一种 NTRU 格上基于身份全同态加密体制设计

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: 全同态加密可以用来解决云计算环境中的隐私保护问题,然而现有体制具有系统参数大、效率低的缺点. 针对现有攻击技术,首先设计了一种高效的 NTRU 格上的基于身份公钥加密体制,无需借助额外的安全性假设,具有更高的安全性和更小的系统参数. 之后,基于近似特征向量技术,构造了一种高效的全同态加密转化方式. 通过将以上两种方法结合,给出了一种高效的基于身份全同态加密体制. 和现有体制相比,除了不需要计算密钥、实现了真正意义上的基于身份特性以外,还减小了密钥、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; 环上带错学习问题; NTRU 格; 近似特征向量
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112 (2018)10-2410-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.10.014

An Identity-Based Fully Homomorphic Encryption Over NTRU Lattice

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

Abstract: Fully homomorphic encryption can be used to solve privacy concerns for data over cloud, while large parameters and low efficiency are the universal issues for present schemes. To oppose mainstream attacks, an identity-based public key scheme over NTRU lattice with smaller parameters, higher security level, and without additional security assumptions is put forward. Take advantage of the approximate eigenvector technique, an efficient fully homomorphic encryption transformation method is raised. And by combining the two skills above, an efficient identity-based fully homomorphic encryption scheme is proposed. Compared with existing schemes, the schemes is fully identity-based without evaluation key, and has smaller keys and ciphertext sizes, leading to higher transmission and computational efficiency.

Key words: fully homomorphic encryption; identity-based encryption; learning with errors over rings; number theory research unit (NTRU) lattice; approximate eigenvector

1 引言

全同态加密(FHE, Fully Homomorphic Encryption)是一种新型加密技术,除了满足一般公钥加密性质,还可以通过对密文进行运算操作,实现对相应明文的相应运算. 该技术可以用于实现隐私保护,进行安全多方计算等. 2009 年,Gentry 基于理想格上的困难问题给出了第一个全同态加密体制[1]. 在此以后,学术界又提出了基于不同代数结构的全同态体制[2~5],对相关领域的研究也在不断发展[6~13].

目前,全同态体制存在的一个较大的问题是密钥尺寸较大,从而在密钥管理上的开销较大,影响体制的效率. 通过引入基于身份加密(IBE, Identity-Based Encryption)的理念,用户公钥可以通过身份标识信息计算获得,可以有效解决这一问题. 目前基于身份的全同态体制(IBFHE, Identity-Based Fully Homomorphic Encryption)的构造方式主要分为两类:第一类以光焱等人在 2014 年提出的体制[14,15](记作 GZF 体制)为代表,体制

收稿日期:2017-06-15;修回日期: 2017-11-01;责任编辑:孙瑶
基金项目:国家自然科学基金(No. 61502533);河南省科技创新杰出青年基金(No. 134100510002);河南省高校科技创新人才支持计划(No. 13HASTIT043);河南省基础与前沿技术研究(No. 142300410002);河南省自然科学基金(No. 162300410335)

在密文运算中需要引入运算密钥防止密文尺寸不断增大.该密钥须使用用户私钥产生,并非真正意义上的IBFHE体制,且这类体制的运算密钥尺寸较大.第二类以Gentry等人在2013年利用近似特征向量技术提出的体制[16](记作GSW体制)为代表,体制的最大特点是无需运算密钥,但体制的密文尺寸较大.

NTRU算法由Hoffstein等人提出[17],被认为具有与求解特定格上困难问题难度相当的安全性[18,19].2014年,Ducas等人提出了一种基于NTRU的IBE体制(记作DLP体制)[20],具有较小的密文尺寸和较高的计算效率.但为了保证安全性,体制在进行加解密过程中使用了密钥封装技术,从而使密文不具有同态性,无法构造FHE体制.

本文首先提出了一个高效的NTRU格上的IBE体制,与DLP体制相比,密钥、密文尺寸减小了52.13%,且安全性更高.之后,基于近似特征向量技术,本文构造了一种将IBE体制转化为IBFHE体制的方法,与GSW体制中的转化方式相比,密文尺寸减小了83.28%.通过将两种思路结合,本文给出了基于NTRU格的IBFHE体制.与现有体制相比,密钥、密文尺寸显著减小.在随机谕示模型下,基于环上带错学习问题(RLWE,Learning With Errors over Rings)和NTRU问题困难性,体制在选择明文和适应性选择身份攻击下具有不可区分性(IND-ID-CPA安全).

2　预备知识

2.1　符号定义

本文符号统一如下:$\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{Z}_q$分别表示整数集,有理数集,实数集,整数模$q$剩余类环.对于$n$次多项式$f(x)$,$\mathcal{R}$表示多项式环$\mathbb{Z}[x]/f(x)$,$\mathcal{R}'$表示多项式环$\mathbb{Q}[x]/f(x)$,$\mathcal{R}_q$表示环$\mathbb{Z}_q[x]/f(x)$.定义$n$维向量$\boldsymbol{a}$的长度为其欧几里德范$\|\boldsymbol{a}\|=\sqrt{\sum_{i=1}^{n}a_i^2}$,定义向量集$\boldsymbol{S}$的长度$\|\boldsymbol{S}\|=\max_{\boldsymbol{a}\in\boldsymbol{S}}\|\boldsymbol{a}\|$.$x\leftarrow\mathcal{D}$表示从概率分布$\mathcal{D}$中随机选取变量$x$,$x\xleftarrow{R}A$表示从集合$A$中随机均匀选取变量$x$.向量$\boldsymbol{a}\in\mathbb{Z}_q^n$可表示为$\boldsymbol{a}=(a_1,\cdots,a_n)$;多项式$b\in\mathcal{R}_q$可表示为$b=(b_1,\cdots,b_n)$,$\mathcal{R}_q$上的多项式和$\mathbb{Z}_q^n$上的向量可以通过系数对应的方式相互转化.矩阵$\boldsymbol{C}$的第$i$行用$\boldsymbol{c}_i$表示,$\boldsymbol{I}_n$表示$n$维单位矩阵.$\varphi(\cdot)$表示欧拉函数.对于多项式$b,c\in\mathcal{R}$,定义$b*c=bc\bmod(x^n+1)$.$\log n$表示$\log_2 n$.

