第 36 卷 第 4 期 计 算 机 工 程 2010 年 2 月
Vol。36 No.4 Computer Engineering February 2010
·安全技术· 文章编号：1000—3428(2010)04—0138—02 文献标识码：A 中图分类号：TP309

基于双线性对的匿代理盲聚合签名方案

毛卫霞，李志慧，柳 烨
(陕西师范大学数学与信息科学学院，西安 710062)

摘 要：利用聚合签名的优点，提出一种基于双线性对的匿代理盲聚合签名方案。聚合签名能将 n 个签名聚合成唯一的一个短签名，从而使 n 个验证等式减少为一个验证等式。理论分析证明，该方案保护了代理签名人的隐私权，使签名的消息不可见，在事后引起争议时还可以追踪到代理签名人的身份。

关键词：代理签名；匿签名；盲签名；聚合签名；双线性对

Anonymous Proxy Blind Aggregate Signature Scheme Based on Bilinear Pairing

MAO Wei-xia, LI Zhi-hui, LIU Ye
(College of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062)

【Abstract】 By utilizing the advantage of aggregate signature, this paper proposes an anonymous proxy blind aggregate signature scheme based on bilinear pairing. An aggregate signature scheme aggregates n signatures into one, thus n verification equations can be reduced to become one. Theory analysis proves that the scheme provides privacy protection for the proxy signer and blinds the message, and in case of dispute later on, the identity of the proxy signer can be traced.

【Key words】 proxy signature; anonymous signature; blind signature; aggregate signature; bilinear pairing

1 概述

代理签名是指原始签名人由于出差、生病、资源限制等原因不能签名，于是将签名权委托给代理签名人，让代理签名人对消息进行签名[1]。代理签名方案有 3 种类型：完全代理，部分代理，具有授权证书的代理。在实际应用中，代理签名人的隐私权需要得到保护。因此，具有授权证书的代理受保护的部分代理签名方案[2-3]受到越来越广泛的关注。

文献[4]提出了匿签名的概念，匿签名是指对于一个有效的签名，用户只知道该签名是由合法的签名者所签，但是不知道签名者到底是谁。文献[4]给出了 2 种匿签名方案，并分析了它们的性能。文献[5]提出了一种有效的可证明安全的匿代理签名方案，但在事后引起争议时，无法追踪到代理签名人的身份，并且对签名消息的长度有一定的限制。文献[6]提出了盲签名的概念。盲签名是指签名者在不知道被签文件内容的情况下对文件进行签名。文献[7]利用双线性配对函数的特性，提出了聚合签名方案。一个聚合签名是一个支持聚合的数字签名：给定来自 n 个不同签名者 i $(1 \le i \le n)$ 对 n 个不同消息 m_i 的 n 个不同的签名，可以将所有的签名聚合成唯一的短签名。该方案在验证的过程中可以减少计算量，但是不具有盲性和匿名性。

2 背景知识

定义 1 令 G_1 和 G_2 分别是阶为大素数 q 的加群和乘群，其中，$q > 2^l$；l 为安全参数；P 为 G_1 的生成元。$\hat{e}: G_1 \times G_1 \to G_2$ 是一个映射，若 $\hat{e}$ 满足下列 3 个性质，则称 $\hat{e}$ 为一个双线性对。

(1)双线性：对所有的 $P,Q \in G_1$ 和 $a,b \in Z$，有 $\hat{e}(aP,bQ) = \hat{e}(P,Q)^{ab}$。

(2)非退化性：存在 $P,Q \in G_1$，使得 $\hat{e}(P,Q) \ne 1$。

(3)可计算性：对所有的 $P,Q \in G_1$，存在有效的算法计算 $\hat{e}(P,Q)$。

在这样的群 G_1 上，存在如下密码学问题：

(1)离散对数问题(DLP)：给定 $P,Q \in G_1$，找出整数 a，使得 $Q = aP$，如果这样的整数 a 存在。

(2)计算 Diffie-Hellman 问题(CDHP)：给定 $P,aP,bP \in G_1$，对于所有的 $a,b \in Z_q^*$，计算 abP。

(3)判定 Diffie-Hellman 问题(DDHP)：给定 $P,aP,bP,cP \in G_1$，对于所有 $a,b,c \in Z_q^*$，判定 $c = ab \bmod q$ 是否成立。

假设群 G_1 上的 CDHP 和 DLP 都是难解问题。当群上的 DDHP 容易而 CDHP 难解时，该群称为 GDH(Gap Diffie-Hellman)群。这样的群可以在超椭圆曲线中找到，并且可以利用超椭圆曲线上的 Weil 对或经改造的 Tate 对来构造双线性对。具体细节见文献[8]。

