Journal of Computer Applications
计算机应用,2021,41(6):1723－1728
ISSN 1001-9081
CODEN JYIIDU
2021-06-10
http://www.joca.cn

文章编号:1001-9081(2021)06-1723-06
DOI:10.11772/j.issn.1001-9081.2020091447

优化的基于错误学习问题的CKKS方案

郑尚文[1],刘　尧[1],周潭平[1,2*],杨晓元[1,3]
(1.武警工程大学 密码工程学院,西安 710086;　2.中国科学院 软件研究所,北京 100090;
3.网络和信息安全武警部队重点实验室(武警工程大学),西安 710086)
(*通信作者电子邮箱850301775@qq.com)

摘　要:针对基于错误学习(LWE)问题的CKKS同态加密方案在密态数据计算中存在的密文大、计算密钥生成复杂以及同态计算效率低的缺陷,运用比特丢弃和同态计算密钥重组的方法,提出了一种优化的LWE型CKKS方案。首先,丢弃密文向量的部分低位比特和同态乘法计算中密文张量积的部分低位比特,从而减小了同态乘法过程中的密文规模;其次,针对比特丢弃对同态计算密钥进行重组和优化,从而去除密钥交换过程中powersof2含有的无关扩展项并降低计算密钥的规模和同态乘法过程中的噪声增长规模。在保证原有方案安全性的基础上,所提优化方案使得计算密钥的维度减少,使得同态乘法的计算复杂性降低。分析结果表明,所提出的优化方案在一定程度上降低了同态计算及计算密钥生成过程的计算复杂性,从而降低了存储开销并提升了同态乘法运算的效率。

关键词:同态加密;错误学习问题;低位比特丢弃;计算密钥;计算复杂性
中图分类号:TP309　　**文献标志码:**A

Optimized CKKS scheme based on learning with errors problem

ZHENG Shangwen[1], LIU Yao[1], ZHOU Tanping[1,2*], YANG Xiaoyuan[1,3]
(1. *College of Cryptographic Engineering, Engineering University of PAP, Xi'an Shaanxi* 710086, *China*;
2. *Institute of Software, Chinese Academy of Sciences, Beijing* 100090, *China*;
3. *Key Laboratory of Network and Information Security of PAP (Engineering University of PAP), Xi'an Shaanxi* 710086, *China*)

Abstract: Focused on the issue that the CKKS (Cheon-Kim-Kim-Song) homomorphic encryption scheme based on the Learning With Errors (LWE) problem has large ciphertext, complicated calculation key generation and low homomorphic calculation efficiency in the encrypted data calculation, an optimized scheme of LWE type CKKS was proposed through the method of bit discarding and homomorphic calculation key reorganization. Firstly, the size of the ciphertext in the homomorphic multiplication process was reduced by discarding part of the low-order bits of the ciphertext vector and part of the low-order bits of the ciphertext tensor product in the homomorphic multiplication. Secondly, the method of bit discarding was used to reorganize and optimize the homomorphic calculation key, so as to remove the irrelevant extension items in powersof2 during the key exchange procedure and reduce the scale of the calculation key as well as the noise increase in the process of homomorphic multiplication. On the basis of ensuring the security of the original scheme, the proposed optimized scheme makes the dimension of the calculation key reduced, and the computational complexity of the homomorphic multiplication reduced. The analysis results show that the proposed optimized scheme reduces the computational complexity of the homomorphic calculation and calculation key generation process to a certain extent, so as to reduce the storage overhead and improve the efficiency of the homomorphic multiplication operation.

Key words: homomorphic encryption; Learning With Errors (LWE) problem; low-order bits discarding; calculation key; computational complexity

0　引言

全同态加密(Fully Homomorphic Encryption, FHE)允许在不解密的状态下对密文进行任意运算,且解密后结果与其对应明文进行同样运算的结果相等。这一优良特性与云计算条件下对数据隐私保护的需求十分契合,具有广阔的应用前景。2009年Gentry[1]首先构造了第一个基于理想格的全同态加密方案Gen09,并且描绘了实现纯全同态加密的"蓝图"——同

收稿日期:2020-09-17;**修回日期:**2020-11-30;**录用日期:**2020-12-03。
基金项目:国家重点研发计划项目(2017YFB0802000);国家自然科学基金资助项目(U1636114,61872384);陕西省自然科学基金资助项目(2020JQ-492);武警工程大学科研创新团队项目(KYTD201805);武警工程大学基础基金资助项目(WJY201910,WJY201914,WJY201912)。
作者简介:郑尚文(1998—),男,湖南宁乡人,硕士研究生,主要研究方向:同态密码、信息安全;　刘尧(1993—),男,山东聊城人,硕士研究生,主要研究方向:同态密码、信息安全;　周潭平(1989—),男,江西鹰潭人,讲师,博士,主要研究方向:同态密码、信息安全;　杨晓元(1959—),湖南湘潭人,教授,博士生导师,硕士,主要研究方向:密码学、信息安全。

态运行解密电路。之后，一系列（全）同态加密方案[2-7]相继被提出，同态加密成为信息安全研究领域的热点，得到迅速发展。目前，同态加密在基因组分析[8]、医疗[9]、金融[10]和安全多方计算（Secure Multi-Party Computation，MPC）等领域[11-12]发挥了重要作用。

