前向安全的代理签名方案

王晓明[1]，陈火炎[1]，符方伟[2]
（1. 暨南大学 信息科学技术学院，广东 广州 510632；2. 南开大学 数学科学学院，天津 300071）

摘 要：将前向安全的概念引入到代理签名体制，提出了一个前向安全的代理签名方案。新方案能实现即使代理签名人的代理签名密钥被泄露，以前所产生的代理签名依然有效。另外，新方案可以对代理签名的有效时间进行控制。

关键词：密码学；代理签名；前向安全
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2005)11-0038-05

Forward secure proxy signature scheme

WANG Xiao-ming[1], CHEN Huo-yan[1], FU Fang-wei[2]
(1. College of Information Science & Technology, Jinan University, Guangzhou 510632, China;
2. School of Mathematics Science, Nankai University, Tianjin 300071, China)

Abstract: A forward secure proxy signature scheme was proposed combining the concept of forward security with proxy signature. This means even if an adversary has gotten the current proxy signers' key, It could not forge proxy signature pertaining to the past, that is, previous generated proxy signatures remain still valid. Furthermore, the scheme can control the proxy signature time of the proxy singer.

Key words: cryptography; proxy signature; forward security

1 引言

在现实世界里，人们经常需要将自己的某些权利委托给可靠的代理人，让代理人代表本人去行使这些权利。在这些可以委托给他人的权利中包括人们的签名权，例如：某公司的经理需要到外地出差，为了不影响公司的业务，该经理可以委托一个可靠的助手，让该助手在他出差期间代表他在一些重要文件上签名。为了解决这个问题，1996 年 Membo 等人提出了代理签名方案[1,2]。在一个代理签名方案中，一个被指定的代理签名人可以代表原始签名人生成有效的代理签名。由于代理签名体制在许多领域都有着重要的应用，因此，对代理签名的研究引起人们普遍的关注。目前，人们已提出了许多种代理签名方案[1~6]。然而，当代理签名人的代理签名密钥被泄露后，这些方案都不能提供任何保护，也就是说，一旦代理签名密钥被泄露，代理签名密钥所产生的所有代理签名将变成无效。因为如果一个攻击者获得代理签名密钥，他就可以伪造代理签名，人们无法区分真实的代理签名和伪造的代理签名。如何减少由于密钥泄露而带来对系统安全的影响，一直是人们十分关注的研究课题。1997 年，R.Anderson 首次提出了前向安全的概念[7]。前向安全就是把整个有效时间分成若干个周期，在每个周期内使用不同的签名密钥产生签名，而验证签名的公钥在整个有效时间内都保持不变。即使当前周期的签名密钥被泄露，也并不影响此周期前签名的有效性。从而大大地减少了由于签名密钥泄露而对系

收稿日期：2004-05-03；**修回日期**：2005-04-01
基金项目：国家自然科学基金资助项目(60172060)；暨南大学自然科学基金资助项目

统带来的影响。如何将前向安全的特性引入到代理签名体制，至今还没有现成的方案。针对这个问题，本文提出了一个前向安全的代理签名方案。本方案能实现即使代理签名人的代理签名密钥被泄露，以前所产生的代理签名依然有效。

另外，大多数的代理签名方案[1~6]，一旦原始签名人将签名权委托给代理签名人，那么代理签名人就具有对这个签名权的永久代理，这对原始签名人是很不利的。原始签名人只希望代理签名人在某一段时间内具有代理签名权，当这段有效期过后，就收回代理签名权。本文提出的前项安全的代理签名方案可以满足这一要求，可以对代理签名的有效时间进行控制。

2　前向安全签名的概念

设签名密钥为σ_0，公钥 y。将 y 的有效时间分为若干时间段，如 1,2,$\cdots T$。在每个时间段内签名人使用不同的签名密钥σ_i (i=1,2,$\cdots T$)，即第 1 时间段内使用σ_1,第 2 时间段内使用σ_2,$\cdots$第 T 时间段内使用σ_T。而验证签名的公钥 y 在整个有效时间内不变。其中不同的时间段的签名密钥是单向更新的，即由 i 时间段的签名密钥σ_i 求不出第 i–1 时间段的签名密钥σ_{i-1}，而且签名人在第 i 时间段开始，并获得新的签名密钥σ_i 后，就从他的机器中删除σ_{i-1}。这样，即使攻击者在第 i 时间段内入侵用户的机器他也只能得到σ_i,而得不到以前的签名密钥σ_{i-1}，σ_{i-2},$\cdots\sigma_0$。

