对一类基于离散对数的代理盲签名体制的伪造攻击

傅晓彤，卢明欣，肖国镇
(西安电子科技大学 综合业务网国家重点实验室,陕西 西安 710071)

摘要：对 Tan 等人的代理盲签名方案,提出了一种伪造攻击,利用该伪造攻击,不诚实的原始签名人可以成功伪造代理签名密钥,从而能够假冒合法代理签名人生成验证有效的代理盲签名,威胁到代理签名人的合法权益. 进而针对所提出的伪造攻击,对 Tan 等人的代理盲签名方案进行改进,克服了代理委托过程中造成代理签名密钥可伪造的因素,即 $\bar{r}$ 的选择性构造,设计了一个新的代理盲签名方案.

关键词：安全性分析;代理盲签名;代理签名;数字签名
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1001-2400(2005)05-0777-04

Forgery attack on a proxy-blind signature scheme

FU Xiao-tong, *LU Ming-xin*, *XIAO Guo-zhen*
(State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China)

Abstract: We propose a forgery attack on a proxy blind signature scheme proposed by Tan et al. By using the forgery attack, a dishonest original signer can forge the proxy signing key and produce valid proxy blind signatures. By successfully identifying the forgery attack, we show that their scheme is insecure. Furthermore, to improve Tan et al's scheme, we propose an improved proxy blind signature scheme.

Key Words: security analysis; proxy blind signature; proxy signature; digital signature

Mambo, Usuda 和 Okamoto 在 1996 年首次提出了代理签名的概念[1]. 代理签名人可以代表原始签名人对消息进行代理签名. 代理签名的基本方法是原始签名人对委托信息(一般是代理签名人的身份信息或其他有效的委托信息)生成一个签名,并将其秘密地交给代理签名人,代理签名人直接使用该签名作为代理私钥,或者用该签名生成一个代理私钥进行代理签名. 这样,代理签名人就可以应用代理签名密钥通过选定的代理签名方案对消息生成代理签名. 代理签名体制具有广泛的应用性,如在电子货币系统中[2],电子商务的移动代理中[3],移动通信[4],格计算,全球分布式网络以及分布式计算等系统中都涉及代理签名的应用[5,6].

1 TLT 代理盲签名方案

设待签名的消息为 m. 安全参数：p, q 为两个大素数,且 $q \mid (p-1)$;g 为 GF(q) 的本原元;h 为一个安全的 Hash 函数;$\|$ 表示比特串的并;A 为原始签名人;B 为代理签名人;$x_A, x_B \in [1, p-1]$ 为原始签名人和代理签名人的私钥,相应的公钥分别为：$y_A = g^{x_A} \bmod p$ 和 $y_B = g^{x_B} \bmod p$. 授权过程如下[7]：

(1) 委托生成：原始签名人 A 随机选择 $\bar{k} \in Z_q^*$,计算 $\bar{r} = g^{\bar{k}} \bmod p$, $\bar{s} = (x_A \bar{r} + \bar{k}) \bmod q$.

(2) 代理传送：A 通过一个安全信道将($\bar{r}$, $\bar{s}$) 发送给代理签名人 B.

(3) 代理验证：B 检验 $g^{\bar{s}} = \bar{r}\, y_A^{\bar{r}} \bmod p$,如果等式成立,$B$ 则接受($\bar{r}$, $\bar{s}$),并计算 $s_P = (\bar{s} + x_B) \bmod q$ 作为他的代理签名私钥.

相应的代理签名公钥为 $y_P = g^{s_P} = g^{\bar{s}} g^{x_B} = \bar{r}\, y_A^{\bar{r}}\, y_B \bmod p$. 接收者可以通过 A 和 B 的公钥 y_A, y_B 以及公

收稿日期：2004-10-23
基金项目：国家重点基础研究发展规划资助项目(G1999035804);国家自然科学基金重大资助项目(90104005)
作者简介：傅晓彤(1977-),女,讲师,博士.

开信息 $\bar{r}$ 计算 y_P.

代理签名生成过程:TLT 方案的签名和提取过程实质上就是用代理签名密钥 s_P 作为签名密钥生成的 Schnorr 盲签名.

(1) B 随机选取 $k \in Z_q^*$,计算: $t = g^k \bmod p$. (1)

(2) B 发送($\bar{r}$, t) 给代理盲签名接收方 R.

(3) R 选择随机数 a, $b \in Z_q^*$, 计算:

$$r = t\, g^b\, y_B^{-a-b} (\bar{r}\, y_A^{\bar{r}})^{-a} \bmod p \quad , \quad e = H(r \parallel m) \bmod q \quad ,$$

$$u = (\bar{r}\, y_A^{\bar{r}})^{-c+b}\, y_A^{-c} \bmod p \quad , \quad e^* = (e - a - b) \bmod q \quad .$$

如果 $r = 0$,接收方 R 将重新选择 a 和 b,当 r, a 和 b 确定之后,R 发送 e^* 给代理签名人 B.

(4) B 接收到 e^* 后,用与式(1) 中相同的 k 计算 $s'' = (e^*\, s_P + k) \bmod q$,并发送 s'' 给 R.

