doi:10.11959/j.issn.1000-436x.2017008

NTRU 格上高效的基于身份的全同态加密体制

段然[1,2]，顾纯祥[1,2]，祝跃飞[1]，郑永辉[1,2]，陈莉[3]

（1. 信息工程大学四院，河南 郑州 450002；2. 数学工程与先进计算国家重点实验室，江苏 无锡 214125；
3. 河南财经政法大学网络信息安全研究所，河南 郑州 450046）

摘 要：全同态加密是目前解决云计算网络数据隐私保护问题的最佳方案，但目前的体制的公钥尺寸普遍较大。首先，通过引入 Kullback-Leibler 散度的概念，构造一种 NTRU 格上的基于身份公钥的加密体制，参数分析表明体制具有较小的密钥和密文尺寸，实验数据表明体制具有较高的加解密效率。其次，利用近似特征向量技术，给出一种方法，将基于身份的公钥加密体制转换为基于身份的全同态加密体制，可以进一步减小密文尺寸。和现有体制相比，除了不需要计算密钥，实现真正意义上的基于身份特性以外，还减小了密钥和密文尺寸，提高了计算和传输效率。

关键词：全同态加密；基于身份加密；NTRU 格；随机谕示模型；近似特征向量

中图分类号：TP309.7 **文献标识码**：A

Efficient identity-based fully homomorphic encryption over NTRU

DUAN Ran[1,2], GU Chun-xiang[1,2], ZHU Yue-fei[1], ZHENG Yong-hui[1,2], CHEN Li[3]

(1. Fourth Department, PLA Information Engineering University, Zhengzhou 450002, China;
2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Wuxi 214125, China;
3. Institute of Network Information Security, Henan University of Economics and Law, Zhengzhou 450046, China)

Abstract: Fully homomorphic encryption is the best solution for solving privacy concerns for data over cloud so far, while large public key size is a general shortcoming for existing schemes. First, by introducing the concept of Kullback-Leibler divergence, an identity-based public key scheme over NTRU lattice with modified ciphertext form was proposed. Analysis on parameter setting showed its small key size and ciphertext size, and experiments revealed its high computational efficiency. Second, with the idea of approximate eigenvector, an improved method to convert the scheme into an identity-based fully homomorphic encryption one was put forward to further reduce ciphertext size. Compared with existing schemes, the converted scheme not only abandons evaluation keys to make it fully identity-based, but also has smaller keys and ciphertext, which results in higher computational and transmission efficiency.

Key words: fully homomorphic encryption, identity-based encryption, NTRU lattice, random oracle model, approximate eigenvector

1 引言

作为一种新兴的公钥加密体制，全同态加密（FHE，fully homomorphic encryption）在满足一般公钥加密性质的基础上，还可以在不对密文进行解密的条件下对密文进行运算，从而实现隐私保护、

收稿日期：2016-01-18；**修回日期**：2016-12-19
通信作者：顾纯祥，gcxiang5209@alinyun.com
基金项目：国家科技支撑计划基金资助项目（No.2012BAH47B01）；国家自然科学基金资助项目（No.61170234, No.61309007, No.61502533）；河南省科技创新杰出青年基金资助项目（No.134100510002）；河南省基础与前沿技术研究基金资助项目（No.142300410002）；河南省高校科技创新人才支持计划基金资助项目（No.13HASTIT043）

Foundation Items: The National Science & Technology Pillar Program (No.2012BAH47B01), The National Natural Science Foundation of China (No.61170234, No.61309007, No.61502533), Henan Sciences and Technology Innovation Talent Project (No.134100510002), Henan Foundation and Advanced Technology Research Project (No.142300410002), Henan University Science and Technology Innovation Talent Support Project (No.13HASTIT043)

安全多方计算等功能。与普通公钥加密体制相比，虽然全同态加密具有密文尺寸大、计算效率低等缺点，但随着云计算等其他互联网技术的不断发展，以及云上隐私外泄事故的频发，全同态加密的必要性日渐凸显。虽然全同态加密的思想提出由来已久[1]，但在之后的很长时间，这一领域一直缺乏突破性的进展。直到 2009 年，Gentry[2]基于理想格构造了第一个真正支持全同态加密的体制。在此以后，又有多种基于不同问题假设的全同态体制被提出[3,4]，全同态体制的设计和分析也成为了密码学的研究热点[5~7]。

在多方安全计算等应用中，如何进行身份认证是全同态体制需要解决的问题。由于全同态体制的密钥尺寸较大，因此常用于身份认证的公钥证书在通信、存储、管理等过程中会造成较大的开销，影响体制的效率。Shamir[8]于 1984 年提出基于身份的公钥加密体制（IBE，identity-based encryption），用户公钥可以通过其唯一的身份标识信息（如电子邮箱地址等）计算获得，用户私钥由可信第三方生成，不再需要公钥证书。目前，基于身份的全同态体制（IBFHE，identity-based fully homomorphic encryption）主要分为 2 类。光焱等[9]提出的 GZF 体制在密文运算中需要引入运算密钥。该密钥虽然和身份相关，但必须使用用户私钥进行计算，不能通过身份标识等公开信息求得，因此，并非真正意义上的 IBFHE 体制。2013 年，Gentry 等[10]利用近似特征向量技术提出了一种基于带错学习问题的 IBFHE 体制（记作 GSW 体制），使同态运算不再需要运算密钥，但体制的密文尺寸较大，效率低下。

NTRU 算法由 Hoffstein 等[11]于 1996 年提出，是一种基于多项式环的公钥密码体制。算法的安全性被认为与求解格上困难问题的最坏情况的难度相近[12]。该体制具有公私钥生成高效、易于并行计算等优点，并且能够抵抗已知的量子算法攻击[13]。

2012 年，López-Alt 等[14]提出了第一个基于 NTRU 上的全同态体制，可以实现多方密文运算。但该体制具有密钥尺寸、密文扩张过大，计算过于复杂等缺点。此外，由于解密密文需要用到所有参与运算的公钥所对应的私钥，因此该体制在实际使用中也存在着私钥容易泄露等问题。

2014 年，Ducas 等[15]提出了一种基于 NTRU 格的 IBE 体制。该体制具有较高的计算效率。但出于安全性证明的需要，体制使用了密钥封装机制（key encapsulation），需要在进行加解密过程中用到一个额外的散列函数。密钥封装机制的引入不但使体制更容易被求解带错学习问题（LWE，learning with errors）的算法攻击[16,17]，并且使密文不具备同态属性，无法在密文之间构造同态运算。

本文首先提出一个基于 NTRU 的 IBE 体制，与现有体制相比，具有较小的密钥、密文尺寸和较高的加解密效率。在此基础上，本文提出一种改进型将 IBE 体制转化为 IBFHE 体制的方法，并与高效的 IBE 体制结合，构造了基于 NTRU 的 IBFHE 体制、基于环上带错学习问题（RLWE，learning with errors over rings）和 NTRU 假设难解性，体制在随机谕示模型下具有选择明文和适应性选择身份攻击下不可区分性（IND-ID-CPA 安全）。在进行了详细的参数选取分析之后，与 GZF 体制相比，该体制的密钥尺寸较小，且不需要运算密钥，与 GSW 体制相比，该体制的公共参数、主公钥、用户私钥以及密文等需要通信传输的参数的尺寸均有较大幅度的减小。与 GSW 体制中的转化方式相比，本文的转化方式进一步减小了密文尺寸。

