doi:10.11959/j.issn.1000-436x.2017098

新的格上基于身份的全同态加密方案

汤永利，胡明星，刘琨，叶青，闫玺玺
（河南理工大学计算机科学与技术学院，河南 焦作 454000）

摘 要：分析以往格上基于身份的全同态加密方案，指出方案效率低的根本原因在于陷门生成和原像采样过程的复杂度过高，为此提出一种新的解决方案。先将新型陷门函数与对偶容错学习（LWE，learning with errors）算法有机结合，构造一种新的格上基于身份的加密方案；再利用特征向量方法转化为格上基于身份的全同态加密方案。对比分析表明，所提方案的陷门生成复杂度显著降低，原像采样复杂度约降低为以往方案的$\frac{1}{3}$，SIVP 近似因子缩小为以往方案的$\frac{1}{\sqrt{m}}$。在标准模型下，方案安全性归约至判定性 LWE 的难解性，并包含严格的安全性证明。

关键词：格；全同态加密；基于身份加密；标准模型；密码学
中图分类号：TP309 **文献标识码**：A

Novel identity-based fully homomorphic encryption scheme from lattice

TANG Yong-li, HU Ming-xing, LIU Kun, YE Qing, YAN Xi-xi
(College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454000, China)

Abstract: The previous identity-based homomorphic encryption schemes from lattice was analyzed. That the high complexity in previous schemes was mainly caused by trapdoor generation and preimage sampling was pointed out. A new solution was proposed. A novel identity-based encryption scheme from lattice by combining new trapdoor function and dual-LWE algorithm organically was constructed, and it was transformed to an identity-based fully homomorphic encryption scheme from lattice by employing the idea of eigenvector. Comparative analysis shows that the scheme's complexity of trapdoor generation has a significant reduction, the complexity of preimage sampling has a nearly three-fold reduction, and the SIVP approximation factor has a $\sqrt{m}$ times reduction. The security of the proposed scheme strictly reduces to the hardness of decisional learning with errors problem in the standard model.

Key words: lattice, fully homomorphic encryption, identity-based encryption, standard model, cryptography

1 引言

近几年，云计算在实现中遇到的问题之一就是如何保证数据的私密性，全同态加密可以很好地解决这个技术难题。1978 年，Rivest 等[1]最早提出利用同态加密来保护数据私密性的想法。直到 2009 年，IBM 研究员 Gentry[2]基于理想格提出第一个全同态加密方案，此后全同态加密方案的设计成为密码学研究领域的热点。

全同态加密作为公钥加密的一种，需要考虑在云环境和安全多方计算中身份认证的问题，一般方法是引入公钥证书，但证书中心的存在也为整个密

收稿日期：2016-11-07；**修回日期**：2017-03-29
通信作者：叶青，yeqing@hpu.edu.cn
基金项目：国家自然科学基金资助项目（No.61300216）；河南省科技厅基金资助项目（No.142300410147）；河南省教育厅基金资助项目（No.12A520021, No.16A520013）；河南理工大学博士基金资助项目（No.B2014-044, No.B2013-043）
Foundation Items: The National Natural Science Foundation of China (No.61300216), The Project of Science and Technology Department of Henan Province (No.142300410147), The Project of Education Department of Henan Province (No.12A520021, No.16A520013), Doctoral Fund of Henan Polytechnic University (No.B2014-044, No.B2013-043)

码系统带来存储、计算、通信与管理等方面的额外开销，而且已有的全同态加密体制普遍存在公钥尺寸过大的问题，因此，与证书相关的开销将严重影响全同态加密体制在实际应用中的效率。虽然近几年该体制的计算效率得到进一步优化[3~5]，但对于公钥尺寸过大的问题，目前仍无根本的解决方案。

基于身份加密（IBE, identity-based encryption）的体制使用用户的唯一身份标识（如手机号码、邮箱地址等）作为公钥，用户的私钥由可信第三方私钥生成中心（KGC, key generation center）利用系统主私钥生成，因此无需公钥证书，所以 IBE 体制消除了与证书有关的计算和存储，可以更有效地管理密钥，减小密钥尺寸。因此，研究者们开始研究如何将基于身份加密的思想与全同态加密相结合，构造基于身份的全同态加密[6~9]（IBFHE, identity-based fully homomorphic encryption）。然而，文献[6]的方案需要借助运算密钥来实现，并非真正意义上的 IBFHE 方案，且方案的陷门生成和原像采样过于复杂，难以应用到实际当中。文献[7]的方案解决了文献[6]中运算密钥的问题，但方案的陷门生成和原像采样过于复杂的问题依旧没有解决。2013 年，Gentry 等[8]提出一个新型的全同态加密方案，利用特征向量的方法使满足相应转化条件的 IBE 方案可转化为 IBFHE 方案，且能够消除运算密钥，但是并未给出具体的方案构造。利用特征向量方法，Clear 等[9]将文献[10]中的 IBE 方案转化为第一个基于标准 LWE 假设的多身份 IBFHE 方案，但其在陷门生成和原像采样算法上没有改进，陷门函数低效的问题没有得到解决。以上方案低效的根本原因在于它们大多基于 Ajtai 等[11]在 ICALP1999 提出的陷门生成算法和文献[10]的原像采样算法构造，因此，方案的效率并不高。

根据 Gentry 等[8]提出的特征向量的转化思想，构造 IBFHE 方案的核心在于首先构造一个能够满足转化条件的 IBE 方案。2008 年，Gentry 等[10]提出对偶 LWE 算法，并基于对偶 LWE 算法构造出第一个随机预言模型下的格上 IBE 方案，同时指出基于 LWE 公钥算法构造格上 IBE 的加密算法在理论上不可行，但其原像采样算法复杂度过大，需要执行高精度实数的正交化迭代运算。2010 年，Agrawal 等[12]基于对偶 LWE 算法构造了一个标准模型下的格上 IBE 方案，但是该陷门生成算法无论是在运行时间还是输出“质量”（陷门的 Gram-Schimt 正交范数的最大值）上，都不满足实际应用。虽然近几年 Agrawal 方案的计算效率得到进一步优化[13,14]，但这些优化方案的陷门生成算法[15]由于采用了计算代价高的 HNF（hermite normal forms）和矩阵求逆运算，且仍采用文献[10]的原像采样算法，所以效率没有得到根本提高。

2012 年，Micciancio 等[16]提出一种新型陷门函数，陷门生成操作仅需 2 个随机矩阵的一次乘运算，且原像采样算法具有输入项为小整数和离线存储空间更小的优点，并基于该陷门函数构造出一种高效的格上数字签名方案和 CCA（chosen ciphertext-secure attack）加密方案，同时给出基于该陷门函数可构造格上 IBE 方案，但未给出方案的具体构造。

为使格上 IBFHE 更具有实际应用可行性，必须解决格上 IBE 陷门生成过程低效和原像采样过程复杂的问题。因此，本文提出一种新的格上基于身份的全同态加密方案。主要贡献有以下几个方面：1) 将 Micciancio 等[16]的新型陷门函数与对偶 LWE 算法[10]有机结合，提出一个新的标准模型下的格上 IBE 方案；2) 借鉴 Gentry 等[8]提出的特征向量思想，消除了以往 IBFHE 方案的运算密钥，将本文 IBE 方案转化为真正意义上的 IBFHE 方案，采用与同类方案相同的安全模型进行严格的安全性证明。结果表明，在标准模型下，本文方案的安全性可归约至判定性容错学习（DLWE，decisional learning with errors）问题的难解性。性能对比分析表明，IBE 方案由于采用新型陷门函数，与同类经典方案相比，效率参数（包括格的维度、高斯参数和模数）明显降低，安全性参数原像采样长度限制参数降低为以往方案的 $\frac{1}{\sqrt{m}}$，LWE 容错率提高 $\sqrt{m}$ 倍；IBFHE 方案与以往同类方案相比，陷门生成复杂度降低为以往方案的 $\frac{1}{47}$，原像采样复杂度降低为以往方案的 $\frac{1}{3}$，且消除了运算密钥，使公私钥尺寸更加小。

