•网络空间安全•

DOI:10.15961/j.jsuese.201901197

本刊网刊

NTRU型多密钥全同态加密方案的优化

车小亮[1,2], 周潭平[1,2], 李宁波[2], 周昊楠[1], 刘龙飞[2], 杨晓元[1,2*]

(1.武警工程大学 密码工程学院, 陕西 西安 710086; 2.网络和信息安全武警部队重点实验室, 陕西 西安 710086)

摘　要:现有的NTRU型多密钥全同态加密方案多是基于2的幂次分圆多项式环构造的, 全同态计算过程使用了复杂的密钥交换操作, 这类方案容易遭受子域攻击, 且同态运算效率较低, 对此本文提出了一个安全性更好、效率更高的NTRU型多密钥全同态加密方案。首先, 将现有方案底层的分圆多项式环扩展应用到素数次分圆多项式环上, 给出了基于素数次分圆多项式环的NTRU型多密钥全同态加密的基础方案模型(B–MKFHE方案), 该方案模型可以抵御更多的子域攻击。其次, 在B–MKFHE方案模型的基础上, 通过扩展密文多项式维度, 优化了NTRU型多密钥同态运算结构, 使得同态运算过程不再需要复杂耗时的密钥交换操作。最后, 根据优化的多密钥同态运算结构, 结合模交换技术, 构造了无需密钥交换的层级的NTRU型多密钥全同态加密方案(M–MKFHE方案)。分析结果表明, 本文提出的M–MKFHE方案能有效抵御子域攻击, 满足IND–CPA安全。与B–MKFHE方案相比, M–MKFHE方案具有更小的存储开销和计算开销, 同态运算过程中产生的噪声值较小, 运算效率较高, 且支持更深层次的同态运算。

关键词:NTRU型多密钥全同态加密; 素数次分圆多项式环; 密文扩展; 同态运算结构; IND–CPA安全

中图分类号:TP391　　**文献标志码**:A　　**文章编号**:2096-3246(2020)05-0186-08

Optimization of NTRU-type Multi-key Fully Homomorphic Encryption Scheme

CHE Xiaoliang[1,2], *ZHOU Tanping*[1,2], *LI Ningbo*[2], *ZHOU Haonan*[1], *LIU Longfei*[2], *YANG Xiaoyuan*[1,2*]

(1.School of Cryptographic Eng., Eng. Univ. of PAP, Xi'an 710086, China; 2.Key Lab. of Network and Info. Security of PAP, Xi'an 710086, China)

Abstract: The previous NTRU-type multi-key fully homomorphic encryption (MKFHE) schemes were constructed over power-of-2 cyclotomic polynomial rings, and the complicated key-switching operations were used in the schemes to complete the fully homomorphic computation. They were suffered from the subfield attacks and had low evaluating efficiency. In this paper, an NTRU-type MKFHE scheme with better security and higher efficiency was proposed. Firstly, the prime cyclotomic polynomial ring was applied to the previous NTRU-type MKFHE schemes, and a NTRU-type MKFHE basic scheme model (B–MKFHE) that could resist more subfield attacks was presented. Secondly, based on the B–MKFHE model, the NTRU-type multi-key homomorphic evaluating structure was optimized by extending the dimension of ciphertext polynomial, so that the complicated and time-consuming key-switching operations were eliminated when running the homomorphic operations. Finally, combined the optimized multi-key homomorphic evaluating structure and modulus-switching technology, a leveled NTRU-type MKFHE scheme (M–MKFHE) without key-switching operations was constructed. The result showed that the proposed M–MKFHE scheme could resist the subfield attacks well and was proved to be IND–CPA security. Compared with the B–MKFHE, the memory (bit-size) and evaluating costs of the M–MKFHE are reduced, and the error magnitude is decreased in the homomorphic evaluating process. In all, the M–MKFHE scheme has higher evaluating efficiency and supports deeper homomorphic evaluations.

收稿日期:2019 – 12 – 16

基金项目:国家重点研发计划项目(2017YFB0802000); 国家自然科学基金项目(U1636114); 国家密码发展基金项目(MMJJ20170112); 陕西省自然科学基金项目(2020JQ-492)

作者简介:车小亮(1987—), 男, 博士生. 研究方向: 信息安全; 密码学. E-mail: xawjchexl@126.com

* 通信联系人 E-mail: xyyangwj@126.com

网络出版时间:2020 – 09 – 15 11 : 40 : 33　　**网络出版地址**:https://kns.cnki.net/kcms/detail/51.1773.TB.20200914.1907.004.html

Key words: NTRU-type MKFHE; prime cyclotomic rings; ciphertext extension; homomorphic evaluating structure; indistinguish-ability under chosen-plaintext attack (IND–CPA) secure

多密钥全同态加密允许对不同用户的密文进行同态运算，运算之后的结果可以由参与计算的用户的密钥联合解密，被广泛应用于安全多方计算[1]、密文检索[2]、隐私保护[3–4]等领域。2012年，López–Alt等[5]首次提出了多密钥全同态加密（multi-key fully homomorphic encryption, MKFHE）的概念，并利用密钥交换技术和模交换技术设计了NTRU型多密钥全同态方案（LTV12方案）。随后，密码学研究者提出了GSW（Gentry–Sahai–Waters）型MKFHE方案、BGV（Brakerski–Gentry–Vaikuntanathan）型MKFHE方案。GSW型MKFHE方案包含，如Clear等[6]提出的CM15方案、Mukherjee等[7]提出的经典的MW16方案、Peikert等[8]提出的满足多跳（multi-hop）的PS16方案，以及Brakershi等[9]提出的BP16方案；BGV型MKFHE方案包含，如Chen等[10]首次提出的CZW17方案、Li等[11]提出的LZY+19方案，以及Chen等[12]提出的CDKS19方案。2019年，Chen等[13]又提出了高效的TFHE（fully homomorphic encryption over the torus）型MKFHE方案。相比较而言，NTRU型MKFHE方案具有加解密速度快、密文尺寸小、密钥量少等优势，它是满足现实应用的快速备选方案，具有较高的理论研究价值和应用价值。

LTV12方案[5]是层级的NTRU型多密钥全同态加密方案，其安全性是基于2的幂次分圆多项式环（$\mathbb{Z}[x]/(x^n+1)$，其中，n为2的幂次）上误差学习（ring learning with errors, RLWE）问题[14]和判定性小多项式比（decisional small polynomial ratio, DSPR）问题[5]。该方案的结构特点是利用密钥交换技术[15]（key-switching）对密文乘积非线性部分进行重线性化，并利用模交换技术[15]（modulus-switching）对不同电路层级的噪声进行约减，以实现全同态运算。目前的研究表明，2的幂次方分圆多项式环可选数量少，且容易遭受子域攻击[16]，因此LTV12方案的安全性受到威胁。针对这个问题，2017年，Yu等[17]提出了基于素数次分圆多项式环的NTRU型单密钥同态加密方案，使得方案中环的选择更加灵活，并且能够抵抗大多数子域攻击。另外，LTV12方案的解密过程中需要反复使用密钥交换技术完成密文重线性化操作，使得其运算复杂，噪声增长过快。Doröz等[18]通过优化LTV12参数，并引入批量处理等技术[19]，提出了较高效的方案DHS16。Bos等[20]使用张量积技术对LTV12方案进行了改进，参数选取满足DSPR问题归约到RLWE问题的条件[21]，使改进方案的安全性仅依赖于RLWE问题。Chen[22]利用提升维数法优化了NTRU型同态加密方案的解密结构，提升了同态运算效率。但上述文献[17–22]成果仅限于NTRU型单密钥全同态加密方案。NTRU型多密钥同态加密研究方面，Chongchitmate等[23]给出了从MKFHE到电路隐私的多密钥全同态加密方案的通用转化框架CO17，并构造了具有电路隐私性的3轮动态安全多方计算协议。现有的NTRU型MKFHE研究成果相对较少，且在增强方案的安全性，提升全同态运算效率方面还有很大研究空间。

