网络学习系统中代理数字签名算法的研究

王 云
WANG Yun

山西师范大学 教育技术与传媒学院,山西 临汾 041004
College of Educational Technology and Communication,Shanxi Normal University,Linfen,Shanxi 041004,China
E-mail:wangyun@sxnu.edu.cn

WANG Yun.Proxy digital signature algorithms of e-learning system.Computer Engineering and Applications,2007,43(34):136-137.

Abstract: The proxy digital signature algorithms based on the ElGamal signature scheme in existence are proposed in e-learning system,and they are mono-proxy digital signature algorithm and multi-proxy digital signature.These digital signature algorithms have the strongpoint of short key,small parameter scale,rapid operation,finer security,and contrast with the proxy digital signature algorithms based on the Fiat-Shamir signature scheme and the Guillou-Quisquater signature scheme.
Key words: e-learning system;digital signature;proxy digital signature

摘 要: 以现有的 ElGamal 数字签名体制为基础,研究了网络学习系统中的代理数字签名算法:单代理数字签名算法和多代理数字签名算法,与目前用得较多的基于 Fiat-Shamir 签名体制的代理数字签名算法和基于 Guillou-Quisquater 签名体制的代理数字签名算法相比,这些算法具有密钥短小、参数规模小、运算速度快和安全性好的优点。
关键词: 网络学习系统;数字签名;代理数字签名
文章编号:1002-8331(2007)34-0136-02 **文献标识码:**A **中图分类号:**TP393

1 网络学习系统中数字签名权力的代理

网络学习是一种融计算机网络技术、卫星通信技术及多媒体技术为一体的双向交互式的教育模式[1]。网络学习系统中信息的存储、传递、处理等过程是在开放的网络上进行,因此信息的安全问题是急需解决的重要问题。信息安全的关键问题是保证信息在信息系统中的保密性和认证性。密码学给解决信息安全问题提供了许多有效的核心技术,它在保证信息的保密性和认证性方面发挥着关键性的作用[2]。不论是手写签名和印签,还是数字签名,它们都代表了签名人的一种权力。称之为签名人的签名权力。在手写签名中,签名权力依赖于签名人的书写习惯和书法特征;在印签中,签名权力依赖于签名人掌握的印章;在数字签名中,签名权力依赖于签名人的秘密密钥。在现实生活中,人们常常根据印章的可传递性,将自己的签名权力委托给代理人,让代理人代表他们在文件上盖章(签名)。例如,某网络学院的院长在外出期间,需要让他的秘书代替他处理学院的业务,包括以学院的名义在一些文件上签名。为此,这个院长可以将学院的公章交给秘书,让秘书能够代表学院在文件上盖章。可以看出,这种委托签名权力的方法有一个特点,即学院的客户(教师、学生等)不因签名人的变更而受到影响。无论盖章人是院长还是秘书,客户得到的印签是相同的。

代理数字签名是网络学习系统中的重要问题,代理数字签名的算法是解决这一问题的关键。可以将网络学习系统中的代理数字签名分为单代理数字签名和多代理数字签名(多个原始签名人 $A_1,A_2,\cdots,A_n$ 将他们对同一个消息 m 的数字签名权力委托给同一个代理签名人,使得代理签名人能够生成一个代表这些原始签名人的数字签名),因此代理数字签名算法也可分为两种:单代理数字签名算法和多代理数字签名算法。目前用得比较多的是基于因子分解问题的代理数字签名算法(主要有基于 Fiat-Shamir 签名体制的代理数字签名算法和基于 Guillou-Quisquater 签名体制的代理数字签名算法[3-6]),这些算法的计算过程都相当复杂,具有密钥长、运算速度慢、参数规模大、安全性不易验证的缺点。下面研究适合于网络学习系统的代理数字签名算法,这些算法均以离散对数问题的 ElGamal 数字签名体制为基础[3,5]。在这些算法中,总是假设 p 是一个大素数,q 等于 $p-1$ 或是 $p-1$ 的一个大的素因子,$g\in Z_p^*$,且 $g^q=1(\mathrm{mod}\,p)$。p,q,g 对每个用户都是公开的。

2 网络学习系统的单代理数字签名

2.1 单代理数字签名算法

(1)参数设定

设 A、B 是数字签名体制的两个用户,A 为 B 的原始签名人(Original signer,即 A 将他的数字签名权力委托给了用户 B),

基金项目:山西省软科学研究项目(No.2007041039-03);山西省教育科学"十一五"规划项目(No.GH-06213);山西师范大学 2006 年教学改革研究重点项目(No.2006JGZH004)。
作者简介:王云(1964-),男,博士,副教授,山西师范大学教育技术与传媒学院院长,主要研究方向:远程教育与多媒体通信。

B 为 A 的代理签名人(Proxy signer)。设 q 是由可信的密钥分配中心秘密选取的大素数，它由密钥分配中心保密;g 是 Z_q^* 的一个生成元;s 是用户 A 的秘密密钥,且 $s\in_R Z_q^*$;p 是用户 A 的公开密钥,且 $p=g^s \pmod q$。

(2)委托过程

①A 随机选取一个数 $k\in_R Z_q^*$,计算出 $K=g^k \pmod q$;

②A 通过秘密密钥 s 产生一个新的秘密密钥 σ,并计算出 $\sigma=s+kK \pmod q$;

③A 将(σ,K)秘密地发送给 B;

④B 验证等式 $g^{\sigma}=pK^k \pmod q$是否成立。如果不成立,则终止协议。

(3)代理签名的生成过程

对于给定的消息 m,B 采用以下步骤生成代理签名:

①选择随机数 $r\in_R Z_q^*$,计算出 $R=g^r \pmod q$;