2 预备知识

2.1 格的相关定义

定义 1 设 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 是 n 维欧式空间 R^n 上 m 个线性无关向量，格 Λ 定义为所有这些向量的整系数线性组合，即 $\Lambda=\left\{\sum_{i=1}^{m}x_i\boldsymbol{b}_i : x_i\in\mathbb{Z}, i=1,\cdots,m\right\}$，其中，向量组 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 称为格的一组基。

定义 2　q 元格。设 $q,n,m\in\mathbb{Z}$，$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，且 $\boldsymbol{u}\in\mathbb{Z}_q^n$，定义

$$\left.\begin{aligned}\Lambda^{\perp}(\boldsymbol{A})&=\left\{\boldsymbol{y}\in\mathbb{Z}^m:\boldsymbol{A}\boldsymbol{y}=\boldsymbol{0}\bmod q\right\}\\ \Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A})&=\left\{\boldsymbol{y}\in\mathbb{Z}^m:\boldsymbol{A}\boldsymbol{y}=\boldsymbol{u}\bmod q\right\}\end{aligned}\right\}$$

定义 3　离散高斯分布。对任意 $\sigma>0$，定义以向量 $\boldsymbol{c}$ 为中心，σ 为参数的格 Λ 上离散高斯分布为 $D_{\Lambda,\sigma,\boldsymbol{c}}(\boldsymbol{x})=\dfrac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{\sigma,\boldsymbol{c}}(\Lambda)}=\dfrac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\sum\limits_{\boldsymbol{v}\in\Lambda}\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}$，其中，$\boldsymbol{x}\in\Lambda$，$\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})=\mathrm{e}^{\frac{-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2}{\sigma^2}}$。

2.2　相关算法和困难问题

本文方案所基于的新型陷门函数的陷门生成算法和与之匹配的原像采样算法分别具体描述为引理 1 和引理 2；对偶 LWE 算法的具体描述请参阅文献[10]。方案安全性证明基于引理 1、引理 3 和定义 4；方案的正确性证明基于引理 4 和引理 5；引理 6 和引理 7 分别用于刻画本文方案陷门单向函数的和方案所基于难题的难解性。

引理 1[16]　设整数 $n\geqslant 1$，$q\geqslant 2$ 和充分大的 $m=O(n\mathrm{lb}q)$，$\bar{m}=m-nk$，$w=nk$，$k=\lceil\mathrm{lb}q\rceil$，可逆矩阵 $\boldsymbol{H}\in\mathbb{Z}_q^{n\times n}$。公开的本原矩阵 $\boldsymbol{G}\in\mathbb{Z}_q^{n\times w}$。存在高效随机算法 $TrapGen(1^n,1^m,q,\boldsymbol{H})$，输出矩阵 $\boldsymbol{A}=\left[\bar{\boldsymbol{A}}\,|\,\boldsymbol{H}\boldsymbol{G}-\bar{\boldsymbol{A}}\boldsymbol{R}\right]\in\mathbb{Z}_q^{n\times m}$ 和陷门矩阵 $\boldsymbol{R}\in\mathbb{Z}_q^{\bar{m}\times w}$，陷门尺寸 $s_1(\boldsymbol{R})\leqslant\sqrt{m}\omega\left(\sqrt{\mathrm{lb}n}\right)$，其中，$\boldsymbol{A}$ 在 $\mathbb{Z}_q^{n\times m}$ 上是统计均匀的。

引理 2[16]　与引理 1 参数相同，设 $\boldsymbol{u}\in\mathbb{Z}_q^n$ 为均匀随机向量，充分大的高斯参数 $\sigma=O\left(\sqrt{n\mathrm{lb}q}\right)$，$\omega\left(\sqrt{\mathrm{lb}n}\right)$ 表示渐进性高于 $\sqrt{\mathrm{lb}n}$，则存在概率多项式时间（PPT, probabilistic polynomial time）算法 $SampleL(\boldsymbol{A},\boldsymbol{M},\boldsymbol{R},\boldsymbol{u},\sigma)$，其中，$\boldsymbol{M}\in\mathbb{Z}_q^{n\times w_1}$，输出向量 $\boldsymbol{e}\in\mathbb{Z}^{\bar{m}+w_1}$，且 $\boldsymbol{e}$ 的分布与 $\mathcal{D}_{\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{F}_1),\sigma\omega\left(\sqrt{\mathrm{lb}n}\right)}$ 统计不可区分，$\Pr\left[\boldsymbol{e}\leftarrow\mathcal{D}_{\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{F}_1),\sigma\omega\left(\sqrt{\mathrm{lb}n}\right)}:\|\boldsymbol{e}\|>\sigma\sqrt{m}\right]\leqslant negl(n)$，其中，$\boldsymbol{F}_1=\left(\bar{\boldsymbol{A}}\,|\,\boldsymbol{M}\right)$。

引理 3[12]　与引理 1 参数相同，设 $\boldsymbol{u}\in\mathbb{Z}_q^n$ 为均匀随机向量，充分大的高斯参数 $\sigma=O\left(\sqrt{n\mathrm{lb}q}\right)$，选取均匀随机矩阵 $\bar{\boldsymbol{R}}\leftarrow\{-1,1\}^{\bar{m}\times w}$，则存在 PPT 算法 $SampleR\left(\boldsymbol{A},\boldsymbol{G},\bar{\boldsymbol{R}},\boldsymbol{T}_{\boldsymbol{G}},\boldsymbol{u},\sigma\right)$，输出向量 $\boldsymbol{e}\in\mathbb{Z}^m$，且 $\boldsymbol{e}$ 的分布与 $\mathcal{D}_{\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{F}_2),\sigma\omega\left(\sqrt{\mathrm{lb}n}\right)}$ 统计不可区分，其中 $\boldsymbol{F}_2=(\bar{\boldsymbol{A}}\,|\,\bar{\boldsymbol{A}}\bar{\boldsymbol{R}}+\boldsymbol{G})$。

引理 4[12]　设 $\boldsymbol{e}$ 为 $\mathbb{Z}^{\bar{m}}$ 中某向量，整数 $\bar{k}=poly(n)$，均匀随机矩阵 $\hat{\boldsymbol{R}}\leftarrow\{-1,1\}^{\bar{m}\times\bar{k}}$，$C$ 为常数，有 $\Pr\left[\left\|\hat{\boldsymbol{R}}\right\|>C\sqrt{\bar{k}+\bar{m}}\right]<\boldsymbol{e}^{-(\bar{k}+\bar{m})}$。

引理 5[12]　设 $\boldsymbol{e}$ 为 $\mathbb{Z}^{\bar{m}}$ 中某向量，容错向量 $\boldsymbol{y}\xleftarrow{\bar{\boldsymbol{\psi}}_{\alpha}^{\bar{m}}}\mathbb{Z}_q^{\bar{m}}$，其中，$\bar{\boldsymbol{\psi}}_{\alpha}^{\bar{m}}$ 表示依据分布 $\bar{\boldsymbol{\psi}}_{\alpha}$ 随机选取的 $\bar{m}$ 维容销向量，$\bar{\boldsymbol{\psi}}_{\alpha}$ 是中心为 0，标准差为 $\dfrac{\alpha}{\sqrt{2\pi}}$ 的 [0,1)上的正态分布所对应的 $\mathbb{Z}_q$ 上的离散分布，则 $\left|\boldsymbol{e}^{\mathrm{T}}\boldsymbol{y}\right|$ 可看作 $[0,q-1]$ 中的整数，满足 $\left|\boldsymbol{e}^{\mathrm{T}}\boldsymbol{y}\right|\leqslant\|\boldsymbol{e}\|q\alpha\omega\left(\sqrt{\mathrm{lb}\bar{m}}\right)+\dfrac{\|\boldsymbol{e}\|\sqrt{\bar{m}}}{2}$。

