# 数字签名技术在现代远程教育管理系统中的应用

鞠宏伟 (济南市农业学校 250023)
李凤银 刘培玉 (山东师范大学信息管理学院 250014)

摘要：本文将双方不可否认的数字签名技术引入现代远程教育管理系统，成功解决了现存远程教育管理系统中存在的需要第三方参预的问题。

关键词：远程教育管理系统 数字签名 公开密钥 私有密钥

## 1 引言

目前的远程教育管理系统还很不完善，有许多技术问题需要进一步研究和探讨，安全技术就是关键技术之一，特别是收费管理、在线考试成绩管理和毕业证书颁发等应用的顺序实施，必须用相应的安全技术和安全策略来保证。文献1中将通用数字签名技术应用于远程教育管理系统的安全及身份认证，一定程度上迎合了这种需求，解决了远程教育管理系统中的安全性问题，但仍需要有第三方—证书管理机构(Certificate Authority)的监督参预。文献2中介绍了一种两方间收方不可否认的数字签名方法，这种数字签名方法实际上可以改进成一种收发双方均不可否认的数字签名方法。本文将这种无需第三方监督的双方均不可否认的数字签名方法应用于现代远程教育管理系统的安全及身份认证管理，并且成功解决了应用中遇到的密钥分配及传输问题，使得远程教育管理系统无需第三方的监督参预就可以安全、顺利、高效地运行。

## 2 数据加密技术及加密算法

所谓数据加密技术，就是对信息进行重新编码，从而达到隐藏信息内容，使得非法用户无法获取信息真实内容的一种技术手段。数据加密过程由各种加密算法来具体实施，它以很小的代价提供较大的安全保护。根据密钥的特点，加密算法可以分为对称密钥加密算法和非对称密钥加密算法(又称公开密钥加密算法)两种。

对称密钥加密算法是传统的加密手段，其思想是：用一个协定的加密函数和一个秘密密钥加密明文，用加密函数的逆函数和同一密钥对密文解密，得到原始明文。这种加密算法执行效率高、速度快，但由于双方共享一个秘密密钥，密钥的传递很困难。

公开密钥加密算法的基本思想是：每个用户拥有两个密钥，一个是公开密钥，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，仅为自己拥有，经用户公开密钥加密的信息只能通过他的私有密钥来解密，反过来，经用户私有密钥加密的信息也只能通过他的公开密钥来解密。当两用户通信时，双方都用对方的公开密钥加密而用自己的私有密钥解密，就可以实现信息的保密传输。

在实际应用中，一般是把公开密钥算法和对称密码算法相结合，用公开密钥进行身份认证和对称密钥的传送，而用对称密钥算法实现信息的保密传输。

## 3 双方均不可否认的数字签名技术

数字签名是指附加在数据单元上的一些数据，或是对数据单元所作的密码变换，这种数据或变换能使数据单元的接收者确认数据单元的来源和数据的完整性，并保护数据，防止被人(例如接收者)伪造。

数字签名技术是建立在公开密钥加密体制基础上，经多次验证的较为理想的认定技术，是一种反事后抵赖的手段，其技术核心是至少要保证以下两个结论成立：

(1) 发送方事后不能否认他发送的报文

(2) 接受方自己不能伪造报文

签名机制的本质特征是该签名只有通过签名者的私有信息才能产生，也就是说，一个签名者的签名只能唯一地由他自己产生。为了保证信息的确是发送方的原信息，没有被非法改动，可采取信息摘要算法：发送方用一个单向函数(如SHA或MD5)从明文消息产生一个固定长度的信息摘要，并用自己的私有密钥加密摘要，创建一个数字签名，将其与消息加密后发送给接收方，接收方解密后用发送方的公开密钥验证签名得到信息摘要，同时他用原来的单向函数作用于收到的消息得到另一个信息摘要，通过比较这两条信息摘要来验证消息的完整性。

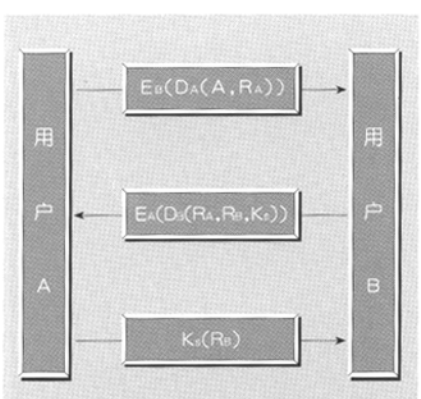


图1 双方不可否认的数字签名

在通用数字签名中发方的反事后抵赖功能是很明显的，但却不能保证收方在事后否认收到了报文，这样，实际上就形成了收发双方均不可否认的数字签名算法(如图1所示)

(1) A先用自己的私有密钥$D_A$签名自己的名字A和一个随机数$R_A$，得到签名报文$D_A(A, R_A)$，再用B的公开密钥$E_B$加密，得到待发送密文$E_B(D_A, R_A)$，然后发送给B。

