第 37 卷 第 14 期
Vol.37 No.14

计 算 机 工 程
Computer Engineering

2011 年 7 月
July 2011

• 安全技术 •

文章编号：1000—3428(2011)14—0112—02 文献标识码：A 中图分类号：TP311.52

一个无证书代理盲签名方案

张建中，彭丽慧，薛荣红

(陕西师范大学数学与信息科学学院，西安 710062)

摘 要：将无证书公钥密码体制和代理盲签名相结合，利用两者的优点，提出一个无证书代理盲签名方案。该方案具有盲签名的盲性以及不可追踪性，同时消除了对证书的依赖，能够解决密钥的托管问题。在适应性选择消息及适应性选择身份攻击下，该方案可以体现出存在性不可伪造的特点，能够有效抵抗公钥替换攻击。

关键词：无证书公钥密码体制；代理盲签名；随机预言机模型；不可追踪性；不可伪造性

Certificateless Proxy Blind Signature Scheme

ZHANG Jian-zhong, PENG Li-hui, XUE Rong-hong

(College of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062, China)

【Abstract】Combined with certificateless public key cryptography with proxy blind signature, a certificateless proxy blind signature scheme is proposed. The scheme enjoys the blindness properties and untraceability, and solves the escrow problem and retains the merits of blind signature without certificate. The new scheme is proved to be secure against existential forgery on adaptively chosen message attack and chosen identity attack.

【Key words】certificateless public key cryptography; proxy blind signature; random oracle model; untraceability; unforgeability

DOI: 10.3969/j.issn.1000-3428.2011.14.036

1 概述

1996 年，Mambo M 等人首次提出代理签名的概念[1]，即原始签名人由于某种原因不能行使签名权时，便将签名权授权给代理签名人，由代理签名人替代行使签名权。代理签名在移动通信、电子货币、电子选举等方面有着广泛应用前景。由于电子支付的匿名性的要求，Chaum D 等人在 1982 年的美国密码学会议上提出盲签名的概念[2]，它是用户和签名者之间的一个交互协议，如果双方都正确执行协议，消息 m 的拥有者可以得到签名者对消息 m 的签名，而签名者不知道所签消息 m 的具体内容，事后签名者也无法追踪消息。结合代理签名和盲签名，文献[3]提出代理签名盲签名得到概念，随后人们提出满足各种需求的代理盲签名方案[4-5]。

基于身份的公钥密码体制的安全性完全依赖于密钥生成中心 KGC，KGC 生成用户的私钥并通过安全信道将其传送给用户。但是，一个恶意的 KGC 可以通过伪造用户的签名来陷害用户，所以该体制不存在真正的不可否认性。文献[6]提出一种无证书公钥密码体制。在该体制中，KGC 不直接生成用户得到私钥，而是根据用户的身份信息生成用户的部分私钥，用户根据 KGC 提供的部分私钥和自己生成的秘密信息共同生成用户私钥。这样就解决了基于身份的公钥密码体制中的密钥托管问题，提高了系统的运行效率。

本文将无证书公钥密码体制与代理盲签名技术结合，充分利用两者的优点，提出一种无证书的代理盲签名方案。

2 相关知识

2.1 双线性映射

设 G_1，G_2 分别为阶为大素数 q 的加法循环群和乘法循环群，P 是 G_1 的一个生成元，即 $G_1=\langle P\rangle$。假设在群 G_1，G_2 中的离散对数问题是难解的。一个双线性对是指满足下面 3 个性质的一个映射：$e:G_1\times G_1\to G_2$。

(1)双线性性：对任意的 $R,Q\in G_1,a,b\in Z_q^*$，都有 $e(aR,bQ)=e(R,Q)^{ab}$；

(2)非退化性：存在 $R,Q\in G_1$，使得 $e(R,Q)\neq 1$；

(3)可计算性：对于任意的 $R,Q\in G_1$，存在一个有效的算法计算 $e(R,Q)$。

这样的双线性映射可以通过有限域上的超奇异椭圆曲线或超椭圆曲线上得到 Weil 对或 Tate 对构造实现。

2.2 相关的数学难题

(1)离散对数问题(DLP)：任意给定 G 中的 2 个元素 P,Q，求整数 $n\in Z_q^*$，使得 $Q=nP$ 成立。

(2)计算 Diffie-Hellman 问题(CDHP)：给定 $P,aP,bP\in G$，其中，$a,b\in Z_q^*$，计算 abP。

(3)双线性对分叉问题：即给定 $P\in G_1$，$r\in G_2$，找到 $Q\in G_1$，使得 $r=e(P,Q)$ 成立是困难的。

3 一个无证书的代理盲签名方案

本文基于无证书密码体制和代理盲签名提出了无证书代理盲签名方案，方案的参与实体为密钥生成中心 KGC、原始签名者 A、代理签名者 B、消息拥有者 C。方案由系统的建立、部分私钥生成、用户密钥的生成、代理授权的产生、代理盲签名的生成、代理盲签名的验证 6 个部分组成。方案具体构造如下：

