安全无可信私钥生成中心的部分盲签名方案①

周 萍[1,2], 何大可[1]

[1](西南交通大学信息科学与技术学院 信息安全与国家计算网格实验室，成都 610031)
[2](四川城市职业学院，成都 610101)

摘 要：目前基于身份的部分盲签名方案或者安全性不高，或者效率较低。针对这些方案的缺陷，通过密码学分析和算法结构设计，提出了一个新的基于身份的无可信私钥生成中心(Private Key Generator, PKG)的、只有一个对运算的部分盲签名方案。证明了方案的强盲性，证明了该方案可以抵抗适应性选择消息和身份攻击，可以抵抗不可信 PKG 的攻击，其安全性依赖于强 l-SDHP 难题。比较了方案和其他类似方案的效率。

关键词：私钥生成中心；部分盲签名；双线性对；不可伪造性；强 l-SDHP 难题

Secure Partially Blind Signature Scheme without Trusted PKG

ZHOU Ping[1,2], HE Da-Ke[1]

1(College of Information Sciences & Technology, Southwest Jiaotong University, Chengdu 610031, China)
2(Urban Vocational College Of Sichuan, Chengdu 610110, China)

Abstract: Current identity-based partially blind signature scheme or the security is not high, or less efficient. Aiming at the defect, through analysis for cryptography and algorithm design, the paper presents an new ID-based partially blind signature scheme with only one bilinear pairing without trusted Private Key Generator (PKG). The proposed scheme has been proved to be strong blindness and be secure against existential forgery on adaptively chosen message and ID attack, and against attack from un-trusted PKG, and be more efficient. Its security relies on the hardness of l-Strong Diffie-Hellman problem (l-SDHP). The difference of the scheme with other likely schemes has been done.

Key words: private key generator; partially blind scheme; bilinear pairing; unforgeability; l-Strong Diffie-Hellman problem

1 引言

盲签名[1]是一种非常典型的数学签名技术。在盲签名中，签名者并不知道所签署文件的具体内容，只是完成对文件的签名。当签名被消息接收者泄露后，签名者不能追踪该签名。盲签名的这种特性被称为盲性。盲性使得盲签名被广泛应用于如电子支付、匿名电子选举等要求保护签名申请者隐私或私有信息的场合。

在盲签名中，签名者完全不知道自己所签署文件的内容，因此可能造成签名被签名申请者滥用，给签名者造成损失。理想的盲签名致力于解决匿名性和可控性之间的矛盾，部分盲签名可以做到这一点。部分盲签名允许签名者增加一些如签名时间、签名有效期、签署消息的性质和范围等附加说明，这样一方面保证了待签消息对签名者的盲性，另一方面阻止了签名申请者提供非法信息而滥用签名，有效保护了签名者的合法权益。

在传统的基于证书的公钥密码体制(PKI)中，用户的公钥与其身份之间的绑定关系是通过公钥证书来实现的，而公钥证书的签发、存储、更新、撤销等都是由可信赖的第三方 CA 来完成。公钥证书的管理需要很大的计算量和很强的存储能力。为此，Shamir 在 1984 年提出了基于身份的密码学思想[2]，即用户的公钥直接从他的身份信息(如姓名，IP 地址，Email 地址)中得

① 基金项目:成都市 2007 年科技攻关项目(07GGYB050GX-010)
收稿时间:2011-09-24;收到修改稿时间:2011-10-30

到，而用户的私钥由一个可信赖的第三方－私钥生成中心 PKG(Private Key Generator)生成。但是这种基于身份的密码体制有一个不可避免的缺陷－密钥托管问题，即 PKG 知道系统内所有用户的私钥，PKG 也就有能力伪造系统内任何人的签名，或解密发给系统内任何人的消息。因为在很多特定的应用环境中，一个被系统内所有人信任的 PKG 并不存在，或一旦 PKG 被攻破将导致灾难性的后果，因此设计基于身份的无可信 PKG 的签名方案就很有意义。

