|  |  |
| --- | --- |
| |  | | --- | | 电子科技大学  UNIVERSITY OF ELECTRONIC SCIENCE AND TECHNOLOGY OF CHINA  硕士学位论文  MASTER THESIS |   论文题目 **基于Node-red与Redis的实时流数据处理模型的设计与应用**  学科专业 **软件工程**  学 号 **201422220209**  作者姓名 **王江波**  指导教师 **教授 刘玓** |

分类号 密级

UDC注1

学 位 论 文

**基于Node-red与Redis的实时流数据处理模型的设计与应用**

（题名和副题名）

**王江波**

（作者姓名）

指导教师 **教授** **刘玓**

**电子科技大学**  **成 都**

（姓名、职称、单位名称）

申请学位级别 **硕士** 学科专业 **软件工程**

提交论文日期  论文答辩日期

学位授予单位和日期 **电子科技大学**

答辩委员会主席

评阅人

注1：注明《国际十进分类法UDC》的类号。

|  |
| --- |
| **Key Management Research and Application in Identity-Based Encryption System** |

A Master Thesis Submitted to

University of Electronic Science and Technology of China

|  |  |
| --- | --- |
| Major: | **Software Engineering** |
| Author: | **Yuhuan Li** |
| Supervisor: | **Senior Engineer Shuquan Li** |
| School: | **School of Infromation and Software Engineering** |

独创性声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。据我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得电子科技大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

作者签名： 日期： 年 月 日

论文使用授权

本学位论文作者完全了解电子科技大学有关保留、使用学位论文的规定，有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许论文被查阅和借阅。本人授权电子科技大学可以将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、汇编学位论文。

（保密的学位论文在解密后应遵守此规定）

作者签名： 导师签名：

日期： 年 月 日

摘 要

公钥密码体制的发展受两个因素影响，分别是安全算法和支持公钥认证的基础设施。在公钥基础设施（Public Key Infrastructure，PKI）中，数字证书通过绑定用户的身份和公钥信息，实现了公钥认证。然而，在实际应用中，由于数字证书的管理和使用需要消耗大量资源，这限制了系统的扩展性。基于身份的加密（Identity-Based Encryption，IBE）体制改变了公钥的产生方式，简化了数字证书的管理。在该体制中，用户的公钥可以直接从唯一标识用户身份的信息中获取，不再需要通过数字证书认证用户的公钥。然而，在IBE方案中，用户的私钥由PKG（Private Key Generator）产生，带来了身份认证，用户私钥托管，私钥安全分发，密钥撤销等问题。

本文分析了现有的密钥管理方案，指出其中存在PKG欺骗，公钥认证等安全问题以及造成的系统负担问题，提出了两个创新性的方案：

第一，本文结合Feldman的可验证秘密共享（Verifiable Secret Sharing，VSS）思想，运用盲签名技术，加入可信中心，协同用户，提出了一种密钥管理方案。由VSS和双线性映射的性质，证明该方案的正确性，得出该方案可以解决密钥托管问题，实现密钥的撤销管理。在密钥产生分发方面，与同类型的其他管理方案，该方案更全面、正确。

第二，针对KGC（Key Generation Center）或KPA（Key Privacy Center）发动的内部攻击、非法用户的外部攻击和物理故障等问题，本文引入第三方信任机构，通过签名和设置有效期，提出了一种密钥分发方案。由双线性映射的性质，证明了方案的正确性并分析了方案的安全性。

本文针对电子邮件存在的安全问题，采用BF-IBE的具体实施方案，给出了关键算法的设计流程和实现方法，使用MIRACL，利用VC++6.0，在本地机上模拟了基于身份的安全电子邮件系统中密钥服务器和用户之间的信息交互，电子邮件客户端的发送加密和解密接收的电子邮件的过程。实验测试证明本系统可以保证邮件在传输过程中的安全性。

**关键词：**基于身份加密，密钥托管，可验证秘密共享，安全电子邮件

**ABSTRACT**

The development of public key cryptosystem is affected by two factors, namely, the security algorithm and the foundation of public key authentication. In Public Key Infrastructure (PKI), the digital certificate is bound to the identities of users and public key information to realize the public key authentication. However, in practical applications, the digital certificate needs to consume a lot of resources, which makes the scalability of the system limited. Identity based encryption (Identity-Based Encryption, IBE) system changes the way of public key generation and simplifies the management of digital certificates. In this system, the user’s public key can be directly obtained from the user’s unique identity information, which no longer needs to use the digital certificate to authenticate the user’s public key. However, the user’s private key is generated by the PKG (Private Key Generator), which results in the identity authentication, the user’s key escrow problem, key security issue, the key revocation and so on.

This thesis analyzes the existing key management schemes, and points out that there are some problems, such as PKG deception, public key authentication and so on, the system burden, then puts forward two innovative schemes:

Firstly, combined with Feldman verifiable secret sharing (Verifiable Secret Sharing, VSS), this thesis proposes a key management scheme which uses the blind signature technology and includes a trusted center as well as the user’s collaborative. By the properties of VSS and bilinear map, the correctness of the scheme is proved, which shows that the scheme can solve the key escrow problem and realize the management of the revocation of the key. In the key generation and distribution, compared with the same type of other management schemes, this scheme is more comprehensive and correct.

Secondly, in view of the problems: internal attacks launched by KGC (Key Generation Center) or KPA (Key Privacy Center), illegal users of external attack and physical fault, this thesis adds the trusted third party to solve these problems by using signature technology and setting the validity period. By the property of bilinear map, the correctness of the scheme is proved and the security of the scheme is analyzed.

This thesis applies the specific implementation scheme of the full BF-IBE to solve the security problem in e-mail system, gives the key algorithms in the design process and realization method, and takes the advantage of MIRACL to simulate the communication process of secure e-mail between the PKG server and user, the process of encryption and decryption of e-mail on local machine with VC++ 6.0. Experimental results show that the system can ensure the security of mail in the transmission process.

**Keywords:** Identity-Based Encryption, Key Escrow, Verifiable Secret Sharing, Secure E-mail

目 录

[第一章 绪论 1](#_Toc449695400)

[1.1 研究背景和意义 1](#_Toc449695401)

[1.2 国内外研究现状 2](#_Toc449695402)

[1.2.1 IBE密钥管理研究现状 2](#_Toc449695403)

[1.2.2 IBE应用研究现状 4](#_Toc449695404)

[1.3 主要工作和研究内容 5](#_Toc449695405)

[1.4 结构安排 6](#_Toc449695406)

[第二章 基于身份加密体制的基础理论和技术 7](#_Toc449695407)

[2.1椭圆曲线密码学 7](#_Toc449695408)

[2.1.1 椭圆曲线的定义和运算 7](#_Toc449695411)

[2.1.2 椭圆曲线安全性分析 8](#_Toc449695412)

[2.2 双线性映射 9](#_Toc449695413)

[2.3 Diffie-Hellman假设及相关问题 9](#_Toc449695414)

[2.4 单向散列函数 10](#_Toc449695415)

[2.5 基于身份加密方案 11](#_Toc449695416)

[2.5.1 基于身份加密方案介绍 11](#_Toc449695417)

[2.5.2 BF-IBE基本方案 11](#_Toc449695418)

[2.5.3 BF-IBE详细方案 12](#_Toc449695419)

[2.5.4 BF-IBE具体实施方案 13](#_Toc449695420)

[2.6 公钥基础设施和基于身份加密的对比分析 14](#_Toc449695421)

[2.6.1 公钥基础设施 14](#_Toc449695422)

[2.6.2 公钥基础设施和基于身份加密的比较 15](#_Toc449695423)

[2.7 本章小结 16](#_Toc449695424)

[第三章 基于身份的密钥管理方案设计 17](#_Toc449695425)

[3.1基于身份加密密钥管理方案分析 17](#_Toc449695426)

[3.1.1 基于秘密共享方案 17](#_Toc449695427)

[3.1.2 多方共管方案 18](#_Toc449695428)

[3.1.3 基于证书方案 19](#_Toc449695429)

[3.1.4 基于无证书方案 20](#_Toc449695430)

[3.1.5 其他密钥管理方案 21](#_Toc449695431)

[3.2 改进的基于秘密共享方案 21](#_Toc449695432)

[3.2.1 改进的方案设计思想 21](#_Toc449695433)

[3.2.2 改进的方案组成 23](#_Toc449695434)

[3.2.3 改进的方案设计 25](#_Toc449695435)

[3.2.4 改进方案分析 27](#_Toc449695436)

[3.3 Lee.B安全私钥分发 31](#_Toc449695437)

[3.3.1 Lee.B安全私钥分发协议 31](#_Toc449695438)

[3.3.2 Lee.B安全私钥分发协议的应用 33](#_Toc449695439)

[3.3.3 Lee.B方案的问题分析 34](#_Toc449695440)

[3.4 改进的Lee.B安全私钥分发 36](#_Toc449695441)

[3.4.1 改进的Lee.B方案 36](#_Toc449695442)

[3.4.2 改进的私钥分发协议的分析 38](#_Toc449695443)

[3.4.3 改进的私钥分发协议的应用 40](#_Toc449695444)

[3.5 本章小结 41](#_Toc449695445)

[第四章 基于身份加密在安全电子邮件系统中的应用 42](#_Toc449695446)

[4.1 电子邮件的介绍 42](#_Toc449695447)

[4.1.1 电子邮件和电子邮件系统 42](#_Toc449695448)

[4.1.2 电子邮件安全解决方案 44](#_Toc449695449)

[4.1.3 电子邮件协议 44](#_Toc449695450)

[4.1.4 S/MIME和PKI技术分析 45](#_Toc449695451)

[4.2 基于身份的安全电子邮件系统的设计 46](#_Toc449695452)

[4.2.1 基于身份的安全电子邮件系统模型 46](#_Toc449695453)

[4.2.2 系统初始化算法流程 47](#_Toc449695454)

[4.2.3 用户私钥提取算法流程 48](#_Toc449695455)

[4.2.4 加密算法流程 50](#_Toc449695456)

[4.2.5 解密算法流程 51](#_Toc449695457)

[4.3 基于身份安全电子邮件系统的实现 53](#_Toc449695458)

[4.3.1 模拟工具 53](#_Toc449695459)

[4.3.2 PKG主要功能实现算法 53](#_Toc449695460)

[4.3.3 邮件客户端加密解密功能实现算法 57](#_Toc449695461)

[4.3.4 PKG和用户之间的通信 59](#_Toc449695462)

[4.3.5 邮件发送和接收 60](#_Toc449695463)

[4.3.6 系统运行界面图和测试 60](#_Toc449695464)

[4.4 本章小结 66](#_Toc449695465)

[第五章 结论 67](#_Toc449695466)

[5.1 研究工作总结 67](#_Toc449695467)

[5.2 研究工作展望 68](#_Toc449695468)

[致谢 70](#_Toc449695469)

[参考文献 71](#_Toc449695470)

[攻读硕士学位期间取得的成果 77](#_Toc449695471)

# 

# 第一章 绪论

1.1 研究背景和意义

网络改变了信息交互的方式，促使信息传播更加迅速，丰富了信息共享的方式，扩大了信息影响的范围。近年来，国内外频频出现各种网络犯罪事件[1]，造成了国家、组织、公司或个人在经济和涉密等方面不同程度的损失。研究网络信息安全，对经济的安全稳定和可持续发展，社会环境的文明健康和安定有序[2]，国家的繁荣兴盛和长治久安非常重要。

网络信息安全[3]是一个系统工程，通过对组成网络的有形硬件，无形软件和虚拟数据的各种安全管理，为用户创造一个多方面、全方位、可信连续的网络活动环境。信息安全技术融合了技术手段和管理手段，对信息资产进行风险预测、风险评估、风险抵御和风险管理，从而维护组织正常运作[4]。信息安全的主题是信息的安全[5]。隐藏信息真实内容，即对信息加密是保护信息安全普遍采用的措施[6]。根据加密密钥和解密密钥分为：对称密码体制和非对称密码体制（公钥密码体制）[7]。传统的加密方案采用移位和替换实现加密，属于对称密码体制中最简单的一种加密方案。

对于使用对称密码体制的应用来说，在进行加密活动时，通信双方同时拥有密钥且必须保证密钥的秘密性。对称密码体制虽然运算速度快、计算效率高。但是，它的安全性取决于两个方面的因素：一是使用的加密算法，二是加密密钥。对称密码体制使用的加密算法鲁棒性好，整个系统安全性高；进行加密的密钥的秘密性高，整个系统也更加安全。这两个因素造成了系统较为脆弱、易于被攻破。随着通信规模的扩大，用户数量的增多，密钥的分配问题变得更加复杂，密钥量成倍地增长，建立安全信道传递密钥的问题表现得也越来越明显[8]。此外，它并不能用于签名和验证。

公钥密码体制中，非法分子无法通过加密密钥使用一定的算法推断得到解密密钥，保证了密钥的安全性。公钥密码体制的安全性是基于数学困难问题的[9]。但是，公钥密码体制存在着公钥和主体身份认证的问题[10]，即公钥真实性问题。传统公钥密码体制中，公钥是通过单向哈希函数对私钥进行哈希运算得到的，具有随机性，公钥和主体信息不具备相关性。因此，公钥和主体身份需要通过认证机制来实现[11]。

为了解决在公钥密码体制中的公钥管理问题，保证信息在网络上的安全传输和使用，运用公钥密码理论和技术，构建了一个为广范围应用提供各种安全服务的安全基础设施——公钥基础设施（PKI）[12]。PKI借助颁发给主体的数字证书，通过证书管理机构（CA）[13]对公钥主体身份的合法性进行审核。它发展成熟，不但不同公司开发推出了PKI产品，而且它和其他技术相结合应用到了实际生活的方方面面。但是，它内部是通过证书服务器管理证书[14]，涵盖了证书的整个使用生命周期，包括了证书从无到有，从有到无的管理策略和机制，系统庞大，操作复杂。

1984年，RSA算法的提出人之一，密码学家Shamir提出了基于身份的加密（IBE）思想[15]，采用和主体信息相关的任意字符串作为公钥，私钥通过私钥产生中心（PKG）产生。与传统的公钥加密技术不同的是，IBE通过PKG使用随机算法产生系统参数。当PKG公布系统参数后，主体可以采用系统参数产生任意主体的公钥，然后使用公钥加密信息得到密文或者进行身份认证。当主体需要使用私钥进行解密或数字签名时，向PKG发送申请，由PKG产生与主体身份信息相对应的私钥。因此，IBE不需要将用户身份的审核交付给第三方机构。信息交互双方可以直接进行安全、保密、可靠地通信和信息交流。自然而然地也就不需要通过CA来管理和维护大量的用户的数字证书，避免了繁琐的证书管理。但是，IBE方案中，PKG的权利过于集中：一方面秘密保管主密钥，另一方面合成用户的私钥。因此，IBE方案天生存在着的密钥管理问题就是：用户密钥托管。此外，由于托管问题，随之而产生的密钥安全分发，身份验证等问题，也限制了IBE在实际中的应用。因此，研究IBE的密钥管理问题对将IBE应用于实际当中，具有安全意义和实用价值[16]。

1971年，Ray Tomlinson发明了电子邮件，改变了不同地域的人们之间信息传递和信息共享的方式。网络扩大了电子邮件的使用范围，丰富了电子邮件的内容，加快了电子邮件传递的速度，越来越多的用户使用电子邮件进行日常的信息交流，工作求职等。但是，网络的开放性使得电子邮件在传输过程中受到多方面的安全攻击，研究安全电子邮件具有经济实用价值。目前，采用PKI技术保护电子邮件安全，主要有两种提供电子邮件安全服务的方法：PGP[17]和S/MIME[18]。如前所述，PKI存在证书管理方面的劣势，实际部署和使用有一定的困难性和复杂性。基于身份的加密无需通过证书绑定用户的身份和公钥，不需要第三方机构CA进行数字签名。将IBE运用到电子邮件中，保障电子邮件安全是一个新的研究方向[19]。

1.2 国内外研究现状

1.2.1 IBE密钥管理研究现状

Shamir提出IBE的思想后，引起了密码学界研究学者的广泛关注，对该方面进行了各个密码学方面的研究。2001年，Boneh和Franklin提出了第一个在随机预言模型下具有选择密文攻击安全的实用的IBE方案[20]。此后，不同的IBE方案的构造也是基于他们提出的IBE方案。

但是，Boneh和Franklin提出的方案，一方面，由于采用有限域上的的椭圆曲线构造的双线性对，计算效率低；另一方面，由于方案的安全性是在ROM[21]下证明得到的，它的安全性有待商榷。后来，研究学者针对这两方面的问题，提出了不同的IBE方案，如不采用ROM的具有选择身份安全的IBE方案[87]，模糊IBE方案[88]，具有等级结构的基于身份加密[44]方案等。在IBE方案多方面不断发展的同时，其自身存在的问题，密钥托管和用户密钥安全分发等密钥管理问题，也越来越受到人们的重视。

对于IBE的密钥管理问题，Boneh和Franklin提出通过Shamir[22]的门限方案实现系统主密钥的共享，以此来降低PKG泄密导致用户私钥不安全性问题。该方案中，一个PKG产生的主密钥分给了多个位于不同位置上的个PKG，私钥可以通过门限方案求和计算得到，该方法只可以解决一个PKG的密钥托管问题。在有N个PKG的应用中，每个可信中心都拥有n个子秘密，对于系统来说，负担太重。2002年，Chen et al.提出的多方共管方案[23]，通过使用n个PKG共同合作，最终用户合成自己的密钥的方法来解决PKG的密钥托管问题。但是，在它们的方案中，当用户进行非法使用时，可信中心之间并没有采取应对的措施。2003年，Gentry提出了一个基于证书[24]的安全私钥分发方案，它使用了用户提供的秘密信息，但是它已经丧失了基于IBE方案的优势。同年，Al-Riyami & Paterson提出了在使用用户提供的秘密信息的同时，无需使用证书的方案，即无证书方案[25]。但是，由于该方案中的公钥是用户产生的，没有提供任何认证方式，因而，只能提供隐含的公钥认证。并且，任何使用该公钥的参与者也无法确信这个公钥是否真正属于这个用户。2004年，Lee. B和Boyd C等人提出了采用多个可信中心[26]来解决用户私钥的安全分发，该方案的构造过程复杂，计算用户私钥和通信开销大，并且系统不能抵御外部敌手的仿冒攻击和PKG造成的内部攻击。2007年，Goyal提出了一个降低IBE中PKG信任等级的方案[27]，对于PKG可能存在的不规范行为进行了严格管理，一旦PKG恶意产生或者分发一个用户的私钥时，就会被系统捕获识别和处理，不需要通过引入多个PKG来解决IBE的密钥托管问题。2009年，Chow提出了一个使用匿名密钥分发（Anonymous Key Issuing，AKI）协议系统架构来保护用户身份的机密性，从而解决密钥托管问题[28]。

1.2.2 IBE应用研究现状

IBE简化了密钥的管理，在PKI中，公钥保存在一个大的数据库中，需要CA来绑定主体身份和公钥，并加上公钥的数字签名，构成数字证书，通过数字证书来管理密钥。IBE除了简化公钥的管理外，还有其他方面的应用，如密钥撤销和密钥代理[20]。

通过在公钥字符串中加入时间信息，设置公钥的有效使用日期，进而实现公钥的撤销（Public Key Revocation）。例如，用户ZhangSan和LiSi使用电子邮件进行通信时，当ZhangSan给LiSi发送电子邮件时，ZhangSan使用LiSi@company||current-year作为加密邮件明文信息的公钥。当LiSi需要解密邮件时，只可以使用当年的私钥恢复明文。当私钥在该年的有效期过后，PKG发送给LiSi一个新的私钥。在PKI中，当用户更新密钥的时候，其他用户需要从CA获取新的数字证书。而在IBE中，通过在公钥中加入时间成分，实现了用户的私钥撤销管理。设置用户对私钥使用的时间区间，当用户更新密钥时，其他用户也不需要获取该用户新的数字证书。对于公司来说，该方法具有更高的灵活性和可操作性。假如，该公司使用LiSi@company||current-date作为该员工的公钥，即在公钥中加入当前日期。当LiSi从公司离职后，该公司的PKG就会停止给LiSi的公钥分发私钥。ZhangSan在使用LiSi的公钥时，不需要频繁地同第三方机构沟通。此外，ZhangSan可以在公钥中加入未来的某个时间成分，那么Lisi在解密的时候，只可以使用指定日期的私钥进行解密。有研究人员对此类应用进行了研究[93]。

