一个新的多代理盲签名方案

毛卫霞,李志慧,柳 烨
MAO Wei-xia,LI Zhi-hui,LIU Ye

陕西师范大学 数学与信息科学学院,西安 710062
College of Mathematics and Information Science,Shaanxi Normal University,Xi'an 710062,China
E-mail:ccde456@163.com

MAO Wei-xia,LI Zhi-hui,LIU Ye.New multi-proxy blind signature scheme.Computer Engineering and Applications,2010,46(12):82-84.

Abstract: Multi-proxy blind signature is a special digital signature which satisfies the security properties of both the proxy signature and blind signature.It permits that an original signer authorizes a group of proxy signers who don't know the concrete content of the message.A new multi-proxy blind signature is proposed based on DLP.This scheme doesn't need security channel to transmit proxy cipher key,and has properities of unforgeability and unlinkability.

Key words: discrete logarithm problem;multi-proxy signature;blind signature;security channel;unforgeability;unlinkability

摘 要:多代理盲签名综合了多代理签名和盲签名的优点,是一种特殊的数字签名。它由一个原始签名人授权给一组代理签名人,并且这组代理签名人并不知道消息的具体内容。基于离散对数问题提出了一种新的多代理盲签名方案。该方案不需要安全信道传送代理密钥,且具有不可伪造性、不可链接性。

关键词:离散对数;多代理签名;盲签名;安全信道;不可伪造性;不可链接性
DOI:10.3778/j.issn.1002-8331.2010.12.022 **文章编号**:1002-8331(2010)12-0082-03 **文献标识码**:A **中图分类号**:TP309

1 引言

1983 年,Chaum 在文献[1]中首次提出了盲签名的概念。关于盲签名,Chaum 曾经给出一个非常直观的说明:所谓盲签名,就是先将隐蔽的文件放进信封里,而除去盲因子的过程就是打开这个信封。当文件在一个信封里时,任何人都不能读它。对文件签名就是通过在信封里放一张复写纸,签名者在信封上签名时,他的签名便透过复写纸签到文件上。

1996 年,Mambo、Usuda、Okamoto 在文献[2]中首次提出了代理签名体制。代理签名在电子商务、电子现金等方面有着广泛的应用,一经提出便受到广泛关注。如某经理由于出差、生病、资源限制等原因而不能签名,于是便将签名权委托给代理签名人,即他的秘书。

代理签名和盲签名有着各自的优点,有时需要同时用到它们。如在电子选举系统、电子支付以及移动代理中均有涉及。当代理权和用户的隐私权都需要的时候,代理盲签名是很好的选择。文献[3]提出了代理盲签名的概念。随后,各种各样的代理签名方案[4-5]被提出,如代理多重签名[6]、多代理签名、多级代理签名[7]、门限代理签名等。

多代理签名是指在一种代理签名方案中,一个原始签名人将签名权委托给一组代理签名人,只有他们合作才能对消息进行签名,它是(t,n)门限的一个特例。Hwang 等在文献[8]中首次提出了多代理签名,解决了多个代理人进行盲签名,有效阻止了代理签名人对签名权的滥用。文献[9]提出了一种基于双线性配对的多代理盲签名方案,但该方案并不能解决代理签名人对签名权的滥用。该文在文献[10]的单代理盲签名方案的基础上,提出了一种新的多代理盲签名方案。

2 代理盲签名方案回顾

2.1 系统初始化

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 为一个安全的单向哈希函数;$\|$ 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;$x_A,x_B\in[1,p-1]$分别为 A、B 的私钥,相应的公钥分别为:$y_A=g^{x_A}(\bmod p)$,$y_B=g^{x_B}(\bmod p)$。

2.2 代理授权阶段

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

(2)B 检验 $g^{s_A}=y_A^{r_A}r_A^{y_B}(\bmod p)$。若成立,$B$ 接受(r_A,s_A),并计

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.10571112,No.60873119);陕西省自然科学基础研究计划资助项目(No.2007A06)。

