基于NTRU的全同态加密方案

李子臣[1],张卷美[2],杨亚涛[2,3],张峰娟[2,3]
(1.北京印刷学院,北京 102600; 2.北京电子科技学院,北京 100070;
3.西安电子科技大学通信工程学院,陕西西安 710071)

摘 要: 本文提出一种基于公钥密码体制(Number Theory Research Unit,NTRU)选择明文攻击(Chosen Plaintext Attack,CPA)可证明安全的全同态加密方案.首先,对NTRU的密钥生成算法进行改进,通过格上的高斯抽象算法生成密钥对,避免了有效的格攻击,同时,没有改变密钥的分布.然后,基于改进的NTRU加密算法,利用Flattening技术,构造了一个全同态加密体制,并在标准模型下证明方案是选择明文攻击不可区分性IND-CPA安全的.

关键词: 全同态加密; 公钥密码体制NTRU; 高斯抽样算法; 可证明安全
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112 (2018)04-0938-07
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.04.023

A Fully Homomorphic Encryption Scheme Based on NTRU

LI Zi-chen[1],ZHANG Juan-mei[2],YANG Ya-tao[2,3],ZHANG Feng-juan[2,3]
(1. *Beijing Institute of Graphic Communication*, *Beijing* 102600, *China*;
2. *Beijing Electronic Science & Technology Institute*, *Beijing* 100070, *China*;
3. *School of Telecommunications Engineering*, *Xidian University*, *Xi'an*, *Shaanxi* 710071, *China*)

Abstract: A fully homomorphic encrgption scheme was presented based on number theory research unit(NTRU), which is provable security about indistinguishable chosen plaintext attack (IND-CPA). Firstly, to avoid the effective lattice attacks, we modified the key generation algorithm of NTRU by Gaussian abstraction algorithm of lattices, and the distribution of the key is not changed. Then, we proposed a new homomorphic encryption scheme based on the improved NTRU encryption algorithm by using the Flattening technique. Its IND-CPA security was proved strictly under the standard model.

Key words: fully homomorphic encryption; number theory research unit; Gaussian abstraction algorithm; provable security

1 引言

全同态加密允许对密文进行任意的运算,运算后的结果解密后等价于对明文进行相应计算的结果.随着互联网技术的日趋成熟和应用的广泛普及,用户的个人信息的隐私性也越来越多地得到重视.而全同态加密正是迎合了这一需求,全同态加密在云计算、密文检索、安全多方计算等方面都有着很重要的应用,因此,全同态加密成为近些年密码学家们的研究热点.早在1978年,Rivest等提出了全同态加密的概念[1].自从全同态加密的概念提出之后,构造全同态加密体制一直是一个公开的难题.密码学家们提出了很多同态加密体制,但它们都只具有单一的同态性,例如,ElGamal加密体制[2]、Goldwasser-Micali加密体制[3]、Paillier加密体制[4]都具有加法同态特性,RSA加密体制[5]具有乘法同态特性.直到2009年,Gentry提出了第一个全同态加密体制[6],开启了全同态密码研究的先河.Gentry的体制是基于理想格,是具有开创性的奠基之作,但是,体制的效率较低,同时实现还较困难.所以,在第一个全同态加密方案提出之后,许多新的全同态加密方案的构造致力于向实际实现上靠近,并且基于更少的困难性假设.例如,基于整数的全同态加密方案[7],基于LWE(Learning With Errors)困难问题的全同态方案[8]以及它的一系列改进方案[9,10],等.在Brakerski,Gentry等提出的基于LWE的BGV方案[11]中,描述了一种新的约减密文噪音的方法"模交换",使得全同态加密方案不再使用Gentry原始框架中的Bootstrapping方法,而Bootstrapping方法正是Gentry的全同态加密方案效率低下的症结所在.2013年,IBM研究中心发布了一个

收稿日期:2016-12-11;修回日期:2017-07-28;责任编辑:孙瑶
基金项目:国家自然科学基金(No.61370188);"十三五"国家密码发展基金(No.MMJJ20170110)

开源代码库 HElib[12],该库实现的是 BGV 方案. 文献[13]提出一种基于同态加密的高效多方保密计算. 文献[14]提出一种基于身份的同态加密方案,方案的安全性基于 RLWE 困难问题. 文献[15]提出的全同态加密方案,降低了密文的扩张率.