IBE方案可以应用于密钥代理中，这个应用假设某一位用户是PKG。首先，该用户启动整个系统，产生系统中的关键参数和该用户的私钥。该用户将关键参数提交给某一个可信的第三方，并获得与之对应的证书。当系统中的其他用户加密时，先要从该用户处获得证书（包含系统参数），才能进行解密。以下介绍两种代理：笔记本代理和职责代理。假设用户ZhangSan是PKG，运行初始化算法，产生该IBE系统的系统参数（sysparams）和主密钥（masterkey）。ZhangSan的公钥和私钥分别是sysparams和masterkey，同时，ZhangSan从CA处获得一个对应于sysparams的证书，masterkey只有ZhangSan知道。

笔记本代理。当LiSi想要发送加密邮件给ZhangSan时，他首先通过获得ZhangSan的证书，然后使用ZhangSan@company.com||current-date加密邮件信息。ZhangSan拥有私钥，可以直接解密得到明文。假设ZhangSan因公出差一周，它可以在笔记本上为这七天设置七个不同的私钥，即使笔记本失窃，非法分子只能攻破这七天的私钥，也无法攻破主密钥。

职责代理。假设ZhangSan有几个不同的助理，分别负责不同的工作，如人力资源，采购等，ZhangSan可以为这些助理分配对应于本职工作的私钥。当其他用户发送邮件时，使用邮件的主题内容行作为公钥进行加密。当他把邮件发送给ZhangSan时，只有拥有该主题行对应职责的助理才可以读取该信息，其他助理不具有阅读权限。

斯坦福大学，Shamus Software和Voltage Security提供了实现BF-IBE的代码库。坦福大学的PBC库和Shamus Software的MIRACL是免费开源的，主要用于学术研究，而Voltage Security公司提供的是具有工业标准的IBE代码库。根据斯坦福大学提供的PBC库，研究人员在Linux操作系统下实现了基于IBE的安全电子邮件系统[92]。Voltage Security公司，开发安全平台，提供安全服务[94]，现已被惠普（HP）公司收购。研究人员使用MIRACL实现IBE方案[103]及其应用[97][102]，把PKI和IBE相结合实现邮件加密[101]，将IBE方案用于电子邮件系统[96]，电子签章系统[95]，即时通信[100]和保密电话[104]中。文献[98]中给出了IBE其他方面的应用。

1.3 主要工作和研究内容

本文针对IBE中存在的密钥管理问题进行了研究，详细分析了MIRACL提供的基于身份加密算法，并模拟实现了基于身份加密的安全电子邮件。主要工作内容如下：

（1）本文对基于身份加密的密钥管理方案进行了介绍，比较分析了不同方案的优缺点。

（2）对Boneh和Franlin提出的基于秘密共享密钥管理方案，指出了其存在的问题：并未完全解决用户私钥托管问题，无法抵抗多于t-1个PKG的合谋攻击，PKG发送的部分主密钥的真实性。针对Boneh和Franklin详细IBE方案，结合Feldman的可验证秘密共享方案（Verifiable Secret Sharing，VSS）的思想，运用盲签名技术，加入可信中心，提出了一种改进的密钥管理方案，并应用于加密和解密中。改进的方案中，用户参与私钥的生成。方案中加入了用户选择的信息，建立了用户部分私钥的安全传输信道；第三方信任机构的加入，对身份进行签名和认证，实现密钥的撤销管理。同时，对改进的方案安全性进行分析，给出了正确性分析证明，并将其同其他同类型的密钥管理方案进行了比较，得出改进方案的密钥管理更全面、正确。

（3）针对Lee.B等人提出的单个PKG和多个KPA方案，指出了其存在：PKG伪造用户身份攻击，非法分子伪造KGC或者KPA对部分私钥进行签名，身份认证次数多和物理故障，提出了一种改进方案，引入第三方信任机构，通过签名和设置有效期，监督KGC，KPA和用户的行为，减少了身份认证次数，对攻击和物理故障采取了应对措施。分析了方案的安全性和正确性，与其同类方案相比，该方案更全面。

（4）详细介绍和分析了MIRACL中提供的IBE具体实施方案中的技术路线和算法流程，将BF-IBE和对称加密算法AES结合，设计了安全电子邮件，使用VC++6.0模拟了IBE安全电子邮件系统通讯过程。

1.4 结构安排

论文共分为五章，结构组织如下：

第一章，绪论，介绍了网络信息安全的基本知识，采用的加密体制，公钥密码体制中存在的密钥管理问题，PKI通过证书解决公钥密码体制密钥管理存在的问题，IBE中采取的密钥管理方案和IBE的应用研究，现有的安全电子邮件解决方案和IBE安全电子邮件方案。

第二章，基于身份加密体制的基础理论和技术，详细介绍了密码学上经常使用的椭圆曲线，椭圆曲线密码学中的困难问题，攻击方法和防御手段，基于身份加密中使用的双线性映射，Diffie-Hellman假设和Diffie-Hellman问题，BF-IBE的基本方案，详细方案算法和具体实施方案，PKI以及IBE和PKI的比较。

第三章，基于身份加密密钥管理方案设计，详细介绍了基于秘密共享方案，多方共管方案，基于证书方案和基于无证书方案，L.Bee的安全私钥分发方案，分析了不同方案中存在的问题。针对Boneh和Franklin提出的基于秘密共享方案，结合Feldman-VSS方案的思想，运用盲签名技术，加入可信中心，提出了改进方案，并将其运用于加密和解密应用中。分析了方案的安全性，并给出了方案的正确性分析证明，最后将其与其他同类型的方案进行了比较。对于L.Bee的安全私钥分发方案中存在着的问题，提出了解决方案，并给出了正确性和安全性分析。

第四章，基于身份加密的安全电子邮件系统。分析了电子邮件的通讯原理，电子邮件存在的安全隐患，安全电子邮件解决方案，详细分析了PKI和S/MIME技术相结合的安全电子邮件方案。分析了MIRACL提供的BF-IBE方案具体实施方案的算法设计和工作流程，并将其运用到PKG服务器设计，客户端设计和电子邮件客户端的设计中，模拟了PKG服务器，客户端和电子邮件客户端的通讯过程，并对该方案的安全性进行了分析。

第五章，总结与展望。总结了本文的研究内容以及心得体会，并提出进一步的研究和下一步的开发任务。

第二章 基于身份加密体制的基础理论和技术

2.1椭圆曲线密码学

随着用户对产品安全要求的提高，RSA[29]加密时使用的密钥的要求会随之提高，这将增加应用程序的处理负担。但是，若采用相同的密钥长度，椭圆曲线密码体制[30]的安全性和计算速度比RSA好。

通常，在密码学研究和实际应用中，采用的是一类特殊的椭圆曲线。该类椭圆曲线具有一些优点，便于其在密码学上使用，更有利于在实际中推广应用。本节将对一般的椭圆曲线进行介绍，然后对上的点的运算以及性质进行介绍，并对攻击椭圆曲线离散对数问题进行了分析，介绍了一些提高安全性的措施。

2.1.1 椭圆曲线的定义和运算

在域上定义的椭圆曲线[30]是由满足如公式（2-1）所示方程的点的轨迹。

|  |  |  |
| --- | --- | --- |
|  |  | （2-1） |

其中，，，的形式如公式（2-2）所示：

|  |  |  |
| --- | --- | --- |
|  |  | （2-2） |

中的，，，的计算如公式（2-3）至（2-6）所示：

|  |  |  |
| --- | --- | --- |
|  |  | （2-3） |
|  |  | （2-4） |
|  |  | （2-5） |
|  |  | （2-6） |

当的特征值不是2或3时，，，曲线方程是。当的特征值等于2时，若，，，则曲线方程是；若，，，曲线方程是。当的特征值等于3时，若，，，曲线方程为；若，，，曲线方程是。

以上讨论的是在一般域上定义的椭圆曲线，对于定义在有限域上的椭圆曲线上的所有点的集合（包括一个无穷远点）。内的两点相加后的第三点也在内，因此，是一个交换群[31]。在下文中指无穷远点。

对于：，的特征值[32]不等于2或者3，具有如下性质：

1. ，，是单位元。
2. 若，则，即，。
3. 设，，其中，，公式（2-7）给出了的，运算方法：

|  |  |  |
| --- | --- | --- |
|  |  | （2-7） |

1. 设，若，则，公式（2-8）给出了的，运算方法：

|  |  |  |
| --- | --- | --- |
|  |  | （2-8） |

设中点的数目为，称为在上的阶，可得范围[33]。若是的特征值，，如果满足：（1）且；（2）是奇数且满足，(a)；(b)，；(c)，之一；（3）是偶数且满足，(a)；(b)，；(c)，条件之一，则。

对于点乘运算，记作，，，它对于椭圆曲线上的执行时间有主导作用。

在实际的加密中，通常采用两类椭圆曲线[34]：

（1）：，其中素数。

（2）：。

2.1.2 椭圆曲线安全性分析

椭圆曲线离散对数问题（Elliptic Curve Discrete Logarithm Problem, ECDLP）：设，阶的点，，找到一个数，使得。

最原始的解决ECDLP问题的是采用穷举搜索法，通过计算直到找到满足条件的。攻击ECDLP除了一般的穷举搜索法外，还有大步小步法，法，加速的，法等一般攻击方法，以及一些特殊的攻击方法，如异常曲线，对攻击等[35]。目前，最有效的解决ECDLP问题的方法依然是在指数时间内并行进行运算的方法[36]。

为了防御多种多样的攻击算法，确保使用的椭圆曲线具备较高的安全性能。除了提高外界的防御措施外，在构造椭圆曲线时，必须严格选择参数。其中一种方法是采用随机算法产生具有某种特性的椭圆曲线，此外，还可以采用CM（Complex Multiplication）[37]等方法。采用随机算法产生特定要求的椭圆曲线时，在上的椭圆曲线，其中，一定要满足：（1）可以被一个大素数（）整除（2）必须确保（）。通过这样的参数设置，可以防御异常曲线等形式的攻击，并且可以确保是稳固的。为了对抗GHS[38]等攻击，只需要选择在（）上的曲线即可。

2.2 双线性映射

阶和阶，是一个大素数。若群和之间的映射满足如下性质，则构成可容许双线性映射（Admissible Billinear Map）：

1. 双线性性。对于，，满足。
2. 非退化性。由于和是素数阶的循环群，所以若，则。
3. 可计算性。对，存在算法在一定时间内计算出。

其中，在选取满足上述三个条件的群，构建两个群之间的时，可以是椭圆曲线上的点组成的集合的一个子群，是在有限域上的乘法群的一个子群，在这两个群之间的Weil对[39]可以用来构造一个可容许双线性映射。但是，在实际应用中，Weil对的计算效率并没有Tate对高，所以为了提高计算效率，在计算实施上使用的是Tate对[40]。

2.3 Diffie-Hellman假设及相关问题

1.Diffie-Hellman相关问题

Difie-Hellman问题（Difie-Hellman Problem，DHP）：设是一个大素数，，，是两个大的随机数，给定和，求值。

计算性Diffie-Hellamn问题（Computatonal Diffie-Hellman Problem，CDHP）：设，，给定，计算。



判定性Diffie-Hellman问题（Decision Diffie-Hellman Problem，DDHP）：对，给定，判断。

双线性Diffie-Hellman问题（Bilinear Diffie-Hellman Problem，BDHP）：对，给定，求得。

判定性双线性Diffie-Hellman问题（Decision Bilinear Diffie-Hellman Problem，DBDHP）：对，判断与的值是否相等。

2.Diffie-Hellman假设

双线性Diffie-Hellman（Bilinear Diffie-Hellman，BDH）假设：对于足够大的，算法解决在上，对于的BDHP的概率是。

假如对于任意的多项式时间内的算法[41]和任意多项式，有不等式成立，则称是满足BDH假设的，通过算法产生的群是BDH困难的。其定义形式如公式（2-9）所示：

|  |  |  |
| --- | --- | --- |
|  |  | （2-9） |

3.BDH参数产生器

BDH参数产生器是一个随机化的算法，将其记为，算法描述：

（1）接收一个参数；

（2）多项式时间内运行；

（3）得到，阶和阶，。

2.4 单向散列函数

哈希函数，是一个压缩函数，它将任意不定长度的输入值哈希成一个固定长度的结果输出，公式（2-10）给出了哈希函数的一个形式化定义：

|  |  |  |
| --- | --- | --- |
|  |  | （2-10） |

其中，即散列函数；代表输入值的集合；代表输出值的集合。

哈希函数在实际生活，计算机以及密码学中，都有广泛的应用。如，当从网站上下载信息或者软件时，可以根据信息或者软件提供者给予的哈希码来判断信息和软件的真实性。

密码学上使用的哈希函数具有一定的特定。设有哈希函数，输入值，，对应的哈希输出值，，若的计算是高效的，并且满足如下所述的三个性质，则称为加密哈希函数，其输出值的长度通常在128bits~512bits。

1. 如果非法分子获取了任意输出值，他无法通过哈希函数找到与该输出值对应的输入值。即，对，找到，使得是计算上不可行的。
2. 对于任意的输出值，哈希函数的输入值集合中不存在两个与其对应的值。即，对，，找到一个，其中，，使得成立，在计算上是困难的。
3. 对于不同的输入，无法得到相同的输出。即，若，使得成立，在计算上是困难的。

哈希函数用在信息认证（Information Authentication），多目标消息的身份验证（Authentication of multi-destination messages），不可否认性（Non-repudiation），密码识别（Identification with passwords）和基于哈希函数的加密算法（Encryption algorithms based on hash functions）等[42]。

2.5 基于身份加密方案

2.5.1 基于身份加密方案介绍

IBE方案由Setup，Extract，Encrypt，Decrypt组成，记作=。Setup是系统初始化，Extract是用户私钥提取，Encrypt是加密算法，Decrypt是解密算法。其中，Encrypt和Decrypt具有一致性。

Setup执行后，产生和。在Extract，Encrypt和Decrypt中都作为输入参数的一部分，分别得到，，。在整个系统中是公开的。而作为Extract中决定用户的关键，必须秘密保管。

Extract是对身份为的用户产生对应的。通过用户提供的，得到，然后将和进行运算，得到。

Encrypt算法使用加密，得到。输入，和，通过一些代数运算得到。即Encrypt提供了一个从到的可行算法，使得经过Encrypt后，变成不易被破解的。

Decrypt算法使用解密，得到。输入，和，通过一些代数运算恢复。Decrypt提供了一个从到的可行算法，使得经过Decrypt后，变成。

2.5.2 BF-IBE基本方案

BF-IBE基本方案采用的双线性映射是椭圆曲线上的Weil对，并且需要保证在群上对于任意的变量的CDHP是困难的。在BF-IBE，在随机预言模型上证明具有语义安全性。设是满足BDH假设的BDH参数发生器，给定一个安全参数：

**Setup**：运行，得到（大素数），阶，阶，。任意挑选，满足。选取，。选取加密哈希函数，。其中，，。主密钥为。系统参数为。

**Extract**：对于，。计算私钥，其中是主密钥。

**Encrypt**：将作为公钥加密，先计算，再选取，密文为，，其中，可以在加密前计算，只需计算一次。

**Decrypt**：用作为公钥加密得到的，通过与该对应的。由，恢复。

Encrypt和Decrypt具有一致性。公式（2-11）给出了具体的推导过程：

|  |  |  |
| --- | --- | --- |
|  |  | （2-11） |

2.5.3 BF-IBE详细方案

BF-IBE详细方案也是采用的双线性映射是椭圆曲线上的Weil对，并且需要保证在群上对于任意的变量的CDHP是困难的。在随机预言模型上具选择密文安全性。设是BDH参数产生器，安全参数。BF-IBE详细方案算法描述如下：

**Setup**：

Step 1：运行，得到（大素数），阶，阶，。随机挑选，使得。

Step 2：随机挑选，得到。

Step 3：挑选，，，。

其中，，。主密钥为。系统参数为。

**Extract**：选定一个字符串，作为加密的公钥。

Step 1：计算。

Step 2：计算。

**Encrypt**：用加密：

Step 1：先通过哈希函数得到，即。

Step 2：随机挑选。

Step 3：通过哈希函数得到，即。

Step 4：依次运算，，，，其中，，，，。公式（2-12）给出了的组成：

|  |  |  |
| --- | --- | --- |
|  |  | （2-12） |

**Decrypt**：若用加密得到的，如果，则拒绝解密；反之，用私钥解密：

Step 1：通过，，使用公式得到。

Step 2：通过，使用公式得到。

Step 3：得到。计算，判断与之间的关系。如果拒绝恢复，反之，执行Step4。

Step 4：输出对应的。

Encrypt和Decrypt具有一致性，证明方法同BF-IBE基本方案相同。

2.5.4 BF-IBE具体实施方案

BF-IBE的具体实施中使用了有限域上的椭圆曲线（），记作；对Weil对进行了改造，使其满足非退化性，然后作为双线性映射；将计算的哈希函数分解成来两步来执行。在随机预言模型下，该方案具有选择密文安全性。系统初始化阶段中的生成和选取算法，用户私钥提取算法，加密算法和解密算法同BF-IBE具体方案一样。本节主要介绍BDH参数生成器，用户私钥提取方法中的改进环节和参数选择要求。

初始化阶段，BDH参数生成器执行过程如下：给定一个安全参数，运行BDH参数生成器随机产生一个位素数，循环计算求得满足条件的部分系统参数：，，的最小素数，将两者之间的关系记作。群是上椭圆曲线：的点群的阶的子群，是的阶的子群。双线性映射是改进后的Weil对。

用户私钥提取中，使用的哈希函数，分解两步，先采用哈希函数，然后使用。其中MapToPoint执行方式的形式化描述如下：

1. 假定已经有一个点；
2. 计算，，，其中；
3. 最后输出。

2.6 公钥基础设施和基于身份加密的对比分析

公钥密码体制的出现，使得信息与通讯技术（Information and Communication Technology，ICT）[43]更加安全。公钥密码体制的核心是加密和解密使用不同的密钥，公钥加密，私钥解密。同对称密码体制相比，一是用户在进行信息通讯时，不再需要进行密钥的交换；二是需要维护的密钥量减少。公钥密钥体制中，由于公钥和用户的身份之间并不存在相关性，在使用过程中，通信双发就无法确认彼此的身份，也就无法保证网络上活动的安全性和不可否认性。因此，公钥密码体制迫切需要一种方案来解决公钥的管理问题，促使其更好地发展。目前，基于信任服务的PKI和基于信任服务的IBE是两种解决办法。PKI发展成熟，体系完善，IBE仍然处在研究和探索阶段。PKI通过数字证书绑定公钥和用户，实现对公钥的认证管理。IBE则不需要借助于证书来管理公钥。繁琐的证书管理，高昂的资源要求和复杂的部署实施越来越限制着PKI的发展应用，而IBE的优势表现的越来越明显。

2.6.1 公钥基础设施

公钥基础设施是一个安全框架，它充分利用了公钥密码体制的理论和技术，为在因特网上进行虚拟活动的用户创造一个安全可信稳定的环境，使得用户可以透明地进行信息加密和数字签名活动。PKI对主体的身份和公钥进行签名，构成了数字证书。它依靠用户数字证书，实现了对该用户身份对应的公钥的管理。