作者简介:毛卫霞(1983-),女,硕士研究生,主要研究领域为有限域,密码学;李志慧(1966-),通讯作者,女,博士,副教授,主要研究领域为有限域,密码学;柳烨(1982-),女,硕士研究生,主要研究领域为有限域,密码学。

收稿日期:2008-10-17 **修回日期**:2008-12-25

算代理签名私钥 $x_p=s_A+x_B r_A \pmod q$,相应的代理签名公钥 $y_p=g^{x_p}=g^{s_A}y_B^{r_A}=y_A^{r_A}r_A^{y_B}y_B^{r_A} \pmod p$,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_p。

2.3　代理盲签名阶段

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

(2)C 选取随机数 $a,b,u\in Z_q^*$,计算

$$r=t^b g^a y_p^{bu} \pmod p,\ e=h(r\parallel m) \pmod q,\ e'=\frac{e}{b}-u \pmod q$$

将 e' 发给 B。

(3)B 收到 e' 后,计算 $s'=k-e'x_p \pmod q$,将 s' 发给 C。

(4)C 收到 s' 后,计算 $s=bs'+a \pmod q$。

则 (m,s,e) 就是一个有效的代理盲签名。

2.4　代理盲签名验证阶段

签名接收人 C 收到 (m,s,e) 后,验证 $e=h(g^s y_p^e \bmod p\parallel m) \pmod q$ 是否成立。若等式成立,则接受签名,否则拒绝。

从这个方案可以看出,该签名具有不可伪造性、不可链接性,但它是一个单代理的盲签名方案,在实际应用的过程中会有一定的局限性,下面给出一种多代理盲签名方案。

3　新的多代理盲签名方案

3.1　系统初始化

(1)系统选取两个大素数 p 和 q,$q|(p-1)$;$g\in Z_p^*$,$o(g)=q$;h 为一个安全的单向哈希函数;$\parallel$ 表示比特串并。公布 p,q,g,h。

(2)原始签名人 A 随机选择 $x_A\in Z_q^*$,令 $y_A=g^{x_A} \pmod p$,x_A 为 A 的私钥,公布 y_A;再随机选取两个大素数 p_0 和 q_0,计算 $n_0=p_0q_0$,$\phi(n_0)=(p_0-1)(q_0-1)$;选取一个大整数 e,使得 $(e,\phi(n_0))=1$ 且 $ed=1 \pmod{\phi(n_0)}$;p_0,q_0,d 为私钥,公布 n_0,e;A 和 B_i 协商制定代理授权书 m_{w_i},其中包括 A 和 B_i 的标志代号,B_i 的代理期限和代理范围等,公布 m_{w_i}。

(3)设代理签名组 $B=\{B_1,B_2,\cdots,B_n\}$,密钥对 (x_{B_i},y_{B_i}),其中 $1\leqslant i\leqslant n$。B_i 随机选取 $x_{B_i}\in Z_q^*$,$y_{B_i}=g^{x_{B_i}} \pmod p$,$x_{B_i}$ 为 B_i 的私钥,公布 y_{B_i}。

3.2　多代理授权阶段

(1)A 计算 $\delta_i=y_{B_i}^{x_A} \pmod{n_0}$,$y_{\delta_i}=g^{\delta_i} \pmod{n_0}$,$t_i=(y_{B_i}^{\delta_i}\cdot y_A^{m_{w_i}})^d \pmod{n_0}$,将 t_i 发给 B_i,公布 y_{δ_i}。