NTRU 公钥加密体制是后量子加密算法中的典型代表[16],是一个基于多项式环的密码体制. NTRU 的安全性可以规约为格上的"近似最近向量问题",可以抵抗已知的量子攻击. 目前为止,并没有任何理由说明 NTRU 加密体制是不安全的[17]. NTRU 加密体制整个过程只包括小整数的加法、乘法以及模运算等线性运算,因此,算法的执行速度较快,被认为是公钥加密体制中最快的算法,也是比较容易实现的算法.

最近,Lopez 等提出基于 NTRU 的全同态加密方案[18],但在密钥生成过程存在格攻击的安全问题,方案的安全性没有严格证明. 本文在此基础上,在密钥生成部分,通过格上的高斯抽样算法生成密钥对,有效避免格攻击,并且不改变密钥的分布. 在加密算法部分,把明文空间由原来的$\mathbb{Z}_2$扩展至$\mathbb{Z}_p$. 利用 Flattening 技术[19],构造一个全同态加密体制,在标准模型下严格地证明了该体制满足 IND-CPA 安全.

2　相关定义及符号表示

2.1　相关定义

定义 1　格上的高斯函数

对于任意的$s>0$,定义$\mathbb{R}^n$上的高斯函数,以$\boldsymbol{c}$为中心,参数为s:

$$\forall \boldsymbol{x}\in\mathbb{R}^n,\rho_{s,c}(x)=\exp\left(\frac{-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2}{s^2}\right) \tag{1}$$

当下标s和$\boldsymbol{c}$缺省时,s和$\boldsymbol{c}$分别看做是 1 和 0.

对于任意的$\boldsymbol{c}\in\mathbb{R}^n$,实数$s>0$,$n$维格$\Lambda$,$\Lambda$的秩为$k\leqslant n$,定义$\Lambda$上的离散高斯分布如下:

$$\forall \boldsymbol{x}\in\Lambda,\ D_{\Lambda,s,\boldsymbol{c}}(x)=\frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{s,\boldsymbol{c}}(\Lambda)} \tag{2}$$

定义 2　整数上的高斯抽样算法

整数$\mathbb{Z}$可以看做一维格,令$t(n)\geqslant\omega(\sqrt{\log n})$,在输入$(s,\boldsymbol{c})$和安全参数$n$的基础上,随机均匀地选择一个整数$\boldsymbol{x}\leftarrow Z=\mathbb{Z}\cap[\boldsymbol{c}-s\cdot t,\boldsymbol{c}+s\cdot t]$,那么,称以概率$\rho_s(\boldsymbol{x}-\boldsymbol{c})$输出$\boldsymbol{x}$.

定义 3[20]　格上的高斯抽样算法

算法输入为n维基$\boldsymbol{B}\in\mathbb{Z}^{n\times k}$,基的秩为$k$,一个足够大的高斯参数$s$,一个中心$\boldsymbol{c}\in\mathbb{R}^n$,$span(\boldsymbol{b}_1,\cdots,\boldsymbol{b}_{k-1})$表示由$\boldsymbol{b}_1,\cdots,\boldsymbol{b}_{k-1}$所张成的空间,输出为一个从$D_{L(B),s,\boldsymbol{c}}$中的一个样本. 过程如下:

(1)如果$k=0$,返回 0.

(2)计算$\tilde{\boldsymbol{b}}_k$,即$\boldsymbol{b}_k$与$span(\boldsymbol{b}_1,\cdots,\boldsymbol{b}_{k-1})$正交的非零向量.

(3)计算$\boldsymbol{t}$,即$\boldsymbol{c}$在$span(\boldsymbol{B})$上的映射,计算标量值$t=\frac{\langle\boldsymbol{t},\tilde{\boldsymbol{b}}_k\rangle}{\langle\tilde{\boldsymbol{b}}_k,\tilde{\boldsymbol{b}}_k\rangle}\in\mathbb{R}$.

