doi:10.11959/j.issn.1000-436x.2015098

标准模型下安全的无证书签名方案

李艳琼，李继国，张亦辰
（河海大学 计算机与信息学院，江苏 南京 211100）

摘 要：随机预言模型下的证明能够为无证书签名方案提供基本的安全保证，但随机预言机的实现方式可能会导致方案不安全。一些标准模型下的方案在提出后被证明无法抵抗公钥替换攻击。为了解决这一问题，构造了一个标准模型下安全的无证书签名方案，基于 NGBDH 和 Many-DH 困难问题，证明所提出的方案对自适应选择消息攻击是存在性不可伪造的。此外，提出的方案具有计算代价和通信代价较低、能够抵抗密钥替换攻击等优点。
关键词：无证书签名；标准模型；NGBDH 问题；Many-DH 问题
中图分类号：TP309 **文献标识码**：A

Certificateless signature scheme without random oracles

LI Yan-qiong, LI Ji-guo, ZHANG Yi-chen
(College of Computer & Information, Hohai University, Nanjing 211100, China)

Abstract: The security of certificateless signature schemes can be proved under the random oracle model. However, any implementation of the random oracle may result in insecure schemes. Some certificateless signature schemes without random oracles are not secure against key replacement attack. In order to solve this problem, a new certificateless signature scheme in the standard model had constructed. Based on the NGBDH and Many-DH assumption, the scheme was proved secure against existentially unforgeable under adaptive chosen message attack. In addition, the proposed scheme enjoys less computation cost and lower communication bandwidth and can resist against key replacement attack.
Key words: certificateless signature; standard model; NGBDH problem; Many-DH problem

1 引言

传统的公钥密码体制使用数字证书认证用户公钥的有效性，这种方法耗费大量的时间、空间和计算，一度成为公钥密码体制发展的障碍。基于身份的密码体制[1]成功地解决了证书管理问题，但存在密钥托管问题。无证书公钥密码体制[2]中，用户的私钥是由两部分构成，即用户选择的秘密值和密钥生成中心产生的部分私钥。密钥生成中心无法获得用户的秘密值，从而避免了密钥托管问题。无证书公钥密码体制的优点吸引了很多学者的研究兴趣，许多无证书签名方案[2~17]也被相继提出。

2004 年，Yum 和 Lee[3]将传统签名方案和基于身份的签名方案相结合，提出了一种无证书签名的一般构造方法。2007 年，Du 等[9]提出一种不使用双线性对运算的无证书签名方案，其安全性规约为 k-CAA 和 Inv-CDH 困难问题，作者在随机预言模型下证明了方案的安全性。2008 年，Tso 等[12]提出一种高效的无证书短签名，该方案的计算代价和通信代价都比较低，因此，可以广泛应用于低带宽通信环境下。2011 年，张福泰等[15]对目前存在的研究成果进行系统的整理、分析、管理和评述，并提出无证书密码体制中存在的不足和下一步应当研究的重点。为了提高计算效率，文献[16]构造了一种不使用双线性对的无证书签名方案。但是，2013 年，王亚飞等[17]指出文献[16]中的方案是不安全的，攻

收稿日期：2014-01-22；**修回日期**：2014-10-28
基金项目：国家自然科学基金资助项目（61272542, 61103183, 61103184）；中央高校基本科研业务费专项基金资助项目（2013B07014）；江苏省“六大人才高峰”基金资助项目(2009182)
Foundation Items: The National Natural Science Foundation of China (61272542, 61103183, 61103184); The Fundamental Research Funds for the Central Universities (2013B07014); The Six Talent Peaks Program of Jiangsu Province (2009182)

击者可以根据非目标身份的签名询问结果计算出用户的秘密值和部分私钥，进而伪造任意消息对应的签名。进一步，王亚飞等[17]提出一种改进的无证书签名方案，目前，新方案的效率在所提出的无证书签名方案中是最高的。

上述无证书签名方案都是在随机预言模型下提出的，而这种设计可能导致方案的不安全[18]。研究表明，标准模型下的安全证明能够为无证书签名方案的设计提供更充分的保障。因此，研究标准模型下可证明安全的无证书签名方案具有重要的理论和现实意义，同时也是本文研究工作的主要动机之一。

在 ASIACCS 2007 会议上，Liu 等[19]提出了第一个标准模型下可证明安全的无证书签名方案。Yu 等[20]提出了一个改进方案，在标准模型下证明他们的方案是存在性不可伪造的。但是，该方案在验证过程中仍然需要 5 个双线性对运算，计算代价比较大。因此，标准模型下安全高效的无证书签名方案的构造成为信息安全研究热点之一。

本文基于文献[21]，构造了一种新的无证书签名方案，基于 NGBDH 和 Many-DH 的困难问题，在标准模型下证明了该方案是存在性不可伪造的。

2 预备知识

2.1 双线性映射

令 G_1、G_2 是阶为素数 q 的乘法循环群，g 为群 G_1 的生成元。$e:G_1\times G_1\to G_2$ 是一个可计算的双线性映射，具有以下性质。

1) 双线性：对任意 $a,b\in Z_q^*$，有 $e(g^a, g^b)=e(g,g)^{ab}$。

2) 非退化性：$e(g,g)\neq 1$。

3) 可计算性：存在有效的算法计算 e。

2.2 困难问题

定义 1 NGBDH 问题(non pairing-based generalized bilinear Diffie-Hellman problem)。令 G 为阶为素数 q 的乘法循环群，g 为群 G 的生成元。给定 (g,g^a,g^b)，其中 $a,b\in Z_q^*$，计算 (g^{abc},g^c)。

如果不存在概率多项式时间算法 A，能以不可忽略的优势成功解决 G 上的 NGBDH 问题，则称群 G 上的 NGBDH 问题是困难的。

定义 2 Many-DH 问题(many Diffie-Hellman problem)。令 G 为阶为素数 q 的乘法循环群，g 为群 G 的生成元。给定 $(g,g^a,g^b,g^c,g^{ab},g^{ac},g^{bc})$，其中 $a,b,c\in Z_q^*$，计算 g^{abc}。

概率多项式时间算法 A 解决 G 上的 Many-DH 问题的优势定义为

$$\mathrm{Succ}_{A,G}^{\text{Many-DH}}=\Pr[A(g,g^a,g^b,g^c,g^{ab},g^{ac},g^{bc})=g^{abc},\ a,b,c\in Z_q^*]$$

如果不存在概率多项式时间算法，能以不可忽略的优势成功解决 G 上的 Many-DH 问题，则称群 G 上 Many-DH 问题是困难的。

3 形式化定义和安全模型

无证书签名的形式化定义和安全模型主要参考文献[4,5,8]中的相关定义。

3.1 形式化定义

无证书签名方案的参与者包括密钥生成中心(KGC)、签名人和验证人。该方案由系统参数设置、部分私钥生成、用户密钥生成、签名和验证 5 个算法组成。

系统参数设置算法。输入安全参数 k，KGC 输出系统主密钥 msk 和系统参数 $params$。其中系统参数 $params$ 公开，而主密钥 msk 由 KGC 秘密保存。

部分私钥生成算法。给定系统参数 $params$、系统主密钥 msk 和用户身份 ID，KGC 产生用户的部分私钥 D_{ID}。

用户密钥生成算法。给定系统参数 $params$ 和用户身份 ID，产生该用户秘密值 x_{ID} 和公钥 PK_{ID}。

签名算法。给定系统参数 $params$、用户身份 ID、用户的部分私钥 D_{ID}、秘密值 x_{ID} 和待签名消息 m，产生签名 σ。

验证算法。给定系统参数 $params$、消息 m、签名 σ、用户身份 ID 以及公钥 PK_{ID}，验证者验证签名的有效性。若 σ 有效，输出 true；否则，输出 false。

3.2 安全模型

在无证书签名中考虑两类敌手 A_{I} 和 A_{II}。A_{I} 刻画了一个不诚实的用户，即 A_{I} 不知道系统主密钥，但可以替换任意用户的公钥。A_{II} 刻画了一个恶意的 KGC，即 A_{II} 知道系统主密钥，但不可以替换用户的公钥。

下面通过敌手 $A\in\{A_{\mathrm{I}},A_{\mathrm{II}}\}$ 与挑战者 B 之间的游戏 1 和游戏 2 来定义无证书签名方案的安全模型。

