文章编号: 1000-1972(2005)04-0065-05

基于 ELGamal签名方程的盲签名方案

王化群[1], 赵君喜[2], 张力军[1]
(1. 南京邮电大学 信息工程系, 江苏 南京 210003
2. 南京邮电大学 应用数理系, 江苏 南京 210003)

摘 要: 为进一步完善 ELGamal盲签名体制, 研究了基于 ELGamal签名方程的盲签名方案。概述了盲签名的定义及其分类标准, 基于不同的签名方程, 和有限域上离散对数难解性假设, 得到了相应的强盲签名和弱盲签名方案。首次系统地对不同的 ELGamal签名方程进行了盲性研究, 并对每一个盲签名方案进行了盲性分析和安全性分析。

关键词: 盲签名方案; ELGamal签名方程; 离散对数
中图分类号: TN915.08; O158 文献标识码: A

Blind Signature Schemes Based on ELGamal Signature Equation

WANG Hua-qun[1], ZHAO Jun-xi[2], ZHANG Li-jun[1]
(1. Department of Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
2. Department of Applied Mathematics and Physics, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: In order to improve the ELGamal blind signature scheme, this paper studies the blind signature schemes based on the ELGamal signature equations. Following a summary of the definition and classification standard of blind signature, based on the different signature equations and the assumption of difficulty in solving the discrete logarithm problem on the finite field, we get the corresponding strong blind signature and weak blind signature schemes. It's the first time to analyze the blind properties of the different ELGamal signature equations. Finally we give the blind analysis and security analysis to each blind signature scheme.

Key words: blind signature schemes; ELGamal signature equation; discrete logarithm

1 引 言

数字签名是公钥密码技术的一类应用, 是一种网络传输的安全工具。通过数字签名能够实现对原始报文的鉴别和不可抵赖性。数字签名协议的一个基本特征是文件的签署者知道他们在签署什么。盲签名是由 David Chaum于 1983年提出的, 要求签名者对所签署消息是不可见的。盲签名在数字现金, 电子投票等领域都有较大的应用价值, 特别是目前的数字现金, 大部分都是采用盲签名的原理实现的。

收稿日期: 2004-09-29

盲签名的基本实现是: 求签名者把明文消息 M 通过盲因子变换为 M', M' 隐藏了明文 M 的内容; 然后把 M' 给签字者进行签名, 得到签名结果 $S(M')$; 最后, 求签名者取回 $S(M')$, 采用逆盲变换处理得到 $S(M)$, 就是 M 的签名, 如图 1所示:

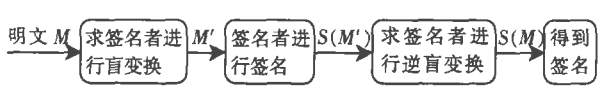


图 1 盲签名的基本实现过程

根据盲签名的盲化程度, 将盲签名分为 3类: 弱盲签名、强盲签名和盲参数签名方案[1]。本文仅讨论前两类盲签名。弱盲签名方案中, 签名者仅知道对盲化后消息的签名信息, 不知道对盲化前消息的

签名信息。若签名者保留对盲化后消息的签名信息,待对盲化前消息的签名公开后,签名者可以找出两者之间的联系,即满足:

(1)消息的内容对签名者来说是不可知的;

(2)求签名者把已签名的消息公开后,签名者能够追踪所签的消息,即签名者能够将 $S(M')$与 $S(M)$进行联系;

强盲签名是一类要求更强的盲签名,它不仅满足盲签名的要求,还要满足下面两个条件:

(1)消息的内容对签名者来说是不可知的;

(2)求签名者把已签名的消息公开后,签名者不能追踪所签的消息,即签名者无法将 $S(M')$与 $S(M)$进行联系。

定义 **1** 假设 u, v是两个随机变量,其概率分布分别为 $P(u)$, $P(v)$,联合概率分布为 $P(u, v)$,如果不存在多项式时间算法区分 $P(u, v)$与 $P(u) * P(v)$,则称 u, v是不可联系的[2,3]。

