# 基于椭圆曲线的代理多重签名的改进方案

逯玲娜,周 梦
(北京航空航天大学 数学与系统科学学院,北京 100191)

**摘要**:在代理签名方案中,代理签名人可以代表原始签名人生成签名。在有些情形,需要一个代理签名能够同时代表多个原始签名人,这就是代理多重签名。随着椭圆曲线密码体制的出现,其以密钥短、安全性高赢得了密码学者及其相关工作者的喜爱。对文献[1]进行研究,发现其不具备强不可伪造性,结合文献[2],提出了一种新的基于椭圆曲线的代理多重签名,不仅保持了原有签名的优越性,也克服了原文不满足强不可伪造性的缺点,同时具有了自己独特的优点:密钥长度短、安全性能高,实现了一个签名人可以同时代表多个原始签名人在文件上进行签名,具有一定的使用价值。

**关键词**:代理签名;椭圆曲线;多重签名;数字签名
**中图分类号**:TN918.4 **文献标识码**:A **文章编号**:1671-5322(2011)01-0048-03

在现实生活中,往往需要参与的各方对某一重要文件进行签字或表决,比如合同的签订、公司文件的发布和重要的人事决定等。引申到数字签名领域,也就要求多个用户对同一消息进行数字签名,称实现多个用户对同一个消息进行签名的数字签名为多重数字签名;多重数字签名的概念是1983年Boyd提出来的,多重数字签名必须满足的安全性质有:

(1) 不可伪造性。这是任何一种数字签名必须具备的性质,是指除签名组成员共同完成签名外,任何人不可能伪造多重签名,包括签名成员的一部分也不可能合谋产生有效的签名。

(2) 不诚实签名者的可识别性。如果签名组成员有不诚实者,试图伪造签名,则在签名过程中或者验证过程中就能被发现,如果签名组中有不诚实者,那么签名不可能完成。

(3) 不可否认性。签名一旦形成,签名组全体成员不能否认其签名。

(4) 可验证性。接收人或验证人能根据协议要求,检验签名的真伪。

1996年,M Mambao等人在文献[3]中研究了代理数字签名问题,并提出了基于素数域的各种代理签名方案,为密码学和数字签名的研究与应用开辟了一个新领域。代理签名方案[4]就是一个被称为原始签名人的用户可以将他的签名权委托给另外一个被称为代理签名人的用户。

不管是多重数字签名还是代理签名,都是满足某些特殊需求的签名,具有一定应用背景,但是在某些情况下,迫切的需要同时满足这两种特性。因为在代理签名方案[5]中,一个代理签名只能代表一个原始签名者。有时,人们需要一个代理者同时代表若干个原始签名者进行签名。比如,一个公司要发表一份涉及行政部、财务部、开发部、销售部、售后服务部等的文件,该文件就必须有这些部门联合签名才有效,或者这些部门委托一个信赖的代理人替他们在该文件上签字。对于前一种情况,可用多重签名方案来解决;对于后一种情况,可用代理多重签名方案来解决,显然后一种解决方案在效率方面可以大大提高。

代理多重签名方案[6],简称为"一代多"方案,由委托过程、签名过程、验证过程组成。参与实体:可信中心TC、若干原始签名者、代理签名者、信息拥有者、信息接受者或验证者。

**收稿日期**:2010-10-19
**基金项目**:国家自然科学基金资助项目(10871017);北京市自然科学基金资助项目(102026)
**作者简介**:逯玲娜(1985-),女,河南省滑县人,硕士生,主要研究方向为代数学与密码学 。

## 1　有限域上的椭圆曲线

设 $F_q$ 是特征值大于 3 的有限域,其中 $q=p^m$,$a,b\in F_q$,满足 $4a^3+27b^2\neq 0$,则在仿射坐标平面上,由参数 $a,b$ 定义在有限域上 $F_q$ 的椭圆曲线 $E(F_q)$ 是方程 $y^2=x^3+ax+b$ 的所有解 $(x,y)$,$x\in F_q$,$y\in F_q$ 连同一个附加的"无穷远点"(记为 $O$)的元素组成的点的集合。$E(F_q)$ 的点数用 $\#E(F_q)$ 表示。点集合 $E(F_q)$ 对应下面的加法规则构成一个 Abel 加法群:群运算的恒等元是 $O$,设 $P,Q\in E(F_q)$,

①$O+O=O$;

②若 $P=O$,则 $-P=O$,且 $P+Q=Q+P=Q$;