近年来，基于双线性对，许多密码学研究者提出了基于身份的部分盲签名方案[3-5]。但在这些方案中，文献 3 的方案具有 4 个对运算，且不能抵抗不可信 PKG 的伪造签名攻击和篡改公共信息攻击[6]；文献 4 的方案需要 3 个对运算，而且该方案不具有不可伪造性，不诚实的 PKG 可以伪造一个有效的部分盲签名[5]；文献 5 的方案虽然可以抵抗不诚实 PKG 的伪造性攻击，但其计算量实为 2 个对运算(除去预计算 $e(Q_2,Q_{pub})$外，每个消息申请者和消息验证者都需要计算一次 $e(Q_2+H_3(c),Q_1)$)。这些方案都至少需要 2 个对运算，而且有些方案不能抵抗不诚实 PKG 的伪造性攻击，有些方案不能抵抗篡改公共信息攻击。另外，在基于对的签名方案中，对运算相对于其他运算是最耗时的，因此应当尽量减少对运算的个数。为此，我们这里给出基于身份的无可信 PKG 的，只有一个对运算的盲签名。相比于其它方案，我们的方案更为高效。

2 新的基于身份无可信PKG的部分盲签名

本节提出一个新的部分盲签名方案。方案是基于身份无可信 PKG 的，并且只有一个对运算。下一节将证明：方案是部分盲的，能够抵抗适应性选择消息和身份攻击下的存在性伪造，可以抵抗不可信 PKG 的攻击。另外，由于只有一个对运算，方案比其他方案[3-5]更为高效。

方案使用两对私钥(S_{ID},S_c)和两对公钥(g_{ID},g_c)，其中自选公私钥对(g_C,S_C)由用户自己生成，部分私钥 S_{ID} 由 PKG 使用系统私钥 s_{pkg} 生成，签名时需要同时使用两对私钥(S_{ID},S_c)。因为 PKG 只能生成用户的部分私钥 S_{ID}，而不知道用户的自选私钥 S_c，因此 PKG 不能伪造合法用户的部分盲签名，方案因而能够抵抗不可信 PKG 的伪造攻击。

(1) 系统建立：设 q 为一个大素数(≥160 比特)，G_1, G_2 分别为 q 阶的加法、乘法循环群，$e: G_1\times G_1\rightarrow G_2$ 是一个双线性映射，P 是 G_1 的任一生成元。PKG 随机选取 $s_{pkg}\in_R Z_q^*$作为系统主密钥，计算系统公钥 $P_{pkg}=s_{pkg}P$，计算 $g=e(P,P)$，然后选取 3 个强抗碰撞 hash 函数 $H_1:\{0,1\}^*\rightarrow Z_q^*$，$H_2:\{0,1\}^*\times G_2\rightarrow Z_q^*$，$H_3:\{0,1\}^*\rightarrow G_1$。PKG 公布系统参数{ G_1,G_2, q, P, e, g, P_{pkg}, H_1,H_2,H_3}，秘密保存系统私钥 s_{pkg}。

(2) 签名密钥生成：每个用户将自己的身份信息发送给 PKG，由 PKG 核实后生成该用户的部分密钥。设某用户的身份为 ID，PKG 计算该用户的部分私钥 $S_{ID}=P/(s_{pkg}+H_1(ID))$，并将 S_{ID} 通过安全的信道发送给用户。用户收到 S_{ID} 后，计算中间变量 $P_1=P_{pkg}+H_1(ID)P$，然后验证等式 $e(S_{ID},P_1)=g$ 是否成立，若成立则接受 S_{ID}，并计算部分公钥 $g_{ID}=e(P,P_1)$，否则要求 PKG 重新计算和发送，直到 S_{ID} 有效为止。

用户随机选取整数 $c\in_R Z_q^*$作为自己的自选私钥 $S_c=c$，计算自选公钥 $g_c=e(cP,P)$，公共信息公钥 $g_{inf}=e(H_3(inf),P_1)$，其中 inf 为用户用于部分盲签名的公共信息。公布自己的公钥(g_{ID}, g_c, g_{inf})和身份信息 ID，安全保存签名私钥(S_{ID}, S_c)。