PKI中最主要和最关键的组成部分是证书管理机构（CA）。它十分特殊，在它提供的服务范围内，所有的实体都信任它，并间接通过其他方式获取更大范围的用户的信任。CA的主要功能可以分为两大板块：密钥管理和证书管理。除此之外，对于CA的跨域操作，必须具备交叉认证的功能。另外，PKI为方便用户查询证书，提供了在线查询服务；设立了专门的密钥备份及恢复系统；具备应用程序接口系统，保证了应用程序和PKI的交互。PKI解决了应用系统中身份认证，数据安全和电子签名三大类问题。

数字证书中维护的信息量大，使用过程繁琐。比如，在用户和CA通信，审查身份时，并不是仅仅查询和验证该用户证书的直接发行者。对于非最高层CA发行的证书，用户还需要从高层CA处获得给他发行证书的CA的证书，验证发行者CA身份的合法性。根据层级信任链条，确定给他发行证书CA的身份的真实性，从而确定签名的有效性，证实用户的身份。以上的分析是假定没有涉及到更新或者撤销数字证书，实际操作中，还需要查询证书撤销列表。在证书撤销列表中维护的信息，也存在着繁琐和复杂的身份审核。

PKI中，用户使用数字证书，可以对公钥所属者的身份进行判别。但是，其使用流程复杂，消耗时间多。此外，对于PKI来说，管理和维护数字证书，负担重。随着系统规模的扩大，PKI的负担更重。

2.6.2 公钥基础设施和基于身份加密的比较

PKI中对于密钥的管理，是通过一系列机构的有机配合完成的。PKI的建立对硬件设备，通信设备，网络带宽要较高的要求，需要耗费大量的人力，财力，物力。数字证书的整个生命周期中，累积的资源消耗多。IBE中的用户身份和公钥不再通过媒介——数字证书来绑定，身份的认证也无需委托给可信第三方。它没有繁琐的证书管理流程，具有更好的应用前景。PKI和IBE存在着相同点，也存在着差异。两者之间的相同点和不同点在表2-1中给出：

表2-1 PKI和IBE比较分析表

|  |  |  |  |
| --- | --- | --- | --- |
|  | | PKI | IBE |
| 相  同  点 | | 公钥密码体制；公钥加密或验证，私钥解密或签名 | |
| 由公钥无法推导出私钥；由公钥和密文，无法得明文 | |
| 安全性都建立在数学困难问题上 | |
| 用户身份都需要认证，在PKI中，用户身份通过CA认证；在IBE中，用户身份通过PKG认证 | |
| 不  同  点 | 密钥对  生成时间 | 同时  产生 | 无需生成公钥，  私钥可以在用时产生 |
| 密钥对  生成方式 | 一是用户自己选取；  二是由CA产生 | 公钥通过身份信息产生，私钥由PKG产生 |
| 密钥对  生命周期 | 长 | 短 |
| 公钥认证方式 | 数字证书 | 无 |
| 公钥撤销方式 | CA的证书撤销列表 | 用户身份||生命周期 |
| 公钥存储方式 | 证书库 | 无需存储 |
| 私钥传输方式 | 若用户自己选取，则无需传输 | 建立安全的信道传输私钥 |
| 系统参数  发布形式 | 所有参数作为公  钥的一部分 | 公开参数由  PKG发布 |
| 可信第三方  工作方式 | CA必须在线，并且可以查询系统中每个用户的状态 | PKG只是在系统建立阶段提供服务 |

表2-1中分析的内容表明，IBE在公私钥对的产生过程，公钥的认证、撤销、存储，系统参数发布以及可信第三方工作方式上具有优势。它不需要通过数字证书来管理用户的公钥，不需要第三方可信机构始终在线服务，具有很好的研究价值和应用前景。

2.7 本章小结

本章分别对椭圆曲线；双线性映射；哈希函数，Diffie-Hellman问题；基于身份加密方案的组成，BF-IBE的基本方案，详细方案和具体实施方案，PKI进行了介绍，列表分析了IBE和PKI，为本文后续章节奠定了理论基础。

1. 基于身份的密钥管理方案设计

基于身份加密的系统中，PKG不但需要对用户身份的合法性进行检查，而且要建立和合法用户之间展开交互信息的安全信息通道。PKG的权利过于集中，一方面会造成PKG负担过重，另一方面PKG被攻破造成用户私钥泄露。在基于身份加密的方案的构建中，PKG是诚实的，具有最高的信任级别，系统中所有的参与者相信它的所有行为。当PKG非法操作时，它可以直接利用合法用户的身份，私自合成私钥解密信息或者进行其他非法活动。PKG和用户之间进行身份认证的通信开销也会随着系统规模的扩大而增加，这限制了IBE在大规模环境中的应用。在现实的通讯环境中，建立安全的信道保证用户私钥的安全分发，类似于对称加密体制中建立安全的信道保证通讯双方交换密钥，这也限制IBE的推广应用。因此，提出安全的基于身份密钥管理方案，减轻PKG的负担，是十分必要的。此外，密钥撤销管理在实际应用中也是需要考虑的。

目前常用的解决办法是对PKG进行分权处理，分别为：多PKG解决方案，基于证书方案，基于无证书方案，降低PKG信任等级方案和匿名密钥分发方案等。多PKG方案采用将IBE中的密钥管理问题分散到多个PKG中，例如Boneh和Frankin的基于秘密共享方案和Lee.B等人提出的使用多个KPA来解决密钥托管问题。本章首先分析和介绍了基于身份加密的密钥管理方案，然后对基于秘密共享方案和Lee.B的安全私钥分发方案进行了深入研究分析。

3.1基于身份加密密钥管理方案分析

3.1.1 基于秘密共享方案

基于秘密共享共享方案，即门限密钥分发方案。2001年，Boneh和Franklin在他们提出的加密方案中采用分布式的密钥产生中心（PKG）来保护主密钥，但是并没有对系统中用户的私钥的隐秘性进行保护。在它们的方案中采用了Adi Shamir的门限秘密共享方案，系统中引入个PKG，通过秘密分割成份，每个PKG拥有，用户私钥是大于等于个PKG，通过公式计算得到，其中是拉格朗日系数，。方案的详细构造过程如下：

在秘密分发初始化阶段，选取一个有限域，其中一个大素数，并在上选择，将发送给个PKG，公开。在分发阶段，在上随机选取，，构造一个如公式（3-1）所示的次多项式：

|  |  |  |
| --- | --- | --- |
|  |  | （3-1） |

部分系统主密钥（），并将其分发给系统中的各个参与者PKG。当进行私钥提取时，任意个PKG先计算（），用户收到各个密钥分片后，计算对应的私钥。

该方案不需要使用零知识证明，具有鲁棒性。将PKG保管主密钥带来的密钥托管问题，通过门限秘密共享方案，采用多个PKG来分散主密钥，就可以解决。但是，在这个方案中，所有的PKG的地位和扮演的角色是相同的。当用户需要获得私钥时，分别同个PKG交换信息：用户发送ID给PKG；PKG验证ID，计算，发送之；用户接收，合成。

这个过程造成了两方面的系统负担：

（1）大量的哈希运算以及其他的代数运算，使得计算效率变低，计算成本增高。

（2）个PKG和用户之间建立安全信道，进行信息验证和分发，提高了对网络传输速率、网络带宽以及PKG的响应速度等方面的要求。此外，如果多于个子PKG蓄意勾结，攻击系统，整个信任PKG的用户都将面临不可估量的损失。所以，主密钥的分割，并没有提高系统的安全性，用户的私钥依然面临着被泄露和恶意使用的风险。

另外一方面，是由于Shamir方案本身存在的问题，它的构建基础取决于方案的参与者和子秘密共享者都可信。如果秘密分发者有欺诈行为，分发虚假的子秘密，即使所有的子秘密共享者共同合作，也无法恢复出IBE方案中的主密钥。如果子秘密共享者发送虚假的子秘密，最后也无法恢复主密钥。

3.1.2 多方共管方案

2002年，Chen et al.提出的多方共管方案中通过个PKG来解决IBE的密钥托管问题。在该方案中生成用户的私钥时，增加了一个字节的字符串，同时对应一个虚拟的可信中心，该可信中心的公钥和该私钥之间存在着对应关系。简单构造过程描述：对于系统的每个PKG，都有自己的主密钥和（），PKG通过公式，和用户的私钥建立关系。当身份为ID的用户申请获得私钥时，同个PKG之间进行通信，计算得到，。给定用户选定一个字节的字符串b=，通过公式计算得到该用户的私钥。对应于该私钥的虚拟中心的主密钥和公钥分别是：

|  |  |  |
| --- | --- | --- |
|  |  | （3-2） |

该方案产生了个不同的公/私钥对，从理论上讲，用户自由选择部分私钥生成用户的私钥的方法来避免用户私钥的泄露，可以防止任意个PKG的恶意合谋攻击。但是，该方案存在四个方面的问题：

第一：个的分发操作是彼此无关，相互独立的。PKG通过公式计算得到，并传送给用户，仅仅只是的组合的一半，用户最后合成的真正的，还取决于用户选定的一个自己的字符串。然而，这个字符串是用户秘密保管的，不会公开。在实际应用中，只有当PKG确保用户会正确使用它分发的密钥时，用户才能从PKG那里得到自己申请的部分私钥。如果，一个环境中存在多个PKG时，不同的PKG对用户的“意见”不统一，即对于不同的，对应的给定使用方法各不相同。那么，对于用户来说，他无法确定的使用方法是按照哪一个PKG的要求，即的运用方法是具有争议的。

第二：该方案中没有针对用户私钥的管理方法，也没有抵御用户非法使用私钥的应对措施。虽然系统假定和属于个不同的PKG，但是系统中的私钥脱离了某个PKG后，使用限制和操作方式，都不在PKG的管辖范围内。

第三：在用户合成私钥的时候，使用的算法非常简单以及各个PKG计算的并行性，攻击者可以通过独立攻击每一个PKG，获得了一个用户的部分私钥，最后通过累加得到用户真正的私钥。

第四：存在着用户身份认证次数频繁的问题，将会造成系统负担过重。

3.1.3 基于证书方案

2003年，Gentry提出一个新颖的解决用户私钥共享问题的方案，该方案通过用户选择秘密信息的方式解决用户私钥托管问题，即基于证书的方案。系统中加入了一个第三方信任权威，保存着整个系统的关键信息：和。系统中用户得到私钥的计算流程：

（1）用户首先随机选择一个秘密并计算他的公钥，然后该用户将ID和发送给可信中心，申请获得证书。可信中心验证用户的身份后，计算，，其中代表有效期，最后计算得到证书，将证书发布并发送给用户。

（2）通过证书，用户

（a）计算；

（b）计算。

在实际应用中，当用户加密，发送时，依次计算，，通过双线性映射得到，任意挑选，计算。对方获取时，恢复明文

。

Gentry的方案提供了一个基于身份加密的密钥管理的方案。该方案解决了用户的托管问题，使得基于身份的加密方案更安全。同时，在可信中心和用户的通信中，不需要通过安全通道，通过公开渠道发送或者发布。但是，它已经变成了一个基于证书的方案，失去了基于身份加密的优势。虽然方案中采用了来管理私钥的有效期，但是，它仍然存在密钥撤销问题。私钥的产生是通过用户和可信第三方权威共同合作产生，但是，在私钥产生的过程中，并没有设置私钥的有效期。如果没有证书，通信双方中的发送者无法确定是否是正确的接收者的公钥。

3.1.4 基于无证书方案

同年，Al-Riyami & Paterson针对Gentry方案中存在的安全问题，采用了无证书的模式，解决了在Gentry方案中存在的问题。该方案的构建过程：假定一个可信中心拥有私钥和公钥。当身份为ID的用户向可信中申请分发私钥时：

（1）用户随机挑选，计算；

（2）建立与可信中心的连接，提供和ID给可信中心，申请分发私钥；

（3）可信中心收到和ID后，（a）审核ID；（b）计算，其中；（c）回馈用户；

（4）用户计算。

加密时，先计算，再随机挑选，通过BF-IBE基本方案中采用的加密流程，得到。假设收到，通过取出被隐藏的信息。虽然，该方案采用用户和PKG合作的方式产生用户的私钥，保证了密钥的隐秘性，但是它仅仅提供了含糊的身份认证。例如，发送方无法确认接收方的是否是正确的，通信具有一定的盲目性和不可控性。只有当发送方和接收方进行了成功的通信后，才可以确认的正确性。当外部敌手利用方案的安全漏洞替换私钥发动攻击时，系统没有设置应对措施。

3.1.5 其他密钥管理方案

具有等级结构的基于身份加密（Hierarchical Identity-Based Encryption，HIBE）[44]引入了多个PKG，每个PKG的管理范围收到了限制，较低等级的PKG的泄密不会对较高等级或者同等级的其他PKG的安全性造成影响，多个PKG分担了系统管理责任和管理范围，减轻了整个系统的密钥管理负担。针对HIBE应用到密钥管理中的研究，其他研究学者提出了自己的解决方案[45,46,64,65]。2007年，Goyal提出了一个降低IBE中PKG信任等级的方案，该方案计算效率高，具有IBE体制的可证安全性。在该方案中，当用户将自己选择的秘密信息交给PKG后，PKG按照方案的执行过程，将传送给合法的用户。PKG不能冒充用户，非法进行操作，违规合成用户的。这是因为，在进行操作时，当伪造的和真实的同时出现，一旦用于解密或者签名，即可以判别出PKG进行了非法操作。2009年，Chow提出了一个使用匿名密钥分发（Anonymous Key Issuing，AKI）协议系统架构用来保护用户身份的机密性。AKI利用了用户身份匿名性的特点，使得PKG无法通过自身自身的私钥，破解或者合成用户最终的私钥。Goyal和Chow提出的方案对于解决IBE的密钥托管问题非常实用，但是缺乏监听机制。

3.2 改进的基于秘密共享方案

3.2.1 改进的方案设计思想

在文献[15]中，Shamir指出IBE方案的安全性取决于以下4个方面：

1. 方案中使用的加密函数的安全性。
2. PKG中存储的主密钥的安全性，它是用户私钥托管问题的关键。
3. PKG分发用户私钥前对用户身份的完全核查。
4. 用户对于的丢失，复制或者未经授权使用采取的预防措施。

本文在2.5.3节中介绍了文献[20]中提出的BF-IBE详细方案，该方案满足BDH假设，在随机预言模型下具有选择密文安全性。在3.1节中，本文详细分析了现阶段解决IBE密钥托管问题的方案。3.1.1节中介绍了文献[20]中提出的解决方案，即基于秘密共享方案，分析了Boneh和Franklin提出的门限共享思想的优点，同时，指出其存在的开放性问题。

在该方案中，提出者假定所有的PKG扮演相同的角色，所以每个PKG都需要单独地对用户的身份进行核查，这必然导致系统开销的增大。文献[75]中指出，对于这个问题可以使一个PKG扮演核查用户身份的角色，其他个PKG扮演签名用户的标识符的角色。但是，这个方法只能解决密钥托管问题，并没有解决安全信道的问题。

对于安全信道的建立，运用盲签名技术，建立PKG和用户之间的安全信道。在文献[69]中，Chaum提出了盲签名的思想。盲签名是一种匿名技术，也是普遍使用的一种盲化技术。不同的研究学者对盲签名方案的研究，应用，分析提出了不同的见解，如在文献[70]中提出了基于双线性对的基于身份的盲签名方案和基于身份的环签名方案，文献[71]中提出基于双线性对的短盲签名方案，文献[72]中给出了基于双线性对的可验证签密方案和部分盲签名方案，文献[73]中针对基于身份加密的代理盲签名方案提出了改进，文献[74]中对基于身份的盲签名方案进行了分析比较。

盲签名技术是一种特殊的数字签名技术[84]。对于消息拥有者Message-Owner和消息签名者Message-Signature，盲签名技术形式化定义如下：

1. 盲化：Message-Owner使用盲因子对消息进行盲化，得到，将发送给Message-Signature。
2. 签名：Message-Signature对进行签名，得到，将发送给Message-Owner。
3. 脱盲：Message-Owner对进行脱盲，得到的签名。

盲签名技术满足一般数字签名的特性，此外，盲签名技术还具有盲性和不可追踪性。

文献[76]中指出，Boneh和Franklin提出的采用门限方案只解决了用户私钥托管问题，而对于用户密钥撤销并没有给出细致的解决办法。在本文的1.2.2节中，关于IBE的应用中，可以在用户的身份表示后面增加时间成分，实现密钥的撤销管理。

此外，文献[77]中指出Shamir的秘密共享方案中假设秘密的分发者和参与者都是诚实的，但是，在实际应用中，很难满足这样的假设。所以，在实际应用中，需要采用不依赖于分发者和参与者都是诚实的秘密共享方案，即可验证的秘密共享（Verifiable Secret Sharing, VSS）方案。

VSS方案分为交互式和非交互的，其中，交互式的VSS方案，效率达不到理想要求，所以，非交互式的VSS得到广泛关注。Feldman的可验证秘密共享（Feldman-VSS）方案[47]和Pedersen的可验证秘密共享（Pedersen-VSS）方案[78]是目前使用最多的两个非交互式VSS方案，它们都是针对门限访问结构的。但是，这两个方案中只有参与者可以验证子秘密的有效性。若分发者和参与者之间存在勾结行为，那么非交互式的VSS方案就是不安全的。

针对该问题，Stadler提出了公开可验证秘密共享（Publicly Verifiable Secret Sharing, PVSS）方案[79]。PVSS方案中，不仅参与者可以验证秘密份额是否正确分发的，其他任何非参与者也可以对秘密份额进行验证。在他之后，相继有不同的PVSS方案提出。Fujisaki和Okamoto的PVSS方案[80]是一个可证明安全的PVSS方案，它比Stadler的PVSS方案效率高，可以用于基于因数分解和离散对数的密钥托管密码系统中，将其转化为公开可验证的密钥托管（Publicly Verifiable Key Escrow, PVKE）。其中，基于因数分解的密钥托管是安全的，但是基于离散对数的密钥托管问题是不安全的。相对于Stadler，Fujisaki和Okamoto的PVSS方案，Shoenmakers的PVSS方案[61]不但提高了效率，而且降低了构造方案中假设前提的复杂度。Villar等人的PVSS方案[62]是基于对的方案，其计算效率可以与Shoenmakers的PVSS方案相媲美。文献[81]-[83]中给出了从2011，2012，2014年的研究学者关于PVSS的研究成果。

PVSS方案可以有效地防止秘密分发者和秘密参与者的欺骗行为，也不需要安全的信道，使得系统更加健全。然而，将PVSS方案运用于实际中，需要进一步的研究和探讨。

在3.1节中，本文详细分析了现阶段解决IBE密钥托管问题的方案。本节基于BF-IBE详细方案，采用Boneh和Franklin提出的门限秘密共享思想，对IBE的密钥管理方案进行了改进。在基于身份的加密系统中，PKG身兼数职，既全权负责的产生和分发，又负责用户身份合法性的识别和鉴定，更需要建立PKG和用户之间的安全信道。因此，在改进方案中，对于PKG主密钥泄露造成用户私钥泄露的问题，采用一个主PKG先分割主密钥，进而多个PKG分享系统部分主密钥；对于系统中用户身份的认证问题，加入一个可信中心；对于PKG和用户之间的安全信道问题，使用了盲签名技术，即在私钥的提取过程中加入了用户随机选择的信息，防止多个PKG合谋恢复用户私钥；对于密钥的撤销问题，在用户的身份标识后加入了时间成分。

3.2.2 改进的方案组成

方案中有一个MPKG（Master Private Key Generator）和个CPKG（Child Private Key Generator），一个可信中心TTA（Trusted Third Authority）和多个用户。

MPKG主要是在初始化阶段产生新的系统参数，并将主密钥使用Feldman可验证秘密共享方案（Verifiable Secret Sharing，VSS）[47]分发给个CPKG，根据文献[15]中提到的在MPKG完成系统参数的分发后，可以将其关闭，退出整个系统。