2　预备知识

2.1　符号定义

本文符号定义统一如下：$\mathbb{Z}^+$、$\mathbb{Z}$、$\mathbb{Q}$、$\mathbb{R}$、$\mathbb{Z}_q$ 分别表示正整数集、整数集、有理数集、实数集、整数模 q 剩余类环。对于 2 的方幂 n，用 $\mathcal{R}$ 表示多项式环 $\frac{\mathbb{Z}[x]}{x^n+1}$，用 $\mathcal{R}'$ 表示多项式环 $\frac{\mathbb{Q}[x]}{x^n+1}$，用 $\mathcal{R}_q$ 表示多项式环 $\frac{\mathbb{Z}_q[x]}{x^n+1}$。向量 $\boldsymbol{va}\in\mathbb{Z}_q^n$ 可表示为 $\boldsymbol{va}=(va_0,\cdots,va_{n-1})$；多项式 $pa\in\mathcal{R}_q$ 可表示为 $pa=(pa_0,\cdots,pa_{n-1})$。$n$ 维向量 $\boldsymbol{va}$ 的长度定义为其欧几里德范数 $\|\boldsymbol{va}\|=\sqrt{\sum_{i=0}^{n-1}va_i^2}$，向量集 S 的长度记作 $\|S\|$，定义为 $\|S\|=\max_{\boldsymbol{va}\in S}\|\boldsymbol{va}\|$。$z\leftarrow\mathcal{D}$ 表示从概率分布 $\mathcal{D}$ 中随机选取变量 z，$z\xleftarrow{R}E$ 表示从集合 E 中随机均匀选取变量 z。$pa_{i,j}$ 表示 pa_i 的第 j 比特（最低位为第 0 比特），$\boldsymbol{c}_i$ 表示矩阵 $\boldsymbol{C}$ 的第 i 列，$\boldsymbol{I}_n$ 表示 n 维单位矩阵。对于多项式 pa、pb，定义 $pa*pb=(pa\cdot pb)\mod(x^n+1)$。对于整数 ia、ib，$\mathrm{GCD}(ia,ib)$ 表示 ia 和 ib 的最大公约数。

除了常用的计算复杂度符号 O、o、Θ、ω 以

外，本文还定义了 $poly(\cdot)$ 和 $negl(\cdot)$。如果 $f(n)=O(n^c)$，则 $f(n)$ 可表示为 $poly(n)$。若对于任意的常数 c，都有 $f(n)=o(n^{-c})$，那么 $f(n)$ 可表示为 $negl(n)$，称为可忽略函数。

2.2 NTRU 格

NTRU 格是一种在密码学运用广泛的特殊格，由于其特殊结构而具有较高的运算效率。

首先给出格的定义。

定义 1 令 $\mathbb{R}^m$ 为 m 维欧氏空间。给定 n 个线性无关向量 $\boldsymbol{b}_0,\boldsymbol{b}_1,\cdots,\boldsymbol{b}_{n-1}\in\mathbb{R}^m$，由这些向量生成的格 Λ，记作 $L(\boldsymbol{b}_0,\boldsymbol{b}_1,\cdots,\boldsymbol{b}_{n-1})$，定义为 $L(\boldsymbol{b}_0,\boldsymbol{b}_1,\cdots,\boldsymbol{b}_{n-1})=\{\sum_{i=0}^{n-1}z_i\boldsymbol{b}_i:z_i\in\mathbb{Z}\}$，一般记作 $L(\boldsymbol{B})$，其中，$\boldsymbol{B}=[\boldsymbol{b}_0\,|\,\boldsymbol{b}_1\,|\cdots|\,\boldsymbol{b}_{n-1}]$。对于格基 $\boldsymbol{B}$，定义 $\tilde{\boldsymbol{B}}$ 为其格拉姆施密特正交化矩阵。$\boldsymbol{B}$ 和 $\tilde{\boldsymbol{B}}$ 满足以下关系

$$\tilde{\boldsymbol{b}}_i=\boldsymbol{b}_i-\sum_{j<i}\mu_{i,j}\tilde{\boldsymbol{b}}_j$$

其中，$\mu_{i,j}=\dfrac{\langle\boldsymbol{b}_i,\tilde{\boldsymbol{b}}_j\rangle}{\langle\tilde{\boldsymbol{b}}_j,\tilde{\boldsymbol{b}}_j\rangle}$，对于格 $L(\boldsymbol{B})$，$\Lambda^{\perp}(\boldsymbol{B})=\{\boldsymbol{ve}\in\mathbb{Z}^m\,|\,\boldsymbol{B}\cdot\boldsymbol{ve}=\boldsymbol{0}\bmod q\}$。

格 $L(\boldsymbol{B})$ 的对偶格记作 $L^*(\boldsymbol{B})$，定义为 $L^*(\boldsymbol{B})=\{\boldsymbol{b}^*\in\mathbb{R}^n:\forall i,\langle\boldsymbol{b}^*,\boldsymbol{b}_i\rangle\in\mathbb{Z}\}$，格基用 $\boldsymbol{B}^*$ 表示。

定义 2[18] 令 $n,q\in\mathbb{Z}^+$，f、g、F、$G\in\mathcal{R}$ 满足 $f*G-g*F=q$。由 f、g、F、G 生成的 NTRU 格是指以矩阵 $\begin{pmatrix}\boldsymbol{A}(f) & -\boldsymbol{A}(g)\\ \boldsymbol{A}(F) & -\boldsymbol{A}(G)\end{pmatrix}$ 的行向量作为格基生成的格，其中，$\boldsymbol{A}(x)$ 表示多项式 x 所对应的卷积矩阵。

2.3 环上带错学习问题

RLWE 问题是一种格上困难问题，是 LWE 问题在多项式环上的推广。Lyubashevsky 等[19]给出了从理想格上近似最短向量问题（Approx SVP，approximate shortest vector problem）最坏情况到判定性环上带错学习问题（DRLWE，decisional RLWE）一般情况的量子归约。

在给出 RLWE 问题的定义之前，先给出几个相关的定义。

定义 3[20] 对于 $n\in\mathbb{Z}^+$，令 $\Lambda\in\mathbb{R}^n$ 为 n 维格。对于 $\mathbb{R}^n$ 上的任意向量 $\boldsymbol{c}$ 及任意实数 $\sigma>0$，有

$$\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{va})=\exp\left(\frac{-\pi\|\boldsymbol{va}-\boldsymbol{c}\|^2}{\sigma^2}\right)\tag{1}$$

$$\rho_{\sigma,\boldsymbol{c}}(\Lambda)=\sum_{\boldsymbol{x}\in\Lambda}\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{va})\tag{2}$$

则格 Λ 上以 $\boldsymbol{c}$ 为中心，以 σ 为标准差的离散高斯分布 $\mathcal{D}_{\Lambda,\sigma,\boldsymbol{c}}$ 表示为

$$\forall\boldsymbol{y}\in\Lambda,\mathcal{D}_{\Lambda,\sigma,\boldsymbol{c}}(\boldsymbol{y})=\frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{y})}{\rho_{\sigma,\boldsymbol{c}}(\Lambda)}\tag{3}$$

当 $\boldsymbol{c}=\boldsymbol{0}$ 时，该分布简写为 $\mathcal{D}_{\Lambda,\sigma}$，称为 $\mathbb{R}$ 上的错误分布，记为 χ。

