第33卷 第21期 计 算 机 工 程 2007年11月
Vol.33 No.21 Computer Engineering November 2007
·安全技术· 文章编号：1000—3428(2007)21—0140—02 文献标识码：A 中图分类号：TP309

一个改进的前向安全的代理签名方案

张晓敏，张建中
(陕西师范大学数学与信息科学学院，西安 710062)

摘 要：指出了一个前向安全签名方案的安全漏洞，认为原方案由于代理签名者的私钥不具有前向安全性，使得整个方案在代理签名者的私钥泄漏后不具有安全性。该文的改进方案对代理签名者的私钥进行了进化，在强RSA假定下，新方案具有真正的前向安全性。
关键词：代理签名；前向安全性；强RSA假定

Improved Forward-secure Proxy Signature Scheme

ZHANG Xiao-min, ZHANG Jian-zhong
(Colledge of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062)

【Abstract】 A secure problem in a forward-secure proxy signature scheme is pointed out, the proxy signer's key does not satisfy the forward-security, so that the original scheme is insecure once the adversary gets the proxy signer's key. The improved scheme proposes an evolution on proxy signer's key, under the strong RSA assumption, the new scheme is truly forward secure.
【Key words】 proxy signature; forward-security; strong RSA assumption

随着计算机网络的普及和数字化时代的到来，如何在网络中实现代理签名权转让成为一个重要问题。1996年，文献[1~2]提出代理签名的概念来解决这一问题。由于代理签名在移动通信、移动代理、电子商务、电子选举、电子拍卖等方面有着重要的应用，因此一经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，取得了丰硕的研究成果[3~5]。

在数字签名系统中，种种原因所造成签名人密钥的泄漏，给系统带来极大的危害。1997年，文献[6]提出了前向安全的数字签名，把整个签名有效时间划分为若干时段，每个时段采用不同的密钥进行签名，而签名验证公钥在整个签名有效期内保持不变。即使当前时段的签名密钥被泄漏，也不影响此签名时段前签名的有效性，从而大大减少了由于密钥泄漏而带来的影响。

基于前向安全的思想，文献[7~9]提出了一些前向安全的代理签名方案，但是目前的前向安全代理签名方案大多不具有真正的前向安全性。文献[9]中提出的前向安全的代理签名方案虽然实现了授权密钥的前向安全，但由于代理签名者的私钥不具有前向安全性，使得整个方案在代理签名者的私钥泄漏后不具有安全性。

1 文献[9]中的方案

文献[9]中提出的前向安全的代理签名方案如下：

初始化阶段：系统选择 $n=p_1p_2=(2qp_1'+1)(2qp_2'+1)$，其中，$p_1\equiv p_2\equiv 3 \bmod 4$；$g$ 是一个 q 阶的元；p_1,p_2,p_1',p_2',q 是安全的大素数；$h(\cdot)$ 是一个安全的 *Hash* 函数，公开 (n,q,g,h)。原始签名人 A 的身份标识为 ID_A，A 随机选择 $k_A\in[1,n]$ 作为私钥，计算 $y_A=g^{k_A} \bmod n$ 作为公钥，选择 (e,d) 满足 $\gcd(e,\varphi(n))=1$，$ed\equiv 1(\bmod \varphi(n))$，公布 (ID_A,y_A,e)。代理签名人 B 的身份标识为 ID_B，B 随机选择 $k_B\in[1,n]$ 作为私钥，计算 $y_B=g^{k_B} \bmod n$ 作为公钥，公布 (ID_B,y_B)。

授权过程：A 选择时间周期 $1,2,\cdots,T$ 及代理终止时间 $\tilde{t}$，计算 $\sigma_0=y_B^{k_A} \bmod n$ 以及 $Y=(\sigma_0^{2^{T+1}}y_A^{ID_B})^{-e} \bmod n$，公布 B 为其代理签名人和参数 $(T,Y,\tilde{t},ID_B)$。

B 计算 $\sigma_0=y_A^{k_B} \bmod n$，并验证等式 $Y=(\sigma_0^{2^{T+1}}y_A^{ID_B})^{-e} \bmod n$ 是否成立，如果等式成立，则 σ_0 为代理签名密钥。

代理签名生成：在第 i 个签名周期开始时，B 计算 $\sigma_i=\sigma_{i-1}^2 \bmod n$ 作为该时段的签名密钥，并删除 σ_{i-1}。设待签名消息为 m，B 随机选择 $\alpha_i,\beta_i\in[1,n]$，计算 $r=g^{2^{T+1-i}\alpha_i} \bmod n$，$z=\sigma_i g^{\beta_i} \bmod n$，$u=h(i\|m\|r\|z\|\tilde{t})$，$s=\alpha_i-\beta_i e-k_B u \bmod q$，消息 m 的前向安全的代理签名为 $(i,m,s,z,u,\tilde{t})$。