基金项目：国家自然科学基金资助项目(10571113)；陕西省自然科学研究计划基金资助项目(2009JM8002)；陕西省教育厅科学研究计划自然科学基金资助项目(07JK375, 2010JK829)

作者简介：张建中(1960－)，男，教授、博士，主研方向：密码学，信息安全；彭丽慧(通讯作者)、薛荣红，硕士研究生

收稿日期：2011-02-23 **E-mail：**bobpep0416@163.com

(1)系统的建立

KGC 首先输入安全参数 1^k，生成系统参数 (G_1,G_2,q,e)；随机选取群 G_1 的一个生成元 $P\in G_1$；随机选取主密钥 $s\in_R Z_q^*$，并计算 $P_{Pup}=sP$ 作为系统的公钥；选取 3 个安全的 Hash 函数 $H_1:\{0,1\}^*\to G_1, H_2:\{0,1\}^*\times G_1\to G_1, H_3:\{0,1\}^*\times G_2\to Z_q^*$。KGC 公开系统参数 $\{G_1,G_2,q,e,P,P_{Pup},H_1(\cdot),H_2(\cdot,\cdot),H_3(\cdot,\cdot)\}$。

(2)部分密钥的提取

KGC 首先验证用户的身份信息 ID_i，其中 $ID_i\in\{0,1\}^*$，并计算其部分私钥为 $D_i=s^{-1}Q_i$，其中 $Q_i=H_1(ID_i)$，然后 KGC 通过安全的秘密信道将 D_i 传送给用户 i，则用户 A,B 的部分私钥为 $D_A=s^{-1}Q_A, D_B=s^{-1}Q_B$，其中，$Q_A=H_1(ID_A), Q_B=H_1(ID_B)$。

(3)密钥的生成

用户 i 收到 D_i 后，首先验证等式 $e(D_i,P_{Pup})=e(Q_i,P)$ 是否成立，以检验其部分私钥的合法性。用户 A,B 分别随机选取 $x_A,x_B\in_R Z_q^*$ 作为其秘密值，并计算其公私钥。A 的私钥为 $S_A=x_AD_A$，对应的公钥为 $P_A=x_AP$；B 的私钥为 $S_B=x_BD_B$，公钥为 $P_B=x_BP$。

(4)代理授权的产生

A 若要将签名权授权给 B，首先生成授权证书 w，其中 w 包括 A, B 的身份信息、代理签名消息的范围、代理权限等信息，然后随机选择 $k_A\in_R Z_q^*$，计算 $r_A=k_AP_{Pup}$，$S_w=S_A+k_AH_2(w,r_A)$，最后将 (w,r_A,S_w) 发送给 B。

B 收到 (w,r_A,S_w) 后，验证等式 $e(S_w,P)=e(Q_A,P_A)e(r_A,H_2(w,r_A))$ 是否成立。如果成立，B 将生成代理签名密钥 $S_p=S_w+S_B$。否则，B 将要求 A 发送有效的授权信息或拒绝接受代理授权。

(5)代理盲签名的产生

设待签消息 $m\in\{0,1\}^*$，消息的拥有者 C 和代理签名者 B 将执行如下的交互协议：

消息拥有者 C　　代理签名者 B

随机选取 $P_2\in_R G_1$，计算 $U'=e(P_2,P_{Pup})$

$\xleftarrow{U'}$

随机选取 $\alpha,\beta\in_R Z_q^*$，计算

$U=U'^{\alpha}\left[e(Q_A,P_A)e(Q_B,P_B)e(r_A,H_2(w,r_A))\right]^{\alpha\beta}$

$h=\alpha^{-1}H_3(m,U)+\beta$

$\xrightarrow{h}$

$V'=hS_p+P_2$

$\xleftarrow{V'}$

$V=\alpha V'$

则消息 m 的代理盲签名为 $\sigma(m)=(w,r_A,U,V)$。

(6)代理盲签名的验证

首先，验证者通过授权证书 w 检验代理签名人是否被授权、消息 m 是否合乎要求、代理签名者是否存在滥用签名权等问题，若都符合要求，则输入系统公开参数、消息 $m\in\{0,1\}^*$、原始签名人和代理签名人的身份信息 ID_A,ID_B 和其公钥 P_A,P_B、代理盲签名 (w,r_A,U,V)，验证下面等式是否成立 $e(V,P_{Pup})=U\left[e(Q_A,P_A)e(Q_B,P_B)e(r_A,H_2(w,r_A))\right]^{H_3(m,U)}$。若等式成立，则 $\sigma(m)=(w,r_A,U,V)$ 是一个有效的代理盲签名。否则，签名无效。