定义　如存在一个单向签名密钥更新算法 KeyUd，使得签名人可以在第 i 时间段将签名密钥由σ_{i-1} 更新为σ_i=KeyUd(σ_{i-1})，并在不同的时间段内使用不同的签名密钥σ_i 生成签名 Sign(σ_i, m)(m 是信息)，而任何签名验证人都可以用一个不变的公钥 y 及时间段的编号 i 进行验证，即 Sign(σ_i, m)满足等式 Ver[y, i,Sign(σ_i, m), $\underline{m}$]=True，则这个数字签名为一个前向安全数字签名。

3　前向安全的代理签名方案

3.1　初始化阶段

(1) 系统首先选择 n=p_1p_2=(2qp_1'+1)(2qp_2'+1)和一个阶为 q 的 $g\in QR_n$（即 g^q=1 mod n），且 p_1 = p_2= 3mod4，其中 p_1，p_2，p_1'，p_2'，q 都为安全的大素数，QR_n 为模 n 的平方剩余集合，然后选择一个安全的单向散列函数 h，公布(n, q, g, h)。

(2) 设 A 是原始签名人，其身份标识号为 ID_A。A 首先选择随机数 $k_A\in$ [1, n]作为私钥，计算

$$y_A = g^{k_A} \bmod n$$

作为公钥，然后选择一对整数(e, d)，且满足

$$\gcd(e,\phi(n))=1 \qquad ed=1 \mod \phi(n)$$

$$\phi(n)=(p_1-1)(p_2-1)$$

公布(ID_A, y_A, e)。

(3) 设 B 为代理签名人，其身份标识号为 ID_B。B 首先选择随机数 $k_B\in$ [1, n]作为私钥，计算

$$y_B = g^{k_B} \mod n$$

作为公钥，最后 B 公布(y_B, ID_B)。

3.2　授权过程

原始签名人 A 将签名权委托给代理签名人 B，授权过程如下：

(1) A 首先选择时间周期 1,2,$\cdots T$ 和代理终止时间$\tilde{t}$ 。然后计算

$$\sigma_0 = y_B^{k_A} \mod n \quad Y=(\sigma_0^{2^{T+|}} y_A^{ID_B})^{-e} \mod n$$

最后公布 B 为他的代理签名人和参数(T, Y, $\tilde{t}$，ID_B)，并保证任何人不能够更改此参数。

(2) B 首先计算

$$\sigma_0 = y_A^{k_B} \mod n$$

然后验证

$$Y=(\sigma_0^{2^{T+|}} y_A^{ID_B})^{-e} \mod n$$

如等式成立，则σ_0 为代理签名密钥。

3.3　前向安全的代理签名产生过程

设待签名的消息为 m。前向安全的代理签名产生过程如下：

(1) 密钥的更新。在每个周期的开始，代理签名人 B 根据前一周期的密钥计算出此周期的密钥

$$\sigma_i = \sigma_{j-1}^2 \mod n$$

其中，σ_{j-1} 为第 j–1 周期的密钥，σ_j 为第 j 周期的密钥，j=1,2,$\cdots T$。然后，代理签名人更新周期序号(j–1 被更新为 j)，删除前一个周期的密钥σ_{j-1}。

(2) 代理签名。B 选择随机数α_i, $\beta_i \in [1, n]$，计算

$$\begin{cases} r = g^{\alpha_i} \mod n \\ z = \sigma_i g^{\beta_i} \mod n \\ u = h(j \| m \| r \| z \| \tilde{t}) \\ s = \beta_i - \beta_i e - k_{\mathrm{B}} u \mod q \end{cases} \tag{1}$$

则前向安全的代理签名为[j, (m, s, ,u, $\tilde{t}$)]。

注 在每个周期开始时，代理签名人可以预先计算

$$g^{2^{T+1-j}} \mod n$$

在每次代理签名前，代理签名人可以预先计算

$$r = (g^{2^{T+1-j}})^{\alpha_i} \mod n \ , \ z = \sigma_i g^{\beta_i} \mod n$$

3.4 前向安全的代理签名的验证

签名验证人收到[j, (m, s, ,u, $\tilde{t}$)]后，首先判断代理签名权是否在有效期内，即现在时间 t 是否大于$\tilde{t}$，如 $t>\tilde{t}$，则代理签名无效。反之，计算

$$r' = (g^s z^e \ y_{\mathrm{B}}^u)^{2^{T+1-j}} Y(y_{\mathrm{A}}^{ID_{\mathrm{B}}})^e \mod n \tag{2}$$

