基于零知识签名的代理签名方案

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　在代理签名方案中，原始签名人将其签名权委托给代理签名人，代理签名人代表原始签名人行使签名权。许多基于Schnorr签名的代理签名方案被提出。但是，其中有一些方案存在着原始签名人假冒代理签名人、伪造代理签名的安全问题。首次使用零知识数字签名的方式进行代理签名，分别提出了两个带有授权书的、保护代理人的代理签名和多重代理签名方案。这两个方案不仅具有强可区分性、强不可否认性，而且具有强不可伪造性，能抵抗原始签名人假冒代理签名人、伪造代理签名攻击。我们的方法可以应用到存在原始签名人伪造的其他ElGamal类代理签名方案。

关键词　多重代理签名，代理签名，知识签名，离散对数

Proxy Signature Schemes Based on Signature of Zero-Knowledge

TAN Zuo-Wen　LIU Zhuo-Jun

(Institute of Systems Science, Academy of Mathematics and Systems Science, CAS, Beijing 100080)

Abstract　In a proxy signature scheme, the original signer delegates its signing power to the proxy singer. Many proxy signature schemes are proposed on basis of Schnorr signature scheme. However, some proxy schemes are insecure against the original's forgery attack. In this paper, we first combine signature of zero-knowledge with proxy signature and propose a secure strong proxy signature scheme with warrants and a secure strong multi-proxy signature scheme. These schemes do not only achieve strong distinguishability and non-repudiation properties but also achieve strong unforgeability property. They are still secure against the original signer's forgery attack. The proposed technique can also be applied to other ElGamal-like proxy signature schemes in which the original signer can impersonate the proxy signer and forge the proxy signature on any message.

Keywords　Multi-proxy signature, Proxy signature, Signature of knowledge, Discrete logarithm

1　引言

代理签名是由M. Mambo等提出来的一个签名概念[8]。代理签名的应用目的是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，便将签名权委托给代理人如秘书等对文件进行签名。这种签名机制在电子交易、移动代理等环境中都有重要的应用，引起了人们极大的兴趣[2,7,5,6]。M. Mambo等[8]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，原始签名人根据私钥计算出代理签名密钥，然后将代理签名密钥通过秘密信道传送给代理签名人。在第三种签名方案中[5]，原始签名人需产生代理授权书。授权书上记载原始签名人及代理签名人的信息、代理授权的时限等，授权书在代理签名的产生与验证时使用。部分代理签名方案可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[5,9]。在现实环境中，多个合法签名人可以将签名权利同时委托给某个人实施多重代理签名[6]，或者一个原始签名人将其签名权同时委托给某个若干代理人组成的群体，进行代理多重签名[2]。但是，许多代理签名方案是不安全的。H.-M. Sun等[10]指出：在文[8]的方案中，代理签名人能将其签名权转移给别人，文[5]提出的方案不能抵抗公钥替换攻击。H.-M. Sun等[12]对基于离散对数的强代理签名方案、多重代理签名方案[6]，保护私密的强代理签名方案[11]及其记名(Nominative)代理方案[4]进行了分析，发现它们都存在着原始签名人伪造代理签名的问题。

我们利用零知识数字签名分别提出了一个代理签名方案和一个多重代理签名方案。它们具有以下特点：代理签名的验证方程中既有代理签名者的公钥和身份ID，又有原始签名人的公钥，实现了实际签名权和代理签名权的有效分离，代理签名人不能否认一个有效的代理签名。本文的两个基于零知识签名的代理签名方案能有效地防止原始签名人假冒代理签名人、伪造代理签名钥，进行代理签名。这种方法可以应用到保护私密的强代理签名方案[11]及其记名代理方案[4]，能克服原始签名人伪造代理签名的缺陷。

2　预备知识

2.1　知识签名

J. Camenisch和M. Stadler依据Schnorr签名提出了知识签名的概念[1]。设G是一个n阶的循环群，g是G的一个生成元，签名者的公私钥对是(x,y)，其中$y=g^x$，m是待签的消息，$H(): \{\}^* \rightarrow \{\}^k$是一个密码学意义上安全的hash函数，$k$是安全参数。