下面给出 RLWE 问题和 DRLWE 问题的定义。

定义 4[3] 对于正整数 n，$q=poly(n)$，以及 $\mathcal{R}$ 上的错误分布 χ，在 $\mathcal{R}_q\times\mathcal{R}_q$ 上定义一个使变量满足 $(pa,pa\cdot s+pb)$ 形式的概率分布 $A_{s,\chi}$，其中，pa 是 $\mathcal{R}_q$ 上的均匀分布，$s\in\mathcal{R}_q$，$pb\leftarrow\chi$。l-RLWE$_{q,n,\chi}$ 问题定义为在给出 $A_{s,\chi}$ 上 l 个相互独立的变量（称为 RLWE 实例）的情况下以接近 1 的概率求出 s。该问题也可表示为给定 $\boldsymbol{a}\in\mathcal{R}_q^l$，$\boldsymbol{b}=\boldsymbol{a}\cdot s+\boldsymbol{ve}\in\mathcal{R}_q^l$（其中，$\boldsymbol{ve}\leftarrow\chi^l$，$s\in\mathcal{R}_q$），求 s。

定义 5[3] 对于正整数 l，n，$q=poly(n)$，以及 $\mathbb{Z}_q$ 上的错误分布 χ，l-DRLWE$_{q,n,\chi}$ 问题的目标是以不可忽略的概率区分以下 2 个分布。

1) 输出 $(\boldsymbol{a},\boldsymbol{b})=(\boldsymbol{a},\boldsymbol{a}s+\boldsymbol{ve})\in\mathcal{R}_q^l\times\mathcal{R}_q^l$，其中，$s\in\mathcal{R}_q$、$\boldsymbol{x}\leftarrow\chi^l$、$\boldsymbol{a}\in\mathcal{R}_q^l$。

2) 输出 $(\boldsymbol{a},\boldsymbol{u})\in\mathcal{R}_q^l\times\mathcal{R}_q^l$，其中，$\boldsymbol{a}\xleftarrow{R}\mathcal{R}_q^l$，$\boldsymbol{u}\xleftarrow{R}\mathcal{R}_q^l$。

如果攻击者区分这 2 个分布的概率可忽略，则称 l-DRLWE$_{q,n,\chi}$ 问题是困难的。

对于 $A_{s,\chi}$ 上的一个 $(pa,pa\cdot s+pb)$，如果只知道 $pa\cdot s+pb$ 的其中 k 位，那么本文将这样的问题称为 $\frac{k}{n}$-RLWE$_{q,n,\chi}$ 问题。

该问题存在如下归约关系。

定理 1[19] 令 $n\in\mathbb{Z}^+$，素数 q 满足 $2\leqslant q\leqslant poly(n)$，$\alpha=poly(n)>0$ 满足 $\alpha q\geqslant\omega\sqrt{\mathrm{lb}n}$。则存在从 $\tilde{O}\left(\dfrac{\sqrt{n}}{\alpha}\right)$-Approx SVP 问题到 l-DRLWE$_{q,n,\chi}$ 问题的多项式时间量子算法，其中，χ 是 $\mathbb{Z}$ 上 $\sigma=\alpha q\left(\dfrac{nl}{\mathrm{lb}(nl)}\right)^{\frac{1}{4}}$ 的离散高斯分布 $\mathcal{D}_{\mathbb{Z},\sigma}$。

通过定理 1 可以看出，对于 DRLWE 问题，在

q、n 相同的情况下，问题的难度随着 l 的减小以及分布 χ 的标准差的增大而增大。

2.4　离散高斯采样函数

2015 年，Lyubashevsky 等[18]提出了一种可以在 NTRU 格上快速实现按离散高斯分布采样的算法。

定理 2[18]　存在进行如下操作的高效的多项式时间算法 CGS($\boldsymbol{B}$,$\boldsymbol{c}$)：算法输入格基 $\boldsymbol{B}=\{\boldsymbol{b}_0,\cdots,\boldsymbol{b}_{n-1}\}$ 和中心 $\boldsymbol{c}$，输出 $\mathcal{D}_{\Lambda(\boldsymbol{B}),\sigma,\boldsymbol{c}}$ 上的采样 $\boldsymbol{w}$。

为了减小体制的参数，引入 Kullback-Leibler 散度的定义来对 2 个分布之间的“距离”进行刻画。

定义 6[15]　令 $\mathcal{P}$、$\mathcal{Q}$ 是可数集 Ω 上的 2 个分布，$S\subset\Omega$ 是 $\mathcal{P}$ 的支集。$\mathcal{Q}$ 到 $\mathcal{P}$ 的 Kullback-Leibler 散度（简称 KL 散度），记作 $D_{\mathrm{KL}}(\mathcal{P}\|\mathcal{Q})$，令对所有 $x>0$ 有 $\ln\left(\frac{x}{0}\right)=+\infty$，定义为

$$D_{\mathrm{KL}}(\mathcal{P}\|\mathcal{Q})=\sum_{i\in S}\ln\left(\frac{\mathcal{P}(i)}{\mathcal{Q}(i)}\right)\mathcal{P}(i) \tag{4}$$

定义 7[21]　平滑参数。对于格 $L(\boldsymbol{B})$ 和实数 $\varepsilon>0$，平滑参数 $\eta_\varepsilon(\boldsymbol{B})$ 定义为满足 $\rho_{\frac{1}{s}\sqrt{2\pi},\boldsymbol{\theta}}(\boldsymbol{B}^*\setminus\boldsymbol{0})\leqslant\varepsilon$ 的最小的 $s(s>0)$。定义 $\eta_\varepsilon'(\boldsymbol{B})=\frac{1}{\sqrt{2\pi}}\eta_\varepsilon(\boldsymbol{B})$。

CGS 算法的输出满足命题 1。

命题 1[15,22]　对任意 $\varepsilon<\frac{2^{-\frac{\lambda}{2}}}{4\sqrt{2n}}$，如果 $\sigma\geqslant\|\tilde{\boldsymbol{B}}\|\cdot\eta_\varepsilon'(\mathbb{Z})$（其中，$\eta_\varepsilon'(\mathbb{Z})\approx\frac{1}{\pi}\sqrt{\frac{1}{2}\ln(2+\frac{2}{\varepsilon})}$），那么 CGS 算法的输出到分布 $\mathcal{D}_{\Lambda(\boldsymbol{B}),\sigma,\boldsymbol{c}}$ 的 KL 散度不超过 $2^{-\lambda}$。

3　NTRU 上基于身份的公钥加密体制设计

本节通过对 Ducas 等[15]提出的 IBE 体制（记作 DLP 体制）中的公私钥、密文结构以及加解密方式等方面进行修改，提出一种无需密钥封装机制的基于 NTRU 体制的 IBE 体制，且参数选取与原始体制相比有较大幅度的减小，可以利用该体制构造高效的 IBFHE 体制。

3.1　体制设计

首先，给出一种高效的对偶加密体制 ND，可以用该体制构造高效的基于身份加密体制。体制的安全参数为 λ，维数 n 为 2 的方幂，模数 q 为素数，分布 χ_1 定义为标准差为 $\sigma_1=1.17\eta_\varepsilon'(\mathbb{Z})\sqrt{q}$ 的离散高斯分布 $\mathcal{D}_{\mathcal{R}_q,\sigma_1}$（其中，$\varepsilon<\frac{2^{-\frac{\lambda}{2}}}{4\sqrt{2n}}$），分布 χ_2 定义为 $\sigma_2=8$ 的离散高斯分布 $\mathcal{D}_{\mathbb{Z},\sigma_2}$，明文空间为 $\{0,1\}$。体制包含密钥生成、加密、解密等 3 个算法。

