doi:10.11959/j.issn.1000-436x.2015136

对一个格基身份签名方案的分析和改进

杨春丽[1,2]，闫建华[1,2,3]，郑世慧[1,2]，王励成[1,2]，杨榆[1,2]
（1. 北京邮电大学 信息安全中心，北京 100876；2. 北京邮电大学 灾备技术国家工程实验室，北京 100876；
3. 鲁东大学 信息与电气工程学院，山东 烟台 264025）

摘 要：首先分析了 Liu 等人 2013 年给出的一个格基身份签名（IBS）方案在安全性证明中存在的问题，进而说明方案的证明达不到作者所宣称的选择身份和自适应选择消息攻击下的强不可伪造性。其次，使用 Boyen10 签名技术（PKC 2010）对此方案中签名算法进行改进，并在标准模型下证明了改进方案在选择身份和自适应选择消息攻击下具有强不可伪造性的安全性质。另外，对比分析了改进的方案和其他 IBS 方案的效率和安全性。
关键词：基于身份的签名；强不可伪造；标准模型；格
中图分类号：TP309 **文献标识码**：A

Analysis and improvement of an identity-based signature scheme from lattices

YANG Chun-li[1,2], YAN Jian-hua[1,2,3], ZHENG Shi-hui[1,2], WANG Li-cheng[1,2], YANG Yu[1,2]
(1.Information Security Research Center, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China;
3. School of Information and Electric Engineering, Ludong University, Yantai 264025, China)

Abstract: Liu *et al* proposed an identity-based signature from lattices in 2013, and proved that it can achieve strong unforgeability in the standard model. Through analysis, the security proof of this scheme has some defect, and then show that the scheme cannot prove the strong unforgeability under selective identity and adaptive chosen-message attacks. Then, using Boyen signing technique (PKC 2010) inpoves the signing algorithm, and proves the strong unforgeability under selective identity and adaptive chosen-message attacks (SU-sID-CMA) in the standard model. In addition, it compares the efficiency and security of the scheme and the other identity-based signatures from lattices.
Key words: identity-based signature; strong unforgeability; standard model; lattices

1 引言

为了克服传统公钥密码体制中身份和公钥绑定的问题，Shamir 在 1985 年首次提出基于身份的密码体制(IBC, identity based cryptography)的概念[1]。在基于身份的密码体制中，用户的公钥是所对应身份的身份串，如 E-mail 地址等。双线性对提出以后，2001 年，Boneh 和 Franklin 基于双线性对给出第一个基于身份的加密体制（IBE）[2]。从此，学者们提出了大量基于身份的加密和签名体制。2005 年，Waters 首次提出一个标准模型下安全的基于身份的加密方案[3]。2006 年，Paterson 等人在 Waters 方案[3]的基础上给出一个标准模型下基于身份的签名（IBS）方案[4]。

然而，随着量子计算的飞速发展，尤其是 1997 年 Shor 提出了一个能够在多项式时间内求解大整

收稿日期：2014-07-01；**修回日期**：2014-10-25
基金项目：国家自然科学基金资助项目(61121061, 61202082, 61370194)；国家自然科学基金中日韩 A3 前瞻计划基金资助项目(61161140320)；中央高校基本科研业务费专项基金资助项目(BUPT2012RC0219, BUPT2013RC0311, BUPT2013RC0308)
Foundation Items: The National Natural Science Foundation of China (61121061, 61202082, 61370194)；The NSFC A3 Foresight Program (61161140320); The Fundamental Research Funds for the Central Universities (BUPT2012RC0219, BUPT2013RC0311, BUPT2013RC0308)

数素分解的算法[5] 。该算法使现有的基于大整数分解问题和椭圆曲线上离散对数问题的密码系统受到一定的威胁，进而基于双线性对上的以上基于身份的密码体制也受到一定的冲击。寻求可以抵抗量子攻击的密码体制（后量子密码）成为现在研究的一个热点和焦点。

幸运的是，基于格的密码体制正好是这样的一种密码系统。同时，它具有另外一些优点：基于格的密码体制的安全性可以规约为平均情况下的格困难问题，Ajtai 已经从理论上证明了格困难问题在最坏情况和平均情况的困难性等价[6]。另外，基于格的密码体制中主要使用有限域上的加和乘线性运算, 无需使用指数运算、对数运算等复杂的运算，计算复杂度较低。近年来，基于格中带错误学习问题（LWE）和小整数解问题（SIS）2 类困难问题，各种密码体制也有了飞速的发展。例如，公钥加密体制[7,8]、数字签名体制[9,10]、基于身份的加密体制[11,12]和全同态加密体制[13,14]等。

在数字签名体制的构造中，人们尽力去寻求能在标准模型下达到强不可伪造安全性质的签名方案。这是由于具有强不可伪造性和标准模型下安全的密码体制更安全[15]。自从 2008 年 Gentry 等人提出原像取样算法[9]以后，学者们使用这一主要技术又给出了很多的格基签名方案。大致可以归结为 2 类，第 1 类是以达到实用高效为目的，这类方案的安全性是在随机预言机模型下证明的，如 Lyu12 签名[16]和 DDLL13[17]签名；第 2 类是以在标准模型下达到安全性且高效为目的，主要以 Boyen10 签名方案[10]和 CHKP12 签名[11] 为代表。随着格基签名算法的提出，基于身份的格基签名方案也陆续有了新的进展。2010 年 Rückert 首次给出一个可以达到强不可伪造性的带层次基于身份的格基签名（HIBS）方案[18]，其主要使用盆景树思想[11]和原像取样算法。后来，Xia 等使用基扩展技术[12]和原像取样算法[9]给出一个不带层次的格基签名方案[19]，并在随机预言机模型下证明了可以达到强不可伪造性。另外，Tian 等人[20]在 2014 年也给出一个高效的格基签名方案，其使用无陷门格基签名方案[16]，因此效率较高，唯一遗憾的是在随机预言机模型下证明安全的。另外，学者还给出了其他带层次基于身份的格基签名方案，如文献[21]。

2013 年，Liu 等人借鉴文献[12]中 IBE 的思想提出一个更高效的 IBS 方案[22]，证明了其方案的安全性并与文献[18]进行了效率对比。但此方案在安全性证明中存在一定的问题，进而说明方案没有证明到作者所称的安全性。本文使用文献[10]中的签名技术对 Liu 等人方案[22]的签名算法进行了改进，给出一个新的 IBS 方案，并基于 SIS 问题假设在标准模型下证明了此方案能达到选择身份和自适应选择消息攻击下的强不可伪造性（SU-sID-CMA）。另外，对新改进的方案和其他 IBS 方案进行了效率和安全性的对比。

2　预备知识

2.1　格定义及 SIS 问题

定义 1[23]（格的定义）令 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$ 是 n 个线性独立的向量，每个 $\boldsymbol{b}_i\in\mathbb{R}^m$。则 n 个向量 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$ 的整线性组合构成 $\mathbb{R}^m$ 上的一个格。具体来说，

$$L(\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n)=\left\{\sum_{i=1}^{n}\boldsymbol{x}_i\boldsymbol{b}_i:\boldsymbol{x}_i\in\mathbb{Z}\right\}$$

这里，向量组 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$ 构成格的一组基，n 和 m 分别称为格的秩和维数。