CKKS17（Cheon-Kim-Kim-Song 2017）同态加密方案由Cheon等[7]在ASIACRYPT17（2017 International Conference on the Theory and Application of Cryptology and Information Security）会议上提出，支持对浮点数进行近似计算，效率较高，是目前最重要、最具前景的同态加密算法之一。与以往同态加密方案明文空间和噪声空间分隔开的设计不同，CKKS17的明文空间没有取模过程，因此也不能在解密后通过相应的模运算来得到准确的解密结果：它将噪声视为明文的一部分，而噪声一方面来源于加密方案中为保证安全性而引入的错误，另一方面也来源于近似计算中的舍入误差，密文解密后不能将明文中的噪声去除，只能以预定的精度输出明文的近似值。在同态运算过程中，计算结果的高有效位（Most Significant Bits，MSBs）能够保留，而不精确的低位比特（Least Significant Bits，LSBs）则在RS（ReScaling）过程中被舍去，以此管理结果密文对应的明文尺寸，这也使得方案所需最大密文模数随乘法深度由指数增长降为线性增长。CKKS17方案提出之后，研究人员在此基础上做了进一步的研究。2018年，Cheon等[13]提出了CKKS17的Bootstrapping技术，将其由层级同态加密推广至完全同态加密，并提出了支持余数系统（Residue Number System，RNS）分解的CKKS17方案的变体[14]；后续，Chen等[15]对Bootstrapping过程进行了优化，使自举的时间降低两个数量级；2019年，Chen等[16]提出了CKKS17的多密钥版本CDKS19（Chen-Dai-Kim-Song 2019），并对该方案应用于神经网络模型的效率进行了测试。

虽然同态加密为云计算中的数据隐私保护提供了一个良好的解决方案，但由于同态加密方案需要对庞大的密态数据进行同态运算，因此在存储和传输加密数据时，无疑会给用户造成较大的通信开销负担。同时，错误学习（Learning With Errors，LWE）型CKKS方案的重线性化过程[17]所需的计算密钥规模庞大，计算复杂，也影响了方案的实际运用。低位比特丢弃（low-order Bits Discarding algorithm，BD）的思想最早出现于格密码中，Zhou等[18]将其应用于同态加密以提高效率。在此基础上，本文结合LWE型CKKS方案的密文结构，通过舍去密文中的部分低位比特来减少存储的比特数，从而降低了重线性化过程中计算密钥的大小和计算开销，提高了方案的存储和计算效率。

1 相关知识和关键技术

本文中向量默认为列向量；定义$\langle\cdot,\cdot\rangle$为两向量的内积；对于实数$x$，$\lceil x \rfloor$表示距离$x$最近的整数，距离相等时优先向上取整；对于整数$q$，$\mathbf{Z}_q$表示在$\left(-\frac{q}{2},\frac{q}{2}\right]$范围内的整数集；$[z]_q$表示对整数$z$模$q$后结果属于集合$\mathbf{Z}_q$内的值；$x \leftarrow D$表示从分布$D$中抽样产生$x$值，特别地，当$D$为有限集时，$a \leftarrow D$表示从分布$D$中均匀地选取产生$x$值；$\lambda$表示安全参数。

1.1 相关定义

定义1 误差学习问题[19]。

设λ为安全参数，令$n = n(\lambda)$是一个整数维数，$q = q(\lambda) \geqslant 2$为一个整数，$\chi = \chi(\lambda)$是整数上的一个分布。判定型$LWE_{n,q,\chi}$定义为区分下面两个分布：1）第一个分布，均匀地从$\mathbf{Z}_q^{n+1}$中选取产生$(\boldsymbol{a}_i, b_i)$；第二个分布，均匀选取$\boldsymbol{s} \leftarrow \mathbf{Z}_q^n$和$\boldsymbol{a}_i \leftarrow \mathbf{Z}_q^n$，计算$b_i = \langle \boldsymbol{a}_i, \boldsymbol{s}\rangle + e_i$，组成$(\boldsymbol{a}_i, b_i) \in \mathbf{Z}_q^{n+1}$。

定义2 B-bound分布[17]。

对于一个整数分布集合$\{\chi_n\}_{n\in\mathbf{N}}$，如果下列等式成立

$$\Pr_{e \leftarrow \chi_n}\left[|e| > B\right] = negl(n)$$

则称整数分布集合$\{\chi_n\}_{n\in\mathbf{N}}$是B-bound分布。

1.2 关键技术

方案运用了*BitDecomp*(*)、*Powersof*2(*)[4]及张量积等方法，具体操作为：

1）$BitDecomp(\boldsymbol{x} \in \mathbf{R}_q^n, q)$：对于输入向量$\boldsymbol{x} \in \mathbf{R}_q^n$，*BitDecomp*将其表示为$\boldsymbol{x} = \sum_{j=0}^{\lfloor \mathrm{lb}\, q\rfloor} 2^j$，其输出为$\left(u_0, u_1, \cdots, u_{\lfloor \mathrm{lb}\, q\rfloor}\right) \in \mathbf{R}_2^{n\lceil \mathrm{lb}\, q\rceil}$，其中$u_j \in \mathbf{R}$。显然，$\boldsymbol{x} = \sum_{j=0}^{\lfloor \mathrm{lb}\, q\rfloor} 2^j u_j$。

2）$Powersof2(\boldsymbol{x} \in \mathbf{R}_q^n, q)$：对于某个输入向量$\boldsymbol{x} \in \mathbf{R}_q^n$，*Powersof*2是*BitDecomp*的逆过程，其输出为$(\boldsymbol{x}, 2\cdot\boldsymbol{x}, \cdots, 2^{\lfloor \mathrm{lb}\, q\rfloor}\cdot\boldsymbol{x}) \in \mathbf{R}_q^{n\lceil \mathrm{lb}\, q\rceil}$。由上述定义，对于给定两个维数相同的向量$\boldsymbol{a}$、$\boldsymbol{b}$，不难验证下面等式：

$$\left\langle BitDecomp(\boldsymbol{a}, q), Powersof2(\boldsymbol{b}, q)\right\rangle = \langle \boldsymbol{a}, \boldsymbol{b}\rangle \bmod q$$

