对一个无证书代理盲签名方案的分析与改进*

张瑛瑛[1]，陈 玮[1]，曾吉文[1,2†]

(1. 新疆师范大学 数学科学学院，乌鲁木齐 830054；2. 厦门大学 数学科学学院，福建 厦门 361005)

摘 要： 通过对葛荣亮等人提出的无证书代理盲签名方案进行分析，从中发现该方案会引起公钥替换攻击和恶意但是被动的 KGC 攻击。为了解决此方案的安全性缺陷，提出了一种改进方案。分析表明，改进的新方案满足无证书代理盲签名方案的所有安全性要求，并且拥有与原方案相同的计算效率。

关键词： 无证书公钥密码体制；代理盲签名；公钥替换攻击；恶意但是被动的 KGC 攻击；双线性对

中图分类号： TP309.2 **文献标志码：** A **文章编号：** 1001-3695(2014)02-0540-03

doi:10.3969/j.issn.1001-3695.2014.02.052

Analysis and improvement of a certificateless proxy blind signature

ZHANG Ying-ying[1], CHEN Wei[1], ZENG Ji-wen[1,2†]

(1. *School of Mathematical Sciences, Xinjiang Normal University, Urumqi* 830054, *China*; 2. *School of Mathematical Sciences, Xiamen University, Xiamen Fujian* 361005, *China*)

Abstract: Through the cryptanalysis of a certificateless proxy blind signature scheme proposed by Ge Rong-liang, it find that this scheme can cause the public replacement attack and malicious-but-passive KGC attack. To avoid these attacks, this paper proposed a new improved scheme. Analysis result shows that the new improved shceme satisfies the requirements of proxy blind signature scheme and has the same computational efficiency compared with the original scheme.

Key words: certificateless public key cryptography; proxy blind signature; public key replacement attack; malicious-but-passive KGC attack; bilinear pairings

0 引言

2003 年的亚洲密码学会议上，Al-Riyami 等人[1]提出了无证书公钥密码学。在无证书公钥密码学中，用户的私钥是由密钥生成中心 KGC 和用户一起合作产生。无证书公钥密码体制的诞生，既克服了基于证书公钥密码体制的证书管理问题，并且也成功地解决了基于身份的密码体制中存在的密钥托管问题。

1996 年，Mambo 等人在文献[2,3]中提出了代理签名的概念。代理签名能让原始签名者将数字签名权利委托给代理签名者，使其能够代理原始签名者签发指定的数字消息，这种签名体制是在当某个签名者因某种原因不能行使自己的签名权利的情况下产生的。1982 年，Chaum 为了实现不可跟踪的支付系统，在文献[4]中提出了盲签名方案的概念。在盲签名方案中，要求签名者不能知道所签消息的内容，并且在盲签名公布后，签名人不能跟踪消息的拥有者，即不能将盲签名与中间信息进行追踪关联。近几年来，为了满足实际的需要，结合代理签名和盲签名双方的优点，Lin 等人[5]在 2000 年提出了代理盲签名，这种方案既具有盲签名的性质又具有代理签名的性质。因而，许多设计者构造的各类代理盲签名方案也就应运而生[6~8]。

对于 Li 等人[9]提出的无证书代理签名方案，Lu 等人在文献[10]中指出该方案会引起伪造攻击，进而提出了新的改进方案。2010 年，Tso 等人在文献[11]中声称其提出的代理签名方案和代理盲签名方案是安全的，但是 Gao 等人[12]发现该签名方案存在严重的安全缺陷，即该方案存在公钥替换攻击。恶意的用户能够替换原始签名人和代理签名人的公钥，从而对任意消息进行有效的签名。最后，Gao 等人给出了一个克服该攻击的改进方法，并且提出了一个新的方案。2010 年，魏春艳等人[13]提出了一个新的无证书代理盲签名方案，葛荣亮等人[14]发现该方案并不安全，即代理签名者可以将签名消息与中间数据链接起来，进而该方案不满足盲签名方案的不可追踪性，因此葛荣亮等人在文献[14]中给出了一个改进方案，本文简称为 GGLZ 方案。本文通过对 GGLZ 方案进行分析，发现该方案会引起公钥替换攻击和恶意但被动的 KGC 攻击，进而对 GGLZ 方案进行了改进，改进后的方案可以抵抗这两种攻击。

