不需消息保密的盲代理签名方案

何迎生，段明秀，彭　胜，鲁荣波

（吉首大学 数学与计算机科学学院，湖南 吉首 416000）

摘　要：提出了一个不需要消息保密的盲代理签名方案，代理签名人的身份除对原始签名人外是保密的，只有指定接收者才能够验证代理签名的有效性，但无法确定代理签名人的身份，出现争议时指定接收者可以通过原始签名人揭示代理签名人的真实身份。以该方案为基础，还构造了一个高效的共享验证签名方案。

关键词：代理签名；盲代理签名；指定接收收者；门限验证

中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1673-9833(2008)04-0034-03

Scheme of Blind Proxy Signature Without Message Secrecy

He Yingsheng，Duan Mingxiu，Peng Sheng，Lu Rongbo

（School of Mathematics and Computer Science，Jishou University，Jishou Hunan 416000，China）

Abstract: A blind proxy signature without message secrecy is proposed. The new scheme can protect the proxy signer's privacy against the other third parties except the original signer, only the designed receiver can validate the proxy signature, but the designed verifier cannot confirm the identity of the proxy signer. The designed verifier can unveil the identity of the proxy signer via the original signer when the dispute exists. Based on the proposed scheme, a novel efficient threshold shared verification signature scheme is constructed.

Key words: proxy signature; blind proxy signature; designed receiver; threshold verification

随着互联网应用的展开，网络安全问题已经成为人们关心的焦点，相关的安全协议不断提出。一些实际应用如电子现金、电子投票、匿名通信等，客观要求保密用户的身份等信息，盲签名[1]、代理签名[2]、不可否认签名[3]、环签名[4]等便可实现匿名签名和认证，但匿名性在保护个人隐私的同时，也同样给犯罪分子带来了可乘之机。为了既保护个人的隐私，又避免犯罪，人们提出了很多方案，如群签名[5]，但由于诸如群成员吊销、如何抵抗联合攻击、如何设计高效、安全的基于身份的群签名等问题尚未得到有效解决，群签名离实用还有一定的距离。

代理签名是指某人授权其他人替自己行使签名权的一种签名。在现有的大部分代理签名方案[2,6,7]中，原始签名人都能根据代理签名辨认出代理签名人的身份。这样原始签名人能对代理签名人的代理签名进行监督，防止代理签名人滥用代理签名权。但在有些情况下，尽管代理签名人忠实地行使着原始签名人委托给自己的代理签名权力，仍然不愿意原始签名人能根据代理签名确定出代理人的身份，如电子选举等。为满足上述要求，文献[8]提出了一个新的概念，称为盲代理签名体制。

本文提出一个盲代理签名方案，适用于不需要消息保密的情形，不仅实现了盲代理签名，而且只有指定接收者才能验证代理签名的有效性。指定接收者要伪造签名等价于伪造 Schnorr 签名[9]，等价于解离散对数问题，其余攻击者要验证签名等价于解 Diffie-Hellman 问题[10]，代理签名人的身份除对原始签名人外是保密的，必要时指定接收者和原始签名人合作可以揭示代理签名人的真实身份。基于该方案，得到了一个适合于分布式处理系统的更为高效的共享验证盲代

收稿日期：2008-05-05

基金项目：湖南省自然科学基金资助项目（07JJ6110），湖南省教育厅基金资助项目（07C522）

作者简介：何迎生（1974-），男，湖南浏阳人，吉首大学讲师，主要研究方面为信息安全，数据挖掘.

理签名方案。

1　系统设置与基本工具

p 和 q 为一对大素数且满足 $q \mid p-1, g \in Z_q^*$，并且 $g^q=1 \bmod p (g \neq 1)$。h 为安全的哈希杂凑函数，m 为需要签名的消息。A 为原始签名人，B 为代理签名人，V 为接收者。m_w 是描述原始签名人 A 授权代理签名人 B 代理权限约定的授权书，包括 A 的标识、B 的代理期限、签名消息范围等内容。x_A 为原始签名人 A 的私钥，把 $y_A = g^{x_A} \bmod p$ 公开，x_B 为代理签名人 B 的私钥，$y_B = g^{x_B} \bmod p$ 为代理签名人 B 的公钥；x_P 为原始签名人 A 和代理签名人 B 共同生成的代理私钥，$y_P = g^{x_P} \bmod p$ 为对应的代理公钥。ID_B 为代理签名人 B 的标识，ID_P 为签名者的标识。x_V 为接收者的私钥，$y_V = g^{x_V} \bmod p$ 为对应的公钥。