签名：签名者选择随机数$r \in_R Z_n$，计算$c=H(m\|y\|g\|$

*)国家重点基础研究发展规划973项目(G.1998030600)。谭作文　博士生，研究方向是信息安全，网络安全与密码学。刘卓军　博士生导师，研究员，主要研究方向为符号计算与信息安全。

g^r)，$s=r-cx \pmod n$，称(c,s)为签名者根据y关于g的离散对数对消息m进行的知识签名。

验证：验证者计算

$c'=H(m\|y\|g\|g^s y^c)$。

若$c'=c$，验证者接受签名；否则拒绝此签名。

在随机预言模型下，基于离散对数假设的所有知识签名是安全的[1]。

2.2 符号说明

A	原始签名人
B	代理签名人
R	代理签名的接受者、验证者
p,q	两个大素数，其中$q\|(p-1)$
w	A发给B的授权书
x_A,y_A	A的私、公密钥对
x_B,y_B	B的私、公密钥对
x_ρ,y_ρ	代理签名私对
s_a,y_a	授权密钥对
$H():\{\}^*\to\{\}^k$	安全的单向hash函数，
k	安全参数。

表中密钥对均存在$y=g^x \pmod p$关系。

3 Lee的两个代理签名方案及其缺陷

3.1 Lee的代理签名方案[6]及其对文[6]中方案的攻击

代理授权阶段：原始签名人A选择随机数$k_A\in_R Z_q^*$，计算$r_A=g^{k_A} \pmod p$，$s_A=x_A H(w,r_A)+k_A \pmod q$，然后将$(w,r_A,s_A)$通过安全信道传送给代理签名人B。

代理签名密钥产生阶段：

B计算g^{s_A}，若$g^{s_A}\neq y_A^{H(w,r_A)} r_A \pmod p$，则拒绝接受A的授权；否则，B接受A的授权，并将$x_\rho=s_A+x_B \pmod q$作为代理签名钥。

代理签名生成阶段：

代理签名人B使用x_ρ进行普通数字签名。记普通签名为$\sigma=sign(m,x_\rho)$，则代理签名为(m,σ,r_A,w)。

代理签名验证阶段：

验证者R收到代理签名(m,σ,r_A,w)后，首先检查授权书w中的内容是否有效，然后计算$y_\rho=y_A^{H(w,r_A)} r_A y_B \pmod p$，运行普通数字签名的验证算法：$verify(m,\sigma,y_\rho)=0$或1。

上述签名方案存在着原始签名人假冒代理人、伪造代理签名攻击[12]：

原始签名人A令$r'_A=y_B^{-1} g^{k_A} \pmod p$，$k_A\in_R Z_q^*$，计算$x'_\rho=x_A H(w,r'_A)+k'_A \pmod q$。$x'_\rho$是一个有效的代理签名密钥，A可以对任意消息$m$假冒代理签名人B进行代理签名，这时验证者无法确认签名(m,σ',r'_A,w)是否是伪造签名。代理签名钥x'_ρ的有效性证明如下：

$y'_\rho=y_A^{H(w,r'_A)} r'_A y_B=y^{H(w,r'_A)} g^{k'_A}=g^{x'_\rho} \pmod p$。

3.2 一个多重代理签名方案[7]及其对它的攻击

假设n个原始签名人$\{A_1,A_2,\cdots,A_n\}$都将它们的签名权托付给代理签名人B。(x_{A_i},y_{A_i})表示原始签名人A_i的私、公钥对，其中$y_{A_i}=g^{x_{A_i}} \pmod p$。

多重代理授权阶段：

A_i如3.1节中的A一样产生(w_i,r_{A_i},s_{A_i})，并将(w_i,r_{A_i},s_{A_i})通过秘密信道传送给代理签名人B。

多重代理签名密钥生成阶段：

若对于每个i，都有$g^{s_{A_i}}=y_{A_i}^{H(w_i,r_{A_i})} r_{A_i} \pmod p$，则B接受授权书，并计算代理签名钥$x_\rho=\sum_{i=1}^{n} s_{A_i}+x_B \pmod q$；如果存在某一个$i$，使得授权方程不成立，B拒绝继续执行协议。