3.2.1　游戏 1

1) 系统参数设置：挑战者 B 执行系统参数设置算法，产生主密钥 msk 和系统参数 $params$。B 将 $params$ 发送给 A_{I}，主密钥 msk 保密。

2) 询问阶段：A_{I} 进行如下询问。

①部分私钥询问。挑战者 B 维护一个记录用户部分私钥的列表 $L_0=(ID,D_{ID})$，该表初始为空。敌手 A_{I} 询问身份为 ID 用户的部分私钥，若 $ID=ID^*$，模拟终止；否则，B 查询表 L_0 中是否存在 ID 项。如果存在，则直接返回 D_{ID} 给敌手 A_{I}；否则，B 运行部分私钥生成算法生成用户的部分私钥，将 (ID,D_{ID}) 添加到表 L_0 中，并返回 D_{ID} 给 A_{I}。

②秘密值询问。挑战者 B 维护一个记录用户秘密值和公钥的列表 $L_1=\{ID,x_{ID},PK_{ID},f_{ID}\}$，该表初始为空，$f_{ID}=0$ 表示用户公钥没有被替换，$f_{ID}=1$ 表示公钥被替换。敌手 A_{I} 询问身份为 ID 用户的秘密值，B 首先查询表 L_0 中是否存在 ID 项。若存在且 $f_{ID}=1$，B 返回 $\perp$ 给敌手；若 $f_{ID}=0$，B 直接返回 x_{ID} 给敌手。若不存在，B 运行用户密钥生成算法生成用户的秘密值和公钥，将 $\{ID,x_{ID},PK_{ID},0\}$ 添加到表 L_1 中，并返回 x_{ID} 给 A_{I}。

③公钥询问。敌手 A_{I} 询问身份为 ID 用户的公钥，B 首先查询表 L_0 中是否存在 ID 项。若存在，B 直接返回 PK_{ID} 给 A_{I}；若不存在，B 运行用户密钥生成算法生成用户的秘密值和公钥，将 $\{ID,x_{ID},PK_{ID},0\}$ 存储到表 L_1 中，并返回 PK_{ID} 给 A_{I}。

④公钥替换询问。敌手 A_{I} 提交 (ID,PK'_{ID})，B 检查表 L_0 中是否存在 ID 项。若不存在，将 $(ID,\perp,PK'_{ID},1)$ 添加到表 L_0 中；若存在，则将 ID 项更新为 $(ID,\perp,PK'_{ID},1)$。

⑤签名询问。敌手 A_{I} 询问身份为 ID 的用户对消息 m 的签名，B 运行签名算法生成签名 σ，并将 σ 返回给 A_{I}。

3) 伪造阶段：A_{I} 输出一个三元组 (m^*,ID^*,σ^*)，如果 (m^*,ID^*,σ^*) 满足如下条件，则称 A_{I} 赢得游戏。A_{I} 赢得游戏的优势定义为 $\mathrm{Succ}_{A_{\mathrm{I}}}^{\mathrm{CLS}}\geqslant\varepsilon$。

① σ^* 是目标身份 ID^* 和目标消息 m^* 的有效签名。

② A_{I} 没有询问过目标身份 ID^* 的部分私钥。

③ A_{I} 没有询问过目标身份 ID^* 对消息 m^* 的签名。

定义 3　如果在概率多项式时间内，不存在一个敌手 A_{I} 在自适应选择身份攻击和自适应选择消息攻击下，能以不可忽略的优势赢得游戏 1，那么就称无证书签名方案对第一类敌手是存在性不可伪造的。

3.2.2　游戏 2

1) 系统参数设置：挑战者 B 执行系统参数设置算法，产生主密钥 msk 和系统参数 $params$，B 把主密钥 msk 和 $params$ 都发送给 A_{II}。

2) 询问阶段：A_{II} 进行如下询问。

①秘密值询问。B 维持一个记录用户秘密值和公钥的列表 $L_1=\{ID,x_{ID},PK_{ID}\}$，该表初始为空。敌手 A_{II} 询问身份为 ID 用户的秘密值，若 $ID=ID^*$，模拟终止。否则，B 查询表 L_1 中是否存在 ID 项。若存在，则直接返回 x_{ID} 给敌手 A_{II}；若不存在，B 运行用户密钥生成算法生成用户的秘密值和公钥，将 $\{ID,x_{ID},PK_{ID}\}$ 添加到表 L_1 中，并返回 x_{ID} 给 A_{II}。

②公钥询问。敌手 A_{II} 询问身份为 ID 用户的公钥，B 首先查询 L_1 中是否存在 ID 项。若存在，则直接返回 PK_{ID} 给敌手 A_{II}；若不存在，B 运行用户密钥生成算法生成用户的秘密值和公钥，将 $\{ID,x_{ID},PK_{ID}\}$ 添加到表 L_1 中，并返回 PK_{ID} 给 A_{II}。

③签名询问。敌手 A_{II} 询问身份为 ID 用户对消息 m 的签名，B 运行签名算法生成签名 σ，并将 σ 返回给 A_{II}。

3) 伪造阶段：A_{II} 输出一个三元组 (m^*,ID^*,σ^*)，如果 (m^*,ID^*,σ^*) 满足如下条件，则称 A_{II} 赢得游戏。A_{II} 赢得游戏的优势定义为 $\mathrm{Succ}_{A_{\mathrm{II}}}^{\mathrm{CLS}}\geqslant\varepsilon$。

① σ^* 是目标身份 ID^* 和目标消息 m^* 的有效签名。

② A_{II} 没有询问过目标身份 ID^* 的秘密值。

③ A_{II} 没有询问过目标身份 ID^* 对消息 m^* 的签名。

定义 4　如果在概率多项式时间内，不存在一个敌手 A_{II} 在自适应选择身份攻击和自适应选择消息攻击下，能以不可忽略的优势赢得游戏 2，那么就称无证书签名方案对第两类敌手 A_{II} 存在性不可伪造的。

4　标准模型下安全的无证书签名方案

提出的无证书签名方案由如下算法组成。

1) 系统参数设置算法。给定安全参数 k，KGC 执行以下步骤生成系统参数。

①令 G_1、G_2 为阶是素数 q 的循环群，g 为群 G_1 的生成元，存在一个可计算的双线性映射 $e: G_1 \times G_1 \to G_2$。

②随机选取 $\alpha \in Z_q^*$，$g_2 \in G_1$，令 $g_1 = g^{\alpha}$，并设置系统主密钥 $msk = g_2^{\alpha}$。

③随机选择 2 个抗碰撞的散列函数 $H_u: \{0,1\}^* \to \{0,1\}^{n_u}$，$H_m: \{0,1\}^* \to \{0,1\}^{n_m}$，其中，$n_u$, $n_m \in Z_q^*$。

④随机选择 $u' \in Z_q^*$，$m' \in G_1$，n_u 维的向量 $\boldsymbol{U} = (u_i)$，n_m 维的向量 $\boldsymbol{M} = (m_j)$，其中，$u_i \in Z_q^*$，$m_j \in G_1$。

KGC 公开 $params = \{G_1, G_2, e, g, g_1, g_2, u', m', \boldsymbol{U}, \boldsymbol{M}\}$ 作为系统参数，系统主密钥 g_2^{α} 保密。

2) 部分私钥生成算法。输入用户身份 $ID \in \{0,1\}^*$，KGC 按照如下步骤生成用户的部分私钥。

①计算 $\tilde{u} = H_u(ID)$，令 $U = \{i \mid \tilde{u}[i] = 1, 1 \leqslant i \leqslant n_u\}$，其中，$\tilde{u}[i]$ 为 $\tilde{u}$ 的第 i bit。

②KGC 随机选择 $r \in Z_q^*$，计算用户的部分私钥 $D_{ID} = (d_1, d_2) = (g_2^{\alpha + r(u' + \sum_{i \in U} u_i)}, g^r)$，并通过安全通道将部分私钥传送给用户。

3) 用户密钥生成算法。用户随机选择 $x_{ID} \in Z_q^*$，把 x_{ID} 作为自己的秘密值，并设置公钥 $PK_{ID} = (pk_1, pk_2, pk_3) = (g^{x_{ID}}, g_1^{x_{ID}}, g_2^{x_{ID}})$。