3）设$\boldsymbol{u}$、$\boldsymbol{v}$分别为n、m维向量，则向量$\boldsymbol{u}$、$\boldsymbol{v}$的张量积定义为$\boldsymbol{u} \otimes \boldsymbol{v} = (u_1v_1, u_1v_2, \cdots, u_1v_m, \cdots, u_nv_1, \cdots, u_nv_m)$。根据张量积和内积的定义，可以证明如下等式：

$$\langle \boldsymbol{u} \otimes \boldsymbol{v}, \boldsymbol{u}' \otimes \boldsymbol{v}'\rangle = \langle \boldsymbol{u}, \boldsymbol{u}'\rangle \cdot \langle \boldsymbol{v}, \boldsymbol{v}'\rangle$$

2 低位方法的应用

2.1 CKKS17方案

CKKS17方案[7]主要包括六个基本算法（*KeyGen*，*Enc*，*Dec*，*Add*，*Mult*，*RS*），本文主要对基于LWE的CKKS加密方案进行优化，下面对该方案作以简要介绍。首先，该方案利用*Ecd*、*Dcd*及缩放因子Δ来实现消息与明文的相互映射。以消息为复数，明文以分圆多项式环$\bar{R} = \mathbf{Z}[X]/\left(\Phi_M(X)\right)$上的元素为例，*Dcd*首先将明文多项式$m(X)$除上因子$\Delta$，然后计算该明文多项式在分圆多项式$\Phi_M(X)$根处的函数值，并取整，得到最终的复数消息向量。而*Ecd*即为*Dcd*的逆变换，具体过程为：

$$C^{\Phi(M)/2} \xrightarrow{\pi^{-1}} H \xrightarrow{\lceil\cdot\rfloor_{\sigma(\bar{R})}} \sigma(\bar{R}) \xrightarrow{\sigma^{-1}} \bar{R}$$

其中：映射π^{-1}表示将复数映射到本身与其共轭复数的集合；σ^{-1}则利用离散傅里叶变换来实现复数向量向分圆多项式环上元素的变换。

在密钥初始化阶段，基于LWE问题生成公私钥对$(\boldsymbol{pk}, \boldsymbol{sk})$以及计算密钥$\boldsymbol{evk}$，用于对明文加解密以及乘法中的重线性

化。与其他基于LWE加密方案不同的是,CKKS17方案中引入了一个新的概念:rescaling,它应用在乘法密文重线性化步骤后,通过将被加密的明文除上一个整数,并利用浮点数和科学计数法在近似计算中的“四舍五入”来去除明文中一些不精确的低位比特,从而使得在同态计算期间,编码前后的消息的大小保持基本不变,同时也保证了方案所需的最大密文模数随运算电路深度呈线性增长,极大提高了方案的效率,促进了方案的实用化发展。根据基于RLWE(Ring LWE)的CKKS方案编写了开源的同态加密库HEEAN。

2.2　低位比特丢弃方法的构造

在同态加密方案[20]的实际使用中,为了提高方案效率,一般使用中国剩余定理(Chinese Remainder Theorem, CRT)将大密文分割成小块密文(模数较小的密文)进行操作,但进行重线性化步骤时仍需要将其转化为一般的表示形式。重线性化过程所使用的计算密钥的尺寸很大,这是影响方案效率的重要因素。针对这一过程,本文提出了一种低位比特丢弃方法,通过有选择地舍弃密文中的部分低位比特从而相应地减小重线性化密钥的尺寸来提高方案效率。下面对本文方法的主要思想进行介绍。

计算机中数的存储通常采用二进制存储,不同比特所处的位置不同所代表的权重也不相同,因此,可以通过舍弃存储密文每一个分量的部分低位比特来减少存储空间,密文整体比特数的降低也能够提升密文通信的效率。由于密钥采样的分布通常是一些“小分布”(采样值的绝对值相对较小),因此丢弃低位比特对噪声的贡献并不会很大。同时在方案的重线性化过程中,丢弃低位比特能够减小计算密钥的大小,从而降低由于重线性化加密私钥所产生的噪声,其具体构造如下。

定义3　低位比特丢弃(BD)方法。

设密文 $\boldsymbol{c}\in\mathbf{Z}_{q_l}^{n}$,$\delta$为丢弃的低位比特位数,比特丢弃方法的主要做法是丢弃输入密文$\boldsymbol{c}$中n个分量各自的低位δ比特,得到$\boldsymbol{c}_{BD}=BD(\boldsymbol{c},\delta)\in\mathbf{Z}_{q_l}^{n}$,其中$\boldsymbol{c}_{BD}$中每一个分量根据丢弃比特向量$\boldsymbol{c}_\delta$最高位0、1取值的不同,有选择地加上进位。即当$\boldsymbol{c}_\delta$的首位比特为1时,向前进位;当$\boldsymbol{c}_\delta$的首位比特为0时,不进位,具体如图1所示。

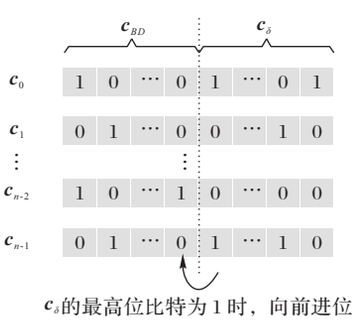

图1　低位比特丢弃方法

Fig. 1　Low-order bits discarding method

选择性地加上进位能够使得丢弃低位比特后的密文向量与原始密文向量的差值更小,更好地控制噪声的增长。单纯的比特丢弃技术并不会降低密文的噪声,但是在密文进行同态运算时丢弃低位比特能够减少相应噪声并提高计算效率,具体到方案同态运算中的应用如下。

2.2.1　低位比特丢弃在同态加法中的应用

同态加法操作由于不涉及进行复杂昂贵的重线性化操作,只需要对输入的两个密文丢弃相应的低位比特即可,如下所述:

设$\boldsymbol{c}_1,\boldsymbol{c}_2\in\mathbf{Z}_{q_l}^{N+1}$是两个加法密文输入,首先对两个密文进行低位比特丢弃,得到$\boldsymbol{c}_1'=BD(\boldsymbol{c}_1,\delta)$,$\boldsymbol{c}_2'=BD(\boldsymbol{c}_2,\delta)$。输出同态加法的结果密文$\boldsymbol{c}_{add}=\boldsymbol{c}_1'+\boldsymbol{c}_2'$。

