第 35 卷 第 6 期 计 算 机 工 程 2009 年 3 月
Vol.35 No.6 Computer Engineering March 2009
·安全技术· 文章编号：1000—3428(2009)06—0194—03 文献标识码：A 中图分类号：TP309

# 基于身份密码的安全电子邮件系统

张 鹏，陈 焘，刘宏伟，喻建平
(深圳大学智能信息研究所，深圳 518060)

**摘 要：**针对现有电子邮件系统中的安全性问题，采用基于身份的密码体制和基于内容的过滤扫描技术，构建具有反垃圾/反病毒功能的邮件服务器及具有涉密扫描功能的邮件网关服务器，设计并实现了邮件系统客户端及其必备管理控制中心。系统具有扫描并过滤涉密邮件、加密或解密邮件、签名或认证邮件等功能，能够满足在不可控、动态和松散企业组织成员间的安全通信。
**关键词：**基于身份；公钥密码；涉密扫描；网关服务器；安全电子邮件

# Secure E-mail System Identity-based Encryption

ZHANG Peng, CHEN Tao, LIU Hong-wei, YU Jian-ping
(Graduate School of Intelligent Information, Shenzhen Univ., Shenzhen 518060)

**【Abstract】** For the secure problems existing in current E-mail systems, this paper establishes the mail server which filters the spam and virus, and the gateway server which filters the secret-involved mails. It accomplishes the secure mail client and the manage control center with the technology of identity-based cryptography and content-based filtering. The system can provide safe communications between these enterprise employees who are uncontrollable and dynamic.
**【Key words】** identity-based; public key cryptography; secret-involved scanning; gateway server; secure E-mail

## 1 概述

电子邮件是 Internet 上应用最广泛的服务之一。邮件应用的不断发展直接导致了邮件自身价值的不断增加，然而现有的电子邮件系统正受到来自各方的安全威胁。例如明文传输的电子邮件被截获造成敏感信息泄漏；病毒邮件的肆虐及垃圾邮件的恶意侵扰消耗了大量的网络资源；机密性较高的商业信息容易被内部员工以电子邮件的形式泄漏等。

对此，多种安全电子邮件方案已被提出并在特定领域中发挥作用，如 PGP[1]，S/MIME[2]等。这些方案的共同特点是使用公钥基础设施 PKI 提供的公钥和私钥对电子邮件进行加密、解密和签名、验证，其中公钥以公钥证书的形式颁发[3]。因此，当用户数量逐渐增多时，密钥的管理将变得非常困难。此外，人们一直通过各种各样的产品来解决网络安全问题，每种产品解决一种问题，随着问题的日益复杂，需要不停地累加相应的产品。这种点状的解决方案不仅增加了实现和管理方面的任务和成本，还导致了网络冲突的大量发生。

针对现有电子邮件系统的以上不足，本文提出了基于身份的短签名方案及风险自适应的最小风险贝叶斯算法，设计并实现了一个基于身份密码体制的综合防泄密反垃圾反病毒等多种功能的安全电子邮件系统。从功能的完整性出发架构系统，使得系统具备加密解密、签名及认证、防止企业机密信息泄漏、抑制垃圾、病毒邮件泛滥等诸多功能，能够应对当今社会的混合型威胁。

## 2 系统设计

### 2.1 系统构架

本系统在 Red Hat Enterprise Linux 4 平台上配置了 Postfix2.2.5 SMTP 服务器，基于 Postfix2.2.5，集成 Amaivs 组件和 ClamAV 组件，配置了具有反垃圾/反病毒功能的邮件服务器、具有拦截涉密邮件功能的网关服务器；在 Linux 4 平台上实现了涉密邮件过滤模块和黑白名单及涉密邮件的管理模块；在 Windows XP 平台上实现了用户端的加密和解密邮件消息、签名及身份认证、私钥生成和安全传送、密钥管理、网关控制管理等一系列的功能模块。系统模型如图 1 所示。

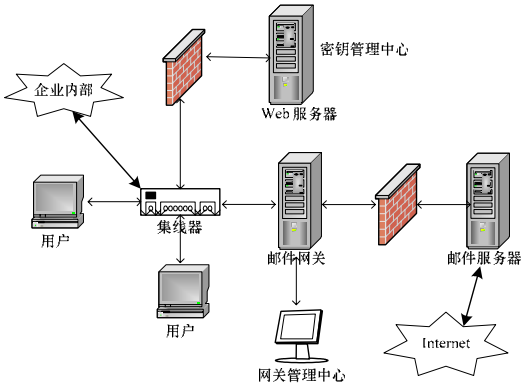


**图 1 安全电子邮件系统模型**

### 2.2 系统流程

假设用户已经在邮件服务器及网关服务器上注册通过，则服务器上存储所有注册用户的用户名和口令的 Hash 值对 $(H(ID), H(password))$，则电子邮件的交互流程如下：