(3) 签名：设签名申请者 Alice 请求用户 Bob(其身份信息为 ID)对消息 m 进行部分盲签名。签名的交互过程如下：

①Bob 随机选取 $k\in_R Z_q^*$，计算 $K=(g_{inf})^{kSc}$，将 K 秘密发送给 Alice。

②盲化消息：Alice 随机选取二个整数 $\alpha,\beta\in_R Z_q^*$，计算：$r=K^{\alpha}(g_{ID})^{\beta}(g_c)^{\alpha\beta H_1(ID)}$，$h=H_2(m\|\inf,r)$，$h'=(\alpha^{-1}h+\beta)\bmod q$。将 h' 发送给 Bob。

③签名：Bob 用自己的私钥(S_{ID} ,S_c)签名：$S'=kS_c\cdot H_3(\inf)+S_c h' H_1(ID)\cdot S_{ID}$，将 S' 发送给 Alice。

④脱盲：Alice 对签名 S' 进行脱盲运算：$S=\alpha S'+\beta P+H_1(ID)\cdot H_3(\inf)$。则消息 m 的部分盲签名即为(S,h,inf)，其中 inf 为 Bob 用于部分盲签名的公共信息。

(4) 验证签名：验证者收到消息 m 的部分盲签名(S, h,inf)后，首先检查 m 是否在 inf 规定的范围内，然后再验证等式：

$$h=H_2(m\|\inf,e(S,P_{pkg}+H_1(ID)P)(g_c^h g_{\inf})^{-H_1(ID)})$$

是否成立。若上述两个条件都成立，消息 m 的部分盲签名(S, h,inf)有效；否则签名无效。

3 新方案的安全性和效率分析

3.1 方案的正确性证明

方案的正确性由下面的定理给出。

定理 1. 方案中的签名是有效的。即消息 m 的部分盲签名(S, h,inf)满足验证等式。

证明 由签名过程可知：

$$\begin{aligned} r &= K^{\alpha}(g_{ID})^{\beta}(g_c)^{\alpha\beta H_1(ID)} \\ &= e(S_c H_3(\text{inf}), P_1)^{k\alpha} e(P, P_1)^{\beta} e(S_c P, P)^{\alpha\beta H_1(ID)} \\ &= e(S_c H_3(\text{inf}), P_1)^{k\alpha} e(P, P_1)^{\beta} e(S_c S_{ID}, P_1)^{\alpha\beta H_1(ID)} \\ &= e(k\alpha S_c H_3(\text{inf}) + \beta P + S_c \alpha\beta H_1(ID) S_{ID}, P_1) \end{aligned}$$

$$\begin{aligned} S &= \alpha S' + \beta P + H_1(ID)\cdot H_3(\text{inf}) \\ &= k\alpha S_c H_3(\text{inf}) + S_c \alpha h' H_1(ID)\cdot S_{ID} + \beta P + H_1(ID)\cdot H_3(\text{inf}) \\ &= k\alpha S_c H_3(\text{inf}) + S_c h H_1(ID) S_{ID} + S_c \alpha\beta H_1(ID) S_{ID}) + \beta P + \\ &\quad H_1(ID)\cdot H_3(\text{inf}) \end{aligned}$$

因此有：$e(S, P_{pkg} + H_1(ID)P)$

$$\begin{aligned} &= r\cdot e(S_c h H_1(ID) S_{ID}, P_1) e(H_1(ID) H_3(\text{inf}), P_1) \\ &= r\cdot e(S_c h H_1(ID) P, P) e(H_1(ID) H_3(\text{inf}), P_1) \\ &= r g_c^{h H_1(ID)} g_{\text{inf}}^{H_1(ID)} \end{aligned}$$