代理签名验证：验证人收到 $(i,m,s,z,u,\tilde{t})$ 后首先验证 t 是否超过代理终止时间 $\tilde{t}$，如果超过，则认为签名无效，否则计算 $r'=(g^s z^e y_B^u)^{2^{T+1-i}}Y(y_A^{ID_B})^e \bmod n$，然后验证下面等式是否成立 $u=h(i\|m\|r'\|z\|\tilde{t})$。如果成立则认为签名是有效的。

一方面，该方案由于代理签名者的私钥 k_B 不具有前向安全性，一旦私钥 k_B 泄漏，任何人都可以像 B 一样计算 $\sigma_0=y_A^{k_B} \bmod n$，从而可以伪造任何时段的代理签名，因而是不安全的。另一方面，即使像原始签名者一样知道 σ_0，不知道 k_B 也无法伪造代理签名，因此，对 σ_0 进行进化是无意义的。

2 改进的前向安全的代理签名方案

本文提出一个改进的方案，新方案不对授权密钥进行进

基金项目：国家自然科学基金资助项目(10571113)；陕西省自然科学基金资助项目(2004A14)
作者简介：张晓敏(1981－)，女，硕士研究生，主研方向：密码学；张建中，教授、博士
收稿日期：2006-12-26 **E-mail**：zhangxiaomin81@163.com

化，而是对代理签名者的私钥进行进化，使其具有前向安全性，即使代理签名者在某一时段的签名密钥泄漏，攻击者也无法获得代理签名者前一时段的签名密钥。具体方案如下：

系统初始化： $n, p_1, p_2, p_1', p_2', q, g, h(\cdot)$ 如前所述，$v \in Z_n^*$ 是一随机数，$x_A, x_B \in Z_n^*$ 分别是原始签名者和代理签名者的私钥，$y_A = x_A^{-v} \bmod n$，$y_B = x_B^{-v} \bmod n$ 分别是对应的公钥，系统将密钥有效期划分为 T 个时段，系统的公开参数是 $(n, y_A, y_B, v, q, g, h(\cdot), T)$。

授权过程：

(1)原始签名者 A 选择代理终止时间 $\tilde{t}$，指定 B 为其代理签名者，然后计算 $a = g^{x_A} \bmod n$，公开 $(\tilde{t}, a, ID_B)$；

(2)如果代理签名者 B 愿意接受代理则计算并公布 $b = g^{x_B} \bmod n$；

(3)原始签名者 A 计算 $\sigma = b^{x_A} \bmod n$ 以及 $Y = \sigma^{-v2^{T+1}} y_A^{-1} \bmod n$，并公布 Y；

(4)代理签名者 B 计算 $\sigma = a^{x_B} \bmod n$ 并验证 $Y = \sigma^{-v2^{T+1}} y_A^{-1} \bmod n$ 是否成立，如果等式成立则接受 A 的授权。

代理签名生成： 在第 i 个签名周期开始时，代理签名者 B 首先进行密钥进化，计算 $x_{B_i} = x_{B_{i-1}}^2 \bmod n$ 并立即删除 $x_{B_{i-1}}$，其中 $x_{B_0} = x_B$。

设签名消息为 m，B 选择 $k_i, \alpha_i, \beta_i \in_R Z_n^*$，计算 $r = g^{k_i} \bmod n$，$w = g^{2^{T+1-i}\alpha_i} \bmod n$，$z = x_{B_i} \sigma^{2^i} g^{\beta_i} \bmod n$，$u = h(i \| m \| w \| r \| z \| t)$，$s = \alpha_i - \beta_i v - k_i u \bmod q$，消息 m 的前向安全的代理签名为 (i, m, r, s, z, u, t)，其中，t 是签名时间。

代理签名验证： 验证人收到 (i, m, r, s, z, u, t) 后首先验证 t 是否超过代理终止时间 $\tilde{t}$，如果超过，则认为签名无效，否则计算 $w' = (g^s z^v r^u)^{2^{T+1-i}} y_A y_B^{2^{T+1}} Y \bmod n$，然后验证下面等式是否成立 $u = h(i \| m \| w' \| r \| z \| t)$。如果成立则认为签名是有效的。

3 方案性能分析

本方案的安全性基于以下假设：

强 RSA 假定：已知 n（n 为两个大素数的乘积，其分解未知）和 $c \in Z_n^*$，找出一个 $\alpha \in Z_n^*$ 满足 $\alpha^r \equiv c \bmod n$ 是一个困难问题。