(5) 生成代理盲签名:R 利用接收到的 s'' 计算 $s = (b + s'') \bmod q$,(m, s, u, e) 就是一个有效的代理盲签名.

代理签名的验证过程 验证者 V 接收到(m, s, u, e) 之后,验证 $e = h(g^s\, y_B^{-e}\, y_A^e\, u \parallel m) \bmod q$. 如果等式成立,$V$ 接受(m, s, u, e),否则拒绝接受(m, s, u, e).

2 伪造攻击

在上面的盲代理签名体制中,作者宣称他们的方案满足多种安全性质,包括不可伪造性,即任何人(甚至原始签名人) 冒充代理签名人生成有效代理签名的概率仅为 $1/q$. 针对不可伪造性提出一种伪造攻击,利用该伪造攻击,不诚实的原始签名人可以成功伪造代理签名密钥,从而能够生成有效的代理签名,即 TLT 代理盲签名方案不满足不可伪造性这一安全性需求.

2.1 伪造代理签名密钥

为伪造代理签名,首先伪造一个有效的代理签名私钥 $\tilde{s}_P$.

不诚实的原始签名人 A 随机选择 $c \in_R Z_q^*$, 进行如下计算.

(1) 计算 $\bar{r} = g^c\, y_B^{-1} \bmod p$.

(2) 计算 $\tilde{s}_P = (x_A\, \bar{r} + c) \bmod q$.

$\tilde{s}_P$ 就是一个有效的代理签名密钥.

相应的公钥为 $\tilde{y}_P = \bar{r}\, y_A^{\bar{r}}\, y_B (= g^{\tilde{s}_P} \bmod p)$. (2)

这是因为 $\tilde{y}_P = \bar{r}\, y_A^{\bar{r}}\, y_B = g^c\, y_B^{-1}\, y_A^{\bar{r}}\, y_B = g^{x_A \bar{r} + c} = g^{\tilde{s}_P} \bmod p$.

于是 ($\tilde{s}_P$, $\tilde{y}_P$) 是一个有效的代理签名密钥对. 即 $\tilde{s}_P = x_A\, \bar{r} + c$ 是一个有效的代理签名私钥. 假冒代理签名人 B 生成有效的代理盲签名时,不诚实的原始签名人 A 使用上述方法所伪造的代理签名私钥 $\tilde{s}_P$ 与签名接收方 R 交互作用生成代理盲签名.

2.2 生成代理盲签名

(1) A 选择随机数 $k \in Z_q^*$,计算: $t = g^k \bmod p$, (3)

并将 ($\bar{r}$, t) 发送给 R.

(2) R 选择两个随机数 a, $b \in Z_q^*$, 计算:

$$r = t\, g^b\, y_B^{-a-b} (\bar{r}\, y_A^{\bar{r}})^{-a} \bmod p \quad , \tag{4}$$

$$e = H(r \parallel m) \bmod q \quad , \tag{5}$$

$$u = (\bar{r}\, y_A^{\bar{r}})^{-c+b}\, y_A^{-c} \bmod p \quad , \tag{6}$$

$$e^* = (e - a - b) \bmod q \quad . \tag{7}$$

如果 $r = 0$, R 重新选择 a 和 b 重复执行上述步骤. 当 r, a 和 b 确定之后,R 计算并发送 e^* 给假冒的代理签名

人 A.

(3) A 收到 e^* 后,计算:

$$\tilde{s}'' = (e^* \tilde{s}_P + k) \bmod q \quad , \tag{8}$$

发送 $\tilde{s}''$ 给 R.

(4) R 收到 $\tilde{s}''$ 后,计算:

$$\tilde{s} = (b + \tilde{s}'') \bmod q \quad , \tag{9}$$

四元组 $(m, \tilde{s}, u, e)$ 就是一个有效的代理盲签名.

2.3　验证过程

代理盲签名的接收者通过如下等式是否成立来验证伪造的签名四元组 $(m, \tilde{s}, u, e)$ 是否是一个合法有效的代理盲签名:$e = h(g^{\tilde{s}} y_B^{-e} y_A^e u \| m) \bmod q$. 也即如果 $r = g^s y_B^{-e} y_A^e u \bmod p$ 成立,则上述验证等式成立.

利用式(2) ~ (9)可以证明如下:

$$\begin{aligned} g^{\tilde{s}} y_B^{-e} y_A^e u &= g^{b+\tilde{s}''} y_B^{-e} y_A^e u = g^{b+(e^*\tilde{s}_P+k)} y_B^{-e} y_A^e u = \\ & g^b g^k (g^{\tilde{s}_P})^{e^*} y_B^{-e} y_A^e u = g^b g^k (\bar{r} y_A^{\bar{r}} y_B)^{e^*} y_B^{-e} y_A^e u = \\ & g^k g^b (\bar{r} y_A^{\bar{r}})^{e^*} y_B^{e^*-e} y_A^e u = g^k g^b y_B^{-a-b} (\bar{r} y_A^{\bar{r}})^{e-a-b} y_A^e (\bar{r} y_A^{\bar{r}})^{-e+b} y_A^{-e} = \\ & g^k g^b y_B^{-a-b} (\bar{r} y_A^{\bar{r}})^{-a} = t g^b y_B^{-a-b} (\bar{r} y_A^{\bar{r}})^{-a} = r \bmod p \quad . \end{aligned}$$

因此,可以看到通过上述验证,验证者将接受 $(m, \tilde{s}, u, e)$ 为代理签名人 B 生成的有效代理盲签名. 不诚实的原始签名人 A 成功的伪造了有效的代理盲签名. 有如下结论:

结论　在 TLT 方案中,一个不诚实的原始签名人 A 可以成功的冒充代理签名人伪造出代理签名的概率为 1. 任何接收者通过验证将接受该签名为合法代理签名人的有效代理签名.

