文章编号: 1007-130X(2009)04-0095-04

基于身份的新型盲签名与代理签名*

New ID-Based Blind Signature and Proxy Signature

农 强[1], 吴顺祥[2]

NONG Qiang[1], WU Shun-xiang[2]

(1. 漳州师范学院计算机科学与工程系, 福建 漳州 363000; 2. 厦门大学自动化系, 福建 厦门 361005)

(1. Department of Computer Science and Engineering, Zhangzhou Normal University, Zhangzhou 363000;
2. Department of Automation, Xiamen University, Xiamen 361005, China)

摘 要: 随着互联网电子商务等业务的迅速发展, 盲签名与代理签名逐渐成为网络安全研究的热点。现有的一些盲签名与代理签名方案大多建立在可信第三方 TTP 的基础之上, 签名能否顺利进行主要依赖于 TTP, 如果 TTP 伪造签名或受到攻击, 那么签名将失效。基于椭圆曲线上的双线性对理论, 提出了一类新的基于身份无需可信第三方的盲签名与代理签名方案。在 CDH 问题是困难的假设下, 新方案被证明是安全的。在计算量方面, 盲签名方案和代理签名方案各仅需两次对运算, 效率比目前最好的 Zhang 和 Wang 方案高一倍。

Abstract: With the rapid development of e-commence and other utilities on the Internet, blind signature and proxy signature have become more important and crucial. But most current schemes depend on the trusted third party(TTP) which can forge a signature of any one. In this paper, the authors present a new ID-based blind signature scheme and a new ID-based proxy signature scheme without TTP based on the bilinear pairings. The proposed schemes are proved to be secure assuming the computational Diffie-Hellman problem is hard. As compared with the most efficient Zhang & Wang scheme to date, the proposed schemes decrease four pairing operations and only require two pairing operations for each scheme.

关键词: 可信第三方; 盲签名; 代理签名

Key words: trusted third party; blind signature; proxy signature

中图分类号: TP309 文献标识码: A

1 引言

盲签名[1]是由电子支付匿名性的要求而提出的, 它与通常数字签名的不同之处在于签名者并不知道他所签发文件的具体内容。正是这个特点, 使得盲签名技术可广泛用于许多领域, 类似的应用场合还有电子投票选举和网上招标、投标等。代理签名[2]的概念由 Mambo 等人于 1996 年首先提出。在代理签名方案中, 原始签名人能把他的签名权授权给代理签名人, 代理签名人可以代表原始签名人行使签名的权利。在现实商品交易、签订合同过程中, 当某人因公务或身体健康原因不能行使签名权时, 一般可委托其秘书用其私章或公章代其签名。在电子商务活动中, 如 CA 证书的签发、电子支票或电子货币的分发等同样要委派其他人替自己行使签名权。

1984 年, Shamir 提出了一个基于身份的加密和签名方案[3], 去除了由 CA 颁发公钥证书所带来的存储和管理开销等问题。后来, 人们发现利用双线性映射可以高效实现密码学上基于身份的加密、签名等应用[4,5]。近几年来, 基于身份的盲签名和代理签名被深入研究[6-9]。分析发现, 这些系统都存在一些问题需要解决, 其中有两个公开问题: 一是密钥托管。在基于身份的密码体制中, 用户的私钥由一个作为可信第三方的私钥生成中心(Private Key Generator, 简称 PKG)产生, 即 PKG 拥有所有用户的私钥, 这将导致 PKG 可以伪造盲签名和代理签名。虽然 Boneh 和 Franklin 在文献[10]中建议使用秘密共享方案在多个 PKG 中共享系统私钥, 但这样足够多的 PKG 合谋还是可以伪造用户签名, 而且要求 PKG 时时在线, 效率较低。二

