第33卷 第12期 计 算 机 工 程 2007年6月
Vol.33 No.12 Computer Engineering June 2007
·安全技术· 文章编号：1000—3428(2007)12—0178—02 文献标识码：A 中图分类号：TP309

一种新型代理签名方案的密码分析及改进

王天银[1]，蔡晓秋[1,2]，张建中[2]
(1. 洛阳师范学院数学科学学院，洛阳 471022；2. 陕西师范大学数学与信息科学学院，西安 710062)

摘 要：对最近提出的一种新型代理数字签名方案——匿名代理数字签名方案进行了密码分析，发现该方案存在安全漏洞：原始签名者可以伪造其指定的代理签名者的有效代理数字签名，还可以诬陷其他任何人为其指定的代理签名者。对该方案进行了改进，安全性分析表明，改进后的方案可以抵抗原始签名者的伪造攻击，并且保留了原方案的一些优点。

关键词：匿名代理签名；可识别性；可跟踪性；伪造攻击

Cryptanalysis and Improvement of New Proxy Signature Scheme

WANG Tianyin[1], CAI Xiaoqiu[1,2], ZHANG Jianzhong[2]
(1. Mathematical Science College, Luoyang Normal University, Luoyang 471022;
2. College of Mathematics and Information Science, Shanxi Normal University, Xi'an 710062)

【Abstract】 Through the cryptanalysis of a new proxy digital signature scheme—anonymous proxy signature digital scheme proposed recently, it is found that this scheme has security leaks and the original signer can not only forge the proxy signer's valid proxy signature, but also frame anyone else as his designated proxy signer. An improvement is given, and the security analysis shows that it can resist the forgery attacks and retains some merits of the original scheme.

【Key words】 Anonymous proxy signature; Indentifiability; Traceability; Forgery attack

1996年，Mambo等提出了代理签名的概念[1,2]，给出了解决数字签名权力委托的有效方法。由于代理签名在移动通信、移动代理、电子商务等方面有着重要的应用，因此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，成果丰硕。迄今已有多种代理签名体制，如代理多签名体制、代理盲签名体制等[3]。

文献[4]给出了一种新型的代理签名方案(G-Z-Y方案)，它在代理签名中隐藏代理签名者的信息，验证者无法从代理签名中识别代理者身份，在出现争议时，验证者可以通过原始签名者揭示代理签名者的身份。这种新型的代理签名方案在实际中适用于一些特殊的场合，具有一定的应用价值。但本文分析发现：该方案不能抵抗原始签名者的伪造攻击，原始签名者可以伪造代理签名者的有效代理签名，并且可以随意修改授权书的内容，而代理签名者无法否认该签名，这对代理签名者很不公平；原始签名者还可以诬陷任何人为其指定的代理签名者。本文对G-Z-Y方案进行了改进，改进后的方案可以解决原方案存在的安全漏洞。

1 G-Z-Y方案

1.1 参数设置

p、q为安全大素数，且q|p-1；g为域$GF(p)$中阶为q的元；h为安全的Hash函数；m_w为授权书(详细描述了代理的诸多事宜)；A、B、V分别表示原始签名者、代理签名者、签名验证者；(x_A,y_A)、(x_B,y_B)分别为原始签名者和代理签名者的公私钥对，且$y_A=g^{x_A} \bmod p$，$y_B=g^{x_B} \bmod p$；x_P为原始签名者和代理签名者共同生成的代理私钥，y_P为x_P对应的公钥，且$y_P=g^{x_P} \bmod p$；ID_B为代理签名者B的标志，ID_P为代理签名者P的标志；$Sig(x,m)$为基于离散对数的数字签名算法，其中，x为签名私钥，m为签名的消息，签名返回值为σ；$Ver(y,\sigma,m)$为验证算法，y为签名者公钥，返回值为真或假。

1.2 代理密钥对的生成

(1)原始签名者A通过安全通道向代理签名者B发送代理授权书m_w，B收到m_w后，秘密计算自己的代理密钥s_B和r_1、s_1，计算过程如下：

$k_B \in_R Z_q^*$，$r_B=g^{k_B} \bmod p$，$s_B=x_B+k_B r_B \bmod q$

$k_1 \in_R Z_q^*$，$r_1=g^{k_1} \bmod p$，$s_1=x_B h(r_B,ID_B,r_1)+k_1 \bmod q$

B将(r_B,ID_B,r_1,s_1)返回给A后，A验证

$g^{s_1} \stackrel{?}{=} y_B^{h(r_B,ID_B,r_1)} r_1 \bmod p$

若成立，A秘密保存(r_B,y_B,ID_B)以备日后需要时揭示代理签名者身份，再计算$Y_P=y_B r_B^{r_B} \bmod p$，并把$Y_P$写入$m_w$中。