(2) 当B收到密文$E_B(D_A(A, R_A))$后，先用自己的私有密钥$D_B$解密，得到A的签铭报文$D_A(A, R_A)$，再用A的公开密钥$E_A$验证(解密)签名报文，得到了A和$R_A$，这样就保证了A的不可否认性。

(3) B再用自己的私有密钥$D_B$签名A的随机数$R_A$、自己的随机数$R_B$和自己临时生成的一个会话密钥$K_S$，得到签名报文$D_B(R_A, R_B, K_S)$，再用A的公开密钥EA加密，得到密文$E_A(D_B(R_A, R_B, K_S))$，然后发给A。

(4) 当A收到B发回的密文$E_A(D_B(R_A, R_B, K_S))$后，先用自己的私有密钥$D_A$解密，得到B的签名报文$D_B(R_A, R_B, K_S)$，再用B的公开密钥$E_B$验证(解密)签名报文，得到$R_A$、$R_B$和$K_S$，这样就又保证了B的不可否认性。

(5) A再用$K_S$加密B的随机数$R_B$得到$K_S(R_B)$并发送给B，同意用密钥$K_S$进行会谈。

(6) 当B收到用他刚刚生成的会话密钥$K_S$加密的$R_B$后，就可以开始用会话密钥$K_S$和B进行通信了。

这样，就在没有第三方参预的情况下保证了收发双方的不可否认性，提供了一种无需第三方监督的收发双方均不可否认的数字签名方法。

## 4 安全及身份认证管理

### 4.1 功能设计

远程教育管理系统在网络体系结构基础上实现网络化的教学和教务管理，为学生提供实时的教育服务，主要应具备安全及身份认证管理、教师和学生管理、学位和课程管理等功能模块(如图2所示)。

(1) 安全及身份认证管理。该模块主要通过双方均不可否认的数字签名技术完成网上所有用户和学校之间相互的身份认证并为两者提供双方均不可否认的、安全可靠的保密通信。

(2) 课件管理。目的是统一教学内容和教学要求，保证教学进度与教学大纲的一致性，保证教学质量。

(3) 考前辅导。主要提供考前集中辅导服务，如网上答疑、在线讨论、模拟考试等。

(4) 试题和考试管理。主要提供在线考试服务，学生通过网上考试可正式获取该门课程的学分，待学分达到学校要求后可申请毕业。

(5) 教师和学生管理。该模块包括了教师管理和学生管理两大模块。教师管理是对学校的教师和职工的人事管理。学生管理主要包括学生的基本情况、入学、学习、毕业等的管理。

(6) 学位和课程管理。主要包括学校的学分和学位管理、专业课程的设置管理、专业设置管理、教学计划管理等。

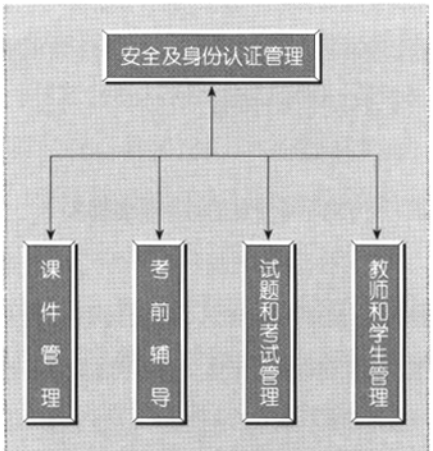

图2 功能模块

### 4.2 双方不可否认数字签名技术的应用

将双方不可否认的数字签名技术应用于现代远程教育管理系统，可以解决现存系统中需要第三方参预的问题。但这种双方不可否认数字签名技术的实现，要求有一个前提：收发双方的密钥必须是利用同一算法产生的，在有第三方参预的数字签名中，这是通过第三方一证书管理机构统一分配密钥来实现的，而在无第三方参预的情况下，密钥的生成和分配问题成为阻碍这种技术得以实现的关键。本文将双方可否认的数字签名技术应用于远程教育管理系统的安全身份认证管理模块，成功解决了这个问题，使得通信双方可在同一公开密钥算法下随时、自主地计算、选择自己的密钥，真正做到了一次一密钥。

为了更好地实现身份认证和注册考试时的安全性及颁发证书的有效性，学生在注册和考试时都必须在一个有摄像条件的机器上进行，以便及时把注册学生的头像动态地传到校方备案，作为以后颁发证书的凭证，这样可以有效地防止冒名注册、冒名考试等作弊现象，保证毕业证书的含金量。

在本远程教育管理系统正式启用前，校方需通过一定的途径(如自己的网站)公布自己所使用的公开密钥算法、签名时使用的单向函数，以及相应的使用说明，还要公布自己的由这一算法产生的公开密钥。