(1)发方通过自己的用户名和口令对登录密钥管理中心 Web，从中提取自己的加解密及签名认证密钥。

(2)发方在系统客户端配置正确的 SMTP 服务器及 POP3

**基金项目：**国家“863”计划基金资助项目(2003AA142060)
**作者简介：**张 鹏(1984－)，女，硕士研究生，主研方向：信息安全；陈 焘，硕士研究生；刘宏伟，博士；喻建平，教授、博士生导师
**收稿日期：**2008-08-30 **E-mail：**zhangpeng_aza@126.com

服务器，输入正确的用户名和口令方能登录，后导入自己下载的相关密钥。

(3)编写邮件、加密签名并发送邮件。

(4)发往 Internet 或内部其他用户的电子邮件被网关服务器拦截，首先对加密邮件进行解密，如图 2 所示，然后进行涉密信息过滤，合法的邮件将由邮件网关继续发送到邮件服务器进行垃圾邮件和病毒邮件过滤。另 Internet 发往内部用户的邮件将进行垃圾邮件和病毒邮件过滤，合法的邮件将保存在邮件服务器上，如图 3 所示。

(5)收方通过邮件用户代理 MUA(Mail User Agent)来取信、读信。加密邮件的解密过程如图 2 所示。

(6)收方在收到邮件后可以到密钥管理中心下载对方公钥对发方身份进行验证，查看邮件的完整性及真实性。

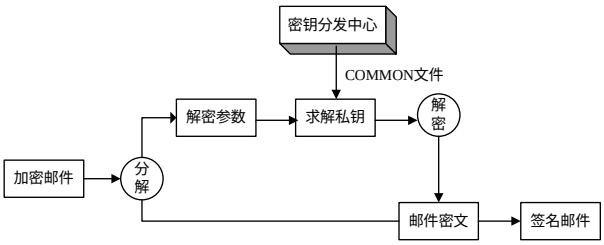


**图 2　解密邮件**

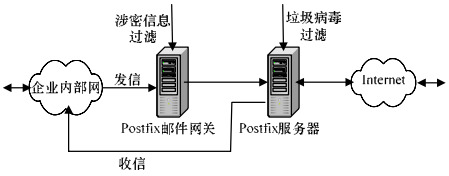


**图 3　过滤系统总框架**

## 3　系统实现

### 3.1　网关管理中心

网关的整个涉密扫描流程如图 4 所示。涉密扫描程序接收外部传过来的参数，比如待扫描邮件的邮件 ID，发信方地址，收信方地址，发信时间和邮件内容等。邮件 ID 唯一确定一封电子邮件，发信方地址和收信方地址用于黑白名单判断，而邮件内容主要用于进行规则匹配。默认设置涉密邮件的阈值为 5.0，也就是说权重值累计超过 5.0 的邮件就会被拦截下来。

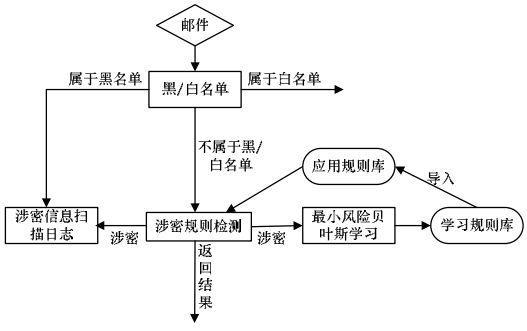


**图 4　涉密邮件扫描流程图**

描述涉密邮件扫描包括写涉密日志的功能的类如下：

```
class CTestMail {
public:
  //成员函数，以下为构造函数
  CTestMail(CString eid, CString efrom, CString eto, CString etime, CString econtent);
  int TestBw();              //测试黑白名单
  float TestRule();          //测试规则
  void WriteLog();
//把拦截到的涉密邮件信息写入日志
  int TestAll();       //综合起来测试
public:
  //数据成员，以下是接收外部传进来的参数
  CString m_szID;                  //邮件 ID
  CString m_szfrom;                //发信方
  CString m_szto;                  //收信方
  CString m_sztime;                //发信时间
  CString m_szcontent;             //邮件内容  };
```

### 3.2　密钥管理中心

密钥的生命周期包括密钥生成、密钥存储、密钥分发、密钥备份与恢复、密钥更新、密钥吊销与销毁。实践表明，从密钥管理渠道窃取密钥比用破译途径窃取密钥容易得多。所以，密钥的管理处于安全系统中的核心地位。同时密钥管理系统的安全也至关重要。该系统建立在 SSL(Secure Socket Layer)通信协议上，具有防止数据泄漏、防止身份伪造、数据完整性验证等功能。