4) 签名算法。已知消息 $m \in \{0,1\}^*$，用户的身份 ID，部分私钥 D_{ID} 和秘密值 x_{ID}，用户按照如下方法生成签名。

①计算 $\tilde{m} = H_m(m)$，令 $M = \{j \mid \tilde{m}[j] = 1, 1 \leqslant j \leqslant n_m\}$，其中，$\tilde{m}[j]$ 为 $\tilde{m}$ 的第 j bit。

②随机选择 $s \in Z_q^*$，计算消息 m 的签名 $\sigma = (V, R_1, R_2) = (d_1^{x_{ID}} (m' \prod_{j \in M} m_j)^s, d_2^{x_{ID}}, g^s)$。

5) 验证算法。验证者收到消息签名对 (m, σ) 后，使用 $params$ 和用户公钥 PK_{ID} 对签名进行验证。若 $e(V, g) = e(g_2, pk_2) e(g_2, R_1)^{u' + \sum_{i \in U} u_i} e(m' \prod_{j \in M} m_j, R_2)$，输出 true；否则，输出 false。

6) 正确性分析。

$$
\begin{aligned}
e(V, g) &= e(g_2^{\alpha x_{ID}} g_2^{r x_{ID}(u' + \sum_{i \in U} u_i)} (m' \prod_{j \in M} m_j)^s, g) \\
&= e(g_2^{\alpha x_{ID}}, g) e(g_2^{r x_{ID}(u' + \sum_{i \in U} u_i)}, g) e((m' \prod_{j \in M} m_j)^s, g) \\
&= e(g_2, g_1^{x_{ID}}) e(g_2, g^{r x_{ID}})^{(u' + \sum_{i \in U} u_i)} e(m' \prod_{j \in M} m_j, g^s) \\
&= e(g_2, pk_2) e(g_2, R_1)^{(u' + \sum_{i \in U} u_i)} e(m' \prod_{j \in M} m_j, R_2)
\end{aligned}
$$

5 安全性证明

根据第 3 节提出的无证书签名方案的定义和安全模型，证明本文提出的无证书签名方案在标准模型下是安全的。

定理 1 如果存在一个概率多项式时间敌手 A_{I}，进行最多 q_e 次部分私钥询问，q_s 次签名询问，以概率 ε 赢得游戏 1。则存在一个算法 B，在多项式时间内以 $\varepsilon' \geqslant \dfrac{\varepsilon}{16 q_s (q_e + q_s)(n_u + 1)(n_m + 1)}$ 的概率成功解决 NGBDH 困难问题。

证明 以 (g, g^a, g^b) 为输入，目标是计算 (g^{abc}, g^c)，利用算法 B 解决 NGBDH 问题。B 扮演挑战者与敌手 A_{I} 进行交互，利用 A_{I} 的能力解决 NGBDH 问题。

1) 系统参数设置：算法 B 按照以下 4 个步骤构造系统参数。

①令 $l_u = 2(q_e + q_s)$，$l_m = 2q_s$。B 随机选择 2 个整数 k_u 和 k_m，满足 $0 \leqslant k_u \leqslant n_u$，$0 \leqslant k_m \leqslant n_m$。对于给定的值 q_e、q_s、n_u、n_m，假定 $l_u(n_u + 1) < q$，$l_m(n_m + 1) < q$。

②随机选择 $x' \in Z_{l_u}$ 及长度为 n_u 的向量 $\boldsymbol{X} = (x_i)$，且 $x_i \in Z_{l_u}$；随机选择 $z' \in Z_{l_m}$ 及长度为 n_m 的向量 $\boldsymbol{Z} = (z_j)$，且 $z_j \in Z_{l_m}$；随机选择 $w' \in Z_{l_m}$ 及长度为 n_m 的向量 $\boldsymbol{W} = (w_j)$，且 $w_j \in Z_{l_m}$。

③对于 $\tilde{u}$ 和 $\tilde{m}$，其中，$\tilde{u} = H_u(ID)$，$\tilde{m} = H_m(m)$，定义以下 3 个函数：$F(\tilde{u}) = x' + \sum_{i \in U} x_i - l_u k_u$，$K(\tilde{m}) = z' + \sum_{j \in M} z_j - l_m k_m$，$L(\tilde{m}) = w' + \sum_{j \in M} w_j$。

④B 构造系统公开参数如下：$g_1 = g^a$，$g_2 = g^b$；$u' = x' - l_u k_u$，$u_i = x_i$，其中，$1 \leqslant i \leqslant n_u$；$m' = g_2^{z' - l_m k_m} g^{w'}$，$m_j = g_2^{z_j} g^{w_j}$，其中，$1 \leqslant j \leqslant n_m$。则

$F(\tilde{u})=u'+\sum_{i\in U}u_i$，$m'\prod_{j\in M}m_j=g_2^{K(\tilde{m})}g^{L(\tilde{m})}$。$B$ 将系统公开参数返回给 A_1，系统主密钥 $msk=g_2^{\alpha}=g^{ab}$ 秘密保存。

2) 询问阶段：算法 B 模拟挑战者与敌手 A_1 进行交互，过程如下。

① 部分私钥询问。B 维持一个列表 $L_0=\{ID,D_{ID},h_{ID}\}$ 用于记录用户的部分私钥，该表初始为空。$h_{ID}=0$ 表示 $F(\tilde{u})\neq 0 \bmod q$，$h_{ID}=1$ 表示 $F(\tilde{u})=0 \bmod q$。A_1 询问用户 ID 的部分私钥，B 计算 $\tilde{u}=H_u(ID)$。当 $h_{ID}=1$ 时，模拟过程终止，B 失败退出。当 $h_{ID}=0$ 时，B 检查表 L_0 中是否存在 ID 项。若存在，则直接返回 D_{ID} 给敌手 A_1；否则，B 随机选择 $r\in Z_q^*$，计算用户的部分私钥 $D_{ID}=(d_1,d_2)=(g_2^{rF(\tilde{u})},g_1^{\frac{1}{F(\tilde{u})}}g^r)$。令 $r'=r-\frac{a}{F(\tilde{u})}$，则可得 $d_1=g_2^{rF(\tilde{u})}=g_2^{(r-\frac{\alpha}{F(\tilde{u})})F(\tilde{u})}g_2^{\alpha}=g_2^{\alpha+(r-\frac{\alpha}{F(\tilde{u})})F(\tilde{u})}=g_2^{\alpha+r'F(\tilde{u})}$，$d_2=g_1^{\frac{1}{F(\tilde{u})}}g^r=g^{-\frac{\alpha}{F(\tilde{u})}}g^r=g^{r-\frac{\alpha}{F(\tilde{u})}}=g^{r'}$。$B$ 返回 D_{ID} 给 A_1，并将元组 $\{ID,D_{ID},0\}$ 添加到表 L_0 中。

②秘密值询问。B 维持一个记录用户秘密值和公钥的列表 $L_1=\{ID,x_{ID},PK_{ID},f_{ID}\}$，该表初始为空。$f_{ID}=0$ 表示用户公钥没有被替换，$f_{ID}=1$ 表示公钥被替换。A_1 询问用户 ID 的秘密值，若 ID 项在 L_1 表中且 $f_{ID}=1$，B 返回 $\perp$ 给 A_1；若 ID 项在 L_1 表中且 $f_{ID}=0$，B 直接返回秘密值 x_{ID} 给 A_1；若表 L_1 中没有 ID 项，B 随机选择 $x_{ID}\in Z_q^*$，计算 $PK_{ID}=(pk_1,pk_2,pk_3)=(g^{x_{ID}},g_1^{x_{ID}},g_2^{x_{ID}})$ 作为公钥。B 发送 x_{ID} 给 A_1，并将元组 $(ID,x_{ID},PK_{ID},0)$ 存储到表 L_1 中。

③公钥询问。A_1 询问身份为 ID 用户的公钥，B 检查 $\{ID,x_{ID},PK_{ID},f_{ID}\}$ 是否在 L_1 表中。若 ID 项在 L_1 表中，B 返回公钥 PK_{ID} 给 A_1；若 ID 项不在 L_1 表中，B 随机选择 $x_{ID}\in Z_q^*$，计算 $PK_{ID}=(pk_1,pk_2,pk_3)=(g^{x_{ID}},g_1^{x_{ID}},g_2^{x_{ID}})$ 作为公钥。B 发送 PK_{ID} 给 A_1，将 $(ID,x_{ID},PK_{ID},0)$ 存储到表 L_1 中。