1 准备工作

1.1 双线性映射

令 G_1 和 G_2 是阶为素数 q 的加法群和乘法群，P 是 G_1 的生成元，若存在映射 $e: G_1 \times G_1 \to G_2$ 满足下列性质，则称此映射为双线性映射：

a) 双线性性。对于任意 $P, Q \in G_1$，以及 $a, b \in Z_q^*$，满足 $e(aP, bQ) = e(P, Q)^{ab}$。

b) 非退化性。存在 $P, Q \in G_1$，满足 $e(P, Q) \neq 1$。

收稿日期： 2013-05-06；**修回日期：** 2013-06-07 **基金项目：** 国家自然科学基金资助项目(11261060)；福建省自然科学基金资助项目(2012J01022)；新疆研究生科研创新资助项目(XJGRI2013130)

作者简介： 张瑛瑛(1989-)，女，硕士研究生，主要研究方向为密码学(zyy450793707@126.com)；陈玮(1988-)，男(通信作者)，硕士研究生；曾吉文(1963-)，男，教授，博导，博士，主要研究方向为密码学.

c) 可计算性。对于任意 $P,Q \in G_1$,存在一个有效的算法计算 $e(P,Q)$。

1.2 离散对数问题

在群 G_1 上,存在离散对数问题: 设 P、Q 是群 G_1 中的两个元素,要找到某一个数 $n \in Z_q^*$,使之满足 $Q = nP$。

2 GGLZ 代理盲签名方案回顾

方案中涉及的成员有密钥生成中心 KGC、原始签名人 A、代理签名人 B、用户 C、签名验证者。

2.1 系统参数生成

G_1 和 G_2 是阶为素数 q 的加法群和乘法群,令 P 是 G_1 的生成元,取双线性映射 $e: G_1 \times G_1 \to G_2$,$g = e(P,P)$。KGC 随机选取 $s \in Z_q^*$ 作为系统主密钥,计算公钥 $P_{pub} = sP$。取三个安全的哈希函数 $H_1: \{0,1\}^* \to G_1$,$H_2: \{0,1\}^* \times G_2 \to Z_q^*$,$H_3: \{0,1\}^* \to Z_q^*$,则系统的公开参数为: $Params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H_3\}$。

2.2 部分私钥提取

假设 A 和 B 的身份信息为 ID_A 和 ID_B,KGC 计算 $Q_A = H_1(ID_A)$ 和 $Q_B = H_1(ID_B)$,并生成部分私钥 $P_A = sH_1(ID_A)$ 和 $P_B = sH_1(ID_B)$,将 P_A 和 P_B 通过安全信道发给用户 A 和 B。

2.3 用户密钥生成

A 和 B 随机选取 $x_A, x_B \in Z_q^*$ 作为自己的秘密值,并计算公钥 $PK_A = x_AP$ 和 $PK_B = x_BP$,公开 PK_A 和 PK_B。则 A 和 B 的私钥为 (x_A, P_A) 和 (x_B, P_B)。

2.4 代理密钥生成

a) 原始签名者 A 建立授权证书 m_w 来说明包含 A、B 的身份信息和授权关系等内容,然后计算 $Q_B = H_1(ID_B)$,生成短签名 $S_w = x_AH_3(m_w)Q_B + P_A$,并将 (m_w, S_w) 通过安全信道发送给 B。

b) B 收到 (m_w, S_w) 后,首先验证等式是否成立: $e(S_w, P) = e(Q_B, PK_A)^{H_3(m_w)} e(Q_A, P_{pub})$,若成立,则计算代理密钥: $S_P = S_w + x_BH_3(m_w)Q_A + P_B$。

2.5 代理盲签名的生成

a) B 选取 $r \in Z_q^*$,计算 $R = g^r$ 并发送给 C。

b) C 任选 $\alpha, \beta \in Z_q^*$ 作为盲化因子,计算 $R' = R^\alpha g^\beta$,$t' = H_2(m, R'g^\alpha)$,$t = H_3(m \| ID_A \| ID_B)\alpha^{-1}t'$,并发送 t 给 B。

c) B 计算 $V' = tS_P + rP$,并发 V' 给 C。

d) C 收到 V' 后,首先计算 Q_A 和 Q_B,然后验证等式 $e(V', P) = \{[e(Q_B, PK_A)\, e(Q_A, PK_B)]^{H_3(m_w)} e(Q_A + Q_B, P_{pub})\}^t R$ 是否成立,若成立,则计算 $U_A = t'Q_A$,$U_B = t'Q_B$,$V = \alpha V' + \beta P$。那么,消息 m 上的代理盲签名为 $\sigma = (m_w, V, U_A, U_B, R')$。