陷门单向函数 $f_{\boldsymbol{A}}(\boldsymbol{e})=\boldsymbol{A}\boldsymbol{e}\bmod q$ 的单向性可以归约到非齐次小整数解问题（ISIS, inhomogeneous small integer solution）的难解性。ISIS 的难解性由引理 6 来刻画。

引理 6[10]　对任意的多项式有界 m，$\beta=poly(n)$，取任意的整数 $q\geqslant\beta\sqrt{n}\omega\left(\sqrt{\mathrm{lb}n}\right)$，若存在一个攻击者 $\mathcal{A}$ 在多项式时间内解决 $\mathrm{ISIS}_{q,m,\beta}$，则存在近似因子为 $\beta\tilde{O}(\sqrt{n})$ 的有效算法求解格上 SIVP（shortest independent vector problem）。

定义 4[17]　容错学习问题和判定性容错学习问题。设 n 为正整数，q 为素数，对 $0<\alpha\leqslant\dfrac{1}{\omega\left(\sqrt{\mathrm{lb}n}\right)}$，定义 Ψ_{α} 是中心为 0，标准差为 $\dfrac{\alpha}{\sqrt{2\pi}}$ 在 $[0,1)$ 上的正态分布，对应 $\mathbb{Z}_q$ 上的离散分布为 $\bar{\Psi}_{\alpha}$。设 χ 为 $\mathbb{Z}_q$ 上的错误分布，定义 $A_{\boldsymbol{s},\chi}$ 为 $(\boldsymbol{u}_i,v_i)=(\boldsymbol{u}_i,\boldsymbol{u}_i^{\mathrm{T}}\boldsymbol{s}+x_i)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上的分布，其中，$\boldsymbol{u}_i\in\mathbb{Z}_q^n$ 是随机选取向量，$x_i\in\mathbb{Z}_q$ 依分布 χ 随机独立选取。$(\mathbb{Z}_q,n,\chi)$-LWE 定义为：给出 m 个 $A_{\boldsymbol{s},\chi}$ 上相互独立的变量，求其对应的向量 $\boldsymbol{s}$。$(\mathbb{Z}_q,n,\chi)$-DLWE 定义为：要求以不可忽视的概率区分 $A_{\boldsymbol{s},\chi}$ 伪随机分布和 $\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上的真随机分布，对 $(\mathbb{Z}_q,n,\chi)$-LWE 问题的求解可在概率多项式时间内归约到 $(\mathbb{Z}_q,n,\chi)$-DLWE 的求解。

DLWE 问题的难解性由引理 7 来刻画。

引理 7[17] 设 $\alpha>0$，$q\geqslant\dfrac{2\sqrt{n}}{\alpha}$，若存在一个攻击者 $\mathcal{A}$ 在多项式时间内解决 $(\mathbb{Z}_q,n,\chi)$ -DLWE 问题，则存在近似因子为 $\tilde{O}\left(\dfrac{n}{\alpha}\right)$ 的有效算法求解格上 SIVP。本文将基于 DLWE 问题的难解性进行安全性证明。

3 方案构造

3.1 符号说明

为表述方便，对本文符号进行说明，如表 1 所示。

表 1 符号说明

符号	意义
$\boldsymbol{A}^{m\times n}$	m 行 n 列矩阵
$\boldsymbol{A}_i$	矩阵 $\boldsymbol{A}$ 的第 i 行
$\boldsymbol{u}$	向量，默认为列向量形式
$\boldsymbol{u}[i]$	向量 $\boldsymbol{u}$ 的第 i 个分量
$\boldsymbol{u}^{\mathrm{T}}$	向量 $\boldsymbol{u}$ 的转置
$\|S\|$	向量集合 S 的长度，等于其中所有向量欧几里得范数的最大值
$\|\tilde{S}\|$	向量集合 S 的 Gram-Schmidt 范数的最大值
$s_1(\boldsymbol{R})$	矩阵 $\boldsymbol{R}$ 的最大奇异值
$negl(n)$	n 的可忽略函数：$f(n)<(n^{-c})$，c 为常数
$poly(n)$	n 的多项式函数：$f(n)=O(n^c)$，c 为常数

3.2 基于身份的加密方案

本节将新型陷门函数与对偶 LWE 算法有机结合构造格上 IBE 方案。方案的基本参数包括：均匀随机矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和其陷门 $\boldsymbol{R}\in\mathbb{Z}^{\bar{m}\times w}$，其中，$n$ 是安全参数，$m=O(n\mathrm{lb}q)$，$\bar{m}=m-nk$，$w=nk$，$k=\lceil\mathrm{lb}q\rceil$，模数 $q=q(n)$；构造一个公开的矩阵 $\boldsymbol{G}=\boldsymbol{I}_n\otimes\boldsymbol{g}^{\mathrm{T}}\in\mathbb{Z}_q^{n\times nk}$，其中，$\boldsymbol{I}_n$ 是 $n\times n$ 单位矩阵，$\boldsymbol{g}^{\mathrm{T}}=\left[1,2,2^2,\cdots,2^{k-1}\right]\in\mathbb{Z}_q^k$；FRD（full-rank differences）函数[12] $H:\mathbb{Z}_q^n\to\mathbb{Z}_q^{n\times n}$。

IBE-Setup$\left(1^n\right)$：选取均匀随机矩阵 $\bar{\boldsymbol{A}}\in\mathbb{Z}_q^{n\times\bar{m}}$，选取 n 维均匀随机向量 $\boldsymbol{u}\in\mathbb{Z}_q^n$，运行算法 $TrapGen\left(1^n,1^m,q,\boldsymbol{H}\right)$，输出矩阵 $\boldsymbol{A}=[\bar{\boldsymbol{A}}|-\bar{\boldsymbol{A}}\boldsymbol{R}]\in\mathbb{Z}_q^{n\times m}$ 和其陷门矩阵 $\boldsymbol{R}\in\mathbb{Z}_q^{\bar{m}\times w}$，输出 $MPK=(\boldsymbol{A},\boldsymbol{u})$，$MSK=\boldsymbol{R}$。

IBE-Extract(MPK,MSK,id)：利用 FRD 编码函数 $H:\mathbb{Z}_q^n\to\mathbb{Z}_q^{n\times n}$ 将用户身份 id 映射为一个可逆矩阵 $\boldsymbol{H}_{id}\in\mathbb{Z}_q^{n\times n}$，运行 $SampleL\left(\boldsymbol{A},\boldsymbol{H}_{id}\boldsymbol{G},\boldsymbol{R},\boldsymbol{u},\sigma\right)$ 算法，输出用户密钥 $\boldsymbol{e}$，满足 $\boldsymbol{A}_{id}\boldsymbol{e}=\boldsymbol{u}$，其中，$\boldsymbol{A}_{id}=\boldsymbol{A}+[\boldsymbol{0}\,|\,\boldsymbol{H}_{id}\boldsymbol{G}]=[\bar{\boldsymbol{A}}\,|\,\boldsymbol{H}_{id}\boldsymbol{G}-\bar{\boldsymbol{A}}\boldsymbol{R}]\in\mathbb{Z}_q^{n\times m}$。

IBE-Enc(MPK,id,b)：为加密明文消息 $b\in\{0,1\}$，选取均匀随机向量 $\boldsymbol{s}\leftarrow\mathbb{Z}_q^n$，选取均匀随机矩阵 $\bar{\boldsymbol{R}}\leftarrow\{-1,1\}^{\bar{m}\times w}$，计算 $c_0=\boldsymbol{u}^{\mathrm{T}}\boldsymbol{s}+x+b\left\lfloor\dfrac{q}{2}\right\rfloor\in\mathbb{Z}_q$，$\boldsymbol{c}_1=\boldsymbol{A}_{id}^{\mathrm{T}}\boldsymbol{s}+\begin{bmatrix}\boldsymbol{y}\\\boldsymbol{z}\end{bmatrix}\in\mathbb{Z}_q^m$，其中，容错量 $x\xleftarrow{\bar{\Psi}_\alpha}\mathbb{Z}_q$，容错向量 $\boldsymbol{y}\xleftarrow{\bar{\Psi}_\alpha^{\bar{m}}}\mathbb{Z}_q^{\bar{m}}$，$\boldsymbol{z}=\bar{\boldsymbol{R}}^{\mathrm{T}}\boldsymbol{y}\in\mathbb{Z}_q^w$，输出密文 $\boldsymbol{CT}=\left(c_0,\boldsymbol{c}_1\right)\in\mathbb{Z}_q\times\mathbb{Z}_q^m$。

