对一种新型代理签名方案的分析与改进

鲁荣波[①②]　何大可[②]　王常吉[③]　缪祥华[②]
[①](吉首大学数学与计算机科学学院　吉首　416000)
[②](西南交通大学信息安全与国家计算网格实验室　成都　610031)
[③](中山大学计算机科学系　广州　510275)

摘　要：Gu-Zhang-Yang(2005)提出了一个不需要可信第三方参与的匿名代理签名方案，由于该方案的签名验证数据中没有回避孤悬因子这一现象，因此并不满足强不可伪造性，原始签名人可以伪造一个有效的代理签名通过验证，并成功地在代理签名者身份揭示阶段向公众证明该伪造的代理签名是由合法的代理签名者产生的。本文在分析该方案安全性的基础上提出了改进的匿名代理签名方案，克服了原方案的不足。

关键词：代理签名；匿名代理签名；孤悬因子；强不可伪造性
中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1009-5896(2007)10-2529-04

Cryptanalysis and Improvement of a New Proxy Signature Scheme

Lu Rong-bo[①②]　He Da-ke[②]　Wang Chang-ji[③]　Miao Xiang-hua[②]
[①](*College of Mathematics and Computer Science, Jishou University, Jishou* 416000, *China*)
[②](*Lab. of Information Security and National Computing Gird, Southwest Jiaotong University, Chengdu* 610031, *China*)
[③](*Department of Computer Science, Sun Yat-Sen University, Guangzhou* 510275, *China*)

Abstract: The proxy signature with proxy signer privacy protection without a trusted third party put forward by Gu-Zhang-yang(2005), does not posses the strong unforgeability property because of not being able to avoid the suspending-factor. With this scheme, the original signer can forge a valid proxy signature and pass the procedure of verification and revelation, therefore he or she can successfully prove it is signed by a legal proxy signer. To avoid this shortcoming, an improvement of a proxy signature scheme with proxy signer privacy protection is proposed based on the analysis of the Gu-Zhang-yang's scheme.

Key words: Proxy signature; Proxy signature with proxy signer privacy protection; Suspending- factor; Strong unforgeability

1　引言

随着公钥密码体制研究的深入和电子商务的迅猛发展，数字签名得到了广泛应用。签名者用自己的私钥对文件进行签名，验证者利用签名者的公钥验证签名的有效性，相对于传统的手写签名，数字签名变得更安全。要设计一个签名方案，在做好签名私钥隐藏的同时还必须公开足够的数据供验证者验证，这些数据便是通常所说的签名数据。签名数据的有效性通常是通过等式来验证的，如果签名数据在验证等式中处于底数或指数位置，攻击者要伪造出一个合乎要求的底数就面临解二次或高次剩余问题，要伪造出一个合乎要求的指数就面临解离散对数问题。文献[1]提出了一个孤悬因子的新概念；在数字签名验证等式中出现的签名数据，如果既不在底数位置上也不在指数位置上，而是作为一个独立的因子，这样的签名数据为孤悬因子。并进一步指出签名数据在验证等式中出现的位置是有一定要求的，在数字签名设计中应明确回避孤悬因子这一现象。

代理签名的概念最早由Mambo, Usuda和Okamoto[2]提出来。在代理签名方案中，原始签名人可以把签名的权利委托给一位或者多位代理签名人，由代理签名人代替他生成有效的签名。自从代理签名的概念被提出以后，代理签名方案就一直是密码学研究者关注的焦点，相继提出有各种各样的代理签名方案，如门限代理签名[3]、代理盲签名[4]、多重代理签名[5]等。在一些实际应用中对参与者即代理签名人的隐私保护是一个必然的要求，如当代理签名人为电子选举中的投票人或为电子拍卖中的竞标人时等等，投票人充当代理签名人的角色，运用原始签名人分发的以证明合法投票身份的委托密钥生成自己的代理签名密钥进行投票时，希望对自己的身份和隐私保护，也就是说代理签名人不愿意让其他人(也可能包括原始签名人在内)能够仅仅根据所接收到的代理签名直接确定出代理签名人的真实身份，而是希望匿名地代表

