基于离散对数的代理盲签名

李方伟，谭利平，邱成刚

(重庆邮电大学移动通信重点实验室 重庆 南岸区 400065)

【摘要】针对文献[4]中代理盲签名方案的缺陷，提出了一种改进的新方案。该方案在代理授权过程中克服了代理签名密钥的可伪造因素，使其安全性等价于解离散对数难题；在盲签名过程中通过引入三个随机数构造了强盲签名。与原方案相比，新方案在真正意义上实现了电子交易中的强不可伪造性和不可链接性，保护了代理签名人的利益和代理交易内容的私密性，有效地防止了交易双方事后抵赖。

关 键 词 离散对数； 代理盲签名； 强不可伪造性； 不可链接性

中图分类号 TN918 **文献标识码** A

A Proxy Blind Signature Scheme Based on DLP

LI Fang-wei, TAN Li-ping, and QIU Cheng-gang

(Key Lab of Mobile Communication Technology, Chongqing University of Posts and Telecommunications Nan'an Chongqing 400065)

Abstract Aiming at the drawbacks of proxy blind signature scheme, we propose a new improved proxy blind signature scheme to overcome the forgery factors. In the blind signature, a strong blind signature is constructed with three random factors. It has really completed unforgeablity and unlinkability in the electronic tractions of business in contrast against the previous ones.

Key words discrete logarithm problem; proxy blind signature; unforgeablity; unlinkability

在电子交易系统中签名授权人(消费者)常常不希望代理签名者(如银行)能将签署的某则消息(用户可以使用的有效电子货币)和某个具体的支付行为联系起来，这样能保证用户的隐私。因此，文献[1]将代理签名和盲签名相结合提出了代理盲签名的概念。文献[2]提出了一种基于Schnor代理盲签名方案。文献[3]指出文献[2]的方案不满足不可伪造性和不可链接性，但并没有给出一个改进的安全的方案。文献[4]提出了一个改进的安全有效的方案，与以前的方案相比，该方案更加安全有效，不再需要安全信道。同时克服了可伪造性和可链接性的缺陷，并把它应用到了电子选举中。

本文对文献[4]的方案进行了安全性分析，该方案不需要安全信道，比原方案有效。然而该方案并不满足强不可伪造性和不可链接性，任何人都可以伪造代理签名人的密钥，从而冒充代理签名者产生有效的签名。同时，代理签名者也可以跟踪签名。为此，本文设计了一种改进的代理盲签名方案，具有强不可伪造性和不可链接性，从根本上保障了代理签名者的合法权益，实现了盲签名的匿名性和不可跟踪性[5]，可将其应用在电子现金系统和电子支付系统中。

1 文献[4]的代理盲签名方案分析

1.1 文献[4]的代理盲签名方案

设待签名的消息为m；安全参数 p、q为两个大素数，且$q|(p-1)$；g为GF(q)的本原元；h为一个安全的单向Hash函数；||表示比特串并；A为原始签名人，B为代理签名人，C为代理签名接收人；$x_A, x_B, x_C \in [1, p-1]$分别为$A$、$B$、$C$的私钥；相应的公钥分别为：$y_A = g^{x_A} \bmod p$， $y_B = g^{x_B} \bmod p$和 $y_C = g^{x_C} \bmod p$。

代理授权过程如下：

(1) 原始签名人A随机选择$k_A \in Z_q^*$，计算$r_A = g^{k_A} \bmod p$， $s_A = x_A + k_A y_B \bmod q$，并将$(r_A, s_A)$发送给代理签名人$B$。

(2) B检验 $g^{s_A} = y_A r_A^{y_B} \bmod p$，如果等式成立，$B$则接受$(r_A, s_A)$，并计算代理签名私钥 $x_p = s_A + x_B y_A \bmod q$，相应的代理签名公钥为 $y_p = g^{x_p} =$

收稿日期：2006 – 10 – 09；修回日期：2007 – 03 – 15
基金项目：重庆市教委科学技术研究项目(KJ060510)；重庆市科委自然科学基金(2007BB2388)
作者简介：李方伟(1960 –)，男，博士，教授，主要从事移动通信技术方面的研究.