IBE-Dec$(MPK,\boldsymbol{sk}_{id},\boldsymbol{CT})$：输入用户密钥 $\boldsymbol{sk}_{id}=\boldsymbol{e}$ 计算 $b'=c_0-\boldsymbol{e}^{\mathrm{T}}\boldsymbol{c}_1\in\mathbb{Z}_q$，如果 $\left|b'-\left\lfloor\dfrac{q}{2}\right\rfloor\right|<\left\lfloor\dfrac{q}{4}\right\rfloor$，输出 1；否则，输出 0。

3.3 基于身份的全同态加密方案

本节利用特征向量的方法将 3.2 节所述方案转化为格上 IBFHE 方案。方案的基本参数如下：L 为本方案可以同态运算的最大电路深度，$q=q(n,L)$，令 $\ell=\lfloor\mathrm{lb}q\rfloor+1$，$N=(m+1)\ell$，$\hat{k}=m+1$，对任意 $\hat{k}$ 维向量 $\boldsymbol{a}$、$\boldsymbol{b}$，$BitDecomp(\boldsymbol{a})$ 表示 N 维向量 $(a_{1,0},\cdots,a_{1,\ell-1},\cdots,a_{\hat{k},0},\cdots,a_{\hat{k},\ell-1})$，其中，$a_{i,j}$ 表示 a_i 分量的第 j 个二进制位，$BitDecomp^{-1}(\boldsymbol{a})=\left(\sum 2^j a_{1,j},\cdots,\sum 2^j a_{\hat{k},j}\right)$ 表示 $BitDecomp$ 的逆运算，令 $Flatten(\boldsymbol{a})=BitDecomp\left(BitDecomp^{-1}(\boldsymbol{a})\right)$，$Powersof\,2(\boldsymbol{b})=(b_1,2b_1,\cdots,2^{\ell-1}b_1,\cdots,b_{\hat{k}},2b_{\hat{k}},\cdots,2^{\ell-1}b_{\hat{k}})$，且有以下 2 个等式成立。

$$\left\langle BitDecomp(\boldsymbol{a}),Powersof\,2(\boldsymbol{b})\right\rangle=\langle\boldsymbol{a},\boldsymbol{b}\rangle$$

$$\begin{aligned}\langle\boldsymbol{a},Powersof\,2(\boldsymbol{b})\rangle&=\left\langle BitDecomp^{-1}(\boldsymbol{a}),\boldsymbol{b}\right\rangle\\&=\left\langle Flatten(\boldsymbol{a}),Powersof\,2(\boldsymbol{b})\right\rangle\end{aligned}$$

IBFHE-Setup$(1^n,1^L)$：调用 *IBE - Setup* 算法，输出 $\boldsymbol{A}=[\bar{\boldsymbol{A}}\,|\,-\bar{\boldsymbol{A}}\boldsymbol{R}]\in\mathbb{Z}_q^{n\times m}$，$MPK=(\boldsymbol{A},\boldsymbol{u})$，$MSK=\boldsymbol{R}$。

IBFHE-KeyGen$(\boldsymbol{R},id)$：调用 *IBE-Extract* 算法生成用户密钥，重新定义用户密钥 $\boldsymbol{e}$ 为 $\bar{\boldsymbol{s}}\leftarrow(1,-\boldsymbol{e})\in\mathbb{Z}_q^{m+1}$，输出 $\boldsymbol{v}=Powersof\,2(\bar{\boldsymbol{s}})$。

IBFHE-Enc$(MPK,id,\mu\in\{0,1\})$：为加密 $\mu\in\{0,1\}$，

构造矩阵 $\boldsymbol{C}' \in \mathbb{Z}_q^{N\times(m+1)}$，矩阵的行为调用 *IBE-Enc* 算法生成 0 ~N 个密文，每行的密文形式为 $\boldsymbol{C}_i' = \left(c_0, \boldsymbol{c}_1^{\mathrm{T}}\right)$。输出 $\boldsymbol{C} = Flatten\left(\mu \boldsymbol{I}_N + BitDecomp\left(\boldsymbol{C}'\right)\right) \in \mathbb{Z}_q^{N\times N}$，其中，$\boldsymbol{I}_N$ 为 N 维单位矩阵。

IBFHE-Dec$(\boldsymbol{C},\boldsymbol{v})$：计算 $\boldsymbol{C}\boldsymbol{v} = \mu\boldsymbol{v} + BitDecomp\left(\boldsymbol{C}'\right)\boldsymbol{v} = \mu\boldsymbol{v} + \boldsymbol{C}'\boldsymbol{s}$，已知 $\boldsymbol{v}$ 的前 ℓ 个系数为 $1,2,\cdots,2^{\ell-1}$，令 $\boldsymbol{v}[i] = 2^i \in \left(\frac{q}{4},\frac{q}{2}\right]$，$\boldsymbol{c}_i$ 为 $\boldsymbol{C}$ 的第 i 行。计算 $x_i \leftarrow \langle \boldsymbol{c}_i, \boldsymbol{v}\rangle$，输出明文 $\mu = \frac{x_i}{\boldsymbol{v}[i]}$。

IBFHE-Eval$(MPK, f, \boldsymbol{C}_1, \boldsymbol{C}_2, \cdots, \boldsymbol{C}_t)$：算法的输入为主公钥 *MPK*，运算函数 f 和属于同一身份 *id* 的一组密文 $\left(\boldsymbol{C}_1, \boldsymbol{C}_2, \cdots, \boldsymbol{C}_t\right)$，输出为一个新的密文 $\boldsymbol{C}_f$，满足对某函数集合 $\mathcal{F}$，任意的 $f \in \mathcal{F}$，有 $Dec(\boldsymbol{sk}_{id}, \boldsymbol{C}_f) = f\left(\mu_1, \cdots, \mu_t\right)$。

同态加法计算式为

$$\left(\boldsymbol{C}_1 + \boldsymbol{C}_2\right)\boldsymbol{v} = \left(\mu_1 + \mu_2\right)\boldsymbol{v} + \left(\boldsymbol{z}_1, \boldsymbol{z}_2\right)$$

同态乘法计算式为

$$\begin{aligned}\left(\boldsymbol{C}_1\boldsymbol{C}_2\right)\boldsymbol{v} &= \boldsymbol{C}_1\left(\mu_2\boldsymbol{v} + \boldsymbol{z}_2\right) = \mu_2\left(\mu_1\boldsymbol{v} + \boldsymbol{z}_1\right) + \boldsymbol{C}_1\boldsymbol{z}_2 \\ &= \mu_1\mu_2\boldsymbol{v} + \mu_2\boldsymbol{z}_1 + \boldsymbol{C}_1\boldsymbol{z}_2 \\ &= \mu_1\mu_2\boldsymbol{v} \bmod q\end{aligned}$$

其中，$\boldsymbol{C}_1\boldsymbol{v} = \mu_1\boldsymbol{v} + \boldsymbol{z}_1$，$\boldsymbol{C}_2\boldsymbol{v} = \mu_2\boldsymbol{v} + \boldsymbol{z}_2$，$\boldsymbol{z}_1, \boldsymbol{z}_2 \xleftarrow{\bar{\psi}_\alpha^N} \mathbb{Z}_q^N$。

4　安全性证明

通常，一个 IBE 方案的安全性需满足选择身份攻击和选择明文攻击下的密文不可区分性（IND-ID-CPA），根据安全强度不同，分为适应性选择身份选择明文攻击（IND-aID-CPA）和选择性选择身份选择明文攻击（IND-sID-CPA）。本文方案是 IND-sID-CPA 安全的，且满足与均匀分布的不可区分性，即挑战密文与密文空间的随机元素不可区分，因此保证了方案的语义安全和接收方的匿名性。