除了常用的计算复杂度符号以外,本文还定义了$\mathrm{poly}(\cdot)$:如果存在常数c使得$f(n)=O(n^c)$,则$f(n)$可表示为$\mathrm{poly}(n)$.

2.2　NTRU格

NTRU格在密码学中具有广泛的应用,具有结构较为特殊和运算效率较高等特点.

定义1[21]　对于m维欧氏空间$\mathbb{R}^m$,给定n个线性无关向量$\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n\in\mathbb{R}^m$,由这些向量作为格基生成的格$\Lambda$,记作$\mathcal{L}(\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n)$或$\mathcal{L}(\boldsymbol{B})$,定义为

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

对于格基$\boldsymbol{B}$,定义$\boldsymbol{B}^*$为$\boldsymbol{B}$的格拉姆施密特正交化矩阵.这两个矩阵满足

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

其中$\mu_{i,j}=\dfrac{\langle\boldsymbol{b}_i,\boldsymbol{b}_j^*\rangle}{\langle\boldsymbol{b}_j^*,\boldsymbol{b}_j^*\rangle}$.

对于格$\mathcal{L}(\boldsymbol{B})$,将格$\Lambda^{\perp}(\boldsymbol{B})$定义为$\Lambda^{\perp}(\boldsymbol{B})=\{\boldsymbol{e}\in\mathbb{Z}^m\mid\boldsymbol{B}\cdot\boldsymbol{e}=\boldsymbol{0}\bmod q\}$.

定义2[22]　对于正整数n,q,令$f,g,F,G\in\mathcal{R}$满足$f*G-g*F=q$.由f,g,F,G生成的NTRU格是指将如下矩阵的列向量作为格基生成的格

$$\begin{pmatrix}\mathcal{M}(f) & -\mathcal{M}(g)\\ \mathcal{M}(F) & -\mathcal{M}(G)\end{pmatrix}$$

其中$\mathcal{M}(\cdot)$是$n\times n$维的反循环矩阵,如

$$\mathcal{M}(f)=\begin{pmatrix}f_1 & f_2 & f_3 & \cdots & f_n\\ -f_n & f_1 & f_2 & \cdots & f_{n-1}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ -f_2 & -f_3 & -f_4 & \cdots & f_1\end{pmatrix}.$$

2.3　环上带错学习问题

RLWE问题是一种格上困难问题,最早由Lyubashevsky等人于2010年提出.该问题的判定性问题记作DRLWE问题(Decisional-RLWE).

对于正整数m,在$\mathbb{Q}$中添加m次本原单位根ξ_m所得到的域扩张$\mathcal{K}=\mathbb{Q}(\xi_m)$称为$m$次分圆数域.令$n=\varphi(m)$,当$m$为2的方幂时,$n=m/2$,此时$\mathcal{K}$上的整数环$\mathbb{Z}[\xi_m]\cong\mathbb{Z}[x]/(x^n+1)$.

定义3[14]　对于正整数n,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$\sigma>0$,定义

$$\rho_{\sigma,\boldsymbol{c}}(x)=\mathrm{e}^{\frac{-\pi\|x-\boldsymbol{c}\|^2}{\sigma^2}}$$

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

将格Λ上以$\boldsymbol{c}$为中心,参数为σ的离散高斯分布$\mathcal{D}_{\Lambda,\sigma,\boldsymbol{c}}(\cdot)$表示为

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

当$\boldsymbol{c}=\boldsymbol{0}$时,该分布简写为$\mathcal{D}_{\Lambda,\sigma}$,也可称作$\mathbb{R}^n$上的错误分布,记作$\chi$.

下面给出与RLWE问题相关的定义.

定义4[18]　对于正整数$n,q=\mathrm{poly}(n)$,"秘密值"$s\in\mathcal{R}_q$,以及$\mathbb{Z}^n$上的误差分布χ,RLWE分布定义为在$\mathcal{R}_q$

$\times \mathcal{R}_q$ 上的满足$(a, a\cdot s+e)$形式的概率分布 $A_{s,\chi}$，其中 $a \xleftarrow{R} \mathcal{R}_q, e \leftarrow \chi$. $(a, a\cdot s+e)$称为 RLWE 分布的一个实例. 在给出 l 个实例的情况下求解 s 的问题称为 l - RLWE$_{q,n,\chi}$问题.

定义 5[18] 对于正整数 $n, q=\mathrm{poly}(n)$，以及$\mathbb{Z}^n$上的误差分布 χ，DRLWE $_{q,n,\chi}$问题的目标是区分如下两个分布.

分布 1：输出$(a,b) \leftarrow A_{s,\chi} \in \mathcal{R}_q \times \mathcal{R}_q$.

分布 2：输出$(a,b) \xleftarrow{R} \mathcal{R}_q \times \mathcal{R}_q$.

如果存在在给出 l 个实例的情况下以不可忽略的优势求解 DRLWE $_{q,n,\chi}$问题的多项式时间算法，那么称 l-DRLWE $_{q,n,\chi}$问题是简单的；否则认为问题是困难的. 如果该问题是困难的，那么称 l-DRLWE $_{q,n,\chi}$假设成立.

Lyubashevsky 等人在文献[18,23]中给出了从理想格上近似最短向量问题(Approx SVP, Approximate Shortest Vector Problem)的最坏情况到 DRLWE 问题一般情况的量子归约.

