第1卷 第4期 信 息 与 电 子 工 程 Vol. 1, No. 4
2003年12月 INFORMATION AND ELECTRONIC ENGINEERING Dec., 2003

文章编号：1672-2892(2003)04-0257-03

# 一个前向安全的强代理签名方案

谭作文，刘卓军

（中国科学院数学与系统科学研究院 系统科学研究所，北京 100080）

**摘 要：**基于代理签名理论和前向安全签名理论，提出了一个前向安全的强代理签名方案，其安全性建立在求离散对数和模合数求平方根是困难的这两个假设的基础上。此方案同时对代理签名人和原始签名人的权益提供了保护，攻击者即使在第i时段入侵系统，也无法伪造第i时段之前的签名，因而具有较高执行效率和较强的安全性。

**关键词：**公钥密码学；数字签名；前向安全；离散对数；模合数求平方根

**中图分类号：**TP393.08 **文献标识码：**A

## 1 引言

普通数字签名能为消息的传输提供完整性和不可否认性，然而一旦签名密钥由于人为疏忽或系统本身的缺陷被泄露，签名的安全性就得不到任何保证。取消签名密钥后，再用签名密钥对文件所作的签名是无效的，但吊销密钥之前所进行的签名也会变得不可信赖。用户可能在对己不利的文件上签名后故意让签名密钥泄露，然后声称此签名无效。为了解决这个问题，人们提出了各种各样的签名方法，如运用秘密分享技术的动态签名，门限签名等。对于一般用户来说，这些签名方案所需通信量及计算量高，很不现实，而且参与密钥分享的各个系统依然面临着密钥泄露的问题。目前，随着使用小型便携式设备如手机等进行金融贸易活动的日益增加，密钥泄露问题变得更加突出。为了减缓密钥泄露所带来的严重后果，Anderson 提出了前向安全签名的概念[1]。Bellare 和 Miner 第一次给出了前向安全签名的正式定义，并基于 A. Fiat 和 A. Shamir 的签名方案[2]给出了两个前向安全签名方案[3]。前向安全签名的基本思想是：在普通签名算法中增加密钥进化算法。密钥进化算法将公钥的生命期分为 T 个时段，每个时段代表一个小时、一天、一周或一个月等。公钥在这 T 个时段总保持不变，私钥随着时段的推进而不断更新。在前向安全签名方案中，攻击者即使在 t 时段入侵系统获得签名密钥，却无法伪造 t 时段之前的签名。取消签名密钥后，系统在 t 时段之前所作的签名仍然有效。正是由于这一显著特点，前向安全签名受到了人们很多的关注。Abdalla 和 Reyzin 基于 Ong-Schnorr 签名方案提出了一个前向安全的签名方案[4]，缩短了文献[3]中的公钥与私钥的长度。Itkins 和 Reyzin 根据改进的 Guillou-Quisquater 签名方案[5]提出了另一个前向安全的签名方案[6]，此方案不仅密钥较短，而且签名算法与加密算法效率较高。

代理签名是由 M. Mambo 等提出来的一个签名概念[7]。原始签名人如公司负责人由于健康或其他原因不能履行签名权利时，便将签名权交给代理人如秘书对文件进行签名。这种签名在电子交易、移动代理等环境中应用很广。文献[7] 根据代理权限大小将代理签名分为三种：完全代理签名、部分代理签名和带有授权书的代理签名。在完全代理签名方案中，原始签名人将其签名私钥交给代理签名人作签名密钥。在部分代理签名方案中，原始签名人先产生代理签名密钥，然后将代理签名密钥通过秘密信道传送给代理签名人。第三种签名方案中，授权书上有原始签名人及代理签名人的信息、代理授权权限等，对代理签名进行验证时要使用授权书。最近，Z. Shao[8] 根据代理签名密钥是否由原始签名人生成将代理签名分为：未对代理人提供保护的代理签名和对代理人提供保护的代理签名。在未对代理人提供保护的签名方案中，原始签名人产生签名密钥，签名验证时仅用到原始签名人的公钥。在此类方案中，代理签名人必须是诚实的，原始签名人独自承担签名责任。在对代理人提供保护的签名方案中，代理人根据原始签名人生成的“签名钥”结合自己的私钥生成代理签名密钥，但原始签名人无法产生有效的代理签名密钥。在此方案中，原始签名人和代理签名人共同承担签名责任。B. Lee 等提出了一个强代理签名方案[9]，它属于第二种情形。本文仅讨论对代理人提供保护且带有授权书的代理签名。

代理签名中也存在着代理人私钥泄露的问题。代理人私钥的泄露会导致恶意用户伪造代理签名，从而对代理人构成诬陷，并使原始签名人利益受损。代理人以往所进行的真实代理签名也会随之失效。本文首次提出了一个前向安全的强代理签名方案。此方案能减轻代理人私钥泄露所带来的损失，能保证代理人私钥泄露之前的签名都是有效的。它与文献中的前向安全签名方案不同的地方在于：文献中的前向安全签名方案大多基于 Fiat