4 方案分析

下面分析方案的有效性、盲性及不可追踪性，并在随机预言模型和椭圆曲线上离散对数问题的难解下，分析了方案的存在性不可伪造。

4.1 有效性证明

由于

$$\begin{aligned}e(V,P_{Pup})&=e(\alpha V',P_{Pup})=\\&e((H_3(m,U)+\alpha\beta)S_p+\alpha P_2,P_{Pup})=\\&e(s^{-1}x_AQ_A+s^{-1}x_BQ_B+k_AH_2(w,r_A),P_{Pup})^{\alpha\beta+H_3(m,U)}e(\alpha P_2,P_{Pup})=\\&(e(Q_A,P_A)e(Q_B,P_B)e(r_A,H_2(w,r_A)))^{\alpha\beta+H_3(m,U)}U'^{\alpha}=\\&U(e(Q_A,P_A)e(Q_B,P_B)e(r_A,H_2(w,r_A)))^{H_3(m,U)}\end{aligned}$$

因此该代理盲签名是有效的。

4.2 盲性

本文提出的一个无证书代理盲签名方案具有盲性和不可追踪性。

对于任意给定的一个有效的代理盲签名 (w,r_A,U,V) 及在代理盲签名过程中产生的视图 (U',h,V')，总存在唯一一对盲因子 α,β，使得下面的等式成立：

$$U=U'^{\alpha}\left[e(Q_A,P_A)e(Q_B,P_B)e(r_A,H_2(w,r_A))\right]^{\alpha\beta} \quad (1)$$

$$h=\alpha^{-1}H_3(m,U)+\beta \quad (2)$$

$$V=\alpha V' \quad (3)$$

由式(3)知，$\alpha\in Z_q^*$ 是唯一存在的，令 $\alpha=\log_{V'}^{V}$。由式(2)可得：$\beta=h-(\log_{V'}^{V})^{-1}H_3(m,U)$，则 β 也是唯一存在的。下证盲因子 α,β 满足式(1)。由于 (w,r_A,U,V) 是一个有效的签名，则：$e(V,P_{Pup})=U\left[e(Q_A,P_A)e(Q_B,P_B)e(r_A,H_2(w,r_A))\right]^{H_3(m,U)}$，只需证 $U'^{\alpha}[e(Q_A,P_A)e(Q_B,P_B)e(r_A,H_2(w,r_A))]^{\alpha\beta}=U$ 即可：

$$\begin{aligned}&U'^{\alpha}[e(Q_A,P_A)e(Q_B,P_B)e(r_A,H_2(w,r_A))]^{\alpha\beta}=\\&e(\alpha P_2,P_{Pup})[e(Q_A,P_A)e(Q_B,P_B)e(r_A,H_2(w,r_A))]^{\alpha\beta}=\\&e(\alpha(V'-hS_p),P_{Pup})[e(Q_A,P_A)e(Q_B,P_B)e(r_A,H_2(w,r_A))]^{\alpha\beta}=\\&e(V,P_{Pup})e(S_p,P_{Pup})^{\alpha h}[e(Q_A,P_A)e(Q_B,P_B)e(r_A,H_2(w,r_A))]^{\alpha\beta}=\\&U[e(Q_A,P_A)e(Q_B,P_B)e(r_A,H_2(w,r_A))]^{H_3(m,U)}\cdot\\&[e(Q_A,P_A)e(Q_B,P_B)e(r_A,H_2(w,r_A))]^{-H_3(m,U)}=U\end{aligned}$$

则 α,β 满足式(1)。由于盲因子 $\alpha,\beta\in_R Z_q^*$ 是随机选取的，由 $V,V'\in G_1$ 通过 $V=\alpha V'$ 求 α 将面临离散对数困难问题，因此代理签名者无法将其签名和有效签名联系起来，方案具有盲性和不可追踪性。

4.3 存在性不可伪造

在文献[6]中，针对无证书盲签名方案定义了 2 种类型的敌手攻击：(1)类型Ⅰ攻击者 A_1 不能询问主密钥，但能替换任何实体的公钥；(2)类型Ⅱ攻击者 A_2 能够询问主密钥，但不能替换公钥。本文中的无证书盲签名对上述 2 种类型的敌手攻击是存在性不可伪造的。

定理 1 在随机预言模型下，对于类型Ⅰ的敌手攻击，该方案是存在性不可伪造的。

在公钥替换攻击中，由于攻击者 A_1 不知道用户 i 的部分私钥 D_i 的信息，因此攻击者不能得到签名者的私钥 S_i。即使主动攻击的敌手能够自己选择 P_i' 来代替用户 i 的公钥 P_i，也无法通过验证方程，因为在验证方程中要用到系统公钥 P_{Pup}。所以，攻击者 A_1 不能够伪造出有效的代理盲签名，方案对于类型Ⅰ攻击者 A_1 的攻击是安全的。

(下转第 117 页)