(2)B_i 收到 t_i 后,计算 $\delta_i=y_A^{x_{B_i}} \pmod{n_0}$,然后验证 $t_i^e=y_{B_i}^{\delta_i}\cdot y_A^{m_{w_i}} \pmod{n_0}$ 是否成立。如果等式成立,B_i 接受代理并计算代理签名密钥 $s_{p_i}=y_A\delta_i+x_B h(m_{w_i},y_A) \pmod q$,$t_{p_i}=g^{s_{p_i}}=y_{\delta_i}^{y_A}y_{B_i}^{h(m_{w_i},y_A)} \pmod p$。私钥为 s_{p_i},B_i 将 t_{p_i} 发给 C。

3.3　多代理盲签名阶段

用户 C 收到 t_{p_i} 后,验证等式 $t_{p_i}=y_{\delta_i}^{y_A}y_{B_i}^{h(m_{w_i},y_A)} \pmod p$ 是否成立。若不成立,要求 B_i 重新发送。若成立,要求代理签名组 B 对消息 m 进行签名。

(1)C 首先计算 $t_p=\prod_{i=1}^{n}t_{p_i}$,并公布 t_p。

(2)B_i 随机选取 $k_i\in Z_q^*$,$u_i=g^{k_i} \pmod p$,将 u_i 发给 C。

(3)C 收到 u_i 后,计算 $u=\prod_{i=1}^{n}u_i$,并公布 u。再随机选取 $a_1,a_2,a_3\in Z_q^*$,计算

$$r=u^{a_2}g^{a_1}t_p^{a_2a_3} \pmod p,\ e=h(r\parallel m) \pmod q,\ e'=\frac{e}{a_2}-a_3 \pmod q$$

将 e' 发给 B_i。

(4)B_i 收到 e' 后,计算 $s_i'=k_i-e's_{p_i} \pmod q$,将 s_i' 发给 C。

(5)C 收到 s_i' 后,计算 $s_i=\sum_{i=1}^{n}s_i'$,$s=a_2s_i+a_1 \pmod q$。

则 (m,s,e) 为有效的多代理盲签名。

3.4　多代理盲签名验证阶段

用户 C 利用签名 (m,s,e),验证 $e=h(g^s t_p^e \bmod p\parallel m) \pmod q$ 是否成立。若等式成立,则接受签名,否则拒绝。

4　方案性能分析

4.1　正确性分析

定理 1　除了原始签名人 A,只有代理签名人 B_i 用自己的私钥 x_{B_i} 可以恢复 δ_i,且如果 $t_i^e=y_{B_i}^{\delta_i}\cdot y_A^{m_{w_i}} \pmod{n_0}$ 成立,则 A 就为真实的多代理授权者。

证明　由 $\delta_i=y_{B_i}^{x_A} \pmod{n_0}=(g^{x_{B_i}})^{x_A} \pmod{n_0}=(g^{x_A})^{x_{B_i}} \pmod{n_0}=y_A^{x_{B_i}} \pmod{n_0}$,$x_{B_i}$ 为 B_i 的私钥知,除了原始签名人 A 只有代理签名人 B_i 可以恢复 δ_i。又由 $t_i^e=[(y_{B_i}^{\delta_i}\cdot y_A^{m_{w_i}})^d]^e \pmod{n_0}=(y_{B_i}^{\delta_i}\cdot y_A^{m_{w_i}})^{ed} \pmod{n_0}$,而 $ed=1 \pmod{\phi(n_0)}$,且 d 由 A 保密,故 $t_i^e=y_{B_i}^{\delta_i}\cdot y_A^{m_{w_i}} \pmod{n_0}$。

因此,A 为真实的多代理授权者。

定理 2　(m,s,e) 是代理签名组 B 使用代理签名私钥 s_{p_i} $(1\leqslant i\leqslant n)$ 代表原始签名人 A 对消息 m 进行的多代理盲签名。