有限域上的离散对数问题：已知 y，p 和 g，找出 $x \in Z_p^*$ 满足 $y = g^x \bmod p$ 是困难问题。

计算式 Diffie-Hellman 问题：已知 g^a 和 g^b，求 g^{ab} 是困难问题。

(1) (i, m, r, s, z, u, t) 是有效的签名。

证明：由 $x_{B_i} = x_{B_{i-1}}^2 \bmod n$ 可知 $x_{B_i} = x_{B_0}^i \bmod n$，由签名过程可知

$$
\begin{aligned}
w' &= (g^s z^v r^u)^{2^{T+1-i}} y_A y_B^{2^{T+1}} Y \bmod n \\
&= (g^{\alpha_i} g^{-\beta_i v} g^{-k_i u} x_{B_i}^v \sigma^{v2^i} g^{\beta_i v} g^{k_i u})^{2^{T+1-i}} y_A y_B^{2^{T+1}} Y \bmod n \\
&= g^{\alpha_i 2^{T+1-i}} x_{B_0}^{v2^{T+1}} \sigma^{v2^{T+1}} y_A y_B^{2^{T+1}} \sigma^{-v2^{T+1}} y_A^{-1} \bmod n \\
&= g^{\alpha_i 2^{T+1-i}} y_B^{-2^{T+1}} y_B^{2^{T+1}} \bmod n \\
&= g^{\alpha_i 2^{T+1-i}} \bmod n \quad = w
\end{aligned}
$$

因此，$u = h(i \| m \| w' \| r \| z \| t)$，$(i, m, r, s, z, u, t)$ 是有效的签名。

(2)该方案具有一般代理签名方案所具有的安全性。

首先，代理权不可伪造，只有原始签名者在代理签名者愿意接受代理的情况下才可以计算代理授权密钥 σ，这是因为已知 g^{x_A} 和 g^{x_B} 而不知道 x_A 或 x_B，由计算式 Diffie-Hellman 问题难解，求 $g^{x_A x_B}$ 是困难的。

其次，代理签名不可伪造。攻击者想伪造代理签名者在第 i 时段的签名，必须得到 x_{B_i}，由 $y_B = x_B^{-v} \bmod n$ 直接得到 x_{B_0}，由强 RSA 假定是困难的；由 $z = x_{B_i} \sigma^{2^i} g^{\beta_i} \bmod n$ 得到 x_{B_i}，由于 σ 和 β_i 未知，是不可行的；此外，如果伪造一个 x_{B_i}，要想通过验证，则必须计算 β_i 满足 $z = x_{B_i} \sigma^{2^i} g^{\beta_i} \bmod n$，由有限域上的离散对数问题难解也是不可行的。

此外，该方案中规定了代理终止时间 $\tilde{t}$，从而具有限制代理权期限的功能；代理授权过程无需安全信道，便于实现；签名验证同时使用原始签名者和代理签名者的公钥，有效地分离了签名权和代理权。

(3)如果代理签名者泄漏了第 i 时段的签名密钥 x_{B_i}，由强 RSA 假定，根据 $x_{B_i} = x_{B_{i-1}}^2 \bmod n$ 计算 $x_{B_{i-1}}$ 是不可行的，因此，该方案还具有前向安全性，第 i 时段的签名密钥 x_{B_i} 泄漏，第 i-1 时段的签名密钥 $x_{B_{i-1}}$ 仍然安全，第 i 时段以前的签名都是安全的。

4 结束语

在代理签名方案中，如何减少由于代理者私钥或是代理授权密钥泄漏所造成的损失是一个急待解决的问题，但是目前的方案大多没有真正实现前向安全。本文在此文献[9]的基础上提出了一个改进的前向安全的代理签名方案，没有权密钥进行进化，而是对代理签名者的私钥进行进化，使得新方案不仅具有一般代理代理签名方案的安全性，而且代理签名者的签名密钥具有真正意义上的前向安全性。在强 RSA 假定、计算式 Diffie-Hellman 问题及有限域上的离散对数问题难解的假设下该方案是安全有效的。

参考文献

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

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

3 Zhang K. Threshold Proxy Signature Schemes[C]//Proc. of 1997 Information Security Workshop, Japan. 1997.

4 Sun H M, Lee N Y, Hwang T. Threshold Proxy Signatures[J]. IEEE Trans. on Computers & Digital Techniques, 1999, 146(5): 259-263.

5 祁 明, Harn L. 基于离散对数的若干新型代理签名方案[J]. 电子学报, 2000, 28(11): 114-115.

6 Anderson R. Two Remarks on Public Key Cryptology[C]//Proc. of the 4th ACM Computer and Communication Security. 1997.

7 Bellare M, Miner S K. A Forward-secure Digital Signature Scheme[C]//Proc. of Advances in Cryptology. 1999.

8 王天银, 张建中. 一个新的前向安全的代理数字签名方案[J]. 计算机工程与应用, 2005, 41(25): 133-135.

9 王晓明, 陈火炎, 符方伟. 前向安全的代理签名方案[J]. 通信学报, 2005, 26(11): 38-42.