# 基于 IBE Service 的新型文件加密系统①

施　健，陈铁明，茆俊康

(浙江工业大学 计算机科学与技术学院，杭州 310023)

**摘　要**：基于身份的公钥加密(Identity-based Encryption，简称 IBE)体制采用用户 ID 作为公钥，无需公钥证书操作，较传统的 PKI 体系具有开发部署简单、应用成本低等优势，尤其适用于密钥集中式管理的企业级应用。设计了一个基于 Web Service 的 IBE 密钥管理服务系统 IBE Service，实现各个网络安全域内的用户密钥管理，提供以用户安全策略为中心的密钥服务；基于 IBE Service 开发了一个面向通用文件加密的客户端应用，主要通过 SOAP 服务接口实现基于 XML 的 IBE 密钥数据交互。新型的文件加密系统可将接收方 ID 直接映射为公钥，接收方自动向 IBE Service 获取私钥完成文件解密，具有安全、便捷等优点，且支持灵活的 ID 安全策略管理。

**关键词**：文件加密；IBE；Web Service；SOAP；XML

## File Encryption System Using IBE Service

SHI Jian, CHEN Tie-Ming , MAO Jun-Kang

(College of Computer Sci. & Tech., Zhejiang University of Technology, Hangzhou 310023, China)

**Abstract**：Identity-based public key encryption (short for IBE) system can directly take user's ID as her public key, without need of public key certificate. Comparing to the traditional PKI, IBE is easy to develop and deploy with lower cost. It is specially suited for the enterprises with centralized key management supported. In this paper, a web service-based IBE key management service system, IBE Service, is firstly proposed, which facilitates users of different security domains to manage IBE keys and provides a user secure policy-centered key service. Based on IBE service, a general file encryption client application is then developed. It utilizes SOAP protocol to implement XML-based IBE key data communications. The proposed new file encryption system can map the receiver's ID as her public key, and the receiver can automatically do decryption by achieving her private key from IBE service. It is more secure, efficient, as well as with flexible ID secure policy supported.

**Key words**：file encryption; IBE; web service; SOAP; XML

## 1　引言

对称密码系统是一种比较传统的加密方式，其加密运算、解密运算使用的是相同的密钥，信息的发送者和信息的接收者在进行信息的传输与处理时，必须共同持有该密码。这就需要足够强的加密算法和安全的密钥管理，因而对称加密主要问题有两点：第一，密钥量问题。在单钥密码系统中，每一对通信者就需要一对密钥，当用户增加时，必然会带来密钥量的成倍增长，因此在网络通信中，大量密钥的产生．存放题。对称密码系统中，加密的安全性完全依赖于对密钥的保护，但是由于通信双方使用的是相同的密钥，人们又不得不相互交流密钥，所以为了保证安全，人们必须使用一些另外的安全信道来分发密钥，代价非常大。

结合公钥加密实现高安全强度的文件加密是改善对称加密的一种方法。目前 PKI[1]已成为业界标准的密钥管理平台，是一套基于公开密钥理论和技术建立起来的安全体系。PKI 的基础技术包括加密、数字签名、数字信封、数据完整性机制等。但是，PKI 系统涉及复杂的数字证书管理，服务器成本高、互操作性差、

① 基金项目:浙江省科技计划项目(2010C31126; 2011C21046);2010 年度浙江省大学生科技创新活动计划项目.
收稿时间:2011-09-07;收到修改稿时间:2011-11-08

用户使用复杂[2]等，从很大程度上阻碍了其应用推广。采用 IBE 体制[3,4]，无需使用数字证书，用户无需管理自己的私钥，可由密钥服务器动态集中生成，系统灵活性大，服务器运行和开发成本低。IBE 体制目前在国际上引起了极大关注，在欧洲部分国家已开始替代 PKI 的计划，有望成为信息安全的新一代标准。

本文即将研究开发一套基于 IBE Service 的文件加密安全应用系统，主要包括基于 Web service[5]的 IBE 密钥管理服务和 IBE 文件加密客户端两部分。IBE 密钥管理服务负责用户的身份管理和认证，以及用户 IBE 密钥请求、密钥生成、密钥策略等管理；IBE 客户端则主要负责对任意文件的加密和解密操作，通过 SOAP 消息交互获得所有相关的 IBE 密钥管理服务。

## 2 基于Web Service的IBE密钥托管服务

### 2.1 IBE 基本原理

IBE 的基本思想是用于加密的公钥可以是用户指定的任意字符串，其加解密过程一般可以分为四个步骤：即参数生成(Setup)算法、密钥生成(Extract)算法、加密(Encrypt)算法和解密(Decrypt)：

