DOI:10.16783/j.cnki.nwnuz.2008.02.011


# 改进的基于身份无可信中心的代理签名

樊 睿，王彩芬
(西北师范大学 数学与信息科学学院，甘肃 兰州 730070)

**摘 要**：根据基于身份无可信中心签名的性质，证明了已有的基于身份无可信中心的代理签名方案是不安全的，不能抵抗PKG的伪造攻击．不诚实的PKG可以伪造用户的授权签名和代理密钥，用伪造的授权签名生成消息的代理签名．对原有方案加以改进，提出了一种新的能够抵抗PKG伪造攻击的签名方案．分析表明，该方案不仅能满足代理签名所要求的所有性质，而且其效率也优于已有方案．

**关键词**：代理签名；基于身份；不可信PKG；BDH问题
**中图分类号**：TN 918.1 **文献标识码**：A **文章编号**：1001-988X(2008)02-0040-04

# Improved ID-based proxy signature without a trusted party

FAN Rui，WANG Cai-fen
(College of Mathematics and Information Science，Northwest Normal University，Lanzhou 730070，Gansu，China)

**Abstract**：The proposed ID-based proxy signature without trusted party is proved insecure by using the property of ID-based signature scheme without trusted PKG，it can not resist forgery attack．A dishonest PKG can forge a warrant signature and proxy signing key，then the PKG can successfully counterfeit original signer，and make the proxy signer to sign message for him．By improving the original scheme，a new scheme is proposed，which can withstand the forgery attack of untrusting PKG．The testing results show that our new proxy signature scheme is more efficient．

**Key words**：proxy signature；ID-based；untrusting PKG；bilinear Diffie-Hellman problem

1984年Shamir提出了基于身份的加密、签名、认证思想[1]，将公开的身份信息(姓名、地址、电子邮件地址等)作为用户公钥部分，用户私钥由一个称为私钥生成中心(PKG)的可信第三方生成．相对于PKI/CA技术，基于身份的密码体制无须公钥证书的管理与鉴别，在应用中带来极大的便利．Boneh和Franklin[2]为基于身份的加密体制定义了一个安全的模型，它的结构基于双线性Diffie-Hellman(BDH)问题．双线性映射及相关计算问题的提出和椭圆曲线上Weil对和Tate对的成功应用[3]，使得基于身份的密码体制可以高效地实现．但是基于身份的方法通常需要交互式身份协议来认证用户的身份．由于SA为每个用户选择私钥，从而SA能产生任意合法用户的有效公私钥对冒充该用户．2005年Liao Jian等人[4]提出了基于身份无可信中心的签名方案，解决了在基于身份的密码体制中密钥托管的问题，如恶意PKG可以解密任何人用公钥加密过的密文，同时，也可以伪造任何人的签名．

代理签名的概念是1996年由Mambo，Usuda和Okamoto[5]首先提出的，它指当某个签名人因某种原因不能签名时，将签名权委托给他人(称为代理人)替自己行使签名权．根据授权可对代理签名进行分类，即完全授权方案(full delegation)、

**收稿日期**：2007-10-11；**修改稿收到日期**：2008-02-26
**基金项目**：甘肃省自然科学基金资助项目(3ZS051-A25-042)；甘肃省科技攻关项目(2GS064-A52-035-03)；西北师范大学学生学术科研资助金资助项目
**作者简介**：樊睿(1983－)，女，甘肃通渭人，硕士研究生．主要研究方向为现代密码学．
E-mail：ruifan83@126.com

部分授权方案(partial delegation)和证书授权方案(delegation by warrant)；部分授权方案又分为代理人受保护(proxy-protected)和代理人不受保护(proxy-unprotected)2 种. 代理签名由原始签名人、代理签名人和验证者 3 方共同参与，一般由 4 个或更多算法组成，包括系统初始化、代理密钥生成、代理签名生成和代理签名验证.