密钥生成算法 ND.Keygen(n,q,1^λ)。算法输入维数 n、模数 q 和系统参数 1^λ，输出公钥 (h,t) 和私钥 $\boldsymbol{sk}$。具体流程：从离散高斯分布 χ_1 上采样 $s',s''\leftarrow\chi_1$，在环 $\mathcal{R}_q$ 上随机均匀选取 $h\xleftarrow{R}\mathcal{R}_q$，将 $\boldsymbol{sk}=(1,-s_0'',-s_{n-1}'',\cdots,-s_1'')$ 作为私钥，计算公钥 $pk=(h,t=hs''+s')$。

加密算法 ND.Enc(pk,m)。算法输入公钥 pk 和要加密的明文信息 $m\in\{0,1\}$，输出用公钥 pk 对 m 加密所得的密文 $\boldsymbol{c}$。具体流程：从 χ_2^n 上随机选取 r、e_1、e_2，计算 $v=r*h+e_1\in\mathcal{R}_q$，$w=r*t+e_2\in\mathcal{R}_q$，将 u 表示为 $\mathbb{Z}_q^n$ 上的向量 $\boldsymbol{u}$，输出 $\boldsymbol{c}=(w_0+\left\lfloor\frac{q}{2}\right\rfloor m,\boldsymbol{u})\in\mathbb{Z}_q\times\mathbb{Z}_q^n$。

解密算法 ND.Dec($\boldsymbol{s}$,c)：算法输入私钥 $\boldsymbol{sk}$ 和明文 m 对应的密文 $\boldsymbol{c}$，输出明文 m。具体流程：将 $\boldsymbol{c}$ 表示为 $\mathbb{Z}_q^{n+1}$ 上的向量，计算并输出 $m=\left\lfloor\frac{\langle\boldsymbol{c},\boldsymbol{sk}\rangle}{\frac{q}{2}}+0.5\right\rfloor$。

下面给出 DLP 体制的参数生成算法。本文的参数生成算法与该算法相同。定义 $x'\in\mathcal{R}'$ 满足 $\mathcal{A}(x')=\mathcal{A}(x)^{\mathrm{T}}$。

参数生成算法 DLP.Setup(n,q,1^λ)。算法输入维数 n、模数 q 和系统参数 1^λ，输出主公钥 h 和主私钥 $\boldsymbol{B}$。具体流程如下。

1) 计算 $\sigma=1.17\sqrt{\frac{q}{2n}}$。

2) 从分布 $\mathcal{D}_{\mathbb{Z}^n,\sigma}$ 中采样 $f,g\leftarrow\mathcal{D}_{\mathbb{Z}^n,\sigma}$，直到满足 $\max\left(\|(g,-f)\|,\left\|\left(\frac{qf'}{f*f'+g*g'},\frac{qg'}{f*f'+g*g'}\right)\right\|\right)\leqslant\sqrt{2n}\sigma$。

3) 利用扩展欧几里德算法，计算 r_f、$r_g\in\mathcal{R}$、R_f、$R_g\in\mathbb{Z}$ 使 $r_ff=R_f\bmod(x^n+1)$、$r_gg=R_g\bmod(x^n+1)$。若 $\mathrm{GCD}(R_f,R_g)\neq1$ 或 $\mathrm{GCD}(R_f,q)\neq1$，则返回步骤 2)。

4) 计算 t_f、$t_g\in\mathbb{Z}$，使 $t_fR_f+t_gR_g=1$。

5) 计算 $qt_gr_g=F''$、$-qt_fr_g=G''$、$k=$

$\left\lfloor \dfrac{F''*f'+G''*g'}{f*f'+g*g'}+0.5 \right\rfloor \in \mathcal{R}$、$F=F''-k*f$、$G=G''-k*g$。

6) 计算主公钥 $h=g*f^{-1} \bmod q$，主私钥 $\boldsymbol{B}=\begin{pmatrix} \boldsymbol{A}(g) & -\boldsymbol{A}(f) \\ \boldsymbol{A}(G) & -\boldsymbol{A}(F) \end{pmatrix}$。

利用 2.4 节提出的高效的离散高斯采样函数构造如下的 IBE 体制。体制包含参数生成、私钥提取、加密和解密 4 个多项式时间算法。

参数生成算法 NIBE.Setup(n,q)。算法调用 DLP.Setup(n,q)算法生成主公钥 h 和主私钥 $\boldsymbol{B}$。生成用于计算用户公钥的抗碰撞散列函数 $H(\cdot)$: $\{0,1\}^* \to \mathbb{Z}_q^n$。

私钥提取算法 NIBE.Extract($\boldsymbol{B}$,id)。算法输入主私钥 $\boldsymbol{B}$ 和用户身份 $id \in \{0,1\}^*$，输出用户私钥 $\boldsymbol{sk}_{id}$。具体流程：首先检查输入的用户身份 id 对应的 $\boldsymbol{sk}_{id}$ 是否在存储列表中，如果存在，则返回存储结果，否则计算用户公钥 $t=H(id) \in \mathbb{Z}_q^n$，调用 2.4 节中的采样算法生成 $(s',s'')=(t,0)-\mathrm{CGS}(\boldsymbol{B},(t,0))$，将 $\boldsymbol{sk}_{id}=(1,-s_0'',-s_{n-1}'',\cdots,-s_1'') \in \mathbb{Z}_q^{n+1}$ 作为用户私钥存储并输出。

加密算法 NIBE.Enc(id,m)。算法输入用户身份 id 和要加密的明文信息 $m \in \{0,1\}$，输出用 id 所对应的公钥 t 对 m 加密所得的密文 c。具体流程：计算 $t=H(id)$，调用 ND.Enc(pk,m)算法计算并输出密文 $\boldsymbol{c}$。

解密算法 NIBE.Dec($\boldsymbol{sk}_{id}$,$\boldsymbol{c}$)。算法调用 ND.Dec($\boldsymbol{sk}_{id}$,$\boldsymbol{c}$)算法计算并输出明文 m。

3.2 正确性和安全性分析

解密正确性。根据加密算法，有 $\langle \boldsymbol{c},\boldsymbol{sk}_{id} \rangle = w_0 - \sum_{i=0}^{n-1} w_i s_{n-i}''$。令 $d=vs''$，根据私钥提取算法，由卷积的性质可知 $\sum_{i=0}^{n-1} u_i s_{n-i}'' = u_0''$，因此，$\langle \boldsymbol{c},\boldsymbol{sk}_{id} \rangle = w_0 - d_0$。又因为 $s'+hs''=t$，所以有

$$\begin{aligned} w-vs'' &= rt+e_2+\left\lfloor \frac{q}{2} \right\rfloor m-(rh+e_1)s'' \\ &= (rs'+e_2-e_1s'')+\left\lfloor \frac{q}{2} \right\rfloor m \end{aligned} \tag{5}$$

因此，只要 $x=rs'+e_2-e_1s''$ 的第 1 项的系数在区间 $(-\frac{q}{4},\frac{q}{4})$ 内即可保证解密正确，由于 $\|x_0\|=\Theta(\sqrt{qn})$，所以只需 q 足够大。参数的具体取值将在 3.3 节中给出。

体制安全性。关于 ND 体制的安全性有以下定理。

定理 3 设系统参数 $n=poly(\lambda), q=poly(\lambda)$ 为安全参数 λ 的多项式，如果 $\left(1+\frac{1}{n}\right)$-DRLWE$_{q,n,\chi_2}$ 问题是困难的，那么体制在随机谕示模型下是 IND-CPA 安全的。