* 收稿日期: 2008-02-10; 修订日期: 2008-05-12
基金项目: 福建省青年科技人才创新资助项目(2008F3110); 国家"十一五"科技支撑计划项目(2007BAK34B04); 国家自然科学基金资助项目(60704042); 福建省教育厅科技项目(JA08156)
作者简介: 农强(1978-), 男, 广西南宁人, 硕士生, 讲师, 研究方向为密码学和网络安全; 吴顺祥, 博士, 教授, 研究方向为信息安全、数据挖掘、智能信息系统、人工智能和机器学习。
通讯地址: 363000 福建省漳州市漳州师范学院计算机科学与工程系; Tel: 13225019267; E-mail: nong_qiang@163.com
Address: Department of Computer Science and Engineering, Zhangzhou Normal University, Zhangzhou, Fujian 363000, P. R. China

是签名实现的效率问题,对运算的运算量很大,效率非常低。2003 年,Chen 等人提出了一个新的基于身份的签名方案[11],使用户不需要对私钥生成中心无条件信任,并在随机预言模型中给出了安全性证明。最近,Zhang 和 Wang 在文献[11]方案的基础上分别提出了一个基于身份的盲签名和一个基于身份的代理签名方案[12]。分析发现,该方案签名时间开销大,并且在验证签名时需要计算四次双线性对运算,较文献[5]的方案需要约两倍的计算开销,效率不高。

针对已提出的方案实现效率慢的问题,本文做了一些必要的改进,提出了效率更高、实现速度更快、基于身份无需可信第三方的盲签名和代理签名方案。新方案保持了文献[5]方案的优点,即可证明的能抵抗适应性选择消息和身份攻击者的存在性伪造,并且能够满足盲签名和代理签名所要求的各种性质,与文献[12]方案相比较,签名效率有明显的提高。

2 预备知识

设$(G_1, +)$和$(G_2, \times)$为 q 阶循环群,q 为大素数,P 为 G_1的生成元,设在群 G_1、G_2 中离散对数问题是困难的。两个群之间的双线性对 $e: G_1 \times G_1 \rightarrow G_2$是满足以下条件的映射:

(1) 双线性性:$e(aP, bQ) = e(P, Q)^{ab}$,对 $\forall a, b \in Z_q^*$, $\forall Q \in G_1$;

(2) 非退化性:$\exists P, Q \in G_1$,满足 $e(P, Q) \neq 1$;

(3) 可计算性:对任意 $P, Q \in G_1$,$e(P, Q)$ 可以在多项式时间内有效计算出来。

定义 1 计算离散对数问题 CDHP (Computational Diffie-Hellman Problem,简称 CDHP):对于 $a, b \in_R Z_q^*$, P 是 G_1的生成元,给定 G_1中的元素 P、aP、bP,计算 abP。

定义 2 计算离散对数假设(Computational Diffie-Hellman (CDH) Assumption):令 IG 是一个 CDH 参数生成器,输入安全参数 1^k,我们说 IG 满足 CDH 假设,如果对于充分大的 k,算法 A 解决关于 G_1 的 CDH 问题具有的优势 $Adv_{IG,A(t)}$ 可定义为:

$$Adv_{IG,A(t)} = \Pr\left(\begin{array}{l} A(q, G_1, aP, bP) = abP, \\ \mid (q, G_1) \leftarrow G(1^k), P \leftarrow G_1, a, b \leftarrow Z_q^* \end{array}\right) \geqslant \varepsilon(k)$$

参数生成器 IG 满足 CDH 假设,如果对任何 k 的概率多项式时间算法 A,优势 $Adv_{IG,A(t)}$ 是可忽略量。在素数阶循环群 G 上,DDHP 在多项式时间内能被解决,但没有任何可能的算法可解决 CDHP,称 G 为 GDH (Gap Diffie-Hellman,简称 GDH)群。GDH 群能在有限域上的超奇异椭圆曲线或超椭圆曲线上找到,双线性映射能通过 Weil 对或 Tate 对构造,本文方案基于 GDH 群。