④公钥替换询问。敌手 A_1 提交公钥替换询问 (ID,PK_{ID}')，B 查询 ID 项是否存在表 L_1 中。如果不存在，那么 B 把 $(ID,\perp,PK_{ID}',1)$ 存储到表 L_1 中；否则，B 把表 L_1 中的 ID 项替换为 $(ID,\perp,PK_{ID}',1)$。

⑤签名询问。敌手 A_1 对 (ID,m) 进行签名询问，B 计算 $\tilde{u}=H_u(ID)$，$\tilde{m}=H_m(m)$，并判断 L_1 表中 ID 的公钥是否被替换。

ⓐ若 L_1 表中 ID 的公钥被替换，假定 $K(\tilde{m})\neq 0 \bmod l_m$，由于 $l_m(n_m+1)<q$，则 $K(\tilde{m})\neq 0 \bmod q$。$B$ 按照如下方式生成签名：随机选取 $r,s\in Z_q^*$，计算 $\sigma=(V,R_1,R_2)=((pk_3)^{rF(\tilde{u})}(pk_2)^{-\frac{L(\tilde{m})}{K(\tilde{m})}}\cdot(m'\prod_{j\in M}m_j)^s,(pk_1)^r,(pk_2)^{-\frac{1}{K(\tilde{m})}}g^s)=((g_2^{\alpha+rF(\tilde{u})})^{x_{ID}}\cdot(m'\prod_{j\in M}m_j)^{s'},(pk_1)^r,g^{s'})$，其中，$s'=s-\frac{\alpha x_{ID}}{K(\tilde{m})}$。$B$ 将 $\sigma=(V,R_1,R_2)$ 返回给敌手 A_1，A_1 验证签名的正确性。

$$
\begin{aligned}
V&=(pk_3)^{rF(\tilde{u})}(pk_2)^{-\frac{L(\tilde{m})}{K(\tilde{m})}}(m'\prod_{j\in M}m_j)^s\\
&=(g_2^{x_{ID}})^{rF(\tilde{u})}g_1^{-\frac{L(\tilde{m})x_{ID}}{K(\tilde{m})}}(m'\prod_{j\in M}m_j)^s\\
&=(g_2^{x_{ID}})^{rF(\tilde{u})}g_1^{-\frac{L(\tilde{m})x_{ID}}{K(\tilde{m})}}(g_2^{K(\tilde{m})}g^{L(\tilde{m})})^s\\
&=(g_2^{x_{ID}})^{rF(\tilde{u})}g_1^{-\frac{L(\tilde{m})x_{ID}}{K(\tilde{m})}}(g_2^{K(\tilde{m})}g^{L(\tilde{m})})^{\frac{\alpha x_{ID}}{K(\tilde{m})}}(g_2^{K(\tilde{m})}g^{L(\tilde{m})})^{s-\frac{\alpha x_{ID}}{K(\tilde{m})}}\\
&=(g_2^{x_{ID}})^{rF(\tilde{u})}g^{-\frac{\alpha x_{ID}L(\tilde{m})}{K(\tilde{m})}}g_2^{\alpha x_{ID}}g^{\frac{\alpha x_{ID}L(\tilde{m})}{K(\tilde{m})}}(g_2^{K(\tilde{m})}g^{L(\tilde{m})})^{s-\frac{\alpha x_{ID}}{K(\tilde{m})}}\\
&=(g_2^{x_{ID}})^{rF(\tilde{u})}g_2^{\alpha x_{ID}}(g_2^{K(\tilde{m})}g^{L(\tilde{m})})^{s'}\\
&=(g_2^{\alpha+rF(\tilde{u})})^{x_{ID}}(m'\prod_{j\in M}m_j)^{s'}
\end{aligned}
$$

$R_2=g^s(pk_2)^{-\frac{1}{K(\tilde{m})}}=g^{s-\frac{\alpha x_{ID}}{K(\tilde{m})}}=g^{s'}$。对敌手 A_1 来说，B 生成的签名与真正的挑战者产生的签名是不可区分的。

若 $K(\tilde{m})=0 \bmod l_m$，模拟过程终止，B 失败退出。

ⓑ若 L_1 表中 ID 的公钥没有被替换且 $F(\tilde{u})\neq 0 \bmod l_u$，$B$ 检查表 L_0 和 L_1 中是否存在 ID 项。若存在，则 B 直接按照签名算法生成消息 m 的签名 σ，并将它返回给敌手 A_1；若不存在，则 B 根据部分私钥询问预言机构造一个部分私钥 D_{ID}，并把它添加到表 L_0 中。然后执行用户密钥生成算法生成用户的秘密值和公钥，并把它们添加到表 L_1 中。最后 B 按照签名算法生成消息 m 的签名 σ，将它返回给敌手 A_1。

ⓒ若 L_1 表中 ID 的公钥没有被替换且 $F(\tilde{u})=0 \bmod l_u$，假定 $K(\tilde{m})\neq 0 \bmod l_m$，由于 $l_m(n_m+1)<q$，则 $K(\tilde{m})\neq 0 \bmod q$。$B$ 按照如下方式生成消息 m 的签名：B 随机选择 $r,s\in Z_q^*$，从表 L_1 中查询 ID 的秘密值 x_{ID}（若表中不存在 ID 项，则运行

用户密钥生成算法生成秘密值和公钥，并将它们添加到表 L_1 中)，然后计算 $\sigma=(V,R_1,R_2)=\ ((pk_3)^{rF(\tilde{u})}\cdot g_1^{-\frac{x_{ID}L(\tilde{m})}{K(\tilde{m})}}(m'\prod_{j\in M}m_j)^{sx_{ID}},(pk_1)^r,g_1^{-\frac{1}{K(\tilde{m})}}g^{sx_{ID}})=((g_2^{\alpha+rF(\tilde{u})})^{x_{ID}}\cdot(m'\prod_{j\in M}m_j)^{s'},(pk_1)^r,g^{s'})$，其中，$s'=sx_{ID}-\frac{\alpha x_{ID}}{K(\tilde{m})}$。$B$ 将 $\sigma=(V,R_1,R_2)$ 返回给敌手 A_1，A_1 验证签名的正确性。

$$
\begin{aligned}
V&=(pk_3)^{rF(\tilde{u})}g_1^{-\frac{x_{ID}L(\tilde{m})}{K(\tilde{m})}}(m'\prod_{j\in M}m_j)^{sx_{ID}}\\
&=(g_2^{x_{ID}})^{rF(\tilde{u})}g_1^{-\frac{x_{ID}L(\tilde{m})}{K(\tilde{m})}}(m'\prod_{j\in M}m_j)^{sx_{ID}}\\
&=(g_2^{x_{ID}})^{rF(\tilde{u})}g_1^{-\frac{x_{ID}L(\tilde{m})}{K(\tilde{m})}}(g_2^{K(\tilde{m})}g^{L(\tilde{m})})^{sx_{ID}}\\
&=(g_2^{x_{ID}})^{rF(\tilde{u})}g_1^{-\frac{x_{ID}L(\tilde{m})}{K(\tilde{m})}}(g_2^{K(\tilde{m})}g^{L(\tilde{m})})^{\frac{\alpha x_{ID}}{K(\tilde{m})}}(g_2^{K(\tilde{m})}g^{L(\tilde{m})})^{sx_{ID}-\frac{\alpha x_{ID}}{K(\tilde{m})}}\\
&=(g_2^{x_{ID}})^{rF(\tilde{u})}g^{-\frac{\alpha x_{ID}L(\tilde{m})}{K(\tilde{m})}}g_2^{\alpha x_{ID}}g^{\frac{\alpha x_{ID}L(\tilde{m})}{K(\tilde{m})}}(g_2^{K(\tilde{m})}g^{L(\tilde{m})})^{sx_{ID}-\frac{\alpha x_{ID}}{K(\tilde{m})}}\\
&=(g_2^{x_{ID}})^{rF(\tilde{u})}g_2^{\alpha x_{ID}}(g_2^{K(\tilde{m})}g^{L(\tilde{m})})^{s'}\\
&=(g_2^{\alpha+rF(\tilde{u})})^{x_{ID}}(m'\prod_{j\in M}m_j)^{s'}
\end{aligned}
$$