证明 通过构造游戏序列的方式对定理 3 进行证明。

Game0

初始化：挑战者 B 运行 ND.Keygen(n,q,1^λ)，生成公钥 $pk=(h,t)$，私钥 $\boldsymbol{sk}$，并将公钥给攻击者 A。

1) 攻击者可以自行或通过挑战者对消息 $m \in \{0,1\}$ 进行加密。若通过挑战者加密，则挑战者需正确返回密文。

挑战：在某个时间点，攻击者向挑战者发起挑战。挑战者随机选取 $m \in \{0,1\}$，运行 ND.Enc(pk,m)计算挑战密文 $\boldsymbol{c}$ 并发送给攻击者。

2) 同 1)一样，攻击者可以自行或通过挑战者对消息 $m \in \{0,1\}$ 进行加密。

猜测：最终，攻击者对挑战步骤中选取的挑战明文进行猜测，输出 $m' \in \{0,1\}$。

Game0 即为标准的 IND-CPA 攻击游戏，将攻击者 A 的优势记作 $Adv_{\mathrm{CPA}}(A)=\left|2\Pr[m'=m]-1\right|$。

Game1

在 Game1 中，挑战者在初始化步骤与 Game0 有所不同。

初始化：挑战者 B 随机均匀选取 h、$t \xleftarrow{R} \mathcal{R}_q$ 作为公钥发送给攻击者 A。

将 Game1 中攻击者 A 的优势记作 $Adv_{\mathrm{Game1}}(A)$。

在 Game1 中，公钥不再通过私钥生成。由于 Game0 中的公钥可以看作 1 个 RLWE 实例，Game1 中的公钥随机均匀选取，因此，若攻击者 A 可以以不可忽略的优势区分 Game0 和 Game1，那么挑战者 B 同样可以以不可忽略的优势求解1-DRLWE$_{q,n,\chi_1}$ 问题。具体操作：对于1-DRLWE$_{q,n,\chi_1}$ 问题的输出 $(a,b) \in \mathcal{R}_q \times \mathcal{R}_q$，挑战者 B 将其作为 ND 体制的公钥给攻击者 A，如果攻击者猜测正确，则挑战者认为这样的 (a,b) 取自 RLWE 分布，否则认为取自随

机分布。如果1-DRLWE$_{q,n,\chi_1}$ 问题是困难的，则攻击者 A 区分 Game0 和 Game1 的优势可忽略，因此有

$$Adv_{\mathrm{CPA}}(A)=Adv_{\mathrm{Game1}}(A)+negl(\lambda) \tag{6}$$

Game2

在 Game2 中，挑战者在挑战步骤与 Game1 有所不同。

挑战：在某个时间点，攻击者向挑战者发起挑战。挑战者随机选取 $(v,\boldsymbol{u})\xleftarrow{R}\mathbb{Z}_q\times\mathbb{Z}_q^n$ 作为挑战密文 c 并发送给攻击者。

将 Game2 中攻击者 A 的优势记作 $Adv_{\mathrm{Game2}}(A)$。

可以看出，在 Game2 中，密钥和密文均随机均匀选取，因此 $Adv_{\mathrm{Game2}}(A)=0$。由于 Game1 中的密文可以看作 $1+\frac{1}{n}$ 个 RLWE 实例，Game2 中的密文随机均匀选取，因此，若攻击者 A 可以以不可忽略的优势区分 Game1 和 Game2，那么挑战者 B 同样可以以不可忽略的优势求解 $(1+\frac{1}{n})$- DRLWE$_{q,n,\chi_2}$ 问题。如果 $(1+\frac{1}{n})$-DRLWE$_{q,n,\chi_2}$ 问题是困难的，那么攻击者 A 区分 Game1 和 Game2 的优势可忽略，则有

$$Adv_{\mathrm{Game1}}(A)\leqslant Adv_{\mathrm{Game2}}(A)+negl(\lambda) \tag{7}$$

由于 Game1 和 Game2 的 DRLWE 问题取自不同的分布，因此如果 $(1+\frac{1}{n})$-DRLWE$_{q,n,\chi_2}$ 问题是困难的，那么 $Adv_{\mathrm{CPA}}(A)=negl(\lambda)$，此时 ND 体制是 IND-CPA 安全的。

下面给出 NIBE 体制的安全性证明。

定理 4　设系统参数 $n=poly(\lambda), q=poly(\lambda)$ 为安全参数 λ 的多项式，如果 NTRU 问题和 $(1+\frac{1}{n})$-DRLWE$_{q,n,\chi_2}$ 问题是困难的，那么 NIBE 体制在随机谕示模型下是 IND-ID-CPA 安全的。

证明　首先，根据定理 3，如果 $(1+\frac{1}{n})$-DRLWE$_{q,n,\chi_2}$ 问题是困难的，那么 ND 体制在随机谕示模型下是 IND-CPA 安全的。

如果存在多项式时间攻击者 A，可以在访问至多 $\mathcal{Q}_{\mathrm{query}}$ 次私钥提取谕示的情况下以不可忽略的优势 ε 破坏 NIBE 体制 IND-ID-CPA 安全性，那么可以通过以下方法构造以 $\frac{\varepsilon}{\mathcal{Q}_{\mathrm{query}}}$ 的优势破坏 ND 体制 IND-CPA 安全性的攻击者 B。

攻击者 B 在得到 ND 体制的公钥 (h,t) 后，随机均匀选取 $i\leftarrow\{1,\cdots,\mathcal{Q}_{\mathrm{query}}\}$，将 h 作为 NIBE 体制的主公钥，并模拟攻击游戏。

散列谕示：对于 A 的第 j 次访问 id_j，如果 $j=i$，那么保存 $(id_j,t,\perp)$，并将 t 交给 A；如果 $j\neq i$，则调用 ND.Keygen，生成公私钥对 $(t_j,\boldsymbol{sk}_j)$，保存三元组 $(id_j,t_j,\boldsymbol{sk}_j)$，并将 t_j 交给 A。

私钥提取谕示：若 A 以身份 id 访问私钥提取谕示，不失一般性地假设 A 已经用 id 访问过散列谕示，因此，B 只需查询已保存的三元组 $(id,t,\boldsymbol{sk})$，将 $\boldsymbol{sk}$ 交给 A。如果 $\boldsymbol{sk}=\perp$，则输出随机值并终止。

挑战谕示：当 A 生成挑战身份 id^* 时，要求 A 没有用 id^* 访问过私钥提取谕示，不失一般性地假设 A 已经用 id^* 访问过散列谕示，如果 $id^*\neq id$，则输出一个随机值并终止；否则，B 从挑战者处得到挑战密文 $\boldsymbol{c}^*$，并将 $\boldsymbol{c}^*$ 交给 A。

对于 A 输出的结果，B 也输出同样的结果。

在模拟过程中，如果 NTRU 问题是困难的，那么当且仅当 $id^*=id_i$ 时，B 未终止并输出结果，因此概率为 $\frac{1}{\mathcal{Q}_{\mathrm{query}}}$。此时，$B$ 成功模拟出 NIBE 攻击游戏。根据假设，可知 A 破坏 NIBE 体制 IND-ID-CPA 安全性的优势为 ε，故 B 攻击 ND 体制的优势为 $\frac{\varepsilon}{\mathcal{Q}_{\mathrm{query}}}$。