然后验证

$$u = h(j \| m \| z \| r' \| \tilde{t}) \tag{3}$$

如式(3)成立，则代理签名有效，否则代理签名无效。

4 方案性能的分析

(1) [j, (m, s, ,u, $\tilde{t}$)]是有效的前向安全的代理签名。

证明 为了证明[j, (m, s, ,u, $\tilde{t}$)]是有效的前向安全的代理签名，则需要证明式(3)成立。

根据式(1)和式(2)得

$$\begin{aligned} r' &= (g^{\alpha_i} g^{-\beta_i e} g^{-k_{\mathrm{B}} u} \sigma_i^e g^{\beta_i e} g^{k_{\mathrm{B}} u})^{2^{T+1-j}} Y(y_{\mathrm{A}}^{ID_{\mathrm{B}}})^e \\ &= (g^{\alpha_i} \sigma_i^e)^{2^{T+1-j}} (\sigma_0^{2^{T+1}} y_{\mathrm{A}}^{ID_{\mathrm{B}}})^{-e} (y_{\mathrm{A}}^{ID_{\mathrm{B}}})^e \\ &= (g^{\alpha_i})^{2^{T+1-j}} \mod n = r \end{aligned}$$

根据式(3)和上式得

$$u = h(j \| m \| z \| r \| \tilde{t}) = h(j \| m \| z \| r' \| \tilde{t})$$

则[j, (m, s, ,u, $\tilde{t}$)]是有效的前向安全的代理签名。

(2) 方案具有前向安全的特性

本方案的前向安全是基于强 RSA 假定[8]。

强 RSA 假定 已知 n 和$\alpha \in Z_n^*$，n 为两个大素数的乘积，则找出一个$\beta \in Z_n^*$，且满足$\beta^r = \alpha \bmod n$ (r>1)是一个非常困难的问题。

如果攻击者已获得代理签名人的第 k 周期的密钥σ_k，企图通过 $\sigma_k = \sigma_{k-1}^2 \bmod n$ 求 σ_{k-1}，这是一个强 RSA 假定的问题，所以攻击者无法通过σ_k 获得 j (j<k)周期的密钥σ_j (j<k)。

如果攻击者已获得代理签名人的第 k 周期的密钥σ_k，并用文献[8]中的方法对同一个 r 给出了两个签名(j, s, z, u)和(j, s', z', u')。如这两个签名是有效的，则

$$(g^s z^e \ y_{\mathrm{B}}^u)^{2^{T+1-j}} = (g^{s'} z'^e \ y_{\mathrm{B}}^{u'})^{2^{T+1-j}} \mod n$$

令 $\tilde{s} = s - s'$, $\tilde{u} = u' - u$， $\delta = \left(\frac{z'}{z}\right)^e$，上式可以写为

$$(g^{\tilde{s}} y_{\mathrm{B}}^{\tilde{u}})^{2^{T+1-j}} = \delta^{2^{T+1-j}} \mod n$$

因为 n 是 Blum 整数，所以

$$(g^{\tilde{s}} y_{\mathrm{B}}^{\tilde{u}})^2 = \delta^2 \mod n$$

根据上式可以计算出δ^2 的一个平方根，这与强 RSA 假定矛盾，所以假设错误。因此，即使攻击者获得第 k 周期的代理签名密钥σ_k，他也无法求出 k 周期以前的代理签名代理密钥σ_j (j<k)，或伪造 k 周期以前的代理签名。

(3) 方案能抵抗伪造攻击

假定知(j, m, r, z, $\tilde{t}$, y_{A}, y_{B}, Y)，攻击者企图通过验证式(见式(2),(3))

$$\begin{aligned} r &= r' \\ &= (g^s z^e \ y_{\mathrm{B}}^{h(j \| m \| r \| z \| \tilde{t})})^{2^{T+1-j}} Y(y_{\mathrm{A}}^{ID_{\mathrm{B}}})^e \mod n \end{aligned}$$

求 s，这相当于求解离散对数的问题。若假定(j, m, s z, $\tilde{t}$, y_{A}, y_{B}, Y)，通过上式求 r，这相当于求解离散对数的问题和单向散列函数求反的问题。若假定(j, m, r, s, $\tilde{t}$, y_A, y_B, Y)，通过上式求 z，这相当于大数分解和单向散列函数求反的问题。因此，本方案能抵抗伪造攻击。

(4) 本方案具有限制代理签名期限的功能。签名人通过签发代理签名权的终止期限 $\tilde{t}$，告知签名验证者，代理签名人的代理签名权是否在有效期内，实现了在时间上对代理签名人的控制。