用户将信息发送给TTA，TTA对其进行签名（主要是附加时间成分）后，将其返还给用户。TTA中存放着与用户身份相关的信息。

CPKG通过和TTA进行交流，验证用户身份，计算用户的部分私钥。任何合法用户都可以和CPKG进行通讯获得部分私钥，可以在TTA中注册信息，查询其他用户的信息。

**系统初始化阶段**。采用的是基于BDH假设的参数生成器（一个算法），选定一个安全参数，通过产生一个大素数和群，以及一个可容许双线性映射。选定4个加密哈希函数。确定本方案接受的明文的长度和所在的集合，并规定使用该方案后，产生的密文的长度和所在的集合。MPKG随机挑选，作为改进方案的主密钥。MPKG利用非交互式可验证的Feldman（Feldman-VSS）门限方案，将主密钥进行分割。并由MPKG分发给各个CPKG，CPKG可以通过Feldman-VSS方案中提供的公式验证收到的子秘密的正确性。然后MPKG，公布新的系统参数，销毁主密钥，并退出整个系统。

**用户私钥提取阶段**。首先由用户随机选取一个数，计算，并将ID和发送给TTA。TTA绑定用户身份和，同时在用户的ID后面串联上时间后组成后发送给用户。然后，用户将TTA发送的和串联起来，使用，哈希计算得到，同运算，得到，将和发送给各个CPKG。接着，CPKG和TTA之间进行通讯，得到，审核用户身份。CPKG审核通过后，才会进行计算，得到，并将传给用户。最后，收到个，根据，对得进行脱盲，得到个，利用可容许双线性映射的性质验证收到的合法性，通过求和，计算得到用户的。

加密和解密应用组成：

**加密过程**。当系统中的两个用户之间进行通信时，假定Alisa和Tom都已经各自的身份信息和发送给了TTA。假若Alisa作为信息发送方，Tom为信息接收方。Alisa同TTA之间进行信息交流，申请获取与Tom的身份对应的和，计算得到。然后由Alisa随机选择一个固定长度的随机字符串，使用哈希函数，，通过多次信息隐藏和整合得到密文，最后通过其他媒介发送给Tom。

**解密过程**。当信息接收方Tom收到后，按照如下的操作得到：

（1）从得到，并对其进行判断。若，则是无效的；若，则有效，继续进行运算。

（2）若有效，则Tom和多个CPKG建立连接，提交自己的和给CPKG。

（3）CPKG收到这些信息后，与TTA建立连接，要求得到用户的数据信息。TTA将与Tom的身份信息对应的返回给CPKG。

（4）CPKG将从TTA处得到的信息和Tom发送的消息进行比较，判断Tom身份的真实性。CPKG证实了Tom的身份后，使用自己保存的，计算Tom的。

（5）Tom和个CPKG重复（2）~（4）的通讯步骤，得到个，最后得到。接着Tom使用得到Alisa在明文中加入的随机字符串，进而通过，得到。最后，通过和计算，判断与是否相等，若不相等，则拒绝恢复密文；若相等，则Tom得到明文。

3.2.3 改进的方案设计

**系统初始化阶段**：给定一个安全参数，MPKG运行产生系统参数和主密钥，并将主密钥通过门限方法分给CPKG，公布新的系统参数，销毁主密钥，并退出整个系统。

1. 输入，启动算法。输出（大素数），阶的，阶的，。随机选取，满足条件。
2. 随机选取，计算。
3. 选取加密哈希函数，，，。
4. 明文空间，密文空间。
5. 运用Feldman-VSS方案，由MPKG在有限域上随机选取，构造多项式一个次拉格朗日多项式，满足，计算，其中；计算验证信息，。将子秘密发送给个CPKG，并公布。
6. 各个CPKG可以通过公式（3-3）

|  |  |  |
| --- | --- | --- |
|  |  | （3-3） |

来验证收到的的正确性。初始化后的新的系统参数是sysparams，sysparams=。MPKG将主密钥销毁后，退出整个系统。

**用户私钥提取阶段**：将作为提取的身份信息。

1. 用户任意挑选信息， 使用sysparams中的，通过运算得到。
2. 用户和TTA建立连接，传输ID和。
3. TTA录入用户的ID和，在用户的ID后面附加上时间，组成。公开用户信息的和，同时将返回给用户。
4. 用户接收到TTA返回的信息，连接和组成一个参数，使用，通过公式得到，再加上用户随挑选的数，使用公式得到经过处理后的。然后，建立和CPKG之间的连接，传输和。
5. CPKGi（）和TTA建立连接，申请获得用户的。TTA将用户的发送给CPKGi（）。
6. CPKGi（）将TTA提供的，与用户申请时传送的，进行审核。判断用户的和TTA提供的是否是完全一致的。若用户和TTA的是相同的，则将用户提供的和各自秘密保存的进行代数运算，通过公式得到，并将通过传输媒介返回给用户。
7. 用户收到CPKGi（）传送的后。首先利用自己选取的信息，得到。这可以通过用户产生的方法得到，因为，所以，在其左边和右边同时乘以得到，将记作，得到。运用可容许双线性映射的性质，通过等式，其中，可以根据公式（3-3）计算得到，从而检验的合法性。然后将验证通过的个部分私钥，通过公式（3-4）得到用户的私钥：

|  |  |  |
| --- | --- | --- |
|  |  | （3-4） |

加密和解密应用设计：

**加密阶段：**假设有两个用户Alisa和Tom，Tom需要将重要的信息发送给Alisa，加密得到。设Alisa的身份信息是，

1. Tom建立和TTA之间的连接，发出请求，获得Alisa的和，这里记作和。
2. Tom使用哈希函数，通过哈希运算，即，得到。
3. Tom在中加入自选的随机字符串，其中。
4. Tom使用哈希函数，将和通过公式组合成。
5. 通过得到，使用哈希函数，得到，组合得到，同时使用将哈希成固定长度的值，与组合，得到。最后，共同组成了，将它们记作。

**解密阶段：**Alisa获取到后，同TTA和多个CPKG通过信息传输介质，进行如下操作：

1. Alisa取出中包含的信息，判断是不是中的元素，假如，则继续进行以下步骤；假如，则不合法。
2. Alisa和TTA，个CPKG之间进行通信，按照根据提取阶段中所进行的步骤（4）~（7），得到同对应的。
3. Alisa使用双线性映射得到，再通过哈希函数，得到，然后得到Tom在中添加的非有用信息，再通过得到。
4. Alisa使用得到，和通过公式，得到，判断和是否相等，假如，则Alisa可以看到；假如，则拒绝恢复。

3.2.4 改进方案分析

方案是针对BF-IBE详细方案的密钥管理问题，采用Feldman-VSS对主密钥进行秘密共享。因此，该方案中的安全性基于BDH假设和非交互式可验证的Feldman秘密共享方案上的。其中，Feldman-VSS方案是条件安全的[85]，它的安全性是建立在离散对数困难问题上的。

1.改进方案中用户私钥托管问题的安全性分析

在主密钥分发阶段，CPKG通过公开的验证信息，通过公式对收到的进行验证，从而防止MPKG的欺骗行为，保证收到的子秘密是正确有效的。在用户私钥提取过程中，针对CPKG可能存在的欺骗行为，采用了可容许双线性映射的性质对的进行验证。

满足BDH假设的随机数产生器，使得产生的参数，群和双线性映射具有安全性，不易被破解。用户私钥的产生通过多个CPKG合作，避免了用户私钥泄密的风险。

在用户私钥提交给各个CPKG的中包含了自主选择的信息，可以抵抗多个CPKG的合谋攻击。即使多个CPKG可以合作，共同按照规定的算法恢复出，也无法只通过得到用户的。TTA中保存着所有合法用户的，若CPKG冒充合法用户的身份，无法通过TTA的合法性检查，从而无法进行非法活动。另外，假使CPKG和TTA之间勾结，得到了用户的和，它也无法从倒推得到用户的自主选择信息，同理CPKG无法通过求得。另外一方面，在CPKG和用户之间建立了安全的部分私钥传输信道，即使非法用户进行了信息监听，也无法窃取部分密钥。

方案中的TTA既保证了用户进行合法操作，限制了CPKG进行非法攻击，也保存了用户的信息供CPKG和其他合法用户查询，同时可以识别非法分子的蓄意攻击。TTA在收到用户的ID和后，将两者绑定在一起，同时在用户的ID中串联了时间，组成了。通过时间，可以对密钥对的有效性进行管理，设置有效期，便于密钥对的撤销，TTA实现了方案的监听。

2.改进方案中加密/解密设计的分析及改进措施

假设TTA，CPKG或者其他用户冒充用户加密虚假信息，并不能在解密阶段被合法接收者识别。例如，犯罪分子Criminal，要发送伪造的信息给Valid，Criminal得到了和，通过加密的1~6步，得到。Valid在解密时，并不能对Criminal的身份进行判定，也就无法识别并不是用户真实的。对于这种攻击，可以增加用户自主选择的信息，防止其它非法分子冒充合法用户进行破坏。改进后的加/解密阶段如下：

**加密阶段：**假设有两个用户Alisa和Tom，Tom需要将重要的信息发送给Alisa，加密得到。设Alisa的身份信息是，

1. Tom建立和TTA之间的连接，发出请求，获得Alisa的和，这里记作和。
2. Tom使用哈希函数，通过哈希运算，即，得到。
3. Tom在中加入自选的随机字符串，其中。
4. Tom随机挑选。
5. 通过得到，使用哈希函数，得到，组合得到，同时使用将哈希成固定长度的值，与组合，得到。最后，共同组成了，将它们记作。

**解密阶段：**Alisa获取到后，同TTA和多个CPKG通过信息传输介质，进行如下操作：

1. Alisa取出中包含的信息，判断是不是中的元素，假如，则继续进行以下步骤；假如，则不合法。
2. Alisa和TTA通讯并获取与Tom对应的，与进行比较。假如，则判定确实是Tom发送的；假如，则是非法的。
3. Alisa和TTA，个CPKG之间进行通信，按照根据用户提取阶段中所进行的步骤（4）~（7），得到同对应的。
4. Alisa使用双线性映射得到，再通过哈希函数，得到，然后得到Tom在中添加的非有用信息，再通过得到。

如公式（3-5）所示，加密和解密具有一致性。

|  |  |  |
| --- | --- | --- |
|  |  | （3-5） |

改进了加/解密后的改进方案，具有更高的安全性。

3.方案的正确性分析

在本文的方案中，证明包括三个方面：CPKG验证收到的的正确性，用户验证的合法性和加密/解密过程一致性。

的正确性分析：

由于本文使用的是Feldman-VSS方案，所以可以推导得出本文中主密钥的安全性。

每个CPKG可以通过公式（3-3）验证。如，取，，则CPKGh通过公式（3-6）和公式（3-7）验证MPKG发送的的正确性。

|  |  |  |
| --- | --- | --- |
|  |  | （3-6） |
|  |  | （3-7） |

的合法性：

用户收到CPKGi（）传送的后。对进行脱盲，然后通过可容许双线性映射的性质验证的合法性，也即正确性。如，用户收到CPKGh的，首先根据公式（3-8）计算得到：

|  |  |  |
| --- | --- | --- |
|  |  | （3-8） |

，然后，根据，其中可以通过公式（3-7）计算得到，进而可以验证的合法性。

加密和解密的一致性：

对于通讯双方Alisa和Tom，发送方Tom将密文发送给Alisa。在加密时，Tom使用随机选择的信息，计算得到，通过公式（3-9）验证加密和加密过程的一致性：

|  |  |  |
| --- | --- | --- |
|  |  | （3-9） |

4.与其他方案的比较

与本文方案进行比较的方案根据采用的秘密共享方案的不同进行分类比较。对于采用Feldman-VSS方案的，比较了Feldman-VSS方案在解决IBE密钥管理问题中作用时机，作用对象和秘密恢复作用不同，并指出本文的优势和独特之处。对于采用Shamir方案的，比较了分割主秘密采用的方式和分割后的验证问题，指出本文采用Feldman-VSS的优势。

文献[66]和[67]中，研究者采用了Feldman-VSS方案对用户私钥进行秘密共享。其中，文献[66]是针对Boneh和Franklin提出的IBE方案中的管理问题进行了研究；文献[67]是针对基于身份认证加密方案中存在的管理问题进行了研究。这两个方案同本文提出的方案的区别在于以下三个方面：

1. Feldman-VSS方案作用时机不同。本文使用Feldman-VSS方案在用户的产生之前，而文献[66]和[67]秘密共享发生在用户的产生后。
2. Feldman-VSS方案作用对象不同。本文中是对主密钥进行分割，分发给个CPKG。而文献[66]和[67]中是对用户随机选择的整数（）进行分割，分发给个参与者。
3. Feldman-VSS方案的秘密恢复作用不同。本文通过公式（3-4）得到用户的。而在文献[66]和文献[67]中其作用是恢复用户的，采用的策略是先恢复，再通过用户公布的信息计算得到。

文献[66]和[67]中，若PKG被攻破，泄露，用户的便不再安全。本文中将进行分割，在安全条件下，可以实现用户的安全。此外，文献[66]和[67]中，并没有提供对用户身份核查和密钥撤销的方法，也没有建立PKG和用户之间传输的安全信道。本文提供了对用户身份核查和密钥撤销的方法。

文献[68]中，同样采用了门限方案实现密钥托管。它不是直接对主密钥进行秘密共享，而是对经过“影子”变换后的（）进行秘密共享。由于它采用的是Shamir的秘密共享方案，所以，对于分割后的（“碎片”）的真实性和有效性，它提供了另外的验证方法。而本文直接采用了可验证的秘密共享方案，不需要再单独设立一个机构SA保存和。文献[68]中，对于用户身份的验证也设置了验证方法，但是，对于用户密钥的撤销管理并没有提供相应的措施。本文提供了密钥撤销管理。

文献[63]中，对于SK-IBE（Sakai Kasahara-IBE）的密钥管理问题，采用Shamir的秘密共享方案对进行了分割，该方案中将作为系统参数公布。如此一来，子PKG的作用形同虚设。用户无需将自己的信息发送给子PKG便可以产生自己的私钥。此外，方案中并没有提供对分割后的子秘密的验证方法。本文中采用了Feldman-VSS方案，将验证信息作为公开参数。既可以保证MPKG和CPKG是诚实的，也避免了用户滥用公开信息，合成私钥。

而关于密钥管理方案的计算效率，一方面计算次数多，另一方面需要进行双线性映射和点乘运运算，相对于文献[63]和文献[68]，其计算效率较低。

5.改进方案的开放性问题

本文提出的方案，由于子秘密是保密的。所以，CPKG对子秘密在分割阶段的正确性可以通过公式（3-3）确保是正确的。用户私钥提取阶段中，用户验证CPKG提供的时，通过双线性映射的性质和公式（3-3）进行验证。在3.1.1中介绍过，PVSS方案可以让系统具有更好的鲁棒性，因此，可以采用PVSS方案来解决IBE的密钥托管问题。文献[86]中采用了PVSS方案对用户的进行了秘密共享，并给出了详细的证明和分析过程。而将PVSS方案对主密钥进行秘密共享，从而解决IBE的密钥托管问题，还需要进一步的研究和探讨。

在本文的方案中，采用TTA，一方面解决用户的密钥撤销问题，另一方面减轻CPKG的负担。但是，采用可信第三方对方案的安全前提有影响。因此，针对BF-IBE详细方案的密钥管理问题，采用无可信中心的密钥管理方案对安全性的提高有益。

3.3 Lee.B安全私钥分发

采用门限方案对进行分割，并不能从本质上解决用户的托管问题。为了更好的解决的托管问题，Lee.B等人提出了使用密钥生成中心，密钥权威机构共同合作产生。用户加入盲因子，建立了安全信道。该方案既可以解决IBE方案中的问题，也保留了基于身份加密的特性，也是分布式环境下的基于身份加密的好的介绍。本节对Lee.B的方案进行了介绍分析，针对存在的问题，提出了一种改进方案。

3.3.1 Lee.B安全私钥分发协议

该协议中的角色：密钥生成中心KGC（Key Generation Center），个密钥权威机构KPA（Key Privacy Authority）和合法用户。

私钥分发的过程由三个阶段组成：

（1）私钥分发阶段。用户向KGC发送他的身份和盲化因子[48]，KGC收到要用户的请求后，首先核查用户的身份，再使用盲方法分发部分私钥给用户。

（2）密钥安全阶段。用户依次向个KPA申请获取私钥秘密服务，KPA使用盲方法返回真正的私钥。

（3）密钥恢复阶段。用户使用脱盲技术恢复真正的私钥。

该安全私钥分发协议包括5个阶段：系统初始化（System Setup），系统公钥初始化（System Public Key Setup），密钥分发（Key Issuing），密钥安全(Key Securing）和密钥恢复（Key Retrieving）。

**阶段1**：系统初始化（System Setup）

主要通过KGC产生。

1. KGC任意挑选（大素数），阶的，阶的以及和，，。
2. KGC随机选取从中选取一个数作为它的主密钥。
3. KGC通过运算得到自己的公钥。其中，，满足条件。
4. KGC将作为公布，并将秘密地保存。记，。

**阶段2**：系统公钥初始化（System Public Key Setup）

主要由多个KPA来完成，该阶段个KPA产生他们的公/私钥对。

1. 对于所有的（）选择他们的各自的主密钥，同时计算他们各自的公钥。
2. 然后，个KPA合作产生系统公钥，系统公钥将会在用户群中作为一个系统参数使用。更具体地说计算，计算，，计算。接着作为系统的公钥公布。用户将使用系统的公钥完成加密，签名认证等等。该过程中的正确性可以通过等式来进行验证，其中。

**阶段3**：密钥分发（Key Issuing）

KGC和用户（身份是ID）之间建立通道，进行信息交互。

1. 用户任意选取一个数，得到一个盲参数。
2. 用户把ID，作为一个整体，传送给KGC，申请分发。
3. KGC核查用户的ID是否是真实合法有效的。
4. KGC通过公式（3-10）运算得到：

|  |  |  |
| --- | --- | --- |
|  |  | （3-10） |

1. KGC通过公式（3-11）计算部分盲私钥：

|  |  |  |
| --- | --- | --- |
|  |  | （3-11） |

1. KGC通过公式（3-12）计算部分盲私钥的签名：

|  |  |  |
| --- | --- | --- |
|  |  | （3-12） |

1. 将部分盲私钥和其对应的签名发送给用户。

在这个阶段中，是盲化因子，建立了KGC与用户传输信息的

安全的通信信息渠道。当用户收到后，可以通过双线性映射的性质（如公式（3-13）所示），对其进行接去盲处理：

|  |  |  |
| --- | --- | --- |
|  |  | （3-13） |

**阶段4**：密钥安全（Key Securing）

由用户和个KPA完成。

1. 用户按照顺序将，，，依次发送给对应的（）。
2. （）核查等式的左边和右边是否等值。
3. （）通过公式（3-14）得到，将与，使用公式（3-15）得到：

|  |  |  |
| --- | --- | --- |
|  |  | （3-14） |
|  |  | （3-15） |

用户按照步骤1~3与一直到进行信息交互，直至从处得

到和。

**阶段5**：密钥恢复（Key Retrieving）

用户通过公式（3-16）计算得到自己的私钥：

|  |  |  |
| --- | --- | --- |
|  |  | （3-16） |

用户通过对私钥进行正确性检查。

3.3.2 Lee.B安全私钥分发协议的应用

Lee.B的协议中，通过个KPA，KGC和用户共同产生的用户的私钥，，可以说是一个真正的采用基于身份加密思想得到的私钥，用户的系统公钥是。在Lee.B协议下生成的和，用户可以用进行加密数据的操作，提高信息的保密性，也可以对其他用户的签名进行审核；用解密使用加密的数据或者信息，或对所发行的文件或者其他信息进行签名。比如，可以用在BF-IBE的基本方案中，或者用于Boneh等人提出的IBS（Identity-Based Signature）方案中。此外，该安全私钥分发协议支持任何合法用户的密钥托管。