故 $r = e(S, P_{pkg} + H_1(ID)P)\cdot g_c^{-hH_1(ID)} g_{\text{inf}}^{-H_1(ID)}$ 成立。因此，验证等式成立。

3.2 方案的安全性分析

3.2.1 部分盲性。

定理 2. 方案是部分盲的。

证明 由方案可知，Alice 对消息 m 进行了盲化处理：$h = H_2(m \| \text{inf}, r)$，$h' = \alpha^{-1} h + \beta$，确保了明文消息的不可见。

若签名人 Bob 保存了每一次签名过程的中间数据 (k, K, h', S')，当 Alice 公开消息 m 及签名(S, h,inf)时，Bob 可以得到 m 及(S, h,inf)。Bob 想找出(k, K, h', S')和(m,inf,S,h)之间的链接关系。

因为在盲化消息及脱盲签名的过程中，使用了两个随机数 α, β，因此从理论上说，只要有 3 个等式连接视图(k, K, h', S')和(m,inf,S,h)，就可以找出二者之间的链接关系，其中 2 个等式用于求出 α, β，第 3 个等式用于判断两个视图之间有没有关系，即(k, K, h', S')到底是不是签名结果(m,inf,S,h)生成过程中的特定的那次中间数据。

本方案中，这 3 个连接等式是：

$$h' = (\alpha^{-1} h + \beta) \bmod q$$

$$S = \alpha S' + \beta P + H_1(ID)\cdot H_3(\text{inf})$$

$$r = K^{\alpha}(g_{ID})^{\beta}(g_c)^{\alpha\beta H_1(ID)}$$

$$= e(S,\ P_{pkg} + H_1(ID)P)\ \cdot g_c^{-hH_1(ID)} g_{\text{inf}}^{-H_1(ID)}$$

理论上，从上面的方程组中，由第 1，2 个方程可以求出 α, β，然后代入第 3 个方程可以验证，若方程成立则(k, K, h', S')可关联到(m,inf,S,h)，否则二者没有关联。但实际上，由第 1 式求出 $\beta = h' - \alpha^{-1} h$ 后，代入第 2 式：$S = \alpha S' + (h' - \alpha^{-1})P$。由循环群上的离散对数难题，无法从上式求出 α。更进一步地，由于下面事实的存在，方程组的第 3 个方程并不能用来判断(k, K, h', S')和(m,inf,S,h)二者之间的关联性。

假设 Bob 保存了某次签名过程(签名消息为 m_0)的中间数据(k_0, K_0, h_0', S_0')，现在 Alice 公布另一次签名过程的结果$(m_1, \text{inf}, S_1, h_1)$。Bob 从 $h_0' = (\alpha^{-1} h_1 + \beta) \bmod q$ $\Rightarrow \beta = h_0' - \alpha^{-1} h_1$，建立等式 $S_1 = \alpha S_0' + \beta P + H_1(ID)\cdot H_3(\text{inf})$，然后计算 $r = K_0^{\alpha}(g_{ID})^{\beta} g_c^{\alpha\beta H_1(ID)}$。

因为对于 Bob 来说，$K_0 = (g_{\text{inf}})^{k_0 Sc}$，$S_0' = k_0 S_c \cdot H_3(\text{inf}) + S_c h_0' H_1(ID)\cdot S_{ID}$ 成立。

为书写简单，记 $P_1 = P_{pkg} + H_1(ID)P$

因此有：$r = K_0^{\alpha}(g_{ID})^{\beta} g_c^{\alpha\beta H_1(ID)}$

$$= e(S_c H_3(\text{inf}), P_1)^{k_0\alpha} e(P, P_1)^{\beta} e(S_c P, P)^{\alpha\beta H_1(ID)}$$

$$= e(S_c H_3(\text{inf}), P_1)^{k_0\alpha} e(P, P_1)^{\beta} e(S_c S_{ID}, P_1)^{\alpha\beta H_1(ID)}$$

$$= e(k_0\alpha S_c H_3(\text{inf}) + \beta P + S_c \alpha\beta H_1(ID) S_{ID}, P_1)$$

