分布式学籍管理系统中的群签名及其实现*

景　旭[1,2],韩永国[1],雷伟杰[1]
(1.西南科技大学 计算机学院,四川　绵阳,621002;2.盐城工学院 教务处,江苏 盐城　224003)

摘　要:结合群签名技术在分布式学籍管理系统中的应用,介绍了数字签名、群签名的原理及特点,详细介绍了分布式学籍管理系统中一种群签名方案的实现过程。该系统具有保密、安全、一致、鉴别的特点,完全实现了手工学籍管理的各道程序,保存群签名,实现了可靠的、无纸化学籍管理。

关键词:数字签名;群签名;学籍管理
中图分类号:TP391　　**文献标识码**:A　　**文章编号**:1671－5322(2003)03－0020－04

传统的学籍管理系统,对每个学生的每门课程成绩一般要经过如下处理过程:首先,由授课教师手工抄写或在电脑上输出每个学生的姓名及成绩,送教研室主任、系主任等系部领导签字,又送教务处有关领导签字,最后由主管学籍的教务处的教师再次输入电脑,才形成电子文档。有些学校虽实现成绩网上提交,但仍要有一个纸质手工签名文档以保证成绩的可靠性。学籍管理的安全性、一致性由纸质签名保证,整个学籍管理过程中有许多冗余及不便。在分布式学籍管理系统中如何消除管理过程中的冗余,保证安全性和一致性?在计算机网络的虚拟世界中,如何保证学生成绩在网络传输或正常管理中未被修改?如何在网上实现手工管理一样完整的签名程序?群签名技术引入分布式学籍管理系统可以较好的解决这个问题,促进网络学籍管理走向成熟、实用。

1　数字签名技术

公钥密码体制的观点是由 Diffie 和 Hellmen 在 1976 年首次提出的,它使密码学发生了一场革命。1977 年由 Rivest,Shamir 和 Adleman 提出了第一个比较完善的公钥密码算法,即 RSA 算法。公开密钥加密的基本思想是:每个用户拥有两个密钥,一个是公开密钥 P_k,它类似于电话本上的号码,对任何用户都公开;另一个是私有密钥 S_k,仅为自己拥有。加密算法 E 和解密算法 D 都是公开的。虽然 S_k 和 P_k 在它们生成过程中有关,但根据 P_k 计算出 S_k 却是不可行的。公开密钥加密体制的安全性依赖于一种特殊的数学函数——单向陷门函数,其性质为:从一个方向求值容易,但逆向计算却很困难。公开密钥算法的特点[1]为:

(1)用加密密钥 P_k 对明文 X 加密后,用解密密钥 S_k 解密即可恢复出明文,即 $D_{Sk}(E_{pk}(X)) = X$;另外加密和解密的运行可以对调,即 $E_{Pk}(D_{Sk}(X)) = X$;

(2)加密密钥不能用来解密,即 $D_{Pk}(E_{Pk}(X)) \neq X$;

(3)在计算机上可以容易地产生成对的 P_k 和 S_k;

(4)从已知的 P_k 推导出 S_k 在"计算上是不可行的"。

一个数字签名方案至少应满足以下 3 个条件[1]:(1)签名者事后不能否认自己的签名;(2)接收者能验证签名,任何其他人都不能仿造签名;(3)当双方关于签名的真伪发生争执时,存在第三方能解决双方之间发生的争执。

2　群签名[2]

在学籍管理系统中,学籍数据需要多人签名,如果学籍数据的提交和多人签名在网上进行,由

* 收稿日期:2003－04－12

作者简介:景　旭(1971-),男,陕西礼泉县人,盐城工学院讲师,西南科技大学在职硕士研究生。

于各签名者在地理上是分布的,因此须确保他们之间的通信安全,防止伪装通信等,需要用群签名技术来实现。

群签名具体实现有很多方法,一种实现方法是按一定顺序对内容签名,各签名方签名是累加的。每个签名者都知道前一位签名者和后一位签名者,且知道他们的公钥。最后一位签名者在所有签名完成后将最终消息和最终签名一起发送给接收方。