格密码中一般使用 2 类特殊定义在 $\mathbb{Z}_q$ 上的满秩整数格。使用矩阵的形式描述如下。

定义 2[23]（q 元格） 给定矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，向量 $y\in\mathbb{Z}_q^n$，其中，n,m,q 为给定的相关参数，定义

$$\Lambda_q^{\perp}(\boldsymbol{A})=\left\{v\in\mathbb{Z}_q^m\mid\boldsymbol{A}v=0(\bmod q)\right\}$$

$$\Lambda_q^{y}(\boldsymbol{A})=\left\{v\in\mathbb{Z}_q^m\mid\boldsymbol{A}v=y(\bmod q)\right\}$$

即所有与矩阵 $\boldsymbol{A}$ 的行向量模 q 正交的向量构成格 $\Lambda_q^{\perp}(\boldsymbol{A})$。而 $\Lambda_q^{y}(\boldsymbol{A})$ 则由向量 y 所在的格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的陪集中向量构成。

以 $\Lambda_q^{\perp}(\boldsymbol{A})$ 为例简单介绍一下格上离散高斯分布的基本概念和基本结论。

定义 3[24]（离散高斯分布）首先给出 $\mathbb{R}^m$ 上以 $s>0$ 为参数，$c\in\mathbb{R}^m$ 为中心的高斯函数：$\rho_{s,c}(x)=\exp(-\pi\|x-c\|^2/s^2)$。从而对于任意 $x\in\Lambda_q^{\perp}(\boldsymbol{A})$，$\Lambda_q^{\perp}(\boldsymbol{A})$ 上的离散高斯分布定义为

$$D_{\Lambda_q^{\perp}(\boldsymbol{A}),s,c}(x)=\frac{\rho_{s,c}(x)}{\rho_{s,c}(\Lambda_q^{\perp}(A))}$$

其中，$\rho_{s,c}(\Lambda_q^{\perp}(\boldsymbol{A}))=\sum_{x\in\Lambda_q^{\perp}(\boldsymbol{A})}\rho_{s,c}(x)$。

格上的困难问题主要有最短向量问题（SVP）、最近向量问题（CVP）、最短独立向量问题（SIVP）

等。另外，大部分加密方案的安全性基于错误学习（LWE）问题，以及大部分签名方案的安全性基于小整数解（SIS）问题。本文主要用到小整数解问题，以下给出详细的定义。

定义 4[24]（SIS 问题）给定一个整数 q，一个随机的矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和一个实数 β。小整数解 $\left(\mathrm{SIS}_{q,n,m,\beta}\right)$ 问题的目的是找到一个非零向量 e，使得 $\boldsymbol{A}e=0(\bmod q)$ 且 $\|e\|\leqslant\beta$。

定理 1[24]（SIS 问题的困难性）对任意的 $m(n)=\Theta(n\log n)$，存在一个 $q(n)=O(n^2\log n)$ 使得对任意函数 $\gamma(n)=\omega(n\log n)$，以不可忽略的概率解决平均情况的 $\mathrm{SIS}_{q,n,m,\beta}$ 问题至少和解决最坏情况的 SIVP_γ 一样困难。

2.2 常用算法

引理 1[25]（陷门生成算法）令 $q\geqslant 3$ 是一个奇数，$m=\lceil 6n\log q\rceil$。存在一个概率多项式时间算法 $\mathrm{TrapGen}(q,n)$ 输出矩阵对 $(\boldsymbol{A},T_A)\in\mathbb{Z}_q^{n\times m}\times\mathbb{Z}^{m\times m}$，其中 $\boldsymbol{A}$ 的分布和 $\mathbb{Z}_q^{n\times m}$ 上的均匀分布统计接近，T_A 是 q-ary 格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的一组短基，同时以很大的概率满足 $\|\tilde{T}_A\|\leqslant O\left(\sqrt{n\log q}\right)$ 和 $\|T_A\|\leqslant O(n\log q)$。

引理 2[9]（离散高斯取样和原像取样）令 $q\geqslant 2$，$\boldsymbol{A}$ 是 $\mathbb{Z}_q^{n\times m}\ (m>n)$ 上的一个随机矩阵，T_A 是 q-ary 格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的一组短基，$\sigma\geqslant\|\tilde{T}_A\|\omega\left(\sqrt{\log m}\right)$，则对任意 $\boldsymbol{u}\in\mathbb{Z}_q^n$，有

1) $\Pr[\boldsymbol{x}\leftarrow D_{\Lambda_q^{\boldsymbol{u}}(A),\sigma}:\|\boldsymbol{x}\|>\sigma\sqrt{m}]\leqslant negl(n)$；

2) 存在一个概率多项式时间算法 $\mathrm{SamplePre}\left(\boldsymbol{A},T_A,\boldsymbol{u},\sigma\right)$ 输出一个向量 $\boldsymbol{x}\in\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A})$，其分布和离散高斯分布 $D_{\Lambda_q^{\boldsymbol{u}}(A),\sigma}$ 统计接近。

引理 3[12,22]（右基取样）令 $q\geqslant 2$，$m>n$，$\sigma\geqslant\|\tilde{T}_B\|s_R\omega\left(\sqrt{\log m}\right)$。存在一个多项式时间算法 $\mathrm{SampleRight}\left(\boldsymbol{A},\boldsymbol{B},\boldsymbol{R},T_B,\boldsymbol{u},\sigma\right)$，其输入是矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times k}$，一个秩为 n 的矩阵 $\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$，一个矩阵 $\boldsymbol{R}\in\mathbb{Z}^{k\times m}$ 和格 $\Lambda_q^{\perp}(\boldsymbol{B})$ 的一组短基 T_B，输出一个向量 $\boldsymbol{e}\in\mathbb{Z}^{m+k}$，其分布服从离散高斯分布 $D_{\Lambda_q^{\boldsymbol{u}}(F_2),\sigma}$。其中，$F_2=\boldsymbol{A}|(\boldsymbol{AR}+\boldsymbol{B})$ 且 $s_R=\sup_{\|x\|=1}\|\boldsymbol{Rx}\|$。

引理 4[12,22]（左基取样）存在一个多项式时间算法 $\mathrm{SampleBasisLeft}(\boldsymbol{A},\boldsymbol{M},T_A,0,\sigma)$，其输入是一个矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m_1}$，一个矩阵 $\boldsymbol{M}\in\mathbb{Z}_q^{n\times m_2}$，格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的一组短基 T_A，输出格 $\Lambda_q^{\perp}(F_1)$ 的一组短基 T_{F_1}。其中，$F_2=\boldsymbol{A}|\boldsymbol{M}$，$\sigma\geqslant\|\tilde{T}_A\|\omega\left(\sqrt{\log(m_1+m_2)}\right)$ 且 $\|\tilde{T}_{F_1}\|=\|\tilde{T}_A\|$。

引理 5[12,22]（右基取样）存在一个多项式时间算法 $\mathrm{SampleBasisRight}(\boldsymbol{A},\boldsymbol{B},\boldsymbol{R},T_B,0,\sigma)$，其输入矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times k}$，$\boldsymbol{M}\in\mathbb{Z}_q^{n\times m}$，$\boldsymbol{R}\in\{-1,1\}^{k\times m}$，格 $\Lambda_q^{\perp}(\boldsymbol{B})$ 的一组短基 T_B，输出格 $\Lambda_q^{\perp}(F_2)$ 的一组短基 T_{F_2}。其中，$F_2=\boldsymbol{A}|(\boldsymbol{AR}+\boldsymbol{B})$，$\sigma\geqslant\|\tilde{T}_B\|s_R\omega\left(\sqrt{\log m}\right)$ 且 $\|\tilde{T}_{F_2}\|\leqslant\|\tilde{T}_B\|(s_R+1)$。

