基于 DSS/DSA 的盲数字签名算法

Blind Digital Signature Algorithm Based on DSS/DSA

周立章　王世伦

（成都师范高等专科学校计算机科学系　成都611930）（四川师范大学计算机学院　成都610068）

Abstract The DSA makes use of public key to verify the integrity of data for receiver and to check sender's identify. In this paper we propose a new blind digital signature scheme based on DSS/DSA, and a new multiblind digital signature scheme is given based above new scheme, the safety of these scheme is more efficient than general blind digital signature.

Keywords DSA, Digital signature, Discrete logarithm, Security

1 前言

数字签名技术是利用数学变换将一份信息或文件映射成另一份称作签名文件的文件，而数学变换往往采用单向散列函数，同时结合公钥加密和对称密钥加密的优点，保证了信息的完整性和不可抵赖性。签名机制的本质是该签名只有通过签名者的私有密钥才能产生，接收者利用签名者的公钥验证签名，第三方（仲裁机构）根据消息上的数字签名进行裁决。而盲数字签名指签名者并不知道所签信息的具体内容，信息的拥有者又可以从签名人关于盲化后信息的签名得到签名人关于真实的信息的签名。盲签名又可分为单盲数字签名和群体盲数字签名，它们在电子商务、电子货币、电子选举等方面能起到特殊的作用。

DSA（Digital Signature Algorithm，数字签名算法）是一种公开密钥算法，它使用公开密钥，为接受者验证数据的完整性和数据发送者的身份。它也可用于由第三方去确定签名和所签数据的真实性。DSA 算法的安全性基于解离散对数难题的困难性，这类签字标准具有较大的兼容性和适用性，成为网络安全体系的基本构件之一。Nyberg 和 Rueppel 提出了基于 DSA 的信息恢复的数字签名[1]，Jan L. Camenisch 等在 the Nyberg-Rueppel 方案的基础上提出了数字签名方案和盲数字签名[2]。本文基于 DSA 的离散对数签名公式变化的基础上提出了一个新的盲数字签名方案，然后在此盲签名的基础提出了一个群体盲数字签名方案。

2 DSA 算法介绍

DSA 是 Schnorr 和 ELGamal 签名算法的变种，是基于计算离散对数难度的一种算法，1994年12月已经被美国 NIST 作为数字签名标准。该算法用到以下参数：

·P 是大素数，其中 $2^{L-1}<p<2^{L}$，512bit<=L<=1024bit 且 L 为64的倍数

·q 是（p－1）的素因子，且 q 的比特长度为160位

·$g=h^{(p-1)/q} \bmod p$ 其中 h 是小于 p－1且满足 $h^{(p-1)/q} \bmod p>1$的任意数

·H(x)：指定的单向 hash 函数，且满足安全 hash 算法 SHA－1。

则 p、q、g 是全局公开密钥[3]。

DSA 用于数字签名[3]的方法是：假设用户 B 要对信息 m 签名，则 B 随机选择整数 x，$0<x<q$，计算：$y=g^{x} \bmod p$，则 x 是 B 的私钥，Y 是 B 的公钥；B 随机选择整数 k，$0<k<q$，则对 m 的签名对（r，s）由如下公式得到：$r=(g^{k} \bmod p) \bmod q$，$s=k^{-1}(h(m)+rx) \bmod q$。其验证签名公式是：$r^{s}=g^{h(m)}y^{r}$。

由于 DSA 的数字签名是基于离散数学难题的，因此签名对（r，s）中的 s 可以通过公式 $ak=(b+cx) \bmod q$[3]经过不同的变化来得到，而相应的签名验证公式为：$r^{a}=g^{b}y^{c}$。如当 a＝s，b＝h(m)，c＝r 时，就得到了原 DSA 的签名公式：$s=k^{-1}(h(m)+rx) \bmod q$ 和签名验证公式：$r^{s}=g^{h(m)}y^{r}$。因此，当我们取 a＝1，b＝－s，c＝r 时，$s=(rx-k) \bmod q$，其验证公式为：$r=g^{-s}y^{r}$。据此我们在 The Nyberg-Rueppel 签名方案[1,2]的基础上提出了一个新的盲数字签名方案，是从基于 DSA 签名公式的变化中演变出来的盲数字签名方案。

