基于素数幂次阶分圆环的 NTRU 型全同态加密方案

秦小月，黄汝维，杨波

引用本文

秦小月，黄汝维，杨波. 基于素数幂次阶分圆环的 NTRU 型全同态加密方案[J]. 计算机科学, 2022, 49(5): 341-346.

QIN Xiao-yue, HUANG Ru-wei, YANG Bo. NTRU Type Fully Homomorphic Encryption Scheme over Prime Power Cyclotomic Rings[J]. Computer Science, 2022, 49(5): 341-346.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210300089

基于素数幂次阶分圆环的 NTRU 型全同态加密方案

秦小月　黄汝维　杨　波
广西大学计算机与电子信息学院　南宁 530004
(1319744146@qq.com)

摘　要　全同态加密支持在不解密的情况下对密文进行任意运算,为云计算的隐私安全提供了一种保护,但目前使用近似特征向量法构造的全同态加密方案需要进行复杂的矩阵乘法计算,存在计算复杂、无法抵御子域攻击等问题。文中使用素数幂次阶分圆环代替 2 的幂次阶分圆环,提出了一种新的全同态加密方案,并通过修改密文形式以及解密结构有效避免了同态乘法中复杂的矩阵乘法计算。与同类方案相比,所提方案在效率上至少提升了 $l\varphi(x)/2d$ 倍,并满足 IND-CPA 安全。

关键词:素数幂次阶分圆环;全同态加密;IND-CPA 安全
中图法分类号　TP309

NTRU Type Fully Homomorphic Encryption Scheme over Prime Power Cyclotomic Rings

QIN Xiao-yue, HUANG Ru-wei and YANG Bo
School of Computer and Electronic Information, Guangxi University, Nanning 530004, China

Abstract　Full homomorphic encryption (FHE) supports arbitrary computation on the ciphertext without the requirement of decryption, which provides protection for privacy security in cloud computing. However, the current FHE scheme constructed using the approximate eigenvector method requires complex matrix multiplications, which is computationally complicated and cannot resist subfield attacks. In this paper, a new FHE scheme was proposed by using the power-of-prime cyclotomic ring instead of a power-of-two cyclotomic ring, and the complex matrix multiplications in homomorphic multiplications were effectively avoided by modifying the ciphertext form and decryption structure. Compared with similar schemes, the proposed scheme improves the efficiency at least by a factor of $l\varphi(x)/2d$ and is secure against IND-CPA attacks.

Keywords　Prime power cyclotomic rings, Fully homomorphic encryption, IND-CPA security

全同态加密支持在加密信息上进行任意运算,计算得到的结果与解密后在明文上直接计算的结果相等,同态加密的特性使其在云计算、医疗、区块链等方面都有广泛的应用[1]。全同态加密方案按照其发展的历程大致可以分为 3 代:第一代全同态加密方案是基于理想格并以 Gentry 方案[2]为蓝图构造的,该类方案的构造方法过于复杂,同态解密效率较低;第二代全同态加密方案是基于 LWE 假设,利用密钥交换等技术来实现方案的构造[3],该类方案使用密钥交换和模交换等技术,涉及多个密钥,并且会出现密钥维数膨胀等问题;第三代全同态加密方案也是基于 LWE 假设,利用近似特征向量实现方案的构造[4]。该类方案的同态加法和同态乘法通过做简单的矩阵加法和乘法来实现,使得方案相对简单、快速且容易理解。2016 年,Doröz 等[5]提出的 F-NTRU 方案以及 Li 等[6]提出的改进方案都是利用 Flatten 技术以及 BitDecomp 技术实现了近似特征向量在 NTRU 体制上构造全同态加密方案的应用,但是利用近似特征向量构造的全同态加密方案的密文是矩阵形式,密文尺寸较大并且需要进行复杂的矩阵乘法,极大地影响了计算效率。2018 年,Khedr 等[7]使用 NTT(Fast Number Theoretic Transform)代替 F-NTRU 方案中的圆形卷积执行矩阵乘法,使计算变得简单,但是这些改进都无法从本质上避免矩阵乘法的操作。

同时,上述方案的安全性都是基于 2 的幂次阶分圆环,基于这种特殊分圆环的方案结构简单,但是无法抵御子域攻击[8-9]和使用 SIMD 技术[10]。Migliore 等[11]也验证了 F-NTRU 方案遭受子域攻击的可能,因此寻找一种更安全的环以保证方案的安全尤为必要。2016 年,Doröz 等[12]首次提出基于素数幂次阶分圆环的 DHS16 方案,用于改进 LTV12 方案[13],提高了方案在实际应用中的效率,但未给出理论上的安全性证明。2018 年,Yu 等[14]将 SS11 方案[15]的环结构改为素数幂次阶分圆环,并利用正则嵌入的高斯分布改进了密钥生成算法,使其安全性得到证明。

为解决上述利用近似特征向量构造全同态加密方案存在的问题,本文提出了一种基于素数幂次阶分圆环的 NTRU 型全同态加密方案。该方案无需密钥交换,在一定条件下消除了 DSPR 假设,可仅依赖于 RLWE 问题假设。同时,本文方案基于素数幂次阶分圆环,能够抵御子域攻击,支持引入

到稿日期:2021-03-08　返修日期:2021-07-22
基金项目:国家自然科学基金(62062009)
This work was supported by the National Natural Science Foundation of China(62062009).
通信作者:黄汝维(ruweih@gxu.edu.cn)

SIMD 技术以提升方案效率。该方案使用矩阵-向量乘法取代了复杂的矩阵乘法运算，在效率上有很大提升，同时方案的密文为向量形式，在存储、运输、计算方面更具优势[16]。此外，本文方案在 Game-Hopping 标准模型的证明下满足 IND-CPA 安全。

1 基础知识

1.1 符号表示

若 A 表示一种算法，则 $x \leftarrow A$ 表示 x 是通过算法计算得到的；若 A 表示一个集合，则 $x \leftarrow A$ 表示 x 是从集合 A 中随机选出的。对于任意整数 q，记 $Z_q = \left[-\frac{q}{2}, \frac{q}{2}\right) \cap Z$，$[x]_q$ 表示 $(x \bmod q) \in Z_q$。用小写英文字母表示多维向量，如向量 $\boldsymbol{y}$，其中 $\boldsymbol{y}_i$ 表示向量 $\boldsymbol{y}$ 的第 i 个分量，未定元为 x 的多项式，用小写英文字母表示，如 $f(x)$。