**收稿日期：**2003-10-08； **修回日期：**2003-12-08

**基金项目：**National Grand Fundamental Research 973 Program of China（1998030600）

**作者简介：**谭作文（1967-），男，博士研究生，主要从事网络安全、通信安全和密码学等方面的研究。

和 Shamir 类签名方案，安全性建立在强 RSA 假设（由 R. Rivest , A. Shamir, L. Adleman 三人研发，故称为 RSA 假设）上；本文提出的前向安全签名方案是基于离散对数签名方案，其安全性依赖于求有限域中离散对数和模合数平方根的困难性。

## 2 前向安全的签名方案模型

一个前向安全的签名方案[4]包括以下四个算法：a) 密钥生成算法：这是一个概率算法。输入安全参数 k 和时段总数 T，算法返回一个初始公私钥对（$SK_1$，$PK$）；b) 签名算法：在第 i（0<i<T）时段，输入密钥 $SK_i$=（$S_i$,i,T）和消息 m，算法返回第 i 时段关于消息 m 的签名（i,SIGN）；c) 验证算法：这是一个确定性算法。输入公钥 PK，消息 m，和签名（i,SIGN），如果签名是有效的，此算法返回 1；否则，算法返回 0；d) 密钥进化算法：此算法输入当前时段 i（0<i<T〉的密钥 SKi，返回下一个时段 i+1 的密钥 SKi+1。

## 3 前向安全的强代理签名方案

定义：对于素数 $p$，若存在两个大素数 $p'$，$q'$，使得 $p=2p'q'+1$，称 $p$ 为强安全素数。

### 3.1 系统建立

假设 Alice 授权 Bob 对消息 m 进行签名。Bob 先随机选择一个强安全素数 $p$ 和 $Z_p^*$ 的一个生成元 g，公布 $p$，$g$。Alice 随机选择一个整数 $x_A$，$1<x_A\le p-1$，计算 $y_A=g^{x_A}$（mod p），Alice 得到公私钥对（$x_A$，$y_A$）。在此签名方案中，签名密钥的有效期分为 T 个时段。Bob 随机选择一个整数 $x_0$，$1<x_0\le p-1$，计算 $y_B=g^{x_0^{2^{T+1}}}$（mod p）。Bob 得到公私钥对的一个初始值（$y_B$，$x_0$）。系统公钥为（$p$，$g$，T，$y_A$，$y_B$），h：$\{0,1\}^*\rightarrow Z_p^*$ 是一个密码学意义下的安全 Hash 函数。

### 3.2 产生代理权

Alice 产生授权书 w，授权书包含 Alice 和 Bob 的身份信息、Alice 对 Bob 的代理签名授权、代理签名时限等，然后在 $Z_{p-1}^*$ 随机选择 $k_A$，计算 $r_A=g^{k_A}$（mod p）和 $s_A=k_A+x_Ah(w,r_A)$（mod p-1），Alice 将（$s_A$，w，$r_A$）传送给 Bob。（$s_A$，$r_A$）可以看成是 Alice 对授权书 w 的签名。

### 3.3 验证代理权

代理签名人 Bob 收到（$s_A$，w，$r_A$）后，检验下列等式是否成立：$g^{s_A}\stackrel{?}{=}r_Ay_A^{h(w,r_A)}$（mod p）。若等式成立，则接受此代理权；否则，Bob 拒绝代理权。

### 3.4 代理签名人私钥进化算法

系统进入 i 时段（0<i<T）时，签名者 Bob 使用 i-1 时段的密钥 $x_{i-1}$ 计算 $x_i=(x_{i-1})^2$(mod p-1)，并立刻从系统中删除密钥 $x_{i-1}$。这时代理签名人的密钥对是（$y_B$，$x_i$）。

### 3.5 产生代理签名钥

Bob 结合第 i 时段的私钥 $x_i$，计算代理签名钥：$x_p=h(w,r_A,i)x_i^{2^{(T+1-i)}}+s_A$（mod p-1）。

### 3.6 代理签名

Bob 在 $Z_{p-1}^*$ 中随机选择 $k_p$，计算 $r_p=g^{k_p}$（mod p）和 $s_p=k_p+x_ph(m,w,r_A,r_p,i)$（mod p-1），然后将其对消息 m 的代理签名（m，i，w，$r_A$，$r_p$，$s_p$）传送给签名接收者或签名验证者。

### 3.7 代理签名验证

签名接收者或签名验证者验证等式：$g^{s_p}=r_p(r_Ay_A^{h(w,r_A)}y_B^{h(w,r_A,i)})^{h(m,w,r_A,r_p,i)}$（mod $p$）。若此等式成立，则接受签名。这是因为：

$$
\begin{aligned}
g^{s_p} &= g^{k_p} g^{x_p h(m,w,r_1,r_p,i)} \\
&= r_p (g^{s_1 + x_i^{2^{T+1-j}} h(w,r_1,i)})^{h(m,w,r_1,r_p,i)} \\
&= r_p (r_A y_A^{h(w,r_1)} g^{x_i^{2^{T+1-j}} h(w,r_1,i)})^{h(m,w,r_1,r_p,i)} \\
&= r_p (r_A y_A^{h(w,r_1)} y_B^{h(w,r_1,i)})^{h(m,w,r_1,r_p,i)} \pmod p
\end{aligned}
$$