多重代理签名产生阶段：

B使用x_ρ关于待签消息m作普通数字签名$\sigma=sign(m,x_\rho)$，从而得到的多重代理签名是$(m,\sigma,r_{A_1},w_1,r_{A_2},w_2,\cdots,r_{A_n},w_n)$。

多重代理签名验证阶段：

验证者R计算代理签名公钥

$y_\rho=y_{A_1}^{H(w_1,r_{A_1})} r_{A_1}\cdots y_{A_n}^{H(w_n,r_{A_n})} r_{A_n} y_b \pmod p$，运行普通数字签名验证算法$verify(m,\sigma,y_\rho)$，若算法输出1，则代理签名有效；若算法输出0，代理签名是无效的。

此方案也存在着原始签名人假冒代理签名人、伪造代理签名攻击[12]。

假设原始签名人A_i试图进行伪造攻击。A_i计算$r'_{A_i}=(\prod_{1\leqslant j\neq i\leqslant n} y_{A_j}^{H(w_j,r'_{A_j})} r'_{A_j})^{-1} \pmod p$，代理签名密钥$x'_\rho=x_{A_i} H(w_i,r'_{A_i})$。代理签名钥的有效性可仿3.1节作验证。运用$x'_\rho$，对于任何消息，$A_i$都可以成功地伪造多重代理签名。

4 新型的代理签名方案和多重代理签名方案

我们利用知识签名来设计新的代理签名方案和多重代理签名方案。新的代理签名方案包括下列过程。

代理授权过程：

原始签名人A在Z_q^*中随机选择一个整数$k_A\in_R Z_q^*$，计算

$r_A=g^{k_A} \pmod p$ (1)

$s_A=x_A H(w,r_A)+k_A ID_B \pmod q$ (2)

然后将(w,r_A,s_A)通过秘密信道传送给代理签名人B。

代理签名密钥产生过程：

与3.1节中密钥产生阶段一样，代理签名者B验证授权方程后，将$x_\rho=s_A+x_B \pmod q$作为代理签名密钥。

代理签名生成过程：

代理签名人B使用x_ρ对消息m进行知识签名，并结合y_B关于基g的离散对数的知识证明、授权公钥y_a关于基g的离散对数的知识证明，产生代理签名(m,σ)。σ是代理签名人公钥y_B、代理签名公钥y_ρ和授权公钥y_a关于基g的离散对数知识的联合知识签名：

$PK[\alpha,\beta,\gamma\,|\,y_1=g^\alpha \wedge y_2=g^\beta \wedge y_3=g^\gamma](m)$。

具体签名过程如下：

代理签名人B计算$y_2=g^{s_A} \pmod p$，$y_3=g^{x_\rho} \pmod p$，$y_1=y_B$，然后B随机选择$r_1,r_2,r_3\in Z_q^*$，并计算

$c=H(m\|w\|r_A\|y_1\|y_2\|y_3\|g\|g^{r_1}\|g^{r_2}\|g^{r_3})$ (3)

$s_1=r_1-cx_B \pmod q$ (4)

$s_2=r_2-cs_A \pmod q$ (5)

$s_3=r_3-cx_\rho \pmod q$ (6)

这样得到的代理签名是(m,w,r_A,c,s_1,s_2,s_3)。

代理签名验证过程：

验证者R收到签名后(m,w,r_A,c,s_1,s_2,s_3)后，计算

$y'_1=y_B$ (7)

$y'_2==y_A^{H(w,r_A)} r_A^{ID_B} \pmod p$ (8)

$y'_3=y'_2 y_B \pmod p$ (9)

$c'=H(m\|w\|r_A\|y'_1\|y'_2\|y'_3\|g\|g^{s_1} y_B^{s_2}\|g^{s_2}(y'_2)^c\|g^{s_3}(y'_3)^c)$ (10)