本文为解决上述问题，首先在提升安全性方面，将现有的NTRU型MKFHE方案基于的2的幂次分圆多项式环扩展应用到素数次分圆多项式环上，给出了基于素数次分圆多项式环上的基础方案模型（B–MKFHE方案）；其次在提高效率方面，在该安全的方案模型的基础上，对NTRU型多密钥同态运算结构进行优化，以消除复杂的密钥交换操作；最后，利用优化后的同态运算结构，结合模交换技术，构造一个高效的NTRU型MKFHE方案（M–MKFHE方案）。

1　相关理论及关键技术

1.1　预备知识

$\boldsymbol{v}\cdot\boldsymbol{w}=\langle\boldsymbol{v},\boldsymbol{w}\rangle=v_1w_1+v_2w_2+\cdots+v_nw_n$表示向量$\boldsymbol{v},\boldsymbol{w}\in R^n$（$n$为整数）的内积，其中，$v_1$为向量$\boldsymbol{v}$的第1个元素。对于$n$维向量$\boldsymbol{v}$，定义其无穷范数$\|\boldsymbol{v}\|_\infty=\max\{|v_1|,|v_2|,\cdots,|v_n|\}$。$l_1$范数表示为$\|\boldsymbol{v}\|_1=\sum_{i=1}^{n}|v_i|$。对于分布$D$，$x\leftarrow D$表示$x$取值于$D$。对于任意分布$x\leftarrow D$，若$\|x\|_\infty\le B$，则称分布$D$的上界为$B$。

素数次分圆多项式环即为环$R=\mathbb{Z}[x]/\phi(x)$，其中，$\phi(x)=x^{n-1}+x^{n-2}+\cdots+1$，$n$是素数。存在素数$q=q(\lambda)$（$\lambda$是安全参数）满足$q=1 \bmod n$，则定义环$R_q=R/qR$中多项式系数取值区间为$[-q/2,q/2)$，其中，$q$不等于2。令$\chi$为环$R$上的错误分布，设$\chi$的上界为$B$，则$\chi$中多项式的系数均在$[-B,B]$之间。即当$a\leftarrow\chi$时，则$\|a\|_\infty\le B$。

引理1[17]　对于素数次分圆多项式环$R=\mathbb{Z}[x]/\phi(x)$，其中，$\phi(x)=x^{n-1}+x^{n-2}+\cdots+1$（$n$是素数），存在任意$a,b\in R$，则有$\|ab\|_\infty\le 2(n-1)\|a\|_\infty\|b\|_\infty$。当$R$的上界为$B$，则有$\|ab\|_\infty\le 2(n-1)B^2$。

引理2[5]　对于素数次分圆多项式环$R=\mathbb{Z}[x]/\phi(x)$，其中，$\phi(x)=x^{n-1}+x^{n-2}+\cdots+1$（$n$是素数），$\chi$是环$R$上的错误分布，设$\chi$的上界是$B$，令$s_1,s_2,\cdots,s_k\leftarrow\chi$，

则有$\left\|\prod_{i=1}^{k} s_i\right\|_{\infty} \leq 2^{k-1}(n-1)^{(k-1)}B^k$。

1.2 困难问题

1)基于素数次分圆多项式环的LWE问题(RLWE$_{\phi,q,\chi}$问题)

定义1 给定安全参数λ, $q=q(\lambda)\in\mathbb{Z}$为一个素整数, $\phi(x)=x^{n-1}+x^{n-2}+\cdots+1$是一个素数次分圆多项式, n是素数。令$R=\mathbb{Z}(x)/\phi(x)$和$R_q=R/qR$。χ是环R上的错误分布。RLWE$_{\phi,q,\chi}$问题是指区分以下两个元组是困难的:一是,元组$(\boldsymbol{a}_i,u)$在R_q^{n+1}上是随机均匀分布的;二是,随机均匀选取$e\leftarrow\chi$,向量$\boldsymbol{a}_i,\boldsymbol{s}\in R_q^n$,计算得到的元组$(\boldsymbol{a}_i,\boldsymbol{a}_i\cdot\boldsymbol{s}+e)\in R_q^{n+1}$。

2)基于素数次分圆多项式环的DSPR假设(DSPR$_{\phi,q,\chi}$假设)

定义2 给定安全参数λ, $q=q(\lambda)\in\mathbb{Z}$为一个素整数, $\phi(x)=x^{n-1}+x^{n-2}+\cdots+1$是一个素数次分圆多项式, n是素数。定义多项式环$R=\mathbb{Z}(x)/\phi(x)$和$R_q=R/qR$,以及环R上的错误分布χ。DSPR$_{\phi,q,\chi}$问题是指难以区分以下两个多项式:一是,多项式$h=2g/f$,其中,$f=2f'+1$且在R_q上可逆,$f',g\leftarrow\chi$;二是,在$R_q=R/qR$上随机均匀采样得到的多项式h。

1.3 关键技术

1)比特分解技术[24]。全同态加密方案中经常用到BitDecomp(·)函数和Powersof2(·)函数进行比特位展开。令$l=\lceil\log q\rceil$,这两个函数具体表述为:

①BitDecomp$(x\in R_q):R_q\mapsto R_2^l$:对于多项式$x\in R_q$,输出$(x_0,x_1,\cdots,x_{l-1})\in R_2^l$。(简述为BitD$(x)\in R_2^l$)。

②Powersof2$(y\in R_q):R_q\mapsto R_q^l$:对于多项式$y\in R_q$,输出$(y,2y,\cdots,2^{l-1}y)$,其中$2^{l-1}<q/2$。(简述为Pof2$(y)\in R_q^l$)。

对于多项式$x,y\in R_q$,很容易验证:$\langle\text{BitD}(x),\text{Pof2}(y)\rangle=\langle x,y\rangle \bmod q$。

2)密钥交换技术(key-switching)[15]。将对应的密文由$c_1\in R_q$(对应的解密密钥为f_1)转换成为密文$c_2\in R_q$(对应的解密密钥为f_2)。令$l=\lceil\log q\rceil$, $\tau=1,2,\cdots,l$,则有:

①KeySwitchGen$(f_1\in R_q,f_2\in R_q)$:给定$h_2\in R_q$,使得$f_2\cdot h_2(\bmod q \bmod 2)=1$,选取向量$\boldsymbol{s}_\tau,\boldsymbol{e}_\tau\leftarrow\chi^l$。输出计算密钥向量$\boldsymbol{\gamma}_\tau=h_2\boldsymbol{s}_\tau+2\boldsymbol{e}_\tau+\text{Pof2}(f_1)\in R_q^l$。

②KeySwitch$(c_1,\boldsymbol{\gamma}_\tau,q)$:计算中间密文向量$\boldsymbol{c}=\text{BitD}(c_1)\in R_q^l$,输出密文$c_2=\boldsymbol{c}\cdot\boldsymbol{\gamma}_\tau=[\langle\text{BitD}(c_1),\boldsymbol{\gamma}_\tau\rangle]_q\in R_q$。

显然,$c_2f_2=c_1f_1+e$,其中e代表密钥交换过程产生的噪声。

3)模交换技术(modulus-switching)[15]。模交换技术可以将模q下的密文c转换成较小的模p($p=q \bmod 2$)下密文c',保证在同样私钥正确解密条件下,噪声规模减小p/q倍。函数具体表述为:

ModulusSwitch(c,q,p):输入$c\in R_q$和较小的模数p,输出一个无限接近$(p/q)\cdot c$的密文$c'\in R_p$,且满足$c'=c \bmod 2$。

2 NTRU型MKFHE的同态运算的基础结构及优化

2.1 基于素数次分圆多项式环上的NTRU型MKFHE基础方案模型

不改变现有NTRU型MKFHE方案的同态运算结构,而优化底层应用的分圆多项式环,可以得到基于素数次分圆多项式环上的NTRU型多密钥全同态加密基础方案模型,即B–MKFHE(basic model of MKFHE)。

2.1.1 基础方案模型

假设两个用户集为K_1、K_2,每个集合有N个用户。不失一般性,设常数$1<d<r-s$, $K_1\cap K_2=\{pk_{d+1},pk_{d+2},\cdots,pk_{d+s}\}$, $K=K_1\cup K_2=\{pk_1,pk_2,\cdots,pk_r\}$,其中$N\leq r\leq 2N$。则联合私钥为$F_K=sk_1sk_2\cdots sk_r$。B–MKFHE基础方案模型的具体表述如下:

1)B – MKFHE.Setup(1^λ):安全参数为λ,素数次分圆多项式环为$R=\mathbb{Z}(x)/x^{n-1}+x^{n-2}+\cdots+1$和$R_q=R/qR$,参数$n$和$q=q(\lambda)$为素整数,$R$中上界为$B=B(\lambda)$的错误分布$\chi$。定义一系列递减的模数$q_0>q_1>\cdots>q_L$,令$B\ll q_L$, $i\in\{0,1,\cdots,L\}$, $l_i=\lceil\log q_i\rceil$。

2)B – MKFHE.KeyGen$(1^n,1^L)$:选取$g^{(i)}$, $f'^{(i)}\leftarrow\chi$,令$f^{(i)}=2f'^{(i)}+1$,使得$f^{(i)}\equiv 1 \bmod 2$,且$f^{(i)}$在R_{q_i}上可逆,若不可逆则重新选取$f'^{(i)}\leftarrow\chi$。令$h^{(i)}=2g^{(i)}/f^{(i)}\in R_{q_{i-1}}$,则$pk=h_0\in R_{q_0}$, $sk=f^{(L)}\in R_{q_L}$;对$\tau\in\{0,1,\cdots,l_{i-1}-1\}$。选取向量$\boldsymbol{s}_\tau^{(i)},\boldsymbol{e}_\tau^{(i)}\leftarrow\chi^{l_{i-1}}$,对用户$t(t\in[r])$,生成计算密钥向量为:

$$\begin{cases}\boldsymbol{\gamma}_{t,\tau}^{(i)}=h_t^{(i)}\boldsymbol{s}_\tau^{(i)}+2\boldsymbol{e}_\tau^{(i)}+\text{Pof2}\left(f_t^{(i-1)}\right)\in R_{q_{i-1}}^{l_{i-1}},\\ \boldsymbol{\zeta}_{t,\tau}^{(i)}=h_t^{(i)}\boldsymbol{s}_\tau^{(i)}+2\boldsymbol{e}_\tau^{(i)}+\text{Pof2}\left(\left(f_t^{(i-1)}\right)^2\right)\in R_{q_{i-1}}^{l_{i-1}}。\end{cases}$$

输出$(pk,sk,evk)=\left(h,f,\{\boldsymbol{\gamma}_{t,\tau}^{(i)},\boldsymbol{\zeta}_{t,\tau}^{(i)}\}\right)$。

3)B – MKFHE.Enc(pk,m):选取参数$\bar{s},\bar{e}\leftarrow\chi$,用公钥$pk$加密明文$m$,输出$c^{(0)}=h_0\bar{s}+2\bar{e}+m\in R_{q_0}$。

4)B – MKFHE.Dec$(sk_1,sk_2,\cdots,sk_N,c^{(L)})$:输入密文$c^{(L)}\in R_{q_L}$,令$u=(sk_1sk_2\cdots sk_N)\cdot c^{(L)}\in R_{q_L}$。输出$m'=u \bmod 2$。

5)B – MKFHE.Eval.Add$(c_1^{(i)},c_2^{(i)})$:输入两个联合密文$c_1^{(i)},c_2^{(i)}\in R_{q_i}$,分别对应的用户公钥集合$K_1$、$K_2$,令$j\in[r]$,则:①计算两个密文的和$c_0^{(i)}=c_1^{(i)}+c_2^{(i)}\in R_{q_i}$;②计算$c_j^{(i)}=\text{KeySwitch}(c_{j-1}^{(i)},\boldsymbol{\gamma}_{t,\tau}^{(i+1)},q_i)$;③令$c_{\text{add}}^{(i)}=c_r^{(i)}$,计算$c_{\text{add}}^{(i+1)}=(q_{i+1}/q_i)\cdot c_{\text{add}}^{(i)}(\bmod 2)$。

6) B−MKFHE.Eval.Mult($c_1^{(i)}, c_2^{(i)}$): 输入两个联合密文$c_1^{(i)}, c_2^{(i)} \in R_{q_i}$, 分别对应的用户公钥集合$K_1$、$K_2$, 令$j \in [r]$, 则: ①计算两个密文的积$c_0^{(i)} = c_1^{(i)} \cdot c_2^{(i)} \in R_{q_i}$。②当$pk_j \in K_1 \cap K_2$时, 计算$c_j^{(i)} = \text{KeySwitch}(c_{j-1}^{(i)}, \boldsymbol{\zeta}_{t,\tau}^{(i+1)}, q_i)$; 否则, 计算$c_j^{(i)} = \text{KeySwitch}(c_{j-1}^{(i)}, \boldsymbol{\gamma}_{t,\tau}^{(i+1)}, q_i)$。③令$c_{\text{mult}}^{(i)} = c_r^{(i)}$, 计算$c_{\text{mult}}^{(i+1)} = (q_{i+1}/q_i) \cdot c_{\text{mult}}^{(i)} (\text{mod } 2)$。

B−MKFHE是基于素数次分圆多项式环上现有NTRU型MKFHE的通用方案模型, 根据文献[17]可知, 其可以抵御更多的子域攻击。但其同态运算结构没有改变, 仍需要循环使用密钥交换操作完成全同态运算。

2.1.2 B−MKFHE的同态运算

由文献[5]可知, 基础方案模型B−MKFHE满足加法和乘法同态性, 且能在任意电路层级完成正确解密。下面以在第$i+1$层完成乘法解密为例, 详细分析B−MKFHE同态解密运算的复杂性和产生的噪声值。对第$i+1$层同态运算后的密文进行解密, 可得:

$$c_{\text{mult}}^{(i+1)} \cdot F_K^{(i+1)} = (q_{i+1}/q_i) \cdot c_{\text{mult}}^{(i)} \cdot F_K^{(i+1)} (\text{mod } 2) \quad (1)$$

