文章编号:1005-0523(2015)06-0110-05

前向安全代理盲签名方案的分析与改进

刘二根,王 霞

(华东交通大学理学院,江西 南昌 330013)

摘要:通过对 Manoj 等人提出的前向安全的代理盲签名方案进行安全性分析,发现该方案在代理授权和代理盲签名阶段存在攻击伪造问题。由此提出了改进的前向安全的基于离散对数的代理盲签名方案。新方案在代理授权阶段将单向散列函数嵌入到短签名中,并改进了签名阶段,克服了原方案的缺陷。在效率上,只比原方案多一次哈希运算,但具有更高的安全性,新方案满足可验证性、可区分性、不可伪造性、不可否认性等性质。

关键词:代理盲签名;前向安全;不可伪造性;代理密钥

中图分类号:TP309 文献标志码:A

DOI:10.16749/j.cnki.jecjtu.2015.06.018

1982 年,Chaum 首次提出了盲签名的概念[1]。所谓盲签名,就是签名者在不知道所签署的消息的具体内容的情况下进行签名,由于这一特性,使得盲签名广泛的应用于电子现金、电子商务等领域。1996 年,Mambo 等人首次提出了代理签名的概念[2],所谓代理签名,就是当签名者因为某些原因,无法亲自签名,这时他需要委托他人代替自己签名。例如,某公司有一份紧急文件需要经理签名,但他在外地出差不能亲自签名,这时他可以将签名权委托给他的秘书,等等。

盲签名和代理签名相结合,可以产生代理盲签名。2000 年,Lin 和 Jan 首次提出了代理盲签名的概念[3],各种代理盲签名方案也应运而生[4-6]。目前,国内外提出了各种类型的代理盲签名,如无证书的代理盲签名方案,基于离散对数问题的代理盲签名,基于身份的代理盲签名等。但这些方案中有些存在缺陷,如不能抵抗公钥替换攻击,不能满足不可追踪性和不可链接性,不能抵抗签名伪造攻击等。2010 年,魏春艳等人提出了一个无证书代理盲签名方案[7],但葛荣亮等人发现该方案不满足不可追踪性[8];2011 年,黄隽等人提出了一个无证书代理盲签名方案[9],但张建中等人发现该方案不能抵抗公钥替换攻击和恶意的 KGC 攻击[10]。代理盲签名同时具有代理签名和盲签名的性质,使得其能够广泛的应用于电子现金、电子商务、电子选举等领域。但一旦代理密钥泄露,那么之前的所有签名都变成无效的。在研究代理盲签名的同时,人们逐渐转向研究安全性能高和降低密钥泄露所带来的损失的代理盲签名, 即具有前向安全的代理盲签名方案。1997 年,Anderson[11]首先提出了前向安全的概念,为了使签名具有前向安全性,就要采用密钥更新的方法,即使代理密钥泄露,也不会影响之前所有时段的代理盲签名。2011 年,魏俊懿等人[12]提出了一个前向安全的无证书代理盲签名方案,2013 年何滨等人[13]指出方案[12]不能满足盲性和原始签名者的伪造攻击。2014 年,Manoj 等人提出一个前向安全的代理盲签名方案[14],通过分析发现,方案在代理授权和代理盲签名阶段均存在攻击伪造。本文提出了一个改进的方案,能够克服原有方案的缺陷,具有更高的安全性,但在计算复杂度上只比原方案多一次哈希运算。

收稿日期:2015-06-23

基金项目:国家自然科学基金项目(11361024,11261019,61472138,61263032);江西省高校科技落地计划项目(KJLD12067);华东交通大学校立科研基金项目(11JC04);江西省科技厅科技项目(20151BDH80071)。

作者简介:刘二根(1965—),男,教授,研究方向为图论及其优化,信息安全。

1　预备知识

离散对数问题(DLP)：给定素数 p，Z_p^* 的生成元 g 和 Z_p^* 元素 a，寻找一个整数 x，$0\leqslant x\leqslant p-1$，使得 $a=g^x \bmod p$。