3 提出的盲签名方案

3.1 系统初始化

输入安全参数 1^k,输出两个阶为 q 的循环群 $(G_1, +)$和 $(G_2, \times)$,q 为大素数,P 为 G_1 的生成元。定义 G_1上的一个双线性映射 $e: G_1 \times G_1 \rightarrow G_2$,同时定义两个强无碰撞安全单向 Hash 函数 $H_1: \{0,1\}^* \times G_1 \rightarrow Z_q^*$, $H_2: \{0,1\}^* \times G_1 \rightarrow G_1$。PKG 选择 $s \in_R Z_q^*$,计算 $P_{pub} = sP$,将 s 秘密保存,公开其系统参数:$Params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$。

3.2 密钥提取

签名者 Alice 选取一个随机数 $r_A \in_R Z_q^*$,计算 $r_A P$ 并把 $r_A P$ 和 r_A的使用期限 T_A发送给 PKG,再把他的身份信息 ID_A 提交给 PKG。PKG 计算 $Q_A = H_2(ID_A \| T_A, r_A P)$,把 Q_A作为 Alice 的公钥。任何人都能在获取 Alice 的签名后从中提取出 $r_A P$,通过系统的公开参数计算出 Alice 的公钥。最后,PKG 把 $S_A = sQ_A$ 作为 Alice 的部分私钥,通过一个安全信道送给 Alice,Alice 的私钥为(S_A, r_A)。

3.3 盲签名

(1) 签名者 Alice 选择 $t \in_R Z_q^*$,计算 $U = tQ_A$,将 U、T_A和 $r_A P$ 发送给 Bob。

(2) 消息持有者 Bob 随机选择两个盲因子 $t_1, t_2 \in_R Z_q^*$,计算 $U' = t_1 U + t_1 t_2 Q_A$和 $h = t_1^{-1} H_1(m, U') + t_2$,然后将 h 发送给签名者 Alice。

(3) Alice 计算 $S = (t + h)(r_A Q_A + S_A)$,将 S 发送给 Bob。

(4) Bob 计算 $S' = t_1 S$,将 $\sigma(m) = (U', S', T_A, r_A P)$作为 Alice 对消息 m 的盲签名。

3.4 验证

验证者首先计算 $Q_A = H_2(ID_A \| T_A, r_A P)$ 和 $h' = H_1(m, U')$,然后验证等式:$e(S', P) = e(U' + h' Q_A, P_{pub} + r_A P)$是否成立。如果成立则接受签名,否则认为该签名无效。签名验证等式的成立可以通过下列等式证明:

$$\begin{aligned} e(S', P) &= e(t_1 S, P) = e(t_1(t+h)(r_A Q_A + S_A), P) = e(t_1(t+h)(r_A + s)Q_A, P) = e(t_1 t Q_A + t_1 t_1^{-1} H_1(m, U') Q_A + t_1 t_2 Q_A, r_A P + P_{pub}) = e(t_1 U + h' Q_A + t_1 t_2 Q_A, r_A P + P_{pub}) = e(U' + h' Q_A, r_A P + P_{pub}) \end{aligned}$$

3.5 盲签名方案的安全性分析

盲签名应该满足不可伪造性、盲性以及不可链接性等安全性要求[6-8],下面分析所提出的新方案满足不可伪造性、盲性以及不可链接性。

定理 1 所提的盲签名方案具有不可伪造性。

证明 假设 PKG 想伪造签名,由于 $S = (t + h)(r_A Q_A + S_A)$,其中 $V = (t + h) S_A$显然可以被 PKG 用其私钥 s 来产生。这样,PKG 就可以计算$(t + h) r_A Q_A = S - V$,进而可以计算 $r_A Q_A = (t + h)^{-1}(S - V)$(求逆在 Z_q^* 进行)。这样,PKG 对于随机的Q_A, $r_A P$ 在不知道r_A的情况下可计算 $r_A Q_A$。这与 CDH 问题难解相矛盾。

