Dec：输入为系统公钥 PK,包含控制访问结构Γ的密文CT_{Γ},一个可以满足控制访问结构的授权者集合{Ai}的公钥集合$\{PK_{A_i}\}$和由这个集合为请求信息 *m=Policy||GID||index* 颁发的授权集合$\{Sig_{m,A_i}\}$。并且有集合$I = \{i: \rho(i) \in \{A_i\}\} = \{1,2,\ldots,l\}$。对应于 LSSS 协议，我们可以知道在多项式时间内找到常量的集合$\{\omega_i | i \in I\}$使得$\sum_{i\in I} \lambda_i \omega_i = s$。则解密算法计算

$$\prod_{i\in I} (e\big(C_i, H(m)\big) e(Sig_{m,i}, C'))^{\omega_i} = e(g, H(m))^{as}$$

之后算法通过计算

$$d = C'/e(g, H(m))^{as}$$

获得私密数据信息。

5.3.5 改进的用于私密信息提取的扩展的属性基加密方案的效率和安全分析

设参与加密的属性个数为 *l*，在我们给出的改进的私密信息提取的扩展的属性基加密方案中，加密的过程中需要 *l* 次配对计算，进行群的指数运算 *2l+1* 次，群的加法运算共 *l*+1 次，但是由于 SPIR 方案需要对所有的数据项进行加密，设所有数据项的数据数量为|DB|，则加密的过程中需要 *l*× |DB|次配对计算，进行群的指数运算（2*l*+1）× |DB|次，群的加法运算共（*l*+1）× |DB|次。在解密的过程中，设参解密的属性个数为 l'则，配对计算公进行了 2*l*'次，群上的指数运算共 *l* 次,群上的加法运算一次。在签名的过程中不需要进行配对计算，只需要 1 次群上的指数运算。在验证签名的过程中只需要进行一次配对计算。

在我们的方案中我们达到了一下几个方面的安全性

- 数据安全性：由于我们协议的构造可以知道当解密用户获得的认证不满足控制结构的时候，是无法通过运算恢复出临时密钥 *s*。这样由于明文信息与 *s* 绑定则无法消除 *s* 解得明文。这样我们的数据是无法被不满足访问控制结构的用户得到。
- 发送者安全性：由于我们采用了 SPIR 协议作为发送者和接收者直接传递数据的途径，而 SPIR 在加密传递和抽取的过程中可以保证接收者只可以从中拿到一条自己请求的数据记录，故此方案的发送者安全性可由 SPIR 协议满足。
- 接收者安全性：此安全性是指发送者并不知道接收者所需要的记录的内容。由于我们采用 SPIR 协议作为发送者和接收者直接传递数据的途径，而 SPIR 协议无论请求者请求任何记录都会将所有的数据加密并发送给接收者。对于接收者发出的请求 *q*，由于发送者无法从中得到关于消息索引的任何信息，在此情况下，发送者无法知晓接收者的具体请求，故接收者的安全性得以保证。
- 认证者安全性：我们协议中是对多授权方基于属性加密的一个进一步的扩展，每个认证者即相当于一个只授权一个属性的授权方，可以独自运行密钥生成函数，所以彼此是相互独立的。无论是个人的私钥生成还是认证过程都可以是相对独立的完成的，故认认证者之间并不需要通过通讯等手段

同步一些信息再加以认证，同时，认证者之间并不知道是否其它认证者已经对接收者进行了认证。

- 接收者的认证可验证性：由于我们采用了 D Boneh[26]的短签名方案作为我们对接收者发放认证的方式，固可以将关于签名的安全性我们可以规约到 CDH 问题。