于是：$e(S_1, P_1) = e(\alpha S_0' + \beta P + H_1(ID)\cdot H_3(\text{inf}), P_1)$

$$= e(k_0\alpha S_c H_3(\text{inf}) + S_c h_1 H_1(ID) S_{ID}$$

$$+ S_c \alpha\beta H_1(ID) S_{ID} + \beta P + H_1(ID) H_3(\text{inf}), P_1)$$

$$= r\cdot e(S_c h_1 H_1(ID) S_{ID}, P_1) e(H_1(ID) H_3(\text{inf}), P_1)$$

$$= r\cdot (g_c)^{h_1 H_1(ID)} g_{\text{inf}}^{H_1(ID)}$$

因此，验证等式 $h_1 = H_2(m_1 \| \text{inf},\ e(S_1, P_{pkg} + H_1(ID)P) g_c^{-h_1 H_1(ID)} g_{\text{inf}}^{-H_1(ID)})$ 成立。

由上述分析可知，任何一次签名的中间数据(k_0, K_0, h_0', S_0')都能够关联到与它毫不相关的签名结果$(m_1, \text{inf}, S_1, h_1)$上去。也就是说，无法找出中间数据$(k, K, h', S')$和签名结果(m,inf,S,h)之间的关联。由文献[7]的定义 7 可知，本方案是部分盲的。

3.2.2 不可伪造性

下面讨论方案的不可伪造性。首先定义基于身份无可信 PKG 签名方案的安全模型[8]。

定义 1. 如果一个基于身份无可信 PKG 的签名方案在自适应选择消息和身份攻击下是存在性不可伪造的，则称该方案是安全的。也即在下面的游戏中，不存在概率多项式时间算法(攻击者)F，通过借助挑战者 B，能够以一个不可忽略的概率优势赢得下面的游戏：

(1) B 运行系统建立算法，生成系统参数，并将参数发送给攻击者。

(2) 攻击者 F 以自适应方式进行下面的询问：

－密钥提取预言机询问：对于任意身份 ID 返回私钥 S_{ID}。

－签名预言机询问：对于任意身份 ID 和任意消息 M，返回由 ID 所对应私钥 S_{ID} 所做的签名(ID,m,S, h)。

(3) 攻击者 F 输出签名(ID*,M*,S*,h*)，这里 ID* 未进行过密钥提取预言机询问，(ID*,M*)也没有进行过签名预言机询问。若(ID*,M*,S*,h*)能够通过签名验证，则 F 赢得游戏。

下面给出 l-SDHP 难题[9]的定义。

定义 2. (*l* 阶 Strong Diffie-Hellman 难题，l-SDHP 难题) 设 G_1 为一个 q 阶加法循环群(q 为素数)，P 为其生成元，$\forall Q \in G_1$,给定 $P,Q,\alpha Q,\alpha^2 Q,\cdots,\alpha^l Q \in G_1$，求一对二元组$(w, P/(w+\alpha))$，其中 $w \in Z_q^*$。

基于分叉引理和 *l*-SDHP 难题，采用与 Barreto[9] 类似的证明方法，可以证明下面的定理(详见文献[9])。

定理 3. 如果存在一个自适应选择消息和身份攻击的伪造签名算法(攻击者)F，在经过对两个随机预言机 H_1, H_2 的 q_{h1} , q_{h2} 次询问及 q_s 次对签名预言机的询问后，能够在时间 t 内，以 $\varepsilon \geq 10(q_s+1)(q_s+q_{h2})/2^k$ 的概率伪造一个有效部分盲签名，那么就存在一个算法(挑战者)B 能够在给定时间 $t' \geq 120686 q_{h2}(t+O(q_s\tau_P))/(\varepsilon(1-l/2^k))+O(l^2\tau_{mult})$ (τ_{mult} 表示 G_1 上一次乘法运算的时间， τ_P 表示一次双线性对运算的时间)内解决 *l*-SDHP 难题，这里 $l = q_{h1}$。