(4)使用定义 2 中的针对$\mathbb{Z}$的高斯抽样算法,选择一个整数$z\leftarrow D_{\mathbb{Z},s/\|\tilde{b}_k\|,t}$.

(5)输出$z\boldsymbol{b}_k+SampleD(\boldsymbol{B}',s,\boldsymbol{t}-z\boldsymbol{b}_k)$,其中,$\boldsymbol{B}'=[\boldsymbol{b}_1,\cdots,\boldsymbol{b}_{k-1}]$.

详细内容可参考文献[20].

定义 4[21]　RLWE

对于安全参数λ,令$f(x)=x^d+1$,其中,d是 2 的幂次. 令$q\geqslant 2$,并且是一个整数. 令$R=\mathbb{Z}[x]/(f(x))$,$R_q=R/qR$,$\chi=\chi(\lambda)$是R上的一个分布. $RLWE_{d,q,\chi}$问题是指区分以下两个分布:

(1)从R_q^2中均匀取样(a_i,b_i).

(2)首先,均匀地从R_q中取样s,即$s\leftarrow R_q$,然后均匀取样$a_i\leftarrow\mathbb{R}_q$,从$\chi$中取样$e_i$,令$b_i=a_i\cdot s+e_i$.

$RLWE_{d,q,\chi}$假设是指$RLWE_{d,q,\chi}$问题是不可行的.

定义 5　B-界多项式

一个多项式$e\in R$是 B-界的,如果满足$\|e\|_\infty\leqslant B$.

定义 6　B-界分布

R上的一组分布$\{\chi_n\}_{n\in N}$是 B-界的,如果从χ_n中选取的所有多项式e满足$\|e\|_\infty\leqslant B$. 也就是说,B-界分布产生 B-界多项式.

定义 7　IND-CPA 安全

定义一个敌手与挑战者之间的游戏,分为以下几个阶段.

初始化阶段:挑战者运行加密体制的密钥生成算法,将生成的公钥交给敌手.

预言机访问阶段:敌手选择明文,询问加密预言机,在得到密文应答之后,敌手可以多次分阶段提交选择的明文,并得到相对应于不同明文的密文.

挑战阶段:敌手选取两个明文m_0和m_1,把这两个明文发送给挑战者,挑战者选取$b\in\{0,1\}$,并把挑战密文$c=Enc_{pk}(m_b)$发送给敌手.

猜测阶段:敌手试图猜测挑战密文所对应的b',当$b'=b$时,认为敌手在攻击游戏中获胜.

如果对于任意一个多项式时间的敌手A,在游戏中获胜的概率$Adv_{IND-CPA}(A)$满足

$$\left|Adv_{IND-CPA}(A)-\frac{1}{2}\right|=negl(\lambda) \tag{3}$$

其中,$negl$是可以忽略,λ是方案的安全参数.

则称该体制是 IND—CPA 安全的.

2.2　参数的表示及选取

对于安全参数λ,方案的参数选取如下:

整数$n=n(\lambda)$.

$p=p(\lambda)$,$q=q(\lambda)$.

n 次多项式 $\phi(x)=\phi_\lambda(x)$.

环 $R=\mathbb{Z}_q[x]/\langle\phi(x)\rangle$ 上的一个 $B(\lambda)$-界的误差分布 $\chi=\chi(\lambda)$.

对于 R 中的元素 $a(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}$,它的 ℓ_∞ 范数表示为 $\|a\|_\infty=\max\{|a_i|\}$,$i=0,\cdots,n-1$.

多项式 $a(x)$ 的系数 $a_i\in\{-\lfloor q/2\rfloor,\cdots,\lfloor q/2\rfloor\}$,符号 $\lfloor\ \rfloor$ 表示向下取整.