2.4 离散高斯采样函数

Lyubashevsky 等人于 2015 年提出了一种高效的从离散高斯分布上采样的算法[22].

定理 1[22] 存在可以进行如下运算的多项式时间算法 CGS：输入格基 $\boldsymbol{B}=\{\boldsymbol{b}_1,\cdots,\boldsymbol{b}_n\}$，中心 $\boldsymbol{c}$，以及高斯参数 σ，输出从 $\mathcal{D}_{\Lambda(\boldsymbol{B}),\sigma,\boldsymbol{c}}$上采样的结果 $\boldsymbol{z}$.

该算法的输出满足如下命题：

命题 1[24] 对于任意的 $\varepsilon < 2^{-\lambda}/(4n)$，如果 $\sigma \geqslant \|\boldsymbol{B}^*\| \cdot \frac{1}{\pi}\sqrt{\frac{1}{2}\ln\left(2+\frac{2}{\varepsilon}\right)}$，那么 CGS 算法的输出与分布 $\mathcal{D}_{\Lambda(\boldsymbol{B}),\sigma,\boldsymbol{c}}$的统计距离不超过 $2^{-\lambda}$.

3 高效的 NTRU 上基于身份的公钥加密体制设计

本节通过对 Ducas 等人提出的 IBE 体制[20]中的加解密算法进行修改，提出了参数更小、效率更高的基于 NTRU 体制的 IBE 体制.

3.1 体制设计

我们首先给出 DLP 体制的参数生成和私钥提取算法.

定义 $x' \in \mathcal{R}'$满足 $\mathcal{M}(x') = \mathcal{M}(x)^{\mathrm{T}}$.

参数生成算法 DLP. Keygen(n,q). 输入多项式环的次数 n 和模数 q，输出主公钥 h 和主私钥 $\boldsymbol{B}$，以及哈希函数 $H:\{0,1\}^* \to \mathbb{Z}_q^n$、$H':\{0,1\}^n \to \{0,1\}^n$. 算法过程如下：

步骤 1 计算 $\sigma_f = 1.17\sqrt{\frac{q}{(2n)}}$；

步骤 2 从分布 $\mathcal{D}_{\mathbb{Z}^n,\rho_f,\sigma_c}$中采样 $f,g \leftarrow \mathcal{D}_{\mathbb{Z}^n,\rho_f,\sigma_c}$，如果

$$\max\left(\|(g,-f)\|, \left\|\left(\frac{qf'}{f*f'+g*g'}, \frac{qg'}{f*f'+g*g'}\right)\right\|\right) > \sqrt{2n}\cdot\sigma,$$

则重新进行采样；

步骤 3 使用扩展欧几里德算法，计算 $r_f, r_g \in \mathcal{R}$，$R_f, R_g \in \mathbb{Z}$使得 $r_f \cdot f = R_f \bmod (x^n+1)$，$r_g \cdot g = R_g \bmod (x^n+1)$. 如果 $\mathrm{GCD}(R_f, R_g) \neq 1$ 或 $\mathrm{GCD}(R_f, q) \neq 1$，则返回步骤 2；

步骤 4 计算 $t_f, t_g \in \mathbb{Z}$使得 $t_f \cdot R_f + t_g \cdot R_g = 1$；

步骤 5 计算 $X = qt_g r_g$，$Y = -qt_f r_g$，$k = \left\lfloor \frac{X*f'+Y*g'}{f*f'+g*g'} + 0.5 \right\rfloor \in \mathcal{R}$，$F = X - k*f$，$G = Y - k*g$；

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

私钥提取算法 DLP. Extract$(\boldsymbol{B}, id)$. 输入主私钥 $\boldsymbol{B}$ 和用户身份 $id \in \{0,1\}^*$，输出用户私钥 sk_{id}：首先检查输入 id 是否在存储列表中. 如果存在，则返回与 id 对应的 sk_{id}. 否则，计算用户公钥 $t \leftarrow H(id)$，调用 CGS 算法采样$(s_1, s_2) \leftarrow (t,0) - \mathrm{CGS}(\boldsymbol{B}, (t,0))$，此时 s_1, s_2 满足 $s_1 + s_2 * h = t$. 将 s_2 作为用户私钥和 id 存储在列表中，然后输出 s_2.

Ducas 等人指出[20]，DLP. Extract$(\boldsymbol{B}, id)$ 算法得到的(s_1, s_2)与 $\sigma_3 = 1.17\|\boldsymbol{B}^*\| \cdot \frac{1}{\pi}\sqrt{\frac{1}{2}\ln\left(2+\frac{2}{\varepsilon}\right)}$的分布 $\mathcal{D}_{\mathbb{Z}^n,\sigma_3}$是统计不可区分的.

然后我们构造如下的 IBE 体制，记作 NE 体制. 体制包含参数生成算法、私钥提取算法、加密算法和解密算法四个多项式时间算法.

参数生成算法 NE. Setup(n,q). 输入多项式环的次数 n 和模数 q，调用 DLP. Keygen(n,q) 算法输出主公钥 h 和主私钥 $\boldsymbol{B}$.

私钥提取算法 NE. Extract$(\boldsymbol{B}, id)$. 输入主私钥 $\boldsymbol{B}$ 和用户身份 $id \in \{0,1\}^*$，调用 DLP. Extract$(\boldsymbol{B}, id)$ 算法得到用户私钥 sk_{id}.