假设存在一个攻击者 F(非 PKG)能产生一个有效的盲签名$(U', S', h', T_A, r_A P)$,则根据神谕重放技术和分叉引理[13],存在另一个有效的算法 Sim 能产生两个有效的盲签名$(U', S', h', T_A, r_A P)$和$(U', S', h'_1, T_A, r_A P)$,其中 $h' \neq h'_1$。使用两个有效的盲签名,Sim 能以一个不可忽略的概率求得 CDH 问题的解,这与 CDH 问题的困难

性假设相矛盾,从而证明本方案是不可伪造的。具体证明过程如下:

给定 CDH 问题的任意一个实例 (P, aP, bP), Sim 设置 $Q_A = aP$, $r_A P + P_{pub} = bP$。在 Sim 与 F 执行了多项式次盲签名发布协议后, Sim 得到两个盲签名 $(U', S', h', T_A, r_A P)$ 和 $(U', S', h'_1, T_A, r_A P)$, 其中 $h' \neq h'_1$。因为这两个盲签名是有效的,所以得到:

$$e(S', P) = e(U' + h' Q_A, r_A P + P_{pub}) \quad (1)$$

$$e(S'_1, P) = e(U' + h'_1 Q_A, r_A P + P_{pub}) \quad (2)$$

从式(1)和式(2)能推导出 $S' - h' abP = S'_1 - h'_1 abP$,从而得到 $abP = (S' - S'_1)/(h' - h'_1)$,即 Sim 解决了 CDH 问题。 □

定理 **2** 所提的盲签名方案具有盲性。

证明 关于盲性的定义可参考文献[6],下面证明签名人不能得到关于签名和被签消息的任何信息。根据签名算法,如果给定一个有效的代理盲签名 $(U', S', T_A, r_A P)$ 以及在签名发行过程中交换的数据 (U, h, S),下列等式成立:

$$S' = t_1 S \quad (3)$$

$$h = t_1^{-1} H_1(m, U') + t_2 (\mathrm{mod}\ q) \quad (4)$$

$$U' = t_1 U + t_1 t_2 Q_A \quad (5)$$

$$e(S', P) = e(U' + h' Q_A, P_{pub} + r_A P) \quad (6)$$

显然,对于任意合法的签名 $(U', S', T_A, r_A P)$,必存在一个唯一的盲因子 $t_1' \in Z_q^*$ 满足式(3),其中 $t_1' = \log_S S'$;同理,也必存在另一个唯一的盲因子 $t_2' \in Z_q^*$ 满足式(4),其中 $t_2' = h - t_1^{-1} H_1(m, U')$。对于式(5),根据双线性映射的非退化性,有:

$$U' = t_1' U + t_1' t_2' Q_A \Leftrightarrow e(U', P_{pub} + r_A P) = e(t_1' U + t_1' t_2' Q_A, P_{pub} + r_A P) \quad (7)$$

因此,只需证明存在两个盲因子 (t_1', t_2') 满足式(7)即可。证明如下:

$$e(t_1' U + t_1' t_2' Q_A, P_{pub} + r_A P) = e(\log_S S' U + \log_S S' (h - (\log_S S')^{-1} H_1(m, U')) Q_A, P_{pub} + r_A P) = e(\log_S S' \cdot tQ_A + \log_S S' \cdot hQ_A, P_{pub} + r_A P)\, e(H_1(m, U') Q_A, P_{pub} + r_A P)^{-1} = e(\log_S S' \cdot (t + h)(r_A Q_A + S_A), P)\, e(S', P)^{-1} e(U', P_{pub} + r_A P) = e((\log_S S') \cdot S, P)\, e(S', P)^{-1} e(U', P_{pub} + r_A P) = e(U', P_{pub} + r_A P)$$

从以上的推导过程可知,盲因子 (t_1', t_2') 总是存在且能满足式(7)的定义,所以在任何视野中看到的盲签名的生成协议都是无链接的,这一点与文献[6]证明签名的盲性原理相同。 □