1.2 分圆多项式

定义 1(分圆多项式)[17] 设 K 是特征为 P 的域，n 是一个不能被 P 整除的正整数，ξ_n 是 K 上的一个 n 次本原单位根，则多项式 $\Phi_n(x) = \prod_{i=1,\gcd(i,n)=1}^{n} (x-\xi^i)$，称为 K 上的 n 次分圆多项式，在有理数域 Q 上添加一个 n 次本原单位根得到域扩张 $K=Q(\xi_n)$，称为 n 次分圆域：

(1)当 $n=2^d, d \in Z^*$ 时，$\Phi_n(x) = x^n + 1$；

(2)当 n 为素数时，$\Phi_n(x) = x^{n-1} + x^{n-2} + \cdots + x + 1$；

(3)当 d 为素数时，$n = d^v, v \in Z^*$，$\Phi_n(x) = \Phi_d(x^{d^{v-1}})$，$R = Z[x]/\Phi_n(x)$ 和 $R_q = R/qR$ 为素数幂次分圆多项式环。

引理 1[17] 设 F_q 为有限域，n 为正整数，且 $\gcd(n,d)=1$，则分圆多项式 $\Phi_n(x)$ 在 $F_q[x]$ 上可分解为 $\frac{\varphi(x)}{d}$ 个不同的首一 d 次不可约多项式 $f_i(x)$ 的乘积，即 $\Phi_n(x) = \prod_{i=0}^{l-1} f_i(x)$，其中 d 是 q 模 n 的指数满足 $q^d \equiv 1 \pmod n$ 的最小整数，$l = \varphi(x)/d$。

引理 2[17] 设 F_q 为有限域，n 为正整数，则 n 阶分圆多项式 Q_n 在 $F_q[x]$ 上不可约的充分必要条件是 q 模 n 的指数为 $\Phi_n(x)$(即 q 是模 n 的原根)。由引理 2 可知，若 $n \equiv \pm 1 \bmod 8$ 是素数或素数的方幂，则 Q_n 在 $F_2[x]$ 上可约[18]。

引理 3[19] 设 $n \in N$，$\Phi_n(x) = x^n + 1$，环 $R = Z[x]/\Phi_n(x)$，对于任意 $a, b \in R$，有：

$$\|ab\| \leqslant \|a\| \|b\| \tag{1}$$

$$\|ab\|_\infty \leqslant n \|a\|_\infty \|b\|_\infty \tag{2}$$

引理 4[14] 设 $n = d^v$，d 为素数，$\Phi_n(x) = \Phi_d(x^{d^{v-1}})$，则 $R = Z[x]/\Phi_n(x)$，对于任意 $a, b \in R$，最坏情况下有：

$$\|ab\|_\infty \leqslant 2\sqrt{\varphi(n)} \|a\|_\infty \|b\|_\infty \tag{3}$$

1.3 RLWE($\boldsymbol{\Phi}, n, q, \chi$)假设

定义 2(RLWE($\boldsymbol{\Phi}, n, q, \chi$)假设)[20] 设 $n = d^v$，d 为素数，$\Phi_n(x) = \Phi_d(x^{d^{v-1}})$，定义多项式环 $R = Z[x]/\Phi_n(x)$，$R_q = R/qR$ 以及环 R 上的正则嵌入下的离散高斯分布 χ。对于随机环元素 $s \leftarrow R_q$，给定形式的任意多项式 $(a_i, b_i = a_i \cdot s + e_i) \in (R_q)^2$，其中 a_i 在 R_q 中是均匀随机的，e_i 来自误差分布 χ，RLWE(Φ, n, q, χ)假设的困难性在于区分 b_i 是来自公式计算还是直接来自 R_q 的均匀分布。

1.4 DSPR($\boldsymbol{\Phi}, n, q, \chi$)假设

定义 3(DSPR($\boldsymbol{\Phi}, n, q, \chi$)假设)[20] 令 $n = d^v$，d 为素数，$\Phi_n(x) = \Phi_d(x^{d^{v-1}})$，定义多项式环 $R = Z[x]/\Phi_n(x)$，$R_q = R/qR$ 以及环 R 上的正则嵌入下的离散高斯分布 χ。给定形式 $h = g/f$，其中 f 和 g 是来自分布 χ 随机采样，满足条件的 f 在 $R_q = R/qR$ 上是可逆的，DSPR(Φ, n, q, χ)假设的困难性在于区别多项式 h 来自公式计算还是直接来自 R_q 上随机的均匀。

1.5 正则嵌入下的高斯分布

定义 4(正则嵌入下的高斯分布)[21] 设 $P(X) \in Z[x]$ 是首一的 n 阶既约多项式，$R = Z[x]/P(x)$，$P(X)$ 在复数域下的根为 $w_1, w_2, \cdots, w_n$，$V = (w_j^{n-i})_{ij}$，$0 \leqslant i \leqslant n-1$，$1 \leqslant j \leqslant n$ 被称为正则变换矩阵，设 $t = t_{n-1}x^{n-1} + t_{n-2}x^{n-2} + \cdots + t_0 \in R$ 系数嵌入表示为 $t_{n-1}, t_{n-2}, \cdots, t_0$，正则嵌入变换表示为 $\sigma(t) = (t_{n-1}, t_{n-2}, \cdots, t_0)V\sigma$，正则嵌入下的高斯分布为：

$$\begin{aligned} t &= \sigma^{-1}(t) = \sigma(t) \cdot V^{-1} \\ D_{z^n,\sigma}(x) &= \rho_\sigma(x)/\rho_\sigma(Z^n) \end{aligned} \tag{4}$$

2 基于素数幂次阶分圆环的全同态加密方案

2.1 SIMD 技术

由引理 2 可知，素数的幂次阶分圆环可在 $F_q[x]$ 上分解为多个不可约多项式，因此本文利用中国剩余定理[22]对明文槽的数据进行批处理，并行执行同态运算，提高方案的执行效率，下面给出具体的过程。