然后判断是否有 $c'=c$。若等式成立，则代理签名有效；否则，代理签名无效。

可类似地建立一个多重代理签名方案。它的多重代理授权与多重代理密钥的产生过程与3.2节中的相仿。多重代理签名的产生过程如下：代理签名人 B 利用其拥有的公钥 y_B、代理签名公钥 y_p 和授权公钥 $y_{a_i}(i=1,2,\cdots,n)$ 关于基底 g 的离散对数知识进行联合知识签名。我们把这个知识签名记作

$PK[\alpha,\beta_1,\beta_2,\cdots,\beta_n,\gamma|y=g^{\alpha}\wedge y_1=g^{\beta_1}\wedge\cdots\wedge y_n=g^{\beta_n}\wedge\bar{y}=g^{\gamma}](m)$。

具体签名过程是：

代理签名人 B 先计算 $y_i=g^{r_{A_i}}(\mathrm{mod}\ p),i=1,2,\cdots,n,\bar{y}=g^{\bar{r}_p}(\mathrm{mod}\ p)$，随机选择 $n+2$ 个数 $r,r_i,\bar{r}\in Z_q^*$，计算

$$c=H(m\|w_1\|\cdots\|w_n\|r_{A_1}\|\cdots\|r_{A_n}\|y\|y_1\|\cdots\|y_n\|\bar{y}\|g\|g^r\|g^{r_1}\|\cdots\|g^{r_n}\|g^{\bar{r}})$$

$$s=r-cx_B(\mathrm{mod}\ q)\tag{11}$$

$$s_i=r_i-cs_{A_i}(\mathrm{mod}\ q)\tag{12}$$

$$\bar{s}=\bar{r}-cx_p(\mathrm{mod}\ q)\tag{13}$$

那么，B 的多重代理签名就是：

$(m,w_1,\cdots,w_n,r_{A_1},\cdots,r_{A_n},c,s_1,\cdots,s_n,\bar{s})$。

多重代理签名的验证过程：接收者 R 计算

$$y'=y_B\tag{14}$$

$$y_i'=y_{A_i}^{H(w_i,r_{A_i})}r_{A_i}^{ID_B}(\mathrm{mod}\ p)\tag{15}$$

$$\bar{y}'=y_B\prod_{i=1}^{n}y_i'(\mathrm{mod}\ p)\tag{16}$$

$$c'=H(m\|w_1\|\cdots\|w_n\|r_{A_1}\|\cdots\|r_{A_n}\|y'\|y_1'\|\cdots\|y_n'\|\bar{y}'\|g\|g^{s}y_B^{c}\|g^{s_1}(y_1')^{c}\|\cdots\|g^{s_n}(y_n')^{c}\|g^{\bar{s}}(\bar{y})^{c})。$$

若 $c'=c$，则 R 接受多重代理签名；否则，此多重代理签名无效。

5 新型代理签名方案性能分析

本文提出的多重代理签名方案与代理签名方案具有相同的安全性质。这里仅对基于零知识签名的代理签名方案作简要的分析。

①(m,w,r_A,c,s_1,s_2,s_3)是有效的代理签名。

根据式(1)和(2)，可把(r_A,s_A)看成是 A 对授权书的签名，故授权方程为：

$$g^{s_A}=y_A^{H(w,r_A)}r_A^{ID_B}(\mathrm{mod}\ p),$$

因此有授权公钥 $y_2=y_2'$。由于 $x_p=s_A+x_B(\mathrm{mod}\ q)$，故对于代理签名公钥 y_p，有

$$g^{x_p}=g^{s_A+s_B}=g^{s_A}\cdot y_B=y_A^{H(w,r_A)}\cdot r_A^{ID_B}\cdot y_B(\mathrm{mod}\ p),$$