$g^{s_A}y_B^{y_A}=y_Ar_A^{y_B}y_B^{y_A}\bmod p$。接收者可以通过$A$、$B$的公钥$y_A$、$y_B$以及公开信息$r_A$计算$y_{\mathrm{p}}$。

代理盲签名过程如下：

(1) B随机选取$k\in Z_q^*$，计算 $t=g^k\bmod p$，并把t发送给代理签名接收人C。

(2) C选择随机数a，$b\in Z_q^*$，进行以下计算：

$$r=tg^{a+x_C}y_{\mathrm{p}}^{-b}\bmod p$$
$$e=h(r\,\|\,m)\bmod q$$
$$e'=e+b\bmod q$$

把e'发给B。

(3) B接收到e'，计算$s'=k-e'x_{\mathrm{p}}\bmod q$，并发送$s'$给$C$。

(4) C利用接收到的s'计算$s=s'+a\bmod q$，(m，s，e)就是一个有效的代理盲签名。

代理盲签名的验证过程为：验证者接收到(m，s，e)之后，验证$e=h(g^sy_{\mathrm{p}}^ey_C\,\|\,m)\bmod q$。如果等式成立则接受，否则拒绝。

1.2　文献[4]的方案分析

文献[4]指出该方案满足不可伪造性和不可链接性。通过分析，发现并非如此。

(1) 不可伪造性

该方案如果原始签名人A想伪造代理签名，就必须拥有一个代理盲签名密钥对(x_{p}，y_{p})。由验证方程$y_{\mathrm{p}}=y_Ar_A^{y_B}y_B^{y_A}$可以看出，只要构造一对($x_{\mathrm{p}}$，$r_A$)满足上式即可。原始签名人$A$在不知道$x_B$的情况下，只需要$r_A$里构造一个因子$h$满足$h^{y_B}=y_B^{-y_A}\bmod p$，不需要解离散对数，很容易解出$h=y_B^{-y_Ay_B^{-1}}\bmod p$。因此原始签名人可以伪造成功。

同理，没有被授权的B也可以构造满足条件的r_A，在文献[6]中有详细的分析和伪造方案。

(2) 不可链接性

当有效的代理盲签名(m, s, e)被公开后，代理签名者B根据自己的(t，s'，e')可以计算$a=s-s'$，$b=e'-e$和$r=g^sy_{\mathrm{p}}^ey_C$，验证等式$r=tg^{a+x_C}y_{\mathrm{p}}^{-b}$。若相等则说明此盲签名是$B$所签，否则不是$B$所签。$B$虽然不知道$C$的密钥$x_C$，但是可以验证等式$r=tg^{a+x_C}y_{\mathrm{p}}^{-b}=tg^ay_Cy_{\mathrm{p}}^{-b}$。因此，该方案具有可链接性。

2　改进的方案与安全性分析

2.1　方案描述

参数设置和原方案相同。

代理授权过程如下：

(1) 原始签名人A随机选择$k_A\in Z_q^*$，计算$r_A=g^{k_A}\bmod p$，$s_A=x_Ar_A+k_Ay_B\bmod q$，并将(r_A，s_A)发送给代理签名人B。

(2) B检验$g^{s_A}=y_A^{r_A}r_A^{y_B}\bmod p$，如果等式成立，$B$则接受($r_A$，$s_A$)，并计算代理签名私钥$x_{\mathrm{p}}=s_A+x_Br_A\bmod q$，相应的代理签名公钥为$y_{\mathrm{p}}=g^{x_{\mathrm{p}}}=g^{s_A}y_B^{r_A}=y_A^{r_A}r_A^{y_B}y_B^{r_A}\bmod p$，接收者可以通过$A$、$B$的公钥$y_A$、$y_B$以及公开信息$r_A$计算$y_{\mathrm{p}}$。

代理盲签名过程如下：

(1) B随机选取$k\in Z_q^*$，计算 $t=g^k\bmod p$，并把t发送给代理签名接收人C。

(2) C选择随机数a，b，$u\in Z_q^*$，进行以下计算：

$$r=t^bg^ay_{\mathrm{p}}^{bu}\bmod p$$
$$e=h(r\,\|\,m)\bmod q$$
$$e'=\frac{e}{b}-u\bmod q$$

把e'发给B。

(3) B接收到e'，计算$s'=k-e'x_{\mathrm{p}}\bmod q$，并发送$s'$给$C$。

(4) C用接收到的s'计算$s=bs'+a\bmod q$，(m，s，e)就是一个有效的代理盲签名。

代理盲签名的验证过程为：验证者收到(m，s，e)之后，验证$e=h(g^sy_{\mathrm{p}}^e\bmod p\,\|\,m)\bmod p$，如果等式成立则接受，否则拒绝。

证明：

$$g^sy_{\mathrm{p}}^e\bmod p=g^{bs'+a}y_{\mathrm{p}}^e\bmod p=$$
$$g^{b(k-e'x_{\mathrm{p}})+a}y_{\mathrm{p}}^{(e'+u)b}\bmod p=$$
$$g^{bk+a}y_{\mathrm{p}}^{bu}\bmod p=$$
$$t^bg^ay_{\mathrm{p}}^{bu}\bmod p=r$$