2006-04-03 收到，2006-09-18 改回
国家自然科学基金(60503005)和湖南省自然科学基金(03JJY6017)资助课题

原始签名人生成代理签名，这样就产生了所谓的匿名代理签名[6]。一般而言，一个安全有效的匿名代理签名需要满足以下安全性需求：

(1)可验证性(verifiability)：利用公开的信息可验证原始签名人对被签消息的授权。

(2)强不可伪造性(strong unforgeability)：除代理签名人以外，任何人包括原始签名人都不可能伪造出代理签名。

(3)强不可否认性(strong non-repudiation)：代理签名人无法否认自己产生的代理签名。

(4)代理保密性(proxy privacy)：单独从代理签名中无法揭露出代理签名人的身份。

(5)可揭示匿名性(anonymity revocation)：当对代理签名发生争议时，能够揭示出代理签名人的身份。

(6)防止滥用性(prevention of misuse)：代理签名人不能使用代理签名密钥进行除合法的代理签名之外的活动。如果发生误用甚至滥用，安全有效的代理签名方案必须具备追究代理签名人责任的功能。

匿名代理签名的提出引起了人们广泛重视，成为了一个新的研究热点[6−9]。但到目前为止，大部分方案存在安全缺陷，文献[6]利用别名技术构造了一个匿名代理签名方案，文献[7]指出该方案不能抵抗原始签名人的伪造攻击。文献[8]提出的方案不满足不可否认性和不能抵抗联合攻击[9]。文献[10]的签名方案也存在安全缺陷(作者在另文中详细阐述)。

最近，谷利泽等人提出了一种匿名代理签名方案[11](简称Gu-Zhang-Yang方案)，其特点在于整个过程不需要可信中心的参与。本文对该方案进行了分析，分析表明，该方案设计过程中没有回避孤悬因子这一现象，该方案并不满足强不可伪造性，原始签名者可以伪造一个有效的代理签名通过验证过程，并且可以成功地在代理签名者身份揭示阶段向公众证明该伪造的代理签名是由合法的代理签名者产生的。最后文章提出了改进方法。

2 Gu-Zhang-Yang方案[11]

符号约定：p 和 q 是一对大素数且满足 $q \mid p-1$，$g \in Z_q^*$ 并且 $g^q = 1 \bmod p (g \neq 1)$；$h$ 为安全的哈希函数；m 为需要签名的消息。A 为原始签名者，B 为代理签名者；V 为验证者；m_w 是指描述原始签名者 A 授权代理签名者 B 代理权限约定的授权书，包括 A 的标识，B 的代理期限、签名消息范围等内容；x_A 为原始签名者 A 的私钥，把 $y_A = g^{x_A} \bmod p$ 公开，x_B 为代理签名者 B 的私钥，$y_B = g^{x_B} \bmod p$ 为代理签名者 B 的公钥；x_P 为原始签名者 A 和代理签名者 B 共同生成的代理私钥；$y_P = g^{x_P} \bmod p$ 为对应的代理公钥；ID_B 为代理签名者 B 的标识；ID_P 为签名者的标识；$\mathrm{Sig}(m,x)$ 是签名者用私钥 x 对消息 m 的一个离散对数型数字签名，签名返回值为 σ；$\mathrm{Ver}(y,\sigma,m)$ 与签名算法相对应的验证算法；y 为签名者的公钥；返回值为真或者假。

2.1 代理密钥的生成(PKG)

第 1 步　原始签名者 A 通过安全通道向代理签名者 B 发送 m_w，B 收到 m_w 后，如果接收代理授权，则计算：$k_B \in {}_R Z_q^*$，$r_B = g^{k_B} \bmod p$，$s_B = x_B + k_B r_B \bmod q$，$k_1 \in {}_R Z_q^*$，$r_1 = g^{k_1} \bmod p$，$s_1 = x_B h(r_B, \mathrm{ID}_B, r_1) + k_1 \bmod q$。