假设在签名过程中签名者得到的消息为$\sum$,求签名者得到的消息签名对为 $(M, (S(M)))$,强盲签名可以非正式地定义为

定义 **2** 在盲签名方案中,如果$\sum$与 $(M, (S(M)))$是不可联系的,则称该盲签名方案为强盲签名方案。

现有许多弱盲签名算法,如文献[4]提出的盲签名方案,文献[5]已给出其弱盲性证明。目前存在的强盲签名算法有盲 RSA 算法,Schnorr算法和基于 Nyberg-Rueppe算法的盲签名等,文献[6]给了介绍。本文给出了基于 ElGamal签名方程的几种弱盲签名方案和强盲签名方案。

2 ElGamal签名方程

ElGamal算法既可用于数字签名,也可用于加解密,其安全性依赖于计算有限域上离散对数的困难性。ElGamal数字签名体制是由 T. ElGamal于1985年提出的,其变体已经用于 DSS中。ElGamal数字签名体制是 Rabin签名体制的变形,也使用了随机数,可称为随机化的数字签名。

在本文中所用的一些参数,其含义如下:

Z_p: 有限域,其中 p是一个大素数,确保在 Z_p中求解离散对数在计算上是困难的;

g: Z_p的本原;

A: 代表请求签名者,即用户 Alice;

S: 代表签名者 Signer

m: 盲化前的消息,即原始消息;

m': 盲化后的消息;

k: Z_p中的随机数,作为签名者 Signer签名时的随机数;

x: 用户 A的私钥;

y: 用户 A的公钥;

α, β: Z_p中的随机数,其函数作为盲化因子;

r, s: 签名者关于盲化后的消息 m'的签名;

r', s': 请求签名者逆盲化后关于盲化前的消息 m的签名。

如果把 ElGamal数字签名过程中用的等式:

$$s=(m-xr)k^{-1} \bmod (p-1)$$

修改为 $u=x*v+k*w \bmod (p-1)$,那么当 $u=m$, $v=r$, $w=s$时,签名方程就是 ElGamal签名过程中使用的等式。如果把 u, v, w分别对应不同次序的 m, r, s就可以得到其它的 ElGamal数字签名体制。

下面列出 6种基本签名方程[7],他们定义了 s和 (r, m, x, k)的关系:

$$m=sk+rx \quad (1)$$

$$m=sx+rk \quad (2)$$

$$r=mx+sk \quad (3)$$

$$r=mk+sx \quad (4)$$

$$s=mk+rx \quad (5)$$

$$s=mx+rk \quad (6)$$

3 基于 ElGamal签名方程的弱盲签名方案

(1)基于签名方程(1)的弱盲签名方案

Step1: S选取随机数 $k\in Z_{p-1}$,计算 $r=g^k$,然后把 r发送给用户 A;

Step2: A随机选取 $\beta\in Z_{p-1}$,计算 $m'=r^{\beta}m \bmod (p-1)$,然后把 m'发送到 S;

Step3: 通过 $m'=xr+ks \bmod (p-1)$计算得到 s,把签名 $(m', (r, s))$发送给 A;

Step4: A计算 $r'=r^{1-\beta} \bmod (p-1)$, $s'=(1-\beta)^{-1}r^{-\beta}s \bmod (p-1)$;

则 A得到签名 $(m, (r', s'))$。

确认者计算: $v_1=y^{r'}r^{s'} \bmod p$, $v_2=g^m \bmod p$,比较 v_1和 v_2,如果 $v_1=v_2$,表示签名有效;否则,签名无效。

签名验证算法证明:

$$m'=xr+ks \bmod (p-1),$$

$$r^{\beta}m=xr+ks \bmod (p-1),$$

$$m=xr^{1-\beta}+(1-\beta)k(1-\beta)^{-1}sr^{-\beta} \bmod (p-1),$$

$$m=xr'+(1-\beta)ks' \bmod (p-1)。$$

又因为 $r'=g^{k(1-\beta)}$, 所以签名 $(m,\ (r',\ s'))$满足签名方程(1), 下面考察签名验证中的等式:

$$v_2=g^m \bmod p=g^{xr'+(1-\beta)ks' \bmod (p-1)} \bmod p$$

$$=y^{r'}r^{s'} \bmod p=v_1$$

由于 $v_1=v_2$, 所以说明该签名验证算法成立。

安全性分析: 该方案的安全性基于 ELGamal签名体制的安全性, 可抵御伪造给定消息数字签名的攻击, 也可抵御窃取签名者私钥的攻击[8]。为防止攻击, 在使用该算法时要求签名者每次签名时使用不同的随机数 k, 同时不能泄漏该随机数 k, 否则攻击者能够求解出用户的私钥 x。

