基于身份的安全邮件认证体系设计与分析*)

刘宏伟[1,2] 谢维信[2] 赵 超[2]

(西安电子科技大学电子工程学院 西安 710071)[1] (深圳大学信息工程学院 深圳 518060)[2]

摘 要 针对电子邮件中的安全问题,利用基于身份的数字签名方案,提出了一个基于身份的安全邮件认证体系,并给出了该体系的软件架构和实现过程。通过分析,该认证体系具有较高的安全级别,同时系统开销较低,适合在邮件系统中使用。系统测试及运行结果表明,该体系是安全且高效的。

关键词 基于身份的密码体制,数字签名,邮件系统,椭圆曲线

Design and Analysis of a Secure Email Authentication System Based on Identity-based Encryption

LIU Hong-Wei[1,2] XIE Wei-Xin[2] ZHAO Chao[2]

(School of Electronic Engineering, Xidian Univ., Xi'an 710071)[1] (School of Information Engineering, Shenzhen Univ., Shenzhen 518060)[2]

Abstract To resolve the security problem in email system, a new ID-based authentication scheme for email system is proposed and implemented based on ID-based signature scheme. The software architecture and its configuration process are presented. It is showed that the scheme is more efficient than some existing ones for higher security level and lower cost by analysis, therefore, the scheme is suitable for use in email system. The system test and result indicate that it is secure and efficient.

Keywords Identity-based cryptography, Digital signature, Email system, Elliptic curve

随着计算机网络的飞速发展,越来越多的信息在通过互联网进行传输,而电子邮件则成为了信息传输的主要工具。由于互联网的开放性,这些信息中又包含许多个人和企业的隐私或机密信息,因而电子邮件的安全问题就显得越发的突出。

目前客户端方式的邮件系统虽已实现了安全认证,但操作比较复杂,只能在特定的计算机上收发邮件,还存在用户密钥保管等问题,应用上存在较大的局限性。而被广泛使用的Web方式的电子邮件系统由于考虑到简单性和易用性,并没有将安全认证技术应用到系统中。如何结合安全认证技术,实现安全且便捷的Web方式电子邮件系统的研究就显得十分重要。

数字签名技术是电子邮件及电子商务安全认证体系的核心,在安全认证服务中的源鉴别、完整性服务、不可否认服务中,都要用到数字签名技术。目前数字签名采用较多的是公钥加密技术,如基于RSA Date Security公司的PKCS、DSA、x.509、PGP等方案,但这些方案或者需要维护复杂的证书库,或者在客户端需要较大的运算和存储开销,因而并不十分适合邮件系统使用。

基于身份的公钥密码体制最初由Shamir[1]提出,其中实体的公钥是直接从其身份(Identity)信息得到,如实体的IP地址、E-mail地址等,其私钥由一个私钥生成中心(TA)的可信第三方生成。第一个实用的基于身份的加密方案IBE(Identity-Based Encryption)由D. Boneh和M. Franklin[2]在2001年设计出来。目前,基于身份的方案包括基于身份的加密体制、可鉴别身份的加密和签密体制、签名体制、密钥协商体制、鉴别体制、门限密码体制、层次密码体制等。

本文通过基于身份的数字签名算法,设计了基于身份的安全邮件认证方案。该方案具有基于身份、不需要证书、签名与验证速度快、系统开销小的优点。

1 系统设计

1.1 流程设计

安全认证体系的流程可分为六个步骤:(1)系统初始化;(2)用户申请密钥对;(3)可信第三方生成密钥对;(4)密钥对分发;(5)生成数字签名信息并发送邮件;(6)接受方验证签名信息以检验发件人身份。其中步骤(2)(3)(4)可以合为一步——密钥生成,整个过程如图1所示。

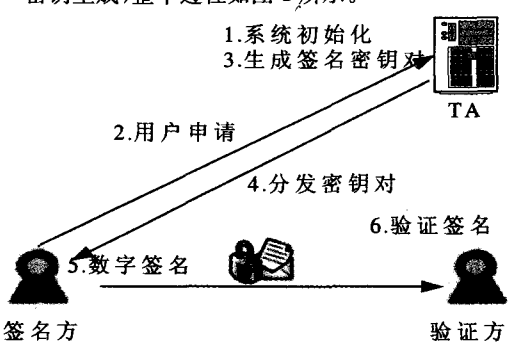

图1 认证系统流程

系统初始化与密钥生成在可信第三方(TA)完成,经过初始化后,TA生成系统参数,该参数一部分作为TA生成用户密钥对的输入,一部分作为用户签名与验证的输入。TA生成用户密钥对后,需要将密钥对安全地传送给用户。为保障

