广义 ELGamal 型盲签名方案的强弱性分析

曾 娜,余 敏
ZENG Na,YU Min

江西师范大学 计算机信息工程学院,南昌 330022
School of Computer Information and Engineering,Jiangxi Normal University,Nanchang 330022,China
E-mail:zengna1113@163.com

ZENG Na,YU Min.Untraceability analysis of generalized ELGamal type blind signature schemes.Computer Engineering and Applications,2008,44(27):119-121.

Abstract: Yao Yi-feng claims that according to his method of affine transform,the strong blind signature scheme is constructed when three blind variables are used,and the weak blind signature scheme is constructed when two blind variables are used.In this paper the authors prove that there is always a set of bind variables that make any two pairs of signed messages related,the blind schemes are always strong no matter two or three blind variables are used.Therefore,Yao Yi-feng's claim is incorrect,and his proof of the untraceability of the blind signature scheme using three blind variables is not very accurate.

Key words: digital signature;blind signature;strong blind signature;weak blind signature

摘 要:分析了基于离散对数问题构造盲签名方案的一些文献中在对盲签名的强弱性分析方面存在的问题。通过证明任意一个合法的消息签名对,都能找到一组盲因子使之与某个盲消息签名对相联系,指出了以姚亦峰的二元仿射变换为构造思想,引入三元随机盲化参数得到的盲签名方案的强盲性证明中"基于离散对数难题"的这一论据是不成立的,重新给出了其强盲性的形式化证明;而使用二元随机盲化参数得到的盲签名方案为弱盲签名的论断是错误的,重新证明它也属于强盲签名。

关键词:数字签名;盲签名;强盲签名;弱盲签名
DOI:10.3778/j.issn.1002-8331.2008.27.038 **文章编号:**1002-8331(2008)27-0119-03 **文献标识码:**A **中图分类号:**TP309

1 引言

数字签名是一项重要的计算机安全技术,它的基本作用是保证传送的信息不被篡改和伪造,并确认签名者的身份。盲签名是一种特殊的数字签名。1983 年,Chuam[1]首先提出了盲签名的概念。盲签名是指签名者并不知道所签文件或消息的具体内容,而文件或消息的拥有者又可以得到签名人关于真实文件或消息的签名。基于盲签名的特点,盲签名技术可广泛应用于电子货币、电子投票、电子支付等系统中,满足这些应用在匿名性方面的要求。

盲签名方案通常是这样实现的:假设 Alice 是签名者,Bob 是消息拥有者。Bob 引入盲因子将原消息 m 盲化为 m',将 m' 发送给 Alice;Alice 对盲消息 m'进行签名并发送$(m',sig(m'))$给 Bob;Bob 将$(m',sig(m'))$除以盲因子得到 Alice 对原消息 m 的签名$(m,sig(m))$。当 Alice 看到$(m,sig(m))$时可以验证它是 Alice 对消息 m 的有效签名,但 Alice 无法将$(m',sig(m'))$和$(m,sig(m))$联系起来。

继文献[1-2]提出的基于因子分解问题、离散对数问题的盲签名方案之后,随着对盲签名研究的不断深入,强盲签名[3]、弱盲签名、部分盲签名的概念陆续被提出。假设 Alice 记录下在某次盲签名过程中观测到的数据集合 U,待 Bob 公布其得到的消息签名对$(m,sig(m))$后,Alice 无法将 U 和$(m,sig(m))$联系起来,则称该签名方案为强盲签名方案,否则称为弱盲签名方案。在强盲签名方案中,签名者事后无法对消息拥有者进行追踪。

国内的一些学者也对盲签名技术进行了研究。姚亦峰等人提出了基于二元仿射变换的广义 ELGamal 型盲签名方案的一般构造方法[4],并列举了具体的实例[5]加以说明。姚亦峰指出在用他的方法构造盲签名时若使用 3 个随机盲化参数,则得到的为强盲签名方案,若使用的随机盲化参数少于 3 个,则相应的盲签名方案为弱盲签名方案。基于姚亦峰的思想和方法,文献[6]引入 3 个随机盲化参数构造了广义 ELGamal 型强盲签名的若干实例,而文献[7]则引入两个随机盲化参数构造了广义 ELGamal 型弱盲签名的若干实例。