证明

$$g^s t_p^e \pmod p=g^{a_2s_i+a_1}t_p^e \pmod p=g^{a_2\sum_{i=1}^{n}s_i'+a_1}t_p^e \pmod p=$$

$$g^{a_2\left[\sum_{i=1}^{n}(k_i-e's_{p_i})\right]+a_1}t_p^e \pmod p=g^{a_2\sum_{i=1}^{n}k_i-a_2e'\sum_{i=1}^{n}s_{p_i}}g^{a_1}t_p^e \pmod p=$$

$$u^{a_2}t_p^{-a_2e'}g^{a_1}t_p^e \pmod p=u^{a_2}t_p^{-a_2e'}g^{a_1}t_p^{a_2(e'+a_3)} \pmod p=$$

$$u^{a_2}g^{a_1}t_p^{a_2a_3} \pmod p=r$$

故 $e=h(r\parallel m) \pmod q=h(g^s t_p^e \bmod p\parallel m) \pmod q$。

由 $s=a_2s_i+a_1 \pmod q$,$s_i=\sum_{i=1}^{n}s_i'$,$s_i'=k_i-e's_{p_i} \pmod q$ 可知,s_i 中含有每个 B_i 的私钥 s_{p_i},且由 $u=\prod_{i=1}^{n}u_i$,$r=u^{a_2}g^{a_1}t_p^{a_2a_3} \pmod p$,$e=h(r\parallel m) \pmod q$ 知,单个 B_i 或少于 n 个人均不能对消息进行签名,故实现了多代理。另外,由 $e=h(r\parallel m) \pmod q$ 可知,h 是安全的单向哈希函数,消息 m 对代理签名组 B 是不可见的,实现了盲签名。

因此,由以上证明可知,(m,s,e) 是代理签名组 B 使用代

理签名私钥 s_{p_i}($1\leqslant i\leqslant n$)代表原始签名人 A 对消息 m 进行的多代理盲签名。

4.2 安全性分析

(1)安全信道的分析

在多代理授权阶段,原始签名人 A 不需要安全信道传送代理密钥 δ_i。由定理 1 的证明可知,只有 A 和 B_i 知 δ_i,其他任何人均不能求出 δ_i。即使攻击者知道(t_i,m_{w_i}),但 m_{w_i} 中已明确指出 B_i 的标志代号,其他任何人获得代理信息(t_i,m_{w_i})是没有意义的,故可以实现公开授权。

(2)不可伪造性

假如攻击者想要伪造多代理盲签名,需要构造满足 $s_{p_i}=y_A\delta_i+x_{B_i}h(m_{w_i},y_A)(\bmod q)$,$t_{p_i}=y_{\delta_i}^{y_A}y_{B_i}^{h(m_{w_i},y_A)}(\bmod p)$这两个条件的($s_{p_i}$,$t_{p_i}$),而 s_{p_i} 中含有 δ_i 和 x_{B_i},只有 A 和 B_i 知 δ_i,x_{B_i} 为 B_i 的私钥,故 A 需知道每个 B_i 的私钥 x_{B_i} 才能伪造签名。另外,除了 A 和 B_i 外,攻击者想从 $y_{\delta_i}=g^{\delta_i}(\bmod n_0)$ 和 $t_i^e=y_{B_i}^{\delta_i}\cdot y_A^{m_{w_i}}(\bmod n_0)$ 中求出 δ_i 将面临离散对数问题,想从 $t_i=(y_{B_i}^{\delta_i}\cdot y_A^{m_{w_i}})^d(\bmod n_0)$ 中求出 δ_i 将面临求解 d 的大数分解问题和离散对数问题。因此,除了代理签名组 B 外,其他任何人均不能伪造签名。

(3)不可链接性

在用户 C 公布签名(m,s,e)后,即使 B_i($1\leqslant i\leqslant n$)保留每一次签名时的序对(e',s_i'),也不能从 $e'=\frac{e}{a_2}-a_3(\bmod q)$ 和 $s=a_2s_i+a_1(\bmod q)$ 中解出 a_1、a_2、a_3,因此不能把这个多代理盲签名与他们以前的某个签名联系起来考虑,从而由公开的签名识别出签名接受者的身份、被签署日期等信息,故方案具有不可链接性。