- 抗共谋攻击：在我们的方案中每一个有效的信息，例如接收者的公钥，认证等等都与一份请求信息 m 唯一的绑定在一起，而 m=Policy||GID||index。则每个认证都与用户的身份直接相关，而在解密的过程中我们可以由公式

$$\prod_{i\in I}(e(C_i, H(m))e(Sig_{m,i}, C'))^{\omega_i} = e(g, H(m))^{as}$$

看出，每一个参与解密的项都与用户的身份信息 GID 相关。故而对于几个攻击者，当他们每个人都不能对特定的消息进行解密，如果他们将属性密钥的集合拼合起来满足了访问控制结构由于请求信息 m 不同，即使共谋将认证信息组合在一起也是无法恢复出临时密钥 s 的。

- 前向安全性：我们的方案没有直接给出关于前项安全性的构造，但是通过对于请求信息 m 中的政策信息 Policy 进行扩充，要求 Policy 中必须含有时间的控制。则这样即使某个授权的用户当前的密钥以及一些认证被攻破，他还是不能直接得到之前会话的信息。

在这个改进的方案中，我们首先扩充了协议的安全性，不但满足了已有的发送者安全性，数据安全性，接收者的认证可验证安全性还增加了符合私密信息提取定义的接收者安全性。在效率上, 虽然在加密的过程中增加了很多多余的计算，但是这些计算为了能够满足接收者的安全也是不可避免的，由于取消了用户私钥的认证，在解密的过程中，相对之前的协议简化了一些。另外，由于系统不需要可信第三方保留系统私钥，这既提高了系统的安全性又扩充了该方案的适用条件。由于在请求信息中不单单可以加入用户的身份信息，还可以加入与时间相关的信息，使得系统在获得抗共谋攻击的同时还可以获得前向安全性等属性。

另外，改进的用于私密信息提取的扩展的属性基加密方案与之前的方案相比，在实际场景中会有更好的应用，因为在请求的信息中我们不仅可以加入时间信息作为前向安全性的保证，也可以作为认证有效信息的一个认证。例如这样一个场景，某在线教育视频点播的付费会员，在接受认证之后就可以从服务器（发送者）下载数据，并用获得认证进行收看自己被授权部分的信息如计算机辅导视频。由于会员的不是终身制的，我们可以对认证信息加入有效时间段，例如把政策 policy 设定为 year=2009。这样加密的过程中，服务器会对数据按照商定的时间有效期进行加密，

则密文的信息是与政策相关的，当我们改变政策时只要服务器端的发送者相应的改变数据，则可以使对某一项数据的访问权限则被收回。新的会员必须通过获取关于新的有效区间的授权才能进行解密。

5.4 本章小结

本章应用了前一章给出的多授权方的加密算法，结合私密信息提取的应用场景给出了两个方案。在本章中从场景描述，函数定义，构造，效率分析和安全分析等几个方面对方案进行了详细的介绍和分析。在本章最后还对给出的两个方案进行了比较。

第六章 总 结

6.1 主要结论

本文致力于研究基于属性的密码系统中的公开问题，包括如何改进方案的效率，提出更多实际的应用场景，增强基于属性的密码系统访问控制结构的表达能力，和对新的方案的安全性证明以及扩展应用。

在改进效率的方面主要着眼于如何减少复杂代数运算，如双线新配对计算。在应用场景方面，主要围绕在多授权方的基于属性的加密方案展开研究。在比较了现有方案的基础上，从中选取了表达能力较强的访问控制结构作为自己提出新方案的访问控制结构，并给予可证安全模型下的证明。新的方案的扩展主要集中在用于一些系统的信息检索。

本文的主要研究成果如下:

- 本文对近年来的基于属性的加密方案，以及相关的一些体系，如基于属性的签名方案，多授权方的基于属性的加密算法等内容进行了分类和总结。从效率，安全，应用等几个方面比较了各个方案的优势和劣势，并给出了一些有代表性方案的构造方法。同时通过介绍整个基于属性加密算法的发展趋势，指出了之后在该领域需要改进的方向。
- 本文提出了一个高效安全的密文政策的多授权方的基于属性的加密方案。并在标准安全模型下给予证明，达到选择属性集的 CPA 安全。与之前的多授权方如 chase[10]相比，无论效率还是访问控制结构表达能力上都有了一些提高。在属性授权方的密钥生成环节则采用独立的生成方式，授权方不需要彼此通讯交互一些信息，甚至不需要从可信第三方获得私钥。由于将用户身份信息通过 Hash 的方式与密文和密钥绑定，使得直接的应用扩展相对容易。
- 从提出的多授权方的基于属性的加密方案进行了扩展，应用于私密信息获取的场景。根据多授权方的基于属性的加密方案的特点，应用了 LSSS 方案构造的访问控制结构，提出了一个可以具有层次区分的认证工作方式的方案。数据本身的授权方式在数据产生时被确定，数据的拥有者在授权能力上各有不同，描述这种授权结构的即基于属性加密方法中的访问控制结构。

- 利用 SPIR 协议对用于私密信息获取的扩展方案进行了改进。在之前方案的有层次区分的认证工作方式基础上，使得方案在获得更多的安全属性，如接收者安全属性，前项安全性等等。同时，可以更方便的进行扩展以适应更多复杂的环境，如多授权方的授权有效时间的假设。

6.2 研究展望

基于属性的加密算法在近年得到广泛的关注不仅仅是因为基于属性的加密算法理论设计上的复杂性，更因为基于属性密码以及相关研究的巨大实际价值。基于属性的加密算法在把对身份的控制和认证扩充为对用户拥有的属性集合的认证，还提供了丰富的控制手段，通过门限，与门和或门等控制单元构造出可以适应很多情况的访问控制结构。

但是现有的一些基于属性的加密算法以及相关的方案还存在以下的一些需要改进和关注的问题：

- 密文政策的基于属性的加密：尽管密钥政策的基于属性的加密也有一定的应用，但是由于密钥政策需要为每一个访问控制结构提供一套密钥，密文政策的基于属性的加密更加接近现实的场景。但目前密文政策的方案还很有限，构造更多的密文政策的基于属性的加密方案将是一件非常有意义的工作。
- 访问控制结构的表达能力：目前，我们已经有了几种方式表达访问控制结构，例如利用门限，与门或门以及非门的访问控制树的方式，通过 LSSS 方案构造出的与授权集相关的方案，以及非单调的方式构造出的访问控制结构等等。但是很多构造增加了大量冗余，或者增加很多限制，例如有对某一属性不能多次出现在访问控制结构的限制等等。这种构造限制了基于属性的加密算法的一些应用，如何能够造出完全与谓词空间等价的访问控制结构也是之后的研究关注的一个方向。
- 减少双线性配对计算：在现有的基于属性的加密算法中，几乎所有的方案都使用了双线性配对计算作为构造的一种便利的方式。但是双线性配对计算本身的计算复杂度较高，如果每个属性的加密或者解密过程都需要靠双线性配对运算来构造则会使基于属性的加密算法效率非常低。甚至有些协议不仅要对参与访问控制结构的属性进行配对运算，其它的属性也有相关的配对运算。如果可以构造一个配对计算次数与属性个数无关的方案将会

使非常有意义的。另外，基于属性的数字签名技术已经有一些研究，但同样因为效率问题没有得到广泛的应用。

- 多授权方的基于属性加密：多授权方的基于属性加密方案作为属性加密的一个特殊分支因为每个授权方的彼此独立，更加适合应用于现实生活。而如何构造一个没有可信中心的，即所有授权方实现真正的平等的方案将是研究的一个重要方向。

参考文献

[1] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Trans. Inf. Theory, 22(6), pages 644 - 654, 1976.

[2] R.L.Rivest, A. Shamir and L.Adleman, ”A method for obtaining digital signatures and public key cryptosystem”, Comm. ACM., 21, pages 120-126,1978.