2.3 基于身份的签名方案及安全性定义模型

基于身份的签名(IBS)方案一般由以下 4 个算法组成[4]。

参数设置(Setup)：输入一个安全参数 n，PKG 以此来产生它的系统公共参数 *PP* 和主私钥 *MSK*，然后将系统公共参数 *PP* 公开，秘密保留主密钥 *MSK*。

私钥提取(Extract)：给定用户身份 *id*，PKG 利用系统公共参数 *PP* 和主密钥 *MSK*，产生身份 *id* 所对应的私钥 SK_{id}，并通过安全信道发送给用户。

签名(Sign)：用户得到私钥 SK_{id}，验证密钥是否由 PKG 产生。若验证通过，则用户利用其身份 *id*、私钥 SK_{id}、PKG 的系统公共参数 *PP* 对消息 μ 进行签名，得到签名 σ。

验证(Verify)：验证者利用 PKG 的系统公共参数 *PP* 和用户身份 *id* 验证签名 σ 的有效性。

通过挑战者 $\mathcal{C}$ 与攻击者 $\mathcal{A}$ 之间的交互游戏来定义选择身份和自适应选择消息攻击下的强不可伪造性（SU-sID-CMA），具体包括如下步骤。

初始化（Initialization）：攻击者 $\mathcal{A}$ 输出他将要挑战的目标身份 id^*。

参数设置(Setup)：挑战者 $\mathcal{C}$ 运行参数设置算法得到系统参数 *PP* 和主私钥 *MSK*，同时公开系统参数 *PP*，将主私钥 *MSK* 自己保密。

私钥提取查询(Extract Queries)：攻击者 $\mathcal{A}$ 可以询问除目标身份 id^* 外的任何身份 *id* 的私钥。挑战者 $\mathcal{C}$ 运行私钥提取算法来进行响应，并将私钥 SK_{id} 发送给攻击者 $\mathcal{A}$。

签名询问(Sign Queries)：攻击者 $\mathcal{A}$ 可以询问任何身份 *id* 对任何消息 μ 的签名。挑战者 $\mathcal{C}$ 首先

通过运行私钥提取算法获得身份 id 的私钥，然后通过运行签名算法来得到签名 σ，并将其发送给攻击者 $\mathcal{A}$。

伪造(Forgery)：攻击者 $\mathcal{A}$ 输出对消息 μ^* 在身份 id^* 下的签名 σ^*。若以下条件成立，则攻击者 $\mathcal{A}$ 攻击成功。

1) 签名（id^*,μ^*,σ^*）能通过验证算法；

2) 攻击者 $\mathcal{A}$ 未对身份 id^* 进行过私钥提取查询；

3) （id^*,μ^*,σ^*）不属于已有签名查询列表，即攻击者 $\mathcal{A}$ 之前未对消息 μ^* 在身份 id^* 下进行签名询问得到签名值 σ^*。

以上游戏中攻击者 $\mathcal{A}$ 的优势定义为 $\mathrm{Adv}_{\mathcal{A}}=\Pr[\mathcal{A}\text{ 成功}]$。

定义 5　如果攻击者 $\mathcal{A}$ 最多运行 t 时间，最多进行了 q_e 次私钥提取查询问和 q_s 次签名询问，以不小于 ε 的优势赢得上述游戏，则称攻击者 $\mathcal{A}$ 是基于身份签名方案的 (ε,t,q_e,q_s) 伪造者。若在基于身份的签名方案中不存在 (ε,t,q_e,q_s) 伪造者，则称方案是 (ε,t,q_e,q_s) 安全的。

3　Liu 等人方案回顾和分析

3.1　Liu 等人方案

Liu 等方案[22]主要借鉴文献[12]的思想，使用了 2 次双陷门的思想。具体方案如下。

参数建立（λ）：输入安全参数 λ，并设置参数 n,m,q,s 为安全参数 λ 的函数。再执行如下操作。

1) 使用算法 TrapGen 生成矩阵对 $(\boldsymbol{A}_0,T_{A_0})\in \mathbb{Z}_q^{n\times m}\times\mathbb{Z}^{m\times m}$，其中，$T_{A_0}$ 是 q-ary 格 $\Lambda_q^{\perp}(A_0)$ 的一组短基，且 $\|\tilde{T}_{A_0}\|\leqslant O\left(\sqrt{n\log q}\right)$。

2) 均匀随机地选择矩阵 $\boldsymbol{A}_1,\boldsymbol{A}_2,\boldsymbol{B},\boldsymbol{C}\leftarrow\mathbb{Z}_q^{n\times m}$ 和一个 n 维向量 $\boldsymbol{u}\leftarrow\mathbb{Z}_q^n$。

3) 定义 $H:\mathbb{Z}_q^n\to\mathbb{Z}_q^{n\times n}$ 为满秩差分映射，这里将 H 看成安全的散列函数。

4) 输出公共参数 $PP=\left(\boldsymbol{A}_0,\boldsymbol{A}_1,\boldsymbol{A}_2,\boldsymbol{B},\boldsymbol{C},\boldsymbol{u},H\right)$ 和主私钥 $MSK=\left(T_{A_0}\right)$。

私钥提取（PP,MSK,id）：输入公共参数 PP、主私钥 MSK 和身份 id。进行如下算法操作。

$T_{id}\leftarrow\mathrm{SampleBasisLeft}\left(\boldsymbol{A}_0,\boldsymbol{A}_1+H(id)\boldsymbol{B},T_{A_0},0,s\right)$，和 $SK_{id}\leftarrow\mathrm{RandBasis}\left(T_{id},s\right)$。最后输出身份 id 所对应的私钥 SK_{id}。

签名（PP,μ,SK_{id}）：输入公共参数 PP、消息 μ 和身份 id 所对应的私钥 SK_{id}。签名者选择一个随机数 $r\in\mathbb{Z}_q$，并执行算法

$\varphi\leftarrow\mathrm{SampleLeft}\left(\boldsymbol{F}_{id},\boldsymbol{A}_2+H(\mu,r)\boldsymbol{C},SK_{id},\boldsymbol{u},s\right)$，其中，$\boldsymbol{F}_{id}=\left(\boldsymbol{A}_0\|\boldsymbol{A}_1+H(id)\boldsymbol{B}\right)$。最后输出消息 μ 的签名 $\sigma=(\varphi,r)$。

验证（PP,σ,id,m）：输入公共参数 PP、消息 μ 在身份 id 下的签名 σ，验证者接收签名 σ 当且仅当 $0<\|\sigma\|\leqslant s\sqrt{3m}$ 和 $\boldsymbol{F}_{id,m,r}\sigma=\boldsymbol{u}$ 同时成立，其中 $\boldsymbol{F}_{id,\mu,r}=\boldsymbol{F}_{id}\|\boldsymbol{A}_2+H(\mu,r)\boldsymbol{C}=\boldsymbol{A}_0\|\boldsymbol{A}_1+H(id)\|\boldsymbol{A}_2+H(\mu,r)\boldsymbol{C}$。