②计算出 $\tau=r^{-1}(m-sR) \pmod{q-1}$;

③以(R,τ,K)作为对 m 的代理签名。

(4)代理签名的验证过程

如果代理签名的接收方收到了消息 m 和代理签名(R,τ,K),那么他通过以下步骤来验证代理签名的有效性:

①计算出:$v=pK^K \pmod q$;

②验证:$Ver(v,(R,\tau,K),m)=True$。

其正确性可以由以下算式证明:

$$v=pK^K \pmod p\equiv g^s g^{kK} \pmod p=g^{s+kK} \pmod p=g^{\sigma} \pmod p$$

即 v 可以被看作与 σ 对应的验证公钥。

2.2　单代理数字签名应用实例

例 1 某网络学院在进行期末考试前，需要通过网络系统将每门课的考试题分发给每个网络学习的用户,为了向学习者保证考试题的可靠性,需要以网络学院的名义对所有这些考试题进行数字签名。由于考试题太多,学院的院长无法亲自审核每门课的考试题,并在这些考试题上签名。一个比较实际的做法是:学院院长将代表学院生成数字签名的权力委托给每门课的任课教师,让他们以学院的名义为其所审核的考试题生成数字签名。

例 2 某网络学院的院长由于业务需要到外地出差，在他出差期间,很可能有人给他发来电子邮件,其中有些电子邮件需要他及时回复。假如他参与了某个重要的科研项目的建设,需要尽快为这个项目提出他的建议,然而,他所去的那里不便使用网络,因此,该院长不得不委托他的秘书或助理代表他处理这些电子邮件,包括代表他在回复这些电子邮件时在回信上生成数字签名。

3　网络学习系统的多代理数字签名

3.1　多代理数字签名算法

(1)参数设定

设 $A_1,A_2,\cdots,A_n,B$ 为数字签名体制的 $n+1$ 个用户,$A_1,A_2,\cdots,A_n$为 B 的原始签名人(Original signer,即 $A_1,A_2,\cdots,A_n$ 将他们对同一个消息 m 的数字签名权力委托给了用户 B,B 为 $A_1,A_2,\cdots,A_n$的代理签名人(Proxy signer),B 能够生成一个代表这些原始签名人的数字签名。

设 q 是由可信的密钥分配中心秘密选取的大素数,它由密钥分配中心保密;g 是 Z_q^*的一个生成元;$s_i(i=1,2,\cdots,n)$是用户 A_i 的秘密密钥,且 $s_i\in_R Z_q^*$;p_i是用户 A_i的公开密钥,且 $p_i=g^{s_i} \pmod q$。

(2)委托过程

对于任意的 $i(1\leqslant i\leqslant n)$,用户 A_i执行以下步骤:

①A_i随机选取一个数 $k_i\in Z_q^*$,计算出 $K_i=g^{k_i} \pmod q$;

②A_i通过秘密密钥 s_i产生一个新的秘密密钥 σ_i,并计算出 $\sigma_i=s_i+k_iK_i \pmod q$;

③将(σ_i,K_i)秘密地发送给 B;

④B 在收到$(1\leqslant i\leqslant n)$后,验证等式$(\sigma_i,K_i)g^{\sigma_i}=p_iK_i^{k_i} \pmod q$是否成立。如果不成立,则终止协议。

(3)多代理签名的生成过程

B 在收到所有的子代理密钥$(\sigma_i,K_i)(1\leqslant i\leqslant n)$后,先计算出:

$$\sigma=\sum_{i=1}^{n}\sigma_i \pmod q$$

然后对于给定的消息 m,采用以下步骤生成代理签名:

①选择随机数 $r\in_R Z_q^*$,计算出 $R=g^r \pmod q$;

②计算出:$\tau_i=r^{-1}(m-s_iR) \pmod{q-1},(1\leqslant i\leqslant n)$;

③计算出:$\tau=\sum_{i=1}^{n}\tau_i \pmod{q-1}$;

④以$(R,\tau,K_1,K_2,\cdots,K_n)$作为对 m 的代理签名。

(4)多代理签名的验证过程

如果代理签名的接收方收到了消息 m 和代理签名$(R,\tau,K_1,K_2,\cdots,K_n)$,那么他通过以下步骤来验证代理签名的有效性。

①计算出:$v=\prod_{i=1}^{n}p_iK_i^{K_i} \pmod q$;

②验证:$Ver(v,(R,\tau,K_1,K_2,\cdots,K_n),m)$=True。

其正确性可以由以下算式证明:

$$v=\prod_{i=1}^{n}p_iK_i^{K_i} \pmod q=\prod_{i=1}^{n}g^{s_i}g^{k_iK_i} \pmod p=$$

$$\prod_{i=1}^{n}g^{s_i+k_iK_i} \pmod p=\prod_{i=1}^{n}g^{\sigma_i} \pmod p$$

即 v 可以被看作与 σ_i对应的验证公钥。

3.2　多代理数字签名应用实例

某网络学院在招生之前召开院长工作会议,参加会议的有各位院领导和有关部门的负责同志,这次会议要形成一个有关招生工作的决议文件,并将该文件在网上公布,以便有意报考该学院的学习者查询,为了保证文件的可靠性,需要参加会议的人员在该文件上签名。但由于参会人员较多,不可能人人都对该文件形成自己的数字签名,比较实际的做法是:所有参会人员对该文件联合生成一个数字签名,并将其数字签名权力委托给学院的秘书。

4　算法的特点与安全性

由于网络学习系统中信息的存储、传递、处理等过程是在开放的网络上进行,因此信息的安全问题是网络学习系统急需解决的重要问题[8]。事实表明,在网络学习过程中,经常会涉及

(下转 152 页)