假设用户采用BF-IBE基本方案，使用公钥加密明文信息，得到如公式（3-17）所示的密文：

|  |  |  |
| --- | --- | --- |
|  |  | （3-17） |

其中，可以通过公式（3-18）恢复：

|  |  |  |
| --- | --- | --- |
|  |  | （3-18） |

用户解密时，通过合法性检查后，在KGC和个KPA的合作下，解密得到。每一个实体可以按照公式（3-19）顺序计算，成功得到：

|  |  |  |
| --- | --- | --- |
|  |  | （3-19） |

在使用Lee.B的协议进行如上过程所描述的加密和解密过程，整个过程的正确性可以通过双线性映射的性质得到证明。在本小节描述的应用中，涉及到的解密操作时，只是一个对进行解密的过程，并不需要进行用户私钥的恢复。

3.3.3 Lee.B方案的问题分析

在该协议中，用户的私钥是通过KGC和多个KPA共同合作计算出来的。如果协议中至少有一个KPA是诚实的，那么协议就可以保证用户的私钥的安全性和秘密性。该协议中只有知道盲化因子的合法用户才可以恢复私钥，成功地解决了IBE中的密钥托管问题，可以应用于对安全性要求较高的复杂程序中。

在Lee.B等的方案中增加了盲因子，建立了安全信道。如果犯罪分子对协议进行外部攻击，采用非法手段监听用户和个KPA之间的通讯，抓取有用的信息（），也无法使用公式（3-12）得到用户的私钥，有效的保证了用户私钥的安全性。

但是在该方案中，存在着以下不足：

（1）系统无法察觉由KGC发动的内部攻击，也就不能阻止KGC非法恢复合法用户的私钥，所以Lee.B等人的协议并没有从真正意义上解决用户的私钥托管安全性问题。从Lee.B私钥分发的操作步骤可以看出，保障私钥的安全是通过（）实现的。但是，在密钥安全阶段，（）仅仅只检查了用户的和，并没有对用户的身份的真实有效性进行核查。这个环节的疏忽，会造成巨大的安全漏洞。在密钥分发阶段，KGC得到了用户的传送的和。系统中并没有其他的机构或者设计其他安全措施对KGC的行为进行约束。因此，KGC可以轻而易举的冒充合法用户，和KPA之间进行沟通，恢复用户的私钥，或进行非法操作，如破解密文信息，或者伪造用户签名。

攻击过程描述如下：

1. 合法用户将自己的身份ID和盲因子发送给KGC。
2. KGC任意挑选，计算。
3. KGC得到用户合法的。
4. KGC得到自己合成的。
5. KGC得到的签名。
6. KGC将合法用户的与自己计算的，，发给。
7. 通过验证PKG发送的信息是合法的。得到，进一步运算得到的签名。将和传送给KGC。
8. KGC再继续按照步骤g中描述的方式与（）进行信息交互，直到将，发送给KGC。
9. KGC利用如下的公式（3-20）恢复用户的私钥

|  |  |  |
| --- | --- | --- |
|  |  | （3-20） |

（2）KGC和KPA抵御非法分子的破坏能力存在着不足。个KPA和KGC假定参加活动的用户都是诚实的，但是其实存在着不诚实的用户。如，KPA通过证明公式证明是的有效签名，若用户通过与某个数的乘积伪造出，从而伪造签名。向合法的KPA提交ID，，和，KPA无法识别出用户的作假行为。此外，会继续为非法分子服务。在某种意义上讲，用户增加的盲因子并没有建立KPA和用户之间进行通信的安全信道。只要非法分子可以破解出，它就不需要再按照协议的流程来进行私钥分发。例如，犯罪分子，可以安装窃听器，或者大量的非法分子操纵傀儡用户，对系统发起攻击，KPA无法对非法分子和合法用户的请求进行区分，当用户的请求超过KPA的承载上限后，造成系统拒绝服务，即使是合法用户也无法正常进行合法活动。这是协议中没有考虑到的，然而，在实际应用中，这是必须考虑的潜在风险，需要采取防范措施。此外，对于非人为因素造成的KPA和KGC无法正常工作，并没有提供相应的预防措施。

（3）用户和KPA之间的身份认证次数多，通信开销较大。在合法用户通过该协议恢复私钥时，将需要和个KPA合作，提交身份，盲因子，自己的部分公钥和与之对应的签名。然后各个KPA先通过参数和，根据双线性映射的性质，由审核用户提交的和是否是相互对应的。若，则证明用户提交的是正确的、。各个KPA都要计算和，并传输给用户。假如系统中只有一个用户请求获取私钥，则KPA和用户之间的认证次数是次；当系统中有（非常大）个用户时，系统的认证次数就是次。当系统规模扩大时，需要进行实时通讯，这个就会造成用户等待时间长，系统负担重的后果。

3.4 改进的Lee.B安全私钥分发

3.4.1 改进的Lee.B方案

在系统中加入第三方可信机构TTP（Trusted Third Party），保存用户身份信息，盲因子和时间。当用户发送ID和时，对两者进行签名。它可以审核用户的身份，暂时保存用户的部分私钥和对该私钥的签名，同时对系统中的KGC和（）中的关键信息进行备份和安全处理。用户在和KGC通讯时，得到的签名时，增加了有效时间，并将时间在（）中进行传递，从而实现对用户私钥和私钥签名的管理。

该安全私钥分发协议包括5个阶段：系统初始化（System Setup），系统公钥初始化（System Public Key Setup），密钥分发（Key Issuing），密钥安全(Key Securing）和密钥恢复（Key Retrieving）。

**阶段1**：系统初始化（System Setup）

主要由KGC和TTP来完成。

1. KGC指定阶为（是大素数）两个群和以及这两个群之间的双线性映射和三个哈希函数，，， 。
2. KGC随机选取从中选取一个数作为它的主密钥。
3. KGC通过运算得到自己的公钥。其中，，满足条件。
4. TTP随机选取，同时计算与其对应的。
5. KGC将一同作为公开，并将秘密地保存。记，。

**阶段2**：系统公钥初始化（System Public Key Setup）

主要由多个KPA来完成，该阶段个KPA产生他们的公/私钥对。

1. 对于所有的（）选择他们的各自的主密钥，同时计算他们各自的公钥。
2. 然后，个KPA合作产生系统公钥，系统公钥将会在用户群中作为一个系统参数使用。更具体地说计算，计算，，计算。接着作为系统的公钥公布。用户将使用系统的公钥完成加密，签名认证等等。该过程中的正确性可以通过等式来进行验证，其中。

**阶段3**：密钥分发（Key Issuing）

KGC，TTP和用户（身份是ID）之间建立通道，进行信息交互。

1. 用户任意选取一个数，得到一个盲参数。
2. 用户将ID，借助通道发给TTP，TTP将ID，串联起来得到，使用哈希函数，得到，并将返回给用户，同时维护一个合法用户的ID，，表。
3. 用户将ID，借助通道发给KGC，申请分发部分私钥。
4. KGC同TTP通讯，通过判断是否成立，核查用户的ID和。
5. KGC通过公式（3-21）运算得到：

|  |  |  |
| --- | --- | --- |
|  |  | （3-21） |

1. KGC通过公式（3-22）计算部分盲私钥：

|  |  |  |
| --- | --- | --- |
|  |  | （3-22） |

1. KGC通过公式（3-23）计算部分盲私钥的签名：

|  |  |  |
| --- | --- | --- |
|  |  | （3-23） |

1. 将部分盲私钥和其对应的签名发送给用户。

在这个阶段中，是盲化因子，建立了KGC与用户传输信息的

安全的通信信息渠道。当用户收到后，可以通过双线性映射的性质（如公式（3-24）所示），对其进行接去盲处理：

|  |  |  |
| --- | --- | --- |
|  |  | （3-24） |

**阶段4**：密钥安全（Key Securing）

由用户和个KPA以及TTP完成。

1. 用户按照顺序将ID，，，依次发送给对应的（）。
2. （）和TTP建立连接，获得用户的，通过核查用户的身份。
3. （）通过哈希函数，计算。核查等式的左边和右边是否等值，判断，之间的对应关系。
4. 若步骤1~3中用户审核全部通过，（）通知TTP更新对应的用户在TTP中的有效使用时间。
5. （）通过公式（3-25）得到，与通过公式（3-26）与对应的：

|  |  |  |
| --- | --- | --- |
|  |  | （3-25） |
|  |  | （3-26） |

1. 当时，将ID，，，，组装在一起。然后，它建立与TTP的连接，将它们传送给TTP。和TTP之间按照步骤3~6进行信息交互，得到和与之相对应的。当时，将和传送给用户。

**阶段5**：密钥恢复（Key Retrieving）

用户通过公式（3-27）计算得到自己的私钥

|  |  |  |
| --- | --- | --- |
|  |  | （3-27） |

用户通过对私钥进行正确性检查。

3.4.2 改进的私钥分发协议的分析

1.改进方案的安全性分析

（1）改进的方案中加入了TTP，保存用户的ID，和，对KGC利用合法用户的ID非法恢复用户的私钥进行了有效的控制。

在密钥分发和密钥安全中，运用双线性映射的性质对用户的身份进行了验证。TTP中有合法用户的ID和信息，KGC或KPA计算，通过判断用户身份的正确性。具体推导过程如式（3-28）所示：

|  |  |  |
| --- | --- | --- |
|  |  | （3-28） |

KGC非法使用合法用户的ID，任意选取，得到。由于在TTP中存放着合法用户的，当KGC要继续运算时，无法使得成立。所以，KGC无法非法恢复用户的私钥。

另外，TTP可以对用户的行为进行监控，比如设置用户向KPA在一定时间内向KPA发送请求的上限，防止用户多次向KPA在一定时间内重复提交相同的申请。对于在实际应用中，KGC出现故障或者KPA出现故障，在TTP中维护KGC的关键信息，并根据门限方案规定当（）中的个和KGC合作即可得到所需要的密钥。

（2）KGC和个KPA在产生合法用户的，，以及，（）时，使用了哈希函数，计算得到与对应的签名，使用对进行了签名，并附加上了有效期。通过双线性映射验证用户提交的和的正确性方案中，用户向第一个KPA提交，，计算，证明正确性过程如式（3-29）所示：

|  |  |  |
| --- | --- | --- |
|  |  | （3-29） |

KPA（）可以通过验证TTA提交的和的正确性，证明的具体过程如前所述。

非法分子是无法得到用户的，保证了合法用户正常使用系统，有效地打击了非法分子发动的拒绝服务攻击，使系统具更高的安全性。

2.改进方案的身份验证及监听分析

（1）在用户私钥安全阶段，将（）合成的部分私钥和对应的签名先发送给TTP，直到产生和，将两者发送给用户。这一改变，大大地减少了用户和（）之间的通讯和身份验证次数，使系统具有更高的效率。在一定时间内，TTP一次将所有数据提交给KPA，减少了用户和KPA直接进行通讯造成的系统冗余。用户不直接和所有的KPA进行身份验证，只需要和TTP之间进行通讯，验证自己身份的合法性，减少了身份验证的次数。

在一个固定的时间段内，假设有个用户申请获得和，从用户，KPA，TTP之间的验证角度来看，在Lee.B的方案中，需要进行次身份验证；在改进的方案中，用户不需要和KPA之间进行通讯，进行身份验证，用户将自己的身份和盲因子交给TTP，TTP直接将所有的身份和盲因子一次性交付给KPA，在这个身份验证过程中，需要进行的身份验证次数是次。通过TTP的代理，降低了通讯的频率，增强了系统的健壮性。

（2）在通常的网络通信中，非法分子可能会采取措施对PKG或KPA进行破坏或者监听，也可能冒充用户的身份进行非法活动，加入TTP后，如法律授权下的政府监管机构。TTP的加入，对用户的身份进行了保存，维护了合法用户的信息。当非法用户想要使用系统进行非法操作时，在身份验证中，无法通过，那么，就无法进行其他的对系统的破坏。用户的私钥信息也可以得到较好的保护。再者，也减轻了PKG和KPA的负担，分工合作，更有利于系统的应用和推广使用。

3.改进方案与其他方案的比较

文献[89]中，研究者针对Lee.B方案中用户身份认证次数多，KGC和所有的KPA合作伪造用户盲因子的问题，引入了可信机构，但是对于伪造签名的问题对和的正确性保证并没有提供有效的保护机制。文献[90]中采用计算与对应的签名，每个KPA需要维护一个私钥服务列表，是私钥的有效期，如果的已失效，则将从私钥服务列表中删除，如此一来加重了KPA的负担。本文中的可信第三方TTA的加入，维护了用户的，和，一方面减少了用户身份的认证次数，另一面又TTA统一维护用户密钥的有效期，减轻了KPA的负担。

4.开放性问题

改进的方案同Lee.B原方案，都使用了大量的双线性运算，且设计过程复杂，所以计算效率较低。此外，改进的方案中引入了可信第三方并不是提高安全性和效率的优化方案。虽然减少了用户身份的验证次数，对存在的内部攻击，外部攻击以及物理因素造成的安全问题进行了抵御，但是，将改进的方案运用于实际中，仍需要进一步的研究和完善。

3.4.3 改进的私钥分发协议的应用

在改进的私钥分发协议下生成的和，用户可以用进行加密数据的操作，提高信息的保密性，也可以对其他用户的签名进行审核；用解密使用加密的数据或者信息，或对所发行的文件或者其他信息进行签名。比如，可以用在BF-IBE的基本方案中，或者用于Boneh等人提出的IBS方案中。此外，该安全私钥分发协议支持任何合法用户的密钥托管。

假设用户采用BF-IBE基本方案，使用公钥加密明文信息，得到如公式（3-30）所示的：

|  |  |  |
| --- | --- | --- |
|  |  | （3-30） |

用户得到，恢复，可采用公式（3-31）：

|  |  |  |
| --- | --- | --- |
|  |  | （3-31） |

用户解密时，通过合法性检查后，在KGC和个KPA的合作下，解密得到。每一个实体可以按照公式（3-32）顺序计算，成功得到：

|  |  |  |
| --- | --- | --- |
|  |  | （3-32） |

3.5 本章小结

IBE体制中存在着天然的密钥托管问题，本章针对IBE的密钥托管问题，进行了研究分析。

（1）对于Boneh和Franklin提出的方案，进行了深入的分析和研究。结合Feldman-VSS方案的思想，运用盲签名技术，加入了TTA，针对BF-IBE具体方案密钥管理问题进行了改进，并将其运用于通讯中的加密和解密过程。分析了方案的安全性，并对新方案的正确性进行了分析证明，同时将其与其他密钥管理方案进行了对比分析，指出了改进方案中存在的开放性问题。

（2）对于Lee.B的方案，指出Lee.B协议中存在内部攻击，外部攻击和物理故障问题。引入了TTP，维护用户的，和信息；在KGC和（）对进行签名时，加入了时间，减少了用户和（）之间进行身份审核的次数；提高了系统对内部攻击，外部攻击和物理故障的风险抵御能力。分析了方案的的安全性，提出了方案的监听设计，将该方案与其他方案进行了对比分析，并指出了改进方案中存在的开放性问题。

1. 基于身份加密在安全电子邮件系统中的应用

电子邮件方便快捷，内容丰富，使用它的人数逐年增长。网易邮箱大师《2014年度互联网邮箱使用情况报告》中，指出中国网民平均每人使用约超过3.8个电子邮箱账户。

然而，对于大部分的电子邮件，没对其传送的信息进行保护。邮件中重要信息的泄露，会给电子邮件的使用者带来不必要的麻烦，造成不可避免的个人财产损失或者隐私暴露。所以，研究安全性、使用性和易用性高的安全电子邮件系统[49]十分重要。目前，采用的主流保证电子邮件安全的是PKI和S/MIME技术相结合的安全电子邮件系统[50]。采用PKI技术，不可避免的带来了繁琐的证书管理。将IBE运用于电子邮件客户端，可以将用户的邮箱地址作为公钥，加密信息或者验证签名，不再需要借助证书作为绑定用户身份和公钥的媒介，精简了安全电子邮件系统的设计，具有研究价值和实用意义。

4.1 电子邮件的介绍

4.1.1 电子邮件和电子邮件系统

电子邮件由信头和信体组成。信头主要包括邮件的发送方，接收方，主题，时间；信体是邮件的正文。RFC822规定，信头和信体之间必须有一空行。

电子邮件是借助电子信息技术提供信息交换的通讯方式。电子邮件系统在通信网络上建立一个分布式的计算机系统，用户进行信息交流时需要借助多个路由和代理来完成。图4-1描述了电子邮件从产生到发送到接收者中间经过的传输过程。



图4-1 电子邮件传输过程示意图

发件人在本地的邮件用户代理上完成电子邮件的编写和发送，用户代理寻找到一个邮件传输代理。邮件传输代理收到邮件后，并不是直接将邮件发送到接收者手中，而是将其缓冲在一个自己维护的消息队列中。然后，邮件传输代理读取邮件中目标地址，判断为目标地址邮箱提供服务的邮件服务器，并将邮件投递到该邮件服务器中。邮件服务器收到邮件后，将其保存在本地数据库中，直到接收者读取邮件。

但是，在实际的网络上进行邮件传输时，并不是通过电子邮件上的目标地址来判断邮件的投递地址的。因为，在邮件传输过程中，服务器会给电子邮件的外面加上一层信封。在实际投递过程中，采用的是信封上的地址或者是信封的信头。如图4-1所示，电子邮件并不是直接从发送方到达接收方的手里的。在传输过程中，需要经过多次的中转。这和实际中进行通讯的过程很相似，在传统的信件通信过程中，一封信从发信人到收信人的手里，需要经过邮局，传输工具，邮递员的合作才能实现。在网络上传递的电子邮件也是类似的形式。图4-2给出了一个形象的电子邮件发送和接受过程。



图4-2 电子邮件传送形象示意图

在实际通讯过程中，用户在客户端2上编写电子邮件，然后通过SMTP协议将其发送到他的SMTP1服务器中。接着，由SMTP1找到收件人所在SMTP2，建立与SMTP2之间的连接，把邮件发送到收件人的SMTP2中。SMTP2等待用户来读取邮件。

从TCP/IP（Transmission Control Protocol/Internet Protocol）四层网网参考模型来分析，电子邮件信息从一个客户端流向另外一个客户端，中转过程中，存在着诸多对其造成安全威胁的因素。总结起来，主要有三个方面，窃听，篡改，伪造。窃听是由网络的开放性导致的，非法分子使用一定的网络嗅探，抓包技术或者安装监听器等，对邮件系统进行监视，窃取有利信息。篡改，当第三方非法操作者，截获了电子邮件信息后，可以对信息进行修改，破坏了电子邮件的真实性和完整性。伪造，在电子邮件中，犯罪分子冒充合法用户的身份，传递虚假邮件。要抵御这些攻击手段，需要采取相应的措施，保证邮件的安全。

4.1.2 电子邮件安全解决方案

当前，结合不同的协议和技术手段，针对邮件产生，传输和服务器三个方面，提出了不同的解决方案。

对于邮件客户端，结合密码学中的数字签名和加密/解密技术，对邮件进行安全处理，隐藏邮件明文信息，保障邮件安全，同时，不增加用户使用电子邮件客户端的难度。采用一些安全协议，借助PKI保证邮件安全。发展成熟且应用广泛的协议主要是PGP（Pretty Good Privacy）和S/MIME（Secure/Multipurpose Internet Mail Extensions）。PGP采用的是哈希函数和公钥密码相结合的技术，保证信件内容的保密性，不可修改和不可否认性。S/MIME是一种基于RSA数据安全的技术，它提供了一个具有一致性的方法来发送和接收安全的MIME数据。相对于PGP，S/MIME使用了CA的层次信任模型，下级对上级身份的认证，CA颁发证书给用户，认证用户身份，使得S/MIME有更高的安全性和扩展性。