加密算法 NE. Enc(id, μ). 算法输入用户身份 id 和明文 $\mu \in \mathcal{R}_2$，输出用户公钥 t 对 μ 加密的密文 c：计算 $t \leftarrow H(id)$. 从 $\{-1,0,1\}^n$ 上均匀随机选取 r, e_1，从参数为 σ 的离散高斯分布 χ 上选取 e_2，从 $\{0,1\}^n$ 上均匀随机选取 k，计算 $u = r*h + e_1 \in \mathcal{R}_q$，$v = r*t + e_2 + \lfloor q/2 \rfloor \cdot k \in \mathcal{R}_q$. 输出 $c = (u, v, \mu \oplus H'(k)) \in \mathcal{R}_q \times \mathcal{R}_q \times \mathcal{R}_2$.

解密算法 NE. Dec(sk_{id}, c)：算法输入用户私钥 sk_{id} 和明文 μ 对应的密文 $\boldsymbol{c} = (u, v, w)$，计算 $w' = v - u *$

$sk_{id}, k = \lfloor 2w'/q + 0.5 \rfloor$,输出明文 $\mu = w \oplus H'(k)$.

解密正确性:由于 $s_1 + s_2 * h = t$,所以有

$$\begin{aligned} v - u * s_2 &= r * t + e_2 - (r * h + e_1) * s_2 \\ &= \lfloor q/2 \rfloor \cdot k + (r * s_1 + e_2 - e_1 * s_2) \end{aligned}$$

当 w'的所有系数都在区间$(-q/4, q/4)$以内时,解密算法可以正确得到 k,从而恢复明文. 系统参数的具体取值将在 3.3 节进行分析.

体制安全性:与 DLP 体制类似,体制的安全性有如下结论.

命题 2[18]　设系统参数 $n = \text{poly}(\lambda), q = \text{poly}(\lambda)$为安全参数 λ 的多项式,如果 NTRU 问题是困难的,1-DRLWE$_{q,n,\chi_1}$和 1-DRLWE$_{q,n,\chi_2}$假设成立,且 H'为安全级别不低于 λ 比特的抗碰撞哈希函数,那么 NE 体制在随机谕示模型下是 IND-ID-CPA 安全的.

3.2　高效的不使用密钥封装技术的基于身份公钥加密体制

我们在本小节中对体制的密钥、密文结构和加解密流程进行修改,以得到可以通过 GSW 方式转化为 IBFHE 体制的 IBE 体制(记作 NE2 体制). 与 DLP 体制通过类似方式修改得到的体制(记作 DLP2 体制)相比,体制的参数更小,效率更高.

NE2 体制包含参数生成、私钥提取、加密和解密四个多项式时间算法.

参数生成算法 NE2. Setup(n, q). 输入维数 n 和模数 q,调用 DLP. Keygen(n, q)算法输出主公钥 h 和主私钥 $\boldsymbol{B}$.

私钥提取算法 NE2. Extract$(\boldsymbol{B}, id)$. 输入主私钥 $\boldsymbol{B}$ 和用户身份 $id \in \{0,1\}^*$,调用 DLP. Keygen(n, q)算法得到(s_1, s_2),用户私钥 $\boldsymbol{sk}_{id} = (-s_2, 1) \in \mathcal{R}_q^2$.

加密算法 NE2. Enc(id, μ). 算法输入用户身份 id 和要加密的明文信息 $\mu \in \mathcal{R}_2$,输出用户公钥 t 对 μ 加密的密文 $\boldsymbol{c}$:计算 $t \leftarrow H(id)$. 从参数为 σ_1 的离散高斯分布 χ_1 上选取 r, e_2,从参数为 σ_2 的离散高斯分布 χ_2 上选取 e_1,计算 $u = r * h + e_1 \in \mathcal{R}_q, v = r * t + e_2 + \lfloor q/2 \rfloor \cdot \mu \in \mathcal{R}_q$. 输出 $\boldsymbol{c} = (u, v) \in \mathcal{R}_q^2$.

解密算法 NE2. Dec$(\boldsymbol{sk}_{id}, \boldsymbol{c})$. 输入用户私钥 $\boldsymbol{sk}_{id}$ 和明文 μ 对应的密文 $\boldsymbol{c} = (u, v)$,计算 $w = <\boldsymbol{sk}_{id}, \boldsymbol{c}>$,输出明文 $\mu = \lfloor 2w/q + 0.5 \rfloor$.

解密正确性与 NE 体制相同.

我们通过如下定理证明体制的 IND-ID-CPA 安全性.

定理 3　设系统参数 $n = \text{poly}(\lambda), q = \text{poly}(\lambda)$为安全参数 λ 的多项式,如果 NTRU 问题是困难的,1-DRLWE$_{q,n,\chi_1}$,1-DRLWE$_{q,n,\chi_2}$,1-DRLWE$_{q,n,\chi_3}$假设均成立,那么 NE2 体制在随机谕示模型下是 IND-ID-CPA 安全的.

证明　根据 NTRU 问题困难性,主公钥 h 与上的均匀分布不可区分.

如果攻击者可以破坏体制的 IND-CPA 安全性,那么攻击者就可以区分(h, t, u, v)和 $\mathcal{R}_q^4$ 上的均匀分布.

从私钥提取算法和加密算法的过程可以看出,区分(h, t)和 $\mathcal{R}_q^2$ 上的均匀分布、(h, u)和 $\mathcal{R}_q^2$ 上的均匀分布、(t, v)和 $\mathcal{R}_q^2$ 上的均匀分布分别等价于求解 1-DRLWE$_{q,n,\chi_3}$、1-DRLWE$_{q,n,\chi_1}$、1-DRLWE$_{q,n,\chi_2}$问题. 因此如果 1-DRLWE$_{q,n,\chi_1}$,1-DRLWE$_{q,n,\chi_2}$,1-DRLWE$_{q,n,\chi_3}$假设均成立,那么 NE2 体制是 IND-CPA 安全的.