2.2.2　低位比特丢弃在同态乘法中的应用

同态乘法中,假设$\boldsymbol{c}_1,\boldsymbol{c}_2\in\mathbf{Z}_{q_l}^{N+1}$是乘法的两个密文输入,$\boldsymbol{s}$为私钥去除首项元素1之后的向量。利用低位比特丢弃方法输出$\boldsymbol{c}_1'=BD(\boldsymbol{c}_1,\delta)$,$\boldsymbol{c}_2'=BD(\boldsymbol{c}_2,\delta)$,$\boldsymbol{c}=\boldsymbol{c}_1'\otimes\boldsymbol{c}_2'\in\mathbf{Z}_{q_l}^{(N+1)^2}$及$\boldsymbol{c}_{BD}=BD(\boldsymbol{c},\delta')\in\mathbf{Z}_{q_l}^{(N+1)^2}$。此时,生成计算密钥的各个参数为$\boldsymbol{A}'_{BD}\leftarrow\mathbf{Z}_{q_l}^{\left((N+1)^2\left(\lceil\mathrm{lb}\,q_l\rceil-\delta'\right)\right)\times N}$,$\boldsymbol{e}_{BD}\leftarrow\chi^{\left((N+1)^2\left(\lceil\mathrm{lb}\,q_l\rceil-\delta'\right)\right)}$,由此可得$\boldsymbol{b}'_{BD}=-\boldsymbol{A}'\boldsymbol{s}+\boldsymbol{s}''+\boldsymbol{e}_{BD}\in\mathbf{Z}_{q_l}^{(N+1)^2\left(\lceil\mathrm{lb}\,q_l\rceil-\delta'\right)}$,且可知此时$\boldsymbol{evk}_{BD}=(\boldsymbol{b}'_{BD},\boldsymbol{A}'_{BD})\in\mathbf{Z}_{q_l}^{\left((N+1)^2\left(\lceil\mathrm{lb}\,q_l\rceil-\delta'\right)\right)\times(N+1)}$,其中$\boldsymbol{s}'=\boldsymbol{sk}\otimes\boldsymbol{sk}$,$\boldsymbol{s}''=BD\left(Powersof2(\boldsymbol{s}'),\delta'\right)=BD\left(Powersof2\left(\boldsymbol{sk}\otimes\boldsymbol{sk}\right),\delta'\right)$。最后,输出同态乘法的结果密文$\boldsymbol{c}_{mult}=BitDecomp(\boldsymbol{c}_{BD})^{\mathrm{T}}\cdot\boldsymbol{evk}_{BD}\left(\mathrm{mod}\,q_l\right)$。

3　基于低位比特丢弃的LWE型CKKS方案

3.1　方案构造

选取合适的基$p>0$,模数q_0,令$q_l=p^l\cdot q_0,0<l\leqslant L$。$HWT(h)$[21]为有符号的、汉明重量为$h$的$N$维$\{-1,0,1\}^N$向量集合,$\lambda$为安全参数。在计算密钥的生成和同态运算中运用了低位比特丢弃方法进行优化,基于低位比特丢弃的LWE型CKKS方案主要包括以下六个算法:

1)密钥生成算法$KeyGen(1^\lambda)$。

①选取质数p和整数q_0、τ,设$q_l=p^lq_0,l=1,2,\cdots,L$,合理选取参数$N=N(\lambda,q_L)$和B-bound错误分布$\chi=\chi\left(\lambda,q_L\right)$作为$LWE_{N,q_L,\chi}$问题的参数。输出$params=(n,q_L,\chi,\tau)$。

②随机选取$\boldsymbol{s}=HWT(h)$,私钥$\boldsymbol{sk}\leftarrow(1,\boldsymbol{s})\in\mathbf{Z}_{q_L}^{N+1}$。随机均匀选取$\boldsymbol{A}\leftarrow\mathbf{Z}_{q_L}^{\tau\times N}$,$\boldsymbol{e}\leftarrow\chi^\tau$。令$\boldsymbol{b}=-\boldsymbol{A}\boldsymbol{s}+\boldsymbol{e}(\mathrm{mod}\,q_L)$,输出方案的公钥$\boldsymbol{pk}=(\boldsymbol{b},\boldsymbol{A})\in\mathbf{Z}_{q_L}^{\tau\times(N+1)}$。

③设$\boldsymbol{sk}'\leftarrow BD\left(Powersof2\left(\boldsymbol{sk}\otimes\boldsymbol{sk}\right),\delta'\right)$,随机均匀选取$\boldsymbol{A}'\leftarrow\mathbf{Z}_{q_l}^{\left((N+1)^2\left(\lceil\mathrm{lb}\,q_l\rceil-\delta'\right)\right)\times N}$与$\boldsymbol{e}'\leftarrow\chi^{\left((N+1)^2\left(\lceil\mathrm{lb}\,q_l\rceil-\delta'\right)\right)}$,令$\boldsymbol{b}'=-\boldsymbol{A}'\boldsymbol{s}+\boldsymbol{sk}'+\boldsymbol{e}'\in\mathbf{Z}_{q_l}^{(N+1)^2\left(\lceil\mathrm{lb}\,q_l\rceil-\delta'\right)}$,输出计算密钥$\boldsymbol{evk}\leftarrow(\boldsymbol{b}',\boldsymbol{A}')\in\mathbf{Z}_{q_l}^{\left((N+1)^2\left(\lceil\mathrm{lb}\,q_l\rceil-\delta'\right)\right)\times(N+1)}$。