因为, $c_{\text{mult}}^{(i)} = \text{BitD}(c_{r-1}^{(i)})(h_r^{(i+1)} \boldsymbol{s}_\tau^{(i+1)} + 2\boldsymbol{e}_\tau^{(i+1)}) + f_r^{(i)} c_{r-1}^{(i)}$, 所以对于$c_{\text{mult}}^{(i)} \cdot F_K^{(i+1)}$, 当$pk_j \in K_1 \cap K_2$时, 经过$r$次循环的密钥交换操作, 可得:

$$\begin{aligned} c_{\text{mult}}^{(i)} F_K^{(i+1)} = {} & \text{BitD}(c_{r-1}^{(i)}) F_K^{(i+1)} \left(h_r^{(i+1)} \boldsymbol{s}_\tau^{(i+1)} + 2\boldsymbol{e}_\tau^{(i+1)}\right) + \\ & \prod_{j=2}^{d} f_j^{(i)} \sum_{j=2}^{d} \text{BitD}(c_{j-1}^{(i)}) F_K^{(i+1)} \left(h_j^{(i+1)} \boldsymbol{s}_\tau^{(i+1)} + 2\boldsymbol{e}_\tau^{(i+1)}\right) + \\ & \prod_{j=d+s+1}^{r-1} f_j^{(i)} \sum_{j=d+s+1}^{r-1} \text{BitD}(c_{j-1}^{(i)}) F_K^{(i+1)} \left(h_j^{(i+1)} \boldsymbol{s}_\tau^{(i+1)} + 2\boldsymbol{e}_\tau^{(i+1)}\right) + \\ & \prod_{j=d+1}^{d+s} (f_j^{(i)})^2 \sum_{j=d+1}^{d+s} \text{BitD}(c_{j-1}^{(i)}) F_K^{(i+1)} \left(h_j^{(i+1)} \boldsymbol{s}_\tau^{(i+1)} + 2\boldsymbol{e}_\tau^{(i+1)}\right) + \\ & F_K^{(i+1)} \left(F_{K_1}^{(i)} F_{K_2}^{(i)} c_0^{(i)}\right) \end{aligned} \quad (2)$$

式中, 因为$F_{K_1}^{(i)} F_{K_2}^{(i)} c_0^{(i)} = F_{K_1}^{(i)} F_{K_2}^{(i)} m_1 m_2 + e_{\text{mult}}$, 所以$c_{\text{mult}}^{(i)} \cdot F_K^{(i+1)} (\text{mod } 2) = m_1 m_2$, 其中, e_{mult}表示解密过程产生的噪声值。由此可见, 完成正确解密需要经过r次循环的密钥交换操作, 运算过程复杂, 产生的噪声值较大。

设在任一电路层初始解密产生的噪声值为$\|c_1^{(i)} \cdot F_{K_1}^{(i)}\|_\infty = \|c_2^{(i)} \cdot F_{K_2}^{(i)}\|_\infty = \psi_0$。根据文献[5], 并由引理2易知, $\psi_0 < 2^{3N-1}(n-1)^{2N-1}(2B+1)^{2N}$。为了表述方便, 令$E_r = 2^{r-1}(n-1)^{(r-1)}(2B+1)^r$, 又因为噪声的上界$B$的选取适用于所有层级同态运算, 根据引理1和引理2可得:

$$\|\text{BitD}(c_{j-1}^{(i)})(h_j^{(i+1)} \boldsymbol{s}_\tau^{(i+1)} + 2\boldsymbol{e}_\tau^{(i+1)}) F_K{}^{(i+1)}\|_\infty \le \frac{3}{2}(n-1)\lceil \log q_i \rceil E_{r+1} \quad (3)$$

进一步可得最终产生的噪声为:

$$\begin{aligned} \|\tilde{c}_{\text{mult}}^{(i)} F_K^{(i+1)}\|_\infty \le {} & \frac{3}{2}(n-1)\lceil \log q_i \rceil E_{r+1} + \\ & \frac{3}{2}(n-1)\lceil \log q_i \rceil E_{r+1} \left(\sum_{j=2, j=d+s+1}^{d, r-1} E_j + \sum_{j=d+1}^{d+s} E_{2j} \right) + \\ & 4(n-1)^2 E_r \psi_0^2 < \frac{3}{4}\lceil \log q_i \rceil E_{2r+s+1} + 4(n-1)^2 E_r \psi_0^2 \end{aligned} \quad (4)$$

将$\psi_0 < 2^{3N-1}(n-1)^{2N-1}(2B+1)^{2N}$代入式(4), 可得产生噪声的量级为$\|\tilde{c}_{\text{mult}}^{(L-1)} F_K^{(L)}\|_\infty = O\left((nB)^{4N}\right)$。

通过分析, B−MKFHE相比于现有的LTV12方案[5]和CO17方案[23], 其安全性基于$\text{DSPR}_{\phi,q,\chi}$和$\text{RLWE}_{\phi,q,\chi}$问题, 能抵御更多的子域攻击。但是, 并没有改变原有的同态运算结构, 导致同态运算过程复杂, 产生的噪声值较大。主要体现在: 一是, 在任一电路层级完成解密, 需要进行r次密钥交换操作; 二是, 产生的噪声同时受第i层和第$i+1$层联合解密私钥的影响, 噪声增长过快。所以, 在保证安全的前提下, 提高同态运算效率, 需要在B−MKFHE的基础上优化同态运算结构和同态运算过程。

2.2 NTRU型多密钥同态运算结构的优化

文献[20,22]对NTRU型单密钥同态加密研究结果表明, 将密文多项式转换成多项式向量的形式, 可以减少或消除同态运算过程的密钥交换操作。作者通过扩展密文多项式, 并结合比特分解技术, 优化NTRU型多密钥同态运算结构, 以消除同态运算过程中的密钥交换操作。

2.2.1 优化方法

在B−MKFHE的基础上进行优化, 使用的素数次分圆多项式环同样是R_q。令$K = K_1 \cup K_2 = \{pk_1, pk_2, \cdots pk_r\}$, 其中$N \le r \le 2N$。给定安全参数$\lambda$, 选取$g, f' \leftarrow \chi$, 令$f = 2f' + 1$, 使得$f \equiv 1 \pmod 2$且在$R_q$上可逆。令$pk = h \in R_q$, $sk = f \in R_q$, $l = \lceil \log q \rceil$。

具体的优化方法是: 将明文m_0转换成向量形式$\boldsymbol{m} = (m_0, 2m_0, \cdots, 2^{l-1}m_0)$, 以扩展密文的维度。并结合BitDecomp(·)函数, 优化同态乘法运算结构。具体步骤如下:

1) 密文扩展。对任一用户$t(t \in [r])$, 用公钥pk_t加密其明文向量$\boldsymbol{m}_t' = (m_t, 2m_t, \cdots, 2^{l-1}m_t)$, 选取向量$\boldsymbol{s}_t, \boldsymbol{e}_t \leftarrow \chi^l$, 输出$\bar{\boldsymbol{c}} = \boldsymbol{m}_t' + h_t \boldsymbol{s}_t + 2\boldsymbol{e}_t \in R_q^l$。

2) 同态运算结构转换。对于两个联合密文向量$\bar{\boldsymbol{c}}_1$, $\bar{\boldsymbol{c}}_2 \in R_q^l$, 对应联合解密私钥为$F_{K_1}$、$F_{K_2}$。进行同态加法运算$\bar{\boldsymbol{c}}_{\text{add}} = \bar{\boldsymbol{c}}_1 + \bar{\boldsymbol{c}}_2 \in R_q^l$, 及同态乘法运算$\bar{\boldsymbol{c}}_{\text{mult}} = \text{BitD}(\bar{\boldsymbol{c}}_1) \cdot \bar{\boldsymbol{c}}_2 \in R_q^l$。

3) 选取解密项。取同态运算后的密文向量$\bar{\boldsymbol{c}}_{\text{add/mult}}$的第1项$\bar{c}_{\text{add/mult},1}$, 令$u = F_K \bar{c}_{\text{add/mult},1} = (sk_1 sk_2 \cdots sk_r) \cdot \bar{c}_{\text{add/mult},1} \in$

