第 36 卷 第 7 期 计 算 机 工 程 2010 年 4 月
Vol.36 No.7 Computer Engineering April 2010
·安全技术· 文章编号：1000—3428(2010)07—0165—03 文献标识码：A 中图分类号：TP309.2

基于身份和多线性映射的代理环签名方案

周晓燕，杜伟章
(长沙理工大学计算机与通信工程学院，长沙 410114)

摘 要：提出一种基于多线性映射的代理环签名方案。该方案能防止原始签名者冒充代理签名者对消息进行签名，通过引入多个密钥生成中心防止其中任何一个对消息进行签名。签名者的签名私钥由多个密钥生成中心共同决定。性能分析结果验证了该方案的可行性和安全性。
关键词：数字签名；代理签名；环签名；多线性映射

Proxy Ring Signature Scheme Based on Identity and Multilinear Mapping

ZHOU Xiao-yan, DU Wei-zhang
(College of Computer and Communication Engineering, Changsha University of Science & Technology, Changsha 410114)

【Abstract】This paper proposes a proxy ring signature scheme based on multilinear mapping. This scheme can prevent the original signer from generating signature for message as a proxy signer and prevent the key generation center from forging proxy ring signature by introducing several key generation centers. The signature private keys of signer are completed by several key generation centers. Performance analysis results show that the scheme is feasible and secure.
【Key words】digital signature; proxy signature; ring signature; multilinear mapping

1 概述

在信息社会中，人们经常需要把自己的签名权利委托给可靠代理人，让代理人代表本人对一些消息文件进行签名。代理签名方案用于实现上述需求，但在此类方案中，代理人的身份没有得到保护。环签名[1]是一种简化的群签名，它不需要群管理员或群建立过程，且签名者的身份完全匿名。环签名中签名者身份的完全匿名性有效保护了实际签名者的隐私权，该特点使其被广泛应用。研究者把环签名和代理签名结合起来，产生了一种新的签名——代理环签名。文献[2]提出代理环签名的思想，但仅将其应用在一个原始签名者授权给多个代理者的环境中。文献[3]针对文献[2]应用受限和运算量过大的缺点，提出一种代理人受保护的代理环签名方案，该方案能有效防止原始签名人对代理签名人签名的伪造，且减少了双线性对的计算量，计算效率较高。文献[4]对文 献[2]方案进行改进，并提供不可否认服务，更好地满足了代理环签名的安全需求。文献[5]指出文献[3]提出的代理环签名方案存在不可计算性等错误，并给出相应的改进方案。

上述基于身份和双线性对的代理环签名方案使用一个密钥生成中心，方案安全的前提是密钥生成中心是完全可信的。若密钥生成中心失信，则方案是不安全的。本文通过引入多个密钥生成中心，克服了上述方案中一个密钥生成中心不可靠的缺点，并结合多线性对的思想[6]，构造一个基于身份和多线性对的代理环签名方案。

2 多线性对

定义 1 设$(G_1,+),(G_2,\cdot)$分别是阶为q的循环加群和循环乘群，其中，q为素数。对映射$e_n:G_1^n\to G_2$，如果满足以下条件：

(1)多线性。对所有$a_1,a_2,\cdots,a_n\in Z_q,P_1,P_2,\cdots,P_n\in G_1$，有$e_n(a_1P_1,a_2P_2,\cdots,a_nP_n)=e_n(P_1,P_2,\cdots,P_n)^{a_1a_2\cdots a_n}$。

(2)非退化性。如果P是G_1的一个生成元，则$e_n(P_1,P_2,\cdots,P_n)$是G_2的生成元。

(3)可计算性。对所有$P_1,P_2,\cdots,P_n\in G_1$，存在一个有效的算法计算$e_n(P_1,P_2,\cdots,P_n)$，则称映射$e_n(P_1,P_2,\cdots,P_n)$为多线性映射。

3 代理环签名

代理环签名方案一般包括 4 个参与方：密钥生成中心(Key Generation Center, KGC)，原始签名者，代理签名者和验证者。

定义 2 一个代理环签名方案是一个包含以下过程的数字签名方案：

(1)系统创建。用于产生原始签名者和代理签名者密钥对和系统参数的多项式事件概率算法。

(2)代理密钥产生。用于产生代理签名密钥对的算法。

(3)签名生成。一个概率算法，当输入待签消息、系统参数、身份集合和代理签名者的代理签名私钥后，输出对该消息的签名。

(4)签名验证。用于在输入对消息的签名、系统参数和身份集合后确定签名是否有效的算法。

一个好的代理环签名应满足以下安全性要求：

(1)签名者的模糊性。给定一个代理环签名后，任何人(代理签名者除外)试图确定真实签名者的身份在计算上是不可

作者简介：周晓燕(1985－)，女，硕士研究生，主研方向：信息安全，密码学；杜伟章，教授、博士后
收稿日期：2009-11-10 **E-mail：**zhouxiaoyan_em@163.com