2)加密算法$Enc(m,\boldsymbol{pk})$。

对于一个整数$m\in\mathbf{Z}$的明文,随机均匀选取一个向量$\boldsymbol{r}\leftarrow\{0,1\}^\tau$。输出其密文$\boldsymbol{c}\leftarrow(m,\boldsymbol{0})+\boldsymbol{pk}^{\mathrm{T}}\cdot\boldsymbol{r}\in\mathbf{Z}_{q_L}^{N+1}$。

3)解密算法:$Dec(\boldsymbol{c}, sk)$。

对于一个密文向量 $\boldsymbol{c}$ 与私钥 $\boldsymbol{sk}$,解密算法为 $m' = \langle \boldsymbol{c}, \boldsymbol{sk} \rangle \pmod{q_l}$。

4)同态加法 $ADD(\boldsymbol{c}_1, \boldsymbol{c}_2)$。

输入两个密文 $\boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathbf{Z}_{q_l}^{N+1}$,计算 $\boldsymbol{c}_1' = BD(\boldsymbol{c}_1, \delta)$, $\boldsymbol{c}_2' = BD(\boldsymbol{c}_2, \delta)$,输出 $\boldsymbol{c}_{add} = \boldsymbol{c}_1' + \boldsymbol{c}_2' \pmod{q_l}$。

5)同态乘法 $Mult(\boldsymbol{c}_1, \boldsymbol{c}_2)$。

输入两个密文 $\boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathbf{Z}_{q_l}^{N+1}$,计算 $\boldsymbol{c}_1' = BD(\boldsymbol{c}_1, \delta)$, $\boldsymbol{c}_2' = BD(\boldsymbol{c}_2, \delta)$, $\boldsymbol{c} = \boldsymbol{c}_1' \otimes \boldsymbol{c}_2' \in \mathbf{Z}_{q_l}^{(N+1)^2}$ 及 $\boldsymbol{c}_{BD} = BD(\boldsymbol{c}, \delta') \in \mathbf{Z}_{q_l}^{(N+1)^2}$,最终输出 $\boldsymbol{c}_{mult} = BitDecomp(\boldsymbol{c}_{BD})^{\mathrm{T}} \cdot \boldsymbol{evk} \pmod{q_l}$。

6)重缩放 $RS_{l \to l'}(\boldsymbol{c})$。

对于输入密文 $\boldsymbol{c} \in \mathbf{Z}_{q_l}^{N+1}$,处于层 l,输出处于层 l' 的新密文 $\boldsymbol{c}' \leftarrow \left\lceil \frac{q_{l'}}{q_l} \boldsymbol{c} \right\rfloor \in \mathbf{Z}_{q_{l'}}^{N+1}$。

3.2 正确性

本文方案的加解密正确性与原始的CKKS17方案大致相同,在此不作阐述,主要论述在运用低位比特丢弃方法之后同态加法和同态乘法的正确性。设 $\boldsymbol{c}_1, \boldsymbol{c}_2$ 分别是对 $m_1, m_2 \in \mathbf{Z}$ 加密的密文,噪声分别为 e_1, e_2。

3.2.1 加法正确性

其同态加法输出 $\boldsymbol{c}_{add} = \boldsymbol{c}_1 + \boldsymbol{c}_2$,满足如下等式:

$$\begin{aligned}\langle \boldsymbol{c}_{add}, \boldsymbol{sk} \rangle &= \langle \boldsymbol{c}_1' + \boldsymbol{c}_2', \boldsymbol{sk} \rangle = \\ &\langle \boldsymbol{c}_1 + \boldsymbol{c}_2, \boldsymbol{sk} \rangle - \langle \boldsymbol{c}_{1\delta} + \boldsymbol{c}_{2\delta}, \boldsymbol{sk} \rangle = \\ &\langle \boldsymbol{c}_1, \boldsymbol{sk} \rangle + \langle \boldsymbol{c}_2, \boldsymbol{sk} \rangle - \langle \boldsymbol{c}_{1\delta} + \boldsymbol{c}_{2\delta}, \boldsymbol{sk} \rangle = \\ &m_1 + m_2 + \left[e_1 + e_2 - \langle \boldsymbol{c}_{1\delta} + \boldsymbol{c}_{2\delta}, \boldsymbol{sk} \rangle \right] \end{aligned} \tag{1}$$

令 $\boldsymbol{c}_{1\delta}$ 和 $\boldsymbol{c}_{2\delta}$ 分别代表相应密文向量丢弃低位 δ 比特后的差值,当

$$\left| m_1 + m_2 + \left(e_1 + e_2 - \langle \boldsymbol{c}_{1\delta} + \boldsymbol{c}_{2\delta}, \boldsymbol{sk} \rangle \right) \right| \leqslant \frac{q_l}{2}$$

$$\frac{\langle \boldsymbol{c}_{add}, \boldsymbol{sk} \rangle - (m_1 + m_2)}{\Delta} = \frac{e_1 + e_2 - \langle \boldsymbol{c}_{1\delta} + \boldsymbol{c}_{2\delta}, \boldsymbol{sk} \rangle}{\Delta} \leqslant \frac{1}{2}$$

Δ 为消息与明文之间转化的缩放量,方案正确性成立。

3.2.2 乘法正确性

其同态乘法输出 $\boldsymbol{c}_{mult} = \boldsymbol{c}_1 \times \boldsymbol{c}_2$,满足如下等式:

$$\begin{aligned}\langle \boldsymbol{c}_{mult}, \boldsymbol{sk} \rangle &= \left\langle BitDecomp(\boldsymbol{c}_{BD})^{\mathrm{T}} \cdot \boldsymbol{evk}_{BD}, \boldsymbol{sk} \right\rangle = \\ &BitDecomp(\boldsymbol{c}_{BD})^{\mathrm{T}} \cdot \boldsymbol{evk}_{BD} \cdot \boldsymbol{sk} = \\ &\left(BD(Powersof2(\boldsymbol{sk} \otimes \boldsymbol{sk})) + \boldsymbol{e}_{BD} \right) \cdot \\ &BitDecomp(\boldsymbol{c}_{BD})^{\mathrm{T}} = \left\langle BitDecomp(\boldsymbol{c}_{BD}), \right. \\ &\left. BD(Powersof2(\boldsymbol{sk} \otimes \boldsymbol{sk})) \right\rangle + \\ &\langle BitDecomp(\boldsymbol{c}_{BD}), \boldsymbol{e}_{BD} \rangle \end{aligned} \tag{2}$$