R_q, 输出明文 $m'=u \bmod 2$。

2.2.2 正确性验证

设$\bar{\boldsymbol{c}}_1F_{K_1}=\boldsymbol{m}'_1F_{K_1}+\boldsymbol{e}'_1$, $\bar{\boldsymbol{c}}_2F_{K_2}=\boldsymbol{m}'_2F_{K_2}+\boldsymbol{e}'_2$, 令$\|\boldsymbol{e}'_1\|_\infty=\|\boldsymbol{e}'_2\|_\infty=\eta$。同态加法运算同B−MKFHE, 满足同态加法运算的正确性。对于同态乘法运算, 解密时由$\bar{\boldsymbol{c}}_{\text{mult}}\cdot F_K(\bmod 2)=\text{BitD}(\bar{\boldsymbol{c}}_1)\cdot\bar{\boldsymbol{c}}_2\cdot F_K(\bmod 2)$, 取第1项可得:

$$\bar{c}_{\text{mult},1}F_K=m_1m_2F_K+\left(m_2F_{K-K_1}e'_{1,1}+\sum_{j=1}^{l}(c_{1,1})_jF_{K-K_2}e'_{2,1}\right) \tag{5}$$

式中, $c_{1,1}$为系数为1或0的多项式, 且有$\|e'_{1,1}\|_\infty=\|\boldsymbol{e}'_1\|_\infty$, $\|e'_{2,1}\|_\infty=\|\boldsymbol{e}'_2\|_\infty$。式(5)即为优化后的同态运算结构形式, 解密时不用考虑$K_1\cap K_2$是否为空的情况, 消除了密钥交换的操作过程。所以, 只要满足$\|\bar{c}_{\text{mult},1}F_K\|_\infty\le q/2$条件, 即可解密成功。

2.2.3 噪声分析

假设联合密文向量$\bar{\boldsymbol{c}}_1$、$\bar{\boldsymbol{c}}_2$均是N个用户的新鲜密文按照第2.2.1节优化方法相乘得到的, 则易得$\eta<(3/2)E_{N+2}+3N(n-1)E_{N+1}$。所以, 由式(5)可得产生的噪声值为:

$$\begin{aligned}&\|\bar{c}_{\text{mult},1}F_K\|_\infty=\\&\quad\|m_1m_2F_K+m_2F_{K-K_1}e'_{1,1}+\sum_{j=1}^{l}(c_{1,1})_jF_{K-K_2}e'_{2,1}\|_\infty=\\&\quad\|m_1m_2F_K\|_\infty+\|m_2F_{K-K_1}e'_{1,1}\|_\infty+\|\sum_{j=1}^{l}(c_{1,1})_jF_{K-K_2}e'_{1,1}\|_\infty\le\\&\quad E_r+2(n-1)E_{r-N}\eta+\left(4(n-1)^2l\right)E_{r-N}\eta\end{aligned} \tag{6}$$

将$\eta<(3/2)E_{N+2}+3N(n-1)E_{N+1}$值代入式(6), 即可得产生的噪声量级为$\|\bar{c}_{\text{mult},1}F_K\|_\infty=O\left((nB)^{2N}\right)$。

由此可见, 优化的NTRU型多密钥同态运算结构, 消除了同态乘法运算利用密钥交换技术进行的密文重线性化操作, 使得产生的噪声量级较B−MKFHE呈指数级别降低。

3 基于素数次分圆多项式环上高效的NTRU型MKFHE方案

虽然, 第2.2节优化的同态运算结构能降低噪声值, 但是, 受参与用户数量的影响, 随着同态运算深度的增加, 噪声增长较快, 无法完成全同态运算。作者结合模交换技术, 构造一个层级的NTRU型多密钥全同态加密方案。由于密文被扩展成多项式向量形式, 模交换之后, 需要解决层级间密文向量的维度不一致问题, 以实现新用户在任一电路层的实时加入。

3.1 密文向量维度的统一

第2.2节优化结构的密文是向量形式, 而使用模交换技术, 会造成不同层级之间密文向量维度不同。设$q_i>q_{i+1}$, 则$l_{i+1}=\lceil\log q_{i+1}\rceil<l_i=\lceil\log q_i\rceil$。设在第$i$层的密文向量为$\bar{\boldsymbol{c}}^{(i)}\in R_{q_i}^{l_i}$, 则第$i+1$层的密文向量为$\bar{\boldsymbol{c}}^{(i+1)}\in R_{q_{i+1}}^{l_{i+1}}$。所以, 随着运算层级的增大, 密文维度减小。要实现不同层级同态运算的正确性, 则需要在变化层级之后统一密文向量的维度。下面实现的方法是定义一个去尾函数DT(discard the tail)进行密文维度的缩减, 具体见定义3。

定义3 DT$(l_i,l_{i+1},\boldsymbol{v}\in R_{q_i}^{l_i})$函数: 当输入为$l_i,l_{i+1},\boldsymbol{v}\in R_{q_i}^{l_i}$时输出$\tilde{\boldsymbol{v}}\in R_{q_i}^{l_{i+1}}$。

定义3表示去掉向量$\boldsymbol{v}\in R_{q_i}^{l_i}$的$l_{i+1}+1\to l_i$项, 使$l_i$维向量$\boldsymbol{v}\in R_{q_i}^{l_i}$转换成为$l_{i+1}$维向量$\tilde{\boldsymbol{v}}\in R_{q_i}^{l_{i+1}}$。

每次模交换完成进入下一层级运算之前, 通过DT函数重新遍历密文向量元素, 使得密文向量维度符合下一层同态运算要求。

3.2 新用户的实时加入

NTRU型方案支持不同密钥对应的密文之间进行同态运算, 无需进行密文扩展, 就能实现新用户的加入。由于优化后的同态运算结构的密文是向量形式, 引入模交换技术之后, 随着电路层级的变化, 密文向量的维度也在变化, 所以, 要实现新用户的加入, 必须使密文维度与对应电路层级相适应, 以保证运算的正确性。

以在第i层和第$i+1$层同态乘法运算为例, 设$q_i>q_{i+1}$, 第i层两个用户集合K_1、K_2对应的密文向量为$\tilde{\boldsymbol{c}}_1^{(i)},\tilde{\boldsymbol{c}}_2^{(i)}\in R_{q_i}^{\lceil\log q_i\rceil}$。根据第2.2节的优化方法, $\tilde{\boldsymbol{c}}_1^{(i)}$、$\tilde{\boldsymbol{c}}_2^{(i)}$分别为$N$个用户的联合密文向量。在第$i$层完成同态乘法, 可得$\tilde{\boldsymbol{c}}_{\text{mult}}^{(i)}=\text{BitD}(\tilde{\boldsymbol{c}}_1^{(i)})\cdot\tilde{\boldsymbol{c}}_2^{(i)}\in R_{q_i}^{\lceil\log q_i\rceil}$, 对应的联合解密密钥为$F_K^{(i)}=f_1f_2\cdots f_r$。转换到第$i+1$层时, 经过模交换操作可得$\tilde{\boldsymbol{c}}_3^{(i+1)}=(q_{i+1}/q_i)\cdot\tilde{\boldsymbol{c}}_{\text{mult}}^{(i)}\in R_{q_{i+1}}^{\lceil\log q_i\rceil}$, 假设在第$i+1$层, 新用户$i_t$(对应解密私钥为$f_{i_t}$, 密文向量$\tilde{\boldsymbol{c}}_{i_t}^{(i+1)}\in R_{q_{i+1}}^{\lceil\log q_{i+1}\rceil}$)加入同态运算。由于向量维度不同, 使得运算无法继续进行, 需要运行DT函数, 转换密文向量$\tilde{\boldsymbol{c}}_3^{(i+1)}$的维度, 得到转换后的密文向量:

$$\tilde{\tilde{\boldsymbol{c}}}_3^{(i+1)}=\text{DT}\left(\lceil\log q_i\rceil,\lceil\log q_{i+1}\rceil,\tilde{\boldsymbol{c}}_3^{(i+1)}\right)\in R_{q_{i+1}}^{\lceil\log q_{i+1}\rceil} \tag{7}$$