③设 $P=(x_1,y_1)$,$Q=(x_2,y_2)$,则 $-P=(x_1,-y_1)$,且 $P+(-P)=O$;若 $Q\neq -P$,则 $P+Q=(x_3,y_3)$,其中 $\begin{cases}x_3=\lambda^2-x_1-x_2\\ y_3=\lambda(x_1-x_3)-y_1\end{cases}$

其中 $\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1}, P\neq Q\\ \dfrac{3x_1^2+a}{2y_1}, P=Q\end{cases}$

## 2　基于椭圆曲线的代理多重签名方案

### 2.1　初始化过程

系统参数:$F_q,E,G,P,h,F_q$ 是有限域,$E$ 是 $F_q$ 上的椭圆曲线非奇异椭圆曲线,且满足安全条件,$G$ 是 $E$ 上的一个有理点,成为基点,$G$ 的阶为 $p$($p$ 为素数),$h$ 为一个 HASH 函数。令 $A_1,A_2,\cdots\cdots,A_n$ 是 $n$ 个原始签名人,他们联合请求一个代理签名人 $B$ 代表他们在一个文件 $m$ 上签名,对任意 $1\leqslant i\leqslant n$,$A_i$ 有一个公开的密钥 $P_i$ 和一个私密密钥 $d_i\in\{1,\cdots\cdots,p-1\}$,使得 $P_i=d_iG$;$B$ 的公开密钥为 $P_b$ 和私密密钥 $d_b\in\{1,\cdots\cdots,p-1\}$,使得 $P_b=d_bG$。

### 2.2　代理密钥的生成

#### 2.2.1　子代理密钥的生成

对任意 $1\leqslant i\leqslant n$,$A_i$ 随机选取 $k_i\in\{1,\cdots\cdots,p-1\}$,计算 $R_i=k_iG=(x_i,y_i)$ 和 $r_i=d_i+k_ix_i(\mathrm{mod}\ p)$。

#### 2.2.2　子代理密钥的发送

对任意 $1\leqslant i\leqslant n$,$A_i$ 将 $(r_i,R_i)$ 作为子密钥通过安全信道传输给 $B$。

#### 2.2.3　子代理密钥的验证

对任意 $1\leqslant i\leqslant n$,$B$ 验证等式 $r_iG\stackrel{?}{=}P_i+x_iR_i$ 是否成立,如果成立,则 $(r_i,R_i)$ 就是一个有效的子代理密钥,否则拒绝这个密钥而请求 $A_i$ 重新发送一个有效的子代理密钥,或者终止协议。

#### 2.2.4　代理密钥的生成

如果 $B$ 确定所有 $(r_i,R_i)(1\leqslant i\leqslant n)$ 都是有效的,那么 $B$ 计算 $r=d_b+\sum_{i=1}^{n}r_i(\mathrm{mod}\ p)$ 作为他的代理密钥,$rG=P_b+\sum_{i=1}^{n}(P_i+x_iR_i)$ 作为代理公钥进行验证。

### 2.3　代理多重签名产生

对于消息 $m$,$B$ 进行代理签名:

2.3.1　随机的选取 $t\in\{1,\cdots\cdots,p-1\}$,计算 $tG=(a,b)$,$u=a(\mathrm{mod}\ p)$。

2.3.2　计算 $e=h(m)$。

2.3.3　计算 $R=t^{-1}(e+ur)(\mathrm{mod}\ p)$。

则消息 $m$ 的代理多重签名即为 $[m,(R,u),R_1,\cdots\cdots,R_n]$

### 2.4　代理签名的验证

接收方或验证者收到 $[m,(R,u),R_1,\cdots\cdots,R_n]$ 后,进行一下验证:

2.4.1　计算 $e=h(m)$。

2.4.2　计算 $\alpha=R^{-1}e(\mathrm{mod}\ p)$,$\beta=R^{-1}u(\mathrm{mod}\ p)$。

2.4.3　计算 $(a',b')=\alpha G+\beta[P_b+\sum_{i=1}^{n}(P_i+x_iR_i)]$,验证等式 $u\stackrel{?}{=}a'(\mathrm{mod}\ p)$,如果成立,则接受这个代理多重签名,否则拒绝。