将整个明文空间 $R_p = R/pR$ 分解为大小相同的 l 子环，对应的明文槽为 $\frac{Z_2[x]}{f_1(x)}, \cdots, \frac{Z_2[x]}{f_l(x)}$，槽内有待加密的明文 $m_i(x)$，然后把槽上的 l 明文合成一个明文空间，$\boldsymbol{c}(\boldsymbol{x})$，$\boldsymbol{c}'(\boldsymbol{x})$ 表示分别使用一个明文空间加密得到的密文，对应的明文分别为 $m_1(x), m_2(x), \cdots, m_l(x)$ 和 $m_1'(x), m_2'(x), \cdots, m_l'(x)$，$l$ 个明文并行执行的同态操作如下：

$$\begin{aligned} &l_{\text{add}}((m_1(x), m_2(x), \cdots, m_l(x)), (m_1'(x), m_2'(x), \cdots, \\ &m_l'(x))) = m_1(x) + m_1'(x), \cdots, m_l(x) + m_l'(x) \end{aligned} \tag{5}$$

$$\begin{aligned} &l_{\text{mult}}((m_1(x), m_2(x), \cdots, m_l(x)), (m_1'(x), m_2'(x), \cdots, \\ &m_l'(x))) = m_1(x) \cdot m_1'(x), \cdots, m_l(x) \cdot m_l'(x) \end{aligned} \tag{6}$$

其中，l_{add} 和 l_{mult} 分别表示对明文进行同态加以及同态乘的批处理操作，因此同态操作可以看作是在明文槽上使用 SIMD 技术并行执行的。由于数组中不同索引处的数据永远无法交互，因此仅靠 l_{add} 和 l_{mult} 运算无法对加密数组执行任意计算。为获得数组的完整操作集，本文引入文献[23]的 l_{permute} 操作实现对数组中的数据进行任意排列，支持明文 $m(x) \rightarrow m(x^{2^i})$ 槽循环移动 i 个明文槽，如当 $i=1$ 时，$m(x)$ 的明文槽循环移动 1 个位置，对应各个明文槽的明文变更为 $m_2(x), m_l(x), \cdots, m_1(x)$，从而实现对数据的完整操作。当密文需要进行解密操作时，使用中国剩余定理的逆向处理，即可解密出 l 个明文。

2.2 方案构造

设 λ 为安全参数，L 为电路层数，n 为维数且为素数的幂次阶，令 $R = Z[x]/\Phi_n(x)$，其中 $\Phi_n(x) = \prod_{i=1,\gcd(i,n)=1}^{n} (x-\xi^i)$ 是分圆多项式，每个 $f_i(x)$ 的次数为 d，$\varphi(n) = dl = n(\lambda, L)$，$F_q^{ld}$ 为明文向量空间，映射 CRT_q 是 F_q^{ld} 到 R_q 的同构映射。

(1)密钥生成算法

选择一个足够大的标准差 σ，使得 f 可以表示为：$f = p \cdot$

$f'+1$，其中 f' 是从正则嵌入下的离散高斯分布 $D_{z^n,\sigma}(x)$ 中取样的一个多项式。输入为 $n,q\in Z,p\in R_q^*,\sigma\in R$，其中 R_q^* 是 R_q 中可逆元素的集合，$R_q=R/qR=Z_q[x]/\Phi$，输出为 $(sk,pk)\in R\times R_q^*$，具体过程如下：

首先从正则嵌入下的离散高斯分布 $D_{z^n,\sigma}(x)$ 中取样 f'，令 $f=p\cdot f'+1$，如果 $f \bmod q\notin R_q^*$，则重新取样；

然后从正则嵌入下的离散高斯分布 $D_{z^n,\sigma}(x)$ 中取样 g，如果 $g \bmod q\notin R_q^*$，则重新取样；

最后返回 $sk=f,pk=h=pgf^{-1}\in R_q^*$。

(2)加密算法

利用中国剩余定理计算明文 $m\leftarrow CRT_q(m_1(x),m_2(x),\cdots,m_l(x))\in R_q$，然后对 0 进行加密，得到一个长度为 $l=\log q$ 的密文向量 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{l-1})^{\mathrm{T}}$，$\boldsymbol{c}$ 是一个 l 维列向量，$\boldsymbol{c}_i$ 是对 0 加密得到的密文，$\boldsymbol{c}_i=hs_i+p\boldsymbol{e}_i$，$\boldsymbol{m}'$ 表示 $(m,0,\cdots,0)$ 列向量形式，$\boldsymbol{e}$ 表示 l 维单位列向量，令 $\boldsymbol{c}'=(\boldsymbol{m}'+\boldsymbol{c})=(c_0+m,c_1,\cdots,c_{l-1})^{\mathrm{T}}$，$\boldsymbol{c}'$ 为消息 $\boldsymbol{m}$ 对应的密文列向量。

(3)加法同态

$\boldsymbol{c}_3^+$ 代表两密文进行加法同态后的结果，由于密文形式相同，因此只需要进行简单的加法操作即可实现加法同态运算。

$$\boldsymbol{c}_3^+=\boldsymbol{c}_1'+\boldsymbol{c}_2' \tag{7}$$

(4)乘法同态

$\boldsymbol{c}_3^*$ 代表两密文进行乘法同态后的结果，密文计算得到的 $\boldsymbol{c}_3^*$ 是列向量与初始密文形式相同，因此无需密钥交换过程：

$$\boldsymbol{c}_3^*=\boldsymbol{e}\cdot(\boldsymbol{c}_1')^{\mathrm{T}}\cdot\boldsymbol{c}_2' \tag{8}$$

(5)解密算法

$\boldsymbol{c}'$ 表示列向量形式的新鲜密文，在进行解密操作时，选取该密文的第一个元素 c_0 进行计算：

$$m=\lfloor c_0 f\rfloor \bmod p \tag{9}$$

根据 $(m_1(x),m_2(x),\cdots,m_l(x))m\leftarrow CRT_q^{-1}(x)\in F_{q^d}^l$，解密出 l 个明文。

