□ 信息安全系列丛书

基于身份的密码学

胡 亮 赵 阔 袁 巍
李宏图 初剑峰

The Cryptography Based on Identity

高等教育出版社
HIGHER EDUCATION PRESS

□ 信息安全系列丛书

基于身份的密码学

胡 亮 赵 阔 袁 巍
李宏图 初剑峰

The Cryptography Based on Identity

JIYU SHENFEN DE MIMAXUE

高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING

图书在版编目(CIP)数据

基于身份的密码学/胡亮等著. —北京:高等教育出版社,2011.1

(信息安全系列丛书)

ISBN 978-7-04-031702-2

Ⅰ.①基… Ⅱ.①胡… Ⅲ.①密码-理论 Ⅳ.①TN918.1

中国版本图书馆 CIP 数据核字(2011)第 003962 号

策划编辑 刘建元 **责任编辑** 刘建元 **封面设计** 王凌波

版式设计 余 杨 **责任校对** 姜国萍 **责任印制** 张福涛

出版发行	高等教育出版社	**购书热线**	010-58581118
社 址	北京市西城区德外大街 4 号	**咨询电话**	400-810-0598
邮政编码	100120	**网 址**	http://www.hep.edu.cn
			http://www.hep.com.cn
		网上订购	http://www.landraco.com
经 销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印 刷	北京市白帆印务有限公司	**畅想教育**	http://www.widedu.com
开 本	787×1092 1/16	**版 次**	2011 年 1 月第 1 版
印 张	11.25	**印 次**	2011 年 1 月第 1 次印刷
字 数	210 000	**定 价**	39.00 元

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换。

物料号 31702-00

序

互联网、电子商务和电子政务的普及，在为社会经济发展带来巨大利益的同时，也带来了更加严峻的安全问题。在网络信息交互的应用环境中，除了信息加密等安全措施以外，还需解决信任问题。公钥基础设施（PKI, public key infrastructure）体系虽然从技术上可以解决网上认证、信息完整性和抗抵赖性等安全问题，但其安全保障是由证书来体现的，证书的管理和维护需要大量的处理资源和带宽资源，部署成本较高。

1984 年，以色列密码学家 Shamir 提出了基于身份的密码体系的思想，直接使用用户的标识，如姓名、电子邮件地址等作为公钥，而用户的私钥则通过一个被称作私钥生成器（PKG, private key generator）的可信任第三方进行计算得到。与传统的 PKI 体系相比，基于身份的密码学体系不再依赖证书，简化了管理密码体系的复杂性，成为密码学领域新兴的研究热点。

2001 年，第一个真正实用的基于身份加密（IBE, identity-based encryption）方案由美国密码学家 Boneh 和 Franklin 利用椭圆曲线上的双线性映射 Weil 配对设计出来。2002 年，美国密码学家 Gentry 和 Silverberg 第一次提出了一个完整建立在随机预言机模型下的、双线性 Diffie-Hellman 假设基础上分层的基于身份密码体系，从而解决了安全传输用户私钥的问题。2003 年，AI-Riyami 和 Paterson 提出了基于一个被称作密钥生产中心（KGC, key generator center）的可信第三方的无证书密码思想，以解决用户密钥由 PKG 托管的问题。2007 年，Goyal 提出了第三方权利受约束的基于身份加密方案（A-IBE, accountable authority identiy-based encryption scheme），在不改变 IBE 方案基础架构的前提下，进一步减少了用户对 PKG 的信任需求。

本书在介绍基于身份密码学研究分支的基础上，全面介绍了作者在基于身份签名算法、基于身份的广播加密算法以及基于身份的密码学典型应用实例方面所做的工作。全书九章安排如下：

第一章是基于身份密码学基础，主要介绍基于身份密码学的发展历程和本书使用的基础定义。

第二章是基于身份签名算法，主要介绍基于身份签名算法的构造模型，给出包括 Shamir 方案、CC-IBS 方案、Narayan 和 Parampalli 方案等在内的典型的基于身份签名方案，详细描述了作者提出的改进方案。