3.2　安全性证明分析

文献[22]的定理 3 中证明了以上 IBS 方案能达到选择身份和自适应选择消息攻击下的强不可伪造性。在其证明过程中的伪造阶段，敌手输出对身份 id^* 的有效签名 (μ^*,φ^*,r^*)，如果在签名查询中已经存在身份 id^* 对消息 μ^* 的签名 (μ^*,φ',r^*)（即强不可伪造），则根据 (μ^*,φ^*,r^*) 和 (μ^*,φ',r^*) 是有效签名，得 $\boldsymbol{F}_{id^*,\mu^*,r^*}\varphi^*=\boldsymbol{u}$ 和 $F_{id^*,\mu^*,r^*}\varphi'=\boldsymbol{u}$。这样最后输出 $v=\varphi^*-\varphi'$ 作为 SIS 问题的解。

事实上，在证明的初始化阶段作者并没有给出 SIS 实例矩阵，而在伪造阶段宣称找到难题 SIS 实例的解。这样导致最直接的想法是 SIS 实例矩阵为 $\boldsymbol{F}_{id^*,\mu^*,r^*}$，而 $\boldsymbol{F}_{id^*,\mu^*,r^*}=(\boldsymbol{A}_0\|\boldsymbol{A}_0\boldsymbol{R})\|\left((\boldsymbol{A}_0\|\boldsymbol{A}_0\boldsymbol{R})\boldsymbol{R}'+\left(H(\mu^*,r^*)-H(id^*)\right)\boldsymbol{C}\right)$。实例矩阵要求必需是一个固定的矩阵，而 $\boldsymbol{F}_{id^*,\mu^*,r^*}$ 的表达式中包含有随机数 r^* 和随机选择的消息 μ^*，这样导致 $\boldsymbol{F}_{id^*,\mu^*,r^*}$ 不是一个固定的矩阵，故 $\boldsymbol{F}_{id^*,\mu^*,r^*}$ 不能作为 SIS 实例矩阵。

因此，SIS 实例矩阵只能为 $\boldsymbol{A}_0$。由于其安全性证明是在标准模型下证的，因此 H 是系统固定的一个抗碰撞的散列函数，这样，$H(\mu^*,r^*)-H(id^*)\neq 0$。而如果 $\boldsymbol{A}_0$ 为 SIS 实例矩阵，则必须要求 $H\left(\mu^*,r^*\right)-H\left(id^*\right)=0$，这意味着找到散列函数 H 的一对碰撞。也就是说，Liu 等人方案[22]的可证明安全是正确的前提是散列函数找到一对碰撞，而由于找到散列函数碰撞的概率是可忽略的，因此这是不合理的。因此，Liu 等人方案[22]没有真正地找到 SIS 实例矩阵 $\boldsymbol{A}_0$ 的解，进而没有证明到作者所宣称的安全性。

4 改进的方案

鉴于以上问题，本文发现文献[10]中的签名算法可以解决这个问题。以下具体给出改进的方案及安全性证明。

4.1 方案描述

参数建立(1^n)：输入安全参数 n，并设置参数 m,q,d,s_1,s_2 为安全参数 n 的函数，其中，$m\geqslant\lfloor 6n\log q\rfloor$ 为格的维数，q 为模数（一般为素数），d 为消息压缩后的长度，s_1,s_2 为高斯参数。定义 $H:\mathbb{Z}_q^n\to\mathbb{Z}_q^{n\times n}$ 为满秩差分映射，这里将 H 看成安全的散列函数。令 $H':\{0,1\}^*\to\{0,1\}^d$ 是另一个安全的散列函数（如 SHA1 或 SHA2），其目的是在以下方案中首先将消息压缩为一个长度为 d 的二元比特串[注1]。另外，还需要执行如下操作。

1) 使用算法 TrapGen 生成矩阵对 $\left(\boldsymbol{A}_0,T_{A_0}\right)\in\mathbb{Z}_q^{n\times m}\times\mathbb{Z}^{m\times m}$，其中，$T_{A_0}$ 是 q-ary 格 $\Lambda_q^{\perp}(\boldsymbol{A}_0)$ 的一组短基，且 $\left\|\tilde{T}_{A_0}\right\|\leqslant O\left(\sqrt{n\log q}\right)$。

2) 均匀随机地选择矩阵 $\boldsymbol{A}_1,\boldsymbol{B}\leftarrow\mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{C}_i\leftarrow\mathbb{Z}_q^{n\times m}$，其中，$i=0,1,\cdots,d$，再均匀随机地选择一个 n 维向量 $\boldsymbol{u}\leftarrow\mathbb{Z}_q^n$。

3) 输出公共参数 $PP=\left(\boldsymbol{A}_0,\boldsymbol{A}_1,\boldsymbol{B},\boldsymbol{C}_i,\boldsymbol{u},H\right)$ 和主私钥 $MSK=(T_{A_0})$。

私钥提取(PP,MSK,id)：输入公共参数 PP、主私钥 MSK 和身份 id，进行如下算法操作。

$SK_{id}\leftarrow\text{SampleBasisLeft}(\boldsymbol{A}_0,\boldsymbol{A}_1+H(id)\boldsymbol{B},T_{A_0},0,s_1)$，最后输出身份 id 所对应的私钥 SK_{id}。这里令 $\boldsymbol{F}_{id}=\boldsymbol{A}_0\,\|\,\boldsymbol{A}_1+H(id)\boldsymbol{B}$，则 $\boldsymbol{F}_{id}SK_{id}=0(\bmod q)$。

签名(PP,μ,SK_{id})：输入公共参数 PP、任意长度消息 $\mu\in\{0,1\}^*$ 和身份 id 所对应的私钥 SK_{id}。签名者执行如下操作：

1) 计算 $\nu=H'(\mu)\in\{0,1\}^d$；

2) 计算 $\boldsymbol{F}_{id}=\boldsymbol{A}_0\,\|\,\boldsymbol{A}_1+H(id)\boldsymbol{B}$；

3) 计算 $\boldsymbol{C}_\mu=\boldsymbol{C}_0+\sum_{i=1}^{d}(-1)^{\nu[i]}\boldsymbol{C}_i$，其中，$\nu[i]$ 为 ν 的第 i bit；

4) 根据离散高斯分布选择向量 $\sigma_2\leftarrow D_{\mathbb{Z}^m,s_2}$；

5) 执行算法：

$\boldsymbol{\sigma}_1\leftarrow\text{SamplePre}\left(\boldsymbol{F}_{id},SK_{id},u-\boldsymbol{C}_\mu\boldsymbol{\sigma}_2,s_2\right)$；

6) 输出消息 μ 的签名 $\boldsymbol{\sigma}=\begin{pmatrix}\boldsymbol{\sigma}_1\\ \boldsymbol{\sigma}_2\end{pmatrix}$。

验证（$PP,\boldsymbol{\sigma},id,\mu$）：输入公共参数 PP、消息 μ 在身份 id 下的签名 $\boldsymbol{\sigma}$，验证者首先计算 $\boldsymbol{F}_{id}=\boldsymbol{A}_0\,\|\,\boldsymbol{A}_1+H(id)\boldsymbol{B}$ 和 $\boldsymbol{C}_\mu=\boldsymbol{C}_0+\sum_{i=1}^{d}(-1)^{\nu[i]}\boldsymbol{C}_i$（这里先计算 $\nu=H'(\mu)$），最后接收签名 $\boldsymbol{\sigma}$ 当且仅当 $0<\|\boldsymbol{\sigma}\|\leqslant s_2\sqrt{3m}$ 和 $\left(\boldsymbol{F}_{id}\,\|\,\boldsymbol{C}_\mu\right)\boldsymbol{\sigma}=u$ 同时成立。令 $\boldsymbol{F}_{id,\mu}=\boldsymbol{F}_{id}\,\|\,\boldsymbol{C}_\mu$，则 $\boldsymbol{F}_{id,\mu}\boldsymbol{\sigma}=u$。