初始化：Setup(M,C,s,$P_{pub}$,*)，生成系统参数和系统主密钥 s，其中 M 为有限的消息空间，C 为有限的密文空间，(s, $P_{pub}$)为主密钥对，*表示其它的一些参数。这里的主密钥 s 严格保密，只有 PKG 知道。

密钥生成：Extract(ID)=$d_{ID}$，利用系统主密钥生成对应用户身份信息的解密私钥，其中 ID 为解密者身份信息，$d_{ID}$ 为解密私钥。

加密：$Encrypt_{ID, P_{pub}}(M) = C$，用消息接受者的身份消息对消息加密，M 为明文消息，C 为对应密文。

解密：$Decrypt_{dID, P}(C) = M$，对密文用相应密钥解密。

IBE 对其中第二步密钥生成与第三步加密没有严格的先后顺序，这也是跟证书加密不同的地方，密钥可以后产生。

### 2.2 IBE 密钥托管服务

在一个基本的 IBE 应用框架中，PKG 作为集中式密钥服务器是系统的核心。IBE 体制无需公钥证书，私钥可由用户向 PKG 请求时动态产生，无需密钥备份机制。用户只要获得 PKG 系统的公开参数，利用接收方的 ID 即可完成基于 IBE 的加密通信；接收方通过 PKG 的身份认证后即可获得其 ID 对应的解密私钥。

IBE 是一种安全、灵活、高效的集中式应用方案，适用于企业级网络安全应用框架，但结合 PKI 体制可有效扩展到 Internet 安全应用。构建 IBE 应用体系需解决的主要问题集中在：PKG 公开参数的管理：PKG 公开参数的安全发布、更新，及不同参数的管理；用户请求的身份认证：用户向 PKG 请求私钥时的大规模身份认证的安全问题；PKG 私钥的安全分发：PKG 向用户分发私钥的安全通信及私钥安全存放问题；用户身份的策略管理：接收方用户 ID 蕴含的安全密钥策略及撤销机制等设计。

### 2.3 密钥管理服务系统

IBE 密钥管理服务的设计目标是为安全应用程序屏蔽 IBE 公钥体制的实现差异，提供一个基于 Web Service 的可信第三方安全服务层。系统总体结构如图 1 所示，以安全策略为中心，包括身份注册管理策略、域和参数管理策略以及安全密钥管理策略，实现 IBE 私钥管理 PKG 服务接口、身份认证服务接口、消息处理接口等系统管理功能。系统向下提供各种 PKG 基础设施的接入服务，支持不同安全域不同系统参数的 PKG；向上提供基于 XML 的 IBE 密钥管理服务[6]，支持各类基于 IBE 的安全应用客户端所需的密钥安全管理服务，本文实现的是一个文件加密客户端应用。

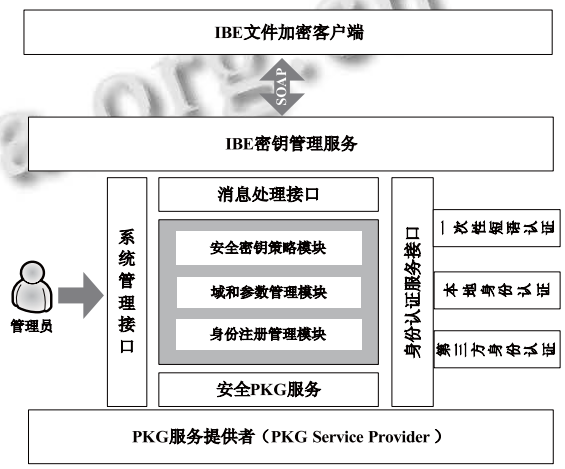


图 1 IBE Service 密钥管理服务系统总体结构

(1) 系统管理模块

系统管理模块主要包括用户身份注册与管理、域和参数管理、XML 密钥策略规范、私钥安全分发方案，以及系统消息统一处理等功能。

身份注册管理支持分层的用户管理，实现组织内部的 RBAC 权限管理与控制，数据库可采用高效的 LDAP 目录存储协议。域和参数管理支持同一个 PKG 服务下不同的域和参数管理。由于 IBE 加密体制下的身份 ID 即代表了用户公钥信息，因此域及参数信息可包含在 ID 中，使公钥的查询和验证具备语义功能。安全密钥策略指定 IBE 的密钥生成和发布方式。例如，A 发送加密信息给 B：先从 IBE 服务平台获得关于 B 所在域的加密公开参数和密钥策略，包括 IBE 加密算法（包括密钥强度）、B 的身份信息（包含撤销策略）、B 向 PKG 请求私钥的安全认证方式等。私钥安全分发是 IBE 应用的安全核心。IBE 密钥管理服务至少应支持服务器单向认证的 SSL 协议，再利用带外方式产生的一次性短语加密私钥（或用户身份注册时的加密口令），通过加密通道安全发送给用户，用户利用一次性短语解密得到私钥。消息统一处理接口为用户与系统之间建立快速、高效、安全的消息交互机制，采用基于 XML 的 SOAP 协议封装消息，具有良好的扩展性。消息处理模块可使用户实现密钥管理服务的异步请求方式，提高 IBE 密钥管理系统的服务性能。