分析已有的基于身份的代理签名[6,7]后不难发现，方案中用户都无条件信任 PKG，而所有用户的私钥都由 PKG 计算，这样 PKG 就可以伪造任意用户的签名. 在文献[4]方案的基础上，张学军[8]等人提出了一种基于身份无可信中心的盲签名和代理签名. 通过分析，发现此代理签名方案不能抵抗 PKG 的伪造攻击，违背了无可信中心的签名方案的规则. 就此提出了一种改进方案，在原有方案的安全基础上增加了抵抗 PKG 伪造攻击的功能. 在授权时使用文献[9]的短签名方案，提高签名效率.

## 1 预备知识

### 1.1 线性 Diffie-Hellman (BDH)问题

设 $G_1$ 与 $G_2$ 是 2 个阶为 $q$ 的循环群，$q$ 为大素数，其中 $G_1$ 以加法的形式表示，$G_2$ 以乘法的形式表示. 假设 $G_1$ 和 $G_2$ 这 2 个群中的离散对数问题都是困难的. 若映射 $\hat{e}: G_1 \times G_1 \longrightarrow G_2$ 为满足下列性质，则此映射称为可容许的双线性映射.

**性质 1**(线性性) $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$，对所有 $P, Q \in G_1$ 和所有 $a, b \in \mathbf{Z}$.

**性质 2**(非退化性) 如果 $P$ 是 $G_1$ 的生成元，则 $\hat{e}(P, P)$是 $G_2$ 的生成元.

**性质 3**(可计算性) 存在一个多项式算法，计算 $\hat{e}(P, Q)$，$\forall P, Q \in G_1$.

定义以下几个密码学问题：

1) 计算双线性 Diffie-Hellman 问题(CDHP). 输入 $P, aP, bP, cP$，输出 $\hat{e}(P, P)^{abc} \in G_2$，$\forall a, b, c \in \mathbf{Z}$.

2) 判定双线性 Diffie-Hellman 问题(DDHP). 给定四元组$(P, aP, bP, cP) \in G_1^4$，$a, b, c \in \mathbf{Z}_q^*$，判断 $c = ab \bmod q$ 是否成立.

3) GDH 群. 如果在群 $G_1$ 上，DDHP 容易但 CDHP 困难，则称 $G_1$ 为 GDH 群.

### 1.2 基于身份无可信中心的代理签名的性质

1) 可验证性. 从代理签名中，验证者可以验证签名的正确性，并确信原始签名人对所签消息的认可.

2) 不可伪造性. 包括 PKG 在内的任何第三方都不能伪造原始签名人的授权签名和代理签名人的代理签名.

3) 可区分性. 任何人都能区分出代理签名和一般签名的不同，并确定出原始签名人和代理签名人的关系.

4) 不可否认性. 一旦代理签名人代表原始签名人建立了有效的代理签名，他便不能否认自己的行为.

5) 防滥用性. 代理签名人不能签署未经授权的信息，代理签名人也不能把签名权力非法转给其他人.

## 2 文献[8]的方案

### 2.1 系统设置

$G_1$ 与 $G_2$ 是 2 个阶为 $q$ 的循环群，满足 1.1 中定义，$P$ 是 $G_1$ 的生成元，$\hat{e}: G_1 \times G_1 \longrightarrow G_2$ 为可容许的双线性映射，定义 4 个密码学上的单向哈希函数 $H_1: \{0,1\}^* \times G_1 \longrightarrow G_1$，$H_2: \{0,1\}^* \times \mathbf{Z}_q^* \times G_1 \longrightarrow G_1$，$H_3: \{0,1\}^* \longrightarrow G_1$，$H_4: G_1 \longrightarrow \mathbf{Z}_q^*$. PKG 选择 $s \in_R \mathbf{Z}_q^*$，计算 $P_{pub} = sP$，将 $s$ 秘密保存，公开系统参数 $p = \{G_1, G_2, \hat{e}, q, P, P_{pub}, H_1, H_2, H_3, H_4\}$.