**证明**:$tG=R^{-1}(e+ur)G=R^{-1}eG+R^{-1}urG=\alpha G+\beta rG=\alpha G+\beta[P_b+\sum_{i=1}^{n}(P_i+x_iR_i)]$。

## 3　方案的安全性分析

### 3.1　满足强壮的不可伪造性

在代理密钥中包含两部分,一部分是原始签名人 $A_1,\cdots\cdots,A_n$ 发过来的子代理密钥,另一部分是 $B$ 的密钥,这样方案中只有能得到代理签名的密钥,即只有代理签名人 $B$ 可以为原始签名人 $A_1,\cdots\cdots,A_n$ 生成有效的代理多重签名。原始签名人 $A_1,\cdots\cdots,A_n$ 或者其他人不能生成有效的代理签名。因为在没有得到所有原始签名人的代理子密钥和 $B$ 的密钥的情况下,任何人都无法生成一个有效的代理多重签名。例如,如果没有得到所有的有效 $r_i(1\leqslant i\leqslant n)$,任何人都无法找到一组

$(r, R_1, \cdots\cdots, R_n)$ 使他满足 $rG = P_b + \sum_{i=1}^{n}(P_i + x_i R_i)$,这是由基于椭圆曲线的离散对数问题的困难性决定的。

### 3.2 满足强壮的不可抵赖性

由于方案满足强壮的不可伪造性可以知道,只有代理签名人能产生代理签名,代理签名人将不能抵赖签过的代理签名,所以满足强壮的不可抵赖性。

### 3.3 代理多重签名的可验证性

由于签名在验证时需要原始签名人 $A_1, \cdots\cdots, A_n$ 和 $B$ 的公钥,所以签名的验证人不仅可以知道是 $B$ 进行的代理多重签名,而且得到了原始签名人 $A_1, \cdots\cdots, A_n$ 的许可。同时任何人可以验证代理多重签名的有效性,即 $tG = R^{-1}(e + ur)G = R^{-1}eG + R^{-1}urG = \alpha G + \beta rG = \alpha G + \beta[P_b + \sum_{i=1}^{n}(P_i + x_i R_i)]$。

### 3.4 可注销性

$A_1, \cdots\cdots, A_n$ 如果想要撤销 $B$ 拥有的代理签名权利,那么他们可以向大家宣布 $R_1, \cdots\cdots, R_n$ 不再有效,从而 $B$ 生成的所有代理签名都随之失效。

## 4 结论

在本文中,首先对文献[1]进行研究,发现其不具有强不可伪造性即 $n$ 个签名人可以联合伪造出来一个有效代理多重签名。基于此,本人对其进行改进,不仅保持了原有签名的优越性,同时具备强壮的不可伪造性,而且新的签名是基于椭圆曲线的,具有密钥短、安全性高的优点。利用代理多重签名,可以有效的实现由一个代理签名人生成代表多个原始签名人的代理签名的目的。本人认为,这种新签名方案在电子商务和网络安全通信方面有广泛的应用前景。

**参考文献:**


[1] 伊丽江. 代理多重签名:一类新的代理签名方案[J]. 电子学报,2001,29(4):560-570.

[2] 杨爱梅. 改进的基于椭圆曲线的代理数字签名和代理多重签名[J]. 网络安全技术与应用,2006(5):88-89.

[3] Mambo M, Usuda k, Okamoto E. Proxy signatures: Delegation of the power to sign message[J]. IEICE Trans, Fundamentals, 1996, E79-A(9):1338-1354.

[4] 伊丽江. 代理签名体制及其应用研究[D]. 西安:西安电子科技大学,2000.

[5] S Kim, S park and D. Won proxy signatures, revisited[A]. Proc. of ICICS97, International. Conference on Information and Communications Security[C]. LNCE, 1334, 1997:223-232.

[6] 吴丹. 基于椭圆趋向的代理数字签名和代理多重数字签名[J]. 浙江大学学报,2005(1):39-41.


# The Improvement of a Proxy Multiple Signature Based on Elliptic Curve


LV Ling-na, ZHOU Meng

(Mathematics and Systems Science Institute of Bei hang University LMIB, Beijing 100191, China)



**Abstract**: The proxy signer can produce a signature for original signer. In some cases, A proxy signer need to represent numbers of the original signers, which is the proxy multiple signature. With the development of elliptic curve cryptography, it wins the fancy of cryptography scholars and workers for its short key and safety. Having researched article[1], I found that it didn't have non-forgery. My paper proposes a new proxy multiple signature, with the combination of the article[2]. It keeps the advantage of original article and overcomes its disadvantage. Furthermore, it has unique advantage which is short key and high security. This paper can represent an original signer to produce a multiple signature, which has some value in use.



**Keywords**: proxy signature; elliptic curve; multiple signature; digital signature

(责任编辑:张英健; 校对:沈建新)