SA 随机生成一个 $t-1$ 次多项式：

$$f(x)=x_V + a_1 x + \cdots + a_{t-1} x^{t-1} \bmod q,$$

式中 $a_i \in Z_q^* (i=1, \cdots, t-1)$，对每个接收者 V_i，SA 计算 $x_{V_i} = f(u_i) \bmod q$，其中 u_i 为用户 V_i 的公开信息。SA 把 x_{V_i} 秘密地发送接收者 $V_i (i=1, \cdots, n)$。

定义 1　满足 $c=H(M \parallel g \parallel h \parallel g_1 \parallel h_1 \parallel g^r h^c \parallel g_1^r h_1^c)$ 的二元组（c,r）称为对消息 $M \in \{0,1\}^*$ 关于 h, h_1 的一个知识签名，记为：

$SPK\{\alpha \mid h=g^\alpha \wedge h_1=g_1^\alpha\}(M)$[11]。

签名者如果知道一个整数 x，满足 $x=\log_g h=\log_{g_1} h_1$，可以按如下步骤计算出这一签名：

第 1 步　选择 $s \in_R Z_n^*$，计算 $h'=g^s$，$h_1=g_1^s$；

第 2 步　计算 $c=H(M \parallel g \parallel h \parallel g_1 \parallel h_1 \parallel h')$；

第 3 步　计算 $r = s - cx \bmod q$。

2　不需消息保密的盲代理签名方案

2.1　代理密钥的生成

第 1 步　原始签名人 A 通过安全通道向代理签名人 B 发送 m_w，B 收到 m_w 后，如果接收代理授权，则计算：$k_B \in_R Z_q^*$，$r_B = g^{k_B} \bmod p$，$s_B = x_B h(r_B, ID_B, r_1) + k_B r_B \bmod q$，$k_1 \in_R Z_q^*$，$r_1 = g^{k_1} \bmod p$，$s_1 = x_P h(r_B, ID_B, r_1) + k_1 \bmod q$。

B 把（r_B, ID_B, r_1, s_1）通过安全通道返回给 A，A 验证等式 $g^{s_1} = y_B^{h(r_B, ID_B, r_1)} r_1 \bmod p$ 是否成立。如果成立，A 秘密保存 (r_B, y_B, ID_B)，并且计算 $Y_P = y_B r_B^{r_B} \bmod p$，把 Y_P 写入 m_w 中。

第 2 步　A 计算：$k_A \in_R Z_q^*, r_A = g^{k_A} \bmod p$，$s_A = x_A h(m_w, r_A, y_V) + k_A r_1 \bmod q$。

A 通过安全信道发送 (r_A, s_A, m_w, y_V) 给 B。B 验证 $g^{s_A} = y_A^{h(m_w, r_A, y_V)} r_A^{r_A} \bmod p$ 是否成立，如果成立，B 秘密保存 $(r_A, s_A, m_w, y_V, s_B)$。

第 3 步　B 生成代理私钥 x_P，即 $x_P=s_A+s_B$。

2.2　代理签名的生成

如果消息 m 符合 m_w 的约定，代理签名者用代理签名私钥 x_P 产生代理签名，即 B 随机选择 $k \in_R Z_q^*$，计算：$v_1 = g^k \bmod p$，$v_2 = y_V^k \bmod p$，$e = h(m, m_w, v_2)$，$s = k - e x_P \bmod q$，代理签名为 (m_w, r_A, v_1, s)。

2.3　代理签名验证

第 1 步　接收者 V 收到签名 (m_w, r_A, v_1, s) 后计算：$y_P = y_A^{h(m_w, r_A, y_V)} r_A^{r_A} Y_P \bmod p$（其中 Y_P 是从 m_w 中取得），此式成立的数学证明如下。