第三章是基于身份的加密算法，主要介绍基于身份加密算法的基础模型、Boneh 和 Franklin 的 IBE 方案、Waters 的 IBE 方案和 Gentry 的 IBE 方案，充分展现 IBE 系统的特点。

第四章是基于身份的分层加密算法（HIBE，hierarchical identity-based encryption），主要介绍相关的基本定义与 HIBE 安全模型、Gentry 和 Silverberg 方案、Boneh 等人的密文长度固定的 HIBE 方案、Au 等人的方案以及 Hu 和 Park 等人对 HIBE 和基于身份的分层签名算法（HIBS，hierarchical identity-based signature）的安全分析与改进。

第五章是基于无证书的签名算法，主要介绍相关的基础定义，以及安全模型、Riyami 的方案、Yum 和 Lee 的方案及分析、Zhang 等人的方案及安全性分析。

第六章是基于无证书的加密算法，主要介绍相关的安全模型、Riyami 的加密方案、Yum 和 Lee 的方案及分析、被动恶意 KGC 攻击、Au 等对 Riyami 方案的分析以及 Hwang 的模型。

第七章是 PKG 受约束的基于身份加密算法，主要介绍相关的定义和模型、Goyal 的 A-IBE 方案以及 Xu 等人的通用 A-IBE 方案。

第八章是基于身份的广播加密（IBBE，identity-based broadcast encryption）算法，主要介绍作者在相关的基本定义及基本模型、基于一次签名的构建方案、基于消息认证码（MAC，message authentication code）方式的构建方案以及基于 q-BDHI（q-bilinear Diffie-Hellman inversion problem）的 IBBE 方案等所做的工作。

第九章是基于身份密码应用，主要介绍作者设计并实现的密钥定时更换基础框架及其在防伪码系统和文件加密系统中的应用实例。

本书不仅包括一些典型的基于身份密码算法，同时也关注了该领域国内外的最新进展。在内容的选择上，本书既突出了广泛性，又注重对要点的深入探讨。语言简练，内容重点突出，逻辑性强，算法经典实用，便于读者花少量的时间尽快掌握基于身份密码学的精髓。

本书兼具专著和教材的双重属性，可作为密码学和信息安全专业的研究生或高年级本科生的教学参考书，也可供密码学和信息安全领域的研究人员学习参考。

作者

2010 年 12 月于长春

目　录

第一章　基于身份密码学基础

1.1　基于身份密码学概述

基于身份密码算法是一门新兴的且正在发展中的公钥密码算法，它的设计思想最早由以色列密码学家 Adi Shamir 提出。这种密码算法的设计目标是让通信双方在不需要交换公私密钥，不需要保存密钥目录，且不需要使用第三方提供认证服务的情况下，保证信息交换的安全性并可以验证相互之间的签名。

当前，影响公钥密码体制下安全系统发展的主要困难不是选择合适的安全算法或如何实施这些算法，而是部署和管理支持密钥真实性的基础设施。这些基础设施需要为用户提供公钥或用户身份与私钥之间关系的安全保证。在传统的公钥基础设施中（例如 PKI，public key infrastructure 体系），这种体系的安全保障是由证书来体现的，其本质是用权威机构来为用户签名。这种管理体制存在很多与证书管理相关的问题：包括撤销、存储和分配以及认证核查用户证书等。这需要占用大量的处理资源和带宽资源。

基于身份密码体制假设存在一个可信的私钥生成器（PKG，private key generator），当新用户第一次加入到网络中时，该中心会给每一个用户生成一个个性化的智能卡，卡中保存用户的私钥。用户可以使用私钥来对自己发送的信息进行加密和签名，同时还可以在不用考虑对方身份的情况下完全独立地解密并验证接收到的信息。

