新的多重代理多重签名方案

汪秋国，施荣华，江 玲

(中南大学信息科学与工程学院 长沙 410083)

【摘要】现有的代理数字签名方案大部分都是基于离散对数问题和大数因子分解问题的方案。该文基于椭圆曲线密码体制，提出了一种新的多重代理多重签名方案，并对方案的安全性进行了分析。方案中，一组原签名人可以共同授权给一组代理签名人，授权代理签名组的所有成员一起可以代替原签名组成员行使签名权利。方案充分利用了椭圆曲线密码体制密钥小、速度快等优点，更加安全、高效，在电子商务和无线网络通信领域具有广泛的应用前景。

关 键 词 离散对数； 椭圆曲线； 代理签名； 安全性

中图分类号 TP309 **文献标识码** A

New Multi-Proxy Multi-Signature Scheme

WANG Qiu-guo, SHI Rong-hua, and JIANG Ling

(School of Information Science and Engineering, Central South University Changsha 410083)

Abstract Up to now all the known proxy digital signature schemes are based on discrete logarithmic problems or big number factorization problems. Based on the elliptic curve, a new multi-proxy multi-signature scheme is proposed. Furthermore, we also analyze the new scheme's security problem. In this scheme, an original group of signers can authorize a group of proxy signers under the agreement of all singers, and only all singers in proxy group can generate multi-proxy multi-signatures instead of the original group of signers. The scheme takes full advantage of elliptic curve cryptosystem, such as shorter private key, higher signature efficiency and so on, so it is more secure and efficient than the existing schemes.

Key words discrete logarithm; elliptic curve ; proxy signature; security

文献[1-2]首先提出了代理签名的概念。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。文献[3]提出了一类新的代理签名方案：代理多重签名。在一个代理多重签名方案中，一个代理签名人可以同时代表多个原始签名人的利益在一个文件上签字。文献[4]提出了一个多重代理多重签名方案，但是目前所提出的代理多签名体制大多数都是基于一般群上的离散对数问题和大数因子分解问题。

本文基于椭圆曲线离散对数问题，提出了一个新的多重代理多重签名方案，方案中由 n 个原始签名人构成的原签名组授权给由 m 个代理签名人构成的代理签名组，让代理签名组来代替原签名组进行签名，只有授权代理签名组的所有成员一起才能代理原签名组进行签名。该方案极大地提高了签名生成和验证的效率，并缩短了签名的长度，在电子商务和网络通信中具有广泛的应用前景。

1 椭圆曲线数字签名算法(ECDSA)

ECDSA方案的思想是：设 E 是 F_q 上的椭圆曲线，系统主域参数 $D=(E,q,G,l,h)$。其中，q 为有限域 F_q 的特征值，G 为 E 上的一个有理点，称为基点，G 的阶为 l (l 为素数)，h 为一个Hash函数。系统每一用户有一私钥 d，相应的公钥 $Q=dG$。ECDSA方案的参与者有签名实体A，可信的中间机构CA负责产生主域参数 $D=(E,q,G,l,h)$和密钥对(d,Q)，验证签名的实体B。

签名过程如下：(1) A选取一个随机数 $k\in\{1,2,\cdots,l-1\}$；(2) 计算 $kG=(x,y)$以及 $r=x \bmod l$，如果 $r=0$，回到步骤(1)继续选择 k；(3) 计算 $e=h(m)$，$s=k^{-1}(e+rd) \bmod l$，如果 $s=0$，回到步骤(1)；(4) 实体A对消息的签名为(r,s)。

验证过程如下：(1) 验证 r 和 s 是$[1,l-1]$中的整数；(2) 计算 $e=h(m)$，$u=s^{-1}e \bmod l$，$v=$

收稿日期：2007－01－25; 修回日期：2007－06－01
基金项目：国家自然科学基金(60773013)；湖南省自然科学基金(02JJY2094)
作者简介：汪秋国(1982－)，男，硕士生，主要从事密码学与信息安全方面的研究.

