三种盲代理多重签名方案的密码分析

王天银[①②] 刘麦学[①] 温巧燕[②]
[①](洛阳师范学院数学科学学院 洛阳 471022)
[②](北京邮电大学网络与交换技术国家重点实验室 北京 100876)

摘 要：对三种盲代理多重签名方案进行了密码分析，在李媛等人(2003)的方案中，任何一个原始签名者可以通过伪造代理密钥的方法产生盲代理多重签名；在康莉等人(2007)的第 1 类盲代理多重签名方案中，攻击者不仅可以伪造任何代理签名者的有效子代理密钥，而且还可以伪造对任何消息的盲代理多重签名；在康莉等人的第 2 类盲代理多重签名方案中，攻击者可以通过伪造代理密钥的方法产生有效盲代理多重签名，从而证明了这 3 种方案都是不安全的。

关键词：代理签名；盲代理签名；多重签名；盲代理多重签名
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2009)02-0493-04

Cryptanalysis of Three Blind Proxy Multi-signature Schemes

Wang Tian-yin[①②] Liu Mai-xue[①] Wen Qiao-yan[②]
[①](*School of Mathematical Science*, *Luoyang Normal University*, *Luoyang* 471022, *China*)
[②](*State Key Laboratory of Networking and Switching Technology*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)

Abstract: Through the cryptanalysis of three blind proxy multi-signature schemes, it shows that in Li Yuan *et al.*'s scheme, any original signer can sign a valid blind proxy multi-signature by the means of forging proxy key, and in Kang Li *et al.*'s first type blind proxy multi-signature scheme, attacker not only can forge any proxy signer's proxy sub-key, but also can forge blind proxy multi-signatures on any message, and in Kang Li *et al.*'s second type blind proxy multi-signature scheme, attacker can sign a valid blind proxy multi-signature by the means of forging proxy key, therefore the three schemes are not secure.

Key words: Proxy signature; Blind proxy signature; Multi-signature; Blind proxy multi-signature

1 引言

1996 年，Mambo 等首先提出了代理签名的概念，给出了解决数字签名权力委托的有效方法[1]。由于代理签名在移动通信、移动代理和电子商务等方面有着重要的应用，所以一提出便受到广泛关注，国内外学者对其进行了深入的探讨与研究。目前，人们已经提出了很多不同类型的代理签名方案[1−5]，但在这些方案中，原始签名人都能根据代理签名确定代理签名人的身份。这对原始签名人是非常有用的，因为原始签名人能对代理签名人的代理签名进行监督，防止代理签名人滥用他们的代理签名权。但在有些情况下，尽管代理签名人忠实地行使着原始签名人委托给自己的代理签名权力，但代理签名人仍然不希望自己的代理签名受到原始签名人的监督，不愿意原始签名人能根据代理签名确定出其身份。为了满足上述要求，文献[5]提出了一种新的代理签名体制-盲代理签名体制。有时，人们需要一个盲代理签名能够同时代表多个原始签名人，为此，文献[6,7]分别给出了盲代理多重签名的概念。

盲代理多重签名体制一般可以分为两类：第 1 类为多个代理签名人受不同原始签名人的委托，联合生成代表原始签名人利益的签名；第 2 类为一个代理签名人同时接受多个原始签名人的委托，利用代理密钥独自生成代表原始签名人利益的签名[7]。

在文献[6]中，李媛，尹为民给出了一种第 2 类盲代理多重签名方案，在文献[7]中康莉等人给出了一种第 1 类盲代理多重签名方案和一种第 2 类盲代理多重签名方案。然而，本文通过对这 3 种盲代理多重签名方案的分析，发现这 3 种方案都存在安全隐患，并不满足盲代理多重签名方案的要求。

2 李媛等人的盲代理多重签名方案[6]

2.1 参数设置

p，q 是大素数，且 $q \mid p-1$，g 为 Z_p^* 的阶为 q 的元；$x_i \in_R Z_q^*$ 为原始签名人 A_i $\left(1 \le i \le n\right)$ 的私钥，对应的公钥为

2007-08-17 收到，2008-01-14 改回
国家 863 计划项目(2006AA01Z419)，国家自然科学基金重大研究计划项目(90604023)，北京市自然科学基金 (4072020)，河南省教育厅自然科学基础研究项目(2007120007, 2008B120005)和洛阳师范学院青年基金(2008-QNJJ-012)资助课题

y_i，且 $y_i = g^{x_i} \pmod p$；$\mathrm{sig}_\sigma(m)$ 为用私钥 σ 对消息 m 进行签名的算法，$\mathrm{ver}(y,s,m)$ 为用私钥 σ 的对应公钥 y 对消息 m 的签名 s 进行验证的算法。