在传统的公钥基础设施中，智能卡在新的用户加入时往往不得不升级更新，而且各类认证中心需要协调其行为，保存一张所有用户的信息列表，并不断更新用户的信息，这使得认证中心的管理工作变得非常复杂。与其相比，基于身份的密码体系最大的优点是密钥生成中心可以在用户智能卡发行完成后关闭，网络可以在完全分散式的状态下运行任意的时间而不需要任何中心的支持。

在传统的公钥体系中，公钥的有效期在公钥证书生成时确定。如图 1.1，在基于身份加密算法中，一个实用系统的公钥终止前 Alice 可以使用公钥 Bob@jlu.edu.cn‖current year 来加密电子邮件，然后发送给 Bob，这样 Bob 只能使用他当年的私钥来实现解密。每年密钥到期后，Bob 需要从 PKG 中获取一个新的私钥，这样就达到了每年私钥到期更换的效果。与证书算法不同的是在每次 Bob

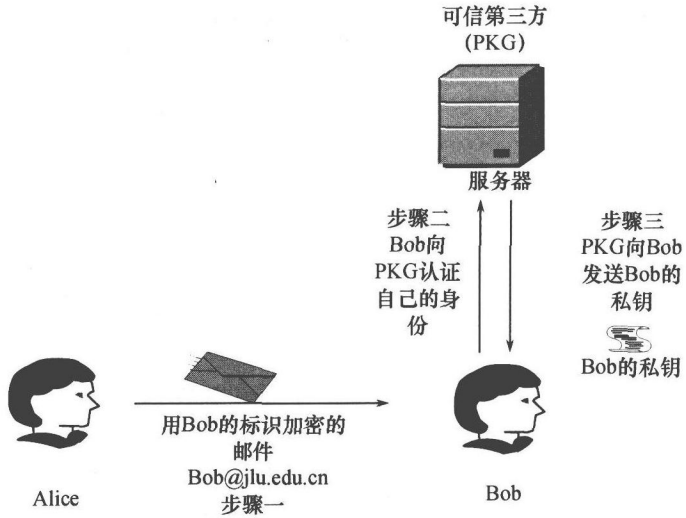

图 1.1 基于身份加密的执行过程

更新私钥后，Alice 并不需要获得新证书。一个更严谨的做法是使用“Bob@ jlu. edu. cn ‖current date”加密发送给 Bob 的电子邮件，这就迫使 Bob 每天需要获取新的私钥。因为 PKG 由公司自己管理，所以对于公司每天更新员工的私钥是可以做到的。有了这个方法，撤销密钥是非常简单的：Bob 离开公司时，他的主密钥需要撤销，公司的 PKG 停止向 Bob 的电子邮件地址发送私钥。因此，Bob 将无权阅读他的电子邮件，而且 Alice 不需要和任何第三方证书目录沟通来获得 Bob 的日常公钥。因此基于身份的加密对于实现需要经常更新的公钥机制是非常有效的。另外，Alice 还可以把信息发送到“未来”，Bob 只能在由 Alice 规定的日期解密电子邮件。因为 PKG 可以很容易授予和撤销用户的密钥，通过这种方法，用户密钥的管理将变得非常简单。

在 Shamir 最初的设计中，这种密码算法特别适合于封闭的群体用户使用，例如跨国公司、大型银行的各个分支机构。因为这些公司的总部可以作为每一个用户所信任的密钥生成中心。基于身份的密码算法可以作为一种新的个人身份识别卡的基础，每一个用户可以用其进行电子签名验证、网上信用卡支付以及电子邮件的签名等活动。这种密码算法以传统公钥密码系统为基础，但也有一些不同之处：其中最核心的一点是公钥密码系统中随机生成公钥与私钥，并将其中的公钥公布。而这种算法使用用户自己选择的信息，如用户姓名、用户的电子邮件、电话号码等信息或这些信息的组合，作为其公钥使用，同时该用户也不能对代表自己的标识加以否定。与用户选择的公钥相对应的私钥则由密钥生成中心生成，并且在用户首次加入到该网络的时候以智能卡的形式颁发给该用户。