$s^{-1}r \bmod l$；(3) 计算$X=uG+vP_A$，记X的坐标为(x_1,y_1)，若$X=0$，则拒绝签名；否则计算$r_1=x \bmod l$；(4) 当且仅当$r=r_1$时，接受签名[5]。

2 新的多重代理多重数字签名方案

系统参数为E，q，G，l，h(定义同ECDSA)，这些参数是公开的，系统内每个成员都知道。令U_i($i=1,2,\cdots,n$)为原签名组中的成员，U_i的秘密密钥为d_{ui}，对应的公开密钥为$P_{ui}=d_{ui}G$；P_j($j=1,2,\cdots,m$)表示代理签名组中的成员，P_j的秘密密钥为d_{pj}，对应的公开密钥为$P_{pj}=d_{pj}G$，他们愿意代表$\{U_1,U_2,\cdots,U_n\}$产生代理签名。授权委托证书为w，w中包含授权时间及代理的有效期限、代理签名的最大次数、原始签名人和代理签名人的公钥等信息。该方案包括代理证书生成、签名生成和签名验证3个阶段。

2.1 代理证书生成

代理证书生成步骤如下：

(1) 每一个原始签名人U_i($i=1,2,\cdots,n$)选取一个随机数$k_{ui}\in\{1,2,\cdots,l-1\}$，计算$K_{ui}=k_{ui}G=(x_{ui},y_{ui})$，并将$K_{ui}$广播给其他$n-1$个原始签名人和$m$个代理签名人；同样地，每一个代理签名人$P_j$($j=1,2,\cdots,m$)选取一个随机数$k_{pj}\in\{1,2,\cdots,l-1\}$，计算$K_{pj}=k_{pj}G=(x_{pj},y_{pj})$，并将$K_{pj}$广播给$n$个原始签名人和$m-1$个代理签名人。

(2) 每一个原始签名人和代理签名人计算：

$$\overline{R}=\sum_{i=1}^{n}K_{ui}+\sum_{j=1}^{m}K_{pj}=(x,y)$$

$$R=x \bmod l$$

(3) 每一个原始签名人U_i($i=1,2,\cdots,n$)计算$V_{ui}=d_{ui}h(w,R)+k_{ui}R \bmod l$，然后将$V_{ui}$广播给其他$n-1$个原始签名人和$m$个代理签名人；同样地，每个代理人$P_j$($j=1,2,\cdots,m$)计算$V_{pj}=d_{pj}h(w,R)+k_{pj}R \bmod l$，并将$V_{pj}$广播给其他$m-1$个代理签名人和$n$个原始签名人。

(4) 每个签名人验证V_{ui}、V_{pj}的正确性：

$$V_{ui}G=h(w,R)P_{ui}+K_{ui}R \quad i=1,2,\cdots,n$$

$$V_{pj}G=h(w,R)P_{pj}+K_{pj}R \quad j=1,2,\cdots,m$$

(5) 若V_{ui}、V_{pj}都是正确的，则每个代理签名人P_j计算：

$$V=\sum_{i=1}^{n}V_{ui}+\sum_{j=1}^{m}V_{pj} \bmod l$$

最后，m个代理签名人P_j($j=1,2,\cdots,m$)被授权作为n个原始签名人的签名代理，代理授权证书为$(R,V,\overline{R})$，不仅n个原始签名人同意，还要m个代理签名人同意，才能完成原签名组向代理签名组授权，使$P_1,P_2,\cdots,P_m$成为原签名组指定的代理签名人。

2.2 签名生成

代理签名组要代理原签名组对消息M进行签名，步骤如下：

(1) 每个代理人P_j随机选择一个整数$a_j\in\{1,2,\cdots,l-1\}$计算：

$$t_j=a_jG=(x_j,y_j)$$

$$\overline{t_j}=x_j \bmod l$$

为了克服文献[6]所提出的攻击，代理签名人P_j($j=1,2,\cdots,m$)不同时广播自己的$\{P_j,t_j\}$，而是按顺序将$\{P_j,t_j\}$对其他成员P_i($i=1,2,\cdots,m,j\neq i$)进行广播；P_i收到成员P_j的t_j后，随机选取$k_i\in[1,q-1]$，计算$L_i=k_iG=(x_{li},y_{li})$，然后P_i将L_i发送给P_j；P_j利用签名秘密选取的a_j，计算$L_i'=L_ia_j=k_ia_jG$，并将L_i'送还给P_i；P_i利用$\{P_j,t_j\}$验证等式$L_i'=t_jk_i$，若等式成立，则P_i接受$\{P_j,t_j\}$，并向P_j发送自己的$\{P_i,t_i\}$，重复执行上述验证过程，直到所有的代理签名人公布的t_j($j=1,2,\cdots,m$)得到验证。