$R_2=g^{sx_{ID}}g_1^{-\frac{1}{K(\tilde{m})}}=g^{sx_{ID}-\frac{\alpha x_{ID}}{K(\tilde{m})}}=g^{s'}$。对敌手 A_1 来说，B 生成的签名与真正的挑战者产生的签名是不可区分的。

若 $K(\tilde{m})=0\bmod l_m$，模拟过程终止，B 失败退出。

3) 伪造阶段：若算法 B 在上述询问中没有失败退出，则敌手 A_1 至少以概率 ε 成功伪造用户 ID^* 对消息 m^* 的有效签名 $\sigma^*=(V^*,R_1^*,R_2^*)$。其中 $V^*=g_2^{\alpha x_{ID}^*}\cdot\ g_2^{r^*F(\tilde{u}^*)x_{ID}^*}(m'\prod_{j\in M}m_j)^{s^*}$，$R_1^*=(pk_1^*)^{r^*}$，$R_2^*=g^{s^*}$。

若 $F(\tilde{u}^*)\neq 0\bmod q$ 或者 $K(\tilde{m}^*)\neq 0\bmod q$，$B$ 终止。否则，B 计算 $\frac{V^*}{(R_2^*)^{L(\tilde{m}^*)}}=\frac{g_2^{\alpha x_{ID}^*}g_2^{r^*F(\tilde{u}^*)x_{ID}^*}(m'\prod_{j\in M}m_j)^{s^*}}{(g^{s^*})^{L(\tilde{m}^*)}}=\frac{g_2^{\alpha x_{ID}^*}(g_2^{K(\tilde{m}^*)}g^{L(\tilde{m}^*)})^{s*}}{(g^{s^*})^{L(\tilde{m}^*)}}=g^{abx_{ID}^*}$。

算法 B 输出 $(g^{abx_{ID}^*},pk_1^*)=(g^{abx_{ID}^*},g^{x_{ID}^*})$ 作为 NGBDH 问题的解。

4) 概率计算：若算法 B 在模拟过程中没有终止，则必须满足以下几个条件。

①部分私钥询问成功，则有 $F(\tilde{u})\neq 0\bmod l_u$。

②签名询问成功，若 ID 的公钥未被替换，则有 $F(\tilde{u})\neq 0\bmod l_u$ 或者 $K(\tilde{m})\neq 0\bmod l_m$；若 ID 的公钥被替换，则有 $K(\tilde{m})\neq 0\bmod l_m$。

③签名伪造成功，则有 $F(\tilde{u}^*)=0\bmod q$ 和 $K(\tilde{m}^*)=0\bmod q$。

设 $\tilde{u}_1,\cdots,\tilde{u}_{q_I}$ 为部分私钥询问或者签名询问中出现的所有用户身份的散列函数 H_u 的输出值(不包括目标身份 ID^*)，$\tilde{m}_1,\cdots,\tilde{m}_{q_M}$ 为签名询问中出现的所有消息 m 的散列函数 H_m 的输出值。显然有 $q_I<q_e+q_s$，$q_M<q_s$ 成立。为了计算方便，定义 4 个事件 A_i、A^*、B_j、B^* 如下

$A_i:F(\tilde{u}_i)\neq 0\bmod l_u$，其中，$i=1,\cdots,q_I$，$A^*:F(\tilde{u}^*)=0\bmod q$

$B_j:K(\tilde{m}_j)\neq 0\bmod l_m$，其中，$j=1,\cdots,q_M$，$B^*:K(\tilde{m}^*)=0\bmod q$

则算法 B 模拟成功的概率 $\Pr[\neg abort]\geqslant\Pr[(\wedge_{i=1}^{q_I}A_i\wedge A^*)\wedge(\wedge_{j=1}^{q_M}B_j\wedge B^*)]$，其中事件 $(\wedge_{i=1}^{q_I}A_i\wedge A^*)$ 和事件 $(\wedge_{j=1}^{q_M}B_j\wedge B^*)$ 是相互独立的。

由假设 $l_u(n_u+1)<q$ 知，如果 $F(\tilde{u})=0\bmod q$ 成立，那么 $F(\tilde{u})=0\bmod l_u$ 也成立。进一步推出若 $F(\tilde{u})=0\bmod l_u$，则存在唯一的 k_u 使 $F(\tilde{u})=0\bmod q$ 成立，其中，$0\leqslant k_u\leqslant n_u$。从而有：$\Pr[A^*]=\Pr[F(\tilde{u}^*)=\ 0\bmod q\wedge F(\tilde{u}^*)=0\bmod l_u]=\Pr(F(\tilde{u}^*)=0\bmod l_u)\Pr[F(\tilde{u}^*)=0\bmod q\mid F(\tilde{u}^*)=0\bmod l_u]=\frac{1}{l_u}\frac{1}{n_u+1}$。

另一方面，$\Pr[\wedge_{i=1}^{q_I}A_i]=1-\Pr[\vee_{i=1}^{q_I}\neg A_i]\geqslant 1-\sum_{i=1}^{q_I}\Pr[\neg A_i]=1-\frac{q_I}{l_u}$。

由于事件 A_i 和 A^* 是相互独立的，所以有

$$
\begin{aligned}
\Pr[(\wedge_{i=1}^{q_I}A_i\wedge A^*)]&=\Pr[\wedge_{i=1}^{q_I}A_i]\Pr[A^*]\\
&=(1-\frac{q_I}{l_u})\frac{1}{(n_u+1)\ l_u}\geqslant(1-\frac{q_e+q_s}{l_u})\frac{1}{(n_u+1)\ l_u}\\
&=\frac{1}{2(q_e+q_s)(n_u+1)}(1-\frac{q_e+q_s}{2(q_e+q_s)})\\
&=\frac{1}{4(q_e+q_s)(n_u+1)}
\end{aligned}
$$

其中，$l_u=2(q_e+q_s)$。

同理 $\Pr(\wedge_{j=1}^{q_M}B_j\wedge B^*)=\frac{1}{4q_s(n_m+1)}$，则 $\Pr[\neg abort]\geqslant\Pr[(\wedge_{i=1}^{q_I}A_i\wedge A^*)\wedge(\wedge_{j=1}^{q_M}B_j\wedge B^*)]\geqslant$

$\frac{1}{16q_s(q_e+q_s)(n_u+1)(n_m+1)}$。

如果模拟没有终止，则敌手 A_{I} 至少以概率 ε 成功伪造一个有效签名。

因此算法 B 成功解决 NGBDH 问题的概率 $\varepsilon' \geqslant \frac{\varepsilon}{16q_s(q_e+q_s)(n_u+1)(n_m+1)}$。

定理 2　如果存在一个概率多项式时间敌手 A_{II}，进行最多 q_k 次秘密值和公钥询问，q_s 次签名询问后，以概率 ε 赢得游戏 2。则存在一个算法 B，在多项式时间内以 $\varepsilon' \geqslant \frac{\varepsilon}{16q_s(q_k+q_s)(n_u+1)(n_m+1)q_k}$ 的概率成功解决 Many-DH 困难问题。

证明　以 $(g,g^a,g^b,g^c,g^{ab},g^{ac},g^{bc})$ 为输入，目标是计算 g^{abc}，利用算法 B 解决 Many-DH 问题。B 扮演挑战者与敌手 A_{II} 进行交互，利用 A_{II} 的能力解决 Many-DH 问题。

1) 系统参数设置：算法 B 按照以下 4 个步骤构造系统参数。

①令 $l_u=2(q_k+q_s)$，$l_m=2q_s$。B 随机选择 2 个整数 k_u 和 k_m，满足 $0\leqslant k_u\leqslant n_u$，$0\leqslant k_m\leqslant n_m$。对于给定的值 q_s、q_k、n_u、n_m，假定 $l_u(n_u+1)<q$，$l_m(n_m+1)<q$。

②随机选择 $x'\in Z_{l_u}$ 及长度为 n_u 的向量 $\boldsymbol{X}=(x_i)$，且 $x_i\in Z_{l_u}$；随机选择 $z'\in Z_{l_m}$ 及长度为 n_m 的向量 $\boldsymbol{Z}=(z_j)$，且 $z_j\in Z_{l_m}$；随机选择 $w'\in Z_{l_m}$ 及长度为 n_m 的向量 $\boldsymbol{W}=(w_j)$，且 $w_j\in Z_{l_m}$。