定理 **3** 所提的盲签名方案具有不可链接性。

证明 盲签名 $\sigma(m) = (U', S', T_A, r_A P)$ 是由消息持有者 Bob 进行脱盲变化后形成的,由于群 G_1 上的离散对数问题是难解的,因此签名者 Alice 不能通过 $S' = t_1 S$ 计算出盲因子 t_1 和 t_2。即使 Alice 保存了 U 和 S,当盲签名 $(U', S', T_A, r_A P)$ 公布后,他也不能确定盲签名 $\sigma(m) = (U', S', T_A, r_A P)$ 是他的哪一次签名,所以新方案具有不可链接性。 □

3.6 效率分析

下面将所提的盲签名方案和文献[12]的方案从计算复杂性方面进行了比较,并将结果总结在表 1 中。表 1 中有关符号的定义如下: 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 Z_q 上的乘操作, I_m 表示 Z_q 上的求逆操作。这里,我们忽略了所有的哈希运算。

表 **1** 所提盲签名方案与文献[**12**]方案的性能比较

方案	盲签名生成阶段	签名验证阶段
文献[12]方案	$10P_m + 2M_u + 3A_d + 2I_m$	$4P_a + 1P_m + 1A_d$
所提方案	$6P_m + 1M_u + 2A_d + 1I_m$	$2P_a + 1P_m + 2A_d$

从各种操作的计算来看, P_a 计算最耗时,然后是 P_m,其它运算相对计算双性对时间开销非常小。从表 1 可以看出,所提的盲签名方案的计算复杂度大约是 $2P_a + 7P_m$,而文献[12]方案的计算复杂度大约是 $4P_a + 11P_m$。因此,所提出的方案比文献[12]方案的效率要高得多。

4 提出的代理签名方案

4.1 系统初始化

输入安全参数 1^k,输出两个阶为 q 的循环群 $(G_1, +)$ 和 $(G_2, \times)$, q 为大素数, P 为 G_1 的生成元。定义 G_1 上的一个双线性映射 $e: G_1 \times G_1 \rightarrow G_2$,同时定义四个强无碰撞安全单向 Hash 函数 $H_1: \{0,1\}^* \times G_1 \rightarrow Z_q^*$, $H_2: \{0,1\}^* \times G_1 \rightarrow G_1$, $H_3: \{0,1\}^* \rightarrow G_1$, $H_4: G_1 \rightarrow Z_q^*$。最后, PKG 选择 $s \in_R Z_q^*$,计算 $P_{pub} = sP$,将 s 秘密保存,公开其系统参数: $Params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H_3, H_4\}$。

4.2 密钥提取

原始签名者 Alice 和代理签名者 Bob 分别秘密选取各自相应的随机数 $r_A, r_B \in_R Z_q^*$,各自计算 $r_A P$、$r_B P$,并把 $r_A P$、$r_B P$ 和 r_A、r_B 的使用期限 T_A、T_B 发送给 PKG,再把他们的身份信息 ID_A、ID_B 各自提交给 PKG。而后, PKG 计算 $Q_A = H_2(ID_A \| T_A, r_A P)$, $Q_B = H_2(ID_B \| T_B, r_B P)$,把 Q_A、Q_B 作为 Alice 和 Bob 的公钥, $S_A = sQ_A$, $S_B = sQ_B$ 作为 Alice 和 Bob 的部分私钥,通过安全通道分别送给 Alice 和 Bob, Alice 的私钥为 (S_A, r_A), Bob 的私钥为 (S_B, r_B)。