标准模型下格上 IBE 方案的 INDr-sID-CPA 安全模型，首先由 Agrawal 等[12]在 Eurocrypt 2010 上提出，并且 Agrawal 等[18]在该安全模型下证明了 PKC 2012 上提出的格上 FIBE（“模糊”IBE）方案的安全性；2016 年，Wang 等[19]提出的 IBE 方案也基于 Agrawal 等提出的安全模型。因此，本文同样基于 Agrawal 等提出的安全模型进行安全性证明。

本文方案的解密正确性由定理 1 和定理 2 刻画。

定理 1　本文 IBE 方案的解密是正确的，对任意的 $id \in ID$，$\left(MPK, MSK\right) \leftarrow IBE\text{-}Setup\left(1^n, 1^L\right)$，$\boldsymbol{sk}_{id} \leftarrow IBE\text{-}Extract(MPK, MSK, id)$ 和消息 $b \in \{0,1\}$，有 $\Pr[Decrypt(MPK, \boldsymbol{sk}_{id}, Encrypt\left(MPK, id, b\right)) = b] = 1 - negl\left(n\right)$ 成立，其中，*ID* 为身份空间。

证明　IBE 方案解密算法的输出为

$$\begin{aligned}b' &= c_0 - \boldsymbol{e}^{\mathrm{T}}\boldsymbol{c}_1 \\ &= \boldsymbol{u}^{\mathrm{T}}\boldsymbol{s} + x + b\left\lfloor\frac{q}{2}\right\rfloor - \boldsymbol{e}^{\mathrm{T}}\left[\boldsymbol{A}_{id}^{\mathrm{T}}\boldsymbol{s} + \begin{bmatrix}\boldsymbol{y}\\ \boldsymbol{z}\end{bmatrix}\right] \\ &= b\left\lfloor\frac{q}{2}\right\rfloor + \underbrace{x - \boldsymbol{e}^{\mathrm{T}}\begin{bmatrix}\boldsymbol{y}\\ \boldsymbol{z}\end{bmatrix}}_{error\text{-}term}\end{aligned}$$

令 $\boldsymbol{e} = \left(\boldsymbol{e}_1 \,|\, \boldsymbol{e}_2\right)$，其中，$\boldsymbol{e}_1 \in \mathbb{Z}_q^{\bar{m}}$，$\boldsymbol{e}_2 \in \mathbb{Z}_q^{w}$，则等式右边的 *error-term* 为 $x - \boldsymbol{e}^{\mathrm{T}}\begin{bmatrix}\boldsymbol{y}\\ \boldsymbol{z}\end{bmatrix} = x - \boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{y} - \boldsymbol{e}_2^{\mathrm{T}}\bar{\boldsymbol{R}}^{\mathrm{T}}\boldsymbol{y} = x - \left(\boldsymbol{e}_1 - \bar{\boldsymbol{R}}\boldsymbol{e}_2\right)^{\mathrm{T}}\boldsymbol{y}$，由引理 2 可知，$\|\boldsymbol{e}\| \leqslant \sigma\sqrt{m}$，因此，由引理 4 可知，$\left\|\boldsymbol{e}_1 - \bar{\boldsymbol{R}}\boldsymbol{e}_2\right\| \leqslant \|\boldsymbol{e}_1\| + \left\|\bar{\boldsymbol{R}}\boldsymbol{e}_2\right\| \leqslant O\left(\sigma\bar{m}\right)$，再由引理 5 可知，*error-term* 被约束为

$$q\sigma\bar{m}\alpha\omega\left(\sqrt{\mathrm{lb}\bar{m}}\right) + O\left(\sigma\bar{m}^{\frac{3}{2}}\right) < \left|x - \boldsymbol{e}^{\mathrm{T}}\begin{bmatrix}\boldsymbol{y}\\ \boldsymbol{z}\end{bmatrix}\right| \leqslant |x| + \left|\left(\boldsymbol{e}_1 - \bar{\boldsymbol{R}}\boldsymbol{e}_2\right)^{\mathrm{T}}\boldsymbol{y}\right|$$

则当 $b = 1$ 时，$\left|b'\left\lfloor\frac{q}{2}\right\rfloor\right| < \left\lfloor\frac{q}{4}\right\rfloor$，输出 $b = b' = 1$；当 $b = 0$ 时，$\left|b' - \left\lfloor\frac{q}{2}\right\rfloor\right| > \left\lfloor\frac{q}{4}\right\rfloor$，输出 $b = b' = 0$。

定理 2　本文 IBFHE 方案的解密是正确的，对密文空间中任意的 $\boldsymbol{C}_i$，$\boldsymbol{v} \leftarrow Powersof\,2\left(1, -\left(IBE\text{-}Extract(MPK, MSK, id)\right)\right) \in \mathbb{Z}_q^N$，能够正确恢复出明文 $\mu \in \{0,1\}$。

证明　IBFHE 方案解密算法的输出为

$$\begin{aligned}\frac{x_i}{\boldsymbol{v}[i]} &= \frac{\langle \boldsymbol{c}_i, \boldsymbol{v}\rangle}{\boldsymbol{v}[i]} \\ &= \frac{\left\langle\left(\mu\left(\boldsymbol{I}_N\right)_i + BitDecomp\left(\boldsymbol{c}_i'\right)\right), \boldsymbol{v}\right\rangle}{\boldsymbol{v}[i]} \\ &= \mu\frac{\boldsymbol{v}[i]}{\boldsymbol{v}[i]} \\ &= \mu\end{aligned}$$

本文方案的安全性由定理 3 和定理 4 刻画。

定理 3 若$\left(\mathbb{Z}_q, n, \bar{\Psi}_\alpha\right)$-DLWE 难解性成立，则本文的 IBE 方案是 INDr-sID-CPA 安全的。

证明 采用基于游戏序列的证明方法，用W_i来定义攻击者在 Game i 中正确猜测出挑战比特的事件，即在 Game i 结束时，$r'=r$，其中，$r\in\{0,1\}$是挑战者为决定挑战密文类型时所使用的随机比特，$r'\in\{0,1\}$是在游戏结束时的猜测阶段，攻击者所输出的对挑战比特 r 的猜解。

Game 0 Game 0 是一个攻击本文方案的攻击者与挑战者之间进行的 INDr-sID-CPA 游戏。

Game 1 设id^*为攻击者待攻击的目标。改变$\boldsymbol{A}$的生成方式，构造矩阵$\boldsymbol{A}$为$\boldsymbol{A}=\left[\bar{\boldsymbol{A}}\,|\,-\boldsymbol{H}_{id^*}\boldsymbol{G}-\bar{\boldsymbol{A}}\boldsymbol{R}\right]$。由引理 1 可知，Game 0 中 TrapGen 算法所生成的矩阵$\boldsymbol{A}=\left[\bar{\boldsymbol{A}}\,|\,\boldsymbol{H}_{id^*}\boldsymbol{G}-\bar{\boldsymbol{A}}\boldsymbol{R}\right]$，因此，矩阵$\boldsymbol{A}$在 Game 1 与 Game 0 中是统计不可区分的，在攻击者看来，$\boldsymbol{A}$在 Game 0 和 Game 1 中是一样的。从而有