又因为 NE2 体制的参数生成算法、私钥提取算法、以及用户公钥的生成方法均与 DLP 体制相同,因此可以用与该体制相同的方法证明 NE2 体制在随机谕示模型下的 IND-ID-CPA 安全性.

3.3　参数选取和效率对比

在本小节中,我们对 NE、NE2 体制的进行参数选取.

命题 2、定理 3 给出了体制 IND-ID-CPA 安全的结论,下面我们结合目前对格上密码体制和格上困难问题求解算法的研究进展[25~27],利用根式埃尔米特因子对体制的安全性进行刻画,确定体制的参数.

与 DLP 体制相似,攻击本文体制的方法为攻击主公钥、用户私钥以及体制的 IND-CPA 安全性. 除了对于 NE2 体制的 IND-CPA 安全性我们选用了效率更高的 Lindner 等人提出的解码攻击[28,29]外,其他攻击方法的分析与文献[20]中相同. 对于解码攻击,令攻击的优势 $\varepsilon = 2^{-32}$.

安全参数是在使用基于"极限裁剪"技术的枚举算法[30]和"最近邻居搜索"技术的筛法[31]的 BKZ2.0 算法[32]和 PBKZ 算法[33]作为格基约减算法时的结果[34]. 令解密错误率不超过 2^{-60}. 我们使用 CPU 为 i7-4790(3.6GHz)、内存为 16GB 的台式计算机对基于 NTL 库和 GMP 库的算法的效率进行评估. 这两个库可以对文中参数选取条件下的所有体制进行有效实现. 我们用 *mpk*, *skid*, *ci*, *evk*, *enc*, *dec* 表示主公钥尺寸、用户私钥尺寸、密文尺寸、运算密钥尺寸、加密时间、解密时间.

表 1　IBE 体制效率对比

体制	n	log$q$	*mpk*	*skid*	*ci*	*enc*	*dec*	λ
DLP	512	23	11.5KB	11.5KB	23.5KB	214μs	173μs	83
NE	256	22	5.5KB	5.5KB	11.25KB	98μs	79μs	91
DLP2	1024	41	41KB	41KB	82KB	506μs	412μs	107
NE2	512	40	20KB	20KB	40KB	237μs	189μs	111

从表 1 可知,NE、NE2 体制的密钥、密文尺寸、加解密时间比 DLP、DLP2 体制小 52.13% ~54.35%,安全性高 4~8 比特,因此在各方面均优于 Ducas 等人的体制. 利用 NE2 体制,我们可以构造具有较小参数的 IBFHE

体制. 下面给出利用 Gentry 等人的构造方式[16]对两种 IBE 体制进行转化所得的 IBFHE 体制进行参数对比(如表 2 所示).

表 2 基于不同 IBE 的 IBFHE 体制效率对比

体制	n	log$q$	*mpk*	*skid*	*ci*	*enc*	*dec*
DLP2	4096	97	388KB	776KB	147.02MB	354ms	132ms
NE2	2048	93	186KB	372KB	67.57MB	159ms	61ms

与基于 DLP2 的 IBFHE 体制相比,使用 NE2 体制优势明显.

4 高效的基于近似特征向量技术的全同态加密转化方法设计

Gentry 等人于 2013 年提出了一种基于近似特征向量技术和 LWE 问题的 IBFHE 体制[16],体制的最大特点是在同态运算中无需使用运算密钥,但密文尺寸较大. 本节通过对后一体制作适当修改,提出的一种使得密文尺寸更小的将 IBE 体制转化为 IBFHE 体制的方法,记作 NF 体制. 该体制还可以通过与 NE2 体制结合进一步优化系统参数、提高效率.

4.1 体制设计

首先,我们定义如下几个函数.

对于$\mathbb{Z}_q^k$上的向量$\boldsymbol{a},\boldsymbol{b}$,$p$ 为 2 的方幂,$l=\lceil \log q/\log p\rceil$,$N=kl$. 将向量 $\boldsymbol{a}$ 的分量 a_i 以 p 进制形式表示为 $a_i=\sum_{j=1}^{\lceil \log_p q\rceil} a_{i,j}p^i$,其中 $a_{i,j}\in\mathbb{Z}_p$,函数 pDecompt($\boldsymbol{a}$)的结果为 N 维向量 $\boldsymbol{a}'=(a_{1,0},\cdots,a_{1,l-1},\cdots,a_{k,0},\cdots,a_{k,l-1})\in\mathbb{Z}_p^N$.

定义函数

$$\text{pDecompt}^{-1}(\boldsymbol{a}')=\left(\sum p^j\cdot a_{0,j},\cdots,\sum p^j\cdot a_{k-1,j}\right).$$

定义函数

$$\text{pFlatten}(\boldsymbol{a}')=\text{pDecompt}(\text{pDecompt}^{-1}(\boldsymbol{a}')).$$

定义函数

$$\text{powersofp}(\boldsymbol{b})=(b_1,pb_1,\cdots,p^{l-1}b_1,\cdots,b_k,pb_k,\cdots,p^{l-1}b_k).$$

NF 体制的具体描述如下.

参数生成算法 NF. Setup(n,q,d). 输入维数 n、模数 q 和最大计算深度 d,调用 IBE 体制的参数生成算法生成并输出主公钥 *mpk* 和主私钥 *msk*.

私钥提取算法 NF. Extract(*msk*,*id*). 输入主私钥 *msk* 和用户身份 *id*,调用 IBE 体制的私钥提取算法生成并输出用户私钥 sk_{id}.

加密算法 NF. Enc(id,μ). 输入用户身份 *id* 和明文 $\mu\in\{0,1\}$,通过如下操作输出密文 $\boldsymbol{C}$:调用 IBE 体制的加密算法得到 $N=2l$ 个对 0 进行加密的密文,以这 N 个密文为列向量得到 $N\times N$ 的矩阵 $\boldsymbol{C}'$,输出密文 $\boldsymbol{C}=\text{pFlatten}(\mu\cdot\boldsymbol{I}_N+\text{pDecomp}(\boldsymbol{C}'))$.