令 $\left\langle \left[BitDecomp(\boldsymbol{c}_1' \otimes \boldsymbol{c}_2') \right]_{\delta'}, (Powersof2(\boldsymbol{sk} \otimes \boldsymbol{sk})) \right\rangle = e_{\delta'}$,故:

$$\begin{aligned}\langle \boldsymbol{c}_{mult}, \boldsymbol{sk} \rangle &= \left\langle BitDecomp(\boldsymbol{c}_1' \otimes \boldsymbol{c}_2'), \right. \\ &\left. (Powersof2(\boldsymbol{sk} \otimes \boldsymbol{sk})) \right\rangle - e_{\delta'} + \\ &\langle BitDecomp(\boldsymbol{c}_{BD}), \boldsymbol{e}_{BD} \rangle = \\ &\langle \boldsymbol{c}_1 - \boldsymbol{c}_{1\delta}, \boldsymbol{sk} \rangle \cdot \langle \boldsymbol{c}_2 - \boldsymbol{c}_{2\delta}, \boldsymbol{sk} \rangle - e_{\delta'} + \\ &\langle BitDecomp(\boldsymbol{c}_{BD}), \boldsymbol{e}_{BD} \rangle = \\ &\left(\langle \boldsymbol{c}_1, \boldsymbol{sk} \rangle - \langle \boldsymbol{c}_{1\delta}, \boldsymbol{sk} \rangle \right) \cdot \left(\langle \boldsymbol{c}_2, \boldsymbol{sk} \rangle - \right. \\ &\left. \langle \boldsymbol{c}_{2\delta}, \boldsymbol{sk} \rangle \right) + \langle BitDecomp(\boldsymbol{c}_{BD}), \boldsymbol{e}_{BD} \rangle - e_{\delta'} = \\ &\left(m_1 + e_1 - \langle \boldsymbol{c}_{1\delta}, \boldsymbol{sk} \rangle \right) \cdot \left(m_2 + e_2 - \langle \boldsymbol{c}_{2\delta}, \boldsymbol{sk} \rangle \right) + \\ &\langle BitDecomp(\boldsymbol{c}_{BD}), \boldsymbol{e}_{BD} \rangle - e_{\delta'} = \\ &m_1 m_2 + e' + \langle BitDecomp(\boldsymbol{c}_{BD}), \boldsymbol{e}_{BD} \rangle - e_{\delta'} \end{aligned} \tag{3}$$

其中,$\left[BitDecomp(\boldsymbol{c}_1' \otimes \boldsymbol{c}_2') \right]_{\delta'}$、$\boldsymbol{c}_{i\delta}$ $(i = 1, 2)$ 分别代表 $\boldsymbol{c}_{BD}$、$\boldsymbol{c}_i$ 丢弃 δ' 位比特向量后与原来向量的差值,即:

$$\left[BitDecomp(\boldsymbol{c}_1' \otimes \boldsymbol{c}_2') \right]_{\delta'} = BitDecomp(\boldsymbol{c}_1' \otimes \boldsymbol{c}_2') - BitDecomp(\boldsymbol{c}_{BD})$$

$$\boldsymbol{c}_{i\delta} = \boldsymbol{c}_i - BD(\boldsymbol{c}_i, \delta)$$

$$e' = m_1 e_2 + m_2 e_1 + e_1 e_2 - \langle \boldsymbol{c}_{2\delta}, \boldsymbol{sk} \rangle (m_1 + e_1) - \langle \boldsymbol{c}_{1\delta}, \boldsymbol{sk} \rangle (m_2 + e_2) - \langle \boldsymbol{c}_{1\delta}, \boldsymbol{sk} \rangle \langle \boldsymbol{c}_{2\delta}, \boldsymbol{sk} \rangle$$

当 $m_1 m_2 + e' - e_{\delta'} + \langle \boldsymbol{e}_{BD}, BitDecomp(\boldsymbol{c}) \rangle \leqslant \frac{q_l}{2}$ 时,且存在 $\frac{\langle \boldsymbol{c}_{BD}, \boldsymbol{sk} \rangle - m_1 m_2}{\Delta} = \frac{e' - e_{\delta'} + \langle BitDecomp(\boldsymbol{c}_{BD}), \boldsymbol{e}_{BD} \rangle}{\Delta} \leqslant \frac{1}{2}$,方案实现正确解密。

4 方案分析

4.1 噪声分析

假设方案加密的明文上限为 ν,密文维数为 $N+1$,δ、δ' 为相应向量丢弃的比特位数。根据 $e_i = \boldsymbol{r}^{\mathrm{T}} \boldsymbol{e}_i (i = 1, 2)$, $\boldsymbol{e}_i \leftarrow \chi$, $\boldsymbol{s} = HWT(h)$, $\boldsymbol{sk} \leftarrow (1, \boldsymbol{s}) \in \mathbf{Z}_{q_L}^{N+1}$,下面对同态加法和同态乘法的噪声上界进行分析。

4.1.1 同态加法噪声

由式(1)可得加法噪声:

$$\begin{aligned}e_{add} &= \langle \boldsymbol{c}_{add}, \boldsymbol{sk} \rangle - (m_1 + m_2) = \\ &\left(e_1 + e_2 - \langle \boldsymbol{c}_{1\delta} + \boldsymbol{c}_{2\delta}, \boldsymbol{sk} \rangle \right) \leqslant \\ &2\tau B + (N+1) 2^{\delta - 1} \end{aligned} \tag{4}$$