维度统一之后, 在第$i+1$层进行同态乘法运算可得$\tilde{\boldsymbol{c}}_{\text{mult}}^{(i+1)}=\text{BitD}(\tilde{\tilde{\boldsymbol{c}}}_3^{(i+1)})\cdot\boldsymbol{c}_{i_t}^{(i+1)}\in R_{q_{i+1}}^{\lceil\log q_{i+1}\rceil}$, 对应的联合解密密钥为$F_{K'}^{(i+1)}=F_K^{(i)}f_{i_t}$。可见, 优化后的同态运算结构同样无需扩展联合密文, 就能实现新用户加入同态运算。

3.3 高效的NTRU型MKFHE方案的构造

3.3.1 具体算法

用M−MKFHE(modified MKFHE)表示优化后的NTRU型多密钥全同态加密方案。给定安全参数λ, 参数$n=n(\lambda)$和素整数$p=p(\lambda)$, 素数次分圆多项式环

$R=\mathbb{Z}(x)/x^{n-1}+x^{n-2}+\cdots+1$和$R_q=R/qR$。$R$上的错误分布为$\chi$，其上界为$B=B(\lambda)$。定义一系列递减的模数$q_0>q_1>\cdots>q_L$，令$B\ll q_L$，$i\in\{0,1,\cdots,L\}$，$l_i=\lceil\log\ q_i\rceil$。M−MKFHE方案的具体描述如下：

1）M−MKFHE.KeyGen$(1^n,1^\lambda)$：选取$g^{(i)},f'^{(i)}\leftarrow\chi$，令$f^{(i)}=2f'^{(i)}+1$，使得$f^{(i)}\equiv 1 \mod 2$，且$f^{(i)}$在$R_{q_i}$上可逆，若不可逆则重新选取$f'^{(i)}\leftarrow\chi$。令$h^{(i)}=2g^{(i)}/f^{(i)}\in R_{q_i}$，则$pk=h_0\in R_{q_0}$，$sk=f_0\in R_{q_0}$；输出$(pk,sk)=(h,f)$。

2）M−MKFHE.Enc(pk,m_0)：选取向量$\tilde{\boldsymbol{s}},\tilde{\boldsymbol{e}}\leftarrow\chi^{l_0}$，用公钥$pk$加密明文向量$\overline{\boldsymbol{m}}=(m_0,2^{d+1}m_0,\cdots,2^{l_0-1}m_0)$。输出密文向量$\tilde{\boldsymbol{c}}:=h_0\tilde{\boldsymbol{s}}+2\tilde{\boldsymbol{e}}+\overline{\boldsymbol{m}}\in R_{q_0}^{l_0}$。

3）M−MKFHE.Dec$(sk_1,sk_2,\cdots,sk_N,\tilde{\boldsymbol{c}}^{(i)})$：选取密文向量$\tilde{\boldsymbol{c}}^{(i)}\in R_{q_i}^{l_i}$的第1项$\tilde{c}_1^{(i)}\in R_{q_i}$，令$u:=(sk_1sk_2\cdots sk_N)\cdot\tilde{c}_1^{(i)}\in R_{q_i}$。输出$m':=u \mod 2$。

4）M−MKFHE.Eval.Add$(\tilde{\boldsymbol{c}}_1^{(i)},\tilde{\boldsymbol{c}}_2^{(i)})$：给定两个密文向量$\tilde{\boldsymbol{c}}_1^{(i)},\tilde{\boldsymbol{c}}_2^{(i)}\in R_{q_i}^{l_i}$，对应的公钥集合分别为$K_1$、$K_2$，令$K=K_1\cup K_2=\{pk_1,pk_2,\cdots,pk_r\}(N\le r\le 2N)$，计算$\tilde{\boldsymbol{c}}_{\text{add}}^{(i)}=[\tilde{\boldsymbol{c}}_1^{(i)}+\tilde{\boldsymbol{c}}_2^{(i)}]_{q_i}\in R_{q_i}^{l_i}$，计算$\tilde{\tilde{\boldsymbol{c}}}_{\text{add}}^{(i+1)}=(q_{i+1}/q_i)\cdot\tilde{\boldsymbol{c}}_{\text{add}}^{(i)}(\mod 2)\in R_{q_{i+1}}^{l_i}$，输出密文向量$\tilde{\boldsymbol{c}}_{\text{add}}^{(i+1)}=\text{DT}\left(l_i,l_{i+1},\tilde{\tilde{\boldsymbol{c}}}_{\text{add}}^{(i+1)}\right)\in R_{q_{i+1}}^{l_{i+1}}$。

5）M−MKFHE.Eval.Mult$(\tilde{\boldsymbol{c}}_1^{(i)},\tilde{\boldsymbol{c}}_2^{(i)})$：给定两个密文向量$\tilde{\boldsymbol{c}}_1^{(i)},\tilde{\boldsymbol{c}}_2^{(i)}\in R_{q_i}^{l_i}$，对应的公钥集合分别为$K_1$、$K_2$，令$K=K_1\cup K_2=\{pk_1,pk_2,\cdots,pk_r\}(N\le r\le 2N)$，计算$\tilde{\boldsymbol{c}}_{\text{mult}}^{(i)}=\text{BitD}(\tilde{\boldsymbol{c}}_1^{(i)})\cdot\tilde{\boldsymbol{c}}_2^{(i)}\in R_{q_i}^{l_i}$，计算$\tilde{\tilde{\boldsymbol{c}}}_{\text{mult}}^{(i+1)}=(q_{i+1}/q_i)\cdot\tilde{\boldsymbol{c}}_{\text{mult}}^{(i)}(\mod 2)\in R_{q_{i+1}}^{l_i}$，输出密文向量$\tilde{\boldsymbol{c}}_{\text{mult}}^{(i+1)}=\text{DT}\left(l_i,l_{i+1},\tilde{\tilde{\boldsymbol{c}}}_{\text{mult}}^{(i+1)}\right)\in R_{q_{i+1}}^{l_{i+1}}$。

3.3.2　同态性质

假设对任一第i层的同态加法和乘法运算进行解密，则联合解密私钥为多项式$F_K^{(i)}=F_K=f_1f_2\cdots f_r$。

1）解密同态加法运算

$$\tilde{\boldsymbol{c}}_{\text{add}}^{(i)}F_K^{(i)}=F_K\cdot\text{Pof2}(m_1+m_2)+\tilde{\boldsymbol{e}}_{\text{add}}\qquad(8)$$

式中，$\tilde{\boldsymbol{e}}_{\text{add}}$为同态加法运算产生的噪声向量。取第1项$\tilde{c}_{\text{add},1}^{(i)}F_K \mod q_i(\mod 2)=(m_1+m_2)$，即可正确解密。

2）解密同态乘法运算

$$\tilde{\boldsymbol{c}}_{\text{mult}}^{(i)}F_K^{(i)}=F_K\cdot\text{Pof2}(m_1\cdot m_2)+\tilde{\boldsymbol{e}}_{\text{mult}}\qquad(9)$$

式中，$\tilde{\boldsymbol{e}}_{\text{mult}}$为同态加法运算产生的噪声向量。取第1项$\tilde{c}_{\text{mult},1}^{(i)}F_K \mod q_i(\mod 2)=m_1m_2$，即可正确解密。

由式(8)和(9)可以看出，同态运算过程不再需要繁琐耗时的密钥交换操作，大大降低了同态运算的复杂性。

4　方案分析

由于M−MKFHE是基于素数次的分圆多项式环构造的，初始的参数(λ,q,n,χ)的选取与现有的方案不同，不能直接与现有的方案（如LTV12、CO17）对比分析。B−MKFHE是现有方案（如LTV12、CO17）在素数次分圆多项式环上的方案模型，将M−MKFHE与B−MKFHE进行对比分析的结果，即是在统一参数选取的条件下，将M−MKFHE的优越性与现有方案对比分析的结果。