③对于字符串 $\tilde{u}$ 和 $\tilde{m}$，其中 $\tilde{u}=H_u(ID)$，$\tilde{m}=H_m(m)$，定义以下 3 个函数：$F(\tilde{u})=x'+\sum_{i\in U}x_i-l_uk_u$，$K(\tilde{m})=z'+\sum_{j\in M}z_j-l_mk_m$，$L(\tilde{m})=w'+\sum_{j\in M}w_j$。

④B 构造系统参数如下：$g_1=g^a$，$g_2=g^b$；$u'=x'-l_uk_u$，$u_i=x_i$，其中，$1\leqslant i\leqslant n_u$；$m'=g_2^{z'-l_mk_m}g^{w'}$，$m_j=g_2^{z_j}g^{w_j}$，其中，$1\leqslant j\leqslant n_m$。则系统公开参数为 $F(\tilde{u})=u'+\sum_{i\in U}u_i$，$m'\prod_{j\in M}m_j=g_2^{K(\tilde{m})}g^{L(\tilde{m})}$，$g$，$g_1=g^a$，$g_2=g^b$，$pk_1^*=g^{x_{ID}^*}$，$pk_2^*=g^{ax_{ID}^*}$，$pk_3^*=g^{bx_{ID}^*}$。$B$ 将系统公开参数和系统主密钥 $msk=g_2^{\alpha}=g^{ab}$ 返回给 A_{II}。

2) 询问阶段：算法 B 模拟挑战者与敌手 A_{II} 进行交互，过程如下。

①秘密值询问。B 维持一个列表 $L_1=\{ID,x_{ID},PK_{ID}\}$ 用于记录用户秘密值和公钥，该表初始为空。A_{II} 询问用户 ID 的秘密值，若 $ID=ID^*$，模拟终止，B 失败退出。否则，B 查询 L_1 列表，若 ID 项在 L_1 列表中，B 直接返回 ID 的秘密值 x_{ID} 给 A_{II}；若表 L_1 中没有 ID 项，B 随机选择 $x_{ID}\in Z_q^*$，计算 $PK_{ID}=(pk_1,pk_2,pk_3)=(g^{x_{ID}},g_1^{x_{ID}},g_2^{x_{ID}})$ 作为公钥。B 发送 x_{ID} 给 A_{II}，把元组 $(ID,x_{ID},PK_{ID},0)$ 存储到表 L_1 中。

②公钥询问。A_{II} 询问用户 ID 的私钥，B 检查 $\{ID,x_{ID},PK_{ID}\}$ 是否在 L_1 列表中。若 ID 项在 L_1 列表中，B 直接返回公钥 PK_{ID} 给敌手 A_{II}；若 ID 项不在 L_1 表中，B 随机选取 $x_{ID}\in Z_q^*$，计算 $PK_{ID}=(pk_1,pk_2,pk_3)=(g^{x_{ID}},g_1^{x_{ID}},g_2^{x_{ID}})$。$B$ 返回 PK_{ID} 给 A_{II}，并将元组 (ID,x_{ID},PK_{ID}) 添加到表 L_1 中。

③签名询问：敌手 A_{II} 对 (ID,m) 进行签名询问，B 首先计算 $\tilde{u}=H_u(ID)$，$\tilde{m}=H_m(m)$。

ⓐ若 $ID=ID^*$，假定 $K(\tilde{m})\neq 0 \bmod l_m$，由于 $l_m(n_m+1)<q$，则 $K(\tilde{m})\neq 0 \bmod q$。$B$ 按照如下生成消息 m 的签名：随机选取 $r,s\in Z_q^*$，计算

$$\sigma=(V,R_1,R_2)=((pk_3)^{rF(\tilde{u})}(pk_2)^{-\frac{L(\tilde{m})}{K(\tilde{m})}}(m'\prod_{j\in M}m_j)^s,(pk_1)^r,$$

$$(pk_2)^{-\frac{1}{K(\tilde{m})}}g^s)=((g_2^{\alpha+rF(\tilde{u})})^{x_{ID}}(m'\prod_{j\in M}m_j)^{s'},(pk_1)^r,g^{s'})$$

其中，$s'=s-\frac{\alpha x_{ID}}{K(\tilde{m})}$。$B$ 将 $\sigma=(V,R_1,R_2)$ 返回给敌手 A_{II}，A_{II} 验证签名的正确性。

$$\begin{aligned}
V&=(pk_3)^{rF(\tilde{u})}(pk_2)^{-\frac{L(\tilde{m})}{K(\tilde{m})}}(m'\prod_{j\in M}m_j)^s\\
&=(g_2^{x_{ID}})^{rF(\tilde{u})}g_1^{-\frac{L(\tilde{m})x_{ID}}{K(\tilde{m})}}(m'\prod_{j\in M}m_j)^s\\
&=(g_2^{x_{ID}})^{rF(\tilde{u})}g_1^{-\frac{L(\tilde{m})x_{ID}}{K(\tilde{m})}}(g_2^{K(\tilde{m})}g^{L(\tilde{m})})^s\\
&=(g_2^{x_{ID}})^{rF(\tilde{u})}g_1^{-\frac{L(\tilde{m})x_{ID}}{K(\tilde{m})}}(g_2^{K(\tilde{m})}g^{L(\tilde{m})})^{\frac{\alpha x_{ID}}{K(\tilde{m})}}(g_2^{K(\tilde{m})}g^{L(\tilde{m})})^{s-\frac{\alpha x_{ID}}{K(\tilde{m})}}\\
&=(g_2^{x_{ID}})^{rF(\tilde{u})}g^{-\frac{\alpha x_{ID}L(\tilde{m})}{K(\tilde{m})}}g_2^{\alpha x_{ID}}g^{\frac{\alpha x_{ID}L(\tilde{m})}{K(\tilde{m})}}\\
&=(g_2^{x_{ID}})^{rF(\tilde{u})}g_2^{\alpha x_{ID}}(g_2^{K(\tilde{m})}g^{L(\tilde{m})})^{s'}\\
&=(g_2^{\alpha+rF(\tilde{u})})^{x_{ID}}(m'\prod_{j\in M}m_j)^{s'}
\end{aligned}$$

$R_2 = g^s (pk_2)^{-\frac{1}{K(\tilde{m})}} = g^{s-\frac{\alpha x_{ID}}{K(\tilde{m})}} = g^{s'}$。对敌手 A_{II} 来说，B 生成的签名与真正的挑战者产生的签名是不可区分的。

若 $K(\tilde{m}) = 0 \bmod l_m$，模拟过程终止，$B$ 失败退出。

ⓑ若 $ID \neq ID^*$ 且 $F(\tilde{u}) \neq 0 \bmod l_u$，$B$ 根据定理 1 中的部分私钥询问预言机构造一个部分私钥 D_{ID}，然后检查表 L_1 中是否存在 ID 项。若存在，则 B 直接按照签名算法生成消息 m 的签名 σ，并将它返回给敌手 A_{II}；若不存在，则 B 执行用户密钥算法生成用户的秘密值和公钥，并把它们添加到表 L_1 中。然后按照签名算法生成消息 m 的签名 σ，将它返回给敌手 A_{II}。

ⓒ 若 $ID \neq ID^*$ 且 $F(\tilde{u}) = 0 \bmod l_u$，假定 $K(\tilde{m}) \neq 0 \bmod l_m$，由于 $l_m(n_m+1) < q$，则 $K(\tilde{m}) \neq 0 \bmod q$。$B$ 按照如下方式生成消息 m 的签名：B 随机选择 $r, s \in Z_q^*$，从表 L_1 中查询 ID 的秘密值 x_{ID} (若不存在，则运行用户密钥生成算法生成用户的秘密值和公钥，并把它们添加到表 L_1 中)，然后计算

$$\sigma = (V, R_1, R_2) = ((pk_3)^{rF(\tilde{u})} g_1^{-\frac{x_{ID}L(\tilde{m})}{K(\tilde{m})}} (m' \prod_{j \in M} m_j)^{sx_{ID}}, (pk_1)^r,$$

$$g_1^{-\frac{1}{K(\tilde{m})}} g^{sx_{ID}} = ((g_2^{\alpha + rF(\tilde{u})})^{x_{ID}} (m' \prod_{j \in M} m_j)^{s'}, (pk_1)^r, g^{s'}),$$