4.1.2 同态乘法噪声

综合式(2)、(3),有:

$$\langle \boldsymbol{c}_{mult}, \boldsymbol{sk} \rangle = m_1 m_2 + e' - e_{\delta'} + \langle BitDecomp(\boldsymbol{c}_{BD}), \boldsymbol{e}_{BD} \rangle$$

其中:

$$e_{\delta'} = \left\langle \left[BitDecomp(\boldsymbol{c}_1' \otimes \boldsymbol{c}_2') \right]_{\delta'}, (Powersof2(\boldsymbol{sk} \otimes \boldsymbol{sk})) \right\rangle$$

$$e' = m_1 e_2 + m_2 e_1 + e_1 e_2 - \langle \boldsymbol{c}_{2\delta}, \boldsymbol{sk} \rangle (m_1 + e_1) - \langle \boldsymbol{c}_{1\delta}, \boldsymbol{sk} \rangle (m_2 + e_2) - \langle \boldsymbol{c}_{1\delta}, \boldsymbol{sk} \rangle \langle \boldsymbol{c}_{2\delta}, \boldsymbol{sk} \rangle$$

各分量的上界为:

$$e_i = \boldsymbol{r}^{\mathrm{T}} \boldsymbol{e}_i \leqslant \tau B$$

$$e_{\delta'} = \left\langle \left[BitDecomp(\boldsymbol{c}_1' \otimes \boldsymbol{c}_2') \right]_{\delta'}, (Powersof2(\boldsymbol{sk} \otimes \boldsymbol{sk})) \right\rangle \leqslant$$

$$(N+1)^2 2^{\delta'-1}$$

$$\langle BitDecomp(\boldsymbol{c}_{BD}), \boldsymbol{e}_{BD}\rangle \leqslant (N+1)^2\left(\lceil \mathrm{lb}\, q_l\rceil - \delta'\right)B$$

$$\langle \boldsymbol{c}_{i\delta}, sk\rangle \leqslant (N+1)2^{\delta-1}$$

由此可得:

$$\begin{aligned} e_{mult} &= \langle \boldsymbol{c}_{mult}, \boldsymbol{sk}\rangle - m_1 m_2 = \\ &e' - e_{\delta'} + \langle BitDecomp(\boldsymbol{c}_{BD}), \boldsymbol{e}_{BD}\rangle \leqslant \\ &2\nu\tau B + (\tau B)^2 + 2(N+1)2^{\delta-1}(\nu+\tau B) + \\ &\left((N+1)2^{\delta-1}\right)^2 + (N+1)^2 2^{\delta'-1} + \\ &(N+1)^2\left(\lceil \mathrm{lb}\, q_l\rceil - \delta'\right)B \leqslant \\ &2\nu\tau B + (\tau B)^2 + 2^{\delta}(N+1)(\nu+\tau B) + (N+1)^2 \cdot \\ &\left[2^{2(\delta-1)} + 2^{\delta'-1} + \left(\lceil \mathrm{lb}\, q_l\rceil - \delta'\right)B\right] \end{aligned} \tag{5}$$

与原来的同态乘法噪声相比,在δ与δ'取合适值时,本文方案既能降低同态乘法运算时计算密钥的复杂性,也能降低噪声和密文的存储开销。

4.2　效率

本文所提出的低位比特丢弃方法能够减小重线性化密钥的尺寸,使原来的计算密钥维度从$(N+1)^2\lceil \mathrm{lb}\, q_l\rceil \times (N+1)$降低至$\left((N+1)^2\left(\lceil \mathrm{lb}\, q_l\rceil - \delta'\right)\right)\times(N+1)$;定义计算复杂性等于向量中各数值元素参与运算的次数,本文方案通过丢弃低位比特,同态乘法的计算复杂性得到明显减小,降低了计算开销;同时,该方案进行通信的每一个密文向量均减少了δ比特,提高了通信效率,也减小了密文向量的存储开销,使该方案在实际使用过程中更加快速高效。本文方案与LWE型CKKS方案的性能对比如表1所示。由表1可以看出,相较LWE型CKKS方案,本文所提优化方案使得计算密钥的维度减少,使得同态乘法的计算复杂性降低。

4.3　安全性

本文提出的低位比特丢弃方法在CKKS17方案上进行了优化,其密钥生成算法、重线性化技术及加解密过程仍与CKKS17保持一致,安全性依赖于LWE问题的困难性。同时,低位比特丢弃技术可视为密文向量的低位比特与另一向量的"与"过程,对安全性没有影响。因此,本文提出的低位比特丢弃方法设计的优化加密方案的安全性与CKKS17方案的安全性相同,可以达到语义安全。

表1　本文方案与LWE型CKKS方案的性能对比

Tab. 1　Performance comparison between proposed scheme and LWE type CKKS scheme

方案类型	密文存储空间/bit	计算密钥尺寸	同态乘法计算复杂性
LWE型CKKS17方案	$(N+1)\lceil \mathrm{lb}\, q\rceil$	$\left((N+1)^2\lceil \mathrm{lb}\, q\rceil\right)\times(N+1)$	$\approx (N+1)^3\lceil \mathrm{lb}\, q_l\rceil$
本文方案	$(N+1)\left(\lceil \mathrm{lb}\, q\rceil - \delta\right)$	$\left((N+1)^2\left(\lceil \mathrm{lb}\, q\rceil - \delta'\right)\right)\times(N+1)$	$\approx (N+1)^3\left(\lceil \mathrm{lb}\, q_l\rceil - \delta'\right)$

5　结语

CKKS17方案作为目前实际应用中重要的一个方案,具有支持浮点数运算的优点。本文在原有方案的基础上通过舍弃密文低位比特的方法,对其进行了优化,提出了优化的LWE型CKKS方案。相较于现在的方案,本文所优化的方案缩减了重线性化密钥的尺寸,使得同态计算的效率得到了提升,且密文向量比特的减少也使得该方案在实际运用过程中的存储和通信效率得以提高。基于RLWE的CKKS方案能够将多个密文打包进行计算,效率更高,下一步将针对RLWE型CKKS方案的优化进行研究。

参考文献 (References)

[1] GENTRY C. Fully homomorphic encryption using ideal lattices [C]// Proceedings of the 2009 41st ACM Symposium on Theory of Computing. New York: ACM, 2009: 169-178.