2　方案[14]回顾和安全性分析

2.1　方案[14]回顾

本方案包括原始签名者 A、代理签名者 B 和签名接收者 R。

1）系统初始化。选择大素数 p，q，使得 $q|p-1$，$g\in Z_q^*$ 是阶为 q 的元。(x_A, y_A)是原始签名者 A 的密钥对，其中 x_A 为私钥，$y_A=g^{xA} \bmod p$ 为公钥；(x_B, y_B)是代理签名者 B 的密钥对，其中 x_B 为私钥，$y_B=g^{xB} \bmod p$ 为公钥；(x_R, y_R)是签名接收者 R 的密钥对，其中 x_R 为私钥，$y_R=g^{xR} \bmod p$ 为公钥；H_1 是一个安全的 Hash 函数。

2）代理授权。首先生成一个包括双方身份、代理权限、代理期限等信息的授权证书 m_ω，原始签名者 A 选择一个随机数 $k_0\in Z_p^*$，计算 $r_0=g^{k_0} \bmod p$，短签名 $s_0=x_A+k_0y_B \bmod q$，并将(r_0, s_0)发送给代理人 B。B 收到(r_0, s_0)验证等式 $g^{s_0}=y_Ar_0^{yB} \bmod p$ 是否成立，若成立，则计算代理私钥 $x_p=s_0+x_{B0}y_A \bmod q$ 和其对应的代理公钥 $y_p=g^{xp} \bmod p$。

3）代理私钥更新。当签名进入第 i 个周期的时候，用第 $i-1$ 个周期的私钥 x_{Bi-1} 来计算本周期的私钥 $x_{Bi}=x_{Bi-1}^2 \bmod q$，计算出 x_{Bi} 后将 x_{Bi-1} 删除。然后代理签名者计算本周期的代理私钥 $x'_p=s_0+x_{Bi}y_A \bmod q$，代理公钥 $y'_p=g^{xp} \bmod p$。

4）签名产生。① 代理签名者 B 随机选择 $k\in Z_p^*$，计算 $r=g^k \bmod p$，并将 r 发给签名接收者 R。② 签名接收者 R 随机选择盲化因子 $\alpha,\beta,\gamma\in Z_p^*$ 计算 $r^*=(r)^\alpha g^{\beta+\gamma R}(y'_p)^{-r} \bmod p$，$e^*=(r^*\|m) \bmod q$，$e=\alpha^{-1}(e^*+\gamma) \bmod q$，并把 e 发送给 B。③ 代理签名者 B 收到 e 后，计算 $s=k-ex'_p \bmod q$，并把 s 发送给 R。④ 签名接收者 R 收到 s 后，计算 $s^*=\alpha s+\beta \bmod q$，$(m_\omega, r^*, s^*, e^*)$是关于 m 的代理盲签名。

5）签名验证。验证者收到关于消息 m 的签名(r^*, s^*, e^*)后，验证等式

$$e^*=H_1(g^{s^*}(y'_p)^{e^*}y_R \bmod p\|m) \tag{1}$$

是否成立，若成立则(r^*, s^*, e^*)是有效的代理盲签名，否则，签名无效。

要验证等式(1)成立，只需验证等式 $g^{s^*}(y'_p)^{e^*}y_R=r^*$ 即可

$$g^{s^*}(y'_p)^{e^*}y_R \bmod p=g^{\alpha s+\beta}(g^{x'p})^{e^*}y_R=g^{\alpha(k-ex'_p)+\beta}(g^{x'p})^{e^*}y_R=g^{\alpha(k-\alpha^{-1}(e^*+r)x'_p)+\beta}(g^{x'p})^{e^*}y_R=g^{\alpha k-rx'p+\beta}g^{xR}=(r)^\alpha g^{\beta+\gamma R}(y'_p)^{-r}=r^* \tag{2}$$

2.2　方案[14]的安全性分析

方案[14]在代理授权和代理盲签名过程中均存在攻击伪造，攻击方法类似于文献[6]。

1）原具有前向安全的代理盲签名方案在代理授权阶段存在一定的攻击。在代理授权阶段，代理签名者在收到(s_0, r_0)后却告知原始签名者自己并没有收到，从而原始签名者在其发送请求下，不得不重新发送(s'_0, r'_0)给原始签名者。那么，代理签名者可以由等式 $s_0=x_A+k_0y_B \bmod q$，$s'_0=x_A+k'_0y_B \bmod q$，可得 $s_0-s'_0=(k_0-k'_0)y_B \bmod q$，左右两边同时加上 x_A，从而有 $s''_0=s_0-s'_0+x_A=x_A+(k_0-k'_0)y_B \bmod q$。$r''_0=g^{k_0-k'_0} \bmod p$，用$(s''_0, r''_0)$代替原来的$(s'_0, r'_0)$，$(s''_0, r''_0)$可以通过验证等式 $g^{s''_0}=y_Ar_0''^{yB} \bmod p$，接下来，代理签名者可以利用自己生成的$(s''_0, r''_0)$来计算代理密钥 $x_p=s''_0+x_{B0}y_A \bmod q$。