其中，$s' = sx_{ID} - \dfrac{\alpha x_{ID}}{K(\tilde{m})}$。$B$ 将 $\sigma = (V, R_1, R_2)$ 返回给敌手 A_{II}，A_{II} 验证签名的正确性。

$$\begin{aligned}
V &= (pk_3)^{rF(\tilde{u})} g_1^{-\frac{x_{ID}L(\tilde{m})}{K(\tilde{m})}} (m' \prod_{j \in M} m_j)^{sx_{ID}} \\
&= (g_2^{x_{ID}})^{rF(\tilde{u})} g_1^{-\frac{x_{ID}L(\tilde{m})}{K(\tilde{m})}} (m' \prod_{j \in M} m_j)^{sx_{ID}} \\
&= (g_2^{x_{ID}})^{rF(\tilde{u})} g_1^{-\frac{x_{ID}L(\tilde{m})}{K(\tilde{m})}} (g_2^{K(\tilde{m})} g^{L(\tilde{m})})^{sx_{ID}} \\
&= (g_2^{x_{ID}})^{rF(\tilde{u})} g_1^{-\frac{x_{ID}L(\tilde{m})}{K(\tilde{m})}} (g_2^{K(\tilde{m})} g^{L(\tilde{m})})^{\frac{\alpha x_{ID}}{K(\tilde{m})}} (g_2^{K(\tilde{m})} g^{L(\tilde{m})})^{sx_{ID} - \frac{\alpha x_{ID}}{K(\tilde{m})}} \\
&= (g_2^{x_{ID}})^{rF(\tilde{u})} g^{-\frac{\alpha x_{ID} L(\tilde{m})}{K(\tilde{m})}} g_2^{\alpha x_{ID}} g^{\frac{\alpha x_{ID} L(\tilde{m})}{K(\tilde{m})}} (g_2^{K(\tilde{m})} g^{L(\tilde{m})})^{sx_{ID} - \frac{\alpha x_{ID}}{K(\tilde{m})}} \\
&= (g_2^{x_{ID}})^{rF(\tilde{u})} g_2^{\alpha x_{ID}} (g_2^{K(\tilde{m})} g^{L(\tilde{m})})^{s'} \\
&= (g_2^{\alpha + rF(\tilde{u})})^{x_{ID}} (m' \prod_{j \in M} m_j)^{s'}
\end{aligned}$$

$R_2 = g^{sx_{ID}} g_1^{-\frac{1}{K(\tilde{m})}} = g^{sx_{ID} - \frac{\alpha x_{ID}}{K(\tilde{m})}} = g^{s'}$。对敌手 A_{II} 来说，B 生成的签名与真正的挑战者产生的签名是不可区分的。

若 $K(\tilde{m}) = 0 \bmod l_m$，模拟过程终止，$B$ 失败退出。

3) 伪造阶段：若算法 B 在上述询问中没有失败退出，则敌手 A_{II} 至少以概率 ε 成功伪造用户 ID^* 对消息 m^* 的有效签名 $\sigma^* = (V^*, R_1^*, R_2^*)$。其中 $V^* = g_2^{\alpha x_{ID}^*} g_2^{r^* F(\tilde{u}^*) x_{ID}^*} (m' \prod_{j \in M} m_j)^{s^*}$，$R_1^* = (pk_1^*)^{r^*}$，$R_2^* = g^{s^*}$。

若 $F(\tilde{u}^*) \neq 0 \bmod q$ 或者 $K(\tilde{m}^*) \neq 0 \bmod q$，$B$ 终止。否则，B 计算 $\dfrac{V^*}{(R_2^*)^{L(\tilde{m}^*)}} = \dfrac{g_2^{\alpha x_{ID}^*} g_2^{rF(\tilde{u}^*) x_{ID}^*} (m' \prod_{j \in M} m_j)^{s^*}}{(g^{s^*})^{L(\tilde{m}^*)}} = \dfrac{g_2^{\alpha x_{ID}^*} (g_2^{K(\tilde{m}^*)} g^{L(\tilde{m}^*)})^{s^*}}{(g^{s^*})^{L(\tilde{m}^*)}} = g_2^{\alpha x_{ID}^*} = g^{abx_{ID}^*}$。

算法 B 输出 $g^{abx_{ID}^*}$ 作为 Many-DH 问题的解。

4) 概率计算：若算法 B 在模拟过程中没有终止，则必须满足以下几个条件。

① 签名询问成功，若 $ID \neq ID^*$，则 $F(\tilde{u}) \neq 0 \bmod l_u$ 或 $K(\tilde{m}) \neq 0 \bmod l_m$；若 $ID=ID^*$，则 $K(\tilde{m}) \neq 0 \bmod l_m$。

② 签名伪造成功，则 $F(\tilde{u}^*) = 0 \bmod q$，$K(\tilde{m}^*) = 0 \bmod q$。

设 $\tilde{u}_1, \cdots, \tilde{u}_{q_I}$ 为秘密值询问或者签名询问中出现的所有用户身份的散列函数 H_u 的输出值(不包括目标身份 ID^*)，$\tilde{m}_1, \cdots, \tilde{m}_{q_M}$ 为签名询问中出现的所有消息 m 的散列函数 H_m 的输出值。显然有 $q_I < q_k + q_s$，$q_M < q_s$ 成立。为了计算方便，定义 4 个事件 A_i、A^*、B_j、B^* 如下

$A_i : F(\tilde{u}_i) \neq 0 \bmod l_u$，其中，$i = 1, \cdots, q_I$，$A^* : F(\tilde{u}^*) = 0 \bmod q$

$B_j : K(\tilde{m}_j) \neq 0 \bmod l_m$，其中，$j = 1, \cdots, q_M$，$B^* : K(\tilde{m}^*) = 0 \bmod q$

则算法 B 模拟成功的概率 $\Pr[\neg abort] \geqslant \Pr[(\wedge_{i=1}^{q_I} A_i \wedge A^*) \wedge (\wedge_{j=1}^{q_M} B_j \wedge B^*)]$，其中事件 $(\wedge_{i=1}^{q_I} A_i \wedge A^*)$ 和事件 $(\wedge_{j=1}^{q_M} B_j \wedge B^*)$ 是相互独立的。

由假设 $l_u(n_u+1) < q$ 知，如果 $F(\tilde{u}) = 0 \bmod q$ 成立，那么 $F(\tilde{u}) = 0 \bmod l_u$ 也成立。进一步推出若 $F(\tilde{u}) = 0 \bmod l_u$，则存在唯一的 k_u 使 $F(\tilde{u}) = 0 \bmod q$ 成立，其中，$0 \leqslant k_u \leqslant n_u$。从而有：$\Pr[A^*] = \Pr[F(\tilde{u}^*) = 0 \bmod q \wedge F(\tilde{u}^*) = 0 \bmod l_u] = \Pr(F(\tilde{u}^*) = 0 \bmod l_u)$；

$\Pr[F(\tilde{u}^*)=0 \bmod q \mid F(\tilde{u}^*)=0 \bmod l_u]=\frac{1}{l_u}\frac{1}{n_u+1}$。

另一方面，$\Pr[\wedge_{i=1}^{q_I} A_i]=1-\Pr[\vee_{i=1}^{q_I}\neg A_i] \geqslant 1-\sum_{i=1}^{q_I}\Pr[\neg A_i]=1-\frac{q_I}{l_u}$。

由于事件 A_i 和 A^* 是相互独立的，所以有

$$\begin{aligned}\Pr[(\wedge_{i=1}^{q_I} A_i \wedge A^*)] &= \Pr[\wedge_{i=1}^{q_I} A_i]\Pr[A^*] \\ &= (1-\frac{q_I}{l_u})\frac{1}{(n_u+1)\ l_u} \geqslant (1-\frac{q_e+q_s}{l_u})\frac{1}{(n_u+1)\ l_u} \\ &= \frac{1}{2(q_e+q_s)(n_u+1)}(1-\frac{q_e+q_s}{2(q_e+q_s)}) \\ &= \frac{1}{4(q_e+q_s)(n_u+1)}\end{aligned}$$