由于 $x_P=s_A+s_B$，$s_A = x_A h(m_w, r_A) + k_A r_A \bmod q$，$s_B = x_B + k_B r_B \bmod q$，$Y_P = y_B r_B^{r_B} \bmod p$，则 $g^{x_P} = g^{s_A+s_B} = g^{x_A h(m_w, r_A)} g^{k_A r_A} g^{x_B} g^{k_B r_B} = y_A^{h(m_w, r_A)} r_A^{r_A} y_B r_B^{r_B} = y_A^{h(m_w, r_A, y_V)} r_A^{r_A} Y_P = y_P \bmod p$。即此成立。

第 2 步　接收者 V 计算 $v_2' = (v_1)^{x_V} \bmod p$，$e = h(m, m_w, v_2')$。

第 3 步　接收者 V 检查 m 是否符合 m_w 的约定，如果符合进入下一步。

第 4 步　接收者 V 验证 $v_1 = g^s (y_P)^e \bmod p$，若成立，则说明签名有效。

2.4　门限验证

门限验证是指验证盲代理签名的能力被 n 个验证服务器按门限方式进行分享。

设 $V=(V_1, V_2, \cdots, V_n)$，群公钥为 $y_V = g^{x_V} \bmod p$，采用文献[12]提出的 DL-Key-Gen 作为密钥分配协议（基本思想参见文献[12]的引述）。

设 V 中 t 个成员的子集 V' 准备验证签名，不妨设为 $V'=(V_1, V_2, \cdots, V_t)$。

第 1 步　$V_i (i=1, 2, \cdots, t-1)$ 计算：

$y_P = y_A^{h(m_w, r_A, y_V)} r_A^{r_A} Y_P \bmod p$（其中 Y_P 是从 m_w 中取得），$I_i = x_{v_i} \lambda_i \bmod q$，这里 x_{v_i} 是接收者 V_i 执行 DL-Key-Gen 协议后得到的 Shamir 的秘密共享 share，λ_i 表示 Shamir 秘密共享方案的 Lagrange 系数，是可以公开计算的。

第 2 步　$V_i (i=1, 2, \cdots, t-1)$ 计算，并广播：

$v_{2i}' = (v_1)^{I_i} \bmod p$。

第3步　$V_i (i=1, 2, \cdots, t-1)$ 计算：$v_2' = \prod_{i=1}^{t} v_{2i}' \bmod p$。剩余验证步骤同第 2.3 节第 3 步和第 4 步。

2.5　揭示代理签名人身份

第 1 步　接收者 V 向原始签名人 A 提供代理签名 (m_w, r_A, v_1, s)，v_2' 以及知识证明的签名：$SPK\{\alpha \mid y_V = g^{x_V} \wedge v_2' = (v_1)^{x_V}\}(M)$，$M$ 表示接收者 V 的身份识别信息。

第 2 步　原始签名人 A 执行代理签名验证过程，其中 v_2' 是接收者 V 发送的，其正确性可通过验证知识证

明的签名$SPK\{\alpha|y_V=g^{x_V}\wedge v_2'=(v_1)^{x_V}\}(M)$的正确性来保证。

第3步 原始签名人A依次取出代理密钥对生成阶段保存的(r_B, y_B, ID_B)，判断等式$Y_P - y_B r_B^{r_B} \bmod p$是否成立（$Y_P$从$m_w$中取得），如果存在$(r_B, y_B, ID_P)$满足等式，则$ID_P$是实现代理签名$(m_w, r_A, v_1, s)$的代理签名人。

3 方案性能分析

1）其它的接收者若要计算$v_2=(v_1)^{x_P} \bmod p$，等价于攻破Diffie-Hellman问题，所以不能进行验证签名的有效性。

2）代理秘钥不可伪造。

证明 对于代理签名秘钥$x_P=s_A+s_B$，假设伪造者B'试图得到x_P，必须同时具备以下2个条件。

I）**得到**s_A 由于$s_A=x_A h(m_w, r_A, y_V)+k_A r_1 \bmod q$，那么必须得到$x_A$和$k_A$，而$x_A$是$A$的秘钥，由$y_A=g^{x_A} \bmod p$解$x_A$是离散对数问题，$k_A$是用户$A$随机选择的，所以伪造者$B'$是不可能计算出$s_A$的。

II）**得到**s_B 由于$s_B=x_B+k_B r_B \bmod q$，那么必须得到x_B和k_B，而x_B是B的秘密密钥，由$y_B=g^{x_B} \bmod p$解x_B是离散对数问题，k_B是用户B随机选择的，所以伪造者B是不可能计算出s_B的。