3 盲数字签名

假设用户 A 要求用户 B 盲签一份信息 m，B 的私钥是 x，公钥是 $y=g^{x} \bmod p$。

3.1 签名生成

（1）用户 B 随机或伪随机选择一整数 k，$0<k<q$；

（2）用户 B 计算 $\bar{r}=(g^{k} \bmod p) \bmod q$；若 $\bar{r}$ 为0，则返回（1）；否则将 $\bar{r}$ 发送至 A；

（3）用户 A 随机或伪随机产生两个整数 a，b，满足 $0<a,b<q$，计算 $\bar{r}'=(\bar{r}^{b} g^{a}) \bmod p$；$r=h(m,\bar{r}') \bmod q$；$r'=rb^{-1} \bmod q$。

其中 H(.) 是使用指定的 hash 函数对信息生成的散列码；若 $r'=0$，则返回（3）；否则用户 A 将 r′发送至 B；

（4）用户 B 计算：$\bar{s}=(r'x-k) \bmod q$；然后将 $\bar{s}$ 发送至用户 A；

（5）用户 A 计算：$s=(b\bar{s}-a) \bmod q$；

则（r，s）就是用户 B 对信息 m 的盲签名对。

3.2 数字签名验证

接收者 A 收到盲签名（r，s），按下列步骤进行验证：（1）获得 B 的公钥 Y；（2）计算：$V=h(m,g^{-s}y^{r})$；

如果 v＝r，则接受签名。

4 群体盲数字签名

群体数字签名分为有序群体数字签名和同时群体数字签

周立章　讲师，研究方向为计算机网络、电子商务及安全。王世伦　硕士，副院长，副教授，研究方向为计算机网络及数据库。

名两种。同时群体数字签名是指各用户同时对同一文件进行签名，最后生成一个复合签名，然后对复合签名进行验证。而群体盲数字签名是群体数字签名和单盲签名的结合，同时群体盲签名是指若干签名者同时对同一文件签名而不知道所签信息的内容，这在电子投票设计、电子货币构造等方面能起特殊作用。下面提出一个同时群体盲数字签名方案。

4.1 系统初始化

签名中心根据 DSA 算法，选出 p，q，g 和 h(x)，(p，q，g) 作为全局公钥，并向所有用户公布。H(x)是满足 SHA－1的单向 Hash 函数。

假设 n 个用户 u_i(I＝1，2，…，n)要进行签名，则 n 个用户首先按下步骤选出自己的公钥和密钥：

(1)用户 u_i 随机或伪随机选择一整数 x_i，0＜x_i＜q，计算 $y_i=g^{x_i} \bmod p$

(2)如果 y_i 为0，则返回(1)

(3)用户 u_i 向签名中心发送 y_i，并公布公钥 y_i，保密私钥 x_i；

4.2 群体盲数字签名的产生

假设用户 A 要求 n 个用户 u_i(i＝1，2，…n)同时盲签一份信息 m，产生群体盲签名步骤如下：

(1)用户 u_i 随机或伪随机选择一整数 k_i，0＜k_i＜q，计算：$r_i=(g^{k_i} \bmod p) \bmod q$；

(2)用户判断 r_i 是否为0，如果 r_i＝0，则返回(1)；

(3)用户 u_i 向 A 和签名中心发送 r_i，一旦 A 收到所有 r_i 后，计算：$\bar{r}=(\prod_{i=1}^{n} r_i \bmod p) \bmod q$；