(2)原始签名者A对增添Y_P的m_w进行签名，过程如下：

$k_A \in_R Z_q^*$，$r_A=g^{k_A} \bmod p$，$s_A=x_A h(m_w,r_A)+k_A \bmod q$

然后A把(r_A,s_A)以及m_w通过安全信道发送给B，B验证

$g^{s_A} \stackrel{?}{=} y_A^{h(m_w,r_A)} r_A \bmod p$

若成立B秘密保存(r_A,s_A,m_w,s_B)。

(3)代理签名者B生成代理私钥$x_P=s_A+s_B \bmod q$。

1.3 代理签名的生成及验证

若消息m符合代理授权书m_w的约定，代理签名者B利用

基金项目：国家自然科学基金资助项目(10271069)；河南省自然科学基金资助项目(0511010300)
作者简介：王天银(1979－)，男，讲师、硕士，主研方向：密码学；蔡晓秋，硕士生；张建中，博士、教授
收稿日期：2006-07-05 **E-mail：**yinwang790720@yahoo.com.cn

签名算法 Sig，使用代理私钥 x_P 生成代理签名 $\sigma_P = Sig(x_P, m)$，有效的代理签名为 $(m, \sigma_P, m_w, r_A, y_A)$。

验证者 V 首先检验消息 m 是否符合授权书 m_w 的约定，若符合，计算

$$y_P = y_A^{h(m_w, r_A)} r_A Y_P \bmod p \quad (Y_P 从 m_w 中得到)$$

然后验证 $Ver(y_P, \sigma_P, m) \stackrel{?}{=} \text{true}$，若成立，代理签名有效，否则无效。

1.4 揭示代理者身份

验证者 V 向原始签名者 A 提供代理签名 $(m, \sigma_P, m_w, r_A, y_A)$，$A$ 首先验证签名的有效性，若有效，A 从 m_w 中得到 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, ID_B)，判断等式 $Y_P \stackrel{?}{=} y_B r_B^{r_B} \bmod p$，若存在 (r_B, y_B, 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。

2 对 G-Z-Y 方案的密码分析

对于 G-Z-Y 方案，给出了 2 种伪造攻击，证明该方案并不安全。

伪造攻击 1 原始签名者 A 可以伪造代理签名者 B 的对任何消息 m' 有效代理签名，并且可以随意改变授权书 m_w 的内容，而且代理签名者 B 不能否认该签名。

伪造攻击过程如下：

(1)原始签名者 A 任意选择 $r \in Z_q$，计算

$$r_A' = g^r Y_P^{-1} \bmod p = g^r (y_B r_B^{r_B})^{-1} \bmod p$$

(2)原始签名者 A 随意产生授权书 m'_w(包含 Y_P)，计算

$$x_p' = r + xh(m_w', r_A') \bmod q$$

(3)原始签名者 A 利用代理密钥 x_p'，计算出对任意消息 m' 的代理签名 $\sigma_p' = Sig(x_p', m')$，有效的代理签名为 $(m', \sigma_P', m_w', r_A', y_A)$。由于

$$y_p' = y_A^{h(m_w', r_A')} r_A' Y_P \bmod p = y_A^{h(m_w', r_A')} g^r Y_P^{-1} Y_P \bmod p$$

$$= g^{x_A h(m_w', r_A') + r} \bmod p = g^{x_A} \bmod p$$

因此，签名 $(m', \sigma_P', m_w', r_A', y_A)$ 可以通过验证者 V 的验证。

若出现争议，验证者 V 将签名 $(m', \sigma_P', m_w', r_A', y_A)$ 提交给原始签名者 A，由于 $Y_P = y_B r_B^{r_B} \bmod p$，因此，可以揭示出代理签名者 B 的身份，使 B 无法否认该签名。