B 把 $(r_B, \mathrm{ID}_B, r_1, s_1)$ 返回给 A，A 验证等式：$g^{s_1} = y_B^{h(r_B,\mathrm{ID}_B,r_1)} r_1 \bmod p$ 是否成立。如果成立，A 秘密保存 $(r_B, y_B, \mathrm{ID}_B)$，并计算 $Y_P = y_B r_B^{r_B} \bmod p$，并把 Y_P 写入 m_w 中。

第 2 步　A 计算：$k_A \in {}_R Z_q^*$，$r_A = g^{k_A} \bmod p$，$s_A = x_A h(m_w, r_A) + k_A \bmod q$。

A 通过安全信道发送 (r_A, s_A) 和 m_w 给 B。B 验证：$g^{s_A} = y_A^{h(m_w,r_A)} r_A \bmod p$ 是否成立，如果成立，B 秘密保存 (r_A, s_A, m_w, s_B)。

第 3 步　B 生成代理私钥 x_P，即 $x_P = s_A + s_B$。

2.2 代理签名算法(PS)

如果消息 m 符合 m_w 的约定，代理签名者用代理签名私钥 x_P 产生代理签名 σ_P，即 $\sigma_P = \mathrm{Sig}(m, x_P)$，代理签名值为 $(m, \sigma_P, m_w, r_A, y_A)$。

2.3 代理签名验证算法(PV)：

第 1 步　验证者 V 检查消息 m 是否符合 m_w 的约定，如果符合，进入第二步，否则认为代理签名 σ_P 无效。

第 2 步　验证者 V 利用代理签名 $(m, \sigma_P, m_w, r_A, y_A)$ 计算 $y_P = y_A^{h(m_w,r_A)} r_A Y_P \bmod p$ (其中 Y_P 是从 m_w 中取得)，然后验证 $\mathrm{Ver}(y_P, \sigma_P, m) = \mathrm{true}$ 是否成立，如果成立，则代理签名有效。

2.4 揭示代理者身份算法(PR)

第 1 步　验证者 V 向原始签名者 A 提供代理签名 $(m, \sigma_P, m_w, r_A, y_A)$，$A$ 使用代理签名验证算法 PV 验证过程代理签名的有效性，如果有效，进入第 2 步。

第 2 步　原始签名者 A 从 m_w 中取出 Y_P，然后依次取出在代理密钥对生成阶段保存的 $(r_B, y_B, \mathrm{ID}_B)$，判断等式 $Y_P = y_B r_B^{r_B} \bmod p$ 是否成立，如果存在 $(r_B, y_B, \mathrm{ID}_P)$ 满足这个等式，则 ID_P 是实现代理签名 $(m, \sigma_P, m_w, r_A, y_A)$ 的代理签名者。

3 对方案的分析

本文对 Gu-Zhang-Yang 方案的分析表明，该方案并不满足该文声称的强不可伪造性。这是由于在验证等式 $y_P = y_A^{h(m_w,r_A)} r_A Y_P \bmod p$ 中出现了孤悬因子 r_A，验证算法无法对 (r_A, s_A) 的合法性进行验证(这里 (r_A, s_A) 实际上是原始签名者 A 对授权证书 m_w 的一个签名)，这样就为伪造者打开了方便之门，一个恶意的原始签名者可以利用已经生成的授权证书 m_w 代理签名来生成一个消息 m (符合 m_w 的约定)的有效的代理签名，能够通过验证过程和代理签名身份揭示过程。

原始签名者 A 可以按照如下过程生成代理签名私钥

x_P：

(1) $c \in {}_RZ_q^*$， $r_A = g^c Y_P^{-1} \bmod p$。

(2)生成代理签名私钥 $x_P = x_A h(m_w, r_A) + c$。

然后，原始签名者 A 利用代理签名算法计算 $\sigma_P = \mathrm{Sig}(m, x_P)$，得到一个代理签名 $(m, \sigma_P, m_w, r_A, y_A)$，该代理签名一定能通过验证算法，并且在代理身份揭示阶段，成功指控该签名是由代理签名者 B 生成的。这是因为：

$$y_P = g^{x_P} = g^{x_A h(m_w, r_A) + c} = g^{x_A h(m_w, r_A)} g^c = Y_A^{h(m_w, r_A)} g^c Y_P^{-1} Y_P$$
$$= y_A^{h(m_w, r_A)} r_A Y_P \bmod p$$