## 4　新方案的安全性分析

上述前向安全的强代理签名方案具有下列性质：a）强不可伪造性：Alice 传送给 Bob 的关于授权书 w 的签名是可以公开的[10]，因此只需考虑 Alice 假冒 Bob 进行代理签名的情形。Alice 必须通过 $y_B^{h(w,r_1,i)} g^{s_1} = g^{x_p} \pmod p$ 来计算 $x_p$，这是一个离散对数问题。b）可验证性：这已在第 3 节末作了说明。c）强可识别性：根据代理签名的验证过程及授权书 w，可以很快确定代理签名人 Bob 和原始签名人 Alice 的身份。d）强不可否定性：代理签名过程中用到了代理签名人和原始签名人的公钥及其代理授权书，Bob 不能否定其代理人身份，Alice 也不能否定其授权人身份。e）防滥用代理权进行签名：在代理签名产生过程中，代理授权书 w 及原始签名人对 w 签名等的运用，能有效地防止代理签名人滥用代理签名权。f）前向安全性：设攻击者在第 i 时段侵入系统，获取了代理签名人 Bob 的私钥或代理签名密钥，要产生第 i 时段之前的有效代理签名钥，攻击者必须计算相应的私钥。这意味着攻击者应该能够解决模合数的二次剩余问题。

## 5　结论

本文提出的新方案在代理签名方案[11]的基础上，利用简便高效的密钥进化算法，实现了前向安全和可强代理签名两个功能。它既能有效地保护代理签名人的代理签名权，又能避免代理签名权的滥用，保护了原始签名人的利益。代理签名人与原始签名人之间无需秘密通讯信道。代理签名人的公私钥及代理签名钥的长度都与时段总数无关。因此，该方案有较高执行效率和较强的安全性。

**参考文献：**


[1] Ross Anderson.Two remarks on public key cryptology. Invited Lecture [A].The fourth ACM Computer and Communication Security [C],1997.

[2] A Fiat,A Shamir.How to prove yourself:practical solutions to identification and signature problems [A].Advances in Cryptology-Crypto'86, Lecture Notes of Computer Science [C],1986,1987: 186-194.

[3] M Bellare,S K Miner. A forward-secure digital signature scheme [A]. Advances in Cryptology-Crypto'99, Lecture Notes of Computer Science [C],1999, 1666: 431-448.

[4] M Abdalla,L Reyzin. A new forward-secure digital signature scheme [A]. Asiacrypt'00, Lecture Notes of Computer Science [C], 2000,1976:116-129.

[5] L C Guillou, J J Quisquater. A "paradoxical" identity-based signature scheme resulting from zero-knowledge [A]. Advances in Cryptology-Crypto'88, Lecture Notes of Computer Science [C],1988, 403: 216-231.

[6] G Itkis,L Reyzin. Forward-secure signatures with optimal signing and verifying [A]. Advances in Cryptology-Crypto'01, Lecture Notes of Computer Science [C],2001, 2139:332-354.

[7] M Mambo,K Usuda,E Okamato. Proxy signature: Delegation of the power to sign messages [A]. IEICE Trans. Fundamentals [C],1996, E79-A: 1338-1353.

[8] Zuhua Shao. Proxy signature schemes based on factoring [A]. Information Processing Letter [J], 2003, 85: 137-143.

[9] B Lee, H Kim, K Kim. Strong proxy signature and its applications [A]. SCI2001 [C],2001, 2: 603-608.

[10] J Y Lee, J H Cheon, S Kim. An analysis of proxy signatures: Is a secure channel necessary? [A]. CT-RST 2003 [C],2003, 2612: 68-79.

[11] S Kim, S Park, D Won. Proxy signatures, revisited. [A]. Proc. of ICICS'97, Lecture Notes of Computer Science [C],1997, 1334: 223-232.


# A Forward Secure Strong Proxy Signature


TAN Zuo-wen，LIU Zhuo-jun

（Institute of Systems Science，AMSS，CAS，Beijing 100080,China）



**Abstract:** A forward secure strong proxy signature scheme is proposed on the basis of the proxy signature schemes and forward secure schemes. The security of the proposed scheme relies on the difficulty of solving discrete logarithm problems and the difficulty of computing square roots modulo a large composite number. The signature scheme provides the safeguard to the rights and interests of both the original and the proxy signers. Even if an adversary can intrude the system and obtain the signature key at time period i, it could not forge the proxy signature before time period i.



**Key words:** public key cryptology; digital signature; forward security; discrete logarithm; square root modulo composites