$$\Pr[W_0]=\Pr[W_1] \tag{1}$$

Game 2 Game 2 与 Game 1 的区别在于 Game 2 中使用 TrapGen 算法来生成$\boldsymbol{G}\in\mathbb{Z}_q^{n\times w}$和格$\Lambda_q^{\perp}(\boldsymbol{G})$的陷门矩阵$\boldsymbol{T}_{\boldsymbol{G}}$，$\boldsymbol{A}$仍保留为 Game 1 中的形式，$\boldsymbol{A}=\left[\bar{\boldsymbol{A}}\,|\,-\boldsymbol{H}_{id^*}\boldsymbol{G}-\bar{\boldsymbol{A}}\boldsymbol{R}\right]$，则$\boldsymbol{A}_{id}=\boldsymbol{A}+[\boldsymbol{0}\,|\,\boldsymbol{H}_{id}\boldsymbol{G}]=\left[\bar{\boldsymbol{A}}\,|\left[\boldsymbol{H}_{id}-\boldsymbol{H}_{id^*}\right]\boldsymbol{G}-\bar{\boldsymbol{A}}\boldsymbol{R}\right]$，由FRD编码函数的定义[12]可知，$\left[\boldsymbol{H}_{id}-\boldsymbol{H}_{id^*}\right]$为可逆矩阵，则挑战者可使用陷门矩阵$\boldsymbol{T}_{\boldsymbol{G}}$进行原像采样来回应攻击者的私钥查询：若$id\neq id^*$，调用算法$\boldsymbol{e}\leftarrow SampleR\left(\boldsymbol{A},\left(\boldsymbol{H}_{id}-\boldsymbol{H}_{id^*}\right)\boldsymbol{G},\boldsymbol{T}_{\boldsymbol{G}},\boldsymbol{u},\sigma\right)$，输出$\boldsymbol{sk}_{id}=\boldsymbol{e}$并回应给攻击者；若$id=id^*$，则$\left[\boldsymbol{H}_{id}-\boldsymbol{H}_{id^*}\right]$为零矩阵且不可逆，游戏终止并返回一个随机比特$r'\in\{0,1\}$。Game 2 中的私钥查询回应方法和矩阵$\boldsymbol{G}$与 Game 1 是统计不可区分的，故攻击者在 Game 2 与 Game 1 中的优势是相同的，即

$$\Pr[W_2]=\Pr[W_1] \tag{2}$$

Game 3 Game 3 与 Game 2 的区别在于挑战密文$\left(c_0^*,\boldsymbol{c}_1^*\right)$不再由加密算法生成，而是从密文空间$\mathbb{Z}_q\times\mathbb{Z}_q^m$中独立随机选取。因为挑战密文是随机选取，所以攻击者的优势可忽略不计。

接下来利用 DLWE 的难解性，证明对于 PPT 敌手来说，Game 3 与 Game 2 是统计不可区分的。

假设存在一个 PPT 敌手$\mathcal{A}$能以不可忽略的优势区分 Game 2 与 Game 3，利用敌手$\mathcal{A}$来构造求解 DLWE 的算法。模拟者$\mathcal{B}$有一系列样本$\left(\boldsymbol{u}_i,v_i\right)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$，$i=0,1,\cdots,\bar{m}$。敌手$\mathcal{A}$向模拟者$\mathcal{B}$宣布自己的攻击身份$id^*$。

系统建立 模拟者$\mathcal{B}$利用样本生成随机矩阵$\bar{\boldsymbol{A}}\in\mathbb{Z}_q^{n\times\bar{m}}$，矩阵$\bar{\boldsymbol{A}}$的第$i$列是向量$\boldsymbol{u}_i, i=0,1,\cdots,\bar{m}$，将样本向量$\boldsymbol{u}_0$作为公共随机向量$\boldsymbol{u}\in\mathbb{Z}_q^n$；其他参数与 Game 2 中生成方式相同。

询问阶段 与 Game 2 类似，模拟者$\mathcal{B}$对敌手$\mathcal{A}$多项式次密钥生成。

挑战阶段 敌手$\mathcal{A}$提交信息$b^*\in\{0,1\}$，模拟者$\mathcal{B}$操作如下：$v_0,v_1,\cdots,v_{\bar{m}}$表示 DLWE 中的$\bar{m}+1$个样本分量，令$\boldsymbol{v}^*=\begin{bmatrix}v_1\\ \vdots\\ v_{\bar{m}}\end{bmatrix}\in\mathbb{Z}_q^{\bar{m}}$，盲化消息比特$c_0^*=v_0+b^*\left\lfloor\frac{q}{2}\right\rfloor\in\mathbb{Z}_q$，令$\boldsymbol{c}_1^*=\begin{bmatrix}\boldsymbol{v}^*\\ \left(-\boldsymbol{R}\right)^{\mathrm{T}}\boldsymbol{v}^*+\boldsymbol{z}\end{bmatrix}\in\mathbb{Z}_q^m$，其中，$\boldsymbol{z}=\bar{\boldsymbol{R}}^{\mathrm{T}}\boldsymbol{y}\in\mathbb{Z}_q^w$，$\boldsymbol{y}\xleftarrow{\bar{\Psi}_\alpha^{\bar{m}}}\mathbb{Z}_q^{\bar{m}}$；选取随机比特$r\in\{0,1\}$，若$r=0$，将$\left(c_0^*,\boldsymbol{c}_1^*\right)$发送给敌手；若$r=1$，随机选择$\left(c_0,\boldsymbol{c}_1\right)\in\mathbb{Z}_q\times\mathbb{Z}_q^m$，并发送给敌手。

若 DLWE 中的分布是伪随机的，则$\boldsymbol{c}^*$的分布与 Game 2 相同。此时，$\boldsymbol{A}_{id^*}=\left[\bar{\boldsymbol{A}}\,|\,-\bar{\boldsymbol{A}}\boldsymbol{R}\right]$。由样本定义可知$\boldsymbol{v}^*=\bar{\boldsymbol{A}}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{y}$，其中，$\boldsymbol{y}\xleftarrow{\bar{\Psi}_\alpha^{\bar{m}}}\mathbb{Z}_q^{\bar{m}}$。因此，上述定义的$\boldsymbol{c}_1^*$满足

$$\begin{aligned}\boldsymbol{c}_1^*&=\begin{bmatrix}\bar{\boldsymbol{A}}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{y}\\ -\boldsymbol{R}^{\mathrm{T}}\bar{\boldsymbol{A}}^{\mathrm{T}}\boldsymbol{s}-\boldsymbol{R}^{\mathrm{T}}\boldsymbol{y}+\boldsymbol{z}\end{bmatrix}\\&=\begin{bmatrix}\bar{\boldsymbol{A}}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{y}\\ \left(-\bar{\boldsymbol{A}}\boldsymbol{R}\right)^{\mathrm{T}}\boldsymbol{s}-\boldsymbol{R}^{\mathrm{T}}\boldsymbol{y}+\boldsymbol{z}\end{bmatrix}\\&=\left(\boldsymbol{A}_{id^*}\right)^{\mathrm{T}}\boldsymbol{s}+\begin{bmatrix}\boldsymbol{y}\\ -\boldsymbol{R}^{\mathrm{T}}\boldsymbol{y}+\boldsymbol{z}\end{bmatrix}\end{aligned}$$

上式的右端是 Game 2 中的挑战密文的$\boldsymbol{c}_1$。又由$v_0=\boldsymbol{u}_0^{\mathrm{T}}\boldsymbol{s}+x$，其中，$x\xleftarrow{\bar{\Psi}_\alpha}\mathbb{Z}_q$，$c_0^*$满足$c_0^*=\boldsymbol{u}_0^{\mathrm{T}}\boldsymbol{s}+x+b^*\left\lfloor\frac{q}{2}\right\rfloor$是 Game 2 中的挑战密文的$c_0$。若 DLWE 问题中的分布是真随机的，则$v_0$在$\mathbb{Z}_q$上是均匀的，$\boldsymbol{v}^*$在$\mathbb{Z}_q^{\bar{m}}$上是均匀的。由标准的剩余散列引理[20]可

知 $\boldsymbol{c}_1^*$ 是 $\mathbb{Z}_q^m$ 上独立均匀的。因此，挑战密文的分布与在 Game 3 中同样是 $\mathbb{Z}_q \times \mathbb{Z}_q^m$ 上均匀的。

猜测阶段　多项式次选择性询问结束后，敌手 $\mathcal{A}$ 猜测与之交互的是 Game 2 还是 Game 3。模拟者 $\mathcal{B}$ 输出 $\mathcal{A}$ 的猜测结果作为对 DLWE 的求解。