(2) 身份认证模块

身份认证模块主要解决用户向 IBE 密钥管理服务请求密钥管理服务时的安全认证，是系统安全运行的基本保障。为了灵活支持多种安全认证方式，并具有良好的扩展功能，系统设计了独立的身份认证服务接口层，为系统安全认证提供接入服务，也可与本地 PKG 系统的无缝集成提供接口。概括地讲，身份认证接口支持挑战-应答式的交互认证、本地用户口令认证、第三方认证服务等三类认证方式。

(3) 密钥生成模块

IBE 的密钥生成模块 PKG 是 IBE 密钥管理系统的技术核心，系统设计了一个基于双线性对的内置安全 PKG 服务，提供基本的 IBE 密码服务。与身份认证模块一样，为了支持分布式异构 PKG 的接入，系统设计了独立的 PKG 服务提供接口，为第三方 PKG 提供安全接入服务，通过 IBE 密钥管理服务对外提供统一的服务接口，有效屏蔽异构 PKG 之间的差异。

(4) 密钥管理服务

为了便于用户在线管理自己的 IBE 密钥，本系统设计提供了用户登录和密钥管理操作界面，具有如下功能：1、增加新私钥标识 ：点击新增按钮，跳转增加新私钥标识界面。用户选择私钥标识类型(邮箱还是其他类型)，用户输入私钥标识，选择私钥的有效期(系统提供)，如果用户选择的是其他类型，还要求用户选择绑定的邮箱(邮箱为用户已激活成功的私钥标识)，ajax 检验私钥标识是否已经被注册。点击提交，后台获取数据，存储到数据库并自动向绑定邮箱或私钥标识发送激活邮件。2、私钥管理：点击私钥管理，页面或显示私钥标识的信息，包括(私钥标识，注册时间，是否生效，私钥到期时间，查看下载历史，查看激活历史，下载用私钥，私钥的撤销，删除)。对于已生效的私钥标识，用户只能对其进行撤销操作，对于失效的私钥标识，用户可以进行删除操作。私钥的下载操作，只有在私钥标识生效的时候才可以进行操作。如果私钥没有激活，用户可以点击重激活来向邮箱重新发送激活邮件已完成注册。

## 3 基于IBE Service的文件加密客户端

### 3.1 IBE 密钥托管服务

所开发的客户端软件可以加密任何类型文件。首先将原文件使用 AES 加密，之后再将 AES[7]的密钥使用 IBE 加密，生产一个安全的文件数字信封。因此，文件加密和解密的基本流程如图 2 和 3 所示。客户端通过 SOAP 协议与服务器进行交互。客户端通过与服务器的交互完成验证用户、下载参数、下载私钥、时间校对等动作。用户的私钥会存放于用户的 PC 上，处于安全性的考虑。客户端的私钥使用 AES 加密存放。同时，客户端使用时间期限的安全

