

多方签名认证算法的设计与实现*

彭绪富, 石曙东

(湖北师范学院计算机科学系, 湖北 黄石 435002)

【摘要】文章提出了电子政务及日常合同、协议业务中数字签名、认证所要解决的各种实际问题,分析了多方数字签名的信息流程,给出了信息流转的六种模式。同时,还设计了无批语多方数字签名和有批语多方数字签名方案,详细设计了基于DSA数字签名标准的有批语多方数字签名的算法程序,解决了电子政务及日常合同、协议业务中数字信息的签名、认证、存档等实际问题。

【关键词】多方; 数字签名; 认证; 方案; 算法

【中图分类号】 TP315

【文献标识码】 A

【文章编号】 1009-8054(2007) 07-0026-03

Algorithmic Design and Realization of Multiparty Signature Authentication*

PENG Xu-fu, SHI Shu-dong

(Department of Computer Science Hubei Normal University, Huangshi Hubei 435002, China)

【Abstract】 Various actual problems are proposed in the process of digital signature authentication of e-government, daily contract and agreement. By analyzing the information flow of multiparty signature, six patterns of information circulation are presented. And the scheme of multiparty digital signature with comments or without comments is designed, particularly the arithmetic program of multiparty digital signature with comments, based on DSA digital signature standard, is designed in great detail. The actual problems, such as signature, authentication and storage of digital information in the e-government, daily contract and agreement are resolved.

【Keywords】 multiparty; digital signature; authentication; scheme; algorithm

0 引言

如何实现安全、高效的数字签名、认证、存档是当今电子政务所要解决的主要问题之一。通过分析整个业务信息流转程序,计算机数字签名、认证、存档所要解决的问题有:

——纸质文档信息转换成电子数据信息(简称数字信息)的规范化、标准化处理与实现。

——数字信息的加密存档与传输。

——数字信息的单方或多方签名、认证、存档。

收稿日期: 2007-03-13

作者简介: 彭绪富, 1964年生, 男, 湖北省浠水县人, 副教授, 硕士, 研究方向: 多媒体技术、多媒体通信; 石曙东, 1963年生, 男, 湖北省阳新县人, 教授, 博士, 研究方向: 计算机网络与信息安全。

* 基金项目: 湖北省自然科学基金项目资助(项目编号: 2006ABA056)

——数字信息的盲签名、不可否认签名及认证、存档。

——序列密钥的产生^{[5][6]}。

以上问题在如今的电子政务、电子商务、电子金融等系统的应用中广泛存在,其实现算法的安全性、可计算性、高效性、实用性是人们所研究的主要内容。下面就信息的多方签名、认证、存档的算法设计与实现进行研究探讨。

1 系统分析

设某用户提交文档信息给部门1、部门2、…、部门n等多家单位,每个部门都要对信息进行审核、认证、批语、签字、盖章、存档、发送等程序处理。文档信息在各部门间的流转方式根据业务项目审批的流程不同,可分为六种模式^{[1][4]}。

——线性模式: 该模式适用于信息处理业务在职能部门间的流转,是一种流水作业形式,如图1所示。

——分支模式: 该模式是将信息处理业务依情况分发到某几个部门审核,审毕通知用户,如图2所示。

——汇聚模式: 该模式是将信息处理业务依情况分成若

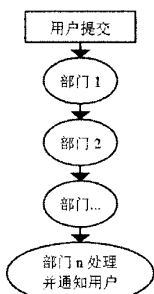


图1 线性模式

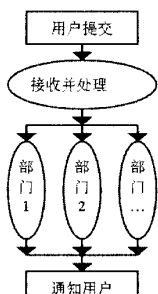


图2 分支模式

干个小业务,每个小业务由相关部门审核,审毕汇聚处理,如图3所示。

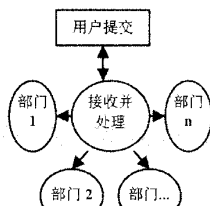


图3 汇聚模式

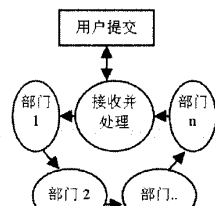


图4 环路模式

——环路模式：该模式是将信息处理业务发送到某部门,该部门审毕转到下一部门,如此直到最后部门审毕,回到信息集成处理平台通知用户,如图4所示。

——混合模式：该模式是对一项复杂的信息处理业务,可能涉及到分支模式、汇聚模式、环路模式等多种模式。

——会签模式：该模式适用于需要多家单位共同发文的业务。

在以上的几种模式中,无论是哪种模式,基本上都要完成如下事务:

——审核并认证:先认证信息来自何方并确认信息的真实性,接着审核信息内容,看是否满足要求,若不满足则说明原因并返转信息。若满足要求,给出批语,并作下一步处理。

——数字签名:对信息进行数字签名。

——存档并发送:数字签名后,根据需要做一些处理,再存档以便查阅,并将信息发送(或加密发送)到下一部门。

2 系统设计

设某用户A有信息 m ,需部门B1、B2、B3、...、Bn等多家单位审核签名,各部门认证签名后,再送用户A及其它各部门存档。根据实际情况,多方签名分无批语签名和有批语签名两种。其算法设计如下:

2.1 无批语多方签名方案设计^[2]

无批语多方签名,适用于各部门对信息 m 已审核,只需对 m 签名即可。如现实中的多部门集中签订协议、合同等,其

算法流程设计如下:

- (1) 用户A对信息 m 签名得 c ,发送签名信息 (m, c) 给B1。
- (2) B1收到 (m, c) ,对 (m, c) 进行认证,若为真,则对 m 签名得 c_1 ,发送 (m, c, c_1) 给B2。
- (3) B2收到 (m, c, c_1) ,并对其认证,若为真,则对 m 签名得 c_2 ,发送 (m, c, c_1, c_2) 给B3。
- (4) 依此进行签名,直到Bn对 m 签名得 c_n ,发送 $(m, c, c_1, c_2, c_3, \dots, c_n)$ 到A, B1, B2, ..., 等部门认证存档备案。

2.2 有批语多方签名方案设计

有批语多方签名是各部门对信息 m 审核后,加入自己的批语,再对有批语信息进行签名,其算法流程设计如下:

- (1) 用户A提供信息 m ,并对 m 签名得 c ,发送 (m, c) 给B1。
- (2) B1收到 (m, c) ,对 (m, c) 认证,若为真,则对 m 加批语 p_1 ,得 $m_1=m+p_1$,再对 m_1 签名得 c_1 ,发送 (m, p_1, c, c_1) 给B2。
- (3) B2收到 (m, p_1, c, c_1) ,对 (m, p_1, c, c_1) 认证,若为真,则对 m 加批语 p_2 ,得 $m_2=m+p_2$,再对 m_2 签名得 c_2 ,发送 $(m, p_1, p_2, c, c_1, c_2)$ 给B3。
- (4) 依此进行签名直到Bn为止,得签名信息 $(m, p_1, p_2, \dots, p_n, c, c_1, c_2, \dots, c_n)$,将此签名信息发送给A, B1, B2, ..., 存档备案。

以上的签名算法中,若 m 较大,需对 m 进行散列函数处理后再签名。

2.3 算法实现^[5]

目前较常用的数字签名算法有基于RSA密码体制、ElGamal密码体制、椭圆曲线密码体制的数字签名算法和基于DSA的数字签名标准的签名算法。在此使用基于DSA的数字签名标准的签名算法设计有批语的多方签名认证的算法程序。

设用户A有信息 m 需用户B1, B2, ..., Bn审核、批语并签名。用户A选一个512比特的素数 p ,一个160比特的素数 q ,且 $q/p-1$,再在 Z_p^* 中选两个整数 α 和 e ,并且满足 $\alpha^q \equiv 1 \pmod p$,即 α 是模 p 的 q 单位根。计算 $\beta \equiv \alpha^e \pmod p$,得密钥空间 $K_A = \{p, q, \alpha, e, \beta\}$ 。公开密钥: p, q, α, β , 保密密钥: e 。

A再选取一个随机数 t ,且满足 $1 \leq t \leq q-1$,并保密,对信息 m 签名如下:

计算: $y \equiv (\alpha^t \pmod p) \pmod q$, $\delta \equiv (m+ey)t^{-1} \pmod q$ 。得签名信息 (m, y, δ) ,发送给B1。B1收到 (m, y, δ) ,作验证计算: $u \equiv m\delta^{-1} \pmod q$, $v \equiv y\delta^{-1} \pmod q$ 。判断同余式: $(\alpha^u \beta^v \pmod p) \pmod q \equiv y$ 是否成立,若成立,则签名为真,否则有假。若签名为真, B1给批语 p_1 ,将 p_1 与 m 合并得 $m_1=m+p_1$ 。B1生成自己的密钥空间 $K_{B1}=\{p_1, q_1, \alpha_1, e_1,$

β_1 }, 再依以上的签名算法对 m_1 签名, 得签名信息(m_1, y_1, δ_1). B1 发送信息($m, y, \delta, p_1, y_1, \delta_1$)给 B2。

B2 收到信息($m, y, \delta, p_1, y_1, \delta_1$), 作验证计算:
 $m_1 = m + p_1, u \equiv m_1 \delta_1^{-1} \bmod q_1, v \equiv y_1 \delta_1^{-1} \bmod q_1$.
 判断同余式: $(\alpha_1^u \beta_1^v \bmod p_1) \bmod q_1 \equiv y_1$ 是否成立, 若成立, 则签名为真, 否则有假。若签名为真, B2 给批语 p_2 , 将 p_2 与 m 合并得 $m_2 = m + p_1$. B2 生成自己的密钥空间 $K_{B2} = \{p_2, q_2, \alpha_2, e_2, \beta_2\}$, 再依以上的算法步骤对 m_2 签名, 得签名信息(m_2, y_2, δ_2)。