因此，$\mathcal{B}$ 求解 DLWE 的优势（$DLWE\text{-}Adv_{\mathcal{B}}$）与 $\mathcal{A}$ 区分 Game 2 和 Game 3 的优势相同。因为 $\Pr[W_3]=\frac{1}{2}$，所以

$$\left|\Pr[W_2]-\frac{1}{2}\right|=\left|\Pr[W_2]-\Pr[W_3]\right|\leqslant DLWE\text{-}Adv_{\mathcal{B}} \tag{3}$$

由式(1)~式(3)可得

$$\left|\Pr[W_0]-\frac{1}{2}\right|\leqslant DLWE\text{-}Adv_{\mathcal{B}} \tag{4}$$

由于不存在 PPT 算法有效求解 DLWE，因此，本文方案是 INDr-sID-CPA 安全的。

以下定理说明，本文所提出的 IBE 方案，利用特征向量的思想转化为 IBFHE 方案，转化后的方案仍然是安全的。

定理 4　若 IBE 方案在标准模型下是 INDr-sID-CPA 安全的，则 IBFHE 方案同样在标准模型下是 INDr-sID-CPA 安全的。

证明　IBFHE 方案的安全模型与 IBE 方案相同，且 IBFHE 方案的 Eval 算法是公开的，不影响方案安全性。由定义 4 中的 LWE 假设可知，在 IBE 方案中加密 0 的密文向量与均匀向量具有不可区分性。因此，本文 IBFHE 方案同样在标准模型下是 INDr-sID-CPA 安全的。

5　性能分析

5.1　IBE 方案的性能分析

陷门生成和原像采样是格上 IBE 方案的主要操作。本文方案的加密和解密采用对偶 LWE 算法，在陷门生成和原像采样阶段采用的是更为高效的陷门函数，所需格的维数更低，那么与格的维数相关的其他参数依次被优化。另外，该陷门函数的原像采样算法，利用 sub-Gaussian 分布的相关性质[16]优化了以往的原像采样技术，且采样过程可以并行化进行，使时间复杂度更低。

本节选择 3 个方案作为参照对象：Agrawal 等在 Eurocrypt 2010 上提出的第一个标准模型下的格上 IBE 方案[12]和 Agrawal 等在 PKC 2012 上提出的格上 FIBE（“模糊”IBE）方案[18]，分别将其称为 Agrawal 2010 方案和 Agrawal 2012 方案；2016 年，Wang 等[19]优化了 Agrawal 2010 方案的公钥尺寸，提出一个具有更小公钥尺寸的 IBE 方案，将其称为 Wang 方案。

通常，格上 IBE 方案比较的参数有格的维数、高斯参数、原像采样长度限制参数、模数以及 LWE 容错率。这几个参数的意义在于格的维数与其他参数紧密相关，其中效率参数（包括格的维度、高斯参数和模数）越低表示方案的效率越高；安全性参数——原像采样长度限制参数越低和 LWE 容错率越高，表示方案越安全。IBE 方案的性能分析对比如表 2 所示，其中，m 表示格的维数，σ 表示高斯参数，α 表示 LWE 容错率，β 表示原像采样长度限制参数。

由表 2 可知，在陷门生成方面，本文方案消除了计算复杂且代价高的 HNF 和矩阵逆运算，本文方案的陷门生成仅需 2 个随机矩阵的一次乘积运算，则格的维数 m 降至 $2n\text{lb}q$；为保证原像采样高斯分布是均匀分布，高斯参数值需大于等于光滑参数值，由引理 1 可知，高斯参数与格的维数的关系为 $\sigma=\sqrt{m}\omega\left(\sqrt{\text{lb}n}\right)$，则本文方案高斯参数降至 $\sqrt{m}\omega\left(\sqrt{\text{lb}n}\right)$；由引理 2 可知，原像采样长度限制参数 $\beta=\sigma\sqrt{m}$，则 β 降至 $m\omega\left(\sqrt{\text{lb}n}\right)$；由引理 6 可知，为确保 ISIS 问题的难解性，需设 $q\geqslant\beta\sqrt{n}\omega\left(\sqrt{\text{lb}n}\right)$，则

表 2　**IBE 方案性能分析对比**

比较参数	Agrawal 2010 方案	Agrawal 2012 方案	Wang 方案	本文方案
m	$6n\text{lb}q$	$5n\text{lb}q$	$6n\text{lb}q$	$2n\text{lb}q$
σ	$m\omega\left(\sqrt{\text{lb}n}\right)$	$m\text{lb}m\omega\left(\text{lb}n\right)$	$(m+6)\omega(\text{lb}n)$	$\sqrt{m}\omega\left(\sqrt{\text{lb}n}\right)$
q	$\sqrt{nm^3}\omega(\text{lb}n)$	$\sqrt{nm^3}\text{lb}m\omega\left(\text{lb}n\right)^{\frac{3}{2}}$	$\left(\sqrt{nm^3}+6\sqrt{nm}\right)\omega\left(\text{lb}n\right)^{\frac{3}{2}}$	$m\sqrt{n}\omega(\text{lb}n)$
β	$\sqrt{m^3}\omega\left(\sqrt{\text{lb}n}\right)$	$\sqrt{m^3}\text{lb}m\omega\left(\text{lb}n\right)$	$\left(\sqrt{m^3}+6\sqrt{m}\right)\omega\left(\text{lb}n\right)$	$m\omega\left(\sqrt{\text{lb}n}\right)$
α	$\left(\sqrt{m^3}\omega\left(\text{lb}n\right)\right)^{-1}$	$\left(\sqrt{m^3}\text{lb}m\omega\left(\text{lb}n\right)^{\frac{3}{2}}\right)^{-1}$	$\left(\left(\sqrt{m^3}+6\sqrt{m}\right)\omega\left(\text{lb}n\right)^{\frac{3}{2}}\right)^{-1}$	$\left(m\omega\left(\text{lb}n\right)\right)^{-1}$

q 降至 $m\sqrt{n}\omega(\mathrm{lb}n)$；由引理 7 可知，为使噪音遍布 $\mathbb{Z}_q^n$ 空间以确保 DLWE 问题的难解性，需有 $\alpha q=\Omega(\sqrt{n})$，则 α 至少是 $(m\omega(\mathrm{lb}n))^{-1}$。另外，在原像采样方面，本文方案消除了原像采样过程中使用高精度实数的正交化迭代运算，利用特殊矩阵 $\boldsymbol{G}$ 和高效的陷门生成算法，可将原像采样算法 f_A^{-1} 高效归约至 f_G^{-1}，则时间复杂度由通常的 $\Omega(n^2\mathrm{lb}^2n)$ 降至 $O(n\mathrm{lb}n)$，进一步可利用并行原像采样算法[21]，采用 n 个处理器并行处理将其降至 $O(\mathrm{lb}n)$。

由以上分析可知，格的维数 m 的降低是参数 σ 和模数 q 变小的主要原因，从而在陷门生成和原像采样阶段更具效率优势。另外，由表 2 看出，相比最优的 Agrawal 2010 方案，本文方案的原像采样长度限制参数 β 降低为 Agrawal 2010 方案的 $\frac{1}{\sqrt{m}}$，LWE 容错率 α 提高了 $\sqrt{m}$ 倍，那么由引理 6 和引理 7 可知，求解 ISIS 和 DLWE 的难度对应的格上 SIVP 近似因子 $\beta\tilde{O}(\sqrt{n})$ 和 $\tilde{O}\left(\frac{n}{\alpha}\right)$ 均降低为 Agrawal 2010 方案的 $\frac{1}{\sqrt{m}}$，因此，本文方案的陷门单向函数和 DLWE 具有更高的难解性。

综上所述，本文 IBE 方案在陷门生成和原像采样 2 个步骤上效率均得到提高，且方案的陷门单向函数和所基于的困难问题具有更高的难解性。

5.2 IBFHE 方案的性能分析

本节选择 2 个方案作为参照对象：2014 年，光焱等[6]提出的基于 LWE 问题的 IBFHE 方案；2015 年，Clear 等[9]在 Crypto 2015 上提出一个多身份的 IBFHE 方案。本文将以上方案称为 GY 方案和 Clear 方案。

