文章编号:1673-9469(2009)02-0106-03

一个代理盲签名方案的进一步改进

成 林,王国骋,亢保元
(中南大学 数学科学与计算技术学院,湖南 长沙 410075)

摘要:文献[7]中给出了一个改进的代理盲签名方案,然而李方伟等人对WANG等人方案的链接性的攻击是错误的;在对李方伟等人的方案进行了分析之后提出了一个改进的方案,并对改进后的方案进行了相应的安全性分析和计算效率分析,结论是改进后的方案与原有的方案相比是一个更为安全高效的代理盲签名方案。

关键词:离散对数;代理盲签名;不可伪造性;不可链接性
中图分类号:TP391 **文献标识码**:A

Improvement of a proxy blind signature scheme

CHENG Lin, WANG Guo-zhan, KANG Bao-yuan
(School of Mathematical Science and Computing Technology, Central South University, Changsha 41007, China)

Abstract: Recently, Li Fang-wei *et al*. presented forgeability and linkability attacks on WANG *et al*'s proxy blind signature scheme and improved WANG *et al*'s scheme, unfortunately LI *et al*'s linkability attack is failed and the scheme still satisfies the unlinkability property; LI *et al*' s proxy blind signature scheme is analysised and impvroved, the new proxy blind signature scheme is of more security and higher efficiency.

Key words: discrete logrithm; proxy blind signature; unforgeability; unlinkability

盲签名[1]是由D.Chaum在1983年首先提出的,它使得请求者能够得到签名人的签名,却不让签名人知道实际被签消息的具体内容,签名人也不能将签名过程与最终签名结果对应起来,盲签名的这种性质称为盲性,它在诸如电子现金,电子选举等场合具有广泛的应用。1996年Mambo、Usuda、Okamoto提出了代理签名[2]的概念,它是指原始签名者把他的签名权授给代理者,代理者代表原始签名者行使他的签名权。代理签名和盲签名有着各自的特点,然而在某些情形下可能需要同时应用他们。在2000年,LIN和JAN结合代理签名和盲签名第一个提出了代理盲签名方案[3]。一个安全的代理盲签名一般要同时拥有代理签名和盲签名的特点,具有不可伪造性、不可链接性、可区分性、不可抵赖性、可注销性,防止滥用代理权等性质。2003年TAN等人在Schnor盲签名的基础上,结合代理签名提出了一种基于离散对数问题的代理盲签名方案[4];SUN[5]等人指出TAN等人的方案不满足不可伪造性和不可链接性,但没有给出一个改进的安全的方案;2005年WANG等人提出了一个改进的方案[6];2008年LI等人指出WANG等人的方案不满足不可伪造性和不可链接性,并给出了一个改进的代理盲签名方案[7]。本文首先对WANG等人的方案的不可链接性进行了分析,分析认为LI等人对WANG等人方案的链接性的分析是错误的,WANG等人方案满足不可链接性;其次对LI等人的方案进行了改进,并进行了相应的安全性分析和计算效率分析。

1 对文献[6]方案的链接性分析

在2008年LI等人指出在WANG等人的方案中,代理签名者可以根据保留的信息和最终的签名对应起来,因此指出WANG等人的方案不具有

收稿日期:2008-12-04
作者简介:成林(1983-),男,河北邢台人,硕士,从事密码学的研究。

不可链接性。具体过程如下:

当有效的代理盲签名(m,s,e)被公布后,代理签名者 B 根据自己的保留的信息(t_i,s'_i,e'_i),代理签名者 B 可以计算 $a_i=s-s'_i \bmod q$, $b_i=e'_i-e \bmod q$, $r_i=t_i g^{a_i+x_c} y_p^{-b_i} \bmod p$ 和 $r=g^S y_p^e y_C \bmod p$,然后代理签名者 B 可以验证等式 $r_i=r$,若等式成立,则说明盲签名是 B 所签,该方案具有可链接性。

下面我们证明这个等式是恒成立的:

$$r_i=t_i g^{a_i+x_c} y_p^{-b_i} \bmod p=t_i g^{s-s'_i+x_c} y_p^{e-e'_i} \bmod p=$$
$$t_i g^{-s'_i} y_p^{-e'_i} g^{s+x_c} y_p^e \bmod p=g^s y_p^e y_c \bmod p=r$$

因此 LI 等人对此方案的链接性的分析是错误的,签名者无法把保留的信息和最终的签名结果对应起来,WANG 等人方案仍具有不可链接性。

2 对文献[7]方案的分析与改进

2.1 方案分析

文献[7]改进后的方案,在代理授权阶段原始签名人由于没有明确签名者的签名范围,容易造成代理签名权的滥用,尽管改进后的方案具有不可伪造性和不可链接性,然而在签名过程中增加了指数运算和逆运算的次数使得计算效率较低,不利于实际应用。