2.2　安全性分析

(1) 原始签名人不可伪造代理签名人签名

代理签名公钥为$y_{\mathrm{p}}=y_A^{r_A}r_A^{y_B}y_B^{r_A}$，要构造满足上式的($x_{\mathrm{p}}$，$y_{\mathrm{p}}$)，关键是从公式中解出$r_A$。对于原始签名人在不知道$x_B$的情况下，求解$r_A$将面临求解离散对数问题，因此原始签名人不能伪造代理签名。

(2) 冒充原始签名人攻击

如果B没有被原始签名人A指定为代理签名者，即B在没有A的同意和指派的前提下想伪造出有效的密钥对(x_{p}，y_{p})，由于不知道x_A求解r_A，同样面临求解离散对数问题。所以，该方案可以防止冒充原始签名人的攻击。

(3) 具有不可链接性

在签名被签名接收者泄漏后，代理签名者B也不能将签名(m, s, e)和(t, s', e')联系起来，因此代理盲签名具有不可链接性。

(4) 不可抵赖性

综合(1)～(2)，除了代理签名人B以外，任何人都不能伪造B的代理签名，所以B不能否认其代理签名。

(5) 代理签名的可区别性

在签名验证阶段使用了不同的等式来验证原始签名和代理签名的有效性，验证等式中含有A和B的公钥，任何人都可以很容易地将原始签名和代理签名区别开。

(6) 可注销性

如果原始签名人A想收回B的代理签名权，即注销B所拥有的代理签名私钥x_p，只需要宣布y_p不再有效，B所生成的代理签名就会随之失效。

3 新方案的特点

(1) 该方案中的盲签名是强盲签名，实现了不可链接性和参与者的匿名性。因为代理签名过程中引入了三个随机数a、b、u，代理签名人知道了(m, s, e)，并不能从$e' = \frac{e}{b} - u$和$s = b s' + a$两个方程中解出a、b、u，也就不能将(t, s', e')和(m, s, e)联系起来。

(2) 在$y_p = y_A^{r_A} r_A^{y_B} y_B^{r_A}$中$r_A$作了一次底数两次指数，任何人想从中解出$r_A$，都面临解离散对数难题。相比于原来的方案，该方案能抵抗强伪造攻击。即除了代理签名人B外任何人都不能产生有效的签名，避免了代理签名私钥生成过程的可伪造因素，保护了代理签名人利益。

4 结 束 语

代理盲签名是一种新的签名技术，是目前研究的热点与难点之一。它具有广泛的应用性，如在电子选举系统、电子支付[7]以及移动代理[8]中都涉及代理盲签名。所以，本文提出了一种改进的代理盲签名方案，其安全性基于离散对数难题，比原方案更加安全。该方案具有强不可伪造性和不可链接性，保护了代理签名人的利益，保证了代理交易内容的私密性，有效地防止了双方事后的抵赖。除此之外，该方案还满足代理盲签名的不可否认性、可验证性、可注销性、盲性等特性，是一个安全有效的代理盲签名方案，具有一定的应用价值。

参 考 文 献

[1] LIN W D, JAN J K. A security personal learning tools using a proxy blind signature scheme[C]//Proceedings of International Conference on Chinese Language Computing. Illinois, USA: [s. n.], 2000: 173-177.

[2] TAN Zuo-wen, LIU Zhuo-jun, TANG Chun-ming. A proxy blind signature scheme based on DLP[J]. Journal of Software, 2003, 14(11): 1931-1935.

[3] SUN H, HSIEH B. On the security of some proxy blind signature schemes[C]//Australasian Information Security Workshop (AISW2004). New Zealand: Dunedin, 2004: 75-78.

[4] WANG Shao-bin, HONG Fan, CUI Guo-hua. Secure efficient proxy blind signature schemes based DLP[C]// Proceedings of the Seventh IEEE International Conference on E-Commerce Technology (CEC'05). [S.l.]: IEEE, 2005: 452-455.

[5] CHAUM D. Blind signatures for untraceable payment[C]// Advances in Cryptology-Crypto'83 Proceedings. London: [s.n.], 1983: 199-203.

[6] 黄文平. 一些不需要安全通道代理签名的分析与改进[J]. 计算机工程与应用, 2005, 41(28): 127-130.

[7] 谷利泽, 张 胜, 扬义先. 代理盲签名方案及其在电子货币中的应用[J]. 计算机工程与应用, 2005, 31(16): 11-13.

[8] 吴 敏, 王汝传. 代理盲签名方案在基于移动代理的电子商务中的应用研究[J]. 南京邮电学院学报, 2005, 25(5): 84-88.

编 辑 税 红