3 NTRU 加密体制

3.1 NTRU 加密体制[16]

密钥生成 KeyGen:

在多项式环 $R=Z[x]/(x^N-1)$ 中,随机选取两个多项式 f,g,次数均为 $N-1$,系数为整数. p,q 是整数,也不需要是素数,满足 $\gcd(p,q)=1$,q 比 p 大. 多项式 f 满足模 p 和模 q 都有逆,分别记为 F_p,F_q,即

$$F_p*f\equiv 1(\mathrm{mod}p) \tag{4}$$

$$F_q*f\equiv 1(\mathrm{mod}q) \tag{5}$$

计算 $h=F_q*g(\mathrm{mod}q)$,上述式子中的 $\mathrm{mod}p$,$\mathrm{mod}q$ 是指多项式的系数分别是区间 $\left[-\frac{p}{2},\frac{p}{2}\right]$ 和 $\left[-\frac{q}{2},\frac{q}{2}\right]$ 中的整数.

那么,公钥 $pk=h$,私钥 $sk=(f,F_p)$.

加密 Enc:

m 表示为多项式,次数为 $N-1$,系数为整数. 随机选取一个多项式 ϕ,次数为 $N-1$,系数为整数.

$$c=p\phi*h+m(\mathrm{mod}q) \tag{6}$$

解密 Dec:

首先计算 $a=f*c(\mathrm{mod}q)$,其中 a 的系数属于集合 $\left\{-\frac{q}{2},\cdots,\frac{q}{2}\right\}$. 然后计算 $m=F_p*a(\mathrm{mod}p)$.

3.2 改进的 NTRU 加密体制

密钥生成 KeyGen(1^λ):

λ 为安全参数.

选择一个足够大的标准差 σ,使得 f 可以表示成如下形式:$f=p\cdot f'+1$,其中,f' 为从离散高斯分布 $D_{\mathbb{Z}^n,\sigma}$ 中取样一个多项式,即 $f\equiv 1(\mathrm{mod}p)$,从而使得解密过程更加高效.

输入:$n,q\in\mathbb{Z}$,$p\in R_q^*$,$\sigma\in\mathbb{R}$,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:一对密钥 $(sk,pk)\in R\times R_q^*$.

具体生成过程如下:

(1)从离散高斯分布 $D_{\mathbb{Z}^n,\sigma}$ 中取样 f',令 $f=p\cdot f'+1$,如果 $f\mathrm{mod}q\notin R_q^*$,重新取样.

当维数 n 取得很大的整数时,f' 是项数为 n 的多项式,f 也是项数为 n 的多项式,R_q 中模 q 可逆的多项式的概率很大,因此,满足条件的 f 的个数很多,保证了 f 可以生成,并且是安全的.

(2)从离散高斯分布 $D_{\mathbb{Z}^n,\sigma}$ 中取样 g,如果 $g\mathrm{mod}q\notin R_q^*$,重新取样.

(3)返回私钥 $sk=f$,公钥 $pk=h=pgf^{-1}\in R_q^*$.

***Enc*(*pk*,*m*):**

明文空间为 $\mathbb{Z}_p$,所有的计算都是在环 $R=\mathbb{Z}_q[x]/\langle\phi(x)\rangle$ 上进行的,即模 q 和模 $\phi(x)$ 运算.

输出密文 $c=hs+pe+m$,其中,s 和 e 都是从 χ 中抽样选取的多项式,且 $c\in R$.

***Dec*(*sk*,*c*):**

$$m=fc(\mathrm{mod}p) \tag{7}$$

下面进行正确性分析:

$$\begin{aligned}m&=fc\\&=f(hs+pe+m)\\&=pgs+fpe+fm\\&=p(gs+fe)+fm\\&=fm(\mathrm{mod}p)\end{aligned} \tag{8}$$

由密钥生成算法可知:$f\equiv 1(\mathrm{mod}p)$,正确性得证.