签名的弱盲性分析: A进行盲变换后, 得到消息 $m'=r^{\beta}m \bmod (p-1)$, 由于 β是随机的, 且对 S是保密的, 所以 S得不到消息 m', 因而满足盲签名的条件; 当消息的签名公布后, 签名者利用 $(m,\ (r',\ s'))$和 $(m',\ k,\ x,\ (r,\ s))$求解 β, 由于 $r'=r^{1-\beta} \bmod (p-1)$, $s'=(1-\beta)^{-1}r^{-\beta}s \bmod (p-1)$, 在已知 $(m,\ m',\ r)$的条件下且在有限域上, 容易得到 $\beta=(1-r'S'^{-1}r^{-1}) \bmod (p-1)$, 所以满足弱盲签名的条件。

(2) 基于签名方程(2)的弱盲签名方案

Step1: S选取随机数 $k\in Z_{p-1}$, 计算 $r=g^k$, 然后把 r发送给用户 A;

Step2: A随机选取 $\beta\in Z_{p-1}$, 计算 $m'=(\beta+1)^{-1}r^{-\beta}m \bmod (p-1)$, 然后把 m'发送到 S;

Step3: S通过 $m'=xs+kr \bmod (p-1)$计算得到 s, 把签名 $(m',\ (r,\ s))$发送给 A;

Step4: A计算 $r'=r^{1+\beta} \bmod (p-1)$, $s'=(1+\beta)r^{\beta} \bmod (p-1)$;

则 A得到签名 $(m,\ (r',\ s'))$。

确认者计算: $v_1=r^{r'}y^{s'} \bmod p$, $v_2=g^m \bmod p$; 比较 v_1和 v_2, 如果 $v_1=v_2$, 表示签名有效; 否则, 签名无效。

签名验证算法证明:

$$m'=xs+kr \bmod (p-1)$$

$$(\beta+1)^{-1}r^{-\beta}m=xs+kr \bmod (p-1)$$

$$m=(\beta+1)xsr^{\beta}+(1+\beta)kr^{\beta+1} \bmod (p-1)$$

$$m=xs'+(1+\beta)kr' \bmod (p-1)$$

又因为 $r'=g^{k(1+\beta)}$, 所以签名 $(m,\ (r',\ s'))$满足签名方程(2), 下面考察签名中的等式:

$$v_2=g^m \bmod p=g^{xs'+(1+\beta)kr' \bmod (p-1)} \bmod p$$

$$=y^{s'}r^{r'} \bmod p=v_1$$

由于 $v_1=v_2$, 所以说明该算法成立。

安全性分析: 同上一个方案。

签名的弱盲性分析: A进行盲变换后, 得到消息 $m'=(\beta+1)^{-1}r^{-\beta}m \bmod (p-1)$, 由于 β是随机的, 且对 S是保密的, 所以 S得不到消息 m', 因而满足盲签名的条件; 当消息的签名公布后, 签名者利用 $(m,\ (r',\ s'))$和 $(m',\ k,\ x,\ (r,\ s))$求解 β, 由于 $r'=r^{1+\beta} \bmod (p-1)$, $s'=(1+\beta)r^{\beta}s \bmod (p-1)$, 在已知 $(m,\ m',\ r)$的条件下且在有限域上, 容易得到 $\beta=(s'r'^{-1}s^{-1}r-1) \bmod (p-1)$, 所以满足弱盲签名的条件。

(3) 基于签名方程(3)的弱盲签名方案

Step1: S选取随机数 $k\in Z_{p-1}$, 计算 $r=g^k$, 然后把 r发送给用户 A;

Step2: A随机选取 $\beta\in Z_{p-1}$, 计算 $m'=r^{\beta}m \bmod (p-1)$, 然后把 m'发送到 S;

Step3: S通过 $r=sk+m'x \bmod (p-1)$计算得到 s, 把签名 $(m',\ (r,\ s))$发送给 A;