基于身份的密码算法就像一个完美的电子邮件系统；当知道对方的姓名和

地址,就可以给对方发送只能被对方读取的信息,同时可以验证来自于对方的签名。这样对于用户来说,通信的加密过程是透明的,所以它可以被对密钥和加密协议一无所知的非专业人员有效地使用。如:当用户 Alice 想给用户 Bob 发送信息时,Alice 使用自己智能卡中的私钥对信息进行签名,然后利用 Bob 用户的公钥对信息进行加密,把加密后的信息连同自己的身份信息发送给用户 Bob。当用户 Bob 收到信息后,首先使用自己的智能卡中的私钥对信息进行解密,然后使用 Alice 用户发来的身份信息验证 Alice 对信息的签名。

在这种密码算法中,用户的私钥不能由自己计算产生,必须由密钥生成中心计算产生。因为如果 Alice 能计算对应于公钥"Alice"的私钥,则同样也能计算出对应于"Bob"等公钥的私钥,这样就会对算法的安全性带来威胁。而密钥生成中心具有一定的特权,它可以知道一些特定的信息,利用这个信息可以为网络中的每一个用户计算出各自的私钥。这种算法的安全性依赖于以下几个因素:

(1) 基本加密算法的安全性;

(2) 密钥生成中心中特有信息的安全性;

(3) 在颁发给用户智能卡之前对用户身份标识核查的彻底性;

(4) 用户对智能卡丢失、被非法复制、非授权使用的防范性。

这种密码算法有效地将发送的信息与用户标识信息紧密联系起来,同时将用户的智能卡与用户本人也联系到一起。像其他发放身份识别卡的发卡机构一样,密钥生成中心应严格审查要发放智能卡的申请人,以避免非法用户冒称合法用户申请智能卡,同时密钥生成中心应保护好计算用户私钥所使用的特权信息以防止用户私钥泄露。对于一般用户而言,用户应该防止自己的智能卡遭到未经授权的使用,同时防止自己智能卡中的私钥在使用时被非法复制。

Shamir 指出,这种密码算法应当具有以下两个附加性质:

(1) 当已知种子密钥 k 后,可以容易计算出任意公钥对应的私钥;

(2) 如果已知任何一对公钥与私钥,计算出种子 k 是非常困难的。

同时,Shamir 也指出,由于 RSA(Rivest Shamir Adleman)加密方案不能同时满足这两个条件,因此不能应用到这种新算法中。因为如果模数 n 对于用户的标识符来说是一个伪随机过程,密钥中心不能将该模数 n 分解,也就不能从公钥 e 计算出私钥 d,假设模数 n 是一个具有一般意义的数,而种子是它的一个秘密的分解因子,这样任何一个知道公钥 e 和对应的私钥 d 的人都可以计算出种子。同时,Shamir 利用 RSA 算法构造了第一个基于身份的签名算法,并推断基于身份密码算法的实现是存在的,并将此问题作为一个公开问题提出,希望有人可以解决此问题。这与 1976 年 Diffie 和 Hellman 刚刚提出公钥密码学时的情况相似,虽然公钥密码学的设计思想被提出的同时也有了良好的应用前景,但是其具体的实现方案直到 1978 年才被研究出来。

自从 1984 年 Shamir 提出这个问题以来，很多基于身份的加密方案被陆续提出。然而，这些方案都不能完全令人满意。有些方案不能抵抗用户共谋，有些方案需要 PKG 对每个私钥请求花费很长的时间，有些方案则需要防硬件篡改。一个可用的基于身份的加密系统一直是一个重要但悬而未决的问题。直到 2001 年，第一个真正实用的基于身份加密（IBE，identity-based encrption）方案由美国密码学家 Boneh 和 Franklin 利用椭圆曲线上的双线性映射 Weil 配对设计出来。其中的公钥可以是任意字符串。该方案包含 4 个算法：