由定理 3，可得到下面的定理：

定理 4. 方案是安全的，能够抵抗适应性选择消息和身份攻击下的存在性伪造。

另外，和一般基于身份的部分盲签名相比[3,7]，本方案更为安全，原因在于下面的定理 5。

定理 5. 方案可以抵抗不可信 PKG 的攻击。

证明：首先假设在协议的执行过程中，PKG 是可信的，或没有被攻击者攻破，则 s_{pkg} 没有被泄露，由定理 3 可知，方案是安全的。

若假设不成立，PKG 是不可信的或已经被攻击者攻破，则 PKG 或攻击者会采取下述二者之一的行动：

① 从(ID, Q_{ID})中推测出用户的签名私钥 S_{ID}，然后进行盲签名。

② 伪造用户的签名私钥和签名公钥，然后进行盲签名。

对于第 1 种情形，要从 $Q_{ID} = g^c$ (其中 g=e(P,P)∈G_2)求出 c,相当于求解离散对数难题 DLP。由离散对数问题的难解性可知，这是不可能的。因此，方案是安全的。

对于第 2 种情形，假设 PKG 要伪造一个身份信息为 ID 的合法用户的签名，PKG 可以按照以下步骤伪造：

(1) PKG 任意选择 $\forall c' \in_R Z_q^*$，计算 $S'_{ID} = c'P/(s_{pkg}+H_1(ID))$，再计算 $Q'_{ID} = g^{c'}$，得到身份信息为 ID 的用户的伪造签名公私钥对(Q'_{ID} , S'_{ID})。

(2) PKG 按照协议的签名步骤对消息 m 执行签名，得到 m 的“合法”签名(S, h)。

当身份为 ID 的用户发现有人伪造自己的签名时，可以向仲裁方要求进行仲裁，他可以向仲裁方提供证据证明这个签名是 PKG 伪造的。用户首先将(ID, Q_{ID})发送给仲裁方，然后用“零知识证明”的方法证明自己知道和(ID, Q_{ID})相对应的 S_{ID}。其过程为：仲裁方首先任意选取一个整数 a，计算 $a(P_{pkg}+H_1(ID)P)$发送给用户，用户计算 $e(S_{ID}, a(P_{pkg}+H_1(ID)P))$并发送给仲裁者。仲裁者验证 $e(S_{ID}, a(P_{pkg}+H_1(ID)P))=(Q_{ID})a$ 是否成立。若成立，则说明 PKG 或者参与伪造了身份为 ID 的合法用户的签名，或 PKG 已被攻破，s_{pkg} 已泄露，仲裁者可据此判定 PKG 是不可信的或不诚实的。这是因为身份信息为 ID 的公私钥对(Q_{ID} , S_{ID})应该只有一对，但现在有两个不同的(Q_{ID} , S_{ID})，(Q'_{ID} , S'_{ID})，说明 PKG 是不诚实的。

由上述分析可知，本方案可以抵抗不可信 PKG 的攻击。

由定理 2,4,5 可知，本方案是部分盲的，能够抵抗适应性选择消息和身份攻击下的存在性伪造，能够抵抗不可信 PKG 的伪造攻击。本方案相对于其他部分盲签名方案[3,4,5,7]更安全。

3.3 方案的效率分析

双线性对运算在所有运算中是最耗时的，一个对运算大约相当于 8 个有限域上模幂运算的计算量。设 Pa 表示一次双线性对运算，Ex 表示一次 G_2 上的幂运算，Mu_1 表示一次 G_1 上的数乘运算，Mu_2 表示一次 G_2 上的乘法，Ad 表示一次 G_1 上的加法。将本文方案和 Chow 方案[7]，FENG 方案[4]的计算量列表比较如下：