证明：$L_i'=k_ia_jG=t_jk_i$　　证毕

(2) 每个代理人P_j计算：

$$\overline{T}=\sum_{i=1}^{m}t_j=(x_t,y_t)$$

$$T=x_t \bmod l$$

$$s_j=(a_jV+d_{pj}T)h(M) \bmod l$$

P_j对消息M的签名就是(t_j,s_j)，并将$(w,(R,V,\overline{R}),M,(t_j,s_j))$发送给代理签名管理员$U_c$。

(3) 管理员U_c首先通过计算等式：

$$VG=R\overline{R}+(\sum_{i=1}^{n}P_{ui}+\sum_{j=1}^{m}P_{pj})h(w,R)$$

是否成立来验证代理证书$(R,V,\overline{R})$的正确性，若不正确，则拒绝该证书。

(4) U_c计算$\overline{T}=\sum_{j=1}^{m}t_j=(x_t,y_t)$，取$T=x_t \bmod l$。

(5) U_c计算$H_j=V^{-1}(h(M)s_iG-P_{pj}T) \bmod l=(X_j,Y_j)$，如果$H_j=0$，拒绝签名；否则取$\overline{t_j}=x_j \bmod l$，判断等式$\overline{t_j}=X_j \bmod l$是否成立来验证每个代理签名人的签名是否正确，若都成立，则计算：

$$S=\sum_{j=1}^{m}s_j \bmod l$$

最后得出信息 M 的多重代理多重签名为$(w,(R,V,\overline{R}),M,(T,S))$。

2.3 签名验证

当接收者收到签名$(w,(R,V,\overline{R}),M,(T,S))$后，首先根据授权委托证书 w 和代理证书$(R,V,\overline{R})$，通过计算等式：

$$VG=R\overline{R}+(\sum_{i=1}^{n}P_{ui}+\sum_{j=1}^{m}P_{pj})h(w,R)$$

是否成立来验证代理签名人 P_j $(j=1,2,\cdots,m)$是否是 n 个原签名人的授权代理签名人；其次计算 $H=V^{-1}h(M)^{-1}(SG-\sum_{j=1}^{m}P_{pj}Th(M))=(X,Y)$，如果 $H=0$，则拒绝这个签名；否则，判断等式 $T=X \bmod l$ 是否成立，如果成立则接受签名。

定理 1 在椭圆曲线多重代理多重签名方案中，如果 $T=X \bmod l$ 成立，则数字签名$(w,(R,V,\overline{R}),M,(T,S))$被验证。