2.6 签名的验证

验证者首先计算 $h = H_3(m \| ID_A \| ID_B)$,$R'' = e(V,P)\{[e(U_B, PK_A)\, e(U_A, PK_B)]^{H_3(m_w)} e(U_A + U_B, P_{pub})\}^{-h}$,然后验证 $R'' = R'$ 是否成立,若成立则接受签名,否则拒绝签名。

3 对 GGLZ 方案的攻击

对于 GGLZ 方案,给出了两种伪造攻击证明该方案并不安全。这两种伪造攻击的类型分别是公钥替换攻击和恶意但是被动的 KGC 攻击。

3.1 公钥替换攻击

GGLZ 方案无法抵抗公钥替换攻击,即普通的攻击者包括原始签名者 A 可以替换 A 的公钥,进而假冒原始签名人,并且可以对代理签名者 B 进行授权。具体步骤如下:

a) 普通攻击者选择随机的 $r_A \in_R Z_q^*$,并计算: $PK_A' = r_AP - H_3(m_w)^{-1}Q_B^{-1}Q_AP_{pub}$。

b) 普通攻击者计算 $S_w' = r_AH_3(m_w)Q_B$,并且选择一个恰当的授权证书 m_w'(包括攻击者和 B 的身份信息,代理签名消息的范围,代理权限等信息)。然后将 (m_w', S_w') 通过安全信道发给代理签名者 B。

c) B 收到 (m_w', S_w') 后,验证等式:

$$e(Q_B, PK_A')^{H_3(m_w)} e(Q_A, P_{pub}) =$$
$$e(Q_B, r_AP - H_3(m_w)^{-1}Q_B^{-1}Q_AP_{pub})^{H_3(m_w)} e(Q_A, P_{pub}) =$$
$$e(Q_B, r_AP)^{H_3(m_w)} e(Q_B, H_3(m_w)H_3(m_w)^{-1}Q_B^{-1}Q_AP_{pub})^{-1} e(Q_A, P_{pub}) =$$
$$e(Q_B, r_AP)^{H_3(m_w)} e(Q_BQ_B^{-1}Q_A, P_{pub})^{-1} e(Q_A, P_{pub}) =$$
$$e(Q_B, r_AP)^{H_3(m_w)} e(Q_A, P_{pub})^{-1} e(Q_A, P_{pub}) =$$
$$e(Q_B, r_AP)^{H_3(m_w)} e(Q_A, P_{pub})^{-1} e(Q_A, P_{pub}) =$$
$$e(r_AH_3(m_w)Q_B, P) = e(S_w', P)$$

通过以上分析,普通攻击者成功伪造了一个有效的 S_w'。可以看出,代理签名人 B 可以用有效的代理私钥 $S_P' = S_w' + x_BH_3(m_w)Q_A + P_B$ 对消息 m 进行盲签名,最后的验证等式也是成立的。故公钥替换攻击成功,GGLZ 方案并不能抵抗公钥替换攻击。

3.2 恶意但被动的 KGC 攻击

GGLZ 方案无法抵抗恶意但被动的 KGC 攻击,这种攻击指的是恶意的 KGC 可以针对某个特定的用户来生成系统参数,从而当该特定用户生成自己的公钥后,恶意的 KGC 可以假冒该用户。针对 GGLZ 方案,原始签名者 A 向 KGC 申请部分代理私钥时,恶意的 KGC 对原始签名者 A 生成了新的系统参数,当原始签名者 A 生成了自己的公钥后,恶意的 KGC 便成功地假冒了原始签名人,并对代理签名者 B 进行授权。具体步骤如下:

a) 恶意的 KGC 选择随机的 $\alpha \in_R Z_q^*$,并计算 $P = \alpha H_1(ID_B)$,$PK_A = x_AP$,$P_{pub} = sP$。

b) 恶意的 KGC 计算 $S_w' = \alpha^{-1}PK_AH_3(m_w') + sH_1(ID_A)$,并且选择一个恰当的授权证书 m_w'(包括 A 和 B 的身份信息,代理签名消息的范围,代理权限等信息)。然后将 (m_w', S_w') 通过安全信道发送给代理签名者 B。