4.3 生成代理密钥

Alice 在开始代理授权之前先准备授权文件 m_W,其中包含代理人信息如代理签名人公钥以及代理签名的文件类型、时间等信息。Alice 首先计算一个短签名 $S_W = H_4(H_3(m_W))\, S_A$,然后将 $(S_W, m_W, T_A, r_A P)$ 发送给 Bob。Bob 验证等式 $e(S_W, P) = e(Q_A, P_{pub})^{H_4(H_3(m_W))}$ 是否成立。如果成立,则计算代理密钥: $S_P = S_W + H_4(H_3(m_W)) * S_B = H_4(H_3(m_W))(S_A + S_B)$。

4.4 签名

当要对消息 m 进行签名时,代理签名者 Bob 选择 $t \in_R Z_q^*$,计算 $U = t(Q_A + Q_B)$, $h = H_1(m, U)$, $S = (t + h)(r_B(Q_A + Q_B) H_4(H_3(m_W)) + S_P)$,则 $\sigma(m) = (U, S, m_W, r_A P, r_B P, T_A, T_B)$ 为 Bob 对 m 的代理签名。

4.5 验证

验证者首先计算 $Q_A = H_2(ID_A \| T_A, r_A P)$, $Q_B =$

$H_2(ID_B \| T_B, r_B P)$, $h = H_1(m, U)$, 再看等式 $e(S, P) = e(U + h(Q_A + Q_B), r_A P + P_{pub})^{H_4(H_3(m_W))}$ 是否成立。如果成立则接受签名, 否则认为该签名无效。详细推导过程如下:

$e(S, P) = e((t + h)(r_B(Q_A + Q_B) H_4(H_3(m_W)) + S_P), P) = e((t + h)(r_B(Q_A + Q_B) + s(Q_A + Q_B)), P)^{H_4(H_3(m_W))} = e((t + h)(r_B + s)(Q_A + Q_B), P)^{H_4(H_3(m_W))} = e((t + h)(Q_A + Q_B), r_B P + P_{pub})^{H_4(H_3(m_W))} = e((t + h)(Q_A + Q_B), r_B P + P_{pub})^{H_4(H_3(m_W))} = e(U + h(Q_A + Q_B), r_B P + P_{pub})^{H_4(H_3(m_W))}$

4.6 代理签名方案的安全性分析

代理签名应该满足可验证性、可区分性、可识别性、不可伪造性、不可否认性、防止滥用性等安全性要求[8, 9], 其中可验证性在 4.5 节中已经证明。由于有效的代理签名 $\sigma(m) = (U, S, m_W, r_A P, r_B P, T_A, T_B)$ 中包含了授权证书 m_W, 而且授权证书 m_W、原始签名者 Alice 和代理签名者 Bob 的公钥 Q_A、Q_B 都要在签名的验证算法中出现, 易证所提的代理签名方案满足可区分性、可识别性、不可否认性、抗滥用性。下面主要证明其满足不可伪造性。

定理 **4** 所提的代理签名方案具有不可伪造性。

证明 由于攻击者(非 PKG)不知道代理签名者 Bob 的代理密钥 S_P, 因此攻击者不能利用代理密钥 S_P 来进行签名。攻击者想要伪造的对消息 m 的代理签名通过验证, 他们必须使$(U, S, m_W, r_A P, r_B P, T_A, T_B)$ 满足验证式: $e(S, P) = e(U + h(Q_A + Q_B), r_A P + P_{pub})^{H_4(H_3(m_W))}$。然而, e 是一个安全的双线性对, 找到一组数$(U, S, m_W, r_A P, r_B P, T_A, T_B)$ 满足上式在计算上是不可行的, 所以满足不可伪造性。

如果 PKG 想伪造签名, 由于 PKG 知道 S_A、S_B, 所以他可以计算代理密钥 S_P, 通过伪造的 $r_A P$、$r_B P$, 进而伪造出能通过验证的"有效"的代理签名。然而, 代理签名者 Bob 可以提供证据证明 PKG 伪造了他的代理签名。他可以先把 $r_B P$ 和 T_B 递交给一个中间人, 就可以证明他知道 S_B。中间人选取一个随机数 $a \in_R Z_q^*$ 把 aP 通过一个安全通道送给 Bob, Bob 计算 $e(S_B, aP)$, 如果等式 $e(S_B, aP) = e(Q_B, P_{pub})^a$ 成立, 那就说明 Bob 知道 S_B, 而且他的 ID_B 在同一个时间期限内对应了 $r_B P$、$r_B' P$。这时, 中间人就可判断 PKG 伪造了 Bob 的代理签名。因为只有 PKG 知道 s, 别人无法得到 S_B, 当然更无法伪造能通过验证的 r_B、$r_B P$。 □