（1）*Setup* 生成全局系统参数和一个主密钥；

（2）*Extract* 使用主密钥生成对应于任意公钥字符串 $ID \in \{0,1\}^*$ 的私钥；

（3）*Encrypt* 使用公钥 *ID* 加密消息；

（4）*Decrypt* 使用相应的私钥解密消息。

该方案达到了 Shamir 提出的设计要求，即使接收者 Bob 尚未设置自己的公钥证书，发送者 Alice 也可以向他发送加密的邮件。该加密方案的性能与 ElGamal 算法性能相当，其安全性基于 Diffie-Hellman 假设。即只要计算双线性群 G_1, G_2 中的 CDH 问题（CDH，computaional Diffie-Hellman problem）是困难的。Boneh 和 Franklin 提出的 IBE 系统可以由 G_1, G_2 上的双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 构建，并在随机预言模型中达到选择密文安全。从此之后，这种体制的效率优势才开始被密码学界广泛关注。与传统的公钥密码学相比，基于身份的密码算法也有一些明显的缺点，如：每个用户从 PKG 的第三方接收自己的私钥，就需要用户向 PKG 认证自己作为合法接收者的身份，从而获取私钥，需要一个专门的安全信道向接收者传送私钥，这一过程存在一定的安全隐患和验证效率问题。为有效识别出一些恶意攻击者伪装成接收者申请私钥，提高验证效率以及私钥传输的安全性都是需要解决的问题，因此 PKG 必须公开嵌入用户私钥的参数信息。在 Alice 向 Bob 发送加密信息前，必须取得这些参数。由于 PKG 知道用户的私钥，也就是密钥托管是基于身份密码系统固有的。对于某些特定的应用，这种托管是一种优势，在一些大型的公司或需要谨慎分级管理事物的网络政务机构中是非常有效的。但对于另一些应用来说，这种托管是严重的安全问题。

不过，基于身份的加密技术的优势是引人注目的。与传统公钥密码学相比，获取真实公钥的问题已被获取公共 PKG 的真实参数问题取代，且后者负担较轻。因为相对总用户数来说，PKG 用户将有较大幅度的减少。一种极限情况是，如果每个人都使用一个 PKG，那么每个人都可以在系统中进行安全通信而不必在网上查询公钥或公共参数。虽然只有一个 PKG 的系统会完全消除网上参数的查询，但对一个大型网络来说，这样做是不可取的，因为这相当于把用户参数获取问题转化为 PKG 之间的参数传递问题。不仅生成私钥的计算代价高，而且必须对 PKG 进行身份验证并建立安全通道来传送私钥。

为了解决安全传输用户私钥的问题，2002 年美国密码学家 Gentry 和 Silverberg 在总结了前人研究成果的基础上第一次提出了一个完整建立在随机预言机模型下、双线性 Diffie-Hellman（BDH，bilinear Diffie-Hellman）假设基础上的分层基于身份密码算法（HIBC，hierarchical identity-based cryptography）该方案将 PKG 的功能分为多层，包括一个根 PKG 和多层的域 PKG。根 PKG 只为域 PKG 生成私钥，并对其进行身份认证。域 PKG 在得到私钥之后又可以利用自己的私钥为下层的域 PKG 生成私钥，直至最终用户的上一层，而这一层的 PKG 往往处于用户的本地或局域网中，这就使得对用户的认证和密钥的传输都在本地进行。如果低层 PKG 的密钥泄露，只会影响其域内用户，而不影响高层 PKG 私钥的安全性。