在代理授权阶段存在问题的原因主要是在等式 $s_0=x_A+k_0y_B \bmod q$ 中，当代理签名人得到两组变量(s'_0, r'_0)，(s_0, r_0)就可以通过将这两个等式相减从而将原始签名者的私钥 x_A 消掉，那么代理签名者可以形成自己的(s''_0, r''_0)从而进行代理密钥的计算，也就是不需要原始签名者对其进行授权。为了能够防止原始签名者的私钥 x_A 被消掉，可以通过将等式 $s_0=x_A+k_0y_B \bmod q$ 改为 $s_0=x_AH_2(m_\omega, r_0)+k_0y_B \bmod q$。

2）原具有前向安全的代理盲签名方案在代理盲签名阶段存在签名伪造问题。攻击者在不知道签名接收者私钥的情况下也能构造一个关于消息 m 在指定周期的签名，这是因为可以用来 y_R 代替 g^{xR}，获得本周期的代理公钥 y'_p，那么 $r^*=(r)^{\alpha}g^{\beta}y_R(y'_p)^{-\gamma}\bmod p$，最终就会得到一个关于消息 m 在这一周期的代理盲签名 (r^*,s^*,e^*)，代理密钥的更新并不会影响签名的伪造。

在代理盲签名阶段存在签名伪造的原因是在等式 $r^*=(r)^{\alpha}g^{\beta+xR}(y'_p)^{-\gamma}\bmod p$，由于 $y_R=g^{xR}\bmod p$ 可以用 y_R 来代替 g^{xR}，也就是在不知道签名接收者私钥的情况下，攻击者可以伪造出关于消息 m 的代理盲签名 (r^*,s^*,e^*)。为了防止这种攻击，可以改变代理盲签名的部分过程，签名接收者随机选取盲化因子 $\alpha,\beta,\gamma\in Z^*_p$，等式 $r^*=(r)^{\alpha}g^{\beta+xR}(y'_p)^{-\gamma}\bmod p$，改为 $r^*=(r)^{\alpha}g^{\beta}(y'_p)^{-\gamma}\bmod p$，等式 $s^*=\alpha s+\beta\bmod q$ 改为 $s^*=\alpha s+\beta-x_R\bmod q$，其余不变。

3 改进的方案及安全性分析和效率分析

3.1 改进的方案

本文的方案是在方案[14]的基础上做的改进，本方案包括原始签名者 A、代理签名者 B 和签名接收者 R。

1）系统初始化。选择大素数 p,q，使得 $q\mid p-1,g\in Z^*_q$ 是阶为 q 的元。(x_A,y_A) 是原始签名者 A 的密钥对，其中 x_A 为私钥，$y_A=g^{xA}\bmod p$ 为公钥；(x_B,y_B) 是代理签名者 B 的密钥对，其中 x_B 为私钥，$y_B=g^{xB}\bmod p$ 为公钥；(x_R,y_R) 是签名接收者 R 的密钥对，其中 x_R 为私钥，$y_R=g^{xR}\bmod p$ 为公钥，H_0、H_1 是安全的 Hash 函数。

2）代理授权。首先生成一个包括双方身份、代理权限、代理期限等信息的授权证书 m_ω，原始签名者 A 选择一个随机数 $k_0\in Z^*_p$，计算 $r_0=g^{k0}\bmod p$，短签名 $s_0=x_AH_0(m_\omega,r_0)+k_0y_B\bmod q$，并将 (r_0,s_0) 发送给代理人 B。B 收到 (r_0,s_0) 验证等式 $g^{s_0}=y_A^{H_0(m_\omega,r_0)}r_0^{yB}\bmod p$ 是否成立，若成立，则计算代理私钥 $x_p=s_0+x_{B0}y_A\bmod q$ 和其对应的代理公钥 $y_p=g^{xp}\bmod p$。