行的。

(2)不可伪造性。只有合法的代理环签名者才能生成有效的代理环签名，原始签名者和其他人不能产生合法的代理环签名。

(3)可验证性。验证者可以验证签名是否为经授权的合法代理环签名。

(4)不可否认性。一旦代理签名者代表原始签名者生成了一个合法的代理环签名，他不能向原始签名者否认他所签署的有效代理环签名。

(5)可鉴别性。任何人都可区别代理人产生的代理环签名和正常环签名。

代理环签名是随着电子投票、电子现金等应用需要的增长而提出的一种新型数字签名形式，它为保护电子商务活动中签名者的隐私权提供了一种重要方法。

4 一种基于多线性映射的代理环签名方案

在本方案中采用 t 个独立的密钥生成中心为用户颁发签名密钥，基于多线性映射提出一个基于 ID 的代理环签名方案。本方案中共有 t 个 KGC，用 $KGC_j(j=1,2,\cdots,t)$ 表示。设 $(G_1,+),(G_2,\cdot)$ 分别是阶为 q 的循环加群和循环乘群。q 为素数，P 为 G_1 的生成元，$e_{t+1}:G_1^{t+1}\to G_2$ 为多线性映射，$H_1:\{0,1\}^*\to G_1$，$H_2:\{0,1\}^*\to Z_q$，$H_3:G_2\to Z_q$ 为抗碰撞的哈希函数。

4.1 系统创建阶段

t 个密钥生成中心 $KGC_j(j=1,2,\cdots,t)$ 分别随机选择 $S_j\in Z_q^*$，计算 $P_{pub}^{(j)}=S_jP$。因为有 t 个 S_j，所以任何一个不可信的 KGC_j 不可能伪造代理签名者的签名，系统的主密钥为 $(S_1,S_2,\cdots,S_j,\cdots,S_t)$。

系统公开参数为

$$(G_1,G_2,e_{t+1},q,P,P_{pub}^{(1)},P_{pub}^{(2)},\cdots,P_{pub}^{(t)},H_1,H_2,H_3) \tag{1}$$

4.2 密钥提取阶段

原始签名者的身份信息用 ID_o 表示，代理签名者的身份信息用 ID_k 表示，原始签名者和代理签名者将其身份信息 ID_o 和 ID_k 分别发送给 t 个密钥生成中心。

t 个密钥生成中心 KGC_j 分别计算 $Q_{ID_o}=H_2(ID_o)$，$Q_{ID_k}=H_2(ID_k)$，$S_{ID_o}^{(j)}=S_jQ_{ID_o}$，$S_{ID_k}^{(j)}=S_jQ_{ID_k}$。原始签名者的公钥为 Q_{ID_o}，代理签名者的公钥为 Q_{ID_k}。t 个密钥生成中心 $KGC_j(j=1,2,\cdots,t)$ 通过安全信道将结果分别发送给代理签名者和原始签名者。

对 $j=1,2,\cdots,t$，原始签名者验证等式 $e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,P_{pub}^{(j-1)},P,P_{pub}^{(j+1)},\cdots,P_{pub}^{(t)},S_{ID_o}^{(j)})=e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,P_{pub}^{(t)},Q_{ID_o})$ 是否成立，若 t 个等式均成立，则原始签名者秘密保存 $S_{ID_o}=(S_{ID_o}^{(1)},S_{ID_o}^{(2)},\cdots,S_{ID_o}^{(t)})$ 作为原始签名者的私钥。代理签名者验证等式 $e_{t+1}(P_{pub}^{(1)},\cdots,P_{pub}^{(j-1)},P,P_{pub}^{(j+1)},\cdots,P_{pub}^{(t)},S_{ID_k}^{(j)})=e_{t+1}(P_{pub}^{(1)},\cdots,P_{pub}^{(t)},Q_{ID_k})$ 是否成立，若 t 个等式均成立，则代理签名者秘密保存 $S_{ID_k}=(S_{ID_k}^{(1)},S_{ID_k}^{(2)},\cdots,S_{ID_k}^{(t)})$ 作为代理签名者的签名私钥。验证等式的证明如下：