3.3　参数选取

通过密码分析技术对 NIBE 体制的系统参数的选取进行研究。

定理 4 证明了体制的 IND-ID-CPA 安全性，下面将使用根式埃尔米特因子（root Hermite factor），结合目前对格的研究结果，对体制的参数选取进行分析。令与安全参数相关的根式埃尔米特因子 $\gamma\leqslant 1.007\,5$，该参数为 Ducas 等[15]的 IBE 体制在维数 $n=512$ 时所能达到的安全级别，此时安全级别 $\lambda\approx 80$。

攻击本体制的方法主要包括攻击主公钥、用户私钥和体制 CPA 安全性。

攻击主公钥的方式为通过寻找足够短的 f、g 来区分 NTRU 格和随机值。根据 Ducas 等[12]的实验结果，与在 $2n$ 维 NTRU 格中找到向量 $\boldsymbol{v}=(f,g)$ 相关的根式埃尔米特因子为

$$\gamma^{2n}=\frac{\sqrt{\frac{2n}{2\pi e}}\det(\Lambda)^{\frac{1}{2n}}}{0.4\|\boldsymbol{v}\|} \tag{8}$$

对于 $n=256$，这一攻击的 γ=1.005 4。

针对本体制用户私钥 $\boldsymbol{sk}_{id}$ 的攻击可以转化为在 $2n$ 维 NTRU 格上找到向量 (s',s'')。根据 Gama 等[23]的研究，与在 $2n$ 维格中找向量 $\boldsymbol{v}=(s',s'')$ 相关的根式埃尔米特因子为

$$\gamma^{2n}=\frac{\|\boldsymbol{v}\|}{\det(\Lambda)^{\frac{1}{2n}}} \tag{9}$$

对于 $n=256$，这一攻击的 γ=1.006 9。

对于针对体制的 CPA 安全性的攻击，不失一般性地考虑对明文 0 加密。由于加密包含操作 $v=r*h+e_1$、$w=r*t+e_2$，且 r、e_1、$e_2\in\{-1,0,1\}^n$，目前最常用的攻击方式是使用与恢复主私钥相同的方法恢复噪声分量 e_1、e_2，或是使用 Micciancio 提出的区分攻击。

对于恢复噪声攻击，根据加解密流程及公私钥关系，有 $(t*h^{-1})*e_1-e_2=(t*h^{-1})*v-w$。由于最终密文只包含 $\boldsymbol{v}$ 的最低位，因此求解 e_1、e_2 可以转化为在行列式为 q 的 $n+2$ 维格上找到向量 $(e_1,e_{20},1)$。对于 $n=256$，当 $\mathrm{lb}\,q\leqslant 828$ 时，有 γ<1.007 5。

对于区分攻击，根据 Micciancio 的研究[24]，与在 $l\leqslant\sqrt{\frac{\mathrm{lb}q}{\mathrm{lb}\gamma}}$ 的情况下以 ε 的优势求解 l-DRLWE$_{q,n,\chi}$ 问题相关的根式埃尔米特因子为（其中，分布 χ 的参数为 σ）

$$\gamma^{l\cdot n}=\frac{q^{\frac{l-1}{l}}\sqrt{\frac{\ln\left(\frac{1}{\varepsilon}\right)}{\pi}}}{\sigma} \tag{10}$$

对于 $n=256$、$\varepsilon=2^{-32}$，当 $\mathrm{lb}\,q\leqslant 63$ 时，有 γ<1.007 5。

因此，当 $n=256$、$\mathrm{lb}\,q\leqslant 63$ 时，3 种攻击的相关的根式埃尔米特因子均不超过 1.007 5。

3.4 效率对比

本节将 NIBE 体制和 DLP 体制，以及移除该 IBE 体制加解密过程中的散列函数所得的 IBE 体制（DLP2 体制）进行效率对比，如表 1 所示。令 $\gamma\leqslant$1.007 5，区分攻击优势 $\varepsilon=2^{-32}$，解密错误率不超过 2^{-60}。时间分析在 CPU 为 i7-4790（3.6 GHz）、内存为 16 GB 的台式计算机上进行，平台为包含 GMP 库和 NTL 库的 Visual Studio 2010。

通过对比可以看出，NIBE 体制的密钥尺寸比 DLP 体制小 39.13%，比 DLP2 体制小 78.13%；NIBE 体制的密文尺寸比 DLP 体制小 70.10%，比 DLP2 体制少 89.02%；NIBE 体制的加密时间比 DLP 体制少 59.91%，比 DLP2 体制少 81.08%；NIBE 体制的解密时间比 DLP 体制少 67.93%，比 DLP2 体制少 84.99%。此外，与 DLP 体制相比，NIBE 体制未使用密钥封装机制。虽然 NIBE 体制每次加密的比特数较少，但通过第 4 节可以看出，在构造 IBFHE 体制时，体制调用 IBE 的加密算法时，加密的明文消息均为 0，因此 IBE 体制每次加密的比特数对 IBFHE 体制的效率没有影响。

利用该 IBE 体制，可以构造具有较小参数的 IBFHE 体制。

4 高效的基于身份的全同态体制设计

本节通过对 Gentry 等[10]构造 FHE 体制的方法作适当修改，并利用这一构造方式将第 3 节中提出的基于 NTRU 的 IBE 体制转化为 IBFHE 体制，记作 NIBFHE 体制。与原始的转化方法相比，体制的参数有所减小，效率相应提高。

4.1 体制设计

在转化过程中，需要使用如下几个函数：令 $\boldsymbol{a}$、$\boldsymbol{y}$ 为 $\mathbb{Z}_q^k$ 上的向量，$l=\left\lceil\frac{\mathrm{lb}q}{2}\right\rceil$，$N$=$kl$。2$b$*Decompt*($\boldsymbol{a}$)的结果为向量 $\boldsymbol{a}'=(a'_{0,0},\cdots,a'_{0,l-1},\cdots,a'_{k-1,0},\cdots,a'_{k-1,l-1})$，满足 $a_i=\sum_{j=0}^{l-1}{}^{j}a'_{i,j}\,4\bmod q$，且所有 $a'_{i,j}$ 为 − 1~2 的整数。

表 1 基于身份的公钥加密体制效率对比

体制	n	lb q	主公钥尺寸/kbit	用户私钥尺寸/kbit	密文尺寸/kbit	加密时间/ms	解密时间/ms
DLP 体制	512	23	11.5	11.5	23.5	0.227	0.184
DLP2 体制	1 024	32	32	32	64	0.481	0.393
NIBE 体制	256	28	7	7	7.03	0.091	0.059

定义 $2bDecompt^{-1}(\boldsymbol{a}')=(\sum_{j=0}^{l-1}4^j a'_{0,j},\cdots,\sum_{j=0}^{l-1}4^j a'_{k-1,j})$。定义 $Flatten(\boldsymbol{a}')=2bDecompt(2bDecompt^{-1}(\boldsymbol{a}'))$。定义 $powersof4(\boldsymbol{y})=(y_0,4y_0,\cdots,4^{l-1}y_0,\cdots,y_{k-1},4y_{k-1},\cdots,4^{l-1}y_{k-1})$。

NIBFHE 体制包含 5 个多项式时间算法，具体描述如下所示。

参数生成算法 NIBFHE.*Setup*(n,q,L)。算法输入维数 n、模数 q 和最大计算深度 L，要求$\lceil \mathrm{lb}q \rceil$为奇数。调用 NIBE.*Setup* 算法生成主公钥 h 等公共参数、主私钥 $\boldsymbol{B}$，并输出公共参数。