c) B 收到 (m_w', S_w') 后,验证等式:

$$e(S_w', P) = e(\alpha^{-1}PK_AH_3(m_w') + sH_1(ID_A), P) =$$
$$e(\alpha^{-1}PK_AH_3(m_w'), P)\, e(sH_1(ID_A), P) =$$
$$e(\alpha^{-1}x_APH_3(m_w'), P)\, e(Q_A, P_{pub}) =$$
$$e(\alpha^{-1}x_A\alpha H_1(ID_B)H_3(m_w'), P)\, e(Q_A, P_{pub}) =$$
$$e(x_AH_1(ID_B), P)^{H_3(m_w')} e(Q_A, P_{pub}) =$$
$$e(Q_B, PK_A)^{H_3(m_w')} e(Q_A, P_{pub})$$

通过以上分析,恶意的 KGC 成功地伪造了一个有效的 S_w'。可以看出,代理签名人 B 可以用有效的代理私钥 $S_P' = S_w' + x_BH_3(m_w)Q_A + P_B$ 对消息 m 进行盲签名,最后的验证等式也是成立的。故恶意但被动的 KGC 攻击成功,GGLZ 方案不能

抵抗恶意但被动的 KGC 攻击。

4 对 GGLZ 方案的改进

通过以上对 GGLZ 方案的分析，本文将对 GGLZ 方案进行改进，改进主要分为两个方面，具体的改进步骤如下：

a) 由以上分析可以看出，GGLZ 方案无法抵抗公钥替换攻击，是因为普通攻击者可以计算出 $H_3(m_w)$，从而推算并构造出原始签名者 A 的公钥。针对普通攻击者可以替换原始签名者 A 的公钥，进而成功地冒充了原始签名者 A 的这个安全漏洞，如果将 A 的公钥嵌入到签名过程中的 H_3 函数运算中，普通攻击者就计算不出 A 的公钥，也就无法替换 A 的公钥，这样就可以抵抗公钥替换攻击。再考虑一点，普通攻击者也可以替换代理签名人 B 的公钥，针对此，本文将 B 的公钥也嵌入到签名过程中的 H_3 函数运算中。具体改进的操作就是将 GGLZ 方案中的 $H_3(m_w)$ 全部改为 $H_3(m_w, PK_A, PK_B)$，相应地将 $H_3:\{0,1\}^* \rightarrow Z_q^*$，修改为 $H_3:\{0,1\}^* \times G_1 \times G_1 \rightarrow Z_q^*$。

b) GGLZ 方案无法抵抗恶意但被动的 KGC 攻击，是因为恶意的 KGC 在用户生成部分私钥时就知道了 $H_1(\mathrm{ID}_A)$ 和 $H_1(\mathrm{ID}_B)$，然后才构造了一个特殊的系统参数 P，且令 $P = \alpha H_1(\mathrm{ID}_B)$，构造了新的系统参数，进而有了原始签名者 A 的公钥和系统的公钥，从而成功地伪造了一个有效的 S_w'。对于这个安全漏洞，可以通过预先生成用户和系统的公钥，后产生用户的部分私钥，并在 KGC 产生部分私钥时将用户身份和公钥一起绑定到 H_1 函数运算中解决，这样就可以抵抗恶意但被动的 KGC 攻击。具体改进的操作是将 GGLZ 方案中 2.2 节和 2.3 节这两步对调，即先进行 2.3 节的用户密钥生成这一过程后进行 2.2 节部分私钥提取，这样就可以保证先生成用户的公钥和系统的公钥，并且将 GGLZ 方案中的 $H_1(\mathrm{ID}_A)$ 和 $H_1(\mathrm{ID}_B)$ 分别改为 $H_1(\mathrm{ID}_A, PK_A)$ 和 $H_1(\mathrm{ID}_B, PK_B)$，相应地就将系统中的 $H_1:\{0,1\}^* \rightarrow G_1$，修改为 $H_1:\{0,1\}^* \times G_1 \rightarrow Z_q^*$。

5 对改进后方案的安全性和效率的分析

由第 4 章的改进方法和具体步骤中可以明显看出，改进后的方案满足 GGLZ 方案所具有的一切对代理盲签名方案的安全性要求，即可验证性、不可伪造性、不可追踪性、不可否认性、可区分性、抗滥用性和盲性。具体只分析可验证性和不可伪造性。