4.2 正确性和参数分析

首先来分析正确性。由于 $\boldsymbol{\sigma}_2\leftarrow D_{\mathbb{Z}^m,s_2}$，根据引理 2 有 $\|\boldsymbol{\sigma}_2\|\leqslant s_2\sqrt{m}$。由引理 2 $\boldsymbol{F}_{id}\boldsymbol{\sigma}_1=\boldsymbol{u}-\boldsymbol{C}_\mu\boldsymbol{\sigma}_2$ 且 $\|\boldsymbol{\sigma}_1\|\leqslant s_2\sqrt{2m}$。因此，$\boldsymbol{F}_{id}\boldsymbol{\sigma}_1+\boldsymbol{C}_\mu\boldsymbol{\sigma}_2=\boldsymbol{u}$，进而 $\left(\boldsymbol{F}_{id}\,\|\,\boldsymbol{C}_\mu\right)\boldsymbol{\sigma}=\boldsymbol{u}$，其中，$\boldsymbol{\sigma}=\begin{pmatrix}\boldsymbol{\sigma}_1\\ \boldsymbol{\sigma}_2\end{pmatrix}$。此外，$\|\boldsymbol{\sigma}\|=\left\|\begin{pmatrix}\boldsymbol{\sigma}_1\\ \boldsymbol{\sigma}_2\end{pmatrix}\right\|\leqslant\sqrt{\|\boldsymbol{\sigma}_1\|^2+\|\boldsymbol{\sigma}_2\|^2}\leqslant s_2\sqrt{3m}$。因此，以上签名方案验证算法正确。

为了方案能正确运行，需要满足如下一些条件：

1) 陷门生成算法 TrapGen 能正常运行，即 $m\geqslant\lfloor 6n\log q\rfloor$；

2) 私钥提取中使用的 SampleBasisLeft 算法能正常运行，即 $s_1>\left\|\tilde{T}_{A_0}\right\|\omega\left(\sqrt{\log(2m)}\right)$；

3) 签名过程中使用的 SamplePre 算法能正常运行，即 $s_2>\left\|\widetilde{SK}_{id}\right\|\omega\left(\sqrt{\log(2m)}\right)$。

由 TrapGen 算法知 $\left\|\tilde{T}_{A_0}\right\|\leqslant O\left(\sqrt{n\log q}\right)$，由 SampleBasisLeft 算法知 $\left\|\widetilde{SK}_{id}\right\|=\left\|\tilde{T}_{A_0}\right\|\leqslant O\left(\sqrt{n\log q}\right)$。因此，取 $m=6n^{1+\delta}$，$s_1=s_2=O\left(\sqrt{n\log q}\right)\omega\left(\sqrt{\log(2m)}\right)=\sqrt{m}\omega\left(\sqrt{\log(2m)}\right)$，其中，$n$ 为安全参数，δ 满足 $n^\delta>\lceil\log q\rceil=O(\log n)$。

所以，签名方案的参数在满足以上条件并按照签名中的算法正常执行的话，整个签名算法是合理正确的。

4.3 安全性

定理 2 在 SIS 问题困难的条件下，以上 IBS 方案在标准模型下达到选择身份和自适应选择消息攻击下的强不可伪造性（SU-sID-CMA）。具体来说，

注1 这里使用散列函数 H' 先将消息压缩为一个固定长度的二元串的目的是：①将使公开参数大小大幅下降，这也是 Boyen10 文章中的一个缺陷。②安全性规约中使 SIS 实例解 β 的长度变小，有利于方案的安全性。

假如 $\mathcal{A}$ 是一个攻击者，其可以进行至多 q_e 次私钥提取查询和 q_s 次签名查询并能以概率 ε 成功伪造一个合法的签名，则存在一个挑战者 $\mathcal{C}$ 以概率 $\varepsilon' \geqslant 5/6q\left(1-\left(q_e+q_s\right)/q\right)\varepsilon$ 能找到 $\mathrm{SIS}_{q,n,m,\beta}$ 问题的一个解，其中，$\beta=2s_2\sqrt{m}\left(1+12\sqrt{2m}\right)\left(1+s_2\sqrt{m(d+1)}\right)$。

证明　以下通过攻击者 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的游戏来证明。

初始化：攻击者 $\mathcal{A}$ 申明要攻击的目标身份为 id^*。挑战者 $\mathcal{C}$ 接到 SIS 问题实例 $\boldsymbol{A}_0 \in \mathbb{Z}_q^{n\times m}$，目的是求 $\boldsymbol{e}_0 \in \mathbb{Z}_q^n$ 使 $\boldsymbol{A}_0\boldsymbol{e}_0=0(\bmod q)$ 且 $0<\|\boldsymbol{e}_0\|\leqslant\beta$。

参数建立：挑战者 $\mathcal{C}$ 如下生成公开参数。

1) 根据离散高斯分布选择 n 维向量 $\boldsymbol{x} \leftarrow D_{\mathbb{Z}^n,s_2}$，并令 $\boldsymbol{u}=\boldsymbol{A}_0\boldsymbol{x}$。

2) 调用算法 TrapGen 生成矩阵对 $(\boldsymbol{B}_i,T_{B_i})\in \mathbb{Z}_q^{n\times m}\times\mathbb{Z}^{m\times m}$（$i=\{0,1\}$），其中 T_{B_i} 是 q-ary 格 $\Lambda_q^{\perp}(B_i)$ 的一组短基。

3) 选择一个随机矩阵 $\boldsymbol{R}\in\{1,-1\}^{m\times m}$；令 $\boldsymbol{R}_i'$ 是一个 $2m\times m$ 的矩阵，其中每一列独立取自离散高斯分布 $D_{\mathbb{Z}^{2m},s_2}$，这里 $i\in\{0,1,\cdots,d\}$；均匀随机选择 d 个数 $h_1,h_2,\cdots,h_d$，且令 $h_0=1$。

4) 令 $\boldsymbol{A}_1=\boldsymbol{A}_0R-H\left(id^*\right)\boldsymbol{B}_1$，$\boldsymbol{C}_i=\boldsymbol{A}_0\boldsymbol{R}_i'+h_i\boldsymbol{B}_0$，$i\in\{0,1,\cdots,d\}$。

私钥提取查询：攻击者 $\mathcal{A}$ 不能对身份 id^* 进行私钥提取查询。挑战者 $\mathcal{C}$ 使用 T_{B_1} 来回答敌手对身份 id（$id\neq id^*$）的私钥提取查询。此时，由 $\boldsymbol{A}_1=\boldsymbol{A}_0\boldsymbol{R}-H\left(id^*\right)\boldsymbol{B}_1$，得

$$\boldsymbol{F}_{id}=\boldsymbol{A}_0\|\boldsymbol{A}_1+H(id)B=\boldsymbol{A}_0\|\boldsymbol{A}_0\boldsymbol{R}+\left(H(id)-H\left(id^*\right)\right)\boldsymbol{B}_1。$$

