弱盲签名方案的构造的一种新方法*)

杜伟章[1,2] 陈克非[1]

(上海交通大学计算机科学与工程系 上海200030)[1] (长沙交通学院计算机工程系 长沙410076)[2]

A New Method of Constructing Weak Blind Digital Signature Schemes

DU Wei-Zhang[1,2] CHEN Ke-Fei[1]

(Dept. of Computer Science & Engineering, Shanghai Jiaotong University, Shanghai 200030)[1]

(Dept. of Computer Engineering, Changsha Communications University, Changsha 410076)[2]

Abstract In this paper, by integrating blind parameter digital signature schemes and the existing weak blind digital signature schemes, on the basis of generalized ElGamal type digital signature schemes, we construct some new weak blind digital signature schemes based on discrete logarithms. We check and analyze these digital signature schemes also.

Keywords Discrete logarithms, Blind parameter signature, Weak blind signature

1 引言

盲签名的概念首先由 D. Chaum[1]于1982年提出。在此之后，人们做了许多努力去构造各种盲签名方案，并将盲签名技术应用于电子货币和电子投票等许多安全应用系统。由于盲签名在各种实际应用中所发挥的重要作用，越来越受到人们的关注。按照对不同参数的盲化以及盲化的强度，祁明在文[2]中将盲签名方案分为如下三类：

(1)盲参数签名方案：签名者知道所签署的消息 m 的具体内容。按协议的设计，签名收方可改变原签名参数，即改变 $sig(m)$ 得到新的签名，但不影响对新签名的认证。所以，签名者虽签了名，但不知或不全知新签名的具体内容。

(2)弱盲签名方案：签名者仅知盲消息 $\overline{m}$ 的签名 $sig(\overline{m})$ 而不知 $sig(m)$，这里 $sig(m)$ 是签名收方利用 $sig(\overline{m})$ 所求得。如果签名者存储 $sig(\overline{m})$ 或其它有关数据，待 $sig(m)$ 公开后，签名者可以找到 $sig(\overline{m})$ 和 $sig(m)$ 的内在联系，从而达到对消息 m 拥有者的跟踪。弱盲签名的一种特殊情况为盲消息签名，在盲消息签名方案中，签名者仅对盲消息 $\overline{m}$ 签名，并不知真实消息 m 的具体内容。这类签名方案的特征是：$sig(m)=sig(\overline{m})$ 或 $sig(m)$ 含 $sig(\overline{m})$ 中的部分数据。因此，只要签名者保留关于盲消息 $\overline{m}$ 的签名，便可确认自己关于 m 的签名。

(3)强盲签名方案：签名者无法将 $sig(\overline{m})$ 和 $sig(m)$ 进行联系。这类盲签名可用于电子货币和电子投票等密码协议的设计。

姚亦峰在广义 ElGamal 签名方案[3]的基础上，在文[4]中基于二元仿射变换构造了两个强盲签名方案，当二元仿射变换的三个参数中某一个取为零，得到的盲签名方案为弱盲签名方案。本文结合盲参数签名方案与已有的弱盲签名方案的构造方法，构造出一些新的弱盲签名方案。

2 方案的构造

J. Camenisch 在文[5]中基于离散对数还构造了如下盲参数签名方案，在此方案中，p 是一个大素数，α 是 $GF(p)$ 中的本原元，签名者 Bob 的秘密钥为 x，$x\in[1,p-1]$，公钥为 $y=\alpha^x \bmod p$：

Alice　　Bob

选择 $m\in[1,p-1]$，随机数 $h\in z_{p-1}^*$，计算

$\beta=\alpha^h \bmod p$　　$\xrightarrow{(m,\beta)}$　　选择随机数 $k\in z_{p-1}^*$，计算 $r'=\beta^k \bmod p$，