(4)A 随机或伪随机选择两个整数 a，b，满足0＜a，b＜q，A 计算：$\bar{r}'=(\bar{r}^b g^a) \bmod p$；

(5)若 $\bar{r}'$ 为0，则返回(4)；否则 A 计算 $r=h(m,\bar{r}',T) \bmod q$；其中 T 是签名中心给的时间戳；

(6)计算 $r'=(rb^{-1}) \bmod q$，将 r′发送至每一位用户 u_i。

(7)用户 u_i 计算：$s_i=(r'x_i-k_i) \bmod q$。然后向签名中心发送 s_i，签名中心进行核实备案；

(8)签名中心收到用户的 s_i，首先计算 $\Delta T=T'-T$(T′为接收到的签名时间)，如果超过规定时间则拒绝；然后验证0＜s_i＜q；若不满足，则群体签名失败；否则计算：$\bar{s}=\sum_{i=1}^{n} s_i \bmod q$；然后将$(\bar{s},T)$发送至 A，A 检查$(\bar{s},T)$是否是来自签名中心；然后计算：$s=(\bar{s}b-a) \bmod q$。则群体盲数字签名对是(r，s)。

4.3 群体盲数字签名验证

验证者 A 按下列步骤进行验证：

(1)从签名中心获取每个用户 u_i 的公钥 y_i，计算 $y=\prod_{i=1}^{n} y_i \bmod p$；

(2)计算 $v=h(m,g^{-r'},y^{r'},T)$；

(3)如果 v＝r，则该复合群体盲数字签名有效，接受签名；否则拒绝接受签名。

5 安全分析

我们对以上两种盲数字签名方案进行安全分析。

(1)根据数字签名的特性，明文信息 m 对用户 B 和 u_i 来说是盲的。因此 B 和 u_i 得到的信息是经过盲化了的。要想求出明文 m 是不可能。因为他需要知道盲因子 b；然后根据单向 Hash 函数及离散对数难题来求解 m，这是不可行的；

(2)在这两种盲签名方案中，每一位签名者 B 和 u_i 有私钥和公钥，攻击者想从签名者的公钥中求解私钥相当于求解离散对数问题；同样攻击者想从签名者公开传送的 r_i 中求解出随机数 k_i 也是一个求离散对数问题。

(3)在同时群体盲数字签名方案中，攻击者想伪造所有签名者的签名，是不可行的，因为他伪造签名相当于求(r，s)满足验证公式，选择 s 计算 r 或选择 r 计算 s 都面临着求解离散对数问题；另外任何非法用户不能伪装成某个合法用户，因为他无此用户的私密钥；同时在群体盲数字签名方案中加入时间标志，可以抵抗签名重播攻击。

(4)在同时群体盲数字签名方案中，用户 u_i 只向用户 A 发送 r_i 和签名中心发送 s_i，因此减少了签名时信息的传输量，保证了签名的安全和正确性，因此具有一定的实用价值。

结论 本文提出了一个基于 DSA 的单盲数字签名和一个群体盲数字签名方案，其安全依赖于 DSA 的安全性，而 DSA 的安全是基于离散对数难题的；随着计算机的飞速发展，它的安全性有待于实践的检验。随着网络迅猛发展以及电子商务、电子货币、电子选举等在 Internet 中的广泛应用，盲数字签名和群体盲数字签名将在网络安全中起到非常重要的作用

参 考 文 献

1 Nyberg K，Rueppel R A. A new Signature Scheme based on the DSA Giving Message Recovery. 1st ACM Conference on Computer and Communications Security，1993，3(5)：58～61

2 Camenisch J L，Piveteau J-M，Stadler M A·Blind signature Based on the Discrete Logarithm Problem·presented at the Rump-Session of Eurocrypt'94，1994，5

3 黄元飞. 陈麟. 唐三平. 信息安全与加密解密核心技术. 上海浦东：浦东电子出版社，2001

4 陈勤. 数字签名算法的比较及其应用. 计算机应用研究，1999，16(10)：10～11

5 Lei H. New digital signature scheme based on discrete logarithm·Electron Lett.，1994，30(5)：396～398

6 Horster P，Michels M，Petersen H. Generalized blind signature schemes based on the discrete logarithm problem. Http://citeseer.nj.nec.com/nrelated/168329/377232.html

7 卢建朱. 陈火炎. 林飞. ElGamal 型多重数字签名算法及其安全性. 计算机研究与发展，2000，37(11)：1335～1339

8 冯登国. 卿斯汉. 信息安全—核心理论与实践. 北京海淀：国防工业出版社，2000