下载私钥时，CGI 程序调用函数 int ibe_ext(CString name) 和 int ibs_ext (char*, CString, CString)执行私钥提取算法，根据系统主密钥和系统参数生成解密密钥和签名认证密钥，再经过 Base64 编码后形成一个私钥文件供用户下载。

### 3.3　系统客户端

客户端主要包括 CSmtp 类、CPop 类、CIbe 类、CIbs 类、CBase64 类、CMIMEMessage 类。CSmtp 类和 CPop 类都是继承 Socket 类。实现结果如图 5 所示。

**图 5　系统客户端**

CIbe 类用来完成对邮件的加密及解密工作。该加密体制是基于 BDHP(Bilinear Diffie-Hellman Problem)[4]难解的假设，结合混合加密方案和基于身份的加密方案的优点的混合加密体制。主要函数定义如下：

```
Void Encmail(char *id, char *mailtext, char *temp, char *y1, char * x1, char * x2, int &maillen);
CString Decodemail(int decmaillen, CString filepath);
```

CIbs 类用来完成对邮件的签名及对发件人身份的认证。该认证系统结合了 BF_IBE 方案[5]的优点和 Boneh 基于 Weil 对的短签名方案[6]的优点。主要函数定义如下：

```
int Sign( char *mailtext, char *signature, int maillength);
int Verify( char *mailtext, char *signatureinfo, bool &right, char *keyfile, int decmaillen);
```

由于邮件在加密后生成的数据为二进制乱码，在这里引入 base64 格式，base64 格式可以把乱码格式转换成没有空格的一串数据，从而避免数据在传输过程中丢失。

```
int Base64Decode(char *buf, const char * base64code, int src_len);
int Base64Encode(char *base64code, const char * src, int src_len);
```

## 4　系统的关键技术及安全设计

### 4.1　关键技术

与传统的公钥算法相比，Shamir 提出的基于身份的密码方案[7]的主要特点是用户的公钥可以由用户的身份信息直接

获得，具有不需要预先注册、便于消息内容扫描等优点。本系统结合 Boneh-Franklin IBE 方案基于身份的优点和 Boneh 基于 Weil 对的短签名方案的优点，提出了一个新的基于身份的可信任可扩展的健壮电子邮件认证系统。该方案具有基于身份、签名信息短、签名速度快、计算量小等优点。

本系统研究了涉密邮件过滤方法的理论基础——最小风险贝叶斯算法，在其基础上提出了风险自适应的最小风险贝叶斯算法，用其来学习训练样本集，构造涉密邮件分类器，对待分类的邮件集进行分类，通过计算涉密邮件被误判的封数来自动修改最小风险贝叶斯算法中的风险值，一直到涉密邮件被误判的比率达到指定的水平为止。

贝叶斯分类算法通常是以英文单词为单位，但系统要处理的邮件是含有中文字符的，这使得提取特征变得相当困难。所以，首先要解决中文分词的问题。中文分词是计算机自动识别文本中词边界的过程，词库是简单分词技术的基础。本系统采用了北京大学计算语言学研究所提供的 1998 年人民日报切分、标注语料库。

### 4.2 安全设计

(1)主密钥的生成与保存：IBE 的主密钥用来生成系统中所有的用户私钥。为了提供高强度的保护，应建立容侵参考模型或在硬件密码模块中生成和存储系统主密钥，以防止主密钥的泄漏。

(2)私钥的生成：TA(Trusted Authority)必须采取访问控制、入侵检测、审计追踪等安全防范措施，保护用于私钥生成的算法程序的安全，并保证计算机与机房的物理和使用环境的安全。

(3)用户身份认证与私钥的安全传送：TA 需要建立安全的数据库存储用户的身份认证信息，私钥通过 SSL 安全信道传送。身份认证也可以利用邮件服务器实现，例如使用邮件服务器的 POP3 认证、IMAP 认证等。

(4)私钥在客户端的保存：常用的方式是用口令或通行短语(pass phrase)生成私钥加密密钥，将私钥加密后保存在本地计算机的硬盘上。更加安全的方式是将私钥保存在智能卡、USB 令牌等便携式设备中。

(5)公钥撤销：通常采用在收件人的 E-mail 地址后附加有效期字段构成公钥的方法，例如使用 szu@szu.edu.cn||2007 形式的字符串作为公钥，其中的附加字段“2007”指定该公钥的有效期为 2007 年。

## 5 结束语

本系统采用基于身份的密码体制，结合混合加密技术、智能邮件内容扫描等技术，构建立体纵深的安全防御体系，可以满足在不可控、动态和松散组织成员间的安全通信。随着对基于身份的密码体制及涉密中文邮件扫描的深入研究，基于身份密码体制的安全电子邮件系统将得到更多政府机构及企业的青睐。

### 参考文献


[1] OpenPGP Message Format[S]. IETF , RFC 2440, 1998-11.