4 全同态加密体制

首先介绍文献[19]中的几个函数和 Flattening 技术. 一个向量 $\boldsymbol{a}=(a_0,\cdots,a_{k-1})$ 分解成它的比特表示如下:

$$BitDecomp(\boldsymbol{a})=(a_{0,0},\cdots,a_{0,l-1},\cdots,a_{k-1,0},\cdots,a_{k-1,l-1})$$

反之,我们也可从比特表示中恢复出这个向量,如下:

$$BitDecomp^{-1}(\boldsymbol{a})=\left(\sum 2^j a_{0,j},\cdots,\sum 2^j a_{k-1,j}\right) \tag{9}$$

$$Flatten(\boldsymbol{a})=BitDecomp(BitDecomp^{-1}(\boldsymbol{a})) \tag{10}$$

然后,基于改进后的 NTRU 加密体制构造全同态加密方案,方案具体如下.

密钥生成算法 KeyGen:

与改进的 NTRU 加密方案的密钥生成算法相同. 即,通过格上的高斯抽样算法得到公私钥对,这样可以避免有效的格攻击,同时不会改变密钥的分布空间[22].

加密算法 Enc:

首先,选取一个明文 $m\in\mathbb{Z}_p$,然后利用改进后的 NTRU 加密体制的加密算法对 0 进行加密,得到一个长度为 $l=\log q$ 的密文向量 $\boldsymbol{c}$,如下:

$$\boldsymbol{c}=(c_{l-1},c_{l-2},\cdots,c_0) \tag{11}$$

其中,c_i 是由改进的 NTRU 的加密体制对 0 加密得到的密文. 即,$c_i=hs_i+pe_i$.

利用 $BitDecomp$ 把 $\boldsymbol{c}$ 转化为一个 $l\times l$ 矩阵 $\boldsymbol{C}$,如下:

$$\boldsymbol{C}=BitDecomp(\boldsymbol{c}^{\mathrm{T}})=(\boldsymbol{c}_{l-1}^{\mathrm{T}},\boldsymbol{c}_{l-2}^{\mathrm{T}},\cdots,\boldsymbol{c}_0^{\mathrm{T}}) \tag{12}$$

其中,$\boldsymbol{c}_i^{\mathrm{T}}$ 是一个二进制多项式.

然后计算 $\boldsymbol{C}'=Flatten(\boldsymbol{I}_l\cdot m+\boldsymbol{C})$,其中,$\boldsymbol{I}_l$ 为 $l\times l$ 单位矩阵.

$\boldsymbol{C}'$即为消息 m 对应的密文矩阵.

解密算法 Dec:

取矩阵 $\boldsymbol{C}'$的最后一行,并应用 $BitDecomp^{-1}$,如下:

$$BitDecomp^{-1}(\boldsymbol{C}'_{(0,l-1)},\boldsymbol{C}'_{(0,l-2)},\cdots,\boldsymbol{C}'_{(0,0)})=\boldsymbol{C}_0 \tag{13}$$

$$m=\lfloor \boldsymbol{C}_0 f\rfloor=\mathrm{mod}p \tag{14}$$

密文计算算法 Eval:

$$\boldsymbol{C}'_3=Flatten(\boldsymbol{C}'_1+\boldsymbol{C}'_2) \tag{15}$$

$$\boldsymbol{C}'_3=Flatten(\boldsymbol{C}'_1\cdot\boldsymbol{C}'_2) \tag{16}$$

5　方案分析

5.1　正确性分析

由加密算法可知:

$$\begin{aligned}\boldsymbol{C}&=BitDecomp(\boldsymbol{c}^{\mathrm{T}})\\&=(\boldsymbol{c}^{\mathrm{T}}_{l-1},\boldsymbol{c}^{\mathrm{T}}_{l-2},\cdots,\boldsymbol{c}^{\mathrm{T}}_0)\\&=\begin{pmatrix}c_{(l-1,l-1)}&c_{(l-1,l-2)}&\cdots&c_{(l-1,0)}\\c_{(l-2,l-1)}&c_{(l-2,l-2)}&\cdots&c_{(l-2,0)}\\\vdots&\vdots&\ddots&\vdots\\c_{(0,l-1)}&c_{(0,l-2)}&\cdots&c_{(0,0)}\end{pmatrix}\end{aligned} \tag{17}$$