在分布式学籍管理系统中,设需要提交学籍数据的教师为 A_1,其提交的数据需要经过教研室主任、系主任、教务处领导等分别签名,按他们的签名顺序分别设为 $A_2, A_3 \cdots\cdots A_n$,完成所有签名后由最后一个签名者 A_n 将最终签名过的数据发送给教务处专门负责学籍管理的教师 B,P_{kA_i} 和 S_{kA_i} 分别为 A_i 的公钥和私钥,P_{kB} 和 S_{kB} 分别为 B 的公钥和私钥,需要发送的消息为 M。则具体群签名实现过程步骤如下:

(1) A_1 用 RSA 算法和 A_1 的私钥 S_{kA_1} 对 M 进行计算,产生数字签名 X_1,并用下一位签名人 A_2 的公钥 P_{kA_2} 对 $(M + X_1)$ 加密,产生 $E_{pkA2}(M + X_1)$ 并发送给 A_2。

(2) A_2 收到 A_1 发来的密文后,A_2 用私钥 S_{kA_2} 对消息解密,$D_{SKA2}[E_{pkA2}(M + X_1)] = M + X_1$,并用 RSA 算法和 A_1 的公钥 P_{kA_1} 对 X_1 验证。如果 X_1 得不到验证,则认为消息非法,签名过程终止。反之,继续下一步。

(3)如果 X_1 得到验证,A_2 把 $(M + X_1)$ 作为消息 M_2,用 RSA 算法和 $AS2$ 的私钥 S_{kA_2} 产生新的 X_2,并用后一签名者 A_3 的公钥 P_{kA_3} 加密产生 $E_{PkA3}(M_2 + X_2)$ 后,发送给后一位签名者 A_3。

(4) A_3 收到 A_2 的密文后,按照步骤(2) ~ (3)处理。每个签名者如此依次签名,直到最后的签名者 A_n。

(5)最后一个签名者 A_n 用接收者 B 的公钥对 $(M_n + X_n)$ 进行加密,产生 $E_{PkB}(M_n + X_n)$ 并送给 B。

多人签名验证步骤如下:

(1) B 收到消息后,用私钥 S_{kB} 对消息解密,产生 $D_{SkB}(E_{skB}(M_n + X_n) = M_n + X_n$;

(2) B 用 RSA 算法和 A_n 的公钥 P_{kAn} 对 M_n 进行计算,可以算出一个数字签名 X_n';

(3)如果 $X_n \neq X_n'$,则数字签名得不到验证,签名验证过程终止,反之,继续下一步;

(4)由多人签名产生的步骤(3)可知 $M_n = M_{n-1} + X_{n-1}$,从中可以分离出 M_{n-1} 和 X_{n-2},按步骤(1) ~ (3)可以继续验证 M_{n-1} 和 X_{n-1},依次验证下去,直至验证到 M 和 X_1,如果 M 和 X_1 通过验证,则整个签名算法成功。

3　数字签名方案的形成

分布学籍管理中的群签名方案实际是一种多重数字签名,数字签名是整个方案的一个重要内容。下面给出单个数字签名方案的实现过程[3]。

3.1　方案描述

p:选取两个大素数 q, t,使得 $p = 2qt + 1$;

g:g 为 Z_p^* 的一个本原;

x:x 属于 Z_p^*;

y:$y \equiv g_x \bmod p$

e:$1 \leq e < \Phi(\Phi(p))$,

且 $(e, \Phi(\Phi(p))) = 1$,$(\Phi(p))$ 为欧拉函数;

d:$ed(\bmod \Phi(\Phi(p))) = 1$;

公钥:(p, g, y, e)

私钥:(q, t, x, d)

3.2　签名过程

对给定的消息 M 属于 Z_p^*,随机选取一个 j 属于 Z_p^*,使得 $gcd(j, p-1) = 1$,并计算 $r = g^{'} \bmod p$,再由下式求 s':

$(M + r)\, x \equiv j + s' \bmod (p-1)$,$s' \in [0, p-2]$;

即 $s' = [(M + r)\, r - j] \bmod (p-1)$,

而后求 s:$s \equiv (s')^d \bmod (p-1)$,

于是得到签名 $(r \parallel s)$;