### 2.2 密钥提取

原始签名人 A 和代理签名人 B 分别秘密选取各自相应的随机数 $r_A, r_B \in_R \mathbf{Z}_q^*$，计算 $r_A P, r_B P$，并把 $r_A P, r_B P$ 和 $r_A, r_B$ 的使用期限 $T_A, T_B$ 分别送给 PKG，再把身份信息 $ID_A, ID_B$ 提交给 PKG. PKG 计算 $Q_A = H_1(ID_A \| T_A, r_A P)$，$Q_B = H_1(ID_B \| T_B, r_B P)$，将 $Q_A, Q_B$ 作为 A，B 的公钥；将 $S_A = sQ_A$，$S_B = sQ_B$ 作为 A，B 的部分私钥，通过安全通道分别送给 A 和 B. A 和 B 的私钥分别为$(S_A, r_A)$和$(S_B, r_B)$.

### 2.3 生成代理密钥

A 建立一个许可证 $m_w$ 来明确说明包含 A 和 B 的身份信息的授权关系，同时也说明该授权关系的使用限制等内容. A 计算一个短签名 $S_w = H_4(H_3(m_w))S_A$，将$(S_w, m_w, T_A, r_A P)$发送给 B. B 验证等式 $\hat{e}(S_w, P) = \hat{e}(Q_A, P_{pub})^{H_4(H_3(m_w))}$ 是否成立. 如果成立，B 计算代理签名密钥 $S_p = S_w + H_4(H_3(m_w))S_B = H_4(H_3(m_w))(S_A + S_B)$.

### 2.4 签名

当要对消息 $m$ 签名时，代理签名人 B 选择 $u\in_R Z_q^*$，计算 $V=H_2(m,u,r_A P+r_B P)$，$S=uS_p+r_B V$，则$(u,S,m_w,T_A,T_B,r_A P,r_B P)$为 B 对 $m$ 的代理签名.

### 2.5 验证

验证者计算 $Q_A=H_1(ID_A\|T_A,r_A P)$，$Q_B=H_1(ID_B\|T_B,r_B P)$，$V=H_2(m,u,r_A P+r_B P)$，然后验证等式 $\hat{e}(S,P)=\hat{e}(Q_A+Q_B,P_{pub})^{uH_4(H_3(m_w))}\cdot\hat{e}(V,r_B P)$，若成立则接受签名，否则拒绝.

## 3 对以上方案的伪造攻击

在上面的代理签名体制中，作者称他们的方案满足不可伪造性，即任何人都不能冒充代理签名人生成有效代理签名，但是却没有考虑 PKG 对授权签名的伪造. 因为 PKG 知道原始签名人的部分私钥 $S_A$，可以伪造用户 A 的授权签名，造成了授权签名的可伪造性. 所以该方案不满足不可伪造性这一安全性需求.

伪造授权签名可以这样构造：由于 PKG 知道用户 A 的部分私钥，PKG 可以建立一个许可证 $m_w'$来伪造说明包含 A 和 B 的身份信息的授权关系，同时也说明该授权关系的使用限制等内容，然后 PKG 计算一个短签名 $S_w'=H_4(H_3(m_w'))S_A$，将$(S_w',m_w',T_A,r_A P)$发送给 B. B 验证等式 $\hat{e}(S_w',P)=\hat{e}(Q_A,P_{pub})^{H_4(H_3(m_w'))}$成立，然后计算代理签名密钥 $S_p'=H_4(H_3(m_w'))(S_A+S_B)$. 这样 PKG 就可以成功地伪造用户 A 的授权签名，而 B 却无法验证该授权是用户 A 的授权还是 PKG 伪造的授权.

## 4 改进方案

改进方案是在文献[7]的基础上构造的. 在授权时为了缩短签名长度提高传输效率，运用文献[9]的不可伪造的短签名方案. 系统设置同 2.1.