[2] VAN DIJK M, GENTRY C, HALEVI S, et al. Fully homomorphic encryption over the integers [C]// Proceedings of the 2010 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 6110. Berlin: Springer, 2010: 24-43.

[3] BRAKERSKI Z, GENTRY C, VAIKUNTANATHAN V. (Leveled) fully homomorphic encryption without bootstrapping [C]// Proceedings of the 2012 3rd Innovations in Theoretical Computer Science Conference. New York: ACM, 2012: 309-325.

[4] GENTRY C, SAHAI A, WATERS B. Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based [C]// Proceedings of the 2013 33rd Annual Cryptology Conference, LNCS 8042. Berlin: Springer, 2013: 75-92.

[5] LÓPEZ-ALT A, TROMER E, VAIKUNTANATHAN V. On-the-fly multiparty computation on the cloud via multi-key fully homomorphic encryption [C]// Proceedings of the 2012 44th Annual ACM Symposium on Theory of Computing. New York: ACM, 2012: 1219-1234.

[6] CHILLOTTI I, GAMA N, GEORGIEVA M, et al. Faster fully homomorphic encryption: bootstrapping in less than 0.1 seconds [C]// Proceedings of the 2016 22nd International Conference on the Theory and Application of Cryptology and Information Security, LNCS 10031. Berlin: Springer, 2016:3-33.

[7] CHEON J H, KIM A, KIM M, et al. Homomorphic encryption for arithmetic of approximate numbers [C]// Proceedings of the 2017 23rd International Conference on the Theory and Applications of Cryptology and Information Security, LNCS 10624. Cham: Springer, 2017: 409-437.

[8] LAUTER K, LÓPEZ-ALT A, NAEHRIG M. Private computation on encrypted genomic data [C]// Proceedings of the 2014 3rd International Conference on Cryptology and Information Security in Latin America, LNCS 8895. Cham: Springer, 2014: 3-27.

[9] WANG S, ZHANG Y, DAI W, et al. HEALER: Homomorphic computation of ExAct Logistic rEgRession for secure rare disease variants analysis in GWAS [J]. Bioinformatics, 2016, 32(2):

211-218.

[10] CHEON J H, KIM M, LAUTER K. Homomorphic computation of edit distance [C]// Proceedings of the 2015 International Conference on Financial Cryptography and Data Security, LNCS 8976. Berlin: Springer, 2015: 194-212.

[11] HAMLIN A, SHELAT A, WEISS M, et al. Multi-key searchable encryption, revisited [C]// Proceedings of the 2018 21st IACR International Conference on Practice and Theory of Public-Key Cryptography, LNCS 10769. Cham: Springer, 2018: 95-124.

[12] 王永建,张健,程少豫,等. 面向云计算的同态加密改进设计[J]. 信息网络安全,2017,17(3):21-26. (WANG Y J, ZHANG J, CHENG S Y, et al. An improved design of homomorphic encryption for cloud computing [J]. Netinfo Security, 2017, 17(3): 21-26.)

[13] CHEON J H, HAN K, KIM A, et al. Bootstrapping for approximate homomorphic encryption [C]// Proceedings of the 2018 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 10820. Cham: Springer, 2018: 360-384.

[14] CHEON J H, HAN K, KIM A, et al. A full RNS variant of approximate homomorphic encryption [C]// Proceedings of the 2018 25th International Conference on Selected Areas in Cryptography, LNCS 11349. Cham: Springer, 2018: 347-368.

[15] CHEN H, CHILLOTTI I, SONG Y. Improved bootstrapping for approximate homomorphic encryption [C]// Proceedings of the 2019 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 11477. Cham: Springer, 2019: 34-54.

[16] CHEN H, DAI W, 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.

[17] 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. Piscataway: IEEE, 2011: 97-106.

[18] ZHOU T, YANG X, LIU L, et al. Faster bootstrapping with multiple addends [J]. IEEE Access, 2018, 6: 49868-49876.

[19] REGEV O. On lattices, learning with errors, random linear codes, and cryptography [J]. Journal of the ACM, 2009, 56(6): Article No. 34.

[20] 车小亮,周昊楠,周潭平,等. 基于NTRU的多密钥同态加密方案解密结构[J]. 计算机应用,2020,40(7):1959-1964. (CHE X L, ZHOU H N, ZHOU T P, et al. Decryption structure of multi-key homomorphic encryption scheme based on NTRU [J]. Journal of Computer Applications, 2020, 40(7): 1959-1964.)

[21] GENTRY C, HALEVI S, SMART N P. Homomorphic evaluation of the AES circuit [C]// Proceedings of the 2012 32nd Annual Cryptology Conference, LNCS 7417. Berlin: Springer, 2012: 850-867.

This work is partially supported by the National Key Research and Development Program of China (2017YFB0802000), the National Natural Science Foundation of China (U1636114, 61872384), the Natural Science Foundation of Shaanxi Province (2020JQ-492), the Project of Innovative Research Team in Engineering University of PAP (KYTD201805), the Fundamental Research Funds of Engineering University of PAP (WJY201910, WJY201914, WJY201912).

ZHENG Shangwen, born in 1998, M. S. candidate. His research interests include homomorphic cipher, information security.

LIU Yao, born in 1993, M. S. candidate. His research interests include homomorphic cipher, information security.

ZHOU Tanping, born in 1989, Ph. D., lecturer. His research interests include homomorphic cipher, information security.

YANG Xiaoyuan, born in 1959, M. S., professor. His research interests include cryptography, information security.