解密算法 NF. Dec($\boldsymbol{sk}_{id},\boldsymbol{C}$). 输入用户私钥 $\boldsymbol{sk}_{id}$和明文 μ 对应的密文 $\boldsymbol{C}$,令 $\boldsymbol{s}_{id}=\text{powerofp}(\boldsymbol{sk}_{id})$,输出明文 $\mu=\lfloor 2\langle \boldsymbol{c}_{N-1},\boldsymbol{s}_{id}\rangle/q+0.5\rfloor$.

同态加法算法 NF. Add($\boldsymbol{C}_1,\boldsymbol{C}_2$). 输入密文 $\boldsymbol{C}_1,\boldsymbol{C}_2$,输出同态加法后的密文 $\boldsymbol{C}=\text{pFlatten}(\boldsymbol{C}_1+\boldsymbol{C}_2)$.

同态乘法算法 NF. Mult($\boldsymbol{C}_1,\boldsymbol{C}_2$). 输入密文 $\boldsymbol{C}_1,\boldsymbol{C}_2$,输出同态加法后的密文 $\boldsymbol{C}=\text{pFlatten}(\boldsymbol{C}_1\cdot\boldsymbol{C}_2)$.

4.2 正确性和安全性分析

对于体制的正确性和安全性,与原转化方法相似,我们用如下定理刻画.

定理 4 如果所基于的 IBE 体制满足如下三条性质,则 NF 体制是 IND-CPA 安全的 IBFHE 体制:

(1)对于用户 *id*,用户私钥 $\boldsymbol{sk}_{id}$和加密所得的密文 $\boldsymbol{c}_{id}$是 $\mathcal{R}_q^2$ 上的向量,且 $\boldsymbol{sk}_{id}$的第二项为 1;

(2)正确性:如果 $\boldsymbol{c}$ 是使用 *id* 对应的公钥对 0 加密所得的密文,令 $E=n\cdot((N-1)\cdot p/2+2^{1+\log q \bmod \log p})+1$,那么$|\langle \boldsymbol{c},\boldsymbol{sk}_{id}\rangle|\cdot 4p(E+1)^d<q$;

(3)安全性:对 0 进行加密所得的密文与 $\mathcal{R}_q^2$ 上的均匀分布是不可区分的.

证明 通过加解密流程,有 $\boldsymbol{C}\cdot\boldsymbol{sk}_{id}=\mu\cdot\text{pDecompt}^{-1}(\boldsymbol{sk}_{id})+\boldsymbol{C}'\cdot\boldsymbol{sk}_{id}$. 如果满足性质 2,那么在进行 d 次同态运算后,$|\boldsymbol{C}'\cdot\boldsymbol{sk}_{id}|$的所有分量均被限制在 $q/4p$ 以内,通过对倒数第二列解密即可保证体制解密的正确性. 如果存在破坏 NF 体制 CPA 安全的攻击者,则表明该攻击者可以区分 $\boldsymbol{c}$ 和 $\mathcal{R}_q^2$ 上的均匀分布. 所以,如果所基于的 IBE 体制满足性质 3,那么 NF 体制具有 IND-CPA 的安全性.

下面我们对 DLP2 体制和 NE2 体制是否满足定理 4.1 中的三条性质进行检验. 根据密钥生成算法,体制的私钥满足性质 1. 对于加密 0 所得的密文 $\boldsymbol{c}$,只要令 $q>4p(E+1)^d\cdot\|\langle \boldsymbol{c},\boldsymbol{sk}_{id}\rangle\|_\infty$,性质 2 就可以得到满足. 因为这两个体制是 IND-ID-CPA 安全的,因此满足性质 3. 所以本转化方式可以将以上两个 IBE 体制转化为 IND-ID-CPA 安全的 IBFHE 体制.

4.3 效率对比

本小节首先利用 GSW 和 NF 这两种转化方法将 DLP2 体制转化为 IBFHE 体制,并进行效率对比,结果如表 3 所示.

表 3 基于不同转化方法的 IBFHE 效率对比

方法	n	log$q$	log$p$	*mpk*	*skid*	*ci*	*enc*	*dec*
GSW	4096	97	1	388KB	776KB	147.02MB	354ms	132ms
NF	4096	131	13	524KB	1.02MB	24.58MB	49ms	23ms

可以看出,与 GSW 中基于 RLWE 的转化方法相比,NF 的密钥尺寸增加了 35.05%,密文尺寸减小了 83.28%,加解密时间减少了 82.40% ~86.11%. 这是由

于两种转化方式的主公钥尺寸均为 $n\log q$ 比特,用户私钥尺寸均为 $2n\log q$ 比特,GSW 转化方式的密文尺寸为 $4n\log^2 q$ 比特,NF 转化方式的密文尺寸为 $4nl^2\log p$ 比特. 由于体制的密钥尺寸较小、密文尺寸较大,且在应用中密钥只需生成、传输一次,而全同态加密需要多个密文参与,因此总体上可以较大的提升传输效率、减小存储空间.

此外,Gentry 等人提出[16],GSW 转化方法可以通过将加密算法中的明文空间由 $\mu \in \{0,1\}$ 改为 $\mu \in \mathbb{Z}_p$ 而实现多比特加密,但会相应使得 $\log q$ 的值增大. 与该方法相比,本文提出的转化方式可以在不增加系统参数的情况下实现多比特加密. 这一改动会使得定理 4.1 中第二条性质里的 E 变为 $E = n \cdot ((N-1) \cdot p/2 + 2^{1+\log q \bmod \log p}) + p$,而在本文的参数选取条件下对 $\log q$ 的影响忽略不计. 下面给出在加密 13 比特时两种转化方法的效率对比(如表 4 所示).