Step4: A计算 $r'=r^{1-\beta} \bmod (p-1)$, $s'=(1-\beta)^{-1}r^{-\beta}s \bmod (p-1)$;

则 A得到签名 $(m,\ (r',\ s'))$。

确认者计算: $v_1=y^m r^{s'} \bmod p$, $v_2=g^{r'} \bmod p$, 比较 v_1和 v_2, 如果 $v_1=v_2$, 表示签名有效; 否则, 签名无效。

签名验证算法证明:

$$r=sk+m'x \bmod (p-1)$$

$$r^{1-\beta}=(1-\beta)kr^{-\beta}(1-\beta)^{-1}s+mx \bmod (p-1)$$

$$r'=(1-\beta)ks'+mx \bmod (p-1)$$

又因为 $r'=g^{k(1-\beta)}$, 所以签名 $(m,\ (r',\ s'))$满足签名方程(4), 下面考察签名中的等式:

$$v_2=g^{r'} \bmod p=g^{(1-\beta)ks'+mx \bmod (p-1)} \bmod p$$

$$=y^m r^{s'} \bmod p=v_1$$

由于 $v_1=v_2$, 所以说明该验证算法成立。

安全性分析: 同上一个方案。

签名的弱盲性分析: A进行盲变换后, 得到消息 $m'=r^{\beta}m \bmod (p-1)$, 由于 β是随机的且对 S是保密的, 所以 S得不到消息 m', 因而满足盲签名的条件; 当 A消息的签名公布后, 签名者利用 $(m,\ (r',\ s'))$和 $(m',\ k,\ x,\ (r,\ s))$, 由方程组 $r'=r^{1-\beta} \bmod (p-1)$, $s'=(1-\beta)^{-1}r^{-\beta}s \bmod (p-1)$求解 $\beta=(1-s'^{-1}r^{-1}sr') \bmod (p-1)$, 所以满足弱盲签名的条件。

4　基于 ELGamal签名方程的强盲签名方案

(1) 基于签名方程(4)的强盲签名方案

Step1: S生成随机数 $k\in Z_{p-1}$, 计算 $r=g^k$, 然后把 r发送给用户 A;

Step2: A随机生成 $\beta\in Z_{p-1}$, 计算 $m'=\beta r^{-\beta+1}m \bmod (p-1)$, 然后把 m'发送到 S;

Step3: S通过 $r=m'k+sx \bmod (p-1)$计算得到 s, 把签名 $(m', (r, s))$发送给 A;

Step4: A计算 $r'=r^{\beta} \bmod (p-1)$, $s'=r'r^{-1}s \bmod (p-1)$;

则 A得到签名 $(m, (r', s'))$。

确认者计算: $v_1=y^{s'}r^{m'} \bmod p$, $v_2=g^{r'} \bmod p$, 比较 v_1和 v_2, 如果 $v_1=v_2$, 表示签名有效; 否则, 签名无效。

签名验证算法证明:

$$r=m'k+sx \bmod (p-1)$$
$$r^{\beta}=\beta km'+r^{\beta-1}sx \bmod (p-1)$$

又因为 $r'=g^{k\beta} \bmod p$, 所以签名 $(m, (r', s'))$满足签名方程(4), 下面考察签名中的等式:

$$v_2=g^{r'} \bmod p=g^{\beta mk+r^{\beta-1}sx \bmod (p-1)} \bmod p$$
$$=y^{s'}r^{m'} \bmod p=v_1$$

由于 $v_1=v_2$, 所以说明该算法成立。

安全性分析: 同上一个方案的安全性分析。

签名的强盲性分析: A对消息 m进行盲变换后, 得到消息 $m'=\beta r^{-\beta+1}m \bmod (p-1)$, 由于 β是随机的且对 S是保密的, 所以 S得不到消息 m', 因而满足强盲签名的条件(1); A公布签名的消息后, 签名者利用 $(m, (r', s'))$和 $(m', k, x, (r, s))$求解 β, 由于 $r'=r^{\beta} \bmod (p-1)$, 在已知 (m, m', r, r', s, s')的条件下求 β属于有限域上的离散对数问题, 求解非常困难, 所以满足强盲签名的条件(2)。