(4)不可否认性

由定理 1 和上面的不可伪造性的证明可知,A 不能否认其对 B 的授权,B 也不能否认对消息的多代理盲签名。

(5)多代理签名的可区分性

在 A 和 B_i 的身份验证阶段和签名验证阶段均使用了 A 和 B_i 的公钥,任何人都可以很容易区别原始签名和多代理签名。

(6)可注销性

如果原始签名人 A 想收回 B_i 的代理权,即注销 B_i 的代理签名私钥 s_{p_i},只需宣布 t_{p_i} 不再有效,B_i 产生的多代理签名就会随之无效。

(7)防滥用性

由定理 2 的证明可知,单个 B_i 或少于 n 个人均不能对消息进行签名,防止了某个 B_i 对签名权的滥用。

5 结束语

多代理盲签名在电子选举、电子商务中有着广泛的应用,它综合了多代理签名和盲签名的优点,具有很强的实用性。基于离散对数问题提出的新方案不需要安全信道传送代理密钥,并且具有不可伪造性、不可链接性、防滥用性,具有更高的安全性,实用性较强。同时可把离散对数问题具体化,考虑基于多项式或基于环上的多代理盲签名,其理论正处于研究过程中。

参考文献:

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

[2] Mambo M,Usuda K,Okamoto E.Proxy signatures:Delegation of the power to sign messages[J].IEICE Transactions on Fundamentals,1996,79(9):1338-1354.

[3] 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.

[4] Wang Shao-bin,Hong Fan,Cui Guo-hua.Secure efficient proxy blind signature schemes based DLP[C]//Proceedings of the Seventh IEEE International Conferenceon E-Commerce Technology CEC'05.[S.l.]:IEEE,2005:452-455.

[5] 谷利泽,张胜,杨义先.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.

[6] 胡振鹏,钱海峰,李志斌.一种高效的代理多重盲签名方案[J].计算机工程,2008,34(13):130-132.

[7] 胡江红,张建中.新的基于双线性对的多级强代理盲签名方案[J].计算机工程与应用,2007,43(18):123-125.

[8] Hwang S,Shi C.A simple multi-proxy signature scheme[C]//Proceeding of the Tenth International Conference on Information Security,2000:134-138.

[9] 王勇兵,姬龙涛,张建中.多代理盲签名方案的设计[J].云南师范大学学报,2008,28(1):71-103.

[10] 李方伟,谭利平,邱成刚.基于离散对数的代理盲签名[J].电子科技大学学报,2008,37(2):172-174.

(上接 81 页)

[4] Ye F,Luo H,Lu S,et al.Statistical en-route filtering of injected false data in sensor networks[C]//Proceedings of 23rd Annual Joint Conference of the IEEE Computer and Communications Societies,INFOCOM,2004:2446-2457.

[5] Ye F,Luo H,Lu S.Statistical en-route filtering of injected false data in sensor networks[J].IEEE Journal on Selected Areas in Communication,2005,23(4):732-744.

[6] 彭志娟,王汝传,王海艳.基于数字水印技术的无线传感器网络安全机制研究[J].南京邮电大学学报:自然科学版,2006,26(4):69-72.

[7] Zhang Wei,Das S,Liu Yong-he.A trust based framework for secure data aggregation in wireless sensor networks[C]//IEEE SECON 2006,September 2006:60-69.

[8] Yao Zhi-ying,Kim D,Doh Y.PLUS:Parameterized and localized trust management scheme for sensor networks security[C]//IEEE Proceedings of MASS 2006,October 2006:437-446.

[9] Han Guang-jie,Choi D,Lim W.A novel sensor node selection method based on trust for wireless sensor networks[C]//International Conference on Wireless Communications,Networking and Mobile Computing,Wicom 2007,2007:2397-2400.