则 (x_P, y_P) 是有效的代理签名密钥对，利用 x_P 按照代理签名算法 PS 产生的代理签名 $(m, \sigma_P, m_w, r_A, y_A)$ 一定能通过验证算法 PV。

在揭示代理签名者身份阶段，由于 Y_P 是合法的，原始签名者一定能找到在代理密钥对生成阶段保存的一组数据 $(r_B, y_B, \mathrm{ID}_B)$，满足 $Y_P = y_B r_B^{r_B} \bmod p$，则由揭示代理者身份算法(PR)得出结论：$\mathrm{ID}_B$ 是实现代理签名 $(m, \sigma_P, m_w, r_A, y_A)$ 的代理签名者。这样就成功地向公众证明该伪造的代理签名是由合法的代理签名者 B 生成的。

4　改进的代理签名

由以上分析可以看出，造成原始签名者 A 能够伪造一个有效代理签名的原因是由于在验证等式 $y_P = y_A^{h(m_w, r_A)} r_A \cdot Y_P \bmod p$ 中出现了孤悬因子 r_A，验证算法无法对 (r_A, s_A) 的合法性进行验证，使得一个有恶意的原始签名者可以随意伪造 r_A。那么一个有效的改进方法就是把 s_A 也作为代理签名的一部分，在验证过程中增加验证 (r_A, s_A) 的有效性，其验证等式为 $g^{s_A} = y_A^{h(m_w, r_A)} r_A \bmod p$，但这样做将增加签名长度和验证运算量。比较之下，下面提出的改进方案不会增加签名长度，而增加的验证运算量也较小。

4.1 代理密钥的生成(PKG)

第 1 步　同原方案 2.1 节第 1 步。

第 2 步　A 计算：$k_A \in {}_RZ_q^*$， $r_A = g^{k_A} \bmod p$，$s_A = x_A \cdot h(m_w, r_A) + k_A r_A \bmod q$。

A 通过安全信道发送 (r_A, s_A) 和 m_w 给 B。B 验证：$g^{s_A} = y_A^{h(m_w, r_A)} r_A^{r_A} \bmod p$ 是否成立，如果成立，B 秘密保存 (r_A, s_A, m_w, s_B)。

第 3 步　同原方案 2.1 节第 3 步。

4.2 代理签名算法(PS)

同原方案 2.2 节。

4.3 代理签名验证算法(PV)

第 1 步　同原方案 2.2 节第 1 步。

第 2 步 验证者 V 利用代理签名 $(m, \sigma_P, m_w, r_A, y_A)$ 计算 $y_P = y_A^{h(m_w, r_A)} r_A^{r_A} Y_P \bmod p$ (其中 Y_P 是从 m_w 中取得，然后验证 $\mathrm{Ver}(y_P, \sigma_P, m) = \mathrm{true}$ 是否成立，如果成立，则代理签名有效。

4.4 揭示代理者身份算法(PR)

同原方案 2.4 节。

5　改进方案的分析

改进方案继承了 Gu-Zhang-Yang 方案的所有优点(详见文献[10])，这里只对其可验证性和强不可伪造性进行分析。

5.1 可验证性分析

定理 1 代理签名者 B 使用代理私钥 x_P，代表原始签名者 A 对消息 m 签名，验证者 V 利用代理签名 $(m, \sigma_P, m_w, r_A, y_A)$ 计算代理公钥：$y_P = y_A^{h(m_w, r_A)} r_A^{r_A} Y_P \bmod p$。然后使用 y_P 验证相应的代理签名，那么 $y_P = g^{x_P} \bmod p$。