2.3 加解密分析

本节将对本文方案的加解密过程以及对应的噪声增长情况进行分析。

由加解密算法可知：

$$\begin{aligned}Dec(Enc(m))&=\lfloor c_0 f\rfloor(\bmod p)=(m+hs_i+pe_i)\\&=mf+pgs_0+pe_0 f(\bmod p)\\&=mf+p(gs_0+e_0 f) \bmod p\\&=mf \bmod p\end{aligned} \tag{10}$$

因为 $f\equiv 1(\bmod p)$，可得 $\lfloor c_0 f\rfloor(\bmod p)=m$，结合：

$$(m_1(x),m_2(x),\cdots,m_l(x))m\leftarrow CRT_q^{-1}(x)\in F_q^{ld} \tag{11}$$

即可解密出 l 个明文。

定理 1(加密噪声) q,n,R_q,χ 是上述加密方案的参数，χ 的上界是 B。任意 $f\leftarrow\chi$ 计算 $f=p\cdot f'+1$，使 $f\equiv 1(\bmod p)$，如果 $f \bmod q\notin R_q^*$，则重新取样。令 $h=Keygen(f)$，$\boldsymbol{c}\leftarrow Enc(h,m)$，则存在 v 且 $\|v\|_\infty\leqslant 2\sqrt{\varphi(n)}((1+p)B^2+B)$，使如下等式成立：

$$\boldsymbol{c}f=mf+pv\in R_q \tag{12}$$

其中，v 为密文的噪声，这里 $mf=m(p\cdot f'+1)$ 中含有 mf' 部分噪声用于更正具有少量包装的消息[24]，因此本文对该部分噪声忽略不计。

证明：根据基本加密方案有 $\boldsymbol{c}f=mf+pgs_0+pe_0 f$，令 $v=pgs_0+pe_0 f$ 代表新鲜密文的噪声，由于 χ 的上界是 B，可知 g,s,e 系数上界为 B，f 系数上界为 $pB+1$。结合引理 4，可得 gs_0 的系数上界为 $2\sqrt{\varphi(n)}B^2$，$e_0 f$ 的系数上界为 $2\sqrt{\varphi(n)}B(pB+1)$，综上可得 v 的系数上界为 $2\sqrt{\varphi(n)}((1+p)B^2+B)$，即 $v_\infty\leqslant 2\sqrt{\varphi(n)}((1+p)B^2+B)$，证毕。

定理 2(解密噪声) 任意 $f,c\in R_q$，且有 $f\equiv 1(\bmod p)$。若满足 $cf=mf+pv\in R_q$，其中 $v_\infty\leqslant q/2p$，则有：

$$Dec(f,c)=m \tag{13}$$

证明：若 $v_\infty\leqslant q/2p$，则：

$$\begin{aligned}Dec(f,c)&=cf(\bmod p)=mf+pv(\bmod p)\\&=mf(\bmod p)=m\end{aligned} \tag{14}$$

结合定理 1，当噪声 v 于 $q/2p$ 时，即可解密成功，证毕。

2.4 同态性分析

(1)加法同态

令 $\boldsymbol{c}_1'$ 与 $\boldsymbol{c}_2'$ 表示使用本文方案进行加密的密文，对应的私钥为 f，密文形式为列向量，$\boldsymbol{c}_3^+$ 表示两者的加法密文，密文形式不变，加法同态性的证明如下：

$$\begin{aligned}\boldsymbol{c}_3^+&=(c_{10}+m_1,\cdots,c_{1l-1})^{\mathrm{T}}+(c_{20}+m_2,\cdots,c_{2l-1})^{\mathrm{T}}\\&=(c_{10}+m_1+c_{20}+m_2,c_{11}+c_{21},\cdots,c_{1l-1}+c_{2l-1})^{\mathrm{T}}\end{aligned} \tag{15}$$

取 $\boldsymbol{c}_3^+$ 的第一行 c_3，$c_3=c_{10}+m_1+c_{20}+m_2$，其中 $c_{10}=hs_{10}+pe_{10}$，$c_{20}=hs_{20}+pe_{20}$，可得：

$$\begin{aligned}c_3 f \bmod p&=(m_1+m_2+hs_{10}+pe_{10}+hs_{20}+pe_{20})f(\bmod p)\\&=(m_1+m_2+pgf^{-1}s_{10}+pe_{10}+pgf^{-1}s_{20}+pe_{20})f(\bmod p)\\&=(m_1+m_2) \bmod p\end{aligned} \tag{16}$$

(2)加法噪声

令 $\boldsymbol{c}_1'$ 与 $\boldsymbol{c}_2'$ 表示使用本文方案进行加密的密文，对应的私钥为 f，c_3 代表新鲜密文进行一次加法同态后的密文的第一行，$E=2\sqrt{\varphi(n)}((1+p)B^2+B)$，$v^+$ 代表进行一次乘法同态的噪声。根据加法定义 $c_3=c_{10}+m_1+c_{20}+m_2$，其中 $c_{10}=hs_{10}+pe_{10}$，$c_{20}=hs_{20}+pe_{20}$，即 $v_1=c_{10}$，$v_2=c_{20}$，$c_3=m_1+m_2+v_1+v_2$，又因为 $v_\infty\leqslant E$，可得 $\|v^+\|_\infty\leqslant 2E=4\sqrt{\varphi(n)}((1+p)B^2+B)$。

(3)乘法同态

令 $\boldsymbol{c}_1'$ 与 $\boldsymbol{c}_2'$ 表示使用本文方案进行加密的密文，对应的私钥为 f，密文形式为列向量，$\boldsymbol{c}_3^*$ 表示两者的乘积密文，密文形式不变，下面进行乘法同态性的验证：

$$\begin{aligned}\boldsymbol{c}_3^*&=\boldsymbol{e}\cdot(\boldsymbol{c}_1')^{\mathrm{T}}\cdot\boldsymbol{c}_2'=(1,1,\cdots,1)^{\mathrm{T}}(c_{10}+m_1,c_{11},\cdots,c_{1l-1})\cdot(c_{20}+m_2,c_{21},\cdots,c_{2l-1})\\&=\begin{bmatrix}c_{10}+m_1 c_{11}\cdots c_{1l-1}\\c_{10}+m_1 c_{11}\cdots c_{1l-1}\\\cdots\\c_{10}+m_1 c_{11}\cdots c_{1l-1}\end{bmatrix}\cdot[c_{20}+m_2 c_{21}\cdots c_{2l-1}]^{\mathrm{T}}=\begin{bmatrix}(c_{10}+m_1)\cdot(c_{20}+m_2)+c_{11}\cdot c_{21}+\cdots+c_{1l-1}\cdot c_{2l-1}\\(c_{10}+m_1)\cdot(c_{20}+m_2)+c_{11}\cdot c_{21}+\cdots+c_{1l-1}\cdot c_{2l-1}\\\cdots\\(c_{10}+m_1)\cdot(c_{20}+m_2)+c_{11}\cdot c_{21}+\cdots+c_{1l-1}\cdot c_{2l-1}\end{bmatrix}\end{aligned} \tag{17}$$