本文将以文献[4]中的一个基于三元随机盲化参数构造的广义 ELGamal 型强盲签名方案为例子, 指出该盲签名方案确实具有强盲性,但原文对其强盲性的证明是不准确的,本文将重新给出形式化证明。接着本文将以文献[7]中的一个基于二元随机盲化参数构造的广义 ELGamal 型弱盲签名方案为例子,指出该盲签名方案为弱盲签名的结论是错误的,并证明该方案

基金项目:973 前期研究项目(No.2007CB316505)。
作者简介:曾娜(1976-),女,硕士研究生,研究方向为信息安全、无线传感器网络;余敏,教授,硕士生导师,研究方向为信息安全、网络计算技术、无线传感器网络。
收稿日期:2007-11-15 **修回日期:**2008-02-18

具有强盲性。除了形式化证明外,在文章的第 4 章,将以一些具体的数据例子来证实本文的观点。

2 三元随机盲化参数构造盲签名

文献[4]中论述了广义 ELGamal 型盲签名方案的一般性构造方法,并且基于三元随机盲化参数构造了两个具体的盲签名方案实例。下面将以其中的一个盲签名方案实例展开说明,证明"该方案是强盲签名"这一结论是正确的,但原文中"基于离散对数难题"的论据是不成立的,本文将对该方案的强盲性给出重新证明。

2.1 方案简介

系统参数:p 是一个大素数,q 是 $p-1$ 的一个大素数因子,g 是 Z_p^* 上的一个 q 阶元,即 $g^q \equiv 1 \bmod p$。Alice 为签名者,Bob 为消息拥有者。Alice 的私钥为 $x \in Z_q$,公钥为 $y=g^x \bmod p$。盲签名的过程如下:

(1)Alice 随机选择 $k' \in Z_q$,计算 $R'=g^{k'} \bmod p$,$r'=R' \bmod q$,将 R' 发送给 Bob。

(2)Bob 随机选择 $a,b,c \in Z_q$,计算 $R=R'^a y^b g^c \bmod p$,$r=R \bmod q$,$m'=a^{-1}r'^{-1}(rm-b) \bmod q$。将 m' 发送给 Alice。

(3)Alice 对消息 m' 签名,即计算 s',满足 $r'm'x=k'+s' \bmod q$,将 s' 发送给 Bob。

(4)Bob 计算 $s=as'-c \bmod q$,并将 (r,s) 作为 Alice 对消息 m 的签名。

签名方程为:$rmx=k+s \bmod q$。

2.2 正确性证明

通过上述盲签名协议得到的 (r,s) 为 Alice 对消息 m 的有效签名。证明过程如下:

$rmx=k+s \bmod q \Leftrightarrow rmx=k'a+bx+c+s \bmod q \Leftrightarrow (rm-b)x=k'a+s+c \bmod q \Leftrightarrow a^{-1}(rm-b)x=k'+a^{-1}(s+c) \bmod q \Leftrightarrow a^{-1}r'^{-1}(rm-b)r'x=k'+a^{-1}(s+c) \bmod q \Leftrightarrow m'r'x=k'+s' \bmod q$

2.3 原强盲性证明

原文献对该方案的强盲性证明如下:在该方案中 Alice 观察到的信息为 $\Sigma'=(k',m',r',s')$,Bob 得到的消息签名对为 (m,r,s),a,b,c 为随机盲化参数。若 Alice 在签名时存贮 $\Sigma'=(k',m',r',s')$,待 Bob 公开 (m,r,s) 后,Alice 可以根据:

$$s=as'-c \bmod q$$

$$m'=a^{-1}r'^{-1}(rm-b) \bmod q$$

$$r=(R'^a y^b g^c \bmod p) \bmod q$$

求解 a、b、c,从而 Alice 可以找出 (m',r',s') 和 (m,r,s) 的联系。但从这 3 个方程不难知道 Alice 解出 a、b、c 必须计算离散对数。因此在难于计算离散对数的前提之下,该方案是一个强盲签名方案。