证明：由于 $x_P = s_A + s_B$， $s_A = x_A h(m_w, r_A) + k_A r_A \bmod q$， $s_B = x_B + k_B r_B \bmod q$， $Y_P = y_B r_B^{r_B} \bmod p$，则

$$g^{x_P} = g^{s_A + s_B} \bmod p = g^{x_A h(m_w, r_A) + k_A r_A + x_B + k_B r_B} \bmod p$$
$$= g^{x_A h(m_w, r_A)} g^{k_A r_A} g^{x_B} g^{k_B r_B} \bmod p$$
$$= y_A^{h(m_w, r_A)} r_A^{r_A} y_B r_B^{r_B} \bmod p$$
$$= y_A^{h(m_w, r_A)} r_A^{r_A} Y_P \bmod p = y_P$$

即 $y_P = g^{x_P} \bmod p$ 成立。

5.2 不可伪造性分析

由于在改进方案中的验证等式 $y_P = y_A^{h(m_w, r_A)} r_A^{r_A} Y_P \cdot \bmod p$ 中避免了孤悬因子这一现象，原始签名者按照第 3 节选择适当的 r_A 来求 x_P 的伪造方法是行不通的，因此即使是原始签名者也不能伪造一个有效的代理签名，该方案满足强不可伪造性。

6　结束语

Gu-Zhang-Yang 方案没有回避孤悬因子这一现象，因此，该方案并不满足强不可伪造性，原始签名者可以伪造一个有效的代理签名通过验证过程，并且可以成功地在代理签名者身份揭示阶段向公众证明该伪造的代理签名是由合法的代理签名者产生的。本文在分析该方案的基础上提出了改进方法，改进的方案继承了原方案的优点，克服了原方案的不足。

参 考 文 献

[1] 曹正军，刘木兰. 数字签名方案中的孤悬因子和冗余数据.计算机学报，2006, 29(2): 249–255.

[2] Mambo M, Usuda K, and Okamoto E. Proxy signature: Delegation of the power to sign messages. *IEICE Trans. on Fundamentals of Electronics Communications and Computer Science*, 1996, E79-A(9): 1338–1354.

[3] Zhang K. Threshold proxy signature schemes. In: Proc of the 1st Int'l Information Security Workshop (ISW'97), Berlin: Springer-Verlag, 1997, LNCS 1396: 191–197.

[4] Lal S and Awasthi A K. Proxy blind signature scheme. Available at http:/eprint.iacr.org/. 2003.

[5] Yi Lijiang, Bai Guoqiang, and Xiao Guozhen. Proxy multi-signature scheme. *Electron. Lett.*, 2000, 36(6): 527–528.

[6] Shum K and Wei V K. A strong proxy signature scheme with proxy signer privacy protection. In: N Shahmehri ed. Proc. of the 11th IEEE Int'l Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises(WETICE'02). New York: IEEE Press, 2002: 55–56.

[7] Sun Hung-Min and Hsieh Bin-Tsan. Cryptanalysis of a strong proxy signature scheme with proxy signer privacy protection. In: Proc of the IEEE 37th Annual 2003 international conference on security Technology. Taipei, Taiwan: IEEE Press, 2003: 474–476.

[8] 王晓明，符方伟. 可撤销匿名性的盲代理签名方案.计算机学报, 2003, 26(1): 51–54.

[9] 傅晓彤，杨礼珍，肖国镇. 对可撤销匿名性的盲代理签名方案的注记. 计算机学报, 2005, 28(8): 1404–1407.

[10] Fu Xiongtong, Kou Weidong, and Xiao Guozhen. A proxy signature scheme with proxy signer privacy anonymity. In: Proc of the IEEE International Conference on E-Commerce Technology for Dynamic E-Business(CEC-East'04) New York: IEEE Press, 2004: 257–260.

[11] 谷利泽，张胜，杨义先.一种新型的代理签名方案.电子与信息学报, 2005, 27(9): 1463–1466.

鲁荣波： 男，1970 年生，副教授，博士生，研究领域为应用密码学.

何大可： 男，1944 年生，教授，博士生导师，主要研究领域为应用密码学、并行计算.

王常吉： 男，1972 年生，副教授，博士，主要研究领域为应用密码学.

缪祥华： 男，1972 年生，讲师，博士，主要研究领域为应用密码学.