$$\begin{aligned}
&e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,P_{pub}^{(j-1)},P,P_{pub}^{(j+1)},\cdots,P_{pub}^{(t)},S_{ID_o}^{(j)})=\\
&\quad e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,P_{pub}^{(j-1)},P,P_{pub}^{(j+1)},\cdots,P_{pub}^{(t)},S_jQ_{ID_o})=\\
&\quad e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,P_{pub}^{(j-1)},S_jP,P_{pub}^{(j+1)},\cdots,P_{pub}^{(t)},Q_{ID_o})=\\
&\quad e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,P_{pub}^{(j-1)},P_{pub}^{(j)},P_{pub}^{(j+1)},\cdots,P_{pub}^{(t)},Q_{ID_o})=\\
&\quad e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,P_{pub}^{(t)},Q_{ID_o})\\
&e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,P_{pub}^{(j-1)},P,P_{pub}^{(j+1)},\cdots,P_{pub}^{(t)},S_{ID_k}^{(j)})=\\
&\quad e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,P_{pub}^{(j-1)},P,P_{pub}^{(j+1)},\cdots,P_{pub}^{(t)},S_jQ_{ID_k})=\\
&\quad e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,P_{pub}^{(j-1)},S_jP,P_{pub}^{(j+1)},\cdots,P_{pub}^{(t)},Q_{ID_k})=\\
&\quad e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,P_{pub}^{(j-1)},P_{pub}^{(j)},P_{pub}^{(j+1)},\cdots,P_{pub}^{(t)},Q_{ID_k})=\\
&\quad e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,P_{pub}^{(t)},Q_{ID_k})
\end{aligned}$$

此时，原始签名者的私钥为 $S_{ID_o}=(S_{ID_o}^{(1)},S_{ID_o}^{(2)},\cdots,S_{ID_o}^{(t)})$。代理签名者的私钥为 $S_{ID_k}=(S_{ID_k}^{(1)},S_{ID_k}^{(2)},\cdots,S_{ID_k}^{(t)})$。

4.3 代理密钥生成阶段

(1)原始签名者生成一个委任状 W，详细记录一些重要信息，如原始签名者和代理签名者的身份、需要的文件等，然后计算

$$S_W=S_{ID_o}H_1(W)=(S_1Q_{ID_o}H_1(W),S_2Q_{ID_o}H_1(W),\cdots,S_tQ_{ID_o}H_1(W))$$

并发送 W 和 S_W 给代理签名者。

(2)代理签名者验证等式

$$\begin{aligned}
&e_{t+1}(S_1Q_{ID_o}H_1(W),S_2Q_{ID_o}H_1(W),\cdots,S_tQ_{ID_o}H_1(W),P)=\\
&\quad e_{t+1}(H_1(W),H_1(W),\cdots,H_1(W),P\times S_{ID_o}^{(1)}\times S_{ID_o}^{(2)}\times\cdots\times S_{ID_o}^{(t)})
\end{aligned}$$

是否成立，若成立，则计算其私钥

$$\begin{aligned}
S_R&=S_W+S_{ID_k}H_1(W)=\\
&(S_1(Q_{ID_o}+Q_{ID_k})H_1(W),S_2(Q_{ID_o}+Q_{ID_k})H_1(W),\cdots,\\
&S_t(Q_{ID_o}+Q_{ID_k})H_1(W))
\end{aligned}\tag{2}$$

此时，代理签名私钥为 S_R，代理签名公钥为 $P_R=(Q_{ID_o}+Q_{ID_k})H_1(W)$。

4.4 签名生成阶段

不失一般性地，假定环 L 中有 n 个成员，它由代理签名者进行选择，环的形成无须其他成员同意和协助，代理签名者只要知道其公钥即可。该环可以表示为

$$L=\{ID_1,ID_2,\cdots,ID_k,\cdots,ID_n\}$$

(1)代理签名者选择 $A\in G_1$，并计算

$$C_{k+1}=e_{t+1}(A,P,\cdots,P) \tag{3}$$

(2)对于 $i=k+1,\cdots,n,0,1,\cdots,k-1$，代理签名者选择 $R_i\in_R G_1$，并按以下公式计算 C_{i+1}：

$$\begin{aligned}
C_{i+1}=e_{t+1}&(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,(Q_{ID_o}+Q_{ID_i})P_{pub}^{(i)},\cdots,\\
&P_{pub}^{(t)},H_3(C_i)H_1(W))^{H_2(m\|L)}\times e_{t+1}(R_i,P,\cdots,P)
\end{aligned}\tag{4}$$