对于邮箱服务器端，采用的服务器必须是安全，可靠，稳定的，为用户提供快速的服务请求响应。对于邮箱服务器来说，主要的问题是垃圾邮件造成的系统崩溃和拒绝服务。采用的是局部解决方案即防火墙技术，一是在公用防火墙上使用邮件服务代理，另一个是安装电子邮件防火墙。

在网络模型中的传输层（Internet Layer）实现对信头信息的保护，由于客户端中，主要是对邮件体中的内容进行了隐藏，并未对邮件头做处理。采用的技术手段主要：一是SSL SMTP（Secure Socket Layer，Simple Mail Transfer Protocol，SSL-SMTP） 和SSL POP（Secure Socket Layer，Post Office Protocol，SSL- POP），二是使用虚拟专用网（Virtual Private Network，VPN）或者其他IP通道技术。VPN对TCP/IP进行了封装处理，自然而然地包括对邮件（信头和信体）的整体处理。

4.1.3 电子邮件协议

SMTP[51]和POP3[52]是在电子邮件系统中使用最广泛的两个协议，用户在邮箱客户端使用SMTP将电子邮件发送到邮箱服务器，使用POP3协议从邮箱服务器获取电子邮件。

SMTP（Simple Mail Transport Protocol，简单邮件传输协议）是TCP/IP诸多协议中的一种，它规定了客户与邮件传输代理之间的通信规则，属于请求/响应式协议。SMTP在两种应用场景中发挥着作用，其一用户的客户端计算机和邮件传输代理之间的通讯，其二是服务器之间的通讯。SMTP接收用户的发出的请求，做出相应的响应，主要是基于ASCII文本，通过命令来实现的。命令的组成包括命令名和参数信息。用户向SMTP服务器发送申请后，SMTP服务器做出相应的响应处理，并将结果返回给客户端，告知用户请求结果。例如，当使用命令行登陆SMTP服务器时，若登陆成功，SMTP服务器会返回250，若登陆不成功，则返回502。SMTP使用的端口号是25，不同的SMTP服务器提供商提供了不同的SMTP服务器地址，如网易126邮箱的smtp.126.com。当使用命令行发送邮件时可以使用telnet smtp.126.com 25登陆126邮箱，发送邮件。

POP3（Post Office Protocol，Version 3，邮局协议），同SMTP一样属于TCP/IP协议中的一个成员，是为邮件客户端用户提供远程管理邮件服务器上邮件的协议。它采用“离线”访问模式处理电子邮件，当用户需要阅读邮件时，使用POP3与邮箱服务器之间建立连接，进行通讯，对邮件进行收取，删除等管理。POP3也是一种请求/应答式协议，提供基于ASII的面向行的命令操作。命令的组成由关键字和可选参数组成，以单行文本的形式发送。POP3命令的应答包括两种形式：单行应答，多行应答，多行应答由单行应答组成。POP3使用的端口号是110，例如，在windows操作系统下使用命令行从指定的邮箱服务器接收邮件时，可以使用telnet pop3.126.com 110连接服务器，然后输入用户名和密码，输入list命令获取邮件信息，retr+邮件编号，获取指定邮件信息。

4.1.4 S/MIME和PKI技术分析

PKI与S/MIME的结合解决了电子邮件在客户端的安全，发件人发送信息的保密性，完整性，不可抵赖性，同时保证了收件人身份的可靠性。

从采用的公钥加密算法角度来说，它采用的最重要的加密算法RSA的密钥安全长度受到美国出口的限制。当密钥长度大于1024位的时候，其他国家不具有使用权限。这个原因影响了RSA算法的安全性，也对PKI/MIME技术的安全性造成了一定的影响。

从PKI的证书管理角度来说，证书的产生，发布，撤销，更新，维护等管理工作，繁琐冗杂。对于用户来说，证书的使用过程复杂。在通讯过程中，当发件人要发送加密邮件给收件人时，需要从CA维护的证书中，定位和查阅收件人的证书。然后使用证书中的公钥信息对要发送的邮件明文进行加密。由于CA的信任模型是层级结构，查找对应用户的数字证书需要耗费大量的时间。数字证书的使用范围限制也是限制其发展的一个因素，证书中的公钥是分类的，有的用于加密，有的用于用户签名，确定用户的需求，查找到对应的证书也是需要时间。另外，不同地域，不同层次的CA之间的交叉认证，证书撤销列表的维护等也限制了PKI在实际中的应用。

4.2 基于身份的安全电子邮件系统的设计

4.2.1 基于身份的安全电子邮件系统模型

基于身份加密的安全电子邮件系统的模型图如图4-3所示：



图4-3 基于身份加密安全电子邮件系统模型图

模型的具体工作流程如下：

（1）PKG运行BF-IBE具体实施方案中的初始化算法，通过输入一个安全的随机数种子，得到系统参数文件和主密钥文件，保密主密钥文件，并提供发送系统参数服务、提取合法用户私钥服务。

（2）发件人向PKG发送请求，申请获取系统参数。PKG将系统参数以文件的形式发送给发件人。

（3）发件人撰写电子邮件，使用对称加密算法，加密邮件明文；使用BF-IBE具体实施方案中的加密算法，将收件人的邮箱地址作为公钥，加密对称加密算法使用的密钥。

（4）发件人发送加密的电子邮件。

（5）收件人获取加密后的邮件。

（6）收件人和PKG之间进行通信，申请获得与自己邮箱地址对应的私钥和系统参数文件。

（7）PKG对用户的身份进行审核，审核通过后，产生与收件人邮箱地址对应的私钥，将系统参数文件和私钥文件传送给用户。

（8）收件人使用PKG发送的系统参数和私钥，采用BF-IBE具体实施方案中的解密算法进行解密，得到会话密钥，然后用该会话密钥解密，得到邮件明文。

4.2.2 系统初始化算法流程

系统初始化流程主要由PKG实现。因为BF-IBE具体实施方案的安全性建立在BDH假设上，Boneh和Franklin给出了一个满足BDH假设的随机数产生器。启动，即开始算法的执行过程，先输入一个安全的数值，然后运行在多项式时间内，直到产生的参数满足要求。

在本文的设计流程中，随机数的产生是以大整数作为基础的。MIRACL提供大数运算的所有算法。在MIRACL内部，规定当使用MIRACL进行运算时，必须先初始化一个Miracl类的虚拟对象，进行整个Miracl系统的初始化，然后再进行其他的运算。在执行算法时，规定必须输入一个满足要求的随机参数作为安全参数（种子）输入，调用函数irand，对整个系统的随机数产生器进行初始化。

大整数、的计算。大整数是一个固定的值，是Solinas素数[91]，其形式化定义为，，是正整数。中间变量，通过进行初始化。其中，作为rand函数的输入值，产生大整数随机数。，和随机函数以及prime函数循环计算得到满足条件的。必须满足三个条件：，，。

根据算法，选取的是定义在有限域上的椭圆曲线，其方程是：。通过函数randn随机选取该椭圆曲线上的一点，使得点是阶的点。如此一来，可以通过点产生一个群，记为。

计算椭圆曲线在上满足的解。

大整数型的，在计算时，已经进行了初化。此时，通过固定值，使用rand函数产生一随机的，将作为主密钥。

通过和产生系统的公钥，。

最后，将，，，，以及的位数存入sysparams文件中，主密钥存入pkgmaster文件中。图4-4是系统初始化算法的流程图：



图4-4 PKG初始化算法流程图

4.2.3 用户私钥提取算法流程

PKG初始化整个系统后，产生了sysparams文件和pkgmaster文件。当用户提出申请私钥请求时，PKG判断用户身份的合法性，然后将用户的ID，sysparams和pkgmaster作为输入参数，计算得到与ID对应的。使用的参数主要有sysparams中的，和masterkey中的，使用构造有限域上的椭圆曲线，其方程是。用户私钥提取算法的执行流程如图4-5：



图4-5 用户的私钥提取流程图

用户的计算，将ID采用map\_to\_point算法，映射成椭圆曲线上的一点，这个算法在用户私钥提取过程之中至关重要。它通过哈希函数，将一个ID哈希成一个小于模数的大数，将作为椭圆曲线的纵坐标，通过，计算得到与之对应的，采用的计算公式是，并返回在椭圆曲线上的点的坐标。最后，通过计算得到用户的，并将的纵坐标存入文件privatkey中，的纵坐标就是用户的私钥。

4.2.4 加密算法流程

在加密的过程中，本文采用了对称加密方法——高级加密标准（Advanced Encryption Standard，AES）[53]，非对称加密方法——Boneh-Franklin IBE相结合的技术进行加密，结合了对称加密方法高效、快捷的特点和非对称加密方法密钥管理简单的特点，使得加密的效率和密钥的安全性得到了保障。加密阶段中，将从PKG提供的sysparams文件，用户的ID以及邮件明文作为输入参数，计算得到邮件密文和会话密钥的密文。加密算法执行流程如图4-6：



图4-6 加密流程图

首先，从sysparams中取出，，，提前产生一个以固定点构成的一个点群。这些点是有限域上的满足方程的椭圆曲线的所有点的子集。确定椭圆曲线方程是。然后，将，，这些点全部设置在该曲线上。接着，将用户输入的ID，采用map\_to\_point函数，转化成椭圆曲线上的一点。对参数，，，，，进行椭圆曲线上的Tate对运算，并判断所使用的Tate对是否是满足可容许双线性性质的映射。若满足双线性，可交换性和非退化性，则继续进行运算；否则，退出加密流程。

若Tate对是可容许双线性映射，则进行邮件明文的加密。系统随机选取一个固定长度的字符串数组作为加密的会话密钥。然后，进行AES加密。AES加密分为三个阶段：初始化AES加密会话，AES加密，结束AES加密会话。在结束AES加密会话之前，将密文存入ciphertext.ibe文件中。

邮件明文加密完成后，使用BF-IBE方案中的加密算法加密AES会话密钥。首先，系统随机选取一个固定长度的字符数组。然后，使用哈希函数，计算得到，进而得到，。接着，使用哈希函数，将在有限域上的点哈希成一个固定长度的字符数组。通过和的异或运算，得到。再使用哈希函数对进行哈希运算，得到运算前的。最后，将其和进行异或运算得到。将的，转化成大整数型的和存入文件key\_file中。

4.2.5 解密算法流程

解密算法的执行过程：首先通过Boneh-Franklin的IBE解密算法得到AES会话密钥，然后使用AES解密算法得到明文信息。解密时，输入文件sysparams，privatkey，ciphertext.ibe，key\_file输出邮件的明文。在下文的描述中，代表会话密钥。是用户的私钥，是Miracl提供的ZZn2型变量。和都是字符数组。在进行解密之前，从sysparams中取出，，，提前产生一个以固定点构成的一个点群。这些点是有限域上满足方程：的椭圆曲线的点群的子群。确定椭圆曲线方程是。将，，这些点全部设置在该曲线上。从private\_key文件中读取出，通过计算得到其在椭圆曲线上的横坐标，并将设置在椭圆曲线上。然后，开始解密。解密流程图如图4-7：



图4-7 解密流程图

读取key\_file中的信息，使用BF-IBE解密，得到会话密钥。首先，通过的纵坐标，得到与其对应的横坐标，将其设置在椭圆曲线上。将和转换成固定长度的二进制的字符串。通过函数判断，，，，是否可以进行椭圆曲线上的Tate运算，并满足可容许双线性映射的性质；若不可以，则拒绝继续解密。若可以，则使用哈希函数，将哈希成一个固定长度的字符串。接着，将和进行异或运算，得到一个字符串数组。使用哈希函数将哈希成一个新的字符串数组。然后，将和进行异或运算，得到字符串数组。最后使用哈希函数，得到大整数，计算的值，和进行比较。若两者相等，则恢复；否则，无法得到。

若成功获得，则可以进行AES解密。解密分为三个阶段：初始化AES解密会话，AES解密，结束AES解密会话。最终，用户得到明文。

4.3 基于身份安全电子邮件系统的实现

4.3.1 模拟工具

本文使用Microsoft Visul C++作为开发工具，运用MIRACL[54]提供的BF-IBE具体实施方案的的整个算法流程，并结合JMail实现了电子邮件的发送和接收，模拟了PKG，用户和电子邮件服务器之间的通信过程。

MIRACL定义了新的数据类型大整数big和大有理数flash，涵盖了多倍精度算法的方方面面。其中，大整数的运算算法是基于Donald.E.Knuth在《计算机程序设计的艺术》中提出的算法。MIRACL是一个可移植的C函数库，提供了对称加密和非对称加密算法的实现方案，能快速实现加密和解密过程，并且计算效率高。针对大整数和大有理数，重载了各种运算，如基本的四则运算；提供了big和bytes相互之间进行类型转换的函数；它提供了AES加密的完整实现算法，给出了椭圆曲线加密和解密的实现流程。

JMail使网站具有发送和收取电子邮件的功能，是一免费的第三方邮件操作组件。它可以提供多方面的功能，在发送邮件的可以携带附件；提供了日志，便于检查邮件发送的问题；可以对邮件的优先级进行设置；提供了对多种格式的邮件的支持；提供了多种发送方式。另外，JMail使用方便，在进行开发的时候，仅仅需要在应用程序中引入jamil的动态链接库，就可以调用JMail实现邮件的发送和接收功能。

4.3.2 PKG主要功能实现算法

在该系统中，PKG主要完成两个方面的任务，一是产生系统参数和主密钥，二是对用户提出的请求作出响应。这个响应分为两种，一个是返回系统参数，二是返回用户的私钥。其中，系统参数通过系统初始化算法来实现，用户私钥通过用户私钥提取算法来实现。

1.系统初始化算法实现

系统初始化中，有两个关键因素：随机数产生器的选取和椭圆曲线方程的确定。以下对随机数产生器和椭圆曲线方程的确定展开描述。

MIRACL提供了随机数产生器。在系统未进行初始化时，先初始化一个Miracl的对象，预先对整个计算进行初始化。Miracl类的构成如下：

class Miracl

{

miracl \*mr; //结构体miracl指针变量mr

public:

Miracl(int nd,mr\_small nb=0) //整型变量mr\_small

{mr=mirsys(nd,nb); //初始化当前程序线程，返回miracl型指针

#ifdef MR\_FLASH //52

mr->RPOINT=TRUE;

#endif}

miracl \*operator&() {return mr;}

~Miracl() {mirexit();} //清除当前Miracl对象，释放所有内部变量

};

在Miracl类中定义的私有成员变量是一个结构体类型的指针，在MIRACL中给出了结构体miracl的具体定义。

Miracl类的构造函数中，最关键的是函数mirsys。该函数接收两个整型变量*nd*和*nb*。当创建一个Miracl的对象时，会自动调用该函数，完成以下的初始化工作：

（1）初始化MIRACL的错误追踪机制。

（2）为系统内的big或flash型变量产生以*nb*为基数的*nd*个数。

（3）初始化16个大整数型的工作变量。

（4）初始化某些实例变量。

（5）通过调动函数irand启动随机数产生器。

该函数的返回值，是一个miral结构体的类型指针。若返回空值，说明内存空间不够；若非空，则返回一个Miracl实例指针，使用这个指针可以访问所有的实例变量。在实际使用时，将这个指针赋值给一个miracl结构体指针。通过这个结构体指针，可以控制输入输出的基数。

对于PKG执行的算法，当的值改变时，MIRACL系统初始化产生的系统内big类型的变量也会随之发生改变。如，若是512位，可以在设置Miracl precision(16,0)；若是1024位，则precision是(32，0)。其中，0代表任意基数。

在确定椭圆曲线方程之前，对于MIRACL系统所使用的大整数进行简单的描述。在MIRACL中提供了Big类，它封装了大整数的基本属性和方法。整个方案中的运算，和大整数密切相关，其部分代码如下：

class Big

{

//成员变量

big fn;

public:

friend Big operator-(const Big&, int);

friend Big operator\*(int,const Big&);

friend Big operator\*(const Big&,const Big&);

friend Big operator/(const Big&,int);

… …

friend int bit(const Big& b,int i) {return mr\_testbit(b.fn,i);}

friend int bits(const Big& b) {return logb2(b.fn);}

friend Big pow(constBig&,int); // x^m

friend Big rand(const Big&); // 产生随机数

friend Big get\_modulus(void);

……

};

此外，模n剩余类ZZn[55]，n2上的算法类ZZn2，椭圆曲线模n[56]类ECn，椭圆曲线模n2类ECn2，有限域上的快速指数预计算[57]EBrick类对于椭圆曲线的构造，椭圆曲线上点的运算，以及椭圆曲线上的Tate对都很重要。本文不再对其进行详细说明。初始化实现时，输入安全参数后，通过函数irand启动随机数产生器，产生系统参数，，，，和，并存入文件sysparams和pkgmaster中。

在MIRACL系统初始化时，要确定BF-IBE加密方案和的位数。本文使用的素数是512位，是160位，MIRACL系统的初始化设置的是precision(16,0)。运行程序时，将其赋值给结构体miracl类型的一个指针*mip*。本文使用上的椭圆曲线，其方程：。通过计算，是一个固定值。是一个大素数，满足，即且。椭圆曲线方程的构造使用了ECn类，它定义的椭圆曲线模n的运算，提供了实例化椭圆曲线的方法。计算椭圆曲线在有限域上的立方根，使用的关键函数是ZZn2 randn2(void)和BOOL isunity()。任意选取椭圆曲线上的一点，通过它可以产生一个点群。通过rand()产生主密钥。最后通过和的运算，计算得到。

2.用户的私钥提取功能实现

当身份为ID的用户向PKG发送申请私钥请求时，PKG先根据用户的ID，采用map\_to\_point函数将用户的ID映射成椭圆曲线上的一个点，再采用公式，得到，的纵坐标就是用户的私钥。最后，将其以16进制字符串的形式写入privatkey中。

函数map\_to\_point是用户私钥提取的关键。先用哈希函数，将ID转化成一个在上小于模数的大整数。再将该大整数作为上椭圆曲线上某一点的纵坐标，计算得到横坐标，返回。其代码如下：

ECn map\_to\_point(char \*ID)

{

ECn Q;

Big x0,y0=H1(ID); //哈希函数

x0=getx(y0); //函数getx

Q.set(x0,y0);

return Q;

}

使用SHA-256[58]作为其基本哈希算法，MIRACL定义了SHA-256的结构体。描述如下：

typedef struct {

mr\_unsign32 length[2]; //无符号整型数组length

mr\_unsign32 h[8]; //无符号整型数组h

mr\_unsign32 w[80]; //无符号整型数组w

} sha256;

执行的算法过程如图4-8所示：

|  |
| --- |
| 输入：任意长度的字符串ID  输出：Big型数 |
| 1. Big型变量*h*，*p*；固定长度字符数组*s*；整型变量*i*，*j*；sha256结构体变量*sh*。 2. 调用函数shs256\_init初始化SHA-256算法。 3. 循环调用函数shs255\_process按字节处理ID，直至ID[*i*]=0。 4. 调用函数shs256\_hash将处理后的结果存入*s*。 5. 给*p*赋值，*p*是模数。 6. 令*h*=1，*j*=0，*i*=1。重新计算*s*，直至得到大于*p*的值*h*。 7. *h*%*p*，返回h。 |

图4-8 H1算法

函数getx，输入一个Big型的数，输出该值在椭圆曲线上的横坐标。设输入值是*y0*，输出值是*x0*。先调用函数get\_modulus()取得模数*p*，再通过*x0 =* (*y0 ^* 2 - 1) *^* (1 / 3) mod *p*得到*x0*。函数set用于判断输入的点的坐标是否是有限域上椭圆曲线上的一点。