2.2 委托过程

(1)每个原始签名人 $A_i\ (1 \le i \le n)$ 随机选择 $k_i \in Z_q^*$，计算 $K_i = g^{k_i} \bmod p$，使得 K_i 与 q 互素，并将 K_i 发送给代理签名人 B；

(2) B 随机选择 $\alpha_i, \beta_i, \lambda_i \in Z_q^*$，计算 $R_i = K_i^{\alpha_i} g^{\beta_i} \bmod p$ 和 $\lambda_i' = \alpha\lambda_i K_i R_i^{-1} \bmod q$，使得 R_i 与 q 互素，并将 λ_i' 发送给 A_i；

(3) A_i 计算 $\sigma_i' = k_i\lambda_i' + x_i K_i \bmod q$，并将 σ_i' 发送给 B；

(4) B 计算 $\sigma_i = \sigma_i' R_i K_i^{-1} + \beta_i\lambda_i \bmod q$，验证 $g^{\sigma_i} = R_i^{\lambda_i} \cdot y_i^{R_i} \bmod p$，若所有的子代理密钥 $(\sigma_i, R_i, \lambda_i)$ 都能通过验证，B 计算代理密钥 $\sigma = \sum_{i=1}^n \sigma_i$，验证公钥为 $y = \prod_{i=1}^n R_i^{\lambda_i} y_i^{R_i} \cdot \bmod p$。

2.3 盲代理多重签名产生及验证过程

对于消息 m，B 计算 $s = \mathrm{sig}_\sigma(m)$，则 $(m, s, R_1, \cdots, R_n, \lambda_1, \cdots, \lambda_n)$ 是 B 作为 $A_1, A_2, \cdots, A_n$ 的代理签名人产生的有效盲代理多重签名。

验证人收到盲代理多重签名 $(m, s, R_1, \cdots, R_n, \lambda_1, \cdots, \lambda_n)$ 后，计算 $y = \prod_{i=1}^n R_i^{\lambda_i} y_i^{R_i} \bmod p$，若 $\mathrm{ver}(y,s,m) = \mathrm{True}$，则签名有效。

3 对李媛等人的盲代理多重签名方案的密码分析

定理 1 任何一个原始签名人可以通过伪造代理密钥的方式伪造有效的盲代理多重签名。

证明 不失一般性，不妨设原始签名人 A_1 欲伪造对消息 m' 的有效盲代理多重签名，伪造过程如下：

(1) A_1 任选 $\lambda_i \in Z_q^*, R_i \in Z_p^*\ (2 \le i \le n)$，计算 $T = \prod_{i=2}^n R_i^{\lambda_i} y_i^{R_i} \bmod p$；

(2) A_1 任选 $\lambda_1 \in Z_q^*$，计算 $R_1 = T^{-\lambda_1^{-1}} \bmod p$；

(3) A_1 计算 $\sigma = x_1 R_1 \bmod q$ 作为代理密钥，验证公钥为 $y = \prod_{i=1}^n R_i^{\lambda_i} y_i^{R_i} \bmod p$。

易知

$$\begin{aligned} y &= \prod_{i=1}^n R_i^{\lambda_i} y_i^{R_i} \bmod p = y_1^{R_1} R_1^{\lambda_1} \prod_{i=2}^n R_i^{\lambda_i} y_i^{R_i} \bmod p \\ &= y_1^{R_1} (T^{-\lambda_1^{-1}})^{\lambda_1} T \bmod p = y_1^{R_1} \bmod p = g^{\sigma} \bmod p \end{aligned}$$

因此 (σ, y) 为有效的代理签名密钥对，原始签名人 A_1 可以用代理密钥 σ 伪造对消息 m' 的签名 $(m', s, R_1, \cdots, R_n, \lambda_1, \cdots, \lambda_n)$，其中 $s = \mathrm{sig}_\sigma(m')$，显然 $\mathrm{ver}(y,s,m') = \mathrm{True}$。证毕

4 康莉等人的第 1 类盲代理多重签名方案[7]

4.1 参数设置

参数 $\{p, q, g, x_i, y_i, A_i, \mathrm{sig}_\sigma(m), \mathrm{ver}(y,s,m)\}$ 同 2.1 节，并设 $B, B_1, B_2, \cdots, B_n$ 为代理签名者。