3　改进方案

从第 2 小节的分析和伪造过程可以看出,TLT 代理盲签名方案的不安全性在于不诚实的原始签名人能够成功伪造验证有效的代理签名密钥对. 通过对参数 $\bar{r}$ 的构造,伪造满足代理签名密钥验证条件的 $\tilde{s}_P$,以及相应的签名公钥 $\tilde{y}_P = \bar{r} y_A^{\bar{r}} y_B = g^{\tilde{s}_P}$. 针对这一伪造攻击,给出一个改进的代理盲签名方案. 该方案基于 Mambo-Okamoto[6] 代理签名方案进行代理签名权利的委托. 代理签名人生成自己的代理签名私钥 s_P. 代理签名公钥为 $y_P = y_A \bar{r}^{\bar{r}} y_B \bmod q$,不同于 TLT 方案中 $\bar{r} y_A^{\bar{r}} y_B$ 里 $\bar{r}$ 的出现形式,这样,不诚实的原始签名人对 $\bar{r}$ 的选择性构造不再能够成功伪造有效的代理签名密钥对. 这是因为 $\bar{r}$ 在 y_P 中的出现形式为 $\bar{r}^{\bar{r}}$,避免了在验证伪造的 s_P 所对应的 y_P 时抵消关于代理签名人 B 的信息 y_B. 从而可以安全地进行代理盲签名,保证了代理签名人的合法权益. 改进方案中涉及的安全参数与 TLT 方案相同. 授权过程如下:

(1) 委托生成:原始签名人 A 随机选择 $\bar{k} \in Z_q^*$,计算 $\bar{r} = g^{\bar{k}} \bmod p$,$\bar{s} = (x_A + \bar{r}\bar{k}) \bmod q$.

(2) 代理传送:A 通过一个安全信道将 $(\bar{r}, \bar{s})$ 发送给代理签名人 B.

(3) 代理验证:B 检验 $g^{\bar{s}} = y_A \bar{r}^{\bar{r}} \bmod p$,如果等式成立,$B$ 则接受 $(\bar{r}, \bar{s})$,并计算 $s_P = (\bar{s} + x_B) \bmod q$ 作为他的代理签名私钥.

相应的代理签名公钥为 $y_P = y_A \bar{r}^{\bar{r}} y_B \bmod p$.

代理盲签名的生成和验证过程与方案所选择的普通盲签名方案的签名和验证过程相同. 例如选择 Schnorr 盲签名方案,则代理盲签名的生成和验证过程将与 TLT 方案类似. 这里不再赘述.

4　结　　论

指出了谭作文等人提出的代理盲签名方案是不安全的. 不诚实的原始签名人能够伪造代理签名密钥,从而假冒代理签名人生成验证有效的代理盲签名. 针对这一不安全性,给出了一个改进方案,避免了代理签名私钥生成过程中造成其可伪造的因素,保护了代理签名人的利益.

参考文献：

[1] Mambo M, Usuda K, Okamoto E. Proxy Signature：Delegation of the Power to Sign Messages[J]. IEICE Trans Fundations, 1996, 79-A(9)：1 338-1 353.

[2] Sun H M, Hsieh B T. On the Security of Some Proxy Signature Schemes[DB/OL]. http：//eprint. iacr. org/2003/068, 2003-11-05.

[3] Lee B, Kim H, Kim K. Strong Proxy Signature and Its Applications[DB/OL]. http：//caislab. icu. ac. kr, 2003-11-05.

[4] Parkand H U, Lee I Y. A Digital Nommative Proxy Signature Scheme for Mobile Communications[A]. Proc ICICS'01[C]. Heidelberg：Springer-Veralg, 2001. 451-455.

[5] Fu Xiaotong, Yi Lijiang, Xiao Guozhen. A New Type of Proxy Multi-Signature Schemes[J]. Journal of Xidian University, 2001, 28(6)：729-731.

[6] Mambo M, Okamoto E. Proxy Crytposystems：Delegation of the Power to Decrypt Ciphertexts[J]. IEICE Trans Fundations, 1997, E80-A(1)：54-63.

[7] Tan Zuowen, Liu Zhuojun, Tang Chunming. A Proxy Blind Signature Scheme Based on DLP[J]. Journal of Software, 2003, 14(11)：1 931-1 935.

(编辑：李维东)

《西安交通大学学报》2004 年第 12 期目录