4.3.3 邮件客户端加密解密功能实现算法

邮件系统客户端完成了两大功能：电子邮件的发送和接收，邮件的加密和解密。通过JMail实现邮件的发送和接收，以下部分对电子邮件加密和解密功能的实现进行描述。

1.加密功能实现

加密算法包括：AES加密和IBE加密。AES加密邮件正文，IBE加密AES的会话密钥。加密后，将信息分别存入ciphtext.ibe和key\_file中。

AES加密邮件正文是在固定区块长度（128位）下的分组加密，加密使用的密钥长度有3种：128，192和256。在进行AES加密时，调用了三个函数，分别完成了初始化AES加密会话、AES加密、结束AES加密会话。AES加密后，将密文存入ciphtext.ibe，AES加密的算法描述如图4-9所示：

|  |
| --- |
| 输入：明文  输出：密文 |
| 1. 调用函数brand产生固定长度的字符数组*key*。 2. 初始化长度为16的字符数组*iv*。 3. 调用aes\_init函数初始化aes加密会话。 4. 使用aes\_encrypt加密邮件明文。 5. 密文存入ciphertext.ibe中。 6. 调用aes\_end结束aes加密会话。 |

图4-9 AES加密算法

IBE加密会话密钥前，发件人要先从PKG处获取系统参数sysparams，再进行加密。在进行加密时，采用了EBrick类提供的初始化方法，得到了一个以固定点构成的一个点群。这些点是上的椭圆曲线的所有点的子集。椭圆曲线上的Tate对是实现IBE加密算法的关键，通过函数extract，g，fast\_tate\_pairing，ecap，line，vertical，判断椭圆曲线上的Tate对运算是否是可容许双线性映射。

BF-IBE方案加密会话密钥时，使用3个哈希函数：，，。

哈希函数，将一个上的ZZn2型的变量转化成一个固定长度的字符串，返回字符串的长度值。其算法描述如图4-10所示：

|  |
| --- |
| 输入：ZZn2型变量*x*，字符串*s*  输出：字符串*s*的长度 |
| 1. 定义结构体sha256变量*sh*，Big型变量*a*，*b*，整型变量*m*。 2. 调用shs256\_init初始化SHA-256算法。 3. 调用get方法转化*a*，*b*的形式。 4. *a*大于0，则循环调用shs255\_process按字节处理*m*。 5. *b*大于0，则循环调用shs255\_process按字节处理*m*。 6. 调用shs256\_hash将处理后的结果存入*s*中。 7. 返回*s*的长度。 |

图4-10 H2算法

哈希函数，将两个任意长度的字符串，转化成一个Big型变量。其算法描述见图4-11所示：

|  |
| --- |
| 输入：字符串*x1*和*x2*  输出：Big型数*a* |
| 1. 定义结构体sha256变量*sh*，Big型变量*a*，整型变量*i*，固定长度的字符串*h*。 2. 调用shs256\_init初始化SHA-256算法。 3. 调用shs256\_process按字节处理*x1*。 4. 调用shs256\_process按字节处理*x2*。 5. 调用shs256\_hash将处理后的结果存入*h*。 6. 将*h*转化为Big型的*a*，返回*a*。 |

图4-11 H3算法

哈希函数接收两个字符串作为输入，并将第一个字符串哈希运算后，存入第二个字符串。BF-IBE方案加密会话密钥后，将*U*的纵坐标，*V*和*W*存入key\_file中。

2.解密功能实现

收件人在进行解密之前，从PKG处获得了sysparams和privatkey，得到了发件人发送的信息。进行解密时，使用IBE的私钥解密，得到AES会话密钥；使用AES解密算法，得到邮件正文。IBE解密是IBE加密的逆过程，关键步骤是BF-IBE方案的解密算法和AES解密算法。

通过如图4-12所示的解密流程，执行BF-IBE方案的解密过程：

|  |
| --- |
| 输入：*U*，*V*，*W*  输出：会话密钥*key* |
| 1. H2处理*W*，得到*pad*，其中*W*通过Tate对计算得到。 2. V和*rho*异或运算得到*rho*，H4处理*rho*和*pad*，得到新的*pad*，*W*和*pad*异或运算得到*key*。 3. H3处理*rho*和*key*，得到一个大整数，该大整数模*q*，得到*r*。 4. 判断*rP*和*U*是否相等，若不等，则拒绝恢复*key*，反之，恢复*key*。 |

图4-12 BF-IBE解密过程

得到会话密钥*key*后，进行AES解密，其执行的算法流程如图4-13所示：

|  |
| --- |
| 输入：密文，会话密钥*key*  输出：明文 |
| 1. 初始化长度为16的字符数组*iv*。 2. 调用aes\_init函数，初始化aes解密会话。 3. 调用aes\_decrypt解密ciphertext.ibe，得到邮件正文。 4. 调用aes\_end结束加密会话。 |

图4-13 AES解密算法

4.3.4 PKG和用户之间的通信

PKG服务器和客户端用户使用TCP，通过VC++的WinSock[59]实现通信。

PKG服务器使用线程机制[60]处理用户的请求，包括监听线程，消息线程，文件线程。其中，消息线程用于服务器和客户端之间的消息交互，文件线程用于传输和接收文件，监听线程用于监听客户端的请求。本文在本地机上模拟了PKG服务器和客户端用户之间传输系统参数文件和用户私钥文件的通信过程。

首先，PKG服务器启动服务，绑定本地的一个端口号，监听客户端用户的连接请求。然后，PKG服务器端输入特定长度的随机数种子，运行系统初始化算法，产生系统参数和主密钥，并将其存入sysparams和pkgmaster中。当用户和PKG服务器建立连接后，PKG服务器根据用户发送的消息，确定用户需要的文件，并将文件发送给用户。当客户端用户发送消息是请求系统参数时，PKG服务器将系统参数文件发送给用户。用户收到系统参数文件后，将其保存在本地电脑上，便于以后进行加密。当客户端用户发出请求私钥的消息时，PKG服务器根据用户发送的电子邮件地址计算用户的私钥，并将用户私钥文件发送给该用户，用户将其安全保存，在以后解密时使用。在通信过程中的对象交互序列图如图4-14所示：

图4-14 PKG和用户交互序列图

4.3.5 邮件发送和接收

电子邮件的发送和接收使用是JMail组件来实现的，在邮件客户端应用程序中加入JMail动态链接库。

当用户邮件发送时，登陆邮件系统客户端，使用SMTP，设置服务器地址和端口号，填写与该服务器对应的邮箱的帐户名和密码，填写收件人的邮箱地址，编辑电子邮件。若采用加密功能，需要和PKG服务器之间建立连接，获取系统参数文件，然后进行加密，则将邮件加密后的密文信息发送出去。若不采用加密则将邮件直接发送出去。发送邮件时，可以实现附件的发送。

用户邮件接收时，使用POP，登陆邮件系统客户端，填写服务器地址和端口号信息，获取该邮箱服务器维护的电子信箱中的邮件。用户若收到加密的电子邮件，则需要和PKG服务器至之间建立连接，获取系统参数文件，同时获取与其电子邮件地址对应的私钥。然后使用该系统参数文件和私钥文件进行解密，得到明文。若是正常的电子邮件，则仍然可以正常读取邮件信息。

4.3.6 系统运行界面图和测试

1.PKG服务器界面图

当登陆PKG服务器后，得到的界面如图4-15，PKG服务器启动服务后，可以进行消息的发送和文件的传输。PKG服务器提供了系统初始化，用户私钥提取，发送和接收文件，发送和接收消息，判断用户请求功能。

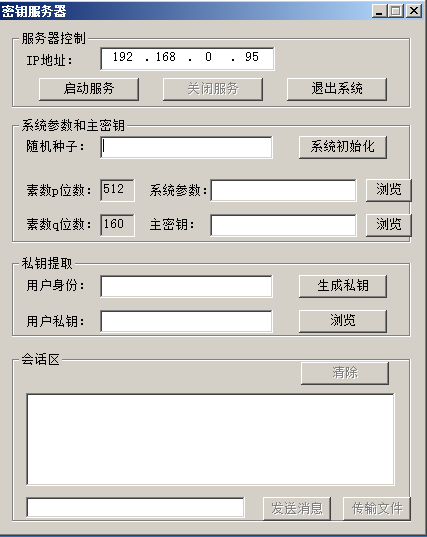


图4-15 PKG服务器运行界面图

2.客户端运行界面图

当启动客户端后的运行界面图如图4-16，当客户端用户连接了服务器之后，才可以进行消息的发送和文件的传输。用户登陆客户端向PKG服务器发送请求，获取系统参数文件，或者向PKG申请获取与自己邮箱地址对应的私钥。当PKG服务器响应用户请求后，用户接收从PKG服务器传送的文件并保存。

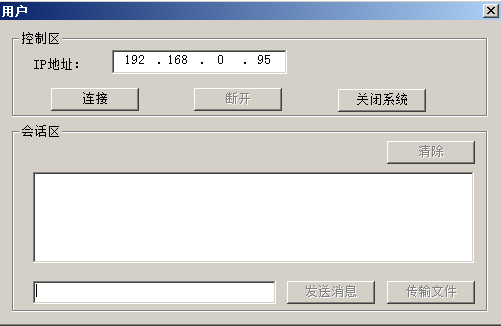


图4-16 客户端运行界面图

3.发送邮件界面图

用户发送邮件的界面图如图4-17：

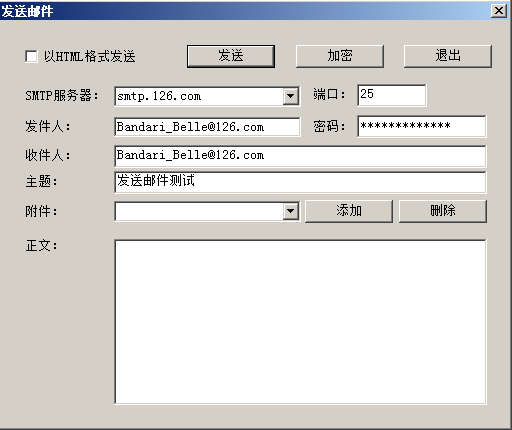


图4-17 发送邮件界面图

当用户要发送邮件时，必须填写完整的服务器和端口号信息。发件人的邮箱帐户，密码，收件人的邮箱地址，主题和正文，可以选择发送或者不发送附件，还可以选择邮件发送的格式。

4.接收邮件界面图

接收邮件界面图如图4-18，当用户将服务器地址，帐户名和密码信息填写完整后，可以从相应的服务器地址中，接收邮件。

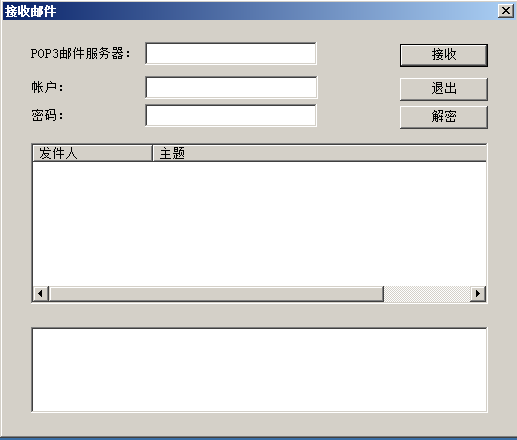


图4-18 邮件接收界面图

5.示例演示

PKG服务器在使用时，随机种子的输入，系统初始化功能和用户私钥提取功能需要可信者进行操作。

演示时，在PKG服务器端输入的随机数种子是：201603171。通信过程中使用邮箱地址是：Bandari\_Belle@126.com，发送的邮件正文信息是：阿拉伯联合酋长国。SMTP服务器和POP服务器分别为：smtp.126.com，pop3.126.com（pop.126.com）。在PKG服务器端运行系统初始化算法产生系统参数文件sysparams，其中的数据如下所示：

*PBITS*=512

*p*=DAA5F03F78DF1558C7046F5E4E506658C13389EFECB2B7AB5651C9EF6CCBDC54A0A2B8C37904A5350C4D44A82B118B7F53ED33287283B3CD26265CB5238E410B

*q*=8000000000000000000000000000000000020001

*Px*=AFA1CF769E03A374D961ECFE1CB185B137F759D76BFB53BD8F6C3BD587BB6D56D0116FACB83FBFC403BED8233D0A01CEC4BD0D94FFE7C5138956E8265C991932

*Py*=2DAAE53C6985DF9B7AFED9A6AAB526E9719E3ABBB7E07A22D4CFCFB385A88CE10B8D5DB99F63D6B0DB4B4EA4FC84939E4E5E57DA4BF06A71A4B7DAD37DE990AA

*Ppubx*=A1B4AB32F98DF6D5C6D783316C693597756BA50939962D368821FBE660129CC5B059CE3EAE7801E8CA7CCCE1271B4578A334652350C9DFCA9867BA1E104B6274

*Ppuby*=B28A7A21C278106773B506D15FB786D23326BE0B2556F8D557AF76BB618E348C55FB21636E480069A6B1642ABA628A06D64D692CE94736F7893EAF940D5CA19D

*cubex*=6D52F81FBC6F8AAC638237AF2728332C6099C4F7F6595BD5AB28E4F7B665EE2A50515C61BC82529A8626A2541588C5BFA9F699943941D9E693132E5A91C72085

*cubey*=91107063846979671FFC66113081A11C910F88A15EA4F3FBBD9DDF790EC303049F6B28AE6B13824A3B856CE8F66383E6E15A1DB1A4B453054B26639B9C54AD2E

发件人发邮件时，若不加密，则直接发送邮件正文；若加密，则发送加密后的邮件正文（ciphtext.ibe）和加密后的会话密钥（key\_file）。发件人发送加密邮件前，先和PKG服务器进行通讯，申请获得系统参数文件，再进行加密发送。其中，ciphtext.ibe中的内容是：锋Uq 踴E橘96|帚，key\_file中的内容如下所示：

*U*=75F905EC87EA44DFEECBFB51E0C103B02B4FC486946A630D06359ABB4659CB4634B4F17C34F4652AE03C5D2EA1BE9C262A64ED6AA0636854A9223543BF596780

*V*=6B4EA74D0F1A53FA7DFEE01D2A911C9F9C96847A67B65558AF9ECF662C387C01

*W*=B2D36A08420BAB14C746FE8C3768E3DE54F37185A70030AD2DEBF3C75C978D6D

图4-19是发件人加密后发送的邮件正文：

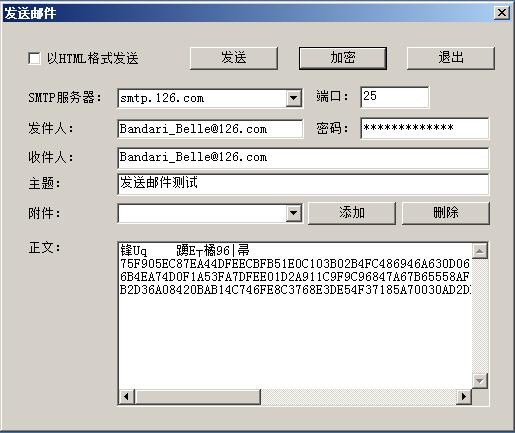


图4-19 发送方发送的邮件

收件人收到的邮件内容如图4-20所示：

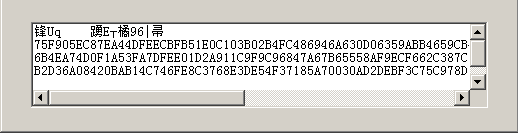


图4-20 收件人收到的邮件

收件人解密邮件前，先和PKG服务器进行通信，得到与其邮件地址对应的私钥，就可以解密得到明文，其私钥信息如下所示：

*Didy*=5CC348046D4C7DA4AA52F197E23CB2A2A62623F16C84A4B43DDE974F02FB2BDBC670B5A333572FD5D1896004E0C413C749C9F1D5DD685C350CFBE26A8E6546ED

收件人解密的结果如图4-21所示：

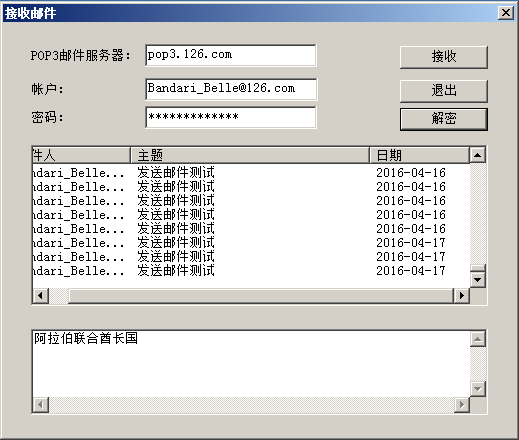


图4-21 接收方收到的邮件内容

5.测试

上文对设计的安全电子邮件系统的运行界面进行了演示，给出了一个演示的示例。另外，本文在本地机（OS：Windows7）上对该系统进行了测试，对邮件明文，包括汉字、中英文（大/小）写、符号（中/英）以及它们的组合进行了测试，测试结果表明，该系统可以实现邮件明文的安全传输。由于在发件人进行加密和收件人进行解密时需要和PKG服务器进行通讯，因而，该安全电子邮件系统在性能上比普通的电子邮件系统略弱，消耗的时间略长，这是进一步需要进行研究和探讨的工作。

4.4 本章小结

本章对BF-IBE具体实施方案，进行了深入研究分析。通过MIRACL提供的库函数，实现了BF-IBE具体实施方案的流程，并将其运用于安全电子邮件中。在本地机上模拟实现了密钥服务器和用户之间的通信过程，以及邮件客户端发送加密的电子邮件和解密加密的电子邮件功能。

1. 结论

5.1 研究工作总结

信息安全始终与任何人休戚相关，提高信息安全性是研究学者一直关注的焦点。对于在网络上传输的信息，对其进行加密是提高信息安全性采用的主要手段。非对称加密密码体制中，公钥是公开的。由于公钥公开，公钥在使用过程中，就产生了用户身份认证的问题。PKI使用数字证书，既实现了对用户公钥管理，又解决了用户身份认证问题。然而，数字证书的管理繁琐，对于系统或者用户来说都是耗时费力的。IBE采用与用户身份有关的字符串作为公钥产生的参数，在进行加密和解密的活动中，不再需要通过数字证书进行用户身份的审核，具有更好的应用前景。

IBE中，用户的私钥是通过PKG产生的，存在着密钥托管问题。私钥由PKG产生后，传输给用户，使得PKG又存在着私钥安全分发的问题。PKG产生私钥时，若不对用户身份的合法性进行审核，又会造成用户私钥泄露的问题。本文，针对这IBE密钥管理中存在的这三个方面的问题进行了研究。

1.对不同的解决IBE密钥管理问题的方案进行了介绍，分析和比较了不同方案的优点和缺点。

2.对Boneh和Franklin提出的基于秘密共享方案进行了研究分析，该方案从PKG的角度考虑解决用户私钥共享问题的解决办法，并没有完全解决用户的私钥托管问题。多个PKG合作，依然可以恢复用户的私钥。用户依然无法识别PKG的欺骗行为。各个PKG也没有对各自拥有的子秘密进行验证。针对这些问题，提出了一种改进方案，MPKG使用Feldman-VSS方案分发系统子秘密给CPKG，并将验证信息作为公共参数公布。TTA中维护了用户的ID，和。在产生用户私钥时，加入了用户选择的信息，由用户计算并将其和一同发送给各个CPKG申请获得。由于在合成用户私钥的过程中，加入了用户选择的信息，增加了TTA对用户和CPKG的行为进行监督，多个CPKG无法恢复用户的私钥，提高了用户私钥的安全性。TTA可以对用户选择的信息进行监听，设置用户密钥的有效期，从而实现了对密钥的撤销管理。最后，对该方案的正确性进行了分析证明，并将该方案同其他的采用秘密共享方案对密钥进行管理的方案进行了分析。