取$\boldsymbol{c}_3^*$的第一行，得：

$$c_3=(c_{10}+m_1)\cdot(c_{20}+m_2)+c_{11}\cdot c_{21}+\cdots+c_{1l-1}\cdot c_{2l-1}$$
$$=m_1\cdot m_2+c_{20}\cdot c_{10}+c_{20}\cdot m_1+c_{10}\cdot m_2+c_{11}\cdot c_{21}+\cdots+c_{1l-1}\cdot c_{2l-1} \tag{18}$$

其中，$c_{10}=hs_{10}+pe_{10}$，$c_{20}=hs_{20}+pe_{20}$，可得：

$$c_3 f \bmod p=(m_1\cdot m_2+c_{20}\cdot c_{10}+c_{20}\cdot m_1+c_{10}\cdot m_2+c_{11}\cdot c_{21}+\cdots+c_{1l-1}\cdot c_{2l-1})f(\bmod p) \tag{19}$$

将$c_{10}=hs_{10}+pe_{10}$，$c_{20}=hs_{20}+pe_{20}$，$h=pg\ f^{-1}$，$f\equiv 1(\bmod p)$代入，可得$\lfloor c_3 f \rfloor(\bmod p)=m_1\cdot m_2$。

(4)乘法噪声

由于两密文进行同态加法后的噪声是两密文的噪声之和，进行同态乘法后的噪声是两密文的噪声之积，可知影响解密正确的因素主要来自乘法同态，因此本文给出乘法同态的噪声以及密文电路L层的计算噪声。

令$\boldsymbol{c}_1'$与$\boldsymbol{c}_2'$为使用本文方案进行加密的密文，对应的私钥为f，c_3代表新鲜密文进行一次乘法同态后的密文的第一行，v^*代表进行一次乘法同态的噪声。根据乘法定义有$c_3=(m_1\cdot m_2+c_{20}\cdot c_{10}+c_{20}\cdot m_1+c_{10}\cdot m_2+c_{11}\cdot c_{21}+\cdots+c_{1l-1}\cdot c_{2l-1})$，其中，$c_{10}=hs_{10}+pe_{10}$，$c_{20}=hs_{20}+pe_{20}$，即$v_1=c_{10}$，$v_2=c_{20}$，根据：

$$c_3=(m_1^{\frac{\varphi(x)}{d}}\cdot m_2^{\frac{\varphi(x)}{d}}+c_{2,0}\cdot c_{1,0}+c_{2,0}\cdot m_1^{\frac{\varphi(x)}{d}}+c_{1,0}\cdot m_2^{\frac{\varphi(x)}{d}}+c_{1,1}\cdot c_{2,1}+\cdots+c_{1,l-1}\cdot c_{2,l-1}) \tag{20}$$

其中，$c_{10}=hs_{10}+pe_{10}$，$c_{20}=hs_{20}+pe_{20}$，可得$v_1=c_{10}$，$v_2=c_{20}$，又因为$m^{\frac{\varphi(x)}{d}}$表示含有$\frac{\varphi(x)}{d}$个明文，可得$(c_{1,0}\cdot m_2^{\frac{\varphi(x)}{d}})=\frac{\varphi(x)}{d}E$，$(c_{2,0}\cdot m_1^{\frac{\varphi(x)}{d}})=\frac{\varphi(x)}{d}E$，即$\|v^*\|_\infty\leqslant 2\frac{\varphi(x)}{d}E+lE^2$。

设第i层的噪声表示为$\boldsymbol{c}^i$，根据同态运算有$\boldsymbol{c}^i=\boldsymbol{c}^{i-1}*\boldsymbol{c}^{i-1}$，本文方案经过第2次乘法电路的计算噪声如下：

$$\boldsymbol{c}^3=\boldsymbol{c}^2*\boldsymbol{c}^2=\left(2\frac{\varphi(x)}{d}E+lE^2\right)*\left(2\frac{\varphi(x)}{d}E+lE^2\right)=\left(2\frac{\varphi(x)}{d}E+lE^2\right)^2 \tag{21}$$

经过一次乘法同态，有$2\frac{\varphi(x)}{d}$个明文进行了乘法同态运算，以此类推，经过深度为L的电路计算，其噪声至多为：

$$\boldsymbol{c}^L=\left(2\frac{\varphi(x)}{d}E+lE^2\right)^{\frac{dL}{\varphi(X)}} \tag{22}$$

只要$\left(2\frac{\varphi(x)}{d}E+lE^2\right)^{\frac{dL}{\varphi(X)}}$不超过$q/2p$，可保证密文解密正确。

2.5 安全性分析

定理3 令$n=d^v$，d和$q\geqslant 8n$为素数，且满足$q\equiv 1 \bmod n$，当$r\geqslant\varphi(n)\sqrt{\frac{2\ln(6)}{\pi}\cdot q^{1/\varphi(n)}}$，存在$1-n^{-\omega(1)}$的概率，使$f,g$满足：