*基金项目:国家863计划资助项目。(2003AA142060);广东省自然科学基金重点项目(04106250);深圳市科技计划资助项目(200513)。刘宏伟 博士生,主要研究方向为:信息安全。

传输信道的安全，本系统将在 TA 与用户之间建立安全 SSL 通信。

发件方生成数字签名，要首先对邮件生成消息摘要，然后用口令读取自己的私钥信息，然后将私钥信息与消息摘要进行特定运算生成数字签名信息。

收件方收到邮件后，首先从邮件中提取签名信息，并读入系统初始化时生成的公共参数信息，对这两部分进行特定运算得到结果 result1，然后对接收到的邮件明文计算消息摘要，并读取发件方公钥，计算得到 result2，然后将 result1 与 result2 作比较来验证发件方身份并保证邮件的完整性。

1.2 模块组成

安全认证系统可分为四个主要的模块：系统初始化模块、用户密钥生成模块、数字签名模块与认证签名模块，如图 2 所示。其中，系统初始化模块与用户密钥生成模块运行在可信第三方，数字签名模块与认证签名模块运行在用户端。

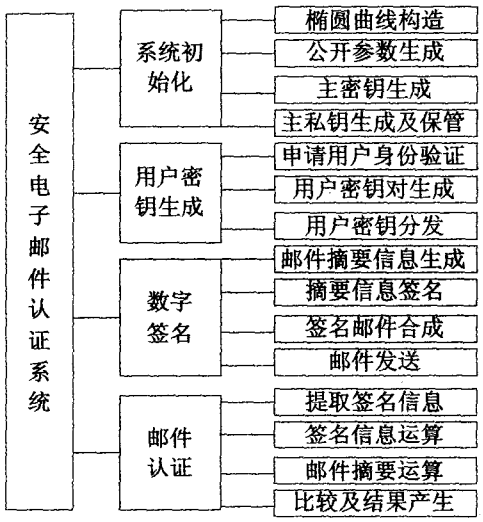

图 2 认证系统模块组成

2 系统实现

2.1 系统环境

系统的可信第三方与用户端运行环境均选择 Windows 操作系统。开发环境为 Windows XP 操作系统，开发工具为 Microsoft Visual C++ 6.0，并选取 Miracl 密码开发包作为辅助工具，版本为 5.2。

Miracle 开发包包括了各种基本的密码算法，在本系统中主要用到开发包中关于大数的运算以及椭圆曲线的相关算法。在 Miracl 开发包的使用上，本文采用静态库的开发模式，其实现过程如下：

1. 生成静态库

在系统具体实现过程中，将会调用部分基本函数，为方便函数调用，要将各种常用的函数集成到一个可供 VC++ 调用的静态库中。生成过程如下：

• 编译并运行 config. c 文件，并将生成文件 mirdef. tst 改名为 mirdef. h。

• 新建工程，工程类型为 Win32 Static Library。

• 添加文件 miracl. lst 中列出的所有形如 mr *. c 的 C 文件，其中文件 miracl. lst 也由 config. c 文件生成。

• 在工程中添加一条指向头文件 mirdef. h 与 miracl. h 的路径。

• 编译运行，生成 miracl 静态库文件 ms32. lib。

2. 调用静态库

在需要调用静态库的工程中，添加上面生成的 Miracl 静态库 ms32. lib。

3. 设置路径

在需要调用静态库的工程中添加一条指向 Miracl 库中的头文件，头文件均放在 Include 文件夹下面。

2.2 函数设计

为了方便整个邮件系统调用认证系统进行数字签名与认证，本认证系统将四个主要过程分别整合设计成相应的四个主函数，以简化系统条理及流程。主函数包括：

1. 系统初始化函数 void setup(void)

该函数主要生成系统参数与可信第三方的公钥和主密钥，生成信息放在两个文件 common. ibe 文件与 master. key 文件中，其中 common. ibe 中包含的信息有系统安全参数、有限域的阶、基于有限域的椭圆曲线上的循环群的阶、循环群的生成元与可信第三方公钥等公开信息。master. key 包含了可信第三方的主密钥。common. ibe 文件存在于可信第三方与用户端(或实时获取)上，而 master. key 只能存放在可信第三方内部，需要安全保护。

2. 生成用户密钥函数 int extract(char * idd)