4.2 委托过程

(1) 每个原始签名人 $A_i\ (1 \le i \le n)$ 随机选择一个数 $k_i \in {}_R Z_q^*$；计算 $K_i = g^{k_i} \bmod p$，并把 K_i 发送给相应的代理签名人 B_i；

(2) $B_i\ (1 \le i \le n)$ 随机选择 $\alpha_i, \beta_i, \lambda_i \in Z_q^*$，计算 $R_i = \lambda_i g^{\alpha_i} K_i^{\beta_i} \bmod p$，$\tilde{\lambda}_i = R_i \beta_i^{-1} \bmod q$，并将 $\tilde{\lambda}_i$ 发送给 A_i；

(3) $A_i\ (1 \le i \le n)$ 计算 $\overline{\sigma}_i = \overline{\lambda}_i x_i + k_i \bmod q$，并将 $\overline{\sigma}_i$ 发送给对应的 B_i；

(4) $B_i\ (1 \le i \le n)$ 计算 $\sigma_i = \overline{\sigma}_i \beta_i + \alpha_i \bmod q$，并验证 $g^{\sigma_i} = y_i^{R_i} R_i \lambda_i^{-1} \bmod p$ 是否成立，若成立，则表示代理密钥 $(\sigma_i, R_i, \lambda_i)$ 是有效的。

4.3 盲代理多重签名的生成过程及验证

(1) $B_i\ (1 \le i \le n)$ 随机选择 $d_i \in Z_p^*$，计算 $D_i = g^{d_i} \bmod p$，并将 D_i 发送给其他用户 $B_j\ (j \ne i)$；

(2) $B_i\ (1 \le i \le n)$ 在收到所有的 $D_j\ (j \ne i)$ 以后，计算 $D = D_1 D_2 \cdots D_n \bmod p$；

(3) $B_i\ (1 \le i \le n)$ 计算 $s_i = \sigma_i m - d_i D \bmod q$，并将 $(R_i, \lambda_i, D_i, s_i)$ 发送给某个特定的用户 B；

(4) B 收到所有的 $(R_i, \lambda_i, D_i, s_i)\ (1 \le i \le n)$ 后，计算 $D = D_1 D_2 \cdots D_n \bmod p$，并检验等式 $\left(y_i^{R_i} R_i \lambda_i^{-1}\right)^m = D_i^D g^{s_i} \cdot \bmod p (1 \le i \le n)$ 是否成立，若都成立，B 计算 $s = \sum_{i=1}^n s_i \cdot \bmod q$，那么以 $(m, s, R_1, R_2, \cdots, R_n, \lambda_1, \lambda_2, \cdots, \lambda_n, D)$ 作为对消息 m 的盲代理多重签名。

验证人在收到签名 $(m, s, R_1, R_2, \cdots, R_n, \lambda_1, \lambda_2, \cdots, \lambda_n, D)$ 后，计算 $v = \prod_{i=1}^n y_i^{R_i} R_i \lambda_i^{-1} \bmod p$，并验证等式 $v^m = D^D g^s \bmod p$ 是否成立，若成立，则签名有效。

5 对康莉等人的第 1 类盲代理多重签名方案的分析

定理 2 攻击者可以伪造任何代理签名者的有效子代理密钥，从而冒充该代理签名者生成有效部分盲代理多重签名。

证明 不失一般性，不妨设攻击者欲伪造代理签名者 $B_i\ (1 \le i \le n)$ 的子代理密钥，过程如下：

攻击者首先通过公开渠道获得原始签名者 A_i 的公钥 y_i，然后任选 $R_i \in Z_p^*$，$\gamma_i \in Z_q^*$，并计算 $y_i^{R_i} R_i \bmod p$，最后令

$\lambda_i = y_i^{R_i} R_i g^{\gamma_i} \bmod p$，$\sigma_i = -\gamma_i \bmod q$。

由于

$$y_i^{R_i} R_i \lambda_i^{-1} \bmod p = y_i^{R_i} R_i (y_i^{R_i} R_i g^{\gamma_i})^{-1} \bmod p$$
$$= g^{-\gamma_i} \bmod p = g^{\sigma_i} \bmod p$$

所以$\left(\sigma_i, R_i, \lambda_i\right)$为有效的子代理密钥，从而攻击者可以冒充代理签名者生成有效部分盲代理多重签名。　　证毕