### 4.1 密钥提取

原始签名人 A 和代理签名人 B 分别秘密选取各自相应的随机数 $r_A,r_B\in_R Z_q^*$，计算 $R_A=r_A P$，$R_B=r_B P$，并把 $r_A,r_B$ 的使用期限 $T_A,T_B$ 分别送给 PKG，再把身份信息 $ID_A$，$ID_B$ 提交给 PKG. PKG 计算 $Q_A=H_1(ID_A\|T_A,R_A)$，$Q_B=H_1(ID_B\|T_B,R_B)$，将 $Q_A,Q_B$ 作为 A 和 B 的公钥；将 $S_A=sQ_A$，$S_B=sQ_B$ 作为 A 和 B 的部分私钥，通过安全通道分别送给 A 和 B. A 和 B 的私钥分别为$(S_A,r_A)$和$(S_B,r_B)$，公钥分别为$(Q_A,R_A)$和$(Q_B,R_B)$.

### 4.2 代理密钥的生成

A 建立一个授权许可信息 $m_w$ 来明确说明包含 A 和 B 的身份信息的授权关系，同时也说明该授权关系的使用限制等内容. A 计算一个短签名 $S_w=r_A H_3(m_w)+S_A H_4(H_3(m_w))$，将$(S_w,m_w,T_A,R_A)$发送给 B. B 验证等式 $\hat{e}(S_w,P)=\hat{e}(H_3(m_w),R_A)\hat{e}(Q_A,P_{pub})^{H_4(H_3(m_w))}$是否成立. 如果成立，B 计算代理签名密钥 $S_p=S_w+H_3(m_w)r_B=H_3(m_w)(r_A+r_B)+S_A H_4(H_3(m_w))$.

### 4.3 签名

当要对消息 $m$ 签名时，代理签名人 B 选择 $u\in_R Z_q^*$，计算 $V=H_2(m,u,R_A+R_B)$，$S=uS_B+S_p V$，则$(u,S,m_w,T_A,T_B,R_A,R_B)$为 B 对 $m$ 的代理签名.

### 4.4 验证

验证者计算 $Q_A=H_1(ID_A\|T_A,R_A)$，$Q_B=H_1(ID_B\|T_B,R_B)$，$V=H_2(m,u,R_A+R_B)$，然后验证等式 $\hat{e}(S,P)=\hat{e}(Q_B,P_{pub})^u\hat{e}(Q_A,P_{pub})^{VH_4(H_3(m_w))}\hat{e}(R_A+R_B,V)^{H_3(m_w)}$是否成立，若成立则接受签名，否则拒绝.

## 5 安全性及效率分析

### 5.1 正确性证明

1) 授权签名的正确性证明. 验证等式 $\hat{e}(S_w,P)=\hat{e}(H_3(m_w),R_A)\hat{e}(Q_A,P_{pub})^{H_4(H_3(m_w))}$是否成立，若成立则为 A 的合法授权签名.

$$\hat{e}(S_w,P)=\hat{e}(r_A H_3(m_w)+S_A H_4(H_3(m_w)),P)=\hat{e}(H_3(m_w),r_A P)\hat{e}(S_A H_4(H_3(m_w)),P)=\hat{e}(H_3(m_w),R_A)\hat{e}(Q_A,P_{pub})^{H_4(H_3(m_w))}.$$

2) 代理签名的正确性证明. 验证等式 $\hat{e}(S,P)=\hat{e}(Q_B,P_{pub})^u\hat{e}(Q_A,P_{pub})^{VH_4(H_3(m_w))}\hat{e}(R_A+R_B,V)^{H_3(m_w)}$，若成立则接受签名，否则拒绝.