该函数用来生成用户的签名用公钥与私钥，接收参数是用户的身份信息字符串，该信息必须能唯一标识用户的身份，如用户的邮箱地址。函数生成 public. key 文件与 private. key 文件，其中 public. key 包含用户签名公钥，private. key 包含用户签名用私钥。用户签名用公钥可以由签名私钥与系统参数一起产生，所以用户如果具有自己的签名私钥，可以自己产生其对应公钥。

3. 数字签名函数 int sign(char * mailtext, char * signature_u, * signature_v)

数字签名函数用来对邮件生成数字签名信息，参数 mailtext 用来接收需要进行签名的邮件明文信息，signature_u，signature_v 返回生成的数字签名信息。在运行过程中需要从 common. ibe 文件中读取系统参数，从 private. key 中读取用户签名用私钥。该函数生成的数字签名信息要与邮件明文信息放在一起，然后进行加密。

4. 验证签名函数 int verify(char * mailtext, char * signatureinfo, bool &right)

该函数用来验证数字签名信息，包括三个参数：mailtext、signature 与 right，分别用来向函数传递邮件明文信息和对应的数字签名信息，以及返回验证结果。邮件明文 mailtext 与签名信息 signatureinfo 是通过解密邮件密文得到的。

2.3 程序实现

系统具体实现的关键代码如下：

```
int setup( void ){   // 系统初始化函数，生成系统参数与主密钥
ecurve(0,1,p,MR_PROJECTIVE); // 生成有限域上的椭圆曲线
while (! P. set(randn())); // 生成椭圆曲线群的生成元 P
s=rand(q); // 生成 TA 主密钥 s
Ppub=s * P; // 生成 TA 的公钥 Ppub
}
int extract( char * idd ) { // 用户密钥生成函数，输入为用户身份信息 idd，并读取 TA 主密钥与系统参数，生成用户密钥对.
Qid =map_to_point(id); // 根据用户身份信息 id 映射到椭圆曲线上
Did=s * Qid; // 生成用户私钥信息 Did
Did. get(x,y); // 提取用户私钥 x
Qid =x * P; // 将用户私钥 x 与生成元 P 做点乘生成用户公钥信息 Qid
```

```
    }
    int sign( char * mailtext, char * signature_u, * signature_v ) {
// 数字签名函数，输入为邮件明文信息，输出为签名信息
    ECn zhy=map_to_point(ver); // 将邮件摘要映射到椭圆曲线
        上一点
    private_key ≫ privatekey; // 读取用户私钥;
    ECn SignatureInfor_u = Signature_u (privatekey,zhy,k,p1)
    ECn SignatureInfor_v = Signature _v(privatekey,zhy,k,p1) //
        生成签名信息
    }
    int verify( char * mailtext, char * signatureinfo, bool &right) {
// 签名验证函数，输入为邮件明文，签名，返回验证结果
    Signature_u. set(x,yy1);
    Signature_v. set(x,yy2); // 提取签名信息
    Qid. set(x,y); // 提取发件人公钥
    HM = map_to_point(ver); // 将邮件摘要映射到椭圆曲线上得
        到 HM
    if(! ecap(P, Signature_u, Signature_v, q, cube) = ! ecap
(Qid, HM, q, cube)) // 验证签名信息
    }
```

3 关键技术

3.1 数字签名

本文认证系统的核心是基于身份的数字签名，选择的签名方案是否合适将直接影响系统的效果。文[5]提出了一种基于身份的数字签名方案，本文主要以该方案为基础，实现了基于身份的安全邮件认证体系。

设 G_1、G_2 分别是 q 阶的加法群和乘法群，其中 q 是素数，设 $\hat{e}:G_1\times G_2\to G_2$ 是一个双线性映射，H_1、H_2 是公开的哈希函数，其中 $H_1:\{0,1\}^*\to G_1^*$，$H_2:\{0,1\}^*\times G_2\to F_q$。

(1)初始化　可信中心 TA 选择 $P\in G_1$，$t\in F_q$，计算 $Q_{TA}=tP$，秘密保存 t，公开 Q_{TA} 和 P；

(2)用户注册　TA 验证用户 A 身份，合法后计算 $Q_A=H_1(ID_A)$ 和 $S_A=tQ_A$，将 S_A 通过安全渠道送给用户 A；

(3)签名　为签名消息 m，选择 $P_1\in G_1$，$k\in F_q$，计算 $r=\hat{e}(P_1,P)^k$，$v=H_2(m,r)$，$u=vS_A+kP_1$；签名为(u,v)