定理 3　攻击者可以独自伪造有效盲代理多重签名。

证明　假定攻击者欲伪造对消息 m' 的盲代理多重签名，攻击过程如下：

(1)攻击者首先通过公开渠道获得原始签名者 $A_1, A_2, \cdots, A_n$ 的公钥 $y_1, y_2, \cdots, y_n$，并任选 $R_1, R_2, \cdots, R_n \in Z_p^*$，$\lambda_2, \lambda_3, \cdots, \lambda_n \in Z_q^*$；

(2)攻击者任选 $d, \eta \in Z_q^*$，并计算 $D = g^d \bmod p$，$\lambda_1 = g^{-\eta} y_1^{R_1} R_1 \prod_{i=2}^{n} y_i^{R_i} R_i \lambda_i^{-1} \bmod p$；

(3)攻击者计算 $s = \eta m' - dD \bmod q$。

则攻击者伪造的对消息 m' 的盲代理多重签名为$\left(m', s, R_1, R_2, \cdots, R_n, \lambda_1, \lambda_2, \cdots, \lambda_n, D\right)$。

由于

$$\left(\prod_{i=1}^{n} y_i^{R_i} R_i \lambda_i^{-1} \bmod p\right)^{m'}$$
$$= \left(\left(\prod_{i=2}^{n} R_i y_i^{R_i} \lambda_i^{-1}\right) y_1^{R_1} R_1 \lambda_1^{-1} \bmod p\right)^{m'}$$
$$= \left(\left(\prod_{i=2}^{n} R_i y_i^{R_i} \lambda_i^{-1}\right) y_1^{R_1} R_1 \left(g^{-\eta} y_1^{R_1} R_1 \prod_{i=2}^{n} y_i^{R_i} R_i \lambda_i^{-1}\right)^{-1} \bmod p\right)^{m'}$$
$$= \left(g^{\eta} \bmod p\right)^{m'} = \left(g^{(s+dD)(m')^{-1}} \bmod p\right)^{m'} = D^D g^s \bmod p$$

即 $v^{m'} = D^D g^s \bmod p$，因此伪造的盲代理多重签名有效。　　证毕

6　康莉等人的第 2 类盲代理多重签名方案[7]

6.1 参数设置

参数设置同 4.1 节。

6.2 委托过程

(1)每个原始签名人 A_i $\left(1 \le i \le n\right)$ 随机选择 $k_i \in {}_R Z_q^*$，计算 $K_i = g^{k_i} \bmod p$，并把 K_i 发送给代理签名人 B；

(2) B 随机选择 $\alpha_i, \beta_i, \lambda_i \in Z_q^*$，计算 $R_i = \lambda_i g^{\alpha_i} K_i^{\beta_i} \bmod p$，$\tilde{\lambda}_i = R_i \beta_i^{-1} \bmod q$，并将 $\tilde{\lambda}_i$ 发送给 A_i；

(3) A_i $\left(1 \le i \le n\right)$ 计算 $\overline{\sigma}_i = \overline{\lambda}_i x_i + k_i \bmod q$，并将 $\overline{\sigma}_i$ 发送给 B；

(4) B 计算 $\sigma_i = \overline{\sigma}_i \beta_i + \alpha_i \bmod q$，并验证 $g^{\sigma_i} = y_i^{R_i} R_i \cdot \lambda_i^{-1} \bmod p$，若所有的子代理密钥$\left(\sigma_i, R_i, \lambda_i\right)$都有效，$B$ 计算代理密钥 $\sigma = \sum_{i=1}^{n} \sigma_i$，验证公钥为 $v = \prod_{i=1}^{n} y_i^{R_i} R_i \lambda_i^{-1} \cdot \bmod p$。

6.3 盲代理多重签名产生及验证过程

对于消息 m，B 计算 $s = \mathrm{sig}_\sigma(m)$，则 $(m, s, R_1, \cdots, R_n, \lambda_1, \cdots, \lambda_n)$ 是 B 作为 $A_1, A_2, \cdots, A_n$ 的代理签名人产生的有效盲代理多重签名。

验证人收到盲代理多重签名 $(m, s, R_1, \cdots, R_n, \lambda_1, \cdots, \lambda_n)$ 后，计算 $v = \prod_{i=1}^{n} y_i^{R_i} R_i \lambda_i^{-1} \bmod p$，若 $\mathrm{ver}(v, s, m) = \mathrm{True}$，则签名有效。