$$\hat{e}(S,P)=\hat{e}(uS_B+S_p V,P)=\hat{e}(uS_B,P)\hat{e}(S_p V,P)=\hat{e}(Q_B,P_{pub})^u\hat{e}(S_A,P)^{H_4(H_3(m_w))V}\cdot\hat{e}((r_A+r_B)H_3(m_w)V,P)=\hat{e}(Q_B,P_{pub})^u\hat{e}(Q_A,P_{pub})^{H_4(H_3(m_w))V}\cdot\hat{e}((r_A+r_B)H_3(m_w)V,P)=\hat{e}(Q_B,P_{pub})^u\hat{e}(Q_A,P_{pub})^{VH_4(H_3(m_w))}\cdot$$

$$\hat{e}(R_A + R_B, V)^{H_3(m_w)}.$$

### 5.2 不可伪造性证明

**定理 1**　假设 CDHP 难解，则改进代理签名方案具有不可伪造性.

**证明**　1) 授权签名的不可伪造性. 因为改进方案的授权签名基于文献[9]不可伪造的短签名，文献[9]已证明是安全的、不可伪造的；且不同于文献[8]，本方案在授权时使用用户 A 自己的部分私钥来防止 PKG 的伪造，而其他用户不知道 A 的私钥，所以不可能伪造 A 的授权签名.

2) 代理签名的不可伪造性. 本代理签名方案基于文献[7]无可信中心的签名方案，该方案已证明是安全的不可伪造的，所以本方案的基本签名也是安全的、不可伪造的. 具体分析如下：将攻击者分为 3 类：普通攻击者、原始签名者和 PKG. 普通攻击者 C 不能伪造消息 $m$ 的代理签名，因为他不知道原始签名人 A 和代理签名人 B 的部分私钥 $r_A$ 和 $r_B$，也无法计算代理密钥 $S_p$，因此无法伪造代理签名. 在计算代理密钥 $S_p$ 时用到 B 的部分私钥 $r_B$，所以 A 也不能伪造消息 $m$ 的代理签名. PKG 不能伪造消息 $m$ 的代理签名，因为虽然 PKG 知道用户 A，B 的部分私钥 $S_A$ 和 $S_B$，但是在产生代理密钥 $S_p$ 的时候用的是用户自己的部分私钥 $r_A$ 和 $r_B$，PKG 无法得到代理密钥 $S_p$，所以 PKG 也无法伪造消息 $m$ 的代理签名.　】

### 5.3 替换公钥攻击

如果不诚实的 PKG 伪造原始签名者的公钥对 $(Q_A', R_A')$和私钥对$(S_A', r_A')$来伪造授权签名和代理签名，其中 $R_A' = r_A' P$，$Q_A' = H_1(ID_A \| T_A, R_A')$，$S_A' = sQ_A'$，则原始签名者可以通过零知识证明 $r_A$ 确实是他的合法部分私钥(用 PKG 的私钥签名的原始签名者真正的部分私钥)，同一个身份 ID 对应了 2 个私钥 $r_A$ 和 $r_A'$，说明PKG 是不诚实的.

### 5.4 可区分性

原始签名者的公钥及代理签名者的公钥都会出现在代理签名的验证等式里，而且代理签名的组成为$(u, S, m_w, T_A, T_B, R_A, R_B)$，授权信息 $m_w$ 也包含在代理签名和签名验证等式里面，因此任何人都可以从授权信息里决定代理签名者的身份，很好地满足可区分性.

### 5.5 不可否认性

由于授权信息 $m_w$ 包含在有效的验证等式里，因此代理签名人不能更改 $m_w$. 原始签名人对授权信息进行了签名，代理签名的验证等式中也包含了此签名，一旦做了授权签名，原始签名人就不能否认自己的签名，并且原始签名人在授权时用到自己的部分私钥，相应的部分公钥包含在 PKG 生成的公钥 $Q_A = H_1(ID_A \| T_A, R_A)$中，A 想要伪造一个部分私钥来否认授权签名，等价于求哈希函数的单向性问题. 代理密钥里面有代理签名者的部分私钥，一旦代理签名者为原始签名者创建了一个有效的代理签名，就无法否认自己的签名.