(4)验证　接收方计算 $r=\hat{e}(u,P)\cdot\hat{e}(Q_A,-Q_{TA})^v$。验证等式 $v=H_2(m,r)$是否成立。

3.2 椭圆曲线构造

基于身份的数字签名方案是建立在椭圆曲线密码学基础之上，因而椭圆曲线的构造是必须的。

设 F_p 为有限域，p 为大素数，F_{p^k} 为其 k 阶扩域，对 $k\geqslant 1$，$F_{p^k}^*$ 为 F_{p^k} 的乘法群，$(E(F_{p^k}),+)$为加法群。选择椭圆曲线参数 $a,b\in F_p$，定义基于有限域的椭圆曲线方程：$E(F_p)$：$y^2\equiv x^3+ax+b(\mathrm{mod}\ p)$，$\#E(F_p)$表示群 $E(F_p)$的大小。选择椭圆曲线 $E(F_p)$上的点 $G=(x_G,y_G)$作为基点，其阶为素数 q，以点 G 为生成元生成 q 循环群$\langle G\rangle$，$h=\#E(F_p)/q$，参数限制如下：

$4a^3+27b^2\neq 0(\mathrm{mod}\ p)$；$\#E(F_p)\neq p$；

$p^B\neq 1(\mathrm{mod}\ n)$ for any $1\leqslant B\leqslant 20$；

$h\leqslant 4$

由于基于身份的数字签名方案主要是基于 Weil 对，所以必须选取 I 型椭圆曲线：$E/F_p:y^2=x^3+1$，其中 $p\equiv 11(\mathrm{mod})\ 12$，$\#E(F_p)=p+1$，$x=\sqrt[3]{y^2-1}(\mathrm{mod}\ p)$，$y=\sqrt{x^3+1}(\mathrm{mod}\ p)$。对于 I 型椭圆曲线一般 k 取 2，约减多项式 $f(x)=(x^2+1)$，则二阶扩域 F_{p^2} 为多项式 a_1x+a_0，由 $F[x]/(x^2+1)$求得。p 的大小决定有限域的大小，是决定椭圆曲线密码系统安全性的关键，因此对于 p 的大小可取$\lceil\log_2 p\rceil=\{112,128,160,192,224,256,384,521\}$

3.3 公开参数生成

(1) 输入安全系数 $n=1024$

(2) 决定安全参数：计算决定有限域 F_p 的阶的参数 $n_p\leftarrow\lfloor n/2\rfloor$；

计算决定循环子群的阶 q 的大小的参数 $n_q\leftarrow\lfloor n/32\rfloor+128$。

(3)构造椭圆曲线及其循环子群：

选择任意长度为 n_q 的素数 q，即$|\log_2^q|=n_q$，为了使生成的椭圆曲线具有更好的性质，建议选取的素数 q 满足 $q=2^a\pm 2^b\pm 1,0<b<a$，；

选择随机数 r，满足 $p=12rq-1$，且 p 的长度为 n_p，即有$|\log_2^q|=n_p$；

任意选择点 P'，坐标(x',y')满足椭圆曲线 $E/F_p:y^2=x^3+1(\mathrm{mod}\ p)$；

计算 $P\leftarrow[12r]P'$；

如果 $P=\infty$，重新选择点 P'，再计算点 P。

(4)生成 TA 主密钥与公钥：

选择随机数 $s,s\in\{1,\cdots,q-1\}$；

计算公钥 $P_{pub}=[s]P$。

(5)公开参数为(t,E,p,q,P,P_{pub})

(6) 可信第三方的主密钥为 s

4 安全性及效率分析

本文中的安全邮件认证系统是采用基于身份的数字签名原理作为基础，该签名的安全性已由文[5]给出证明，因而在 DLP 和 CDHP 难解的假设下，本方案是安全的。

基于身份的密码体制是建立在椭圆曲线密码学(ECC)的基础上的。相对于 RSA 等密码体制来说，椭圆曲线密码体制出现较晚，已成为近年来安全领域中的研究热点之一。

ECC 体制的安全性基础是有限域中椭圆曲线上的点群中的离散对数问题(ECDLP)。目前的研究结果是解决椭圆曲线离散问题比有限域上的离散对数问题更加困难。ECDLP 被认为是指数级的难度，而 RSA 是亚指数级的。

在椭圆曲线密码体制中使用较小的密钥，可以达到使用更大的有限域的密钥同样的安全性。RSA、DL 与 EC 密码体制的参数的规模[6](密钥的规模)比较如表 1 所示。