证明：如果对消息 M 的签名$(w,(R,V,\overline{R}),M,(T,S))$是正确的，那么：

$$S=\sum_{j=1}^{m}s_j=\sum_{j=1}^{m}(a_jV+d_{pj}T)h(M)$$

$$L=SG-\sum_{j=1}^{m}P_{pj}Th(M)=$$

$$\sum_{j=1}^{m}(a_jV+d_{pj}T)h(M)G-\sum_{j=1}^{m}P_{pj}Th(M)=$$

$$\sum_{j=1}^{m}(t_jV+P_{pj}T)h(M)-$$

$$\sum_{j=1}^{m}P_{pj}Th(M)=\sum_{j=1}^{m}t_jVh(M)$$

$$H=(X,Y)=V^{-1}h(M)^{-1}L=$$

$$V^{-1}h(M)^{-1}(\sum_{j=1}^{m}t_jVh(M))=\sum_{j=1}^{m}t_j$$

$$\overline{T}=\sum_{j=1}^{m}t_j=(x_t,y_t)$$

由于 $T=x_t \bmod l$，因此 $T=X \bmod l$ 成立，签名将被验证者接受[7]。

3 安全性分析

(1) 代理证书$(R,V,\overline{R})$不可伪造

个人证书(K_{ui},V_{ui})是不能伪造的，不妨假设 U_1 伪造了他的个人证书(K'_{u1},V'_{u1})，他必须使等式成立：

$$V'_{u1}G=h(w,R)P_{u1}+K'_{u1}R'$$

式中 $K'_{u1}+\sum_{i=2}^{n}K_{ui}+\sum_{j=1}^{m}K_{pj}=(\overline{X},\overline{Y})$；$R'=\overline{X} \bmod l$。如果 K'_{u1} 是已知的，要想从等式 $V'_{u1}G=h(w,R)P_{u1}+K'_{u1}R'$ 中得到 V'_{u1}，必须解决椭圆曲线离散对数问题，这是不可能的；同样，如果 V'_{u1} 是已知的，要想得到 K'_{u1} 也是不可能的。所以个人授权证书(K_{ui},V_{ui})是不能伪造的，从而代理证书$(R,V,\overline{R})$是不能伪造的[8]。

(2) 该方案能抵抗文献[6]提出的伪造攻击

攻击者无法靠公布假的 t_j 来达到伪造有效的多重代理多重签名的目的。由于该方案具有可验证性，不失一般性，当代理签名群内攻击者 P_1 在试图获得其他签名成员的 t_j $(j=1,2,\cdots,m)$之前，必须按照事先规定好的验证顺序给其他成员送去其 t_1，其他成员 P_j $(j=1,2,\cdots,m)$随机选取 $k_j\in[1,q-1]$，计算 $L_1=k_jG$，将 L_1 发送给 P_1，要求其利用其签名时所选择的 a_1 对 L_1 进行签名，即 $L'_1=L_1a_1$，并将签名结果 L'_1 送还给 P_j，P_j 利用 P_1 公布的 t_1 对式子 $L'_1=t_1k_j$ 进行验证，看其是否成立，如果成立，则说明 P_1 所公布的 t_1 是真的，否则，得出 P_1 公布的是虚假的 t_1。

(3) 代理签名(T,S)不可伪造

从方程 $H=V^{-1}h(M)^{-1}(SG-\sum_{j=1}^{m}P_{pj}Th(M))=(X,Y)$中可知，验证方程包括所有代理人的公钥，因此必须所有代理人合作才能生成有效的多重代理多重签名。若攻击者不知道代理证书$(R,V,\overline{R})$，则攻击者不能伪造代理签名(T,S)，因代理证书不可伪造，攻击者也就不能从上面一个含有3个未知数的方程中解出(T,S)；若攻击者通过某种方法得知了代理证书$(R,V,\overline{R})$，也不能试图伪造签名(T,S)。不失一般性，假设 P_1 为攻击者，虽然 P_1 知道代理证书$(R,V,\overline{R})$，但是要从验证方程中求出(T,S)在计算上是不可行的。因为若 P_1 首先选定 T，则求解 S 将面临椭圆曲线离散对数问题；同样若先选定 S，求解 T 也将面临椭圆曲线离散对数难题。因而所有的代理人合作才能生成代理签名(T,S)，且代理签名(T,S)不可伪造[9]。

(4) 签名者私钥的安全性

由于在每次代理签名授权过程中，原始签名人和代理签名者的私钥 d_{ui} 和 d_{pj} 都是与随机数 k_{ui} 和 k_{pj} 一起使用的，不同的授权过程选择的随机数也不

同。所以，即使经过了多次授权，也不会暴露签名者的私钥。同样，在每次签名过程中，代理签名者私钥 d_{pj} 总是和随机数 a_j 一起使用，不同的签名过程选择的随机数也不同。因而，在一个授权期限内，代理签名次数再多，也不会危及签名者私钥的安全。

(5) 强不可否认性[10]

代理证书必须由 n 个原始签名者和 m 个代理签名者共同参与才能产生，所以每个原始签名者都不能否认自己参与了授权过程，每个代理签名者也不能否认自己参与了授权过程并获得了授权。代理签名组一旦产生了一个有效的代理签名，就不能否认他们合作生成的代理签名，因为代理签名的产生需要用到所有代理签名者的私钥，所以任何少于 m 个代理签名者合谋也无法获得有效的代理签名，这也使每个签名者事后都不能否认自己参与了签名过程，否认签名等于宣称自己的私钥泄密。