$\xleftarrow{(r',s')}$　　$s'=k^{-1}\cdot(m+xr')\bmod p-1$

新签名 $sig(m)=(r,s)$，

其中 $r=r'$，

$s=s'h^{-1} \bmod p-1$

验证方程：

$r'=\alpha^m\cdot y^r \bmod p$

下面结合盲参数签名方案与已有的弱盲签名方案的构造方法，基于离散对数构造出一些新的弱盲签名方案。

方案1

Alice　　Bob

选随机数 $h\in z_{p-1}^*$，计算

$\beta=\alpha^h \bmod p$

$\xrightarrow{\beta}$　　选随机数 $k\in z_{p-1}^*$，计算 $r'=\beta^k \bmod p$

选随机数 $a\in z_{p-1}^*$，计算　　$\xleftarrow{r'}$

$r=r'^a \bmod p$，

$m'=m\cdot r'\cdot r^{-1} \bmod p-1$

$\xrightarrow{m'}$　　计算 $s'=k^{-1}\cdot(m'x-r') \bmod p-1$

$s=a^{-1}\cdot h^{-1}\cdot r\cdot r'^{-1}\cdot s' \bmod p-1$　　$\xleftarrow{s'}$

$sig(m)=(r,s)$

验证方程：$y^m=r^r\cdot\alpha^r \bmod p$

签名的验证：

由 $s'=k^{-1}\cdot(m'x-r') \bmod p-1$，得

$x=m'^{-1}\cdot(s'k+r') \bmod p-1$　　(1)

若 $y^m=r^r\cdot\alpha^r \bmod p$ 成立，则 $y^m=(\alpha^{ahk})^s\cdot\alpha^r \bmod p$，

即 $\alpha^{mx}=(\alpha^{ahk})^s\cdot\alpha^r \bmod p$，由此可得

$mx=sahk+r \bmod p-1$　　(2)

*)国家自然科学基金(60273049)和国家自然科学基金重大研究计划项目(90104005)资助课题。杜伟章　副教授，博士后，研究方向为通信与密码学。陈克非　博士导师，教授，主要研究方向为密码理论与技术，网络与信息安全。

将(1)式代入(2)式中,得

$m\cdot m'^{-1}\cdot(s'k+r')=sahk+r \bmod p-1$

比较 k 前面的系数和常数项,可得

$$\begin{cases} m\cdot m'^{-1}\cdot s'=sah \bmod p-1 \\ m\cdot m'^{-1}\cdot r'=r \bmod p-1 \end{cases}$$,这样

$$\begin{cases} r\cdot r'^{-1}\cdot s'=sah \bmod p-1 \\ m\cdot m'^{-1}\cdot r'=r \bmod p-1 \end{cases}$$

所以 $$\begin{cases} s=a^{-1}\cdot h^{-1}\cdot r\cdot r'^{-1}\cdot s' \bmod p-1 \\ m'=m\cdot r'\cdot r^{-1} \bmod p-1 \end{cases}$$

上述过程逆推,即得 $y^m=r'\cdot\alpha^{r'} \bmod p$ 成立。

方案的分析:

在上述盲签名方案中,如果签名者保留(m',r',s',β,k),则当 Alice 公开 sig(m)=(r,s)后,Bob 由 $s=a^{-1}\cdot h^{-1}\cdot r\cdot r'^{-1}\cdot s' \bmod p-1$可求得$(ah)'=s^{-1}\cdot r\cdot r'^{-1}\cdot s' \bmod p-1$。为了证实 sig(m)=(r,s)是从 sig$(m')=(m',r',s')$所求得,Bob 只需验证等式 $r=(\alpha^h)^{(ah)'} \bmod p$ 是否成立,若成立,则可确认 sig(m)和 sig(m')相对应。这说明上述方案是一个弱盲签名方案。