(2)基于签名方程(5)的强盲签名方案

Step1: S生成随机数 $k\in Z_{p-1}$, 计算 $r=g^k \bmod p$, 然后把 r发送给用户 A;

Step2: A随机生成 α, $\beta\in Z_{p-1}$, 计算 $m'=\alpha^{-1}g^{-\beta}r^{1-\alpha}m \bmod (p-1)$, 然后把 m'发送到 S;

Step3: S通过签名方程 $s=xm'+kr \bmod (p-1)$计算得到 s, 并把签名 $(m', (r, s))$发送给用户 A;

Step4: A计算 $r'=r^{\alpha}g^{\beta} \bmod p$, $s'=\alpha r^{-1}r's+\beta r' \bmod (p-1)$;

则 A得到签名 $(m, (r', s'))$。

确认者计算: $v_1=y^{m'}r^{r'} \bmod p$, $v_2=g^{s} \bmod p$, 比较 v_1和 v_2, 如果 $v_1=v_2$, 表示签名有效; 否则, 签名无效。

签名验证算法证明:

$$s=xm'+kr \bmod (p-1)$$
$$\alpha g^{\beta}r^{\alpha-1}s=xm+\alpha g^{\beta}r^{\alpha-1}kr \bmod (p-1)$$
$$\alpha g^{\beta}r^{\alpha-1}s+\beta g^{\beta}r^{\alpha}=xm+(\alpha k+\beta)g^{\beta}r^{\alpha} \bmod (p-1)$$

又因为 $r'=r^{\alpha}g^{\beta}=g^{\alpha k+\beta} \bmod p$, 所以签名 $(m, (r', s'))$满足签名方程(5), 下面考察签名中的等式:

$$v_2=g^{s'} \bmod p=g^{xm+(\alpha k+\beta)r \bmod (p-1)} \bmod p$$
$$=y^{m}r^{r'} \bmod p=v_1$$

由于 $v_1=v_2$, 所以说明该算法成立。

安全性分析: 同上一个方案的安全性分析。

签名的强盲性分析: A对消息 m进行盲变换后, 得到消息 $m'=\alpha^{-1}g^{-\beta}r^{1-\alpha}m \bmod (p-1)$, 由于 α, β是随机的, 并且对 S是保密的, 所以 S得不到消息 m', 因而满足强盲签名的条件(1); 当用户 A公布消息 m的签名后, 签名者利用 $(m, (r', s'))$和 $(m', k, x, (r, s))$, 由方程组 $r'=r^{\alpha}g^{\beta} \bmod p$, $s'=\alpha r'r^{-1}s+\beta r' \bmod (p-1)$求解 α, β, 在已知条件下求 α, β属于有限域上的离散对数问题, 求解非常困难, 即签名者在利用 $(m, (r', s'))$和 $(m', k, x, (r, s))$得不到 $(m, (r', s'))$与 $(m', (r, s))$之间的联系, 所以满足强盲签名的条件(2)。

(3)基于签名方程(6)的强盲签名方案

Step1: S生成随机数 $k\in Z_{p-1}$, 计算 $r=g^k \bmod p$, 然后把 r发送给用户 A;

Step2: A随机生成 α, $\beta\in Z_{p-1}$, 计算 $r'=r^{\alpha}g^{\beta} \bmod p$, $m'=\alpha r'^{-1}m \bmod (p-1)$, 然后把 m'发送到 S;

Step3: S通过 $s=km'+xr \bmod (p-1)$计算得到 S, 把签名 $(m', (r, s))$发送给 A;

Step4: 计算 $s'=r^{-1}r's+\beta m \bmod (p-1)$;

则 A得到签名 $(m, (r', s'))$。

确认者计算: $v_1=y^{r'}r^{m'} \bmod p$, $v_2=g^{s} \bmod p$, 比较 v_1和 v_2, 如果 $v_1=v_2$, 表示签名有效; 否则, 签名无效。

签名验证算法证明:

$$s=km'+xr \bmod (p-1)$$
$$s=k\alpha r'^{-1}m+xr \bmod (p-1)$$
$$r'r^{-1}s+\beta m=(\alpha k+\beta)m+xr' \bmod (p-1)$$
$$s'=(\alpha k+\beta)m+xr' \bmod (p-1)$$