$$\|f\|\leqslant\omega(\sqrt{n\ln n})\cdot\|p\|r \tag{23}$$

$$\|g\|\leqslant\omega(\sqrt{\ln n})\cdot r \tag{24}$$

此时方案的安全性仅依赖于RLWE(Φ,n,q,χ)假设，并在RLWE(Φ,n,q,χ)假设下具有IND-CPA安全。

证明当f,g满足上述情况时，存在$1-n^{-\omega(1)}$的概率使得：

$$\|f\|\leqslant\omega(\sqrt{\ln n})\cdot\|p\|r \tag{25}$$

对于多项式f'，同样的参数对于公式$f=p\cdot f'+1$也成立，即存在$1-n^{-\omega(1)}$的概率使得$\|f\|\leqslant 1+\|p\|\|f'\|\leqslant\omega(\sqrt{\ln n})\cdot\|p\|r$。结合引理4可得，存在$1-n^{-\omega(1)}$的概率使得$\|f\|\leqslant 1+2\sqrt{\varphi(n)}\|p\|\|f'\|\leqslant\omega(\sqrt{\ln n})\cdot\|p\|r$。对于2的幂次阶和素数环，此时已经证明一般情况下多项式f,g取值很小，因此具有一定宽度r的采样f,g，在保证f,g的范数增长不会带来庞大的噪声增长而影响单次同态乘法运算的情况下，使公钥h在R_q上几乎均匀分布，结合逆元的性质可知f,g的逆元f^{-1},g^{-1}属于R_q，得：

$$\frac{g}{f}=g\cdot f^{-1} \tag{26}$$

DSPR假设允许$h=2g/f$更改为$2h'$，RLWE(Φ,n,q,χ)假设允许$c^*=hs+2e+m$更改为$c^*=u+m$，其中e的取值范围很小，可以忽略不计。结合式(26)，可将DSPR假设中的分数形式转换成RLWE(Φ,n,q,χ)假设中的乘积形式，因此方案的安全性归约于RLWE(Φ,n,q,χ)假设的证明成立。这里首先给出IND-CPA安全的定义。

定义5(IND-CPA安全) 设有某公钥加密方案ε，在有界多项式时间内，若存在一个极小函数$negl(\lambda)$使得敌手A的优势为：

$$Adv_{\text{IND-CPA}}(A)=|\Pr[A(pk,Enc_{pk}(m_0=1)]-\Pr[A(pk,Enc_{pk}(m_1=1)]|$$
$$=negl(\lambda) \tag{27}$$

其中，$negl(\lambda)$可省略，λ是方案的安全参数，游戏中包含一个多项式时间的敌手A，令$Adv_{\text{IND-CPA}}(A)$表示敌手A在游戏中获胜的概率。接着采用基于游戏的Game-Hopping方法证明在RLWE(Φ,n,q,χ)的假设下具有IND-CPA安全，证明如下。

Game0：标准的IND-CPA游戏，即挑战者调用全同态加密体制的KeyGen算法，将生成的公钥pk交给敌手A。A具备访问加密预言机的能力，挑战者输出挑战密文$\boldsymbol{c}=Enc_{pk}(m_b)$，敌手$A$尝试区分$\boldsymbol{c}$所对应的明文，$m_b$，$b\in(0,1)$，Game0中敌手$A$的优势为：

$$Adv_{\text{IND-CPA}}(A)=\Pr[A(pk,Enc_{pk}(m_0=1)]-\Pr[A(pk,Enc_{pk}(m_1=1)]| \tag{28}$$

Game1：Game1与Game0的区别在于公钥pk的生成方式，Game1中的公钥pk不是通过私钥sk和正则嵌入下的高斯采样，而是直接从R_q^*中随机均匀选取。由定义3可知，离散高斯分布输出的结果与R_q^*上的分布式概率是不可区分的，由文献[25]可知，离散高斯分布输出的结果与R_q^*上的分布式的统计距离在$2^{-\Omega(n)}$以内，因此有：

$$|Adv_{\text{Game1}}(A)-Adv_{\text{IND-CPA}}(A)|\leqslant 2^{-\Omega(n)} \tag{29}$$

Game2：Game2与Game1的区别在于Game2中的加密算法不再按照方案的加密算法进行加密，而是直接从$\{0,1\}$中随机均匀选取。由定理3可知，本文方案中DSPR(Φ,n,q,χ)问题假设已规约到RLWE(Φ,n,q,χ)，因此在Game2与Game1中，敌手A的优势差在于解决RLWE(Φ,n,q,χ)问题。

$$|Adv_{\text{Game2}}(A)-Adv_{\text{Game1}}(A)|\leqslant \text{RLWE}(\Phi,n,q,\chi)$$
$$Adv(A)) \tag{30}$$

Game3：在 Game3 中，挑战者给出的挑战密文 $\boldsymbol{c}$ 不再由加密算法生成，而是随机均匀地从{0，1}中随机均匀选取，Game3 的安全性分析与 Game2 相同，有：

$$|Adv_{\text{Game3}}(A)-Adv_{\text{Game2}}(A)|\leqslant \text{RLWE}(\Phi,n,q,\chi)Adv(A) \tag{31}$$

在 Game3 中，挑战者给出的公钥 pk、挑战密文 c 都是随机的，与明文 m_b，$b\in(0,1)$ 无关。因此，敌手 A 在 Game3 中的优势为 0，即：

$$Adv_{\text{Game3}}(A)=0 \tag{32}$$

由式(27)—式(32)可得：

$$Adv_{\text{IND-CPA}}(A)\leqslant 2^{-\Omega(n)}+\text{RLWE}(\Phi,n,q,\chi)Adv(A)+\text{RLWE}(\Phi,n,q,\chi)Adv(A) \tag{33}$$

综上，在 DSPR(Φ,n,q,χ) 困难假设下，$Adv_{\text{IND-CPA}}(A)$ 可忽略，本文方案是 IND-CPA 安全的，证毕。

3 性能分析

本节将对本文方案与 F-NTRU 方案进行分析，从密文尺寸以及同态计算复杂度等方面展示本文方案的优势。

3.1 密文尺寸分析

使用近似特征向量法构造的 F-NTRU 方案的密文是由两个次数小于 2^n 形式的多项式构成的，且密文扩展为 $\lceil\log q\rceil\cdot\lceil\log q\rceil$ 的矩阵形式，由引理 3 可知，该尺寸上界为 $\lceil\log q\rceil^2\cdot n\cdot\log q^2$，加密使用的公钥由两个多项式组成，可得公钥尺寸为 $n\cdot\log q^2$，F-NTRU 方案解密时用到 1 个次数小于 2^n 且系数小于 $(2B+1)$ 的多项式私钥，因此私钥尺寸大小为 $\log(2B+1)$。本文方案密文为 $\lceil\log q\rceil$ 维向量形式的多项式，由于此方案是基于素数幂次阶的分圆多项式，根据引理 4 可得，本文方案的密文尺寸为 $2\lceil\log q\rceil\sqrt{\varphi(n)}\cdot\log q^2$。本文方案的公钥和私钥基于的分圆多项式与 F-NTRU 方案不同，因此方案的公钥和私钥的尺寸相比 F-NTRU 方案也有些变化，分别为 $2\varphi(n)\cdot\log q^2$ 和 $\log(2B+1)$，具体如表 1 所列。