3）代理私钥更新。当签名进入第 i 个周期的时候，用第 $i-1$ 个周期的私钥 x_{Bi-1} 来计算本周期的私钥 $x_{Bi}=x^2_{Bi-1}\bmod q$，计算出 x_{Bi} 后将 x_{Bi-1} 删除。然后代理签名者计算本周期的代理私钥 $x'_p=s_0+x_{Bi}y_A\bmod q$，代理公钥 $y_p'=g^{x'p}p$。

4）签名产生。

① 代理签名者 B 随机选择 $k\in Z^*_p$，计算 $r=g^k\bmod p$，并将 r 发给签名接收者 R。

② 签名接收者 R 随机选择盲化因子 $\alpha,\beta,\gamma\in Z^*_P$，计算 $r^*=(r)^{\alpha}g^{\beta}(y'_p)^{-\gamma}\bmod p$，$e^*=H_1(r^*\|m)\bmod q$，$e=\alpha^{-1}(e^*+\gamma)\bmod q$ 并把 e 发送给 B。

③ 代理签名者 B 收到 e 后，计算 $s=k-ex'_p\bmod q$，并把 s 发送给 R。

④ 签名接收者 R 收到 s 后，计算 $s^*=\alpha s+\beta-x_R\bmod q$，$(m_\omega,r^*,s^*,e^*)$ 是关于消息 m 的代理盲签名。

5）签名验证。验证者收到关于消息 m 的签名 (r^*,s^*,e^*) 后，验证等式

$$e^*=H_1(g^{s^*}(y'_p)^{e^*}y_R\|m)\bmod q \tag{3}$$

是否成立，若成立则 (r^*,s^*,e^*) 是有效的代理盲签名，否则，签名无效。

3.2 安全性分析

1）可验证性。要验证等式(3)只需要验证 $g^{s^*}(y'_p)^{e^*}y_R=r^*$ 即可

$$g^{s^*}(y'_p)^{e^*}y_R\bmod p=g^{\alpha s+\beta-xR}(g^{xp'})^{e^*}y_R=g^{\alpha(k-ex'_p)+\beta-x_R}(g^{x'p})^{e^*}y_R=g^{\alpha(k-\alpha^{-1}(e^*+r)x'_p)+\beta-x_R}(g^{x'p})^{e^*}y_R=g^{\alpha k-rx'_p+\beta-x_R}y_R=(r)^{\alpha}g^{\beta}(y'_p)^{-\gamma}=r^* \tag{4}$$

2）可区分性。因为授权证书 m_ω 包括双方的身份信息等，因此任何人可通过 m_ω 知道对应的代理签名者。

3）不可否认性。因为授权证书 m_ω 包括原始签名者和代理签名者身份信息、代理权限、代理期限等内

容，所以一旦代理盲签名有效，那么原始签名者和代理签名者都不可以否认自己的签名。

4）不可伪造性。由短签名 $s_0=x_AH_0(m_\omega,r_0)+k_0y_B \bmod q$，可知要想知道原始签名者的私钥 x_A，那么首先要求出 k_0，但 $r_0=g^{k_0} \bmod p$，求 k_0 相当于解离散对数问题，这是困难的，因此代理签名者不能假冒原始签名者进行代理授权。代理密钥 $x'_p=s_0+x_{Bi}y_A \bmod q$，要想知道代理密钥要首先知道代理签名者 B 的私钥 x_{Bi}，因此其他人不知道 x_{Bi} 的情况下是无法进行代理盲签名的。想要找到满足签名验证等式 $e^*=H_1(g^{s^*}(y'_p)^{e^*}y_R \bmod p\|m)$ 的一组有效签名 (r^*,s^*,e^*) 是困难的。

5）前向安全性。由于第 i 个周期代理签名者的私钥 $x_{Bi}=x^2_{Bi-1} \bmod q$，代理私钥 $x'_p=s_0+x_{Bi}y_A \bmod q$，在不知道本周期代理签名者私钥的情况下是无法进行本周期代理私钥的计算的。假设第 i 个周期的代理私钥被泄露，那么攻击者能够知道本周期代理签名者的私钥 x_{Bi}，但不能求得第 $i-1$ 个周期代理签名者的私钥 x_{Bi-1}，从而无法知道第 i 个周期的代理私钥，也无法伪造第 i 个周期之前的代理盲签名。