另外，记 $\boldsymbol{M}_{id}=\left(H(id)-H\left(id^*\right)\right)\boldsymbol{B}_1$，因 $H(id)-H\left(id^*\right)\neq 0$（由于 $H(id)\neq H\left(id^*\right)$），从而 T_{B_1} 也是 $\Lambda_q^{\perp}(\boldsymbol{M}_{id})$ 的一组短基。进而可以使用算法 SampleBasisRight 来求得 $\Lambda_q^{\perp}(\boldsymbol{F}_{id})$ 的短基：$SK_{id}\leftarrow\mathrm{SampleBasisRight}\left(\boldsymbol{A}_0,\boldsymbol{M}_{id},\boldsymbol{R},T_{B_1},0,s_1\right)$。最后挑战者返回 SK_{id} 作为对身份 id 的私钥查询，并将 (id,SK_{id}) 添加到列表 L1（初始为空集）中。

签名查询：考虑身份 id 对消息 μ 的一个签名。

1) 如果 $id\neq id^*$，则挑战者查看列表 L1 看身份 id 的私钥是否被查询过，如果已经查询过，则直接使用 id 的私钥 SK_{id} 对消息 μ 执行签名算法；如果 id 的私钥没有被查询过，则挑战者自己执行私钥提取查询求得 id 的私钥 SK_{id}，然后再签名。

2) 如果 $id=id^*$，则 $\boldsymbol{F}_{id}=\boldsymbol{A}_0\|\boldsymbol{A}_1+H(id)\boldsymbol{B}=\boldsymbol{A}_0\|\boldsymbol{A}_0\boldsymbol{R}$。计算矩阵 $\boldsymbol{R}_\mu=\boldsymbol{R}_0'+\sum_{i=0}^{d}(-1)^{\mu[i]}\boldsymbol{R}_i'$ 和 $h_\mu=h_0+\sum_{i=0}^{d}(-1)^{\mu[i]}h_i$。由 $\boldsymbol{C}_i=\boldsymbol{F}_{id}\boldsymbol{R}_i'+h_i\boldsymbol{B}_0$，可得 $\boldsymbol{C}_\mu=\boldsymbol{C}_0+\sum_{i=0}^{d}(-1)^{\mu[i]}\boldsymbol{C}_i=F_{id}\boldsymbol{R}_\mu+h_\mu\boldsymbol{B}_0$。如果 $h_\mu=0$，则终止模拟，否则，T_{B_0} 也是 $\Lambda_q^{\perp}\left(h_\mu\boldsymbol{B}_0\right)$ 的一组短基。从而可以使用算法 SampleRight 来求得签名 $\boldsymbol{\sigma}\leftarrow\mathrm{SampleRight}\left(\boldsymbol{F}_{id},h_\mu\boldsymbol{B}_0,\boldsymbol{R}_\mu,T_{B_0},\boldsymbol{u},s_2\right)$。最后返回 $\boldsymbol{\sigma}$ 作为身份 id 对消息 μ 的签名，并将 $(\boldsymbol{\sigma},id,\mu)$ 添加到列表 L2（初始为空集）中。以下说明此签名是一个合法的签名。

由算法 SampleRight 得 $\left(\boldsymbol{F}_{id}\|\boldsymbol{F}_{id}\ \boldsymbol{R}_\mu+h_\mu B_0\right)\boldsymbol{\sigma}=\boldsymbol{u}$ 且 $\|\boldsymbol{\sigma}\|\leqslant s_2\sqrt{3m}$。因 $\boldsymbol{R}_\mu=\boldsymbol{R}_0'+\sum_{i=0}^{d}(-1)^{\mu[i]}\boldsymbol{R}_i'$ 和 $h_\mu=h_0+\sum_{i=0}^{d}(-1)^{\mu[i]}h_i$ 知 $\boldsymbol{F}_{id}\boldsymbol{R}_\mu+h_\mu\boldsymbol{B}_0=\boldsymbol{C}_\mu$，进而，$\left(\boldsymbol{F}_{id}\|\boldsymbol{C}_\mu\right)\boldsymbol{\sigma}=\boldsymbol{u}$。因此，$(\boldsymbol{\sigma},id,\mu)$ 是一个合法的签名。

伪造：敌手输出身份 id^* 对消息 μ^* 一个合法的签名 $\boldsymbol{\sigma}^*$。根据是否对消息 μ^* 签名在身份 id^* 下签名查询过，可分为以下 2 种情况。

1) 如果 (id^*,μ^*) 之前查询过，即在列表 L2 中存在 $(\boldsymbol{\sigma}',id^*,\mu^*)$ 且 $\boldsymbol{\sigma}'\neq\boldsymbol{\sigma}^*$。此时，$\boldsymbol{F}_{id^*,\mu^*}=\boldsymbol{F}_{id^*}\|\boldsymbol{C}_{\mu^*}=\ \boldsymbol{A}_0\|\boldsymbol{A}_0\boldsymbol{R}\|\boldsymbol{F}_{id}\boldsymbol{R}_{\mu^*}+h_{\mu^*}\boldsymbol{B}_0$。如果 $h_{\mu^*}\neq 0$，则终止模拟。进而 $\boldsymbol{F}_{id^*,\mu^*}=\boldsymbol{A}_0\|\boldsymbol{A}_0\boldsymbol{R}\|\boldsymbol{F}_{id}\boldsymbol{R}_{\mu^*}=\boldsymbol{A}_0\|\boldsymbol{A}_0\boldsymbol{R}\|\left(\boldsymbol{A}_0\|\boldsymbol{A}_0\boldsymbol{R}\right)\boldsymbol{R}_{\mu^*}$。由于 $\boldsymbol{\sigma}'$ 和 $\boldsymbol{\sigma}^*$ 是 2 个合法的签名，因此 $\boldsymbol{F}_{id^*,\mu^*}\boldsymbol{\sigma}^*=\boldsymbol{F}_{id^*,\mu^*}\boldsymbol{\sigma}'=\boldsymbol{u}$，因此 $\boldsymbol{F}_{id^*,\mu^*}(\boldsymbol{\sigma}^*-\boldsymbol{\sigma}')=0$。将 $\boldsymbol{\sigma}'$ 和 $\boldsymbol{\sigma}^*$ 分别分解为 $\boldsymbol{\sigma}'=\begin{pmatrix}\boldsymbol{\sigma}_1'\\ \boldsymbol{\sigma}_2'\\ \boldsymbol{\sigma}_3'\end{pmatrix}$ 和 $\boldsymbol{\sigma}^*=\begin{pmatrix}\boldsymbol{\sigma}_1^*\\ \boldsymbol{\sigma}_2^*\\ \boldsymbol{\sigma}_3^*\end{pmatrix}$。从而有

$$\left(\boldsymbol{A}_0\|\boldsymbol{A}_0\boldsymbol{R}\|\left(\boldsymbol{A}_0\|\boldsymbol{A}_0\boldsymbol{R}\right)\boldsymbol{R}_{\mu^*}\right)\begin{pmatrix}\boldsymbol{\sigma}_1^*-\boldsymbol{\sigma}_1'\\ \boldsymbol{\sigma}_2^*-\boldsymbol{\sigma}_2'\\ \boldsymbol{\sigma}_3^*-\boldsymbol{\sigma}_3'\end{pmatrix}=0$$

$$\boldsymbol{A}_0\left[\left(\boldsymbol{\sigma}_1^*-\boldsymbol{\sigma}_1'\right)+\boldsymbol{R}\left(\boldsymbol{\sigma}_2^*-\boldsymbol{\sigma}_2'\right)+\left(\boldsymbol{R}_{\mu^*}^{(1)}+\boldsymbol{R}\boldsymbol{R}_{\mu^*}^{(2)}\right)\left(\boldsymbol{\sigma}_3^*-\boldsymbol{\sigma}_3'\right)\right]=0$$