由上可知，即使是原始签名人也不能伪造有效的代理签名密钥，只有合法的代理签名人才能产生一个有效的代理签名密钥，才能代表原始签名人进行签名。由代理授权过程知道，接收者是由原始签名人指定的，指定接收者的公钥已经嵌入授权中，即使是代理签名人也无法改变。

3）指定接收者伪造签名(m_w, r_A, v_1, s)等价于伪造Schnorr签名。

证明 如果V伪造了有效的(m_w, r_A, v_1, s)，由于V拥有私钥x_V，则只要计算$v_2=v_1^{x_V} \bmod p$，(m, s, v_2)即是有效的伪造Schnorr签名。

反之，若V能够伪造有效的Schnorr签名(m, s, v_2)，计算$v_1=v_2^{x_V^{-1}} \bmod p$，则$(m_w, r_A, v_1, s)$为有效的代理签名。

而Schnorr签名不可伪造，所以V不可能伪造有效的(r, e, s)，其它接收者更不可能伪造。

4）此方案满足盲代理要求

代理签名(m_w, r_A, v_1, s)中没有包含代理签名人的身份，虽然$Y_P - y_B r_B^{r_B} \bmod p$，但由于$r_B$是保密的，因此从$Y_P - y_B r_B^{r_B} \bmod p$是无法计算出$y_B$的，也就是接收者$V$只能验证签名的有效性，但并不知道代理签名人的真实身份。由第2.5节可以知道，在需要时，原始签名人A和指定接收者V合作揭示代理签名人的身份。

5）由于只有代理签名人才能生成合法的代理签名秘钥x_P，第三方即使是原始签名人也无法得到x_P，因此不能否认由A和指定接收者揭示的代理签名是由自己生成的。

4 结语

本文提出了一种不需要消息保密的盲代理签名方案，只有指定的接收者可以验证签名的有效性。将该方案扩展成共享验证，得到了一个高效的适合于分布式处理系统的共享验证盲代理签名方案，该方案在实际应用中有一定的价值。

参考文献：

[1] Chaum D. Blind signatures for untraceable payments[C]// Advances in Cryptology-Proceedings of Crypto'82. New York：Prenum Publishing Corporation，1982：199-204.

[2] Mambo M, Usuda K and Okamoto E. Proxy signature[C]// Proceedings of the 1995 Symposium on Cryptography and information security(SCIS'95). Japan：[s.n.]，1995：147-158.

[3] Chaum D，Van Antwerpen H. Undeniable signatures[C]// Advances in Cryptology-CRYPTO'89. Berlin: Springer-Verlag，1990：212-216.

[4] Rivest R，Shamir A，Tauman Y. How to leak a secret[C]// Advances in Cryptology-ASIACRYPT'01. Berlin：Springer-Verlag，2001：552-565.

[5] Chaum D, Heyt V F. Group signatures[C]// Proceedings of Eurocrypt'91. Berlin：Springer-Verlag，1991：257-265.

[6] Zhang K. Threshold Proxy Signature Schemes[C]//The 1st International Information Security Workshop (ISW'97). Berlin：Springer-Verlag，1997：191-197.

[7] Yi Lijiang， Bai Guoqiang， Xiao Guozhen. Proxy Multi-Signature Scheme[J]. Electronics Letters，2000，36(6)：527-528.

[8] Yi L J，Xiao G Z. Blind proxy signature scheme[C]// Proceedings of CCICS'2001. Beijing：Science Press，2001：88-95.

[9] Schnorr C. Efficient Signature Generation by Smart Cards[J]. Journal of Cryptology，1991，4(3): 161-174.

[10] Diffe W，Hellman M E. New Directions in Cryptography [J]. IEEE Transactions on Information Theory，1976，22 (6): 644-654.

[11] Frankel Y，Tsiounis Y，Yung M. Indirect Discourse Proof：Achieving Fair Off-Line Cash [C]// Advances in Cryp-tology-Asiacrypt'96. Berlin：Springer-Verlag ，1996：286-300.

[12] Raimondo M D，Gennaro R. Provably secure threshold password-authenticared key exchange [C]//Advances in Cryptology-EUROCRYPT 2003. Berlin：Springer-Verlag，2003：507-523.

（责任编辑：罗立宇）