定义 2 设 $A = \{A_1, A_2, \cdots, A_n\}$ 为签名者集合，C 为攻击者。假设有一个 A_s 的签名 σ_{A_s}，则 C 能够猜出 σ_{A_s} 是 A_s 所签的概率为 $\frac{1}{n+\varepsilon}$。若 $\varepsilon = 0$，C 的成功概率为 $\frac{1}{n}$，此时，称该签名

基金项目：国家自然科学基金资助项目(60873119)；陕西省自然科学基础研究计划基金资助项目(2007A06)
作者简介：毛卫霞(1983－)，女，硕士研究生，主研方向：密码学；李志慧，副教授、博士；柳 烨，硕士研究生
收稿日期：2009-08-27 **E-mail：**ccde456@163.com

具有全匿名性。

3 基于双线性对的匿代理盲聚合签名方案

令 O 为原始签名者，$\{P_1,P_2,\cdots,P_n\}$ 为代理签名者的集合，U 为用户，M 为管理者。消息 $m\in\{0,1\}^*$ 由 n 个不同的子消息组成，即 $m=\{m_1,m_2,\cdots,m_n\}$。有一个公告牌，读者只能下载和阅读，不能更改和书写，参与者要公布的信息均写在公告牌上。

首先介绍管理者(文献[4]称为 Anonymous Signature Service Provider)的身份。管理者有 3 个职责：(1)向用户保证签名是由合法的签名者所签；(2)向签名者保证签名者的身份不被泄露；(3)在事后引起争议时，由管理者公开签名者的身份。管理者只是起到隐藏签名者身份的作用，并不能真正地决定签名。用户知道从管理者那儿所得到的签名并不是签名者的真正签名，但确是由合法的签名者所签。

3.1 系统初始化阶段

参数 $(G_1,G_2,q,l,P,\hat{e})$ 与定义 1 中的参数相同，定义安全的哈希函数 $H_0:\{0,1\}^*\times G_1\to Z_q^*$ 和 $H_1:\{0,1\}^*\to G_1$。公布 $(G_1,G_2,q,\hat{e},P,H_0,H_1)$。

3.2 密钥生成阶段

原始签名者 O、代理签名者 $P_i\in\{P_1,P_2,\cdots,P_n\}$、管理者 M 分别随机选取 $x_0,x_i,x\in Z_q^*$ 为各自的私钥，其公钥依次为 $y_0=x_0P$，$y_i=x_iP$，$y=xP$。用户 U 随机选取 $x_u\in Z_q^*$ 为私钥，其公钥为 $y_u=x_uP$。

3.3 代理授权阶段

代理授权阶段包括 2 个步骤：

(1)原始签名者 O 和代理签名者集合 $\{P_1,P_2,\cdots,P_n\}$ 商议制定代理授权书 m_w，其中包括原始签名者和代理签名者的身份、代理签名文件的范围、代理终止日期等信息。原始签名者 O 随机选取 $r\in Z_q^*$，计算 $R=rP$，$s=r-x_0H_0(m_w,R)\bmod q$。然后发送 s 给代理签名者集合 $\{P_1,P_2,\cdots,P_n\}$，公布 (m_w,R)。

(2)代理签名者集合 $\{P_1,P_2,\cdots,P_n\}$ 接收到 s 后，验证式(1)是否成立。

$$R=sP+H_0(m_w,R)y_0 \tag{1}$$

若成立，$\{P_1,P_2,\cdots,P_n\}$ 接受代理，每个代理签名者 $P_i\in\{P_1,P_2,\cdots,P_n\}$ 计算其代理签名私钥 $Psk_i=s-x_iH_0(m_w,R)\bmod q$，其对应的公钥为

$$Pub_i=Psk_i\cdot P=sP-H_0(m_w,R)y_i=R-H_0(m_w,R)(y_0+y_i) \tag{2}$$

3.4 代理签名阶段

代理签名阶段包括 3 个步骤：

(1)用户 U 首先检验式(2)是否成立，若成立，随机选取 $u_1,u_2\in Z_q^*$，计算 $t_i'=H_1(m_i\,\|\,m_w)$，$t_i=u_1^{-1}t_i'-u_2y_u$。然后发送 $t_i(i=1,2,\cdots,n)$ 给管理者 M。

(2)管理者 M 随机选取 $P_s\in\{P_1,P_2,\cdots,P_n\}$（$P_s$ 不一定就是 P_i），令 $t_i=t_{P_s}$，发送 (Pub_s,t_{P_s}) 给代理签名者 P_s，请 P_s 对消息 m_i 进行盲签名。