2.4 原强盲性证明中存在的问题

设 Alice 在某次盲签名过程中记录下所有的观测数据 $U=(k',m',R',r',s')$。之后 Bob 公开了一个有效消息签名对 $sig(m)=(r,s)$。若要找到一组盲化参数 (a,b,c),使得可以重构原盲签名过程,或者说使得 U 和 $sig(m)=(r,s)$ 相联系,就要找到一组 (a,b,c) 使得下列方程组成立:

$$\begin{cases} r=(R'^a y^b g^c \bmod p) \bmod q \\ m'=a^{-1}r'^{-1}(rm-b) \bmod q \\ s=as'-c \bmod q \end{cases} \quad (1)$$

当 Bob 公开签名 $sig(m)=(r,s)$ 后,Alice 可根据签名等式 $mrx=k+s \bmod q$ 求得 $k=mrx-s \bmod q$,并且满足 $r=(g^k \bmod p) \bmod q$(因为 $sig(m)=(r,s)$ 是个有效签名)。由于 $k=k'a+bx+c \bmod q \Rightarrow r=(R'^a y^b g^c \bmod p) \bmod q$,所以:

$$\begin{cases} k=k'a+bx+c \bmod q \\ m'=a^{-1}r'^{-1}(rm-b) \bmod q \\ s=as'-c \bmod q \end{cases} \Rightarrow \text{方程组(1)} \quad (2)$$

因此只要找到一组盲化参数 (a,b,c),使得方程组(2)成立,就能够重构原盲签名过程。而要从方程组(2)中解出 a、b、c 并不需要解离散对数问题,因此原论述中用于证明强盲性的"基于离散对数难题"的依赖条件是不成立的。

重新给出上述方案的强盲性证明。

2.5 强盲性的重新证明

证明如下定理:

定理 1 设 $U=(k',m',R',r',s')$ 为 Alice 在某次盲签名协议中所记录下来的观测值,对于任意的一个合法的消息签名对 $sig(m)=(r,s)$,都存在若干组解 (a,b,c),使得方程组(2)成立,也即使得 U 和 $sig(m)=(r,s)$ 相联系。

证明 求解方程组:

$$\begin{cases} m'=a^{-1}r'^{-1}(rm-b) \bmod q \\ s=as'-c \bmod q \end{cases} \quad (3)$$

解得:

$$\begin{cases} b=rm-m'ar' \bmod q \\ c=as'-s \bmod q \\ a \text{ 为自由变量} \end{cases} \quad (4)$$

将所得解代入,得:$k'a+bx+c=k'a+(rm-m'ar')x+(as'-s)=k'a+rmx-m'ar'x+as'-s=(k'+s'm'r'x)a+(rmx-s)=rmx-s=k \bmod q$。所以方程组(3)$\Leftrightarrow$方程组(2)

因此解空间(4)也是方程组(2)的解。又由于方程组(2)$\Rightarrow$方程组(1)所以方程组(4)中的任何一个特解都可用来重构原盲签名过程。证毕。

既然任意的一个合法签名 $sig(m)=(r,s)$ 都能找到随机盲化参数 (a,b,c),使得其盲签名过程得以重构。因此 Alice 无法确定 $sig(m)=(r,s)$ 是否为从 $U=(k',m',R',r',s')$ 构造而来的盲签名结果,从而不能对盲签名进行追踪,因而该签名方案具有强盲性。

3 二元随机盲化参数构造盲签名

文献[7]按照姚亦峰的方法引入二元随机盲化参数构造了基于广义 ELGamal 签名的盲签名方案,并声明它们为弱盲签名方案。下面以其中的一个方案(原文中的第 3 个方案)为例,证明该方案不是弱盲签名方案,而是强盲签名方案。

3.1 方案简述

系统参数:p 是一个大素数,g 是 Z_p^* 上的本原元。Alice 为签名者,Bob 为消息拥有者。Alice 的私钥为 $x \in Z_p$,公钥为 $y=g^x \bmod p$。盲签名的过程如下:

(1)Alice 随机选择 $k' \in Z_p$,计算 $r'=g^{k'} \bmod p$,将 r' 发送给 Bob。

(2)Bob 随机选择 $a,b \in Z_p$,计算 $r=r'^a g'^b \bmod p$,$m'=ar'^{-1}m \bmod p-1$,将 m' 发送给 Alice。

(3)Alice 对消息 m' 签名,即计算 s',满足 $r'x=m'k'+s' \bmod p-1$,将 s' 发送给 Bob。

(4)Bob 计算 $s=r\,r'^{-1}s'-bm \bmod p-1$,并将$(r,s)$作为 Alice 对消息 m 的签名。

签名方程为:$rx=mk+s \bmod p-1$,验证方程为:$y^{r}=r^{m}g^{s} \bmod p$。

3.2　正确性证明(略)

3.3　原弱盲性证明

原文献对该方案的弱盲性证明如下:当消息拥有者 Bob 公开了 m 的签名(r,s)后,签名者 Alice 可求得 $a'=m'm^{-1}r\,r'^{-1}$,$b'=(r\,r'^{-1}s'-s)m^{-1}$,若满足 $r=r'^{a}g^{b} \bmod p$,则可确认 $a'=a,b'=b$,从而确认(r',s')与(r,s)相联系。

下面将重新证明该方案属于强盲签名方案。

3.4　重新证明方案的强盲性

设 Alice 在某次盲签名过程中记录下所有的观测数据 $U=(k',m',r',s')$。当 Bob 公开了一个有效签名结果 $sig(m)=(r,s)$后,Alice 可根据签名等式 $rx=mk+s \bmod p-1$ 求得 $k=m^{-1}(rx-s) \bmod p-1$,并且满足 $r=g^{k} \bmod p$。

若要找到一组盲化参数(a,b),使得能够重构原盲签名过程,即使得 U 和 $sig(m)=(r,s)$相联系,则要找到一组解(a,b)使得下列方程组成立:

$$\begin{cases} m'=ar^{-1}r'm \bmod p-1 \\ s=r\,r'^{-1}s'-bm \bmod p-1 \\ r=r'^{a}g^{b} \bmod p \end{cases} \tag{5}$$

由于 $r=r'^{a}g^{b} \bmod p \Leftrightarrow k=k'a+b \bmod p-1$,所以

$$\text{方程组(5)}\Leftrightarrow\begin{cases} m'=ar^{-1}r'm \bmod p-1 \\ s=r\,r'^{-1}s'-bm \bmod p-1 \\ k=k'^{a}+b \bmod p-1 \end{cases} \tag{6}$$

因此满足方程(6)的解(a,b)可用来重构原盲签名过程。将证明如下定理:

定理 2　设 $U=(k',m',r',s')$为 Alice 在某次盲签名协议中所记录下来的观测值,对于任意的一个合法的消息签名对 $sig(m)=(r,s)$,都存在一组解(a,b),可用来重构一个盲签名过程,即存在一组解(a,b)使得方程组(6)成立。

证明　求解方程组:

$$\begin{cases} m'=ar^{-1}r'm \bmod p-1 \\ s=r\,r'^{-1}s'-bm \bmod p-1 \end{cases} \tag{7}$$

解得:

$$\begin{cases} a=m'm^{-1}r\,r'^{-1} \bmod p-1 \\ b=(r\,r'^{-1}s'-s)m^{-1} \bmod p-1 \end{cases} \tag{8}$$

将该组解代入,得:

$$\begin{aligned} k'a+b&=k'm'm^{-1}r\,r'^{-1}+(r\,r'^{-1}s'-s)m^{-1}= \\ &k'm'm^{-1}r\,r'^{-1}+r\,r'^{-1}s'\,m^{-1}-sm^{-1}= \\ &m^{-1}r\,r'^{-1}(k'm'+s')-sm^{-1}=m^{-1}r\,r'^{-1}\,r'x-sm^{-1}= \\ &m^{-1}rx-sm^{-1}=m^{-1}(rx-s)=m^{-1}mk=k \bmod p-1 \end{aligned}$$