### 5.6 防止签名权力的滥用

由于有了授权信息 $m_w$ 的限制，而 $m_w$ 就出现在代理签名的验证等式中，因此代理签名人不能签署未经授权的信息，当然代理签名人也不能把签名权力非法转给其他人.

### 5.7 效率分析

从计算复杂性方面分析比较文中方案和文献[6,7]的方案，并将结果总结在表 1 中. 表 1 中的相关符号定义如下：$P_a$ 表示双线性映射中的对操作，$P_m$ 表示 $G_1$ 上的标量乘，$A_d$ 表示 $G_1$ 上的点加操作，$M_u$ 表示 $\mathbf{Z}_q^*$ 上的乘操作，$M_u G_2$ 表示 $G_2$ 上的乘操作，$\mathrm{Ex}\, G_2$ 表示 $G_2$ 上的指数运算，$H_s$ 表示哈希函数. 考虑到 $Q_A = H_1(ID_A \| T_A, r_A P)$，$Q_B = H_1(ID_B \| T_B, r_B P)$，$\hat{e}(Q_A, P_{pub})$，$\hat{e}(Q_B, P_{pub})$可提前进行计算，因此在分析计算复杂性时对以上操作进行了预计算.

**表 1　文中方案与其他方案的性能比较**

| 方案 | 代理密钥生成 | 代理签名 | 签名验证 |
|---|---|---|---|
| 文献[5]方案 | $2P_a+3P_m+M_uG_2+2A_d+3H_s$ | $2P_m+A_d+H_s$ | $3P_a+3M_uG_2+\mathrm{Ex}\,G_2+2H_s$ |
| 文献[6]方案 | $2P_a+3P_m+M_uG_2+2\mathrm{Ex}\,G_2+2A_d+2H_s$ | $P_a+2P_m+\mathrm{Ex}\,G_2+A_d+H_s$ | $P_a+2M_uG_2+2\mathrm{Ex}\,G_2+H_s$ |
| 文中方案 | $2P_a+3P_m+2M_u+\mathrm{Ex}\,G_2+2A_d+4H_s$ | $2P_m+A_d+H_s$ | $2P_a+P_m+2M_uG_2+3\mathrm{Ex}\,G_2+3H_s$ |

以上操作中，$P_a$ 计算最耗时，然后是 $P_m$. 分析表 1 可以看出，文中方案的计算复杂度大约为 $4P_a+6P_m$ 数量级，文献[6]方案的计算复杂度大约为 $5P_a+5P_m$ 数量级，文献[7]方案的计算复杂度大约为 $4P_a+5P_m$ 数量级，而在其他操作上文中方案的效率也远比其他 2 种方案高. 因此，文中的方案整体效率要比文献[6]的高，与文献[7]差不多，但是本方案却解决了文献[7]中 PKG 的密钥托管问题.

(下转第 56 页)

$$\nabla_{\mu}^{(5)}\Phi(x,z)=(\partial_M{}^5-\mathrm{i}g_5A_{\mu}{}^5)\Phi=$$
$$(\partial_{\mu},\partial_z)\Phi-\mathrm{i}g_5(A_{\mu},A_5)\Phi, \quad (16)$$

及协变导数的模方

$$|\nabla^{(5)}\Phi|^2=(\nabla_{\mu}^{(5)}\Phi)^*(\nabla_{\mu}^{(5)}\Phi)=$$
$$\frac{z^2}{R^2}\{|\nabla_{\mu}\Phi|^2+(\nabla_{\mu}^{(5)}\Phi)^*(\partial_z-\mathrm{i}g_5A_5)\Phi+$$
$$(\partial_z+\mathrm{i}g_5A_5)\Phi^*\nabla_{\mu}\Phi-$$
$$\mathrm{i}g_5A_5(\partial_z\Phi^*\Phi-\Phi^*\partial_z\Phi)+g_5{}^2A_5{}^2|\Phi|^2\}. \quad (17)$$

## 3 结论

本文从用以描述强子内部胶子紫外动力学的SU(2)杨米尔斯拉氏量和用以描述强子外部红外动力学的FN规范势分解拉氏量出发，通过对拉氏量的通伦内插，半定量地得到一个与Karch和Katz的软墙模型相对应的超引力五维全息模型，从另一个角度证明了量子色动力学的确存在全息原理模型描述. 笔者期望这里提出的计算能够为研究夸克禁闭机制带来新的参考，并期望进一步的研究能得到强子谱计算方案.