学生要想接受某学校提供的远程教育，必须首先通过该校公布的公开密钥算法及使用说明产生自己的一对密钥，将其中之一公开作为公开密钥，另一个保留作为私有密钥。学生有了密钥后就可以向学校提出注册申请，申请时需提交姓名、性别、出生年月、身份证号、头部相片以及自己的公开密钥等相关资料。

校方核实注册申请的真实性后，收取一

定的费用，并为该学生注册、签发"学生证"，作为以后接受远程教育服务的凭证，学生证上至少要包含学号、姓名、性别、出生年月、头部相片、身份证号、享有的权限、有效期限及校方的签名等相关信息，当然还可以包含学生的通信地址、E-mail 地址等信息。

具体实现步骤可描述如下(如图 3 所示)：

(1) 申请注册时，学生先用校方公布的单向函数对自己的注册申请计算信息摘要，再用自己的私有密钥对信息摘要签名，然后用校方的公开密钥把签名、注册申请及自己的公开密钥加密，并发送给学校。

(2) 校方用自己的私有密钥对收到的信息解密，得到学生的签名、注册申请和公开密钥，然后用学生的公开密钥验证学生的签名，接着用得到的信息摘要验证接收信息的完整性，验证通过后，同意注册。校方对自己的同意意向计算信息摘要，签名后，再用学生的公开密钥把同意意向和签名加密，并发送给学生。

(3) 学生收到校方的意向后进行解密，用校方的公开密钥验证校方的签名，接着用信息摘要验证接收信息的完整性，确认无误后把自己的信用卡号及密码签名、加密后发送给校方。

(4) 校方收到学生的信用卡后，按规定收费，并为该学生注册，签发学生证。最后将学生证签名、加密后发送给学生。

(5) 学生收到学生证后妥善保存，在申请网上学习时，只需提交学生证及自己的公开密钥，即可以享有学生证上标识的网上教育服务。

学生证到期后，通过重新注册交费即可重新使用。而且，学生可以随时用一对新密钥代替旧密钥，这时只需在申请网上学习时提交新密钥的公开密钥部分即可；同样道理，校方也可以随时更改自己的通信密钥，只要及时公开自己的公开密钥即可。这样，既实现了学校和学生之间的保密通信，又验证了双方的身份，实现了双方的不可否认性，更为关键的是解决了密钥的分配和传输问题。在整个通信过程中，由校方的安全及身份认证管理中心负责学生的身份认证、校方的签名及相应的加密解密问题而无需第三方的参预。

## 5 结束语

本文在现代远程教育管理系统中，引入双方不可否认的数字签名技术，并且成功地解决了应用中遇到的密钥分配及传输问题，在没有第三方参预的情况下顺序实现了所有的安全通信及身份认证，并且真正做到了一次一密钥。虽然该方法增加了通信次数，但确实能够在没有第三方参预的情况下，有效地防止因任何一方事后否认自己的行为而引发的争端，最大可能地维护学校与学生双方的利益，充分体现出公正平等的通信原则，且保密性好，能够迎合现代远程教育管理系统对安全性的需求，是一种可行的解决方案。

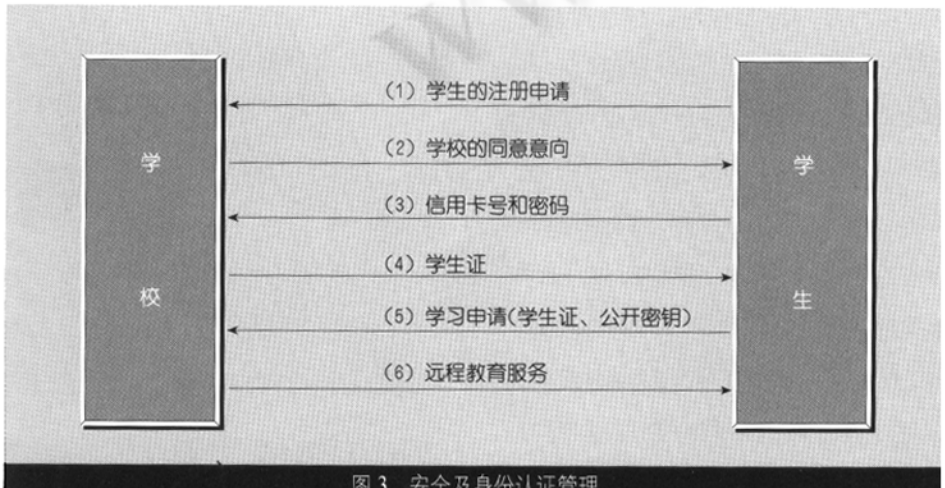


图 3 安全及身份认证管理

参考文献：

1 刘青云，章剑林，商玮，远程教育管理系统的身份认证研究与设计，计算机应用研究，2001，18(8)：44-46。

2 王志巍，吴丽红，王天青，两方间收方不可否认的数字签名，计算机工程，2001，27(7)：107-108。

3 付小青，徐智勇，邓宗海，收方不可否认的数字签名，小型微型计算机系统，1997，18(4)：12-14。