4.1　安全性分析

M−MKFHE方案是在B−MKFHE的基础上进行的优化，同样可以抵御更多的子域攻击，安全性是基于$\text{RLWE}_{\phi,q,\chi}$和$\text{DSPR}_{\phi,q,\chi}$问题。由于同态运算的结构改变了，需要证明M−MKFHE方案是否满足IND−CPA安全。

定义4[25]　同态加密方案中，对于任意多项式时间敌手A，存在一个可忽略的函数$negl(\lambda)$，使得

$$Adv_{\text{CPA}}[A]=|\Pr[A(pk,evk,\text{HE.Enc}_{pk}(m_0)=1]-\Pr[A(pk,evk,\text{HE.Enc}_{pk}(m_1)=1]|=negl(\lambda)$$

成立，则称该同态加密方案是IND−CPA安全的，其中，$m_b(b\in\{0,1\})$是明文，$(pk,evk,sk)\leftarrow\text{HE.KeyGen}(1^\lambda)$。

定　理　选择参数(λ,n,χ,q)使得在$\text{DSPR}_{\phi,q,\chi}$和$\text{RLWE}_{\phi,q,\chi}$问题的困难性假设成立，则M−MKFHE方案是IND−CPA安全的。

证明：假设敌手A在下面的IND−CPA游戏中可以获得系统参数和对加密预言机的询问，在此条件下，攻击者想要以一个不可忽略的优势识别出m_b，分为以下游戏阶段：

Game0：标准的IND−CPA游戏，挑战者C调用全同态加密体制M−MKFHE.KeyGen$(1^n,1^\lambda)$算法，将公钥$pk=h$给敌手A。挑战者输出密文向量$\boldsymbol{c}'=$M−MKFHE.Enc(pk,m_b)，敌手A尝试区分密文向量$\boldsymbol{c}'$所对应的明文向量Powerof2(m_b)。令密文向量$\boldsymbol{c}'=(c_1',c_2',\cdots,c'_{\lceil\log\ q\rceil})$，则$c'_\xi=hs_\xi+2e_\xi+m_{b,\xi}\in R_q(\xi\in[\lceil\log\ q\rceil])$，所以，对于密文向量中每个密文元素，敌手$A$具有相同的优势以区分对应的明文：

$$Adv_{\text{IND−CPA}}[A]=|\Pr[A(pk,\text{M−MKFHE.Enc}_{pk}(m_{0,\xi})=1]-\Pr[A(pk,\text{M−MKFHE.Enc}_{pk}(m_{1,\xi})=1]|。$$

Game1：与Game0的区别在于$pk=h$直接从R_q中随机选取，而不通过$f'\leftarrow\chi$计算得到。根据$\text{DSPR}_{\phi,q,\chi}$假设，离散高斯分布输出的样本与$R_q$上的均匀分布是概率不可区分的，所以$Adv_{\text{Game1}}[A]=Adv_{\text{IND−CPA}}[A]$。

Game2：区别于Game1，密文不经过M−MKFHE算法进行加密，而直接从$R_q^{\lceil\log\ q\rceil}$中随机均匀选取。与Game1相比，敌手$A$的优势在于解决$\text{RLWE}_{\phi,q,\chi}$问题，所以$|Adv_{\text{Game2}}[A]-Adv_{\text{Game1}}[A]|=Adv_{\text{RLWE}_{\phi,q,\chi}}[A]$。

又因为在Game2中，挑战者给出的公钥pk和挑战密文向量$\boldsymbol{c}'$都是随机的，与明文m_b没有关系。因此，敌手A在Game2中的优势为0，即$Adv_{\text{Game2}}[A]=0$。进一步可得$Adv_{\text{IND−CPA}}[A]=Adv_{\text{RLWE}_{\phi,q,\chi}}[A]$，其中解决$\text{RLWE}_{\phi,q,\chi}$问

题的优势可忽略。

综上所述，在$\mathrm{DSPR}_{\phi,q,\chi}$和$\mathrm{RLWE}_{\phi,q,\chi}$问题的困难性假设条件下满足：

$$Adv_{\mathrm{IND-CPA}}[A]=|\Pr[A(pk,\mathrm{M-MKFHE.Enc}_{pk}(m_{0,\xi})=1]-\Pr[A(pk,\mathrm{M-MKFHE.Enc}_{pk}(m_{1,\xi})=1]|=negl(\lambda)。$$

所以M−MKFHE方案是IND−CPA安全的。 证毕。

4.2 效率分析

4.2.1 存储开销

以在第i层完成一次同态运算为例，对比分析M−MKFHE与B−MKFHE在密文和密钥方面的存储开销。相比于B−MKFHE，M−MKFHE的公钥和私钥生成方式相同，所以公钥和私钥的尺寸没有改变。然而，M−MKFHE的密文扩展成了$\lceil\log q_i\rceil$维的多项式向量，其密文尺寸为$2(n-1)\lceil\log q_i\rceil\log q_i$ bit；另外，M−MKFHE在同态运算过程中，不需要生成计算密钥，所以层级之间的计算密钥尺寸为0 bit。

4.2.2 计算开销

通过计算实验消耗时间，分析同态运算的计算开销。忽略多项式系数（$[-q/2,q/2)$内的实数）乘法耗时的差异性，定义素数次分圆多项式环上两个多项式完成一次乘法计算用时为Δt s，BitDecomp(·)函数进行一次多项式分解用时为Δt_1 s，完成$\lceil\log q_i\rceil$个多项式求和计算用时为Δt_2 s。以密文在第i层完成一次同态乘法运算为例，在不做任何模q_i和模2处理的情况下，B−MKFHE完成一次同态乘法运算开销为：

$$T_{\mathrm{B}}\approx r(\lceil\log q_i\rceil\Delta t+\Delta t_1+\Delta t_2)+2N\Delta t\approx(r\lceil\log q_i\rceil+2N)\Delta t+r\Delta t_1+r\Delta t_2 \tag{10}$$

而M−MKFHE完成一次同态乘法运算开销为：

$$T_{\mathrm{M}}\approx(\lceil\log q_i\rceil+r)\Delta t+\lceil\log q_i\rceil\Delta t_1+\Delta t_2 \tag{11}$$

所以在参数q_i、n、N正常选取情况下，显然$T_{\mathrm{B}}>T_{\mathrm{M}}$。

M−MKFHE与B−MKFHE的存储开销和计算开销对比，如表1所示。

表 1 B−MKFHE和M−MKFHE的存储开销和计算开销对比

Tab. 1 Comparison of memory (bit-size) and evaluating costs between B−MKFHE and M−MKFHE

类型	密文尺寸/bit	计算密钥尺寸/bit	运算开销/s
B−MKFHE	$2(n-1)\log q_i$	$r(n-1)\lceil\log q_i\rceil\log q_i$	$(r\lceil\log q_i\rceil+2N)\Delta t+r\Delta t_1+r\Delta t_2$
M−MKFHE	$2(n-1)\lceil\log q_i\rceil\log q_i$	0	$(\lceil\log q_i\rceil+r)\Delta t+\lceil\log q_i\rceil\Delta t_1+\Delta t_2$

由表1可知，相对于B−MKFHE，虽然M−MKFHE的密文尺寸增大了$\lceil\log q_i\rceil$倍，但不需要生成计算密钥，所以M−MKFHE的总存储开销降低了。另外，M−MKFHE消除了复杂的密钥交换操作，使得计算开销比B−MKFHE降低了约r倍，所以M−MKFHE同态运算效率更高。