设定 $R_n=R_0$，计算

$$R_k=A-H_2(m\|L)H_3(C_k)P_R \tag{5}$$

$$R=\sum_{i=1}^{n}R_i \tag{6}$$

$$C=\sum_{i=1}^{n}C_i \tag{7}$$

$R_n=R_0$ 和式(5)保证了 $C_n=C_0$，因此，$\{C_1,C_2,\cdots,C_n,C,R\}$ 为代理签名者对消息 m 的代理环签名。

4.5 签名验证阶段

给定所有环成员的身份集 L，消息 m 以及代理环签名 $\{C_1,C_2,\cdots,C_n,C,R\}$，验证者可以通过如下公式检查代理环签名的合法性：

$$\prod_{i=1}^{n} C_i = e_{t+1}(P_{pub}^{(1)}, P_{pub}^{(2)}, \cdots, P_{pub}^{(t)}, H_1(W)\cdot$$
$$(Q_{ID_o}\cdot\sum_{i=1}^{n} H_3(C_i)+\sum_{i=1}^{n} Q_{ID_i}\cdot H_3(C_i)))^{H_2(m\|L)}\cdot$$
$$e_{t+1}(R,P,\cdots,P)$$

如果上式成立，则该签名为有效的代理环签名。

5 性能分析

5.1 可行性分析

在公式 $C_{i+1}=e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,(Q_{ID_o}+Q_{ID_i})P_{pub}^{(i)},\cdots,P_{pub}^{(t)},H_3(C_i)H_1(W))^{H_2(m\|L)}\times e_{t+1}(R_i,P,\cdots,P)$ 中，由于 $H_1(W)\in G_1$，$H_3(C_i)\in Z_q$，因此可以计算出 $H_3(C_i)\times H_1(W)\in G_1$。在公式 $R_k=A-H_2(m\|L)H_3(C_k)P_R$ 中，因为 $H_2(m\|L)\in Z_q$，$H_3(C_k)\in Z_q$，$P_R\in G_1$，所以可以计算出 $R_k=A-H_2(m\|L)H_3(C_k)P_R\in G_1$。

5.2 安全性分析

根据代理环签名的安全需求，分析本文提出的基于身份和多线性对的代理环签名方案的安全性。

(1)签名者模糊性。对一个由环 $L=\{ID_1,ID_2,\cdots,ID_k,\cdots,ID_n\}$ 产生的合法代理环签名 σ_m，当 $i\neq k+1$ 时，所有 C_i 都由式(4)生成。由于 $R_i\in G_1$ 是被代理签名者随机均匀选择的，因此 C_i 在 $G_2(i\neq k)$ 中是均匀分布的。代理环签名的起点 C_{k+1} 由式(3)计算。因为 $A\in G_1$ 是被代理签名者随机均匀选择的，所以 C_{k+1} 在 G_2 中是均匀分布的。无论谁对消息 m 进行了签名或环成员数量有多大，σ_m 对每个环成员都是等概率的。因此，给定一个代理环签名后，攻击者(原始签名者除外)即使有无穷的计算资源，他试图确定真实签名者身份的概率不会超过 $1/n$(n 为环成员的数量)。

(2)不可伪造性。对于一个身份集 $L=\{ID_1,ID_2,\cdots,ID_k,\cdots,ID_n\}$，假定 A 不是真实签名者，当他试图伪造一个合法的代理环签名时，可以通过选择一个身份信息 ID_j，与 $KGC_j(j=1,2,\cdots,t)$ 执行协议得到密钥对 $(Q_j,S_j^{(1)},S_j^{(2)},\cdots,S_j^{(t)})$，其中，$Q_j=H_2(ID_j)$，$S_j^{(i)}=S_iQ_j(i=1,2,\cdots,t)$。为达到伪造代理环签名的目的，攻击者需要多次选择 ID_j，以使 $H_2(ID_j)=H_2(ID_k)$，其中，ID_k 为代理签名者(真实签名者)的身份信息。但由散列函数的性质可知，这是不可能的，又由于代理签名私钥中包含代理签名者的私钥信息，因此原始签名者也无法伪造代理环签名。所以，在本文提出的方案中，代理环签名是不可伪造的。