4.7 效率分析

下面将所提的代理签名方案和文献[12]方案从计算复杂性方面进行了比较, 并将结果总结在表 2 中。表 2 中有关符号的定义和表 1 相同。这里, 我们也忽略了所有的哈希运算。

表 **2** 所提代理签名方案与文献[**12**]方案的性能比较

方案	代理签名生成阶段	签名验证阶段
文献[12]方案	$3P_m + 2A_d$	$4P_a + 1P_m + 2A_d$
所提方案	$3P_m + 2A_d$	$2P_a + 1P_m + 3A_d$

从表 2 可以看出, 我们的代理签名方案的计算复杂度大约是 $2P_a + 4P_m$, 而文献[12]方案的计算复杂度大约是 $4P_a + 4P_m$。因此, 我们的方案效率更高。

5 结束语

本文提出了一个基于身份无需可信第三方的盲签名方案, 同时提出了一个基于身份无需可信第三方的代理签名方案, 证明了其正确性并进行了安全性和性能分析。在 CDHP 困难假设下, 该方案被证明是安全的。与目前已有的方案相比, 所提的方案效率更高。将来的工作是设计更有效的基于身份的盲签名和代理签名方案和在标准模型下可证安全的盲签名和代理签名方案。

参考文献:

[1] Chaum D. Blind Signatures for Untraceable Payments[C]// Porc of Crypto' 82, 1982: 199-204.

[2] Mambo M, Usuda K, Okamoto E. Proxy Signatures: Delegation of the Power to Sign Messages[J]. IEICE Trans on Fundamentals, 1996, 79(9): 1338-1354.

[3] Shamir A. An Identity-Based Cryptosystems and Signature Schemes[C]// Proc of Crypto' 84, 1984: 47-53.

[4] Boneh D, Lynn B, Shacham H. Short Signatures from the Weil Pairing[C]// Proc of ASIACRYPT' 01, 2001: 514-532.

[5] Cha J C, Cheon J H. An Identity-Based Signature from Gap Diffie-Hellman Groups[C]// Proc of Public Key Cryptography 2003, 2003: 18-30.

[6] Zhang F, Kim K. ID-Based Blind Signature and Ring Signature from Pairings[C]// Proc of Asiacrpt' 02, 2002: 533-547.

[7] Huang Z J, Chen K F, Wang Y M. Efficient ID-Based Signatures and Blind Signatures[C]// Proc of CANS' 05, 2005: 120-133.

[8] Zhang F, Kim K. Efficient ID-Based Blind Signature and Proxy Signature from Bilinear Pairings[C]// Proc of ACISP' 03, 2003: 312-323.

[9] Boldyreva A, Palacio A, Warinschi B. Secure Proxy Signature Schemes for Delegation of Signing Rights[EB/OL]. [2007-10-13]. http://eprint.iacr.org/2003/096.

[10] Boneh D, Franklin M. Identity-Based Encryption from Weil Pairing[J]. SIAM Journal of Computing, 2003, 32(3): 586-615.

[11] Chen X F, Zhang F G, Kim K. A New ID-Based Group Signature Scheme from Bilinear Pairings[EB/OL]. [2007-12-11]. http://eprint.iacr.org/2003/116.

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

[13] Pointcheval D, Stern J. Security Arguments for Digital Signatures and Blind Signatures[J]. Journal of Cryptology, 2000, 13(3): 316-396.