可以看出,在加密 13 比特的条件下,与 GSW 转化方法相比,NF 的密钥尺寸不变,密文尺寸减小了 90.83%,加解密时间减少了 90.33% ~91.18%,优势更加明显.

我们利用将 NE 体制与 NF 转化方式结合,得到 NFE 体制(如表 5 所示),并与现有的 IBFHE 体制进行效率对比,主要包括:①光焱等人提出的基于带错学习问题的 GZF 体制[15];②辛丹等人提出的基于 RLWE 问题的 XGZ 体制[35];③Gentry 等人提出的基于带错学习问题的 GSW 体制[16];④通过 MP 环上陷门采样函数[36]将 GSW 体制转换为基于 RLWE 问题的体制;⑤康元基等人提出的基于任意分圆环技术和 RLWE 问题的 KGZ 体制[37];⑥通过 DLP 基于 NTRU 格的陷门采样函数[20]将 GSW 体制转化为基于 RLWE 问题和 NTRU 问题的体制. 对于 NFE 体制,取 $\log p = 11$.

表 4　多比特加密条件下不同转化方式的 IBFHE 效率对比

方法	n	$\log q$	$\log p$	*mpk*	*skid*	*ci*	*enc*	*dec*
GSW	4096	131	13	524KB	1.02MB	268.14MB	557ms	241ms
NF	4096	131	13	524KB	1.02MB	24.58MB	49ms	23ms

根据表 5 可以看出,表中的前四种体制由于运算密钥尺寸或密文尺寸过大,因此效率远低于 NFE 体制. 与后两种体制相比,NFE 体制的主公钥、用户私钥、密文尺寸以及加解密时间减少均有不同程度减小,且安全性不低于这两种体制. 因此,在保证安全性相当的前提下,NFE 体制的系统参数更小、效率更高.

表 5　IBFHE 体制效率对比

体制	n	$\log q$	*mpk*	*skid*	*ci*	*evk*	*enc*	*dec*	λ
(1)	2146	75	48.25GB	46.05MB	23.02MB	162.74EB	–	–	120
(2)	2048	82	26.27MB	26.43MB	26.27MB	28.30TB	–	–	104
(3)	1659	58	17.25GB	10.64MB	113.31TB	0	–	–	120
(4)	1024	57	6.35MB	6.40MB	40.98GB	0	–	–	61
(5)	1708	62	1.01MB	1.11MB	757.63MB	0	1.84s	678ms	120
(6)	4096	97	388KB	776KB	147.02MB	0	354ms	132ms	127
NFE	2048	122	244KB	488KB	12.38MB	0	25ms	12ms	127

5　总结

对全同态加密体制而言,在不降低安全性的条件下减小密钥密文尺寸、提高效率可以有效提升体制的实用性. 本文首先设计了一种高效的 NTRU 格上的 IBE 体制,无需借助额外的安全性假设,密钥、密文尺寸和运算时间与现有体制相比显著减小,且安全性也有所提高. 之后,本文提出了一种基于近似特征向量技术的将环上 IBE 体制转化为 IBFHE 体制的方法,与现有转化方法相比,密钥尺寸略有增加,密文尺寸大幅减小. 通过将两种方法结合,可以进一步减小密文尺寸,且无需运算密钥.

参考文献

[1] Gentry C. Fully homomorphic encryption using ideal lattices[A]. Proceedings of the 41st Annual ACM Symposium on Theory of Computing[C]. New york:ACM,2009. 169 – 178.

[2] Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and security for key dependent messages[A]. Proceedings of the 31st Annual International Cryptology Conference[C]. Berlin:Springer,2011. 505 – 524.

[3] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE[J]. SIAM Journal on Computing,2014,43(2):831 – 871.

[4] Brakerski Z,Gentry C,Vaikuntanathan V. (Leveled) Fully homomorphic encryption without bootstrapping[J]. ACM Transactions on Computation Theory, 2011, 18(3): 169 – 178.

[5] 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 DH,ZHU SX,WANG L,et al. Fully homomorphic encryption scheme from RLWE[J]. Journal of Communications,2014,35(1):173 - 182. (in Chinese)

[6] Zhang P,Yu JP,Wang T. A homomorphic aggregate signature scheme based on lattice[J]. Chinese Journal of Electronics,2012,21(4):701 - 704.

[7] Gentry C,Groth J,Ishai Y,et al. Using fully homomorphic hybrid encryption to minimize non-interative zero-knowledge proof[J]. Journal of Cryptology,2015,28(4):820 - 843.

[8] Ducas L,Micciancio D. FHEW:Bootstrapping homomorphic encryption in less than a second[A]. Proceeding of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin:Springer,2015. 617 - 640.

[9] Gorbunov S,Vaikuntanathan V,Wichs D. Leveled fully homomorphic signatures from standard lattices[A]. Proceedings of the 47th Annual ACM on Symposium on Theory of Computing[C]. New york:ACM,2015. 469 - 477.

[10] Peikert C,Shiehian S. Multi-key FHE from LWE,revisited[A]. Proceedings of the 13th IACR Theory of Cryptography Conference[C]. Berlin:Springer,2016. 217 - 238.

[11] Benhamouda F,Lepoint T,Mathieu C,et al. Optimization of bootstrapping in circuits[A]. Proceedings of the 28th Annual ACM-SIAM Symposium on Discrete Algorithms[C]. New york:ACM,2017. 2423 - 2433.