4.3 同态运算电路深度

根据第2.2.3节分析可知，M−MKFHE在第i层完成一次同态乘法解密产生的噪声为：

$$\|\tilde{\boldsymbol{c}}_{\mathrm{mult}}^{(i)}\boldsymbol{F}_K^{(i)}\|_\infty\le E_r+(n-1)(3E_{r+2}+6N(n-1)l_iE_{r+1}) \tag{12}$$

假设参与用户数量不变，M−MKFHE在第i层完成两次同态乘法运算之后再进行解密，可得产生的噪声值：

$$\|\tilde{\boldsymbol{c}}_{\mathrm{mult}}^{(i),2}\boldsymbol{F}_K^{(i)}\|_\infty\le E_r+(1+2(n-1)l_i)^2((3/2)E_{2r-N+2}+3N(n-1)E_{2r-N+1}) \tag{13}$$

式中，$\tilde{\boldsymbol{c}}_{\mathrm{mult}}^{(i),2}$为完成两次同态乘法运算之后的密文向量乘积。即$\|\tilde{\boldsymbol{c}}_{\mathrm{mult}}^{(i),2}\boldsymbol{F}_K^{(i)}\|_\infty=O\left((nB)^{3N}\right)$，该值仍小于式(4)所产生的噪声值。所以，在选取相同的参数条件下，B−MKFHE在第i层完成一次同态乘法运算，M−MKFHE则至少能完成两次同态乘法运算。也就是说，在产生噪声相近情况下，B−MKFHE完成L层电路深度的同态运算，M−MKFHE至少能完成$2L$层电路深度的同态运算，同态运算电路深度更大。

5 结 论

为了提高现有的NTRU型MKFHE方案抵御子域攻击能力和同态运算效率，作者优化设计了一种基于素数次分圆多项式环上的高效的NTRU型MKFHE方案（M−MKFHE方案）。该方案的安全性得到提升，支持更深电路层级的同态运算，且效率较高，具有较好的实用性。优化后的方案虽然不需要生成计算密钥，但增加了密文的维度，使得用户生成密文的复杂性较大。如何进一步降低存储开销，构造性能更加优越的NTRU型多密钥同态运算结构，是下一步继续研究的方向。

参考文献：

[1] Hamlin A,Shelat A,Weiss M,et al.Multi-key searchable encryption,revisited[M]//Public-Key Cryptography — PKC 2018.Cham:Springer,2018:95–124.

[2] Ben−Or M,Wigderson A.Completeness theorems for non-cryptographic fault-tolerant distributed computation[C]// Proceedings of the Twentieth Annual ACM Symposium on Theory of computing (STOC'88).New York:ACM,1988: 1–10.

[3] Huang Haiping,Gong Tianhe,Chen Ping,et al.Secure two-party distance computation protocol based on privacy homomorphism and scalar product in wireless sensor networks[J].Tsinghua Science and Technology,2016,21(4):

385–396.

[4] Yang Xiaoyuan,Tu Guangsheng,Kong Yongjun,et al.Multi-identity fully homomorphic encryption scheme supporting threshold decryption[J].Journal of Sichuan University (Engineering Science Edition),2019,51(4):133–139.[杨晓元,涂广升,孔咏骏,等.支持门限解密的多身份全同态加密方案[J].工程科学与技术,2019,51(4):133–139.]

[5] López−Alt A,Tromer E,Vaikuntanathan V.On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption[C]//Proceedings of the 44th symposium on Theory of Computing (STOC'12).New York:ACM,2012:1219–1234.

[6] Clear M,McGoldrick C.Multi-identity and multi-key leveled FHE from learning with errors[M]//Advances in Cryptology—CRYPTO 2015.Berlin:Springer,2015:630–656.

[7] Mukherjee P,Wichs D.Two round multiparty computation via multi-key FHE[M]//Advances in Cryptology—EUROCRYPT 2016.Berlin:Springer,2016:735–763.

[8] Peikert C,Shiehian S.Multi-key fhe from lwe,revisited[M]//Theory of Cryptography—TCC 2016.Berlin:Springer,2016:217–238.

[9] Brakerski Z,Perlman R.Lattice-based fully dynamic multi-key FHE with short ciphertexts[M]//Advances in Cryptology—CRYPTO 2016.Berlin:Springer,2016:190–213.

[10] Chen Long,Zhang Zhenfeng,Wang Xueqing.Batched multi-hop multi-key FHE from ring-LWE with compact ciphertext extension[M]//Theory of Cryptography—TCC 2017.Cham:Springer,2017:597–627.

[11] Li Ningbo,Zhou Tanping,Yang Xiaoyuan,et al.Efficient multi-key FHE with short extended ciphertexts and directed decryption protocol[J].IEEE Access,2019,7:56724–56732.

[12] Chen Hao,Dai Wei,Kim M,et al.Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security.New York:ACM,2019:395–412.

[13] Chen Hao,Chillotti I,Song Y.Multi-key homomorphic encryption from TFHE[M]//Advances in Cryptology – ASIACRYPT 2019.Cham:Springer,2019:446–472.

[14] Lyubashevsky V,Peikert C,Regev O.On ideal lattices and learning with errors over rings[M]//Advances in Cryptology—EUROCRYPT 2010.Berlin:Springer,2010:1–23.

[15] Brakerski Z,Vaikuntanathan V.Efficient fully homomorphic encryption from (standard) LWE[C]//Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science.Palm Springs:IEEE,2011:97–106.

[16] Albrecht M,Bai Shi,Ducas L.A subfield lattice attack on overstretched NTRU assumptions[M]//Advances in Cryptology—CRYPTO 2016.Berlin:Springer,2016:153–178.

[17] Yu Yang,Xu Guangwu,Wang Xiaoyun.Provably secure NTRU instances over prime cyclotomic rings[M]// Public-Key Cryptography—PKC 2017.Berlin:Springer,2017:409–434.

[18] Doröz Y,Hu Yin,Sunar B.Homomorphic AES evaluation using the modified LTV scheme[J].Designs,Codes and Cryptography,2016,80(2):333–358.

[19] Brakerski Z,Gentry C,Vaikuntanathan V.(Leveled) fully homomorphic encryption without bootstrapping[C]//Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ITCS'12).New York:ACM,2012:309–325.

[20] Bos J W,Lauter K,Loftus J,et al.Improved security for a ring-based fully homomorphic encryption scheme[M]//Cryptography and Coding—IMACC 2013.Berlin:Springer,2013:45–64.

[21] StehléD,Steinfeld R.Making NTRU as secure as worst-case problems over ideal lattices[M]//Advances in Cryptology—EUROCRYPT 2011.Berlin:Springer,2011:27–47.

[22] Chen Zhigang.Research and design of fully homomorphic encryption based on lattice[D].Nanjing:Nanjing University of Aeronautics and Astronautics,2015.[陈智罡.基于格的全同态加密研究与设计[D].南京:南京航空航天大学,2015.]

[23] Chongchitmate W,Ostrovsky R.Circuit-private multi-key FHE[M]//Public-Key Cryptography—PKC 2017.Berlin:Springer,2017:241–270.

[24] Gentry C,Sahai A,Waters B.Homomorphic encryption from learning with errors:Conceptually-simpler,asymptotically-faster,attribute-based[M]//Advances in Cryptology—CRYPTO 2013.Berlin:Springer,2013:75–92.

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

（编辑　赵　婧）

引用格式: Che Xiaoliang,Zhou Tanping,Li Ningbo,et al.Optimization of NTRU-type multi-key fully homomorphic encryption scheme[J].Advanced Engineering Sciences,2020,52(5):186–193.[车小亮,周潭平,李宁波,等.NTRU型多密钥全同态加密方案的优化[J].工程科学与技术,2020,52(5):186–193.]