5.1 改进后方案的可验证性和不可伪造性分析

从第 4 章的改进方法和具体步骤中可以知道，本文将 $H_3(m_w)$ 全部改为 $H_3(m_w, PK_A, PK_B)$ 以及将 $H_1(\mathrm{ID}_A)$ 和 $H_1(\mathrm{ID}_B)$ 全部分别改为 $H_1(\mathrm{ID}_A, PK_A)$ 和 $H_1(\mathrm{ID}_B, PK_B)$，其他算法过程与原方案相同。故改进后方案能保证最终验证等式是成立的。

针对 3.1 节公钥替换攻击，本文在 $H_3(m_w)$ 中嵌入 A 和 B 的公钥。这样一来，显然计算 $H_3(m_w, PK_A, PK_B)$ 在计算 A 和 B 的公钥之后。故改进后的方案可以抵抗公钥替换攻击。针对 3.2 节恶意但被动的 KGC 攻击，本文在 $H_1(\mathrm{ID}_A)$ 和 $H_1(\mathrm{ID}_B)$ 中分别嵌入 A 和 B 的公钥。这样一来，显然计算 $H_1(\mathrm{ID}_A, PK_A)$ 和 $H_1(\mathrm{ID}_B, PK_B)$ 在计算用户的公私钥之后。改进后的方案可以抵抗恶意但被动的 KGC 攻击。故本文的方案满足不可伪造性。

5.2 改进后方案的效率分析

从第 4 章的改进方法和具体步骤中可以发现，本文将 $H_3(m_w)$ 全部改为 $H_3(m_w, PK_A, PK_B)$ 以及将 $H_1(\mathrm{ID}_A)$ 和 $H_1(\mathrm{ID}_B)$ 全部分别改为 $H_1(\mathrm{ID}_A, PK_A)$ 和 $H_1(\mathrm{ID}_B, PK_B)$，其他算法过程与原方案相同。可以发现，改进后的方案在计算量上并未作任何增加，故改进后的方案与原方案具有相同的计算效率。

6 结束语

本文对一个无证书代理盲签名方案进行了安全性分析，指出了该方案存在两种安全性缺陷，给出了对该方案的公钥替换攻击和恶意但被动的 KGC 攻击，为此对其提出了相应的改进方案。改进方案在保持效率不变的前提下，具有更高的安全性。

参考文献：

[1] AL-RIYAMI S, PATERSON K. Certificateless public key cryptography [M]//Advances in Cryptology-ASIACRYPT. Berlin: Springer-Verlag, 2003: 452-473.

[2] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures for delegating signing operation [C]//Proc of the 3rd ACM Conference on Computer and Communications Security. New York: ACM Press, 1996: 48-57.

[3] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures: delegation of the power to sign messages [J]. IEICE Trans on Fundamentals of Electronics, Communications and Computer Sciences, 1996, 79(9): 1338-1354.

[4] CHAUM D. Blind signatures for untraceable payments [C]//Advances in Cryptology. 1982: 199-203.

[5] 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.

[6] VERMA G K. A proxy blind signature scheme over braid groups [J]. International Journal of Network Security, 2009, 9(3): 214-217.

[7] HE De-biao, CHEN Jian-hua, HU Jin. An ID-based proxy signature schemes without bilinear pairings [J]. Annals of Telecommunications, 2011, 66(11-12): 657-662.

[8] SUN Ying, XU C, YU Y, *et al*. Improvement of a proxy multi-signature scheme without random oracles [J]. Computer Communications, 2011, 34(3): 257-263.

[9] LI X, CHEN K, SUN L. Certificateless signature and proxy signature schemes from bilinear pairings [J]. Lithuanian Mathematical Journal, 2005, 45(1): 76-83.

[10] LU R, HE D, WANG C. Cryptanalysis and improvement of a certificateless proxy signature scheme from bilinear pairings [C]//Proc of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. 2007: 285-290.

[11] TSO R, YI X. Certificateless proxy signature and its extension to blind signature [C]//Proc of the 4th International Conference on Network and System Security (NSS). 2010: 542-547.

[12] GAO B, HU G, HAN L. Cryptanalysis of a certificateless proxy signature and its extension to blind signature [C]//Proc of IEEE International Conference on Computer Science and Automation Engineering (CSAE). 2012: 356-359.

[13] 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.

[14] 葛荣亮，高德智，梁景玲，等. 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, 714.