3.3　效率分析

新方案是将原方案代理授权阶段的 $s_0=x_A+k_0y_B \bmod q$ 改成 $s_0=x_AH_1(m_\omega,r_0)+k_0y_B \bmod q$，代理盲签名阶段的 $r^*=(r)^\alpha g^{\beta+xR}(y'_p)^{-y} \bmod p$ 改成 $r^*=(r)^\alpha g^\beta(y'_p)^{-y} \bmod p$，$s^*=\alpha s+\beta \bmod q$ 改成 $s^*=\alpha s+\beta-x_R \bmod q$，并在原方案中加入了授权证书 m_ω。新的方案能够抵抗在代理授权阶段和代理盲签名阶段的攻击和伪造，但在计算复杂度上只是增加了一次哈希运算。

4　结论

本文提出了一个改进的无证书代理盲签名方案，克服了原方案的缺陷，同时保留了原方案的前向安全性，使得代理密钥泄露后的损失减小；即使代理密钥泄露，攻击者也无法伪造过去时段的代理盲签名，之前的签名仍然有效。改进的方案具有可验证性、不可否认性、可区分性、不可伪造性等性质。由于代理盲签名具有盲签名的特点，也具有代理签名的特点，它可以广泛的应用于需要保护用户隐私和匿名性的场合，如电子现金、电子商务等。

参考文献：

[1] CHAUM D. Blind signatures for untraceable payments[C]//Advance in Cryptology–Crypto'82，1983：199–203.

[2] MAMBO M，Usuda K，Okamoto E. Proxy signatures for delegating signing operation [C]//Proceedings of 3rd ACM Conference on Computer and Communications Security. New York: ACM Press，1996：48–57.

[3] LIN W D，JAN J K. A security personal learning tools using a proxy blind signature scheme [C]// Proc of International Conference on Chinese Language Computing，2000：273–277.

[4] 张学军，王育民. 高效的基于身份的代理盲签名[J]. 计算机应用，2006，26(11)：2586–2588.

[5] 陈玲玲，亢保元，张磊.一种高效的基于身份的代理盲签名方案[J].华东交通大学学报，2008，25(1)：113–116.

[6] 张碧军，何明星. 一个基于代理盲签名的电子选举方案[J]. 西华大学学报：自然科学版，2013，32(4)：10–13.

[7] 魏春艳，蔡晓秋. 新的无证书代理盲签名方案[J]. 计算机应用，2010，30(12)：3341–3342.

[8] 葛荣亮，高德智，梁景玲，张云. 无证书代理盲签名方案的安全性分析及改进[J]. 计算机应用，2012，32(3)：705–706.

[9] 黄隽，杜伟章. 无证书代理盲签名方案[J]. 计算机工程与应用，2011，47(31)：73–75.

[10] 张建中，杨丽. 无证书代理盲签名方案的密码学分析与改进[J]. 计算机工程与应用，2014，50(4)：90–93.

[11] ANDERSON R. Invited lecture [C]//Proceedings of the 4th ACM Conference on Computer and Communications Security，Zurich，Switzerland，1997：1–7.

[12] 魏俊懿,杨晓元,余丹. 一种前向安全的无证书代理盲签名方案[J]. 计算机工程与应用,2011,47(34):95-97.
[13] 何滨,杜伟章. 前向安全无证书代理盲签名方案的分析与改进[J]. 计算机工程与应用,2013,49(22):104-109.
[14] MANOJ KUMAR CHANDE,BALWANT SINGH THAKUR. An improved proxy blind signature scheme with forward security[J]. International Journal of Computer Applications,2014(85):1-4.

Analysis and Improvement of Forward Secure Proxy Blind Signature Scheme

Liu Ergen, Wang Xia

(School of Science, East China Jiaotong University, Nanchang 330013, China)

Abstract: Through the security analysis of the forward secure proxy blind signature scheme proposed by Manoj et al., this study found out that the scheme can not resist the forgery attack during proxy phase and signature generation phase. In order to avoid these attacks, an improved forward secure proxy blind signature scheme was presented based on DLP. The improved scheme overcame the drawbacks in the original scheme by embedding one-way hash function in short signature during proxy phase and improving signature generation phase. In the efficiency, the improved scheme was more secure with one more hash operation compared with the original scheme, which has verifiability, distinguishability, unforgeability, nonrepudiation, etc.

Key words: proxy blind signature; forward secure; unforgeable; proxy key

(责任编辑　姜红贵)