文章编号:1005－0523(2006)02－0164－02

考试管理系统中群签名的实现

于桂海

(山东工商学院 数学与信息科学学院,264005)

摘要:主要讨论为了在考试管理系统中实现数据的安全性和一致性,结合数字签名技术,介绍了群签名在管理系统中的实现.

关 键 词:数字签名;群签名;数据管理

中图分类号:TP391 **文献标识码**:A

1 概述

传统的考试管理系统,对每个学生每门课程成绩一般要经过如下的处理过程:首先,任课教师统计成绩,送教研室主任、系主任、教务处等签字,最后交给主管成绩的教务处教师手中,形成电子文档.成绩管理的安全性由纸质签名保证,而且整个过程中还有许多冗余和不变.为此可以采用考试管理系统,本文主要讨论考试管理系统中成绩管理的安全性和一致性问题的解决.

1 考试管理系统中的群签名

在考试管理系统中,考试成绩数据需要多人签名,如果成绩数据的提交和多人签名在网上进行,由于签名者在地理上往往是分布的,因此为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办法,一种方法是按一定的顺序对内容签名,各签名者的签名是累加的.每一位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受方.

在考试管理系统中,设需要提交数据的教师为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,按他们签名的顺序分别设为$A_2, A_3, \cdots, A_n$,完成最终签名后最后由签名者A_n将最终签名过的数据发送给专门负责成绩管理的教师B.设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,需要发送的数据为M,则具体的群签名实现过程步骤如下:

签名过程:

(1) A_1用一种椭圆曲线签名算法和A_1的私钥S_{kA_1}对M进行计算,产生数字签名X_1,并用下一位签名者A_2的公钥P_{kA_2}对$M+X_1$加密,产生$E_{pkA_2}(M+X_1)$,并发送给A_2.

(2) A_2收到密文后,用私钥S_{kA_2}对密文解密$D_{skA_2}(E_{pkA_2}(M+X_1))=M+X_1$,并对用$A_1$的公钥$P_{kA_1}$对$X_1$进行验证.如果验证不通过,则签名过程中止,反之,继续下一步.

(3) 如果X_1得到验证,A_2将$M+X_1$作为消息M_2重复上述两步.每个签名者如此依次签名,直到最后的签名者A_n.[1]

(4) A_n用接受者B的公钥对M_n+X_n进行加

收稿日期:2005－06－13

作者简介:于桂海(1978－),男,山东烟台人,硕士研究生,主要从事代数学及其应用、信息安全方面的研究.

密,得到 $E_{pkB}(M_n+X_n)$并发送给 B.

验证过程:

(1) B 得到密文后,用私钥 S_{kB}进行解密,$D_{skB}(E_{pkB}(M_n+X_n))=M_n+X_n$);

(2) B 用本文的椭圆曲线签名算法和 A_n 的公钥 P_{kA_n}对 M_n 进行计算,可以得到一个 $X_n^{'}$;

(3) $X_n \neq X_n^{'}$,如果,则签名失败;反之,继续下一步;

(4) 由签名过程知,$M_n=M_{n-1}+X_{n-1}$,从中分离出 M_{n-1}和 X_{n-1},按上述(1)—(3)的验证过程,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 得到验证,则整个签名过程成功.

2　群签名的实现

考试管理系统中的群签名中的每一位签名者实际上完成了一个独立的数字签名,数字签名包括密钥获取、签名、验证 3 个模块,各模块具体实现如下:

2.1　密钥获取模块

签名者初次使用系统或更改密钥时,需要选择系统参数$\{q, FR, a, b, G, n, h\}$,系统参数的生成和选取可以根据 *ECDSA* 中的方法.下面是密钥获取算法的流程图:

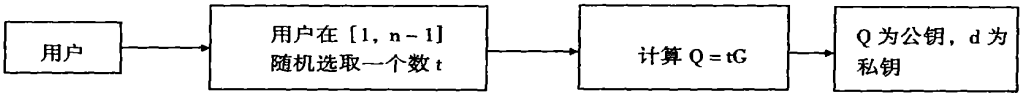

图 1　用户密钥的获取过程

2.2　签名模块

签名者对消息进行签名时,输入自己的私钥,即可得到对消息的签名.下面是签名算法流程图:

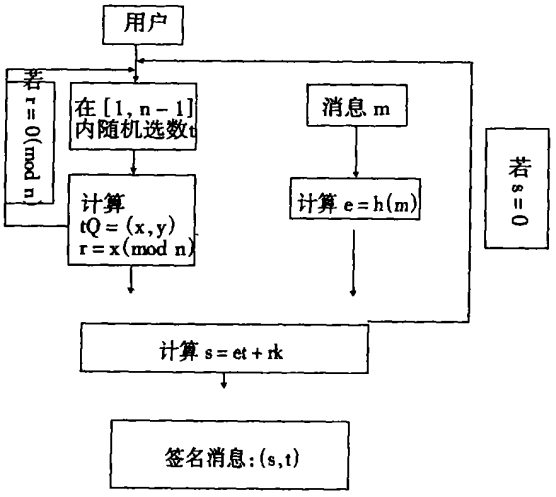

图 2　签名算法流程图

2.3　验证模块

接收者收到签名消息后,将其作为验证模块的输入进行验证.

3　总结

成绩数据属于重要信息,在进行成绩提交时应保证数据的安全性和一致性,上述群签名技术既保证了数据确实是所声称的教师提交的,又实现了人工管理中的审阅程序,同时在数据传输过程中始终实施密文传输,有效防止数据被窃取和篡改.

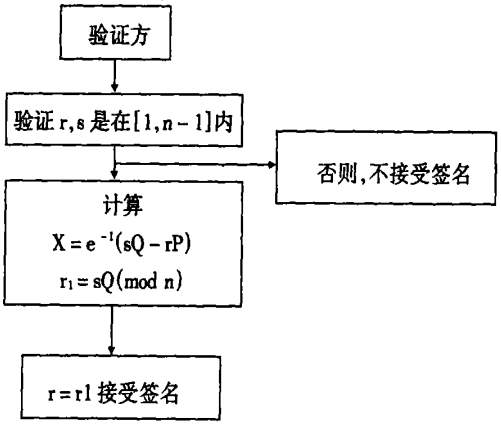

图 3　验证模块流程图

参考文献:

[1] Jan Hrusku, Keith Jackson. Cmputer Security Solutions[M]. CRC press, JNC, 1990.

[2] William Stallings 著,杨明译.密码编码学与网络安全:原理与实践[M].北京:电子工业出版社,2001.

(下转第 170 页)

rate Financial Searching for Systems Integration Supplemnt. 1996(9):30.

http://www.gloriamundi.org/var/vw/20010210.htm, 2001—02—10.

[4] A. Chekhlov, S. Uryasev and M. Zabarankin. Portfolio Optimization with Drawdown Contraints[J]. THEORY PROBAB. APPL. VOL. 44, No. 1, 2000.

[5] A. Chekhlov, S. Uryasev and M. Zabarankin. Drawdown Measure in Portfolio Optimization[J]. International Journal of Theoretical and Applied Finance, V. 8, No. 1, 2005.

[6] B. V. de. Melo Mendes and R. P. Camara Leal. Maximum Drawdown: Models and Applications[J]. working paper[J], Federal University at Rio de Janeiro, 2004.

[7] Stephan Johri, PD. Dr. Diethelm Wiirtc, Dr. kai. Nagel Portfolio optimization with hedge funds: Conditional Value At Risk And Conditional Draw-Down At Risk For Portfolio Optimization With Alternative Investments[J]. March 16, 2004.

[8] Alexei Chekhlov, Stanislav Uryasev, Michael Zabarankin. Drawdown Measure in Portfolio Optimization Research Report[J]. 2003.

Investment Portfolio Optimization Model Based on Conditional Drawdown-at-Risk

YAN Li-jun, TANG Shao-ling

(School of Mathematics and Computer science; Hunan Normal University, Changsha, 410080, China)

Abstract: In this article, we mainly introduce a new tool of measuring risk—DaR model and CDaR model and their characteristic. These models are based on the Drawdown function and the Maximal drawdown function and the Average drawdown function. We mainly discuss how to establish Investment portfolio optimization model based on Conditional Drawdown-at-Risk according to investors' risk lover and transform them into the linear programming (LP) model. From the analysised result of the A market's of our country, we know this model can greatly satisfy the investors' s different risk lover and different risk tolerance horizontals, and can obtain the most superior investment portfolio quickly and conveniently.

Key words: CDaR; investment portfolio; optimized model.

(上接第 165 页)

The Implement of Group Signature in Examination Management System

YU Gui-hai

Abstract: This paper introduces the safety and unity in examination management system, and describes the implement of group signature.

Key words: digital signature; group signature; data management