也就是说 $y_3=y_3'$。从而，若代理签名人 B 遵守协议，则代理签名的验证是正确的。

②新签名方案具有强可识别性和强不可否认性。

由式(1)和(2)可知，授权密钥生成过程使用了签名人 B 的身份 ID_B；根据式(7)、(8)、(9)、(10)可知，代理签名验证过程使用了原始签名人 A 和代理签名人 B 的公钥。这样，新的代理签名方案实现了原始签名权与代理签名权的有效分离。代理授权书 w 限制了代理签名人拥有代理权的时限，从而有效地防止了代理签名人滥用代理签名权，进一步保证了此方案的强可识性和强不可否认性。因此对于一个有效的代理签名，Bob 不能否定其代理人身份，A 也不能否定其授权人身份。

③新签名方案具有不可伪造性。

授权书的签名(w,r_A,s_A)是通过秘密通道传送给代理签名人的，其他人得不到这些参数。即使通过非法手段截获(w,r_A,s_A)，它们没有 B 的私钥也不能产生有效的代理签名密钥。如果换用伪造者自己的私钥，则式(7)、(8)、(9)、(10)通过授权书、B 的公钥计算出来的结果不会满足验证方程 $c'=c$，因此无法伪造 B 的代理签名。

原始签名人 A 对授权书 w 的签名(w,r_A,s_A)是 Schnorr 签名。代理签名人 B 根据此签名无法计算出 A 的私钥、伪造 A 的签名。

若原始签名人 A 企图进行伪造攻击，因 A 拥有授权书的签名(w,r_A,s_A)，它能够选择合适的 r_A'，计算代理签名密钥 x_p'，但是由于 A 不知道代理签名人的私钥 x_B，无法提供 y_B 关于 g 离散对数的知识证明。因此，A 伪造的代理签名不会满足验证方程 $c'=c$。

小结 本文将零知识数字签名运用到代理签名方案中，提出了带有授权书、保护代理签名人的代理签名方案和多重代理签名方案，并对新方案进行了安全分析。这两个方案克服了文[6]和[7]的缺陷，能对原始签名人和代理签名人提供公平性保护，原始签名人不能再进行伪造攻击。本文提出的方法可以应用到其他存在原始签名人伪造攻击的 ElGamal 类代理签名方案，如保护私密的强代理签名方案[11]及其记名代理方案[4]等。

参考文献

1 Camenisch J, Stadler M. Efficient group signature schemes for large groups. Advances in Cryptology-CRYPTO'97, Springer Verlag, 1997, 1294: 410～424

2 Hwang S J, Chen C C. A new proxy multi-signature scheme. In: Intl. workshop on cryptology and network security, Tankang University Taipei, Taiwan, 2001. 26～28

3 祁明，韩亮. 代理签名与阈下信道的封闭. 计算机工程与应用，2001. 25～27

4 Kim S J, Park S J, Won D H. Nominative signatures. In: Proc. of ICIEIC'95, 1995. 68～71

5 Kim S J, Park S J, Won D H. Proxy signatures, revisited. ICICS'97, LNCS 1334, Springer-Verlag, 1997. 223～232

6 Lee B, Kim H, Kim K. Strong proxy signature and its applications. In: Proc. of SCIS, 2001. 603～608

7 Lee B, Kim H, Kim K. Secure mobile agent using strong non-designated proxy signature. In: Proc. of ACISP, LNCS 2119, Springer-Verlag, 2001. 474～486

8 Mambo M, Usuda K, Okamoto E. Proxy signatures: Delegation of the power to sign messages. IEICE Trans. Fundamentals, 1996, E79-A: 1338～1353

9 Petersen H, Horster P. Self-certified keys-concepts and applications. In: Proc. Communication and Multimedia Security'97, Chapman & Hall, 1997. 102～116

10 Sung H-M, Hsieh B-T. Remarks on two non-repudiable proxy signature schemes. In: Proc. of ninth national conf. on information security, 1999. 241～246

11 Shum K, Wei V K. A strong proxy signature scheme with proxy signer privacy protection. In: Proc. of eleventh IEEE Intl. Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, 2002. 55～56

12 Sun H-M, Hsieh B-T. On the security of some proxy signature schemes. Available at: http://eprint.iacr.org/2003/068