私钥提取算法 NIBFHE.*Extract*($\boldsymbol{B}$,id)。算法调用 NIBE.*Extract* 算法生成并输出用户私钥 $\boldsymbol{sk}_{id}$。

加密算法 NIBFHE.*Enc*(id,m)。算法输入用户身份 id 和要加密的明文信息 $m\in\{0,1\}$，输出用 id 所对应的公钥对 m 加密所得的密文 $\boldsymbol{C}$。具体流程：首先调用 NIBE.*Encrypt* 算法生成 $N=\left\lceil \frac{\mathrm{lb}q}{2} \right\rceil(n+1)$ 个以 0 作为明文进行所得的密文，令 $\boldsymbol{C}'$ 为由这 N 个密文作为行向量排列而成的矩阵，输出 $\boldsymbol{C}=Flatten(m\boldsymbol{I}_N+2bDecomp(\boldsymbol{C}'))$。

解密算法 NIBFHE.*Dec*($\boldsymbol{sk}_{id}$,$\boldsymbol{C}$)。算法输入用户私钥 $\boldsymbol{sk}_{id}$ 和明文 m 对应的密文 $\boldsymbol{C}$，输出明文 m。具体流程：令 $\boldsymbol{sk}'_{id}=powerof4(\boldsymbol{sk}_{id})$，计算并输出 $m=\left\lfloor \frac{\langle \boldsymbol{c}_{N-2},\boldsymbol{sk}'_{id}\rangle}{\frac{q}{8}}+\frac{1}{2} \right\rfloor \bmod 2$。

同态加法算法 NIBFHE.*Add*($\boldsymbol{C}_1$,$\boldsymbol{C}_2$)。算法输入进行同态加法运算的密文 $\boldsymbol{C}_1$、$\boldsymbol{C}_2$，输出新密文 $\boldsymbol{C}=Flatten(\boldsymbol{C}_1+\boldsymbol{C}_2)$。

同态乘法算法 NIBFHE.*Mult*($\boldsymbol{C}_1$,$\boldsymbol{C}_2$)。算法输入进行同态乘法运算的密文 $\boldsymbol{C}_1$、$\boldsymbol{C}_2$，输出新密文 $\boldsymbol{C}=Flatten(\boldsymbol{C}_1\boldsymbol{C}_2)$。

4.2　正确性和安全性分析

首先考虑同态运算的正确性。对于同态加法，有 $\boldsymbol{C}=Flatten((m_1+m_2)\boldsymbol{I}_N+2bDecomp(\boldsymbol{C}'_1+\boldsymbol{C}'_2))$，NIBFHE.*Dec*$(\boldsymbol{sk}_{id},\boldsymbol{C})=(m_1+m_2)\bmod 2$。每次同态加法运算后，噪声不超过原密文的 2 倍。对于同态乘法，有 $\boldsymbol{C}\boldsymbol{sk}'_{id}=m_1m_2\boldsymbol{sk}'_{id}+m_2\boldsymbol{e}_1+\boldsymbol{C}_1\boldsymbol{e}_2$，NIBFHE.*Dec* $(\boldsymbol{sk}_{id},\boldsymbol{C})=m_1m_2$（其中，$\boldsymbol{e}_1$、$\boldsymbol{e}_2$ 表示密文 $\boldsymbol{C}_1$、$\boldsymbol{C}_2$ 中的噪声）。由于 m_2 的系数为 $\{0,1\}$，$\boldsymbol{C}_1$ 的所有系数都限制在 $[-1,2]$ 上，因此，每次同态乘法后，噪声不超过原密文的 2N+1 倍。

对于体制的正确性和安全性，有以下定理。

定理 5　如果 NIBE 体制满足以下 3 条性质，则 NIBFHE 体制是 IND-CPA 安全的 IBFHE 体制。

性质 1　对于用户身份 id，其用户私钥 $\boldsymbol{sk}_{id}$ 和用 id 对应的公钥所得的密文 $\boldsymbol{c}_{id}$ 是 $\mathbb{Z}_q^{n+1}$ 上的向量，且 $\boldsymbol{sk}_{id}$ 的第 1 个分量的系数为 1。

性质 2　解密正确性。如果 $\boldsymbol{c}$ 是加密 0 得到的密文，那么 $\left|\langle \boldsymbol{c},\boldsymbol{sk}_{id}\rangle\right|<\frac{q}{16(2N+1)^L}$。

性质 3　体制安全性。加密 0 得到的密文和 $\mathbb{Z}_q\times\mathbb{Z}_q^n$ 上的均匀分布不可区分。

证明　可以看出，$\boldsymbol{C}\cdot\boldsymbol{sk}'_{id}=m\cdot\boldsymbol{sk}'_{id}+\boldsymbol{C}'\cdot\boldsymbol{sk}_{id}$。根据性质 2，在进行不超过 L 次同态运算后，$\left|\boldsymbol{C}'\cdot\boldsymbol{sk}_{id}\right|$的所有分量均小于 $\frac{q}{16}$。因此，如果加密的消息为 0，那么 $\left\langle \boldsymbol{c}_{N-2},\boldsymbol{sk}'_{id}\right\rangle$ 距离 0 比 $\frac{q}{8}$ 近，否则情况相反，即可保证体制解密的正确性。如果存在破坏 NIBFHE 体制 CPA 安全的攻击者，那么该攻击者即可区分 $\boldsymbol{c}$ 和从 $\mathbb{Z}_q^{n+1}$ 上均匀分布取得的结果。因此，如果 NIBE 体制满足性质 3，那么 NIBFHE 体制就是 IND-CPA 安全的。

接下来，验证 NIBE 体制是否满足定理 5 中的 3 条性质。根据私钥的结构，体制满足性质 1 是显然的。对于加密 0 所得的密文，有 $\langle \boldsymbol{c},\boldsymbol{sk}_{id}\rangle=rs'+e_2-e_1s''$。因此，只要在参数选取时令 q 足够大即可满足性质 2。如果区分加密 0 的密文和 $\mathbb{Z}_q\times\mathbb{Z}_q^n$ 上的均匀分布的概率不可忽略，那么同样可以以不可忽略的概率攻击 NIBE 体制。又因为 NIBE 体制是 IND-ID-CPA 安全的，因此，可以满足性质 3。所以，NIBFHE 体制是 IND-CPA 安全的。

4.3　效率对比

将 NIBFHE 体制和现有的 2 种 IBFHE 体制，以及根据目前相关领域研究进展尚未提出但可能存在的 IBFHE 体制进行效率对比。可能的潜在体制为将这 2 种体制由基于 LWE 问题改为基于 RLWE 问题[3]，并利用 Lyubashevsky 等[19]提出的任意分圆环思想将 RLWE 问题中环的维度由 2 的方幂拓展为任意正整数（具有较小的系统参数，但计算效率较低），以及使用 Gentry 等的转化方式对 DLP2 体制和 NIBE 体制进行转化。令 $\gamma\leqslant1.007\,5$，区分攻击

优势 $\varepsilon = 2^{-32}$，解密错误率不超过 2^{-60}。由于体制的参数普遍较大，因此，时间分析均使用与 3.4 节相同设备的估计值。

从表 2 可以看出，前 4 个体制的运算密钥或密文尺寸较大，因此效率较差。如果同时使用 GSW 体制的转化方式，与基于 DLP2 的 IBFHE 体制相比，基于 NIBE 的体制的密钥尺寸减小了 89.64%，密文尺寸减小了 99.73%，加密时间缩短了 99.24%，解密时间缩短了 99.65%。利用本文提出的转化方式对 NIBE 进行转化，所得的 NIBFHE 体制的密钥尺寸仅增大了 5.17%，而密文尺寸减小了 42.86%，加密时间缩短了 45.29%，解密时间缩短了 42.07%，传输和计算效率有较大提升。