本文 IBFHE 方案的安全模型和格的维数 $m=2n\mathrm{lb}q$ 与以上 2 个方案相同，方案性能对比分析如表 3 所示。其中，安全参数 n=284，q=2^{24}，则格的维数 m=13 632。

由表 3 看出，与其他方案相比，本文 IBFHE 方案不仅具有标准模型下的可证明安全性，消除了运算密钥，而且消除了陷门生成过程中的 HNF 和矩阵逆运算，使陷门生成复杂度降低为以往方案的 $\frac{1}{47}$；原像采样过程消除了以往的正交化迭代运算，使原像采样复杂度降低为以往方案的 $\frac{1}{3}$。在公私钥尺寸上，因为消除了运算密钥，所以公私钥尺寸明显缩小，且公钥矩阵的维数比 Clear 方案低一维。

综上所述，本文 IBFHE 方案不仅具有标准模型下的可证明安全性，消除了运算密钥，而且本文方案陷门生成和原像采样复杂度更低，具有更低的公私钥尺寸。因此，本文 IBFHE 方案更具有实际应用可行性。

6 结束语

全同态加密在云环境下能够良好地保护用户隐私和云端数据。基于身份的全同态加密方案，融合基于身份加密和全同态加密的思想，能够有效解决公钥尺寸过大对于全同态加密应用效率的影响。本文将新型陷门函数和对偶 LWE 算法相结合，提出一种新的标准模型下的格上 IBE 方案，解决了格上 IBE 方案陷门难以实现和原像采样复杂的问题。在 IBE 方案基础之上，利用特征向量的思想将 IBE 方案转化为 IBFHE 方案，并消除了运算密钥。在标准模型下，方案的安全性可归约至判定性容错学习问题（DLWE）的难解性，并给出了严格的安全性证明。相比已有的 IBFHE 方案，本文方案在效率和安全性上均有提高。

本文方案的不足在于安全性仅满足选择性选择身份选择明文攻击下的语义安全，相比适应性选择身份选择明文攻击下的语义安全还有待改进，在某些安全需求更高的应用场景中使用会有限制。因此，如何将本文方案改进为满足适应性选择身份选择明文攻击下语义安全的格上基于身份的全同态

表 3 IBFHE 方案性能分析对比

IBFHE 方案	标准模型	运算密钥	陷门生成复杂度 ($\times10^{10}$)	原像采样复杂度 ($\times10^{10}$)	公钥尺寸/MB	私钥尺寸/KB
GY 方案	否	有	乘次数 64.65 加次数 64.65	乘次数 69.04 加次数 68.80	50.4	76.2
Clear 方案	否	无	乘次数 64.65 加次数 64.65	乘次数 69.04 加次数 68.80	472.6	1.66
本文方案	是	无	乘次数 1.374 加次数 1.374	乘次数 23.15 加次数 23.15	472.5	1.66

加密方案将是值得进一步研究的问题。

参考文献：

[1] RIVEST R, ADLEMAN L,DERTOUZOS M. On data banks and privacy homomorphisms[C]//IEEE 17nd Annual Symposium on Foundations of Computer Science (FOCS1978). 1978:169-177.

[2] GENTRY C. Fully homomorphic encryption using ideal lattices[C]//The 41rd ACM Symposium on Theory of Computing (STOC2009). 2009: 169-178.

[3] DUCAS L, MICCIANCIO D. FHEW. Bootstrapping homomorphic encryption in less than a second[C]//Advances in Cryptology EUROCRYPT 2016. 2015:617-640.

[4] BRAKERSKI Z, PERLMAN R. Lattice-based fully dynamic multi-key FHE with short ciphertexts[C]//Advances in Cryptology CRYPTO 2016. 2016:190-213.

[5] NUIDA K, KUROSAWA K. (Batch) Fully homomorphic encryption over integers for non-binary message spaces[C]//Advances in Cryptology EUROCRYPT 2015. 2015:537-555.

[6] 光焱, 祝跃飞, 费金龙, 等. 利用容错学习问题构造基于身份的全同态加密体制[J]. 通信学报, 2014,35(2):111-117.
GUANG Y, ZHU Y F, FEI J L, et al. Identity-based fully homomorphic encryption from learning with error problem[J]. Journal on Communications, 2014, 35(2): 111-117.

[7] 康元基, 顾纯祥, 郑永辉, 等. 利用特征向量构造基于身份的全同态加密体制[J]. 软件学报, 2016,27(6): 1487-1497.
KANG Y J, GU C X, ZHENG Y H, et al. Identity-based fully homomorphic encryption from eigenvector[J]. Journal of Software, 2016, 27(6): 1487-1497.

[8] GENTRY C,SAHAI A, WATERS B. Homomorphic encryption from learning with errors. Conceptually-simpler, asymptotically-faster, attribute-based[C]//Advances in Cryptology CRYPTO 2013. 2013:75-92.

[9] CLEAR M, MCGOLDRICK C. Multi-identity and multi-key leveled FHE from learning with errors[C]//Advances in Cryptology CRYPTO 2015. 2015: 630-656.

[10] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[C]//The 40th ACM Symposium on Theory of Computing(STOC2008). 2008:197-206.

[11] AJTAIM. Generating hard instances of the short basis problem[C]// Automata, Languages and Programming(ICALP1999). 1999:1-9.

[12] AGRAWAL S, BONEHD, BOYEN X. Efficient lattice (H)IBE in the standard model[C]//Advances in Cryptology EUROCRYPT2010. 2010:553-572.

[13] APON D, FAN X, LIU F H. Fully-secure lattice-based IBE as compact as PKE[R]. IACRePrint Cryptography Archive, 2016.

[14] YAMADA S. Adaptively secure identity-based encryption from lattices with asymptotically shorter public parameters[C]//Advances in Cryptology EUROCRYPT 2016. 2016:32-62.

[15] ALWEN J, PEIKERT C. Generating shorter bases for hard random lattices[C]//The 26th International Symposium on Theoretical Aspects of Computer Science. 2009:535-553.

[16] MICCIANCIO D, PEIKERT C. Trapdoors for lattices, simpler, tighter, faster, smaller[C]//Advances in Cryptology EUROCRYPT 2012. 2012: 700-718.

[17] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[J]. The Annual ACM Symposium on Theory of Computing, 2009, 56(6):84-93.

[18] AGRAWAL S, BOYEN X, VAIKUNTANATHAN V, et al. Functional encryption for threshold functions(or fuzzy IBE) from lattices[C]//The 15th International Conference on Practice and Theory in Public Key Cryptography. 2012:280-297.

[19] WANG F H, LIU Z H, WANG C X. Full secure identity-based encryption scheme with short public key size over lattices in the standard model[J]. The International Journal of Computer Mathematics, 2016, 93(6):854-863.

[20] DODIS Y, OSTROVSKY R, REYZIN L. Fuzzy extractors. How to generate strong keys from biometrics and other noisy data[J]. The Society for Industrial and Applied Mathematics (SIAM), 2008, 38(1): 97-139.

[21] PEIKERT C. An efficient and parallel gaussian sampler for lattices[C]//Advances in Cryptology CRYPTO 2010. 2010: 80-97.

作者简介：

汤永利（1972-），男，河南孟州人，博士后，河南理工大学教授、硕士生导师，主要研究方向为信息安全、密码学。

胡明星（1994-），男，河南鹿邑人，河南理工大学硕士生，主要研究方向为密码学。

刘琨（1978-），女，河南焦作人，河南理工大学副教授、硕士生导师，主要研究方向为信息安全、密码学。

叶青（1981-），女，辽宁营口人，博士，河南理工大学讲师、硕士生导师，主要研究方向为密码学。

闫玺玺（1985-），女，河南灵宝人，河南理工大学讲师、硕士生导师，主要研究方向为密码学。