2.2 对文献[7]方案的改进

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:$r_A=g^{k_A} \bmod p$, $s_A=x_A h(m_w,r_A)+k_A y_B \bmod q$,并将$(r_A,s_A,m_w)$发送给代理签名人 B。其中,$m_w$ 是指由 A 制定的代理授权书,主要包括 A 和 B 的标志、B 的代理期限、代理签名文件的的范围等。

2)B 接收到(r_A,s_A,m_w)后检验等式 $g^{s_A}=y_A^{h(m_w,r_A)} r_A^{y_B} \bmod p$ 是否成立,如果成立,B 则接受(r_A,s_A,m_w),并计算 $x_P=s_A+x_B \bmod q$,相应的代理签名公钥为 $y_P=g^{x_P}=g^{s_A} y_B^{r_A}=y_A^{h(m_w,r_A)} r_A^{y_B} y_B \bmod p$, B 公开信息 r_A 和 y_P。

代理盲签名过程如下:

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

2)C 接收者 C 验证 $y_P=y_A^{h(m_w,r_A)} r_A^{y_B} y_B \bmod p$ 是否成立,若成立随机选择 $a,u \in Z_q^*$,计算 $r=tg^a y_P^u \bmod p$, $e=h(r \cdot m) \bmod q$, $e'=e-u \bmod q$ 把 e' 发给 B。

3)B 接收 e',计算 $s'=k-e'x_P \bmod q$,并发送 s' 给 C。

4)C 接收到的 s' 后验证 $t=g^{s'} y_P^{e'} \bmod p$ 是否成立,若成立则计算 $s=s'+a \bmod q$,(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 $e=h(g^s y_P^e \bmod p \cdot m) \bmod q$。如果等式成立则接受,否则拒绝。

证明: $g^s y_P^e \bmod p=g^{s'+a} y_P^e \bmod P=g^{k-e'x_P+a} g^{\varphi(e'+u)} \bmod P=g^{k+a+x_P+u} \bmod P=tg^a y_P^u \bmod p=r$

3 安全性分析

1)不可伪造性。原始签名人不可伪造代理签名人签名。如果原始签名人 A 想伪造代理签名,一种方法是设法拥有代理签名者的签名私钥(x_P,y_P),由式 $x_P=s_A+x_B \bmod q$,因为原始签名人 A 不知道代理签名者的私钥 x_B,所以不能推出 x_P;另一种方法是原始签名人 A 伪造出有效的密钥对$(\hat{x}_P,\hat{y}_P)$,由验证方程 $y_P=y_A^{h(m_w,r_A)} r_A^{y_B} y_B \bmod p$ 可以看出,A 欲伪造成功必须构造出$(\hat{x}_P,\hat{r}_P)$使得 $g^{\hat{x}_P}=y_A^{h(m_w,r_A)} \hat{r}_A^{y_B} y_B \bmod p$,这将面临离散对数问题,因此原始签名人不可伪造代理签名人签名。

代理签名人不可伪造代理盲签名。代理签名者 B 在没有 A 的同意和指派的前提下欲伪造出有效的密钥对$(\hat{x}_P,\hat{y}_P)$,由验证方程 $g^{s_A}=y_A^{h(m_w,r_A)} r_A^{y_B} \bmod p$, $y_P=y_A^{h(m_w,r_A)} y_A^{y_B} y_B \bmod p$ 可知,B 必须伪造$(\hat{s}_A,\hat{r}_A)$使得 $g^{\hat{s}_A}=y_A^{h(m_w,r_A)} \hat{r}_A^{y_B} \bmod p$ 和 $\hat{y}_P=y_A^{h(m_w,r_A)} \hat{r}_A^{y_B} y_B \bmod p$ 同时成立,这也将面临离散对数问题,代理签名人不能冒充原始签名人伪造签名。

请求签名者 C 不能伪造签名。假如签名接收者 C 根据签名算法伪造消息 $\hat{m}$ 的代理盲签名$(\hat{m}_w,(m_w,r_A),(\hat{s},\hat{e}))$,那么 C 可任取 $\hat{k}$,计算 $\hat{t}=g^{\hat{k}} \bmod p$,接着任取 $\hat{a}$, $\hat{u}$,并计算 $\hat{r}=\hat{t}g^{\hat{a}} y_P^{\hat{u}} \bmod p$, $\hat{e}=h(\hat{r} \cdot \hat{m}) \bmod q$, $\hat{e}'=\hat{e}-\hat{u} \bmod q$,在没有 B 参与的情况下 C 无法得到相应 $\hat{s}'$,这是因为 $\hat{s}'=\hat{k}-\hat{e}' x_P \bmod q$, x_P 对于 C 是不可能得到的,而若根据 $\hat{r}=g^{\hat{s}'} y_P^{\hat{e}'} \bmod p$ 计算 $\hat{s}'$ 是离散对数问题,由 $\hat{s}=\hat{s}'\hat{a} \bmod q$ 可知 C 无法得到 $\hat{s}$,即 C 无法伪造出 $\hat{m}$ 的代理盲签名$(\hat{m}_w,(m_w,r_A),(\hat{s},\hat{e}))$。