5 结束语

在全同态加密体制中，如何在保证安全性的条件下优化计算和传输效率是体制设计时所必须考虑的因素。本文提出了一个基于 NTRU 格的 IBE 体制，在与安全参数相关的根式埃尔米特因子 $\gamma \leqslant 1.007\,5$ 的条件下，与现有基于 NTRU 格的 IBE 体制相比，密钥尺寸缩小了至少 39.13%，密文尺寸减小了至少 70.10%，加解密时间缩短了至少 59.91%。利用该 IBE 体制构造的 IBFHE 体制的密钥和密文尺寸从 Gbit、Tbit 级减小到 Mbit 级，优势明显。此外，本文提出了一种通过 IBE 体制构造 IBFHE 体制的转化方法，与现有转化方法相比可以有效减小密文尺寸。由于本体制的密文的代数结构为整数模环上元素，因此，NIBFHE 体制是基于 LWE 问题的一般格进行构造的。如果可以构造基于 RLWE 问题或 NTRU 格的转换方式，则可以进一步优化包括密文尺寸在内的参数的大小。

参考文献：

[1] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169-180.

[2] GENTRY C. Fully homomorphic encryption using ideal lattices[C]// 41st Annual ACM Symposium on Theory of Computing (STOC 2009), Bethesda, USA. 2009: 169-178.

[3] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[J]. Journal of the ACM, 2013, 60(6): 43-65.

[4] BRAKERSKI Z, VAIKUNTANATHAN V. Efficient fully homomorphic encryption from (standard) LWE[J]. SIAM Journal on Computing, 2014, 43(2): 831-871.

[5] TREPACHEVA A, BABENKO L. Known plaintexts attack on polynomial based homomorphic encryption[C]//7th International Conference on Security of Information and Networks (SIN 2014), Glasgow, UK. 2014.

[6] YASUDA M, SHIMOYAMA T, KOGURE J, et al. Secure statistical analysis using RLWE-based homomorphic encryption[C]//20th Australasian Conference on Information Security and Privacy (ACISP 2015), QUT, Australia. 2015: 471-487.

[7] 汤殿华, 祝世雄, 王林, 等. 基于 RLWE 的全同态加密方案[J]. 通信学报, 2014, 35(1): 173-182.
TANG D H, ZHU S X, WANG L, et al. Fully homomorphic encryption scheme from RLWE[J]. Journal on Communications, 2014, 35(1): 173-182.

[8] SHAMIR A. Identity-based cryptosystems and signature schemes[C]// CRYPTO '84, Santa Barbara, California, USA. 1984: 47-53.

[9] 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.

[10] GENTRY C, SAHAI A, WATERS B. Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based[C]//33rd Annual International Cryptology Conference (CRYPTO 2013), Santa Barbara, CA, USA, 2013: 75-92.

[11] HOFFSTEIN J, PIPHER J, SILVERMAN J H. NTRU: a ring-based public key cryptosystem[C]//ANTS III, Portland, Oregon, USA. 1998: 267-288.

表 2 **基于身份的全同态加密体制效率对比**

体制	n	lb q	主公钥尺寸	用户私钥尺寸	密文尺寸	运算密钥尺寸	加密时间	解密时间
GZF	927	41	2.69 Gbit	5.94 Mbit	2.97 Mbit	1.22 Tbit	3.12 s	9.01 ms
GZF+任意环	944	42	3.18 Mbit	6.35 Mbit	3.21 Mbit	481.81 Gbit	12.09 ms	8.67 ms
GSW	1 040	47	4.45 Gbit	4.38 Mbit	19.61 Tbit	0	33.24 d	5.18 h
GSW+任意环	1 608	70	329.77 kbit	439.69 kbit	188.79 Gbit	0	13.69 min	2.97 min
GSW+DLP2	2 048	70	140 kbit	280 kbit	76.56 Gbit	0	3.46 min	1.20 min
GSW+NIBE	256	58	14.5 kbit	14.56 kbit	211.90 Mbit	0	1.57 s	0.25 s
NIBFHE	256	61	15.25 kbit	15.31 kbit	121.07 Mbit	0	0.86 s	0.15 s

[12] DUCAS L, DURMUS A, LEPOINT T, et al. Lattice signatures and bimodal Gaussians[C]//33rd Annual International Cryptology Conference (CRYPTO 2013), Santa Barbara, CA, USA. 2013: 40-56.

[13] PEIKERT C. Lattice cryptography for the internet[C]//6th International Conference on Post-Quantum Cryptography (PQCrypto 2014). Waterloo, ON, Canada. 2014: 197-219.

[14] LÓPEZ-ALT A, TROMER E, VAIKUNTANATHAN V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption[C]//44th Annual ACM Symposium on Theory of Computing (STOC 2012). Portland, USA, 2012: 1219-1234.

[15] DUCAS L, LYUBASHEVSKY V, PREST T. Efficient identity-based encryption over NTRU lattices[C]//20th Annual International Conference on the Theory and Application of Cryptology and Information Security (AsiaCrypt 2014), Kaohsiung, Taiwan (R.O.C.). 2014: 22-41.

[16] ALBRECHT M R, FAUGERE J C, FITZPATRICK R, et al. Lazy modulus switching for the BKW algorithm on LWE[C]//17th IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC 2014). Buenos Aires, Argentina, 2014: 429-445.

[17] KIRCHNER P, FOUQUE P A. An improved BKW algorithm for LWE with applications to cryptography and lattices[C]//35th Annual International Cryptology Conference (CRYPTO 2015). Santa Barbara, CA, USA, 2015: 43-62.

[18] LYUBASHEVSKY V, PREST T. Quadratic time, linear space algorithms for gram-schmidt orthogonalization and gaussian sampling in structured lattices[C]//34th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EuroCrypt 2015). Sofia, Bulgaria, 2015: 789-815.

[19] LYUBASHEVSKY V, PEIKERT C, REGEV O. A toolkit for ring-LWE cryptography[C]//32rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (Euro Crypt2013). Athens, Greece, 2013: 35-54.

[20] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM (JACM), 2009, 56(6): 34-43.

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

[22] DUCAS L, NGUYEN P Q. Faster Gaussian lattice sampling using lazy floating-point arithmetic[C]//18th Annual International Conference on the Theory and Application of Cryptology and Information Security (AsiaCrypt 2012). Beijing, China, 2012: 415-432.

[23] GAMA N, NGUYEN P Q. Predicting lattice reduction[C]//27th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EuroCrypt 2008). Istanbul, Turkey, 2008: 31-51.

[24] MICCIANCIO D. Lattice-based cryptography[M]. US: Encyclopedia of Cryptography and Security, 2011.

作者简介：

段然（1989-），男，山西大同人，信息工程大学博士生，主要研究方向为格密码理论、全同态加密。

顾纯祥（1976-），男，安徽霍山人，信息工程大学教授、硕士生导师，主要研究方向为密码学。

祝跃飞（1962-），男，浙江杭州人，信息工程大学教授、博士生导师，主要研究方向为密码学、网络与信息安全。

郑永辉（1976-），男，江西乐平人，信息工程大学副教授，主要研究方向为密码学。

陈莉（1968-），女，江苏如皋人，河南财经政法大学教授，主要研究方向为信息安全理论与技术。