(5) 现有的一些代理签名方案，委托代理签名都采用秘密方式送给代理签名人，而本方案不需用秘密方式送代理签名密钥给代理签名人。代理签名人是通过计算而得到的代理签名密钥

$$\sigma_0 = y_{\mathrm{A}}^{k_{\mathrm{B}}} \mod n$$

并通过原始签名人公开的一些代理参数来验证的(见 3.2 节)。因为代理签名人 B 必须用他的私钥钥 k_{B}，才能计算出正确的代理签名密钥(σ_0)，否则计算出的代理签名密钥不等于原始签名人公开的代理参数 Y 中的σ_0。又因为任何人都无法得到 B 的私钥，所以任何攻击者都不能计算出正确的代理签名密钥。没有正确的代理签名密钥，也就无法产生能通过代理签名验证式的代理签名。因此本方案能抵抗假冒代理签名人事件的发生，而且又不需要安全的通信通道送代理签名密钥，所以方法简单、方便、安全。

(6) 签名接收人在认证签名时必须同时使用原签名人和代理签名人的公钥，使签名权和代理签名权实现了有效地分离。

(7) 方案能抵抗外部攻击。如攻击者想从代理签名人的公钥求解私钥 k_{B}，这相当于求解离散对数的问题。同样攻击者想从公布的

$$Y = (\sigma_0^{2^{T+1}} y_{\mathrm{A}}^{ID_{\mathrm{B}}})^{-e} \mod n$$

求密钥σ_0，这相当于大数分解的问题。如攻击者企图从

$$z = \sigma_i g^{\beta_i} \mod n$$

求σ_j，在不知道β_j 情况下，根本无法求σ_j。因此，本方案能抵抗外部攻击。

5　结束语

本文提出的前向安全的代理签名方案与已往的代理签名方案相比，增加了前向安全特性，对代理签名的有效时间进行了控制。一个代理签名方案具有前向安全的特性在实际中是很有用，例如，在 2000 年 3 月 2 日，用户 A 到一个公证机关，希望公正机关对一个文件进行公证，并希望公证过的文件在 2000 年 3 月 2 日后具有永久的法律效应。我们假设这个公证机关是受国家授权，产生的公证书具有法律效应。公证机关对用户 A 的文件进行公证，并用他的私钥对该文件进行签名产生一个公证书，这里签名方案是采用的普通代理签名方案。然而，不幸的是在 2000 年 8 月 4 日，公正机关的私钥被泄露，显然，用该私钥产生的所有公证书都作废了。因为，公正机关私钥已被泄露，那么攻击者就可能用此私钥伪造公证机关的公证书，人们无法区分那些公证书是真还是假。但是，如果公证机关采用签名方案是具有前向特性，他的私钥是周期更换，那么即使现在这个周期的私钥被泄露，在这个周期以前的私钥还是安全，也就是说，在这个周期以前产生的公证书都是有效的。因为，攻击者无法利用现在被泄露的这个周期的私钥得到这个周期以前的私钥，也就无法伪造公证机关的公证书。从上面例子，可以看到在代理签名方案中引入前向安全是很有用。

参考文献：

[1] MAMBO M, USUDA K, OKAMOTO E. Proxy signature: delegation of the power to sign messages[J]. IEICE Trans Fundamentals, 1996, 79(9): 1338-1354.

[2] MAMBO M, USUDA K, OKAMOTO E. Proxy signature for delegating signing operation[A]. Proc 3rd ACM Conference on Computer and Communications Security[C]. New Delhi: ACM Press, 1996. 48-49.

[3] YI L J, BAI G Q, XIAO G Z. Proxy multi-signature scheme: a new type of proxy signature scheme[J]. Electronics Letters, 2000, 36(6): 527-528.

[4] ZHANG K. Non-repudiable proxy signature schemes[EB/OL]. http://citeseer.nj.nec.com/360090. html, 1999.

[5] ZHANG K. Threshold proxy signature schemes[A]. 1997 Information Security Workshop[C]. Japan, Springer-Verlag, 1997. 191-197.

[6] KIM S, PARK S, WON D. Proxy signature, revisited[A]. Proceedings ICICS'97, Lecture Notes in Computer Science 1334[C]. Berlin: Springer-Verlag, 1997. 223-232.

[7] ANDWESON R. Invited lecture[EB/OL]. http://citeseer. nj.nec.com/anderson06forwarssecure.html, 1997.

[8] KOZLOY A, REYZIN L. Forward secure signature with fast key update[EB/OL]. http://citeseer.nj.nec.com/kozlov02forwarssecure.html, 1998.