表 1　RSA、DL 和 EC 提供等效安全级别的密钥长度

	安全级别(位)				
	80SKIPDACK	112 3DES	128 AES	192 AES	256 AES
EC 的参数 q	160	224	256	384	512
RSA 模 n	1024	2048	3072	8192	15360
DL 模 p					

而系统效率方面，传统的数字签名技术 RSA 与 DSA 中，用户的签名公钥与私钥都是 CA 机构或可信机构随机产生的，当证书颁发机构生成了用户的签名密钥对后，需要保存每个用户的签名公钥和私钥，当用户数量巨大时，管理上非常困难，维护的代价很高，而且占用 CA 机构的很多资源。

而基于身份的认证系统中，用户的密钥对与自己的身份信息相对应，可信第三方只需知道用户的邮件地址就可以随时生成用户对应的密钥对，而不需要存储所用用户的密钥信

(下转第 114 页)

上述分析表明，如果协议应答方 R 已经将商品项($item_R$，r_R，key_R)发送给发起方 O，R 能获得来自 O 的 ($item_O$，key_O，r_O)或证词项 $sig_T(m_1, m_2, y_R)$。

对双方串节点路径的分析表明，当一方已发送商品给另一方后，必能获得其所期望的商品项或来自可信方的证词，没有任何一方较另一方处于优势，即 ASW 协议是弱公平的。

结束语 现有的形式化分析研究多集中在认证协议和密钥交换协议。而电子商务协议具有更为复杂的协议结构，如分支结构，或由多个子协议组成，使得难以使用传统的信念逻辑进行分析。本文对串空间逻辑进行了扩展，使之能分析带密文项的电子商务协议。还提出串节点路径分析法，以利用串空间逻辑分析带复杂结构的协议，从而给出了一种较为通用的电子商务协议形式化分析方法。文中成功地对 ISI 支付协议和 ASW 协议进行串空间分析，形式化地证明了 ISI 协议不满足公平性，而 ASW 协议则满足公平性。基于串空间逻辑的复杂协议自动分析器是我们今后研究的方向。

参 考 文 献

1 Asokan N. Fairness in electronic commerce:[PhD thesis]. University of Waterloo, 1998
2 Dolev A, Yao A C. On the security of public-key protocols. IEEE Transactions on Information Theory, 1983, 2(29): 198～208
3 Burrows M, Abadi M, Needham R. A logic of authentication. ACM Transactions on Computer Systems, 1990, 8(1):18～36
4 Kailar R. Accountability in electronic commerce protocols. IEEE Transactions on Software Engineering, 1996, 22(5): 313～328
5 周典萃，卿斯汉，周展飞. Kailar 逻辑的缺陷. 软件学报，1999，10(12):1238～1245
6 Ryan P, Schneider S. Modelling and analysis of security protocols. Addison-Wesley Publishing Co, 2000
7 Lowe G. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. Software Concepts and Tools, 1996, 17: 93～102
8 Heintze N, Tygar J D, Wing J, et al. Model checking electronic commerce protocols. In: Proc. 2nd USENIX Workshop on Electronic Commerce, 1996. 147～164
9 卿斯汉. 密码学与计算机网络安全. 北京：清华大学出版社，2000. 127～147
10 卿斯汉. 一种新型的非否认协议. 软件学报，2000，11(10)：1338～1343
11 周典萃，卿斯汉，周展飞. 一种分析电子商务协议的新工具. 软件学报，2001，12(9)：1318～1328
12 白硕，隋立颖，陈庆锋，等. 安全协议的验证逻辑. 软件学报，2000，11(2)：213～221
13 陈庆锋，白硕，王驹，等. 电子商务安全协议及其非单调动态逻辑验证. 软件学报，2000，11(2)：240～250
14 Thayer F J, Herzog J C, Guttman J. Strand spaces: Why is a security protocol correct? In: Proc the 1998 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, 1998. 160～171
15 Thayer F J, Herzog J C, Guttman J. Honest ideals on strand space. In: Proc. 11th IEEE Computer Security Foundations Workshop, IEEE Computer Society Press, 1998
16 Thayer F J, Herzog J C, Guttman J. Strand spaces: Proving security protocols correct. Journal of Computer Security, 1999, 7(2-3): 191～230
17 Medvinsky G, Neuman B C. Netcash: a design of practical electronic currency on the Internet. In: Proc. ACM Conf. on Computer and Communication Security. New York: ACM Press, 1993. 76～82
18 Asokan N, Schunter M, Waidner M. Optimistic protocols for fair exchange. In: Proc. 4th ACM Conf. on Computer and Communication Security. ACM Press, 1997. 6～17