在基于身份密码算法中，用户私钥是由 PKG 利用主密钥产生的。同样 PKG 也能伪造任何实体的签名，因此这种算法不能提供真正的不可抵赖性。多 PKG 的提出和阈值技术的使用在一定程度上可以解决密钥托管问题，但是必须增加额外的通信和基础设施。因此，基于身份密码算法只能限于小范围或需要安全限制的应用。为了解决用户密钥由私钥生成中心托管的问题，AI-Riyami 和 Paterson 在 2003 年提出了无证书密码思想。在他们的方案中，同样需要一个被称作密钥生产中心（KGC，key generator center）的可信第三方。KGC 利用实体 A 的身份 ID_A 和主密钥为实体 A 提供部分私钥，并且这一过程是需要保密和认证的。也就是 KGC 必须保证这部分私钥必须安全地分发到正确的实体手中。

实体 A 将它的部分私钥和一些秘密信息结合生成实际的私钥 SA，因此 KGC 就不能获得 A 的私钥。实体 A 将它的一些秘密信息和 KGC 的公共参数结合计算出公钥 PA。由于 A 在生成 SA 时不需要 PA，公钥也不再仅仅从身份计算出来，所以这个系统不再是完全意义上的基于身份系统。实体 A 的公钥可以通过发送消息时添加附加信息或发布在公开的目录中以便其他用户使用。但是不需要额外的安全措施来保护 A 的公钥，特别是不需要证书。实体 B 只需要用 PA 和 ID_A 向 A 发送加密信息或验证 A 的签名。

由于缺少对公钥的认证信息（例如：公钥证书），所以敌手能够通过一个伪造的密钥来代替 A 的公钥。这似乎给敌手很大权力，并且也成为无证书公钥体制的一个漏洞。不过通过分析可知，敌手通过以上的攻击方式不能得到任何有价值的信息，因为计算正确的私钥需要由 KGC 生成的部分私钥，所以在没有正确的私钥的情况下，敌手不能解码被伪造的公钥加密的密文，也不能产生可以被伪造的公钥验证的签名等等。但必须假定 KGC 不能采用下面攻击的形式：因为可以获得实体的部分私钥，KGC 可以生成任何实体的公/私钥对并可以发布这个公钥，所以 KGC 可以扮演任何实体。也就是说，KGC 是被认为不会替换实体公钥的。但是 KGC 可以从事其他的敌对活动，例如：对密文进行窃听，并解密密

文。在基于身份密码算法中,用户必须信任 PKG 不会去滥用私钥;但在无证书密码中,用户仅仅需要相信 KGC 不去发布伪造的公钥。与基于身份密码算法相比,无证书密码中对可信任第三方的信任依赖可以大幅降低。

由于 PKG 有能力计算任何身份所对应的私钥,基于无证书机制虽然降低了对 PKG 的信任度,但并未完全解决这一问题。实际上,只要需要信任 PKG,当 PKG 滥用其权利时,完全信任和部分信任使得基于身份的密码系统都存在安全缺陷。也就是说,如果 PKG 愿意,它可以自由地从事任何的恶意行为却不会面临任何法律制裁。这些恶意行为可能包括:为任何的用户解密和读取信息,或者更糟的是,可以为任何身份生成和分配私钥。尽管它具有很出色的性能,但事实上已经成为减缓 IBE 使用的一个重要原因。由于存在密钥托管或部分密钥托管问题,IBE 的用户被限制在小的且封闭的组中,该组中只有一个中心受信权威是可用的,这些都引起了对该体系的广泛争论。

2007 年,Goyal 创造性地提出了一种对密钥托管问题的完全解决方案。该方案在不改变 IBE 方案基础结构的条件下,进一步减少了用户对 PKG 的信任需求。该方案称为第三方权利受约束的基于身份加密方案(A-IBE, accountable authority identity-based encryption scheme)。