其中，$\boldsymbol{R}_{\mu^*}^{(1)}$ 是 $\boldsymbol{R}_{\mu^*}$ 的前 m 行，$\boldsymbol{R}_{\mu^*}^{(2)}$ 是 R_{μ^*} 的后 m 行。令 $\boldsymbol{e}_0=\left(\boldsymbol{\sigma}_1^*-\boldsymbol{\sigma}_1'\right)+\boldsymbol{R}\left(\boldsymbol{\sigma}_2^*-\boldsymbol{\sigma}_2'\right)+\left(\boldsymbol{R}_{\mu^*}^{(1)}+\boldsymbol{R}\boldsymbol{R}_{\mu^*}^{(2)}\right)\left(\boldsymbol{\sigma}_3^*-\boldsymbol{\sigma}_3'\right)$

为 SIS 问题的解。下证 $e_0 \neq 0$，且 $\|e_0\| \leqslant \beta$。

$$\|\boldsymbol{e}_0\| = \left\|\left(\boldsymbol{\sigma}_1^* - \boldsymbol{\sigma}_1'\right) + \boldsymbol{R}\left(\boldsymbol{\sigma}_2^* - \boldsymbol{\sigma}_2'\right) + \left(\boldsymbol{R}_{\mu^*}^{(1)} + \boldsymbol{R}\boldsymbol{R}_{\mu^*}^{(2)}\right)\left(\boldsymbol{\sigma}_3^* - \boldsymbol{\sigma}_3'\right)\right\|$$

$$\leqslant \left\|\left(\boldsymbol{\sigma}_1^* - \boldsymbol{\sigma}_1'\right)\right\| + \left\|\boldsymbol{R}\left(\boldsymbol{\sigma}_2^* - \boldsymbol{\sigma}_2'\right)\right\| + \left\|\left(\boldsymbol{R}_{\mu^*}^{(1)} + \boldsymbol{R}\boldsymbol{R}_{\mu^*}^{(2)}\right)\left(\boldsymbol{\sigma}_3^* - \boldsymbol{\sigma}_3'\right)\right\|。$$

由于 $\left\|\left(\boldsymbol{\sigma}_i^* - \boldsymbol{\sigma}_i'\right)\right\| \leqslant \left\|\boldsymbol{\sigma}_i^*\right\| + \left\|\boldsymbol{\sigma}_i'\right\| \leqslant 2s_2\sqrt{m}$，其中，$i \in \{1,2,3\}$。$\|\boldsymbol{R}\| \leqslant 12\sqrt{2m}$，$\left\|\boldsymbol{R}_{\mu^*}^{(1)}\right\| \leqslant s_2\sqrt{m(d+1)}$，$\left\|\boldsymbol{R}_{\mu^*}^{(2)}\right\| \leqslant s_2\sqrt{m(d+1)}$。因此，$\|\boldsymbol{e}_0\| \leqslant 2s_2\sqrt{m} + 12\sqrt{2m}2s_2\sqrt{m} + \left(1+12\sqrt{2m}\right)s_2\sqrt{m(d+1)}2s_2\sqrt{m}$

$$\leqslant 2s_2\sqrt{m}\left(1+12\sqrt{2m} + \left(1+12\sqrt{2m}\right)s_2\sqrt{m(d+1)}\right)$$

$$\leqslant 2s_2\sqrt{m}\left(1+12\sqrt{2m}\right)\left(1+s_2\sqrt{m(d+1)}\right) = \beta$$。另外，由文献[10]中的引理 26 得 $\Pr\{\boldsymbol{e}_0 \neq 0\} \geqslant 2/3$。

2) 如果 (id^*, μ^*) 之前未查询过。则 $\boldsymbol{F}_{id^*,\mu^*}\boldsymbol{\sigma}^* = \boldsymbol{u} = \boldsymbol{A}_0\boldsymbol{x}$，即 $\left(\boldsymbol{A}_0 \| \boldsymbol{A}_0\boldsymbol{R} \| \left(\boldsymbol{A}_0 \| \boldsymbol{A}_0 R\right)\boldsymbol{R}_{\mu^*}\right)\begin{pmatrix}\boldsymbol{\sigma}_1^* \\ \boldsymbol{\sigma}_2^* \\ \boldsymbol{\sigma}_3^*\end{pmatrix} = \boldsymbol{A}_0\boldsymbol{x}$，进而 $\boldsymbol{A}_0\left[\boldsymbol{\sigma}_1^* + \boldsymbol{R}\boldsymbol{\sigma}_2^* + \left(\boldsymbol{R}_{\mu^*}^{(1)} + \boldsymbol{R}\boldsymbol{R}_{\mu^*}^{(2)}\right)\boldsymbol{\sigma}_3^* - \boldsymbol{x}\right] = 0$。令 $\boldsymbol{e}_0 = \boldsymbol{\sigma}_1^* + \boldsymbol{R}\boldsymbol{\sigma}_2^* + \left(\boldsymbol{R}_{\mu^*}^{(1)} + \boldsymbol{R}\boldsymbol{R}_{\mu^*}^{(2)}\right)\boldsymbol{\sigma}_3^* - \boldsymbol{x}$ 为 SIS 问题的解。下证 $\boldsymbol{e}_0 \neq 0$，且 $\|\boldsymbol{e}_0\| \leqslant \beta$。

$$\|\boldsymbol{e}_0\| = \left\|\boldsymbol{\sigma}_1^* + \boldsymbol{R}\boldsymbol{\sigma}_2^* + \left(\boldsymbol{R}_{\mu^*}^{(1)} + \boldsymbol{R}\boldsymbol{R}_{\mu^*}^{(2)}\right)\boldsymbol{\sigma}_3^* - \boldsymbol{x}\right\|$$

$$\leqslant \left\|\boldsymbol{\sigma}_1^*\right\| + \left\|\boldsymbol{R}\boldsymbol{\sigma}_2^*\right\| + \left\|\left(\boldsymbol{R}_{\mu^*}^{(1)} + \boldsymbol{R}\boldsymbol{R}_{\mu^*}^{(2)}\right)\boldsymbol{\sigma}_3^*\right\| + \|\boldsymbol{x}\|$$

$$\leqslant s_2\sqrt{m} + 12\sqrt{2m}s_2\sqrt{m} + \left(1+12\sqrt{2m}\right)\cdot s_2\sqrt{m(d+1)}s_2\sqrt{m} + s_2\sqrt{m}$$

$$\leqslant s_2\sqrt{m}\left(2+12\sqrt{m} + \left(1+12\sqrt{2m}\right)s_2\sqrt{m(d+1)}\right)$$

$$\leqslant s_2\sqrt{m}\left(2+12\sqrt{m} + \left(1+12\sqrt{2m}\right)s_2\sqrt{m(d+1)}\right)$$

$$\leqslant 2s_2\sqrt{m}\left(1+12\sqrt{2m}\right)\left(1+s_2\sqrt{m(d+1)}\right) = \beta$$

另外，由文献[9]中的引理 2.9 得，$\Pr\{e_0 = 0\} \leqslant negl(n)$。

最后，根据文献[10]中的引理 27 可知，在以上模拟游戏过程中，查询阶段和伪造阶段都不终止的概率至少是 $\frac{1}{q}\left(1 - \frac{q_e + q_s}{q}\right)$。因此，挑战者 $\mathcal{C}$ 以概率 $\varepsilon' \geqslant (1/2.2/3+1/2)1/q\left(1-(q_e+q_s)/q\right)\varepsilon = 5/6q(1-(q_e+q_s)/q)\varepsilon$ 能返回一个 SIS 问题实例的解。