[2] S/MIME Version 2 Message Specification[S]. RFC 2311, 1998-03.

[3] 彭海涛, 史清华. 基于身份的安全电子邮件系统[J]. 计算机工程, 2005, 31(13):124-125.

[4] Bao Feng, Deng R, Zhu Huafei. Variations of Diffie-Hellman Problem[C]//Proceedings of the 5th Conference on Information and Communications Security. [S. 1.]: IEEE Press, 2003: 301-312.

[5] Boneh D, Franklin M. Identity-based Encryption from the Weil Pairing[J]. SIAM J. of Computing, 2003, 32(3): 586-615.

[6] Boneh D, Lynn B, Shacham H. Short Signatures from the Weil Pairing[J]. J. Cryptology, 2001, 17(4): 297-319.

[7] Shamir A. Identity-based Cryptosystems and Signature Schemes[C]//Proceedings of Crypto'84. [S. 1.]: Springer-Verlag, 1984: 47-53.


编辑 索书志

(上接第 193 页)

序列发生器产生的序列进行测试的结果。可以看出，该发生器所产生的随机位序列具有较好的统计特性。

**表 1 演化随机序列发生器随机测试结果**

| | *P-value Low* | *P-value High* | *Pass Ratio* |
|---|---|---|---|
| Frequency | 0.922 | 0.989 | 1.000 |
| Block-Frequency | 0.715 | 0.747 | 0.926 |
| Cusum-Forward | 0.927 | 0.963 | 0.886 |
| Cusum-Reverse | 0.373 | 0.450 | 0.901 |
| Runs | 0.479 | 0.546 | 0.797 |
| Long Runs of ones | 0.287 | 0.332 | 0.624 |
| Rank(32×32) | 0.421 | 0.672 | 0.700 |
| Spectral DFT | 0.885 | 0.957 | 0.985 |
| Non-overlapping | 0.545 | 0.848 | 0.841 |
| Overlapping | 0.677 | 0.833 | 0.729 |
| Universal | 0.776 | 0.884 | 0.976 |
| Approx Entropy | 0.992 | 0.998 | 0.999 |
| Lempel-ziv | 0.887 | 0.895 | 0.907 |
| Linear Complexity | 0.586 | 0.653 | 0.869 |
| Serial($m$=5) | 0.912 | 0.978 | 0.984 |

## 6 结束语

本文提出了一个高速、低价和低功耗的基于 LFSR 的演化随机序列发生器。并进行统计测试以检测这种发生器所产生的随机序列的质量。实验结果表明，由于使用了 FIPS 140-1 测试统计量构建适应度函数，因此随机序列发生器具有良好的统计特性。它既可以用软件实现也可以用硬件实现。改变参数或选择更好的适应度函数或使用遗传算法可以设计具有更好统计特性的随机序列发生器。而且演化算法可以用来设计结构能重新配置的 LFSR，以产生更好的随机位序列。

### 参考文献


[1] Callegari S, Rovatti R, Setti G. Embeddable ADC-based True Random Number Generator for Cryptographic Applications Exploiting Nonlinear Signal Processing and Chaos[J]. IEEE Transactions on Signal Processing, 2005, 53(2): 793-805.

[2] Kocher P, Jaffe J, Jun Benjamin. Differential Power Analysis[C]// Proc. of Advance in CRYPTOLOGY'99. Heidelberg, Germany: Springe-Verlag, 1999: 388-397.

[3] Tsoi K H, Leung K H, Leong P H W. Compact FPGA-based True and Pseudo Random Number Generators[C]//Proceedings of the 11th Annual IEEE Symposium on Field-programmable Custom Computing Machines. Washington, USA: IEEE Press, 2003.

[4] Sharaf M, Mansour H A, Zayed H H, et al. A Complex Linear Feedback Shift Register Design for the A5 Key Stream Generator[C]//Proceedings of the 22nd National Conference on Radio Science. 2005. Cario, Egypt: [s. n.], 2005.

[5] Golino G. Improved Genetic Algorithm for the Design of the Optimal Antenna Division in Sub-arrays: A Multi-objective Genetic Algorithm[C]//Proc. of IEEE International Conference on Radar. [S. l.]: IEEE Press, 2005.


编辑 张 帆