3.3　验证过程

接收方收到 $(M, (r \parallel s))$ 后,用下式来验证

$y^{m+r} \equiv r \cdot g^w \bmod p$,$w \equiv s^e \bmod p - 1$

4　群的建立及群成员加入

分布式学籍管理系统中的群签名为了保证群签名手续的完整,签名按顺序进行,需要建立群中心(GC)和密钥分配中心(KDC),负责群的建立、成员加入、签名顺序形成等。

4.1　群的建立由两步构成

第 1 步,KDC 建立群公钥。

KDC 选择两个模数 N_1, N_2 满足:

$N_1 = (2P + 1)(2Q + 1)$

$N_2 = (2p + 1)(2q + 1)$

$P, Q, (2P + 1), (2Q + 1), p, q, (2p + 1), (2q + 1)$均为素数。

然后,KDC 选择满足如下两式的素数 E_1, E_2:

$\gcd(E_1, \phi(N_1) = 1$

$\gcd(E_2, \phi(N_2) = 1$

将 $\{N_1, N_2, E_1, E_2\}$作为群公钥,并秘密保存 $\phi(N_1)$和 $\phi(N_2)$。

第 2 步,成员加入群。

假设 A_i 想成为群的一个成员,他向 KDC 申请,KDC 选择两个随机数 R_{i1}和 R_{i2},并计算满足以下两式的 D_{i1}和 D_{i2}:

$E_{i1} D_{i1} \equiv 1 (\mathrm{mod}\, R_{i1} \phi(N_1))$

$E_{i2} D_{i2} \equiv 1 (\mathrm{mod}\, R_{i2} \phi(N_2))$

将 D_{i1}和 D_{i2}秘密传送给 A_i,将 D_{i2}秘密传送给 GC。GC 将(D_{i2}, ID_i)做为 A_i 的标识,A_i 将(D_{i1}, D_{i2})作为私钥。现在,A_i 已加入群。

设 A_i 以群的名义对消息 M 签名,A_i 计算如下:

$S_1 = (M \parallel t)^{D_{i1}} \mathrm{mod}\, N_1$

$S_2 = (M)^{D_{i2}} \mathrm{mod}\, N_2$

$\{S_1, S_2\}$是签名,t 是时间。

4.2 签名按如下方式验证

$M \parallel t = S_1^{E_1} \mathrm{mod}\, N_1$

$S_1 = S_2^{E_2} \mathrm{mod}\, N_2$

GC 可以利用(D_{i2}, ID_i, S_1, S_2)计算出消息的签发者。

5 数字签名方案的实现

分布式学籍管理系统中的群签名系统中每一个签名者实际上完成一个独立数字签名,数字签名包括密钥获取、签名、验证 3 个模块。各模块块具体实现如下:

5.1 秘钥获取模块[3]

签名者初次使用系统或更改秘钥时,需要输入一个初值 p ',系统根据初值产生两个大数 q '和 t ',而后在这两个大数附近确定两个大素数 q 和 t,再由 $p = 2qt + 1$ 确定 p,对 p 进行素性检查,若 p 为素数,即可由此生成签名的私钥和验证的公钥,否则,重新输入初值。算法流程如图 1 所示。

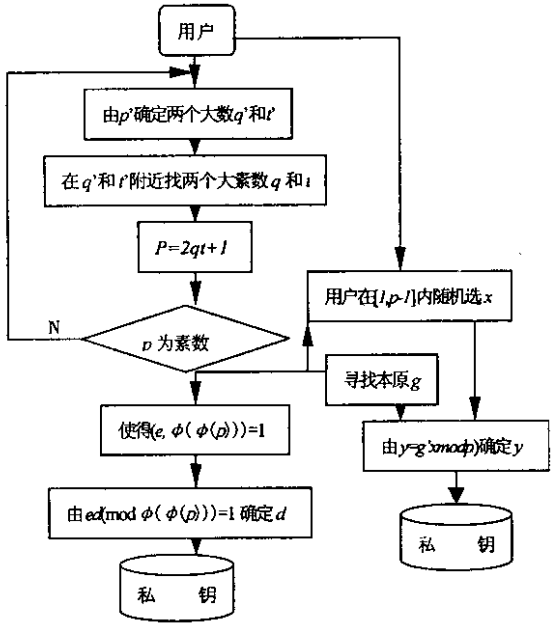

图 1 用户秘钥的获取过程

Fig.1 The Flow Diagram of the User Private Key

5.2 签名模块[3]