表 1 三个类似方案的计算量比较

Chow 方案[7]	FENG 方案[4]	本方案
初始化阶段： $1Mu_1$	初始化阶段： $1Mu_1$	初始化阶段： $1Pa+1Mu_1$
密钥生成阶段： $1Mu_1$ 对部分密钥的 验证：无	密钥生成阶段： $2Mu_1$ 对部分密钥的 验证：无	密钥生成阶段： $3Pa+2Mu_1+1Ad$ 对部分密钥的 验证：有
部分盲签名生成阶段： $10Mu_1+4Ad$	部分盲签名生成阶段： $7Mu_1+2Ad$	部分盲签名生成阶段： $4Ex+4Mu_1+$ $2Mu_2+2Ad$
签名验证阶段： $3Pa+1Mu_1+1Mu_2+1Ad$	签名验证阶段： $3Pa+1Mu_1+1Mu_2+1Ad$	签名验证阶段： $1Pa+2Ex+1Mu_1+2Mu_2+1Ad$

从表 1 可以看出，新方案在安全性增强的前提下，保证了很高的效率。本文方案相比于 Chow 方案、FENG 方案，在密钥生成阶段增加了对部分密钥的验证功能，由此增加的计算量为 1Pa，但由于对部分密钥 SID 的验证功能是基于身份无可信 PKG 的签名应具备且十分重要的一项安全特性(它保证了用户所获得部分密钥的正确性，进而奠定了整个系统正常运行的基础)，因此增加的计算量是值得的。虽然在初始化阶段和密钥生成阶段共增加了 3Pa 的计算量，但由于这两个阶段分别只在系统建立时运行一次，及每个用户生成公私钥对时才运行一次，因此增加的运算量并不影响以后签名的效率。反之，签名生成阶段和签名验证阶段是每个消息就要运行一次，本方案在这两个阶段的计算量相比于 Chow 方案和 FENG 方案大为减少，在性能上有较大的优势，适合在频繁传递消息和验证签名的电子政务和电子商务中使用。

4 结语

本文提出了一个基于身份无可信 PKG 的，只有一个对运算的部分盲签名方案，并证明了方案的强盲性和不可伪造性。方案可以抵抗适应性选择消息和身份攻击，可以抵抗不可信 PKG 的攻击，其安全性依赖于强 l-SDHP 难题，和其他类似方案相比具有更高的效率。基于身份无可信 PKG 的、只有一个对运算的部分盲签名方案，因其更强的可靠性和更高的效率，将在电子商务、电子政务和匿名电子投票等领域发挥更大的作用。

参考文献

1 Chaum D. Blind Signature for Untraceable Payments. Advances in Cryptology- CRYPTO’82 Proceedings. Plenum Press, 1983:199–233.

2 Shamir A. Identity-based Cryptosystems and Signature Schemes. Advances in Cryptology-CRYPTO’84 Proceedings. LNCS 196,1984.47–53.

3 农强,郝艳华,黄茹芬.对一种高效部分盲签名方案的密码学分析及改进.云南师范大学学报, 2010,30(1):32–35.

4 冯涛,彭伟,马建峰.安全的无可信 PKG 的部分盲签名方案.通信学报,2010,31(1):128–134.

5 张小萍,钟诚.高效无可信私钥生成中心部分盲签名方案.计算机应用,2011,31(4):992–995.

6 李明祥,王涛,罗新方.对两种基于双线性对的部分盲签名方案的密码学分析.计算机应用研究,2011,28(2):435–438.

7 Chow S, Hui L, Yiu S. Two Improved Partially Blind Signature Schemes from Bilinear Pairings. ASIACRYPTO 2005:Advances in Cryptology. Berlin: Springer-Verlag, 2005: 316–328.

8 Boneh D, Boyen X. Short Signatures without Random Oracles. Eurocrypt’04. volume 3027 of LNCS, page 56– 73, Springer, 2003.

9 Barreto PSLM, Libert B, McCullagh N, et al. Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps. Advances in Cryptology- ASIACRYPT’05. Berlin: Springer-Verlag, 2005.515–532.