2)不可链接性。在此方案中代理签名者 B 可以观察到的信息为(t_i,s'_i,e'_i),若 A 存贮$(t_i,s'_i,$

表1 改进前后的计算量表

Tab.1 Computational complexity improved

方案	代理阶段	签名阶段	验证阶段	总运算量
LI等人的方案[7]	5E+4M	9E+7M+I	2E+M	16E+12M+I
改进后的方案	5E+3M	7E+6M	2E+M	14E+10M

e'_i),待用户C公开(m,s,e)后,代理签名者B可以计算$a_i = s - s'_i \bmod q$,$u_i = e'_i - e \bmod q$,然后代理签名者B可以计算$r_i = t_i g^{a_i} y_P^{u_i} \bmod p$,$r = g^t y_P^e \bmod p$,最后代理签名者B验证$r_i = r$是否成立。下面我们证明这个等式是恒成立的。

$$r_i = t_i g^{a_i} y_P^{u_i} \bmod p = t_i g^{s-s'_i} y_P^{e-e'_i} \bmod p = t_i g^{-s'_i} y_P^{-e'_i} g^t y_P^e \bmod p = g^t y_P^e \bmod p = r$$

所以签名者无法把保留的信息和最终的签名结果对应起来,即该方案具有不可链接性。

3)不可抵赖性。综合(1),(2)可知除了代理签名人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。

4)可区分性。由等式$g^{y_A} = y_A^{h(m_w, r_A)} r_A^{y_B} \bmod p$可以验证原始签名的有效性,由等式$y_P = y_A^{h(m_w, r_A)} r_A^{y_B} y_B \bmod p$,可以看出$y_P$含有原始签名人和代理签名人的公钥$(y_A, y_B)$,由验证方程$e = h(g^t y_P^e \bmod p \cdot m) \bmod q$可以验证代理签名$(s,e)$的有效性,同时验证方程也反映出签名$(s,e)$是由授权方和代理方共同完成的。

5)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,那么可以在系统内向用户广播消息,宣布y_P不再有效,从而B生成的代理签名就会随之失效。

6)防止代理签名权的滥用。在代理授权阶段原始签名人在授权书中明确了签名者的签名范围,有效地阻止了代理签名权的滥用。

4 效率分析

在进行签名的过程中占据大部分时间的是指数运算,乘法运算和逆运算,我们将李方伟等人的方案[7]和我们改进的方案进行了比较,并将方案的计算量列入表1中,表中E,M,I,分别表示取模意义下的指数运算,乘法运算和逆运算。

从表中容易看出改进后的方案指数运算和乘法运算的次数减少了,避免了求逆运算,因此改进后的代理盲签名方案有效的提高了签名速度。

5 结论

对文献[7]改进后的方案不仅同时拥有代理签名和盲签名的特点,也弥补了原有方案中代理者可以滥用代理权的缺陷,减少了求幂运算和乘法运算的次数,避免了求逆运算,有效的提高了签名的速度,因此改进后的方案是一个更为安全高效的代理盲签名方案,可应用到电子货币、电子投票、电子拍卖等电子商务领域。

参考文献:

[1] CHAUM D. Blind signature for untraceable payment [A]. Advances in Cryptology - Eurocrpt'82 Proceedings [C]. New York: Plenum Press, 1983, 199-203.

[2] MAMBO M, USUDA K, OKAMOTO E. Proxy proxy siganature: Delegation of the power to sign message[J]. IEICE Trans Fundations 1996, 79-A(9): 1338-1353.

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

[4] TAN ZUOWEN, LIU ZHUOJUN, TANG CHUNMING. A blind proxy siganature scheme based on DLP[J]. Journal of Software, 2003, 14(11): 1931-1935.

[5] SUN H, HSIEH B. On the some proxy blind proxy siganature schemes [C]. Australasian Information Security Worshop (AISW2004). New Zealand: Dunedin, 2004: 75-78.

[6] WANG SHAOBIN, HONG FAN, CUI GUOHUA. Secure efficient proxy blind proxy siganature schemes based on DLP [C]. Proceedings of the Seventh IEEE International Conference Technology(CEC'05). [S.L]: IEEE, 2005: 452-455.

[7] LI FANGWEI, TAN LIPING, QIU CHENGGANG. A proxy blind proxy siganature scheme based on DLP[J]. Journal of University of Electronic Science and Technology of China, 2008, 37(2): 172-174.

(责任编辑 刘存英)