3.对Lee.B等人提出的采用一个KGC和多个KPA共同管理密钥的方案，针对该方案存在PKG假冒用户身份发动攻击，非法分子伪造KPA或KGC发送的部分私钥签名，以及认证次数过多，物理故障问题，提出了一种改进方案，加入了TTP，在密钥分发和密钥安全阶段对用户身份进行认证，监督KGC，KPAn和用户的操作；在KGC和KPAn产生部分私钥签名时，加入了时间T；针对用户和KPAn身份认证次数频繁的问题，在密钥安全阶段，采用了先将部分私钥和与之对应的签名发送给TTP，直到第n个KPA产生部分私钥和部分私钥的签名，再将该信息发送给用户，减少了KPA和用户之间的身份认证次数。最后，将改进的方案同其他同类方案进行了比较。

4.电子邮件中存在着安全隐患，将IBE应用于安全电子邮件中，可以避免证书管理。本文采用BF-IBE的具体实施方案，通过MIRACL提供的库函数，使用VC++ 6.0模拟了基于身份的安全电子邮件系统中密钥服务器和用户之间的信息交互，电子邮件客户端的发送加密的电子邮件，解密接收的电子邮件的过程，对于将IBE应用于实际中有一定的参考价值，将BF-IBE具体实施方案用于保证电子邮件也有现实意义。

5.2 研究工作展望

通过对BF-IBE基本方案的理论研究和实际应用模拟，对IBE密钥密钥管方案的分析和研究，总结本文的工作中存在的不足之处，对本文进一步的研究工作如下：

结合基于秘密共享方案的思想，对BF-IBE详细方案中的密钥管理问题进行的研究工作，在以下方面需要进行继续研究：

1. 由于使用的仍然是门限方案，所以并没有从本质上解决用户的私钥托管问题。在方案中，主要采用了可验证秘密共享方案的思想，对于子秘密正确性的判断，可以采用公开可验证的秘密共享方案，这是进一步的研究探讨工作。
2. 由于使用了第三方信任机构，监督了用户的行为，但是对于主PKG和子PKG之间可能存在的勾结行为并没有采取相应的措施。
3. 系统中对监听的设计对于在实际操作中的设计和详细的操作方案并未给出细致的研究和推导过程，这也是下一步密钥管理中需要考虑的问题。

针对Lee.B等人的方案提出的改进方案中，需要继续进行探讨的是：第三方信任机构的引入对于方案的安全性和效率有影响，如何在不引入可信第三方的前提下，解决方案中存在的问题，是需要进行进一步的研究和探讨的。

本文中的基于身份加密的安全电子邮件系统是一个模拟系统，将其应用于实际当中，需要进一步的深入研究。在进行邮件正文加密时，存在一些需要进一步解决的问题，如加密内容和加密内容的长度受到限制。此外，需要在电子邮件客户端实现签名功能，保证信息发送者无法否认他发送过该邮件。

致谢

诚挚地感谢我的导师李树全老师，在学习上指引我，在生活上关心我，在思想上影响我。在学术研究上，老师身体力行，兢兢业业，勤勤恳恳，数十年如一日，坚持目标，锲而不舍。在培养学生上，不遗余力，谆谆教诲，始终为学生的将来考虑。老师待人和蔼可亲，老师的一言一行影响着我，他教我如何做学问，如何做人，将对我今后的生活产生深远的影响。老师的深厚情谊我将终身难忘。

感谢我的师母在生活上的关心和照顾。

感谢大型主机实验室的所有老师，提供了良好的实验室学习环境。他们对学术研究的热忱，对科研事业的奉献，我看在眼里，记在心里，时时刻刻鞭策自己要努力学习，勤奋向上，不忘师恩。感谢实验室的所有师兄，师弟，师妹们，在学习上的互相探讨，共同学习，在生活上的互动互助，让研究生的生活丰富多彩。

感谢信息与软件工程学院的每一位老师，传授知识，扩展在计算机方面的见识和远见。

最后，感谢我的爸爸妈妈和我的弟弟，没有他们的无条件的支持，没有他们的包荣，没有他们的默默付出，就没有现在的我。感谢我的亲人，感谢他们对我的关心和关照。

感谢帮助过我的每一个人，感恩这段路上的相伴。

参考文献

1. 盘冠员.网络犯罪案件中的取证问题——从香港“艳照门”事件谈起[J].证据学论坛,2008, 00: 258-267
2. 苗圩.促进互联网安全健康可持续发展[J].中国经济和信息化,2014, 17: 20-21
3. 张靓.计算机网络信息安全及防护技术[J].通讯世界,2016, 01: 87
4. 俞承杭.信息安全技术[M].北京:科学出版社,2005
5. 范渊.信息安全的十大风险与实践[J].服务外包,2015, 04: 72-74
6. Hamid R, et al. Applied cryptography for cyber security and defense[M]. New York: IGI Global, 2010, 1-50
7. 包伟.对称密码体制与非对称密码体制比较与分析[J].硅谷,2014, 10: 138-139
8. 毕方明,苏成,张虹.网络通讯中基于对称密码体制的密钥管理[J].计算机工程与设计,2006, 27(10): 1749-1751
9. Arditti D, Charles O, Nguyen Ngoc S. ANONYMOUS AUTHENTICATION METHOD BASED ON AN ASYMMETRIC CRYPTOGRAPHIC ALGORITHM[P]. EP, EP1774699, 2007
10. Branscomb B, Black D, Perry J R. Network device identity authentication[P]. US, US7240364, 2007
11. Diffie W. The first ten years of public-key cryptography[J]. Proceedings of the IEEE, 1988, 76(5): 560-577
12. Lambrinoudakis C, Gritzalis S, Dridi F, et al. Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy[J]. Computer Communications, 2003, 26(16): 1873-1883
13. Spalding M. Deciding Whether or not to use a Third Party Certificate Authority[J]. Network Security, 2000, 2000(6): 7-8
14. Naor M, Nissim K. Certificate revocation and certificate update[J]. IEEE Journal on Selected Areas in Communications, 2000, 18(4): 561-570
15. Shamir A. Identity-based cryptosystems and signature schemes[C]. Proc of CRYPTO on Advances in Cryptology, Berlin, 1984, 47-53
16. Agrawal D P, Deng H, Mukherjee A. Threshold and identity-based key management and authentication for wireless ad hoc networks[P]. US, US8050409, 2011
17. Whitten A, Tygar J D. Why Jonny Can’t Encrypt: A Usability Evaluation of PGP 5.0[J]. Proceedings of the Ninth Usenix Security Symposium, 1999: 14-14
18. Yu J, Xia H, Zhao H, et al. Forward-Secure Identity-Based Signature Scheme in Untrusted Update Environments[J]. Wireless Personal Communications, 2015: 1-25
19. Mitchell M T, Kallman W R, Hoffman D L. SECURE EMAIL[P]. US, US20100031333, 2010
20. Dan B, Franklin M. Identity based encryption from the Weil pairing[C]. Proc of the Crypto Lncs, 2003, 213-229
21. Bleumer G. Random Oracle Model[J]. Encyclopedia of Cryptography & Security, 2005: 1027-1028
22. Dawson E, Donovan D. The breadth of Shamir's secret-sharing scheme[J]. Computers & Security, 1994, 13(1): 69-78
23. Chen L, Harrison K, Soldera D, et al. Applications of Multiple Trust Authorities in Pairing Based Cryptosystems[J]. Lecture Notes in Computer Science, 2002, 2437: 260-275
24. Gentry C. Certificate-based Encryption and the Certificate Revocation Problem[C]. Advances in Cryptology-Euroerypt’03, Berlin, 2003, 272-293
25. Ai-Riyami S and Paterson K G. Certifieateless Public Key Cryptography[C]. Advances in Cryptology-Asiaerypt 2003, Berlin, 2003, 452-473
26. Lee B, Boyd C, Dawson E, et al. Secure Key Issuing in ID-based Cryptography[C]. In proceedings of the Second Australian Information Security Workshop-AISW 2004, Australia, 2004, 69-74
27. Goyal V. Reducing Trust in the PKG in Identity Based Cryptosystems[C]. Proceedings of the 27th annual international cryptology conference on Advances in cryptology, Berlin, 2007, 430-447
28. Sherman S. M, Chow. Removing Escrow from Identity-Based Encryption[C]. International Conference on Public Key Cryptography–PKC 2009, Irvine, 2009, 256-276
29. Kocher P C. Timing Attacks on Implementations of Di e-Hellman, RSA, DSS, and Other Systems[C]. International Cryptology Conference on Advances in Cryptology, Santa Barbara, 1996, 104-113
30. Yow K C, Dabholkar A. A Light-Weight Mutual Authentication and Key-Exchange Protocol Based on Elliptical Curve Cryptogaphy for Energy-Constrained Devices[J]. International Journal of Network Security & Its Applications, 2010, 2(2): 123-132
31. Chen S L. A NOTE ON CHARACTER OF A FINITE ABLIAN GROUP[J]. Journal of Qingdao University, 2003
32. 孙家昶.特征值问题的预变换方法(II):任意三角形域Laplace特征值的计算分析[J].计算数学,2012, 34(1): 1-24
33. Kato K. Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via BdR. Part I[M].Germany: Springer Berlin Heidelberg, 1993, 50-163
34. Ohkawa K, Iijima T, Chao J. GHS attack to elliptic curves on cubic fields of odd characteristic using B.Smith's hyperellptic-to-nonhyperelliptic transform[J]. Technical Report of Ieice Isec, 2011, 110: 151-157
35. Maurer M, Menezes A, Teske E. Analysis of the GHS Weil Descent Attack on the ECDLP over Characteristic Two Finite Fields of Composite Degree[J]. Lms Journal of Computation & Mathematics, 2002, 5: 127-174
36. Somsuk K. Decreasing Size of Parameter for Computing Greatest Common Divisor to Speed up New Factorization Algorithm Based on Pollard Rho[M]. Germany: Springer Berlin Heidelberg, 2015, 399-405
37. Lang S. Complex Multiplication[M]. Germany: Springer Berlin Heidelberg, 1973, 37-56
38. Diem C. The GHS-attack in odd characteristic[J]. J.ramanujan Math.soc, 2003(1): 1-32
39. Heiden G J V D. Drinfeld modular curve and Weil pairing[J]. Journal of Algebra, 2004, 299(1): 374-418
40. Galbraith S D, Harrison K, Soldera D. Implementing the Tate Pairing[M]. Germany: Springer Berlin Heidelberg, 2002, 324-337
41. Renegar J. A polynomial-time algorithm, based on Newton's method, for linear programming[J]. Mathematical Programming, 1987, 40(1): 59-93
42. Park M S, Weon T. Method and apparatus for processing server load balancing by using the result of hash function[P]. US, US2014033417, 2014
43. Huggins A C, Ritzhaupt A D, Dawson K. Measuring Information and Communication Technology Literacy using a performance assessment: Validation of the Student Tool for Technology Literacy (ST 2 L)[J]. Computers & Education, 2014, 77(2): 1-12
44. Horwitz J, Lynn B. Toward Hierarchical Identity-Based Encryption[M]. Germany: Springer Berlin Heidelberg, 2002, 466-481
45. Patra R, Surana S, Nedevschi S. Hierarchical identity based cryptography for end-to-end security in DTNs[C]. International Conference on Intelligent Computer Communication and Processing, Cluj-Napoca, 2008, 223-230
46. Wang L. Research on Key Updating Issues of IBE with Wildcards[J]. Computer & Digital Engineering, 2012
47. Feldman P. A practical scheme for non-interactive verifiable secret sharing[J]. Foundations of Computer Science Annual Symposium on, 1987: 427-438
48. Kamikatano M, Tsumanuma T, Kashima T. Display apparatus, manufacturing method thereof, pattern display method, blind apparatus, and blind method[P]. US, US8372316, 2013
49. Olkin T M, Moreh J. Secure e-mail system[P]. US, US6584564, 2003
50. 吕立霞.基于PKI和S/MIME的安全WEBMAIL系统的研究与实现[J].网络安全技术与应用, 2008(6): 54-56
51. Myers J G, Myers J G. SMTP Service Extension for Authentication[J]. Rfc Internet Engineering Task, 2007
52. 陈磊.POP3协议的安全策略研究及其实现[D].上海:上海交通大学, 2008
53. Daemen J, Rijmen V. The Design of Rijndael: AES-The Advanced Encryption Standard[J]. Springer-Verlag, 2002: 229-234
54. 耿芹,冀承,张键红.基于MIRACL大数运算库的代理签名算法的实现[C].2008年全国数学与信息科学研究生学术研讨会(MIC 2008), 北京, 2008
55. 唐再良.论模n剩余类环Zn的性质与扩张[J].绵阳师范学院学报,2008, 27(8): 6-11
56. Dai Y J, Yang C. (t,n)Threshold Signature Encryption Scheme Based on Ellipse Curve Cryptosystem[J]. Application Research of Computers, 2004, 21(9): 142-143
57. 王成伟.快速有限域计算算法与实现研究[D].成都:电子科技大学, 2003
58. Gilbert H, Handschuh H. Security Analysis of SHA-256 and Sisters[J]. Lecture Notes in Computer Science, 2003, 3006: 175-193
59. 王晓鹏.TCP/IP下的Socket及Winsock通信机制[J].航空计算技术,2004, 34(2): 126-128
60. Ma J. Multi-Thread Programming Under MS Windows Using MFC[J]. Microcomputth Applications, 2000
61. Schoenmakers B. A simple publicly verifiable secret sharing scheme and its application to electronic voting[M].Germany: Springer Berlin Heidelberg, 1999, 148-164
62. Somayeh Heidarvand, Jorge L. Villar. Public Verifiability from Pairings in Secret Sharing Schemes[C].International Workshop SAC 2008, Sackville, 2009, 294-308
63. 申远.基于身份的密钥管理方案研究[D].开封:河南大学, 2009, 27-31
64. 陈静.基于身份的密码体制研究及其应用[D].成都:电子科技大学, 2005, 34-43
65. 刘学.基于身份的密码体制密钥管理研究[D].济南:山东大学, 2012, 26-36
66. 韦琳娜,高伟,梁斌梅.一种基于身份私钥的秘密共享方案[J].计算机工程, 2012, 38(23): 137-138
67. 封化民,孙轶茹,孙莹.基于身份认证加密的私钥共享方案及其应用[J].计算机应用研究, 2014, 05: 1507-1510.
68. 周加法.基于身份公钥密码的密钥托管问题研究[D].成都:信息工程大学, 2006, 13-20
69. Chaum D. Blind Signatures for Untraceable Payments[M]. US: Springer US, 1982
70. Zhang F, Kim K. ID-Based Blind Signature and Ring Signature from Pairings[M]. Germany: Springer Berlin Heidelberg, 2002, 533-547
71. J. Zhang, X. Su. Another Efficient Blind Signature Scheme Based on Bilinear Map[C]. Wireless Communications Networking and Mobile Computing (WiCOM) 2010 6th International Conference on, Chengdu, 2010, 1-4
72. Fangguo Zhang, Reihaneh Safavi-Naini, Willy Susilo. Efficient Verifiably Encrypted Signature and Partially Blind Signature from Bilinear Pairings[J]. Lecture Notes in Computer Science, 2004, 2904: 191-204
73. Zhang X J. Two Improved ID-based Proxy Blind Signatures[J]. Computer Engineering, 2009, 35(3): 15-17
74. Ribarski P, Antovski L. Comparison of ID-based blind signatures from pairings for e-voting protocols[C]. International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija, 2014, 1394-1399
75. Antončić, V, Galinović, A. Key management in Identity Based Encryption schemes[C]. MIPRO 2010 Proceedings of the 33rd International Convention,.Opatija, 2010, 1235-1239
76. Oh J H, Lee K K, Moon S J. How to solve key escrow and identity revocation in identity-based encryption schemes[C]. International Conference on Information Systems Security, Kolkata, 2005: 290-303
77. 杨彦炯.(t,n)门限秘密共享体制的研究[D].南京:南京理工大学, 2008, 10-13
78. Pedersen T P. Non-interactive and information-theoretic secure verifiable secret sharing[M]. Germany: Springer Berlin Heidelberg, 2001, 129-140
79. Stadler M.Publicly verifiable secret sharing[M]. Germany: Springer Berlin Heidelberg, 2001, 190-199
80. Fujisaki E, Okamoto T. A practical and provably secure scheme for publicly verifiable secret sharing and its applications[M]. Germany: Springer Berlin Heidelberg, 2010, 32-46
81. Jhanwar M P. A Practical (Non-interactive) Publicly Verifiable Secret Sharing Scheme[C]. International Conference on Information Security Practice and Experience. Springer-Verlag, Guangzhou, 2011, 273-287
82. Tian Y, Peng C, Ma J. Publicly Verifiable Secret Sharing Schemes Using Bilinear Pairings[J]. International Journal of Network Security, 2012, 14(3), 116-122
83. Kahrobaei D, Vidaurre E. Publicly Verifiable Secret Sharing Using Non-Abelian Groups[J]. Eprint Arxiv, 2014
84. 宋敏.盲签名技术理论及应用研究[D].济南:山东大学, 2013, 7-8
85. 刘雁孝.(k,n)门限密钥共享技术研究[D].西安:西安电子科技大学, 2012, 23-27
86. 李大伟,杨庚,朱莉.一种基于身份加密的可验证秘密共享方案[J].电子学报,2010, 38(9): 2059-2065
87. Dan B, Boyen X. Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles[J]. Journal of Cryptology, 2004, 2004(4), 223-238
88. Sahai A, Waters B. Fuzzy Identity-Based Encryption[J]. Lecture Notes in Computer Science, 2004, 3494: 457-473
89. 王进.基于身份密码体制及其应用的研究[D].济南:山东大学, 2007, 41-47
90. 王宣丹.IBE关键技术的研究及在安全电子邮件中应用.哈尔滨:哈尔滨理工大学, 2009, 26-33
91. Luther Martin. Introduction to Identity-Based Encryption[M]. Boston: Artech House, 2008, 16
92. 彭海涛,史清华.基于身份加密的安全电子邮件系统[J].计算机工程, 2005, 13: 124-125+150
93. 杨浩淼,孙世新,李洪伟. 基于身份加密的非交互式密钥吊销[J]. 计算机应用, 2006, 02: 332-334
94. 侍伟敏. PKI、IBE关键技术的研究及应用[D].北京:北京邮电大学, 2006, 4
95. 刘宏伟.基于身份的电子签章系统设计研究[J]. 计算机工程与设计, 2008, 22307: 1735-1738
96. 徐剑,李晶,张钊,周福才.基于身份密码体制的安全电子邮件系统[J]. 计算机工程, 2009, 32809: 179-181+184
97. 赵旭东.一种基于身份加密的安全电子邮件方案研究与实现[D].成都:西南交通大学, 2010, 31-46
98. 王皓.基于身份密码体制的研究[D].济南:山东大学, 2012, 13-14
99. 马春光,王九如,武朋,张华. 基于M-IBE的异构传感网密钥管理协议[J]. 计算机研究与发展, 2013, 5010: 2109-2116
100. 王磊.基于身份密码体制的研究及其在即时通信中的应用[D].沈阳:东北大学, 2013, 33-59
101. 王维.基于Mozilla Add-On的IBE邮件加密研究[D].武汉:武汉理工大学, 2014, 77-81
102. 刘镪,王胜男.基于身份标识的密码体制及其在安全电子邮件的应用[J]. 信息安全与技术, 2014, 5206: 70-72
103. 续素芬,李树国.基于身份加密体系IBE的软件实现[J]. 计算机应用与软件, 2015, 3204: 301-304+325
104. 周绍午.一种基于身份的密码体制的保密电话方案[J]. 移动通信, 2015, 39816: 77-81

攻读硕士学位期间取得的成果

论文：

1. 李树全,李玉欢.基于Asmuth-Bloom门限体制的IBE私钥共享方案[J].计算机应用研究, 2016（已录用，待刊）

科研项目：

1. 电子科技大学新实验室建设项目.银行主机系统. 2014
2. 电子科技大学新实验室建设项目.主机专业工程能力综合训练课程II-主机移动系统应用开发. 2015

奖学金：

1. 电子科技大学研究生学业二等奖学金. 2013
2. 电子科技大学研究生学业三等奖学金. 2014