所以,方程组(7)$\Leftrightarrow$方程组(6),而解公式(8)也是方程组(6)的解,可用来重构一个盲签名过程。证毕。

由于任意合法签名 $sig(m)=(r,s)$都能存在一组(a,b),可用来重构一个盲签名过程。因此,当消息拥有者 Bob 公开了一个签名后,Alice 无法确认该签名是否是由 $U=(k',m',r',s')$构造而来的盲签名结果,从而不能对签名消息进行追踪,因而该签名方案具有强盲性。

4　数据实例

本章以实际的签名数据为例来证实本文的观点:在任何的一个合法消息签名对与某个特定的盲消息签名之间都存在一组盲因子,使得两者发生联系,得以重构一个盲签名过程。

本文 2.1 节的盲签名方案:设 $p=107,q=53,g=69$ 为 q 阶元,私钥为 $x=26$,公钥为 $y=69^{26} \bmod 107=41$。假设某次盲签名中,签名者记录下的盲签名数据为 $U=(m'=51,k'=17,R'=101,r'=48,s'=31)$,而消息接受者由此得到的消息签名对为$(m''=38,r''=8,s''=27)$,使用的盲因子为$(a'=3,b'=9,c'=13)$。假设另一个消息拥有者公开了从另一个盲签名过程得来的消息签名对$(m=36,r=22,s=38)$,则可按公式(4)令 $a=11$(a 也可取其他值从而得到其它解),计算 $b=rm-m'ar' \bmod q=46,c=as'-s \bmod q=38$,可以验证$(a=11,b=46,c=38)$可用来重构一个盲签名过程,使得 U 和一个原本无关的$(m=36,r=22,s=38)$相联系。而在求解的过程中并不需要面对离散对数的难题。

本文 3.1 节中的盲签名方案:设 $p=47,g=39$ 为 Z_p^* 上的本原元,私钥为 $x=16$,公钥为 $y=39^{16} \bmod 47=4$。假设某次盲签名中,签名者记录下的盲签名数据为 $U=(m'=21,k'=35,r'=33,s'=23)$。假设有另一合法的消息签名对$(m=15,r=21,s=20)$,它并不是从上述盲签名产生而来的。按公式(8)计算得到 $a=m'm^{-1}r\,r'^{-1} \bmod p-1=31$,$b=(r\,r'^{-1}s'-s)m^{-1} \bmod p-1=37$。可以验证这组盲化参数$(a=31,b=37)$可用来重构一个盲签名过程,即使得 U 和$(m=15,r=21,s=20)$相联系,而它们原本是无关的两个签名。

5　结论

本文分析了关于离散对数问题构造盲签名方案的一些文献在对盲签名的强弱性分析方面存在的问题和错误,以其中的两个盲签名方案实例证明了以姚亦峰的二元仿射变换为构造思想,引入三元随机参数或是二元随机参数得到的盲签名方案均为强盲签名方案。本文只列举了两个实例进行证明,而上述文献中其他的一些盲签名实例的强弱性可做类似的证明。

参考文献:

[1] Chaum D.Blind signature for untraceable payments[C]//Advances in Cryptology-Crypto'82.New York:Springer-Verlag,1983:199-203.

[2] Chamenisch J,Piveteau J M,Stadler M A.Blind Signatures Based on the Discrete Logarithm Promblem[C]//Eurocrypt'94,1995:428-432.

[3] Harn L.Cryptanalysis of the blind signature based on the discrete logarithm problem[J].Electronic Letters,1995,31(14):1136-1137.

[4] 姚亦峰,朱华飞,陈抗生.基于二元仿射变换的广义 ELGamal 型盲签名方案[J].电子学报,2000,28(7):128-129.

[5] 姚亦峰,蒋兴浩,刘小红,等.两个基于离散对数的盲签名方案[J].计算机工程与应用,2001,37(9):106-107.

[6] 杜伟章,陈克非.基于二元仿射变换构造强盲签名方案[J].通信学报,2003,12.

[7] 赵泽茂,刘凤玉.广义 ELGamal 型弱盲签名的构造方法[J].计算机工程与设计,2004,12.