又因为 $r'=r^{\alpha}g^{\beta}=g^{k\alpha+\beta}$, 所以签名 $(m, (r', s'))$满足签名方程(6), 下面考察签名中的等式:

$$v_2=g^{s'} \bmod p=g^{(\alpha k+\beta)m+xr \bmod (p-1)} \bmod p$$
$$=y^{r'}r^{m'} \bmod p=v_1$$

由于 $v_1 = v_2$, 所以说明该算法成立。

安全性分析: 同上一个方案的安全性分析。

签名的强盲性分析: A 对消息 m 进行盲变换后, 得到消息 $m' = \alpha r'^{-1} m \bmod p$, 由于 α, r' 是随机的并且对 S 是保密的, 所以 S 得不到消息 m, 因而满足强盲签名的条件 (1); A 公布签名的消息后, 签名者利用 $(m, (r', s'))$ 和 $(m', k, x, (r, s))$ 由方程组

$$\begin{cases} r' = r^{\alpha} g^{\beta} \bmod (p-1) & (\text{I}) \\ s' = r^{-1} r' s + \beta m \bmod (p-1) & (\text{II}) \end{cases}$$

求解 α, β, 在已知 $(m, (r', s'))$ 和 $(m', k, x, (r, s))$ 的条件下利用方程 (II) 容易求得 $\beta = (r^{-1} r' s - s') m^{-1} \bmod (p-1)$, 但利用方程 (I) 计算 α 属于求有限域上的离散对数问题, 求解非常困难, 即签名者利用 $(m, (r', s'))$ 和 $(m', k, x, (r, s))$ 得不到 $(m, (r', s'))$ 与 $(m', (r, s))$ 之间的联系, 所以满足强盲签名的条件 (2)。

5 结束语

本文基于 6个 ELGamal签名等式提出了相应的盲签名算法。对前 3个签名等式给出了相应的弱盲签名方案, 对后 3个签名等式给出了相应的强盲签名方案。这几种盲签名方案的安全性都是基于有限域上的求解离散对数的难题, 因而是安全的。

参考文献:

[1] 杜伟章, 陈克非. 基于离散对数问题构造弱盲签名方案[J]. 计算机工程与应用, 2003, 16: 11~12.

[2] GOLDWASSER S, MICALI S. Probabilistic encryption[J]. Journal of Computer and System Sciences, 1984, 28(2): 270~299.

[3] HARN L. Group oriented (t, n) threshold signature and multisignature[J]. IEE Proc Computers and Digital Technignes, 1994, 141(5): 307~313.

[4] CARMENISCH J L, PIVETAU J M, STADLER M A. Blind signatures based on the discrete logarithm problem[A]. Rump Session of Eurocrypt' 94[C]. Perugia, Italy, 1994.

[5] HARN L. Cryptanalysis of the blind signatures based on the discrete logarithm problem[J]. Electronics Letters, 1995, 31(14): 1136.

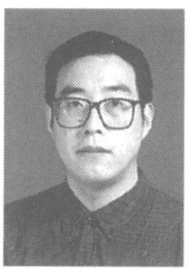
[6] 张先红. 数字签名原理及技术[M]. 北京: 机械工业出版社, 2004.

[7] MENEZES A, VAN OORSCHOR PC, VANSTONE S. Handbook of Applied Cryptography[M]. New York: CRC Press, 1996.

[8] 冯登国. 密码分析学[M]. 北京: 清华大学出版社; 广西: 广西科学技术出版社, 2000.

作者简介:

王化群 (1974 –), 男, 山东济宁人。南京邮电大学信息工程系博士生。1997年和 2000年分别毕业于山东师范大学和华东师范大学数学系, 获理学学士和硕士学位。目前主要研究方向: 无线网络的安全。



赵君喜 (1963 –), 男, 陕西渭南人。南京邮电大学应用数理系副教授。主要研究领域为通信信号处理、小波分析等。

张力军 (1942 –), 男, 浙江苍南人。南京邮电大学信息工程系教授, 博士生导师。

(本见刊 2005年第 3期第 26页)