方案2

Alice　　Bob

选随机数 $h\in z_{p-1}^*$,计算

$\beta=\alpha^h \bmod p$

$\xrightarrow{\beta}$　选随机数 $k\in z_{p-1}^*$,计算

$r'=\beta^k \bmod p$

选随机数 $a\in z_{p-1}^*$,计算 $\xleftarrow{r'}$

$r=r'^a \bmod p$,

$m'=m\cdot r^{-1}\cdot r' \bmod p-1$

$\xrightarrow{m'}$　计算

$s'=k^{-1}\cdot(r'x-m') \bmod p-1$

$s=a^{-1}\cdot h^{-1}\cdot r\cdot r'^{-1}\cdot s' \bmod p-1$ $\xleftarrow{s'}$

sig$(m)=(r,s)$

验证方程:$y^r=r'\cdot\alpha^m \bmod p$

方案3

Alice　　Bob

选随机数 $h\in z_{p-1}^*$,计算

$\beta=\alpha^h \bmod p$

$\xrightarrow{\beta}$　选随机数 $k\in z_{p-1}^*$,计算

$r'=\beta^k \bmod p$

选随机数 $a\in z_{p-1}^*$,计算 $\xleftarrow{r'}$

$r=r'^a \bmod p$,

$m'=r'^{-1}\cdot rm \bmod p-1$

$\xrightarrow{m'}$　计算

$s'=k^{-1}\cdot(x-r'm') \bmod p-1$

$s=a^{-1}\cdot h^{-1}\cdot s' \bmod p-1$ $\xleftarrow{s'}$

sig$(m)=(r,s)$

验证方程:$y=r'\cdot\alpha^{r'm} \bmod p$

方案4

Alice　　Bob

选随机数 $h\in z_{p-1}^*$,计算

$\beta=\alpha^h \bmod p$

$\xrightarrow{\beta}$　选随机数 $k\in z_{p-1}^*$,计算

$r'=\beta^k \bmod p$

选随机数 $a\in z_{p-1}^*$,计算 $\xleftarrow{r'}$

$r=r'^a \bmod p$,

$m'=rm\cdot r'^{-1} \bmod p-1$

$\xrightarrow{m'}$计算

$s'=k^{-1}\cdot(r'm'x-1) \bmod p-1$

$\xleftarrow{s'}$

$s=a^{-1}\cdot h^{-1}\cdot s' \bmod p-1$

sig$(m)=(r,s)$

验证方程:

$y^{r'm}=r'^r\cdot\alpha \bmod p$

方案5

Alice　　Bob

选随机数 $h\in z_{p-1}^*$,计算

$\beta=\alpha^h \bmod p$

$\xrightarrow{\beta}$　选随机数 $k\in z_{p-1}^*$,计算

$r'=\beta^k \bmod p$

选随机数 $a\in z_{p-1}^*$,计算 $\xleftarrow{r'}$

$r=r'^a \bmod p$,

$m'=r+m-r' \bmod p-1$

$\xrightarrow{m'}$　计算

$s'=k^{-1}\cdot(x-r'-m') \bmod p-1$

$s=a^{-1}\cdot h^{-1}\cdot s' \bmod p-1$ $\xleftarrow{s'}$

sig$(m)=(r,s)$

验证方程:

$y=r'\cdot\alpha^{r'+m} \bmod p$

方案6

Alice　　Bob

选随机数 $h\in z_{p-1}^*$,计算

$\beta=\alpha^h \bmod p$

$\xrightarrow{\beta}$　选随机数 $k\in z_{p-1}^*$,计算

$r'=\beta^k \bmod p$

选随机数 $a\in z_{p-1}^*$,计算 $\xleftarrow{r'}$

$r=r'^a \bmod p$,

$m'=r+m-r' \bmod p-1$

$\xrightarrow{m'}$　计算

$s'=k^{-1}\cdot[(r'+m')x-1] \bmod p-1$

$s=a^{-1}\cdot h^{-1}\cdot s' \bmod p-1$ $\xleftarrow{s'}$

sig$(m)=(r,s)$

验证方程:

$y^{r'+m}=r'\cdot\alpha \bmod p$

仿照方案1的检验和分析方法,可对方案2-6进行检验和分析。

参 考 文 献

1 Chaum D. Blind signatures for untraceable payments. Advances in Cryptology-Crypto'82, New York: Plenum Press, 1983. 199～203

2 祁明,张凌. 盲参数签名及其应用. 计算机工程与应用,2001(14):33～34,57

3 Harn L, Xu Y. Design of generalized ElGamal type digital signature schemes based on discrete logarithm. Electronics Letters, 1994, 30(24): 2025～2026

4 姚亦峰,蒋兴浩,刘小红,陈抗生. 两个基于离散对数的盲签名方案. 计算机工程与应用,2001(9):106～107

5 Camenisch J, Piveteau J-M, Stadler M. Blind signature based on the discrete logarithm problem. Advances in Cryptology-Eurocrypt'94, Springer-Verlag, 1995. 428～432