(3)代理签名者 P_s 计算 $\sigma_s'=Psk_sH_0(m_w,R)(t_{P_s}+y_0+y_s)$，将 σ_s' 发送给管理者 M。

3.5 管理者签名阶段

管理者签名阶段包括 2 个步骤：

(1)因为有 n 个子消息 m_i，所以有 n 个签名 σ_i' $(i=1,2,\cdots,n)$。管理者 M 将 n 个签名 σ_i' $(i=1,2,\cdots,n)$ 聚合成一个签名 $\sigma'=\sum_{i=1}^{n}\sigma_i'$。公布 σ'。

(2)管理者 M 验证式(3)是否成立，若成立，管理者 M 计算 $\sigma_i=xH_0(m_w,R)\sigma_i'$，将 $\sigma_i(i=1,2,\cdots,n)$ 发送给用户 U。

$$\hat{e}(\sigma',P)=\prod_{i=1}^{n}\hat{e}(H_0(m_w,R)(t_{P_i}+y_0+y_i),Pub_i) \tag{3}$$

3.6 用户验证阶段

用户 U 把 n 个签名 $\sigma_i(i=1,2,\cdots,n)$ 聚合成一个签名 $\sigma=\sum_{i=1}^{n}\sigma_i$，并验证式(4)是否成立。若成立，签名 σ 就是关于消息 m 的匿代理盲聚合签名。

$$\hat{e}(\sigma,P)=\hat{e}(\sigma',H_0(m_w,R)y) \tag{4}$$

4 方案分析

4.1 正确性分析

分析式(3)和式(4)的正确性。

$$\hat{e}(\sigma',P)=\hat{e}(\sum_{i=1}^{n}\sigma_i',P)=\hat{e}(\sum_{i=1}^{n}Psk_iH_0(m_w,R)(t_{P_i}+y_0+y_i),P)=\prod_{i=1}^{n}\hat{e}(H_0(m_w,R)(t_{P_i}+y_0+y_i),Pub_i)$$

$$\hat{e}(\sigma,P)=\hat{e}(\sum_{i=1}^{n}\sigma_i,P)=\hat{e}(\sum_{i=1}^{n}xH_0(m_w,R)\sigma_i',P=\hat{e}(\sum_{i=1}^{n}\sigma_i',H_0(m_w,R)y)=\hat{e}(\sigma',H_0(m_w,R)y)$$

4.2 性能分析

性能分析阶段包括 6 个方面：

(1)全匿名性和可追踪性：从管理者 M 的身份看出，用户 U 和代理签名者集合 $\{P_1,P_2,\cdots,P_n\}$ 对管理者 M 具有绝对的信任，因此，满足全匿名性和可追踪性。

(2)不可伪造性：方案中有 2 个签名阶段：代理签名阶段和管理者签名阶段。在代理签名阶段，攻击者想利用等式 $\sigma_s'=Psk_sH_0(m_w,R)(t_{P_s}+y_0+y_s)$ 伪造签名，需知道 Psk_s，而 Psk_s 为代理签名者 P_s 的代理签名私钥，求解 Psk_s 将面临离散对数问题，因此，攻击者无法伪造签名。在管理者签名阶段，攻击者想利用等式 $\sigma_i=xH_0(m_w,R)\sigma_i'$ 伪造签名，需知道 x，而 $x\in Z_q^*$，攻击者只能采取猜测的方式，其成功的概率为 $1/q$。

(3)可验证性：管理者 M 已经利用式(3)验证了代理签名的正确性，并在验证的过程中使用了原始签名人的公钥 y_0，因此，原始签名人 O 同意将签名权委托给代理签名者集合 $\{P_1,P_2,\cdots,P_n\}$。用户 U 可以利用式(4)验证管理者 M 签名的正确性，并且用户 U 对管理者 M 具有绝对的信任。因此，原始签名人 O 不能否认将签名权委托给代理签名者集合 $\{P_1,P_2,\cdots,P_n\}$。

(4)可区分性：代理授权书 m_w 中已标明原始签名人 O 和代理签名人 $\{P_1,P_2,\cdots,P_n\}$ 的身份，并且有管理者 M 的参与，因此，任何人可以区分匿代理盲聚合签名和一般的签名。

(5)防止滥用性：代理授权书 m_w 中已明确规定了代理签名人 $\{P_1,P_2,\cdots,P_n\}$ 签名文件的范围和代理终止时间等信息，因此，对于任何没有授权要签署的文件，每个代理签名者都不能用自己的代理签名私钥签署。

(下转第 143 页)