(3)可验证性。根据代理环签名生成的过程可以得到如下公式：

$$C_{i+1}=e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,(Q_{ID_o}+Q_{ID_i})P_{pub}^{(i)},\cdots,$$
$$P_{pub}^{(t)},H_3(C_i)H_1(W))^{H_2(m\|L)}\times e_{t+1}(R_i,P,\cdots,P)$$
$$\prod_{i=1}^{n} C_i=\prod_{i=1}^{n} e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,(Q_{ID_o}+Q_{ID_i})P_{pub}^{(i)},\cdots,$$
$$P_{pub}^{(t)},H_3(C_i)H_1(W))^{H_2(m\|L)}\times$$
$$e_{t+1}(R_i,P,\cdots,P)=$$
$$e_{t+1}((Q_{ID_o}+Q_{ID_1})P_{pub}^{(1)},P_{pub}^{(2)},\cdots,$$
$$P_{pub}^{(t)},H_3(C_1)H_1(W))^{H_2(m\|L)}\times e_{t+1}(R_1,P,\cdots,P)\cdot$$
$$e_{t+1}(P_{pub}^{(1)},(Q_{ID_o}+Q_{ID_2})P_{pub}^{(2)},P_{pub}^{(3)},\cdots,$$
$$P_{pub}^{(t)},H_3(C_2)H_1(W))^{H_2(m\|L)}\times e_{t+1}(R_2,P,\cdots,P)$$
$$\vdots$$
$$e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,(Q_{ID_o}+Q_{ID_o})P_{pub}^{(n)},\cdots,$$
$$P_{pub}^{(t)},H_3(C_n)H_1(W))^{H_2(m\|L)}\times e_{t+1}(R_n,P,\cdots,P)=$$
$$e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,P_{pub}^{(t)},(Q_{ID_o}+Q_{ID_1})$$
$$H_3(C_1)H_1(W))^{H_2(m\|L)}\times e_{t+1}(R_1,P,\cdots,P)\cdot$$
$$e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},P_{pub}^{(3)},\cdots,P_{pub}^{(t)},(Q_{ID_o}+Q_{ID_2})$$
$$H_3(C_2)H_1(W))^{H_2(m\|L)}\times e_{t+1}(R_2,P,\cdots,P)\cdot$$
$$\vdots$$
$$e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,P_{pub}^{(n)},\cdots,P_{pub}^{(t)},(Q_{ID_o}+Q_{ID_n})$$
$$H_3(C_n)H_1(W))^{H_2(m\|L)}\times e_{t+1}(R_n,P,\cdots,P)=$$
$$\prod_{i=1}^{n} e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,P_{pub}^{(t)},(Q_{ID_o}+Q_{ID_i})$$
$$H_3(C_i)H_1(W))^{H_2(m\|L)}\cdot e_{t+1}(R,P,\cdots,P)$$
$$e_{t+1}(P_{pub}^{(1)},P_{pub}^{(2)},\cdots,P_{pub}^{(t)},H_1(W)\cdot(Q_{ID_o}\cdot\sum_{i=1}^{n} H_3(C_i)+$$
$$\sum_{i=1}^{n} Q_{ID_i}\cdot H_3(C_i)))^{H_2(m\|L)}\cdot e_{t+1}(R,P,\cdots,P)$$

因此，代理环签名是可验证的。

(4)不可否认性。因为代理签名私钥 $S_R=S_W+S_{ID_k}H_1(W)$ 中包含代理签名者的身份信息，所以他不能向原始签名者否认由其生成的有效代理环签名。

(5)可鉴别性。由于代理签名者本人的公钥与代理签名公钥不同，因此任何人都可以区别由代理签名者产生的代理环签名和正常环签名。

6 结束语

本文借鉴在双线性对上提出的代理环签名思想，提出一种基于多线性映射的代理环签名方案。本方案继承了原有基于双线性对的代理环签名的优点，并通过多个密钥生成中心有效避免了任何一个不可信密钥生成中心对代理环签名的伪造。但多个密钥生成中心的引入导致方案结构较复杂，该问题有待研究并解决。

参考文献

[1] Rivest R L, Shamir A, Tauman Y. How to Leak a Secret[C]//Proc. of ASIACRYPT'01. [S. l.]: Springer-Verlag, 2001: 552-565.

[2] Zhang Fangguo, Safavi-Naini R, Lin Chih-Yin. New Proxy Signature, Proxy Blind Signature and Proxy Ring Signature Schemes from Bilinear Pairings[Z]. Cryptology Eprint, 2003.

[3] Lang Weimin, Yang Zongkai, Cheng Wenqing, et al. A New Improved ID-based Proxy Ring Signature Scheme from Bilinear Pairings[J]. Journal of Harbin Institute of Technology, 2006, 13(6): 688-691.

[4] 杨少春，郎为民. 基于身份和双线性对的代理环签名方案[J]. 微计算机信息, 2006, 22(12): 79-81.

[5] 吕小红，郎为民，夏　婧. 一种改进的代理环签名[J]. 微计算机信息, 2006, 22(27): 79-81.

[6] 隗　云，鲍皖苏. 基于多线性映射的环签名研究[J]. 计算机应用研究, 2008, 25(2): 524-525.

编辑　陈　晖