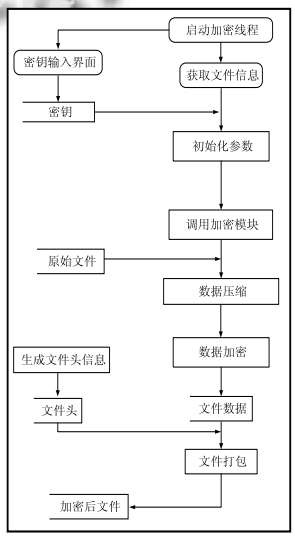


图 2 文件加密流程

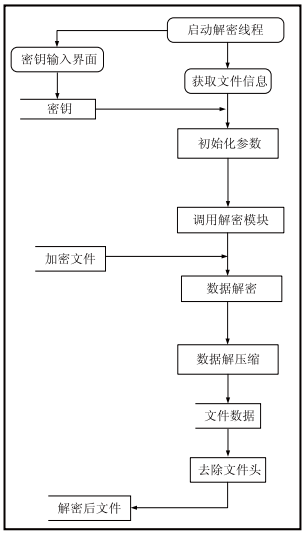


图 3 文件解密流程

策略，当客户端私钥超过期限（如一个月），客户端会删除该私钥。

### 3.2 文件加密数据结构

设计密文头部数据结构如图 4 所示。

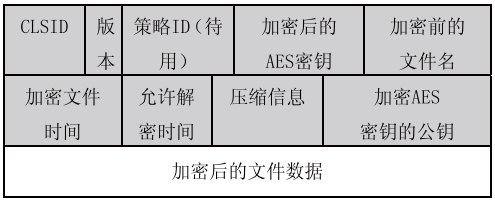


图 4 基于 IBE 和 AES 的文件加密结构图

其中，CLSID 表示唯一的文件格式标识符。AES 的密钥使用 IBE 加密，存放于文件头部，而 IBE 的私钥存放于 IBE 托管服务器端，加密时使用公钥，解密时使用私钥，公钥是公开的，而私钥则在服务器端保存，需要时联网下载。私钥在网络传输以及在客户端上是加密存放的，加密的密钥是用户的密码。

## 4 系统测试与安全分析

### 4.1 文件加密解密性能

采用 Visual C++ 6.0 开发实现了基于 IBE 的文件加密客户端，可实现对任意文件的加密和解密操作。为测试加密性能，在 Windows XP SP3 环境下（CPU 为 AMD Athlon(tm) II X2 240 Processor 2.81 GHz，内存为 DDR2 2GB），对 160MB 大小的二进制编译文件进行了加密测试，并与目前流行的 PGP 文件加密进行了对比，测试结果表明本文开发的文件加密具有安全强度大、密钥长度小、执行效率高等优势。

表 1 文件加密性能对比结果

| CLSID | 版本 | 策略ID（待用） | 加密后的AES密钥 | 加密前的文件名 |
|---|---|---|---|---|
| 加密文件时间 | | 允许解密时间 | 压缩信息 | 加密AES密钥的公钥 |
| 加密后的文件数据 | | | | |

### 4.2 系统安全性讨论

AES 算法的安全性：AES 算法基于排列和置换运算，其作为新一代的数据加密标准汇聚了强安全性、高性能、高效率、易用和灵活等优点，在各领域广泛运用。

IBE 算法的安全性：IBE 可以采用椭圆曲线(ECC)算法，理论计算表明，ECC160 位参数的安全强度与 RSA1024 位参数相当，效率很高。

通信的安全性：通信过程中的重要数据由 AES 加密传输，并采用 SSL 协议，安全性高。

系统的安全性：AES 的密钥使用非对称的 IBE 加密保护，避免了密钥传递过程中可发生的安全问题。IBE 密钥使用托管服务器管理，即系统的安全性依赖于托管服务器。只要服务器是安全的可信赖的则系统的安全性具有保证。

但是，由于 IBE 的密钥是由托管服务器进行集中式管理。一旦服务器被攻破，或者托管服务器不能被信任，则会出现但单点失效的问题。建议用户使用可以信赖的服务提供方。例如，学校的学生可以使用所在学校提供的密钥托管服务。

## 5 结论

基于身份的公钥文件加密系统提供了 IBE Service 密钥管理服务,并在此基础上实现一种面向通用文件加密的客户端应用。IBE service 密钥管理服务是一个基于 Web Service 的可信第三方安全服务层，提供各种安全策略。客户端应用以接收方身份 ID 为公钥，将 AES 加密后的密钥再经过 IBE 加密,可以通过与 IBE service 服务进行数据交互，接收方通过向 IBE Service 请求对应的私钥解密，安全方便。该系统可以为用户提供安全、高效、便捷的加密服务，同时能与其它应用系统无缝集成，具有良好的拓展性。

## 参考文献

1 荆继武,林璟锵,冯登国.PKI 技术.北京:科学出版社, 2008.5.
2 张剑青,刘旭东,怀进鹏.基于 XML 的密钥管理的研究与实现.计算机研究与发展,2003,40(1):75−80.
3 Boneh D, Franklin MK. Identity−Based Encryption from the Weil Pairing Advances in Cryptology Proceedings of CRYPTO 2001. IEEE, 2001:235−248.
4 胡亮,初剑峰,林海群,袁巍,赵阔. IBE 体系的密钥管理机制.计算机学报,2009,32(3):544−556.
5 沈雪.基于 Web Services 的分布式优化算法服务平台的实现[硕士学位论文].浙江大学, 2007.
6 陈铁明,李伟.IBE-XKMS:一个基于 XML 的 IBE 密钥管理服务体系.电信科学,2010(7):121−127.
7 Daemen J, Rijmen V. AES Proposal: Rijndael. AES Algorithm Submission, September 3, 1999.