总的来说,在 A-IBE 方案的密钥生成协议中,当用户收到来自 PKG 的私钥种子信息时,用户通过秘密选取"迹"信息来部分地决定用户私钥的生成。因此,从直觉上来说,由于 PKG 并不知道用户秘密选取的"迹",因此也就无法独立生成具有相同"迹"的该用户的私钥。另一方面,由于私钥种子信息的秘密性,用户在没有 PKG 的帮助下也无法额外地生成不同"迹"的私钥。因此在实际应用中,若某用户发现有人知道他的一个有效的且不同"迹"的私钥时,那么该用户就可以充分地认定 PKG 伪造了他的私钥,从而进行索赔。较具体地说,Goyal 首次给出了 A-IBE 的定义及其特殊的安全性定义,并且分别基于 Gentry 和 Waters 的 IBE 方案,构造了两个具体的可证明安全的 A-IBE 方案。Goyal 方案的特点如下:

(1) 在这个 IBE 方案中,对应每个身份 ID 都可能存在指数个解密密钥。

(2) 已知一个身份的解密密钥,想获得其他的解密密钥是很困难的。

(3) 用户们使用一个安全密钥产生协议,从 PKG 上面获取与其自身身份所对应的解密密钥。这个协议允许用户为其身份获得一个单独的解密密钥 d_{ID},而不需要让 PKG 知道具体获得了哪一个。

(4) 如果 PKG 为有恶意用途的身份产生一个解密密钥 d'_{ID},尽管这种可能微乎其微,但是它也将区别于用户所获得的密钥 d_{ID}。因此密钥对(d'_{ID},d_{ID})将会成为 PKG 恶意行为的证据(因为在正常情况下,每个身份只能有一个密钥)。

虽然 PKG 确实能够被动地解密所有用户信息。但是,对于私钥 d'_{ID}的分配

来说 PKG 是被严格限制的。密钥 d'_{ID} 的完整信息使实体 E 与诚实用户 U(具有身份 ID 和密钥 d_{ID})能够一起合作,将(d'_{ID},d_{ID})作为欺诈证据对 PKG 提出控告(进而可能停止它的业务或给 E 和 U 大量金钱作为补偿,这将是 E 和 U 乐于接受的)。这意味着在任何时候,如果 PKG 为有恶意目的身份产生解密密钥的话,那么将存在陷入高额索赔的风险。

在基于身份密码学的基础上,研究基于身份的广播加密算法也具有重要的应用价值。广播加密(BE,broadcast encryption)是由 Fiat 和 Naor 提出的。一个广播者加密消息给监听广播信道的一组用户 S。在集合 S 中的用户可以用自己的私钥解密广播的消息。

Delerablée、Paillier 和 Pointcheval 扩展了广播加密的概念,提出了动态广播加密(DBE,dynamic broadcast encryption)。一个动态广播加密系统是一个开始并不把所有用户都初始化的广播加密系统。基于此特性,任意新用户都可以对之前分发的密文进行解密。因此,动态广播加密系统适合于很多应用,比如 DVD 加解密。然而,许多应用例如 VOD 视频点播,需要前向安全,这时动态广播加密系统就不适合了。最初,Delerablée 使用了略强的攻击模型,该攻击模型允许挑战者在获得系统公开参数之前适应性地选择密文,这是静态攻击模型的一个增强版。

Smart 提出的多接收者密钥封装机制(mKEM, multi-receiver key encapsulation)是一个有效的多步的密钥封装机制。后来,mKEM 的概念被扩展为多个基于身份接收者的密钥封装机制(mID-KEM,multi-receiver identity-based key encapsulation),密文的长度随着接收者的数目而增长。Chatterjee 和 Sarkar 提出了第一个 mID-KEM 协议来达到子线性的密文长度,密文的长度是 $|S|/N$,其中私钥的长度是 N,S 是接收者身份集合。因此,他们介绍了第一个 Mid-KEM 协议,实现了子线性的密文个数。最近,Abdalla 等提出了一种方案,采用不变大小的密文,但是私钥的数量是 $o(n^2_{\max})$。