**参考文献：**

[1] POLCHINSKI J, STRASSLER M J. Hard scattering and gauge/string duality [J]. *Phys Rev Lett*, 2002, **88**: 031601.

[2] GUY F de TERAMOND, STANLEY J BRODSKY. Hadronic spectrum of a holographic dual of QCD[J]. *Phys Rev Lett*, 2005, **94**: 201601.

[3] ANDRESS Karch, EMNUEL Katz, DAM T Son, et al. Linear confinement and AdS/QCD[J]. *Phys Rev* D, 2006, **74**: 015005.

[4] 黄克孙. **夸克、轻子与规范场**[M]. 北京：北京师范大学出版社，1988：81-113.

[5] FADDEEV L, NIEMI A J. Partially dual variables in SU(2) Yang-Mills theory [J]. *Phys Rev Lett*, 1999, **82**: 1624-1627.

[6] FADDEEV L, NIEMI A J. Partially dual variables in SU(*N*) Yang-Mills theory [J]. *Phys Lett* B, 1999, **449**: 214-218.

[7] 段一士，葛墨林. SU(2)规范理论与*N*个磁单极运动体系的电动力学[J]. **中国科学**(A辑)，1979(11)：1072-1081.

[8] 贾多杰，艾德臻. 强耦合SU(2)杨米尔斯理论的对偶超导真空[J]. *HEP&NP*, 2007, **31**(5)：431-436.

(责任编辑 孙晓玲)

(上接第43页)

**参考文献：**

[1] SHAMIR A. Identity-based cryptosystems and signature schemes[M]//BLAKLE G R, CHAUM D. *Advances in Cryptology*: *CRYPTO* '84, Berlin: Springer, 1984: 7-53.

[2] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[M]//KILIAN J. *Advances in Cryptology*: *CRYPTO* 2001, Berlin: Springer, 2001: 213-229.

[3] BONEH D, BOYEN X. Secure identity based encryption without random oracles[M]//*Advances in Cryptology*: *CRYPTO* 2004, Berlin: Springer, 2004: 443-459.

[4] LIAO Jian, XIAO Jun-fang, QI Ying-Hao, et al. ID-Based signature scheme without trusted PKG [M]//*Advances in CISC* 2005. Berlin: Springer, 2005: 53-62.

[5] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures for delegating signing operation [M]// *Advances in* 3*rd ACM Conference on Computer and Communications Security* (*CCS* '96). New York: ACM Press, 1996: 48-57.

[6] XU Jing, ZHANG Zheng-feng, FENG Deng-guo. ID-Based proxy signature using bilinear pairings [M]//CHEN G. *Advances in Parallel and Distributed Processing and Applications*: *ISPA* 2005 *Workshops*. Berlin: Springer, 2005: 359-367.

[7] ZHANG Fang-guo, KIM K. Efficient ID-based blind signature and proxy signature from bilinear pairings [M]//*Advances in ACISP* 2003. Berlin: Springer, 2003: 312-323.

[8] 张学军，王育民. 基于身份无可信中心的盲签名和代理签名[J]. **计算机应用**, 2006, **26**(10)：2307-2309.

[9] BONEH D, LYNN B, SHACHAM H. Short signature from the Weil pairing [M]//BOYD C. *Advances in Cryptology*: *Asiacrypt* 2001. Berlin: Springer, 2001: 514-532.

(责任编辑 惠松骐)