[12] 陈振华,李顺东,王道顺,等. 集合成员关系的安全多方计算及其应用[J]. 电子学报,2017,45(5):1109 - 1116.
CHEN ZH,LI SD,WANG DS,et al. Secure multiparty computation of set membership and its applications[J]. Acta Electronica Sinica,2017,45(5):1109 - 1116. (in Chinese)

[13] Chen H,Hu YP,Lian ZZ. Properties of SV-style homomorphic encryption and their application[J]. Chinese Journal of Electronics,2017,26(5):926 - 932.

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

[15] 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 YF,Fei JL,et al. Identity-based fully homomorphic encryption from learning with error problem[J]. Journal of Communications,2014,35(2):111 - 117. (in Chinese)

[16] Gentry C,Sahai A,Waters B. Homomorphic encryption from learning with errors:Conceptually-simpler,asymptotically-faster,attribute-based[A]. Proceedings of the 33rd Annual International Cryptology Conference[C]. Berlin:Springer,2013. 75 - 92.

[17] Hoffstein J,Pipher J,Silverman JH. NTRU:A ring-based public key cryptosystem[A]. Proceeding of the 3rd International Algorithmic Number Theory Symposium[C]. Berlin:Springer,1998. 267 - 288.

[18] Lyubashevsky V,Peikert C,Regev O. On ideal lattices and learning with errors over rings[J]. Journal of the ACM,2013,60(6):43.

[19] Stehlé D,Steinfeld R. Making NTRU as secure as worst-case problems over ideal lattices[A]. Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin:Springer,2011. 27 - 47.

[20] Ducas L,Lyubashevsky V,Prest T. Efficient identity-based encryption over NTRU lattices[A]. Proceedings of the 20th Annual International Conference on the Theory and Application of Cryptology and Information Security[C]. Berlin:Springer,2014. 22 - 41.

[21] Peikert C. A decade of lattice cryptography[J]. Foundations and Trends in Theoretical Computer Science,2016,10(4):283 - 424.

[22] Lyubashevsky V,Prest T. Quadratic time,linear space algorithms for gram-schmidt orthogonalization and gaussian sampling in structured lattices[A]. Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin:Springer,2015. 789 - 815.

[23] Lyubashevsky V,Peikert C,Regev O. A toolkit for ring-LWE cryptography[A]. Proceedings of the 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin:Springer,2013. 35 - 54.

[24] Ducas L,Nguyen PQ. Faster gaussian lattice sampling using lazy floating-point arithmetic[A]. Proceedings of the 18th Annual International Conference on the Theory and Application of Cryptology and Information Security[C]. Berlin:Springer,2012. 415 - 432.

[25] Kirchner P,Fouque PA. An improved BKW algorithm for LWE with applications to cryptography and lattices[A]. Proceedings of the 35th Annual International Cryptology Conference[C]. Berlin:Springer,2015. 43 - 62.

[26] Lepoint T,Naehrig M. A comparison of the homomorphic encryption schemes FV,and YASHE[A]. Proceedings of the 7th International Conference on Cryptology in Africa[C]. Berlin:Springer,2014. 318 - 335.

[27] Gama N,Nguyen PQ. Predicting lattice reduction[A].

Proceedings of the 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin:Springer,2008. 31 – 51.

[28] Micciancio D, Regev O. Lattice-Based Cryptography [M]. Berlin:Springer,2011. 713 – 715.

[29] Lindner R, Peikert C. Better key sizes (and attacks) for LWE-based encryption[A]. Proceedings of the 11th International Conference on Topics in Cryptology[C]. Berlin: Springer,2011. 319 – 339.

[30] Gama N, Nguyen PQ, Regev O. Lattice enumeration using extreme pruning[A]. Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin:Springer,2010. 257 – 278.

[31] Becker A, Ducas L, Gama N, et al. New directions in nearest neighbor searching with applications to lattice sieving [A]. Proceedings of the 27th Annual ACM-SIAM Symposium on Discrete Algorithms [C]. New york: ACM, 2016. 10 – 24.

[32] Chen Y, Nguyen PQ. BKZ 2.0:Better lattice security estimates[A]. Proceeding of the 17th International Conference on the Theory and Application of Cryptology and Information Security[C]. Berlin:Springer,2011. 1 – 20.

[33] Aono Y, Wang YT, Hayashi T, et al. Improved progressive BKZ algorithms and their precise cost estimation by sharp simulator[A]. Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques [C]. Berlin: Springer, 2016. 789 – 819.

[34] Albrecht MR, Player R, Scott S. On the concrete hardness of learning with errors[J]. Journal of Mathematical Cryptology,2015,9(3):169 – 203.

[35] 辛丹,顾纯祥,郑永辉,等. 利用 RLWE 构造基于身份的全同态加密体制[J]. 电子学报,2016,44(12):2887 – 2893.
XIN D, GU CX, ZHENG YH, et al. Identity-based fully homomorphic encryption from ring learning with errors problem[J]. Acta Electronica Sinica,2016,44(12):2887 – 2893. (in Chinese)

[36] Micciancio D, Peikert C. Trapdoors for lattices: Simpler, tighter, faster, smaller[A]. Proceedings of the 31th Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin: Springer, 2012. 700 – 718.

[37] 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 YJ, GU CX, ZHENG YH, et al. Identity-based fully homomorphic encryption from eigenvector[J]. Journal of Software,2016,27(6):1487 – 1497. (in Chinese)

作者简介

段　然　男. 1989 年生于北京. 现为信息工程大学博士生,研究方向为信息安全.
E-mail:darkrs@ qq. com

顾纯祥　男. 1976 年生于安徽霍山. 现为信息工程大学教授,研究方向为网络和信息安全.

祝跃飞　男. 1962 年生于浙江杭州. 现为信息工程大学教授,研究方向为信息安全.

郑永辉　男. 1976 年生于江西乐平. 现为信息工程大学副教授,研究方向为密码学.

陈　莉　女. 1968 年生于江苏如皋. 现为河南财经政法大学教授,研究方向为信息安全理论与技术.