(上接第 80 页)

提出的方案计算开销就比较高。反之，如果大量的邻居节点认证只是为了获得网络的使用权限，那么我们的方案就可以取得比较好的效果。

结论 本文在分析以往移动自组网密钥协商协议的基础上，综合移动自组网的实际需要，提出了一种适用于移动自组网的密钥协商方案，减轻了节点的计算和通信开销，同时实现了身份认证的功能。本文所提出的方案比较简单，安全性较好，计算和通信开销小，因此非常适合于移动自组网这种能量和计算资源有限的网络。我们下一步的研究目标是结合匿名认证方案和 MPLS 标签交换的局部性来实现移动自组网的匿名安全路由，并结合信任相关的理论来阻挡来自网络的内部的攻击，实现节点回收的功能。

参 考 文 献

1 Zhu S, Xu S, Setia S, et al. Establishing Pair-wise Keys for SecureCommunication in Ad Hoc Networks: A Probabilistic Approach. In: IEEE ICNP, 2003
2 Kong J, Zerfos P, Luo H, et al. Providing Robust and UbiquitousSecurity Support for MANET. In: IEEE ICNP, 2001
3 Narasimha M, Tsudik G, Yi J H. On the Utility of Distributed Cryptography in P2P and MANETs: The Case of Membership Control. In: IEEE ICNP, 2003
4 Jarecki S, Saxena N, Yi J H. An Attack on the Proactive RSA Signature Scheme in the URSA Ad Hoc Network Access Control Protocol. In: ACM SASN, 2004
5 Joux A. A one-round protocol for tripartite Diffie-Hellman. In Algorithmic Number Theory Symposium -ANTS-IV, Springer-Verlag LNCS1838, 2000. 385～394
6 Boneh D, Gentry C, Lynn B, et al. Aggregate and verifiably encrypted signatures from bilinear maps. In: Biham E, ed. Proc. of the Eurocrypt 2003. LNCS 2656, Warsaw: Springer-Verlag, 2003. 416～432
7 Smart N P. An identity-based authenticated key agreement protocol based on the Weil pairing. Electronics Letters, 2002, 38: 630～632
8 Chen L, Kudla C. Identity based authenticated key agreement protocols from pairings. CSFW'03, 2003. 219～236
9 Ertaul L, Lu W M. ECC based threshold cryptography for secure data forwarding and secure key exchange in MANET (I). In: Boutaba R, Almeroth K, Puigjaner R, et al. eds. Networking 2005. LCNS 3462, Canada: University of Waterloo, Springer-Verlag GmbH, 2005. 102～113
10 Zhang Y, Liu W, Lou W W. Anonymous Communications in Mobile Ad Hoc Networks. IEEE INFOCOM, 2005

(上接第 86 页)

息，可大大减轻可信第三方的负担。

结束语 本文采用基于身份的密码体制作为基础，提出了一套切实可行、安全高效的邮件安全认证方案，该方案系统开销小，安全级别较高，有效地实现了 Web 方式电子邮件系统中的安全认证问题。系统实际运行结果表明，该认证系统结果正确，运行速度较快，运行状况良好。

参 考 文 献

1 Shamir A. Identity-based cryptosystems and signature schemes [J]. In: Advances in Cryptology-CRYPTO84, Vol. 196 of LNCS, Springer-Verlag, 1984. 47～53
2 Boneh D, Franklin M. Identity-based Encryption from the Weil Pairing [C]. Advance in Cryptology-CRYPTO 2001. LNCS 2139, 2001. 213～229
3 Boneh D, Franklin M. Short Signatures from Weil Pairing [C]. Boyd C ASIACRYPT 2001. Berlin: Springer-Verlag, 2001. 514～532
4 Menezes A, Okamoto T, Vanstone S. Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field [J]. IEEE Trans on Information Theory, 1993, 39(5): 1639～1646
5 Hess F. Efficient identity based signature schemes based on pairings [C]. In SAC'02: Revised Papers from the 9th Annual International Workshop on Selected Areas in Cryptography. Springer-Verlag, 2003. 310～324
6 Hankerson D, Menezes A, Vanstone S. Guide to Elliptic Curve Cryptography [M]. Publishing House of Electronics Industry, 2005, 8: 5～20