7　对康莉等人的第 2 类盲代理多重签名方案的分析

定理 4　攻击者可以通过伪造代理密钥的方式伪造有效的盲代理多重签名。

证明　假定攻击者欲伪造对消息 m' 的盲代理多重签名，伪造过程如下：

(1)攻击者首先通过公开渠道获得原始签名者 $A_1, A_2, \cdots, A_n$ 的公钥 $y_1, y_2, \cdots, y_n$，并任选 $R_1, R_2, \cdots, R_n \in Z_p^*$，$\lambda_2, \lambda_3, \cdots, \lambda_n \in Z_q^*$；

(2)攻击者任选 $\eta \in Z_q^*$，计算 $\lambda_1 = g^{-\eta} y_1^{R_1} R_1 \prod_{i=2}^{n} y_i^{R_i} R_i \lambda_i^{-1} \cdot \bmod p$，并令 $\sigma = \eta \bmod q$；

(3)攻击者计算 $s = \mathrm{sig}_\sigma(m')$，伪造的盲代理多重签名为 $(m', s, R_1, \cdots, R_n, \lambda_1, \cdots, \lambda_n)$。

由于

$$v = \prod_{i=1}^{n} y_i^{R_i} R_i \lambda_i^{-1} \bmod p = \left(\prod_{i=2}^{n} R_i y_i^{R_i} \lambda_i^{-1}\right) y_1^{R_1} R_1 \lambda_1^{-1} \bmod p$$
$$= \left(\prod_{i=2}^{n} R_i y_i^{R_i} \lambda_i^{-1}\right) y_1^{R_1} R_1 \left(g^{-\eta} y_1^{R_1} R_1 \prod_{i=2}^{n} y_i^{R_i} R_i \lambda_i^{-1}\right)^{-1} \bmod p$$
$$= g^{\eta} \bmod p = g^{\sigma} \bmod p$$

即 (σ, v) 为有效的代理密钥对，所以 $\mathrm{ver}(v, s, m') = \mathrm{True}$。　　证毕

8　结束语

盲代理多重签名在电子商务和电子投票系统中具有一定的应用价值，本文对他人提出的 3 种盲代理签名方案进行了密码分析，分别指出了它们存在的安全漏洞。考虑进一步的研究工作，希望设计出可证明安全的盲代理签名方案。

参 考 文 献

[1] Mambo M, Usuda K, and Okmoto E. Proxy signatures: Delegation of the power to sign messages [J]. *IEICE Trans. on Fundamentals of Electronic Communications and Computer Sciences*, 1996, E79-A(9): 1338–1354.

[2] 谷利则, 张胜, 杨义先. 一种新型的代理签名方案[J]. 电子与信息学报, 2005, 27(9): 1463–1466.
Gu Li-ze, Zhang Sheng, and Yang Yi-xian. A new type of proxy signature scheme [J]. *Journal of Electronics & Information Technology*, 2005, 27(9): 1463–1466.

[3] Hsu C L, Tsai K Y, and Tsai P L. Cryptanalysis and

improvement of nonrepudiable threshold multi-proxy multi-signature scheme [J]. *Journal of Systems and Software*, 2007, 177(2): 543–549.

[4] Lu E J L, Hwang M S, and Huang C J. A new proxy signature scheme with revocation [J]. *Applied Mathematics and Computation*, 2005, 161(3): 799–806.

[5] 伊丽江. 代理签名体制及应用研究[D]. [博士论文], 西安电子科技大学, 2000.
Yi Li-jiang. Study on proxy signature schemes and their applications [D]. Xi'dian University, 2000.

[6] 李媛, 尹为民. 一种具有双重性质的盲代理签名[J]. 计算机应用研究, 2003, 20(11): 16–19.
Li Yuan and Yin Wei-min. A kind of blind proxy signature with dual property [J]. *Application Research of Computers*, 2003, 20(11): 16–19.

[7] 康莉, 蔡勉, 王亚军. 基于 Nyberg-Rueppel 签名体制的盲代理多重签名[J]. 通信学报, 2007, 28(3): 116–119.
Kang Li, Cai Mian, and Wang Ya-jun. Blind proxy multi-signature schemes based on Nyberg-Rueppel signature scheme[J]. *Journal on Communications*, 2007, 28(3): 116–119.

王天银： 男，1979 年生，博士生，研究方向为密码学.

刘麦学： 男，1953 年生，教授，主要从事代数和组合数学研究.

温巧燕： 女，1959 年生，教授，博士生导师，主要研究方向为密码学与信息安全.