其中，$l_u=2(q_e+q_s)$。

同理 $\Pr(\wedge_{j=1}^{q_M} B_j \wedge B^*)=\frac{1}{4q_s(n_m+1)}$，则 $\Pr[\neg abort] \geqslant \Pr[(\wedge_{i=1}^{q_I} A_i \wedge A^*)\wedge(\wedge_{j=1}^{q_M} B_j \wedge B^*)] \geqslant \frac{1}{16q_s(q_k+q_s)(n_u+1)(n_m+1)}$。

如果模拟没有终止，则敌手 A_{II} 至少以概率 ε 成功伪造一个有效签名。同时 B 还要猜测敌手 A_{II} 准备伪造签名的用户身份 ID，并设置该用户的公钥作为 Many-DH 问题的输入，则 B 猜测用户身份成功的概率是 $\frac{1}{q_k}$。

因此算法 B 成功解决 Many-DH 问题的概率 $\varepsilon' \geqslant \frac{\varepsilon}{16q_s(q_k+q_s)(n_u+1)(n_m+1)q_k}$。

6　效率分析

将本文中的方案与文献[19]和文献[20]中的方案相比较，通过计算代价和通信代价两方面来评价方案的性能。由于 $e(g_2, pk_2)$ 可进行预计算，所以在计算验证算法计算代价时，省去该部分计算量。表 1 中符号 E、M、BP、$|G|$、n_u、n_m 定义如下：符号 E 表示群指数运算，M 表示群中元素的点乘运算，BP 表示双线性对运算，$|G|$ 表示群中元素的长度，n_u 表示用户身份 ID 的字符串长度，n_m 表示消息 m 的字符串长度。由表 1 可以看出，与文献[19]和文献[20]中的方案相比，本文的方案在签名算法需要较少的点乘运算和指数运算，在验证算法中点乘运算和双线性对运算的数目也是最少的，因而计算代价最低。而且本文方案的签名长度也比文献[20]方案短，因而计算代价较低。

表 1　标准模型下无证书签名方案的效率分析

方案	签名算法	验证算法	签名长度
文献[19]方案	$(\frac{n_u+n_m}{2}+3)M+6E$	$(\frac{n_u+n_m}{2})M+6BP$	$3\|G\|$
文献[20]方案	$(\frac{n_u}{2}+4)M+7E$	$(\frac{n_u+1}{2})M+E+5BP$	$4\|G\|$
本文方案	$(\frac{n_m}{2}+1)M+4E$	$(\frac{n_m}{2})M+E+3BP$	$3\|G\|$

7　结束语

本文提出了一种新的标准模型下安全的无证书签名方案，方案的安全性可规约为 NGBDH 和 Many-DH 困难问题。由于在安全模型中刻画了密钥替换攻击，所以提出方案能够抵抗密钥替换攻击。该方案在签名验证过程中只需要 3 个双线性对运算，签名长度仅需要 3 个群中元素的长度。与同类标准模型下的方案相比，提出方案的计算效率和通信效率有所提高，根据 MIRACL[22]的结果，与模指数运算相比，双线性对运算依然是很耗时的密码运算。这种耗时的双线性对运算影响了它的广泛应用，尤其是在计算受限的无线传感器网络。

参考文献：

[1] SHAMIR A. Identity-based cryptosystems and signature schemes[A]. Proceedings of the Crypto'84[C]. Santa Barbara, California, USA, 1984. 47-53.

[2] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[A]. Proceedings of the Asiacrypt'2003[C]. Taibei, China, 2003. 452-473.

[3] YUM D H, LEE P J. Generic construction of certificateless signature [A]. Proceedings of the ACISP'2004[C]. Sydney, Australia, 2004. 200-211.

[4] HU B C, WONG D S, ZHANG Z F, *et al*. Key replacement attack against a generic construction of certificateless signature[A]. Proceedings of the ACISP'2006[C]. Melbourne, Australia, 2006. 235- 246.

[5] HUANG X Y, SUSILO W, MU Y, *et al.* On the security of certificateless signature schemes from asiacrypt 2003[A]. Proceedings of the CANS'2005[C]. Xiamen, China, 2005.13-25.

[6] GORANTLA M C, SAXENA A. An efficient certificateless signature scheme[A]. Proceedings of the CIS'2005[C]. Xi'an, China, 2005. 110-116.

[7] YAP W S, HENG S H, GOI B M. An efficient certificateless signature scheme[A]. Proceedings of the EUC'2006 Workshops[C]. Seoul, Korea, 2006. 322-331.

[8] LI J G, HUANG X Y, MU Y, *et al*. Cryptanalysis and improvement of

an efficient certificateless signature scheme[J]. Journal of Communications and Networks, 2008, 10(1): 10-17.

[9] DU H Z, WEN Q Y. Efficient and provably-secure certificateless short signature scheme from bilinear pairings [EB/OL]. http://eprint.iacr.org/2007/250, 2007.

[10] CHOI K Y, PARK J H, HWANG J Y, *et al*. Efficient certificateless signature schemes[A]. Proceedings of the ACNS'2007[C]. Zhuhai, China, 2007. 443-458.

[11] HUANG X Y, MU Y, SULILO W, *et al*. Certificateless signature revisited [A]. Proceedings of the ACISP'2007[C]. Townsville, Australia, 2007.308-322.

[12] TSO R, YI X, HUANG X Y. Efficient and short certificateless signature [A]. Proceedings of the CANS'2008[C]. Hong-Kong, China, 2008. 64-79.

[13] HARN L, REN J, LIN C L. Design of DL-based certificateless signature schemes[J]. Journal of Systems and Software, 2009, 82(5): 789-793.

[14] TIAN M M, HUANG L S. Cyrptanalysis of a certificateless signature scheme without pairing[J]. International Journal of Communication Systems, 2012, 25(11):1432-1442.

[15] 张福泰, 孙银霞, 张磊等. 无证书公钥密码体制研究[J]. 软件学报, 2011, 22(6): 1316-1332.
ZHANG F T, SUN Y X, ZHANG L, *et al*. Research on certificateless public key cryptography[J]. Journal of Software, 2011, 22(6): 1316-1332.

[16] 王圣宝, 刘文浩, 谢琪. 无双线性配对的无证书签名方案[J]. 通信学报, 2012, 33(4): 93-98.
WANG S B, LIU W H, XIE Q. Certificateless signature scheme without bilinear pairings[J]. Journal on Communications, 2012, 33(4): 93-98.

[17] 王亚飞, 张睿哲. 强安全无对的无证书签名方案[J]. 通信学报, 2013, 34(2): 94-99.
WANG Y F, ZHANG R Z. Strongly secure certificateless signature scheme without bilinear pairings[J]. Journal on Communications, 2013, 34(2): 94-99.

[18] BELLARE M, BOLDYREVA A, PALACIO A. A uninstantiable random oracle-model scheme for a hybrid-encryption problem[A]. Proceedings of the Eurocrypt'2004[C]. Interlaken, Switzerland, 2004. 171-188

[19] LIU J K, AU M H, SUSILO W. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model[A]. Proceedings of the ASIACCS'2007[C]. New York, USA, 2007. 273-283.

[20] YU Y, MU Y, WANG G, *et al*. Improved certificateless signature scheme provably secure in the standard model[J]. IET Information Security, 2012, 6(2): 102-110.

[21] 李继国, 姜平进. 标准模型下可证安全的基于身份的高效的签名方案[J]. 计算机学报, 2009, 32(11): 2130-2136.
LI J G, JIANG P J. An efficient provably secure identity-based signature scheme in the standard model[J]. Chinese Journal of Computers, 2009, 32(11): 2130-2136.

[22] MIRACL. Multiprecision integer and rational arithmetic C/C++ library [EB/OL]. http://indigo.ie/~mscott.

作者简介：

李艳琼（1987-），女，河南商丘人，河海大学硕士生，主要研究方向为密码学理论与技术。

李继国（1970-），男，黑龙江富裕人，博士，河海大学教授、博士生导师，主要研究方向为信息安全、密码学理论与技术、云计算安全等。

张亦辰（1971-），女，黑龙江齐齐哈尔人，河海大学博士生，主要研究方向为密码学理论与技术。