[3] Amit Sahai and Brent Waters, ”Fuzzy identity-based encryption”, In EUROCRYPT, pages 457-473, 2005.

[4] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters, ”Attribute-based encryption for fine-grained access control of encrypted data”, In ACM Conference on Computer and communications Security, pages 89-98, 2006.

[5] Cheung, L., Newport, C.: Provably Secure Ciphertext Policy ABE. In: ACM conference on Computer and Communications Security (ACM CCS). (2007)

[6] V Goyal, A Jain, O Pandey, A Sahai Bounded Ciphertext Policy Attribute Based Encryption Lecture Notes in Computer Science, 2008 – Springer

[7] C Cocks. An identity based encryption scheme based on quadratic residues. Lecture Notes in Computer Science, 2001 – Springer.

[8] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security

and Privacy, IEEE Computer Society (2007)321-334

[9] Amos Beimel. Secure Schemes for Secret Sharing and Key Distribution. PhD thesis, Israel

Institute of Technology, Technion, Haifa, Israel, 1996.

[10] Melissa Chase. Multi-authority attribute-based encryption. In The Fourth Theory of CryptographyConference (TCC 2007), 2007.

[11] R Ostrovsky, B Waters. Attribute-Based Encryption with Non-Monotonic Access Structures. - Proceedings of the 14th ACM conference on Computer, 2007 - portal.acm.org

[12] Huang Lin, Zhenfu Cao, Xiaohui Liang, and Jun Shao. Secure threshold multi-authority attribute based encryption without a central authority. INDOCRYPT 2008, Lecture Notes in Computer Science, Springer, 5365: 426-436, 2008.

[13] V Bozovic, D Socek, R Steinwandt, VI Villányi. Multi-authority attribute based encryption with honest-but-curious central authority. eprint.iacr.org

[14] Ibraimi, L.; Petkovic, M.; Nikova, S.I.; Hartel, P.H.; Jonker, W. Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes. Centre for Telematics and Information Technology, University of Twente. URN:NBN:NL:UI:28-65471

[15] Mohamed Layouni, Maki Yoshida, Shinago Okamura.: Efficient Multi-Authorizer accredited Symmetrically Private Information Retrieval. Information and Communications Security(Proceedings of the 10th International ICICS Conference, Birmingham, UK, 2008) (UK) 387-393

[16] D Khader. Attribute Based Group Signature with Revocation. 2007-mirror.cr.yp.to

[17] D Khader. Attribute Based Group Signature . 2007-mirror.crypto

[18] D Khader. Authenticating with Attribute. 2008-eprint.crypto

[19] J Li, K Kim. Attribute-Based Ring Signatures. eprint.iacr.org

[20] H Maji, M Prabhakaran, M Rosulek. Attribute based signatures: achieving attribute-privacy and collusion-resistance. eprint.iacr.org

[21] E. Kushilevitz and R. Ostrovsky. Replication is Not Needed: Single Database, Computationally Private Information Retrieval. In 38th Annual Symposium on

[22] A. Beimel and Y. Stahl. Robust Information-Theoretic Private Information Retrieval. In Third Conference on Security in Communication Networks, Lecture Notes in Computer Science 2576, pages 326–341. Springer-Verlag,2002.

[23] D. Asonov. Private Information Retrieval: An overview andcurrent trends. In Proceedings of the ECDPvA Workshop, Informatik 2001, September 2001.