表 1 密文尺寸的对比

Table 1 Comparison of the size of ciphertext

方案	密文规模	公钥规模	私钥规模	多项式
F-NTRU	$\lceil\log q\rceil^2\cdot n\cdot\log q^2$	$n\cdot\log q^2$	$\log(2B+1)$	$\Phi_n(x)=x^n+1$
本文方案	$2\lceil\log q\rceil\cdot\sqrt{\varphi(n)}\cdot\log q^2$	$2\varphi(n)\cdot\log q^2$	$\log(2B+1)$	$\Phi_n(x)=\Phi_d(x^{d^{v-1}})$

由表 1 可以发现，相比 F-NTRU 方案，本文方案在私钥规模保持不变的情况下，对公钥规模进行了优化，并且本文方案的密文规模从 $\lceil\log q\rceil^2\cdot n\cdot\log q^2$ 降低到了 $2\lceil\log q\rceil\cdot\sqrt{\varphi(n)}\cdot\log q^2$，有效约减了密文规模，使密文在存储与传输上更具有优势。

3.2 计算复杂度分析

这里假定进行一次向量相加的时间消耗为 T_{add}，进行一次向量相乘的时间消耗为 T_{mult}，F-NTRU 进行一次同态加法 $\boldsymbol{C}_1'+\boldsymbol{C}_2'$，实际上是进行了 l 次向量相加，进行一次同态乘法 $\boldsymbol{C}_1'\cdot\boldsymbol{C}_2'$，实际上是进行了 $l\times l$ 次向量相乘，而本文方案进行一次同态加 $\boldsymbol{c}_1'+\boldsymbol{c}_2'$ 实际上是进行 1 次向量加法，进行一次同态乘法 $\boldsymbol{c}_3'=\boldsymbol{e}\cdot(\boldsymbol{c}_1')^{\mathrm{T}}\cdot\boldsymbol{c}_2'$，实际上是进行了 $2l$ 次向量乘法，因为 $\boldsymbol{e}\cdot(\boldsymbol{c}_1')^{\mathrm{T}}\cdot\boldsymbol{c}_2'$ 先是由一个单位列向量与行向量相乘，其计算量约等于进行了 l 次同态乘法，求得的矩阵结果再与一个列向量运算，其计算量实际上进行了 l 次向量乘法，并且本文方案在计算中使用中国剩余定理将多个明文打包到一个密文中，进行并行化处理，有效提高了计算效率，具体如表 2 所列。

表 2 计算复杂度对比

Table 2 Comparison of computational complexity

方案	加密明文	通信量/个	加法计算量	乘法计算量
F-NTRU	$2\frac{\varphi(x)}{d}$	$2\frac{\varphi(x)}{d}$	$\frac{\varphi(x)}{d}\cdot l\cdot T_{add}$	$\frac{\varphi(x)}{d}\cdot l\cdot l\cdot T_{mult}$
本文方案	$2\frac{\varphi(x)}{d}$	2	T_{add}	$2l\cdot T_{mult}$

本文方案将密文改为向量形式使其在计算效率上有 $l/2$ 倍效率的提升，而批处理技术的引入使得计算效率在这个基础上继续提升了 $\varphi(x)/d$ 倍，因此本文方案在效率上与 F-NTRU 方案相比总共提升了至少 $l\varphi(x)/2d$ 倍。就通信成本而言，本文方案中的明文空间均被划分为 $\varphi(x)/d$ 个明文槽，有着较低的通信成本和计算代价。通常来说，矩阵-向量乘法会比矩阵乘法计算快 $O(l^2)$ 个数量级，但是由于本文方案没有使用 Flatten 技术将密文进行二值化，乘法的取值计算化会比二值化数值慢，庆幸的是在计算大量值是 0 的矩阵向量乘积时实际花费的时间会大大缩短，因此本文方案使用矩阵-向量乘法取代矩阵乘法在效率上属于重大突破。

3.3 噪声分析

第 2.4 节给出了本文噪声增长的情况分析，为了与 F-NTRU 方案在噪声方面进行比较，这里给出对 F-NTRU 方案噪声增长的情况分析。

令 c_1' 与 c_2' 表示使用 F-NTRU 方案进行加密后的密文，对应的私钥为 f，$\boldsymbol{c}_3$ 代表新鲜密文进行一次乘法同态后的密文的第一行，v^* 代表进行一次乘法同态的噪声。根据 F-NTRU 方案乘法定义，有：

$$\boldsymbol{c}_3=(m_1\cdot m_2+c_{2,0}\cdot c_{1,(0,0)}+c_{2,0}\cdot m_1+c_{1,0}\cdot m_2+\cdots+c_{1,(0,l-1)}\cdot c_{2,l-1}) \tag{34}$$

其中，$c_{10}=hs_{10}+pe_{10}$，$c_{20}=hs_{20}+pe_{20}$，可得 $v_1=c_{10}$，$v_2=c_{20}$，通过与本文方案的噪声观察发现，F-NTRU 方案的噪声是将本文方案产生的噪声中的 $c_{1,j}\cdot c_{2,j}$ 替换成了 $c_{1,(0,j)}\cdot c_{2,j}$，因此该形式的噪声等同缩小为原来的 $1/l$，噪声 $\|v^*\|_\infty\leqslant 2E+E^2$。设第 i 层的噪声表示为 c^i，根据同态运算 $c^i=c^{i-1}*c^{i-1}$，F-NTRU 方案经过第 2 次乘法电路计算的噪声如下：

$$c^3=c^2*c^2=(2E+E^2)*(2E+E^2)=(2E+E^2)^2 \tag{35}$$

经过一次乘法同态，有两个明文进行了乘法同态运算，以此类推，经过深度为 L 的电路计算，噪声至多为：

$$\boldsymbol{c}^L=(2E+E^2)^L \tag{36}$$

只要 $(2E+E^2)^L$ 不超过 F-NTRU 方案的解密条件，即可保证密文解密正确。虽然本文方案进行一次乘法同态操作的噪声增长幅度比 F-NTRU 方案大，但是 F-NTRU 方案的噪声增长频率是本文方案的 $\varphi(x)/d$ 倍，因此本文方案在噪声中的性能更好。