伪造攻击 2 原始签名者 A 可以诬陷任何人 C 为其指定的代理签名者。

伪造攻击过程如下：

原始签名者 A 任意选择 $r_C \in Z_P^*$，秘密保存 (r_C, y_C, ID_C)，计算

$$Y_P = y_C r_C^{r_C} \bmod p$$

并把 Y_P 写入 m'_w 中，然后原始签名者 A 通过伪造攻击 1 的步骤(1)~步骤(3)伪造出对任何消息 m' 有效代理签名 $(m', \sigma_P', m_w', r_A', y_A)$。

由于 $Y_P = y_C r_C^{r_C} \bmod p$，因此，原始签名人可以声称 C 为其指定的代理签名者，签名 $(m', \sigma_P', m_w', r_A', y_A)$ 是由 C 生成的。

3 改进方案及其密码分析

3.1 改进方案

对 G-Z-Y 方案进行了如下少许但重要的改进：

(1)在 1.2 节步骤(1)中，要求原始签名者 A 不但保存 (r_B, y_B, ID_B)，还保存对 (r_B, ID_B) 的签名 (r_1, s_1)；在 1.4 节揭示代理签名者身份中，要求 A 首先验证 (r_B, ID_B) 的有效性，即验证

$$g^{s_1} \stackrel{?}{=} y_B^{h(r_B, ID_B, r_1)} r_1 \bmod p$$

(2)在 1.2 节步骤(2)中，将原始签名者 A 对增添 Y_P 的授权书 m_w 的签名改为

$$k_A \in_R Z_q^*, \quad r_A = g^{k_A} \bmod p$$

$$s_A = x_A h(m_w, r_A) + k_A r_A \bmod q$$

相应的代理公钥变为

$$y_P = y_A^{h(m_w, r_A) r_A^{r_A}} Y_P \bmod p$$

所有参数及其它过程均不变。

3.2 方案密码分析

由 3.1 节的改进方法可以看出，改进方案满足 G-Z-Y 方案所具有的一切对代理签名的安全性要求。下面分析改进方案可以抵抗本文提出的原始签名者 A 的伪造攻击。

在G-Z-Y方案中，原始签名者 A 的 2 种伪造攻击之所以能够成功，关键是原始签名者 A 可以通过确定 $r_A = g^r Y_P^{-1} \bmod p$，在代理公钥 $y_P = y_A^{h(m_w, r_A)} r_A Y_P \bmod p$ 中消去 Y_P。由于其知道 x_A，可以很容易地计算出代理私钥

$$x_P = r + x_A h(m_A, r_A) \bmod q$$

因此可以伪造有效代理签名。改进后的方案只要能确保原始签名人 A 无法把 Y_P 从代理公钥 $y_P = y_A^{h(m_w, r_A)} r_A Y_P \bmod p$ 中消去即可。

在改进方案中，代理公钥为 $y_P = y_A^{h(m_w, r_A)} r_A^{r_A} Y_P \bmod p$，原始签名者 A 若想消去 Y_P 就必须从下式中求出 r_A：

$$r_A^{r_A} = g^r Y_P^{-1} \bmod p = g^r (y_B r_B^{r_B})^{-1} \bmod p \quad (r \in z_q)$$

由于这是一个离散对数问题，在计算上是不可行的，因此，原始签名者 A 不能通过消去 Y_P 获得代理私钥 x_P，也就不能伪造有效代理签名。

另外，改进方案在揭示代理签名者身份中还要求原始签名者 A 提供对代理签名者身份 ID_p 的有效性证明，由于原始签名者 A 不能伪造 ID_p 的有效签名，因此可以抵抗原始签名者 A 对其他人的诬陷。

4 结束语

代理签名是目前研究的一个热点问题，在实际中有着广泛的应用前景，因此受到广泛的关注。本文针对最近提出的一种新型的代理签名方案，给出了 2 种伪造攻击，证明了该方案的不安全性，并给出了相应的改进方案。

参考文献

1 Mambo M, Usuda K, Okamoto E. Proxy Signatures for Delegating Signing Operation[C]//Proceedings of the 3rd ACM Conference on Computer and Communications Security, New Dehi, India. 1996: 48-57.

2 Mambo M, Usuda K, Okamoto E. Proxy Signatures: Delegation of the Power to Sign Messages[J]. IEICE Trans. on Fundamentals, 1996, E79-A(9): 1338-1354.

3 李继国, 曹珍富, 李建中, 等. 代理签名的现状与进展[J]. 通信学报, 2003, 24(10): 114-124.

4 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.