4.4 效率分析

本文对比了改进的方案和原方案以及其他基于身份的格基密码方案的效率和安全性。效率方案主要从公开参数大小，签名密钥长度和签名长度 3 个方面来比较，而安全性主要是说明在哪种模型下能达到什么安全性，具体如表 1 所示。

由表 1 可以看出，在随机预言机模型下安全的方案效率更高，而在标准模型下的方案效率较低。这在密码学中是一个公认的事实。改进后的方案在签名密钥长度和签名长度和原方案完全一样，而公开参数大小比原方案的大，这也是为了达到所宣传的安全性所付出的代价。

5 结束语

本文首先指出 Liu 等人方案[22]中安全证明中存在的问题，然后给出一个改进的 IBS 方案及其安全性证明，改进的方案能真正达到选择身份和自适应选择消息攻击下强不可伪造（SU-sID-CMA）安全性质。

表 1 效率及安全性比较

方案	公开参数大小	签名密钥长度	签名长度	安全模型	安全性
文献[18]方案	$nm\log q$	$3m\log q$	$3m\log q$	ROM	SU
文献[20]方案	$nm\log q$	$mk\log q$	$m\log(12\sigma)$	ROM	EU
文献[19]方案	$nm\log q$	$(m+1)\log q$	$(m+1)\log q$	ROM	SU
文献[22]方案	$(5m+1)n\log q$	$4m^2\log q$	$3m\log q$	SM	
改进后本方案	$((d+4)m+1)n\log q$	$4m^2\log q$	$3m\log q$	SM	SU

注：这里的大小和长度都以 bit 为单位。其中 n, m, q 都是系统参数，表达的意义一样。且 $m \gg k$，$\sigma \ll q$，d 表示消息压缩后的长度，其值为 160~256。ROM 表示随机预言机模型，SM 表示标准模型，EU 表示存在性不可伪造性，SU 表示强不可伪造性。

参考文献：

[1] SHAMIR A. Identity-based cryptosystems and signature schemes[A]. Advances in Cryptology[C]. Springer Berlin Heidelberg, 1985. 47-53.

[2] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[A]. Advances in Cryptology CRYPTO 2001[C]. Springer Berlin Heidelberg, 2001. 213-229.

[3] WATERS B. Efficient identity-based encryption without random oracles[A]. Advances in Cryptology–EUROCRYPT 2005[C]. Springer Berlin Heidelberg, 2005. 114-127.

[4] PATERSON K G, SCHULDT J C N. Efficient identity-based signatures secure in the standard model[A]. Information Security and Privacy[C]. Springer Berlin Heidelberg, 2006. 207-222.

[5] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Journal on Computing, 1997, 26(5): 1484-1509.

[6] AJTAI M. Generating hard instances of lattice problems[A]. Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing[C]. ACM, 1996. 99-108.

[7] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM (JACM), 2009, 56(6): 34.

[8] MICCIANCIO D, PEIKERT C. Trapdoors for lattices: simpler, tighter, faster, smaller[A]. Advances in Cryptology–EUROCRYPT 2012[C]. Springer Berlin Heidelberg, 2012. 700-718.

[9] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[A]. Proceedings of the 40th Annual ACM Symposium on Theory of Computing[C]. ACM, 2008. 197-206.

[10] BOYEN X. Lattice mixing and vanishing trapdoors: a framework for fully secure short signatures and more[A]. Public Key Cryptography–PKC 2010[C]. Springer Berlin Heidelberg, 2010. 499-517.

[11] CASH D, HOFHEINZ D, KILTZ E, *et al*. Bonsai trees, or how to delegate a lattice basis[J]. Journal of Cryptology, 2012, 25(4): 601-639.

[12] AGRAWAL S, BONEH D, BOYEN X. Efficient Lattice (H) IBE in the Standard Model[M]. Advances in Cryptology–EUROCRYPT 2010. Springer Berlin Heidelberg, 2010: 553-572.

[13] BRAKERSKI Z, VAIKUNTANATHAN V. Efficient fully homomorphic encryption from (standard) LWE[A]. Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on[C]. IEEE, 2011. 97-106.

[14] BRAKERSKI Z, GENTRY C, VAIKUNTANATHAN V. (Leveled) Fully homomorphic encryption without bootstrapping[A]. Proceedings of the 3rd Innovations in Theoretical Computer Science Conference[C]. ACM, 2012. 309-325.

[15] LEURENT G, NGUYEN P. How risky is the random-oracle model[A]. Advances in Cryptology-CRYPTO 2009[C]. Springer Berlin Heidelberg, 2009.445-464.

[16] Lyubashevsky V. Lattice signatures without trapdoors[A]. Advances in Cryptology EUROCRYPT 2012[C]. Springer Berlin Heidelberg, 2012: 738-755.

[17] DUCAS L, DURMUS A, LEPOINT T, *et al*. Lattice signatures and bimodal Gaussians[A]. Advances in Cryptology–CRYPTO 2013[C]. Springer Berlin Heidelberg, 2013. 40-56.

[18] RÜCKERT M. Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles[A]. Post-Quantum Cryptography[C]. Springer Berlin Heidelberg, 2010. 182-200.

[19] XIA F, YANG B, SUN W. An efficient identity-based signature from lattice in the random oracle model[J]. Journal of Computational Information Systems, 2011, 7(11): 3963-3971.

[20] TIAN M, HUANG L. Efficient identity-based signature from lattices[A]. ICT Systems Security and Privacy Protection[C]. Springer Berlin Heidelberg, 2014. 321-329.

[21] TIAN M, HUANG L, YANG W. A new hierarchical identity-based signature scheme from lattices in the standard model[J]. IJ Network Security, 2012, 14(6): 310-315.

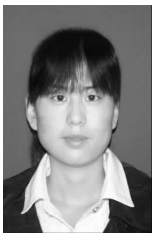
[22] LIU Z, HU Y, ZHANG X, *et al*. Efficient and strongly unforgeable identity-based signature scheme from lattices in the standard model[J]. Security and Communication Networks, 2013, 6(1): 69-77.

[23] MICCIANCIO D, GOLDWASSER S. Complexity of Lattice Problems: a Cryptographic Perspective[M]. Springer, 2002.

[24] MICCIANCIO D, REGEV O. Worst-case to average-case reductions based on Gaussian measures[J]. SIAM Journal on Computing, 2007, 37(1): 267-302.

[25] ALWEN J, PEIKERT C. Generating shorter bases for hard random lattices[J]. Theory of Computing Systems, 2011, 48(3): 535-553.

作者简介：



杨春丽（1986-），女，山西忻州人，北京邮电大学博士生，主要研究方向为信息安全、基于格的密码学。

闫建华（1977-），男，山东聊城人，北京邮电大学博士生，主要研究方向为基于格的密码学、信息安全。

郑世慧（1979-），女，山东日照人，北京邮电大学讲师，主要研究方向为经典密码和协议的分析与设计。

王励成（1971-），男，甘肃镇原人，博士，北京邮电大学副教授，主要研究方向为现代密码学、网络安全和可信计算。

杨榆（1978-），女，云南昆明人，博士，北京邮电大学讲师，主要研究方向为信息安全、信息隐藏和数字水印。