[24] BZ Chor, O Goldreich, E Kushilevitz.Private Information Retrieval - US Patent 5,855,018, 1998

[25] Mohamed Layouni, Maki Yoshida, Shinago Okamura.: Efficient Multi-Authorizer Accredited Symmetrically Private Information Retrieval. Information and Communications Security(Proceedings of the 10th International ICICS Conference, Birmingham, UK, 2008) (UK) 387-393

[26] Mohamed Layouni. Acredited symmetrically private information retrieval. In Miyaji, A., Kikuchi, H., Rannenberg, K., eds.: IWSEC. Volume 4752 of Lecture Notes in Computer Science Springer (2007) 262-277

[27] D Boneh, B Lynn, H Shacham:Short signatures from the Weil pairing.Journal of Cryptology, 2004 Volume 17, Number 4 297-319

[28] Lipmaa, H.: An oblivious transfer protocol with log-squared communication. In: Proceedings of the 8th International Information Security Conference. Volume 3650 of LNCS, Springer-Verlag (2005) 314–328

[29] D. Boneh and X. Boyen, Effcient selective-ID secure identity-based encryption without random oracles," Advances in Cryptology | EUROCRYPT '04, LNCS 3027, pp. 223238, Springer-Verlag, 2004.

[30]D. Boneh and X. Boyen, Secure identity based encryption without random oracles," Advances in Cryptology {CRYPTO '04, LNCS 3152, pp.443{459, Springer-Verlag, 2004.

[31] L. M. Kohnfelder, Towards a practical public-key cryptosystem, B.S. Thesis, supervised by L. Adleman, MIT, Cambridge, MA, May 1978.

[32] Dan Boneh and Matthew K. Franklin, Identity-based encryption from the weil pairing, In CRYPTO, pages 213-229, 2001.

[33] Dan Boneh and Matthew K. Franklin, Identity-based encryption from the weil pairing, SIAM J. Computing, 32(3), pages 586-615,2003.

[34] Craig Gentry, Practical Identity-Based Encryption Without Random Oracles, In EUROCRYPT'06, pages 445-464, 2006.

[35] R.L.Rivest, The MD5 Message Digest Algorithm, RFC 1321, Apr. 1992.

[36] NIST, Digital Signature Standard(DSS), Federal Information Processing Standards Publication 186, 1994.

[37] Ronald Cramer and Victor Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack", In CRYPTO '98, pages 13-25, 1998.

[38] Ronald Cramer and Victor Shoup, "Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption", In EUROCRYPT, pages 45-64, 2002.

[39] D.Dolev, C.Dwork and M.Naor, "Non-malleable cryptography.", In Proc. of STOC'91, pages 542-552, 1991.

[40] Q Tang, D Ji Verifiable Attribute-Based Encryption. mirror.cr.yp.to

[41] L Cheung, J Cooley, R Khazan, C Newport Collusion-Resistant Group Key Management Using Attribute-Based Encryption eprint.iacr.org

[42] Ibraimi, L., Tang, Q., Hartel, P.H., Jonker, W. Efficient and Provable Secure Ciphertext-Policy Attribute-Based Encryption Schemes (2009)

[43]Shannon,C.E., Communication theory of Secrecy System, Bell Syst, Tech, Jounal Vol 28,656-715

致 谢

在此首先我要感谢恩师曹珍富教授对我的辛勤指导。曹老师献身密码学事业二十余年，桃李芬芳，无论在学术上还是思想上都给我带来了很大的影响；我还要感谢在本科及硕士学习阶段指导过我的各位老师，他们给我带来了智慧与知识，更教会了我如何努力与成才；我还要感谢在实验室与我一起工作的师兄师姐，他们给我树立了榜样，使得我有了奋斗和前进的目标。最后我还要感谢我的家人，没有他们在背后默默地支持我，我也不可能有今天的成绩。

上海交通大学

学位论文原创性声明

本人郑重声明：所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已经注明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

学位论文作者签名：单忆南

日期：2010 年 1 月 1 日

上海交通大学

学位论文版权使用授权书

本学位论文作者完全了解学校有关保留、使用学位论文的规定，同意学校保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权上海交通大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

保密□，在____年解密后适用本授权书。

本学位论文属于

不保密☑。

（请在以上方框内打"√"）

学位论文作者签名：单忆南　　指导教师签名：

日期：2010年1月1日　　日期：2010年1月5日