其中,$c_{(i,j)}$表示二进制多项式 $\boldsymbol{c}^{\mathrm{T}}_i$ 中第 j 项的系数.

$$\boldsymbol{I}_l\cdot m+\boldsymbol{C}=\begin{pmatrix}m&0&\cdots&0\\0&m&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&m\end{pmatrix}+\begin{pmatrix}c_{(l-1,l-1)}&c_{(l-1,l-2)}&\cdots&c_{(l-1,0)}\\c_{(l-2,l-1)}&c_{(l-2,l-2)}&\cdots&c_{(l-2,0)}\\\vdots&\vdots&\ddots&\vdots\\c_{(0,l-1)}&c_{(0,l-2)}&\cdots&c_{(0,0)}\end{pmatrix}$$

$$=\begin{pmatrix}c_{(l-1,l-1)}+m&c_{(l-1,l-2)}&\cdots&c_{(l-1,0)}\\c_{(l-2,l-1)}&c_{(l-2,l-2)}+m&\cdots&c_{(l-2,0)}\\\vdots&\vdots&\ddots&\vdots\\c_{(0,l-1)}&c_{(0,l-2)}&\cdots&c_{(0,0)}+m\end{pmatrix}$$

$$\boldsymbol{C}'=Flatten(\boldsymbol{I}_l\cdot m+\boldsymbol{C}) \tag{18}$$

$Flatten$ 函数是把上面的矩阵转化为 0/1 矩阵.

取矩阵 $\boldsymbol{C}'$的最后一行,计算

$$\begin{aligned}&BitDecomp^{-1}(\boldsymbol{C}'_{(0,l-1)},\boldsymbol{C}'_{(0,l-2)},\cdots,\boldsymbol{C}'_{(0,0)})\\&=BitDecomp^{-1}(c_{(0,l-1)},c_{(0,l-2)},\cdots,c_{(0,0)}+m)\\&=\sum_{i=0}^{l-1}2^i\boldsymbol{C}'_{(0,i)}\\&=m+\sum_{i=0}^{l-1}2^i c_{(0,i)}=m+c_0\end{aligned} \tag{19}$$

$$\therefore\quad \boldsymbol{C}_0=m+c_0=m+hs_0+pe_0 \tag{20}$$

$$\begin{aligned}\boldsymbol{C}_0 f&=(m+hs_0+pe_0)f=mf+pgf^{-1}s_0 f+pe_0 f\\&=mf+pgs_0+pe_0 f\end{aligned} \tag{21}$$

$$\begin{aligned}\lfloor \boldsymbol{C}_0 f\rfloor\mathrm{mod}p&=(mf+pgs_0+pe_0 f)\mathrm{mod}p\\&=mf\mathrm{mod}p\end{aligned} \tag{22}$$

$$\because\quad f\equiv 1(\mathrm{mod}p)$$

$$\therefore\quad \lfloor \boldsymbol{C}_0 f\rfloor\mathrm{mod}p=m \tag{23}$$

证毕.

5.2　同态性分析

加法同态:

$$\boldsymbol{C}'_1+\boldsymbol{C}'_2=\begin{pmatrix}c_{1(l-1,l-1)}+m_1&c_{1(l-1,l-2)}&\cdots&c_{1(l-1,0)}\\c_{1(l-2,l-1)}&c_{1(l-2,l-2)}+m_1&\cdots&c_{1(l-2,0)}\\\vdots&\vdots&\ddots&\vdots\\c_{1(0,l-1)}&c_{1(0,l-2)}&\cdots&c_{1(0,0)}+m_1\end{pmatrix}+\begin{pmatrix}c_{2(l-1,l-1)}+m_2&c_{2(l-1,l-2)}&\cdots&c_{2(l-1,0)}\\c_{2(l-2,l-1)}&c_{2(l-2,l-2)}+m_2&\cdots&c_{2(l-2,0)}\\\vdots&\vdots&\ddots&\vdots\\c_{2(0,l-1)}&c_{2(0,l-2)}&\cdots&c_{2(0,0)}+m_2\end{pmatrix}$$