B2 发送信息($m, y, \delta, p_1, y_1, \delta_1, p_2, y_2, \delta_2$)给 B3。依此签名验证直到 B_n 为止。得多方签名信息: ($m, y, \delta, p_1, y_1, \delta_1, p_2, y_2, \delta_2, \dots$)。Bn 将此多方签名信息存档, 并发送到其它各方验证存档。

3 结语

本文设计的多方数字签名认证方案及算法程序, 能较好

地解决多方协议、多方签订合同及多部门审核签名认证等问题。为电子政务、电子商务等系统中的信息流转提供了安全可靠的技术支持。

参考文献

- [1] 高科. 网上联合审批中的互联互通应用集成平台[DB/OL].
<http://www.soft6.com/know/detail.asp?id=BCAGGG>, 2003-11-24 /2006-12-28.
- [2] 王衍波, 薛通. 应用密码学[M]. 北京: 机械工业出版社, 2003; 92-193.
- [3] 黄向东, 潘郁. 公钥密码体制下协议设计的安全准则及一种网络审批协议[J]. 电子政务, 2005, (22): 72-76.
- [4] 句群慧, 张华新, 胡维华. 基于 JEE 的部门交互式审批平台的设计与实现[J]. 计算机应用与软件, 2005, 22(12): 139-141.
- [5] 丁卫平, 邓伟, 沈学华. 基于二次剩余的加密和签名算法在公文流转审批系统中的应用[J]. 计算机与现代化, 2005, (9): 71-73. 

(上接第 25 页)

也是可以理解的: 这是我们的商业机密, 关系到股东和战略合作伙伴(即美国宇航局)的巨大利益, 我们没有义务公开技术诀窍。这本来就不是一个纯学术问题, 而是一个对抗性问题, 根本不允许在正规的学术会议上发表。至于没有给出足够长度的数据, 等到 2008 年第四季度 1024 位量子计算机出来后, 这种说法将不攻自破。

(3) D-Wave 进展中的核心技术是美国宇航局的量子计算芯片, 这是美国政府 5 个量子计算计划中浮出海面的冰山一角。D-Wave 的贡献主要是低温设备和控制系统软件设计, 双方的关系类似于研制 CPU 的 Intel, 以及组装电脑的中关村公司。该进展是否属于美国政府量子计算计划中的一个合同项目, 目前还不能确定。但是, 美国政府在量子计算上的投资远大于 D-Wave 的 2000 万美元风险投资, 一定有更重要的成果。

(4) 美国政府量子计算计划的保密做得很好。美国宇航局站出来说话, 声

明由他们完成了最关键的研究环节, 并不是要公开技术原理, 而是向全世界展示一种姿态和威慑力。我们也可以把这个事件看作一次意外的泄密事故。

(5) 《自然》杂志在刻意制造朦胧的氛围。不然, 他们为什么没有把美国政府的量子计算计划与 D-Wave 的进展联系起来分析?

(6) 目前量子计算机最重要、最直接的应用目标是密码破译。完成了这个目标, 就可以假冒全世界所有银行的电子签名, 这是多么大的经济利益和战略竞争力! 然而, 与 2001 年 IBM 研制成功 7 个量子位的量子计算机不同, 无论是 D-Wave 发布的消息, 还是美国政府的发言, 以及《自然》杂志的评论, 都很少讨论这个敏感话题, 表现为刻意的回避。

(7) 国外信息安全产业界对 D-Wave 的进展表现为一种耐人寻味的沉默。显然, 如果承认这个进展, 就意味着信息安全的底层技术——RSA、DH 和 ECC 公钥密码体制将在 2009 年被彻底攻破, 从而导致全世界 PKI 系统的崩溃, 这将标志着一个信息恐怖主义时代

的来临。

参考文献

- [1] 陆晓亮, 胡苏太. 量子计算机的发展现状及趋势[J]. 高性能计算发展与应用, 2006, 1: 7-11.
- [2] 唐川. 16 量子位量子计算机问世[J]. 中国科学院国家科学图书馆《科学动态监测快报》, 2007, 4: 1-3.
- [3] Brumfiel G. Quantum Computing at 16 Qubits Programmable Computer Solves Sudoku and Sets Seating Charts. News@nature.com, ISSN: 1744-7933, Published online: 15 February 2007, doi: 10.1038/news070212-8.
- [4] Nature Physics Editorial. Reach for the stars. Nature Physics, 2007, 3(4): 211.
- [5] Wim van Dam. Quantum Computing In the 'death zone'? Nature Physics, 2007, 3(4): 220-221.
- [6] <http://www.dWavesys.com>. 