(6) 可注销性

授权委托证书 w 中包含授权时间及代理的有效期限，代理签名的最大次数等信息。原始签名人可以注销代理签名组成员的代理权限，防止代理权限的滥用。

(7) 签名的高效性

本方案是基于椭圆曲线构造的，因此在提供良好的安全条件下，具有速度快、密钥量小、软硬件便于实现的优点。

4 结束语

随着网络技术的不断发展和网络应用系统的增加，保证网络信息的完整性和真实性，数字签名技术越来越重要。椭圆曲线数字签名算法因其“密钥短、安全性高”的突出优点，在实际环境中应用越来越广泛，代理签名由于其实用性，应用也很广泛。本文把多重代理多重签名和椭圆曲线相结合，提出了一种新的多重代理多重签名方案，它是一个安全有效的签名方案，在电子商务、电子政务和网络通信等领域具有实际的应用前景[11]。

参 考 文 献

[1] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures for delegation signing operation[C]//Proc of the 3rd ACM Conference on Computer and Communication Security. [S.l.]: ACM Press, 1996.

[2] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures: Delegation of the power to sign message[J]. IEICE Transactions on Fundamentals of Electronic Communication and Computer Science, 1996, E79-A(9): 1338-1354.

[3] 伊丽江, 白国强, 肖国镇. 代理多重签名: 一类新的代理签名方案[J]. 电子学报, 2001, 29(4): 569-570.
YI Li-jiang, BAI Guo-qiang, XIAO Guo-zhen. Proxy multi-signature: a new type of proxy signature schemes[J]. Acta Electronica Sinica, 2001, 29(4): 569-570.

[4] 李传目. 多重代理多重签名方案[J]. 计算机工程, 2003, 29(21): 43-44.
LI Chuan-mu. A multi-proxy multi-signature scheme[J]. Computer Engineering, 2003, 29(21): 43-44.

[5] 纪家慧, 李大兴. 新的代理多签名体制[J]. 计算机研究与发展, 2004, 141(14): 715-719.
JI Jia-hui, LI Da-xing. A new proxy multi-signature scheme[J]. Journal of Computer Research and Development, 2004, 141(14): 715-719.

[6] GUO Li-feng, WANG Gui-lin. Insider attacks on multi-proxy multi-signature schemes[J]. Computer & Electrical Engineering, 2007, 33(2): 88-93.

[7] 秦志光, 张险峰, 周世杰, 等. 基于ECC的门限数字签名方案及其安全性[J]. 电子科技大学学报, 2005, 34(1): 109-112.
QIN Zhi-guang, ZHANG Xian-feng, ZHOU Shi-jie, et al. Threshold digital signature scheme based on ECC and its security[J]. Journal of University of Electronic Science and Technology of China, 2005, 34(1): 109-112.

[8] CHEN T S, HUANG K H, CHUNG Y F. Digital multi-signature schemes based on the elliptic curve cryptosystem[J]. Journal of Computer Science and Technology, 2004, 19(4): 570.

[9] 曹天杰, 林东岱, 薛 锐. 基于椭圆曲线的代理多签名方案的安全性分析[J]. 小型微型计算机系统, 2006, 27(5): 798-801.
CAO Tian-jie, LIN Dong-dai, XUE Rui. Security analysis of some proxy multi-signature schemes based on elliptic curve cryptosystem[J]. Journal of Chinese Computer Systems, 2006, 27(5): 798-801.

[10] MEHTA M, HARN L. Efficient one-time proxy signature [J]. IEE Proc Communication, 2005, 152(2): 129-133.

[11] LEE J Y, CHEON J H, KIM S. An analysis of proxy signatures: Is a secure channel necessary?[C]//Topics in Cryptology CT-RSA, the Cryptographers' Track at the RSA Conference 2003, LNCS2612. Berlin, Heidelberg: Spring-Verlag, 2003.

编 辑 税 红