在总结以上方案的基础上,本书分别利用一次签名机制和 MAC 机制构造了两个高效的基于身份广播加密算法。

1.2 基础定义

1.2.1 双线性映射

定义 1 双线性映射(指数形式)。设 G_1 是由 g 产生的循环加法群,它的阶是素数 p,G_2 是同阶的循环乘法群,映射 $e:G_1\times G_1\rightarrow G_2$ 是一个线性映射,如果映射满足下面的条件:

(1) 双线性:对于所有的 $u,v\in G,a,b\in Z_p$,有 $e(u^a,v^b)=e(u,v)^{ab}$。

(2) 非退化性:存在 $e(g,g)\neq 1$。

(3) 可计算性:对于所有的 u,v,存在一个有效的算法计算 $e(u,v)$。

定义 2 双线性映射(对数形式):我们称映射 e 是双线性映射,如果:G_1 是一个 q 阶加法循环群,G_2 是一个 q 阶乘法循环群,$G_1\times G_1\rightarrow G_2$ 具有以下属性:

(1) 双线性:对任意 $Q,R\in G_1,a,b\in Z$,有 $e(aQ,bR)=e(Q,R)^{ab}$。

(2) 非退化性:该映射不把 $G_1\times G_1$ 上的所有配对映射到 G_2 上。

(3) 可计算性:存在一个有效的算法对于任何 $Q,R\in G_1$,可以计算 $e(Q,R)$。

1.2.2 数学难题与安全性

各种数学难题和假设是构建密码学安全性的基础,而安全性的高低直接决定了一个密码学方案的安全强度。本节在对典型的数学难题进行回顾的基础上,进一步总结了 IBE 方案安全性的各种数学难题基础。

DH 相关问题(DHP,Diffie-Hellman problem)

DH 问题:

定义 3 给定一个大素数 q,一个大整数生成元 $g\in Z_q^*$,以及由大随机数 a,b 生成的 $g^a \bmod q$ 和 $g^b \bmod q$,要求找到 $g^{ab} \bmod q$。

DH 问题是 Diffie-Hellman 密钥交换算法安全性的基础,这种安全性是建立在有限域内计算离散对数(DL,discrete logarithm)的困难性基础之上的。

CDH 问题(CDH,computational Diffie-Hellman problem):

定义 4 对于随机给定的$\langle P,aP,bP\rangle$,其中 a,b 属于具有 q 阶的点群 Z_q^*,计算 abP 的值。

同 DH 问题一样,CDH 问题的困难性也是基于离散对数的。

DDH 问题(DDH,decision Diffie-Hellman problem):

定义 5 区分对于给定的元组$\langle P,aP,bP,abP\rangle$和$\langle P,aP,bP,cP\rangle$之间的分布,即判断 c 是否等于 $ab \bmod q$,其中 a,b,c 属于具有 q 阶的点群 Z_q^*。

在具有 q 阶的加法循环点群 G_1 上,DDH 问题的判定是容易的。因为在群 G_1 上,对于给定的 $P,aP,bP,cP\in G_1$,可以构造出多项式时间可计算的双线性映射 e,来验证 $c=ab \bmod q\Leftrightarrow e(aP,bP)=e(P,cP)$。

q-DHI 问题(q-DHI,q-Diffie-Hellman inversion problem):

定义 6 给定 $q+1$ 维元组$\langle g,g^x,g^{x^2},\cdots,g^{x^q}\rangle\in G^{q+1}$,计算 $g^{1/x}\in G$。

q-DHI 假设为一个更自然的复杂性假设,且问题描述中不要求使用随机预言机模型。因此,基于 DH 假设的构建可以被依赖于 q-DHI 假设的构建所取代。

q-SDH 问题(q-SDH,q-strong Diffie-Hellman inversion problem):

定义 7 给定维 $q+1$ 元组$\langle g,g^x,g^{x^2},\cdots,g^{x^q}\rangle\in G$,计算$(c,g^{1/(x+c)})$,其中 c,