结束语 本文提出了一种基于素数幂次阶分圆环的

NTRU 型全同态加密方案，在一定条件下能消除 DSPR 假设，使方案仅依赖于 RLWE 假设。该方案无需密钥交换，使用矩阵-向量乘法取代了复杂的矩阵乘法运算，与 F-NTRU 方案相比，本文方案的密文在存储、运输和计算上具有明显优势。

参 考 文 献

[1] LI R Q, JIA C F. A multi key homomorphic encryption scheme based on NTRU[J]. Acta Cryptologica Sinica, 2020, 7 (5): 683-697.

[2] GENTRY C. Fully Homomorphic Encryption Using Ideal Lattices[J]. Proceedings of the Annual Acm Symposium on Theory of Computing, 2009, 9(4): 169-178.

[3] BRAKERSKI Z. Fully homomorphic encryption without modulus switching from classical GapSVP[C]// Advances in Cryptology-CRYPTO, 2012. Springer Berlin Heidelberg, 2012: 868-886.

[4] GENTRY C, SAHAI A, WATERS B. Homomorphic encryption from learning with errors: Concept ually-simpler, Asymptotically faster, attribute based[C]// Advances in Cryptology (CRYPTO 2013). Berlin, Heidelberg: Springer, 2013: 75-92.

[5] DORÖZ Y, SUNAR B. Flattening NTRU for Evaluation Key Free Homomorphic Encryption [J]. Journal of Mathematical Cryptology, 2020, 14(1): 66-83.

[6] LI Z C, ZHANG J M, YANG Y T, et al. A Fully homomorphic Encryption Scheme Based on NTRU[J]. ACTA Electronica Sinica, 2018, 46(4): 938-944.

[7] KHEDR A, GULAK G. SecureMed: Secure Medical Computation Using GPU-Accelerated Homomorphic Encryption Scheme [J]. IEEE J Biomed Health Inform, 2018, 22(2): 597-606.

[8] ALBRECHT M, BAI S, DUCAS L. A subfifield lattice attack on overstretched NTRU assumptions[C]// Proceedings of Annual Cryptology Conference. Cham: Springer, 2016: 153-178.

[9] CHEONJ H, JEONG J, LEE C. An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without an encoding of zero[J]. LMS Journal of Computation and Mathematics, 2016, 19(A): 255-266.

[10] SMART N P, VERCAUTEREN F. Fully homomorphic SIMD operations[J]. Designs, Codes& Cryptography, 2014, 71: 57-81.

[11] MIGLIORE V, BONNORON G, FONTAINE C. Practical Parameters for Somewhat Homomorphic Encryption (SHE) Schemes on Binary Circuits[J]. IEEE Transactions on Computers, 2018, 67: 1550-1560.

[12] DORÖZ Y, HU Y, SUANR B. Homomorphic AES evaluation using the modified LTV scheme[J]. Designs, Codes and Cryptography, 2016, 80(2): 333-358.

[13] LÓPEZ-ALT A, TROMER E, VAIKUNTANATHAN V. On-the fly rnultiparty computation on the cloud via multikey fully homornorphic encryption[C]// Proceedings of the 44th Annual ACM Symposium on Theory of Comnputing. ACM, 2012: 1219-1234.

[14] YU Y, XU G, WANG X. Provably Secure NTRU Instances over Prime Cyclotomic Rings[C]// IACR International Workshop on Public Key Cryptography. 2017.

[15] STEHLÉ D, STEINFELD R. Making NTRU as secure as worst-case problems over ideal lattices[C]// Springer-Verlag. 2011.

[16] QIN X Y, HUANG R W. Research on the homomorphic encryption of NTRU system [J/OL]. Computer Application Research: 1-8. [2021-02-22]. https://doi. org/10. 19734/j. issn. 1001-3695. 2020. 07. 0213.

[17] RUDOLF L, HARALD N, COHN F M. Finite fields[M]. Cambridge University Press, 1997.

[18] CHEN Y L. Cyclotomic polynomials over finite fields[J]. Journal of Hubei Normal University (Natural Science Edition), 2012, 32 (2): 1-5.

[19] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[C]// Advances in Cryptology-EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. French Riviera: ACM, 2010.

[20] CHE X L, ZHOU H N, ZHOU T P, et al. Decryption structure of multi key homomorphic encryption scheme based on public key cryptosystem [J/OL]. Computer Application: 1-7. [2021-04-28]. http://kns. cnki. net/kcms/detail/51. 1307. TP. 20200604. 1434. 002. html.

[21] ZHOU H N, LI N B, CHE X L, et al. Multi key holomorphic scheme based on prime power order cyclotomic polynomial ring [J]. Information Network Security, 2020, 20 (5): 83-87.

[22] CHEON J H, KIM J, LEE M S, et al. CRT-based fully homomorphic encryption over the integers[J]. Information Sciences, 2015, 310: 149-162.

[23] ADRIANA L A, ERAN T, VINOD V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption[C]// Proceedings of the 44th symposium on Theory of Computing. ACM, 2012: 1219-1234.

[24] HOFFSTEIN J, SILVERMAN J. Optimizations for NTRU [J]. Proceedings Public Key Cryptography & Computational Number Theory, 2000.

[25] LYUBASHEVSKY V, PEIKERT C, REGEV O. A toolkit for ring-LWE cryptography[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer, 2013: 35-54.

QIN Xiao-yue, born in 1997, postgraduate, is a member of China Computer Federation. Her main research interests include holomorphic encryption of NTRU system and so on.

HUANG Ru-wei, born in 1978, Ph. D, professor, is a member of China Computer Federation. Her main research interests include cloud computing and homomorphic encryption.

（责任编辑：喻藜）