签名者对消息进行签名时,输入自己的签名私钥,即可得到该消息的签名。算法流程图如图 2 所示。

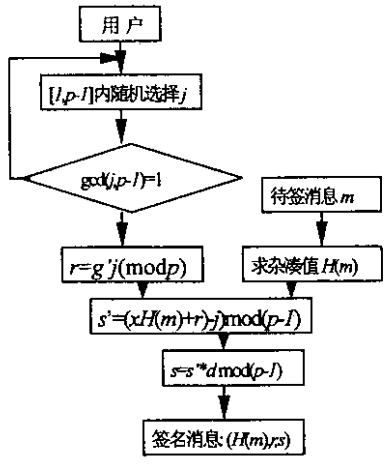

图 2 签名流程图

Fig.2 The Flow Diagram of the Signature

5.3 验证模块[3]

接收者收到签名消息后,将其作为验证模块的输入,在模块内进行验证,输出验证模块,算法流程图如图 3 所示。

6 方案具体工作流程

系统中,需提交学籍数据的教师首先在自己

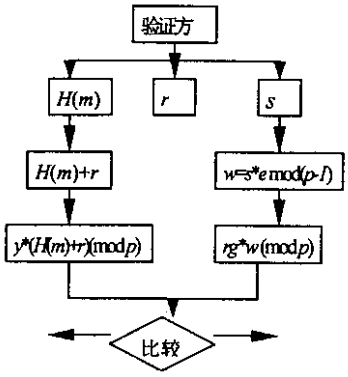

图 3　验证流程

Fig.3　The Flow Diagram of Test

的机器上安装用户秘钥生成程序、签名流程程序、验证流程程序,生成自己的公钥和私钥,将私钥妥善保存,同时将公钥存放在公钥薄并经 KDC 授权,形成完整的签名顺序表。当需提交学籍数据时,用私钥签名,并用下一签名者教研室主任的公钥对学籍数据及教师的签名进行加密,然后发往教研室主任。教研室主任收到报文,解秘、验证签名后,用自己的私钥给收到的报文签名,并将收到的报文和自己的签名用系主任的公钥加密,然后,发往系主任,依次类推,最后一位签名者将签名手续完备的报文发给教务处负责学籍管理的教师。负责学籍管理的教师验证签名完备、正确后,将成绩导入学籍管理库,保存签名文档以备核查,完成正确学籍数据提交[4~5]。

7　总结

学籍管理中的学籍数据属于重要信息,利用分布式学籍管理提交学籍数据时应保证数据安全性、一致性,文中提出用群签名技术进行学籍数据提交,既保证了学籍数据确是所声称的教师提交的,又实现了人工管理中的审阅程序,同时由于在传输过程中报文始终以密文形式传送,防止成绩在没有正式公布前被窃取。只要完整保存签名报文,必要时就可以进行鉴别认证,防止学籍管理中出现蓄意更改成绩的事件发生,完全实现学籍管理的无纸化。文中所述的群签名方案也可应用于电子政务中进行文件的提交与分发。

参考文献:

[1] Jan Hrusku, Keith Jackson. Computer Security Solutions[M]. CRC press, JNC, 1990.
[2] 谭凯军,诸鸿文,顾尚杰.基于数字签名方案 DSS/DSA 的几种应用方案[J].计算机研究与发展,1999,(5):21 – 23.
[3] 杨莉英,陈基禄,李春祥,等.数字签名技术与校园网办公自动化系统[J].华北电力大学学报,2001,(1):63 – 67.
[4] 杨良海,陈克非.一种新的群签名系统[J].计算机工程,1999,(10):44 – 49.
[5] William Stallings.密码编码学与网络安全:原理与实践[M].第 2 版.杨明译.北京:电子工业出版社,2001.

The Application of the Group Signature in Distributed Teaching Management System

JING Xu[1,2], HAN Yong-guo[1], LEI Wei-jie[1]

(1. Computer Science And Engineering School, Southwest University Of Science And Technology, Sichuan Mianyang 6210021, China
2. Study Officeof Yancheng Institute of Technology, Jiangsu Yancheng 224003, China)

Abstract: This paper introduces not only the traits and priples of the digital signature and the group signature but also a realized procedure of a group signature in the distributed teaching management.

Keywords: Digital signature; Group signature; Teaching Management System