$$=\begin{pmatrix}c_{1(l-1,l-1)}+m_1+c_{2(l-1,l-1)}+m_2&c_{1(l-1,l-2)}+c_{2(l-1,l-2)}&\cdots&c_{1(l-1,0)}+c_{2(l-1,0)}\\c_{1(l-2,l-1)}+c_{2(l-2,l-1)}&c_{1(l-2,l-2)}+m_1+c_{2(l-2,l-2)}+m_2&\cdots&c_{1(l-2,0)}+c_{2(l-2,0)}\\\vdots&\vdots&\ddots&\vdots\\c_{1(0,l-1)}+c_{2(0,l-1)}&c_{1(0,l-2)}+c_{2(0,l-2)}&\cdots&c_{1(0,0)}+m_1+c_{2(0,0)}+m_2\end{pmatrix}$$

$\boldsymbol{C}'_3=Flatten(\boldsymbol{C}'_1+\boldsymbol{C}'_2)$是把上面的矩阵转化为 0/1 矩阵.

下面对 $\boldsymbol{C}'_3$按照同态解密算法进行解密.

取上述矩阵的最后一行,并应用 $BitDecomp^{-1}$,如下:

$$\begin{aligned}&BitDecomp^{-1}(c_{1(0,l-1)}+c_{2(0,l-1)},\cdots,c_{1(0,0)}+m_1+c_{2(0,0)}+m_2)\\&=m_1+m_2+\sum_{i=0}^{l-1}2^i(c_{1(0,i)}+c_{2(0,i)})\\&=m_1+m_2+c_{1(0)}+c_{2(0)}=\boldsymbol{C}_3\end{aligned}$$

其中,$c_{1(0)}=hs_{1(0)}+pe_{1(0)}$,$c_{2(0)}=hs_{2(0)}+pe_{2(0)}$.

$$\begin{aligned}&\lfloor C_3 f\rfloor\mathrm{mod}p\\&=(m_1+m_2+hs_{1(0)}+pe_{1(0)}+hs_{2(0)}+pe_{2(0)})f\mathrm{mod}p\\&=(m_1+m_2+pgf^{-1}s_{1(0)}+pe_{1(0)}+pgf^{-1}s_{2(0)}+pe_{2(0)})f\mathrm{mod}p\\&=m_1+m_2\end{aligned}$$

加法同态得证.

乘法同态:

$$\boldsymbol{C}_1' \cdot \boldsymbol{C}_2' = \begin{pmatrix} c_{1(l-1,l-1)}+m_1 & c_{1(l-1,l-2)} & \cdots & c_{1(l-1,0)} \\ c_{1(l-2,l-1)} & c_{1(l-2,l-2)}+m_1 & \cdots & c_{1(l-2,0)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{1(0,l-1)} & c_{1(0,l-2)} & \cdots & c_{1(0,0)}+m_1 \end{pmatrix} \cdot \begin{pmatrix} c_{2(l-1,l-1)}+m_2 & c_{2(l-1,l-2)} & \cdots & c_{2(l-1,0)} \\ c_{2(l-2,l-1)} & c_{2(l-2,l-2)}+m_2 & \cdots & c_{2(l-2,0)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{2(0,l-1)} & c_{2(0,l-2)} & \cdots & c_{2(0,0)}+m_2 \end{pmatrix} \tag{24}$$

$\boldsymbol{C}_3' = Flatten(\boldsymbol{C}_1' \cdot \boldsymbol{C}_2')$ 把上述矩阵转化为 0/1 矩阵.

下面对 $\boldsymbol{C}_3'$ 按照同态解密算法进行解密.

上述乘法所得矩阵的最后一行的元素为:

$$\begin{aligned} & c_{1(0,l-1)} \cdot [c_{2(l-1,l-1)}+m_2] + c_{1(0,l-2)} \cdot c_{2(l-2,l-1)} + \\ & \quad \cdots + [c_{1(0,0)}+m_1] \cdot c_{2(0,l-1)} \\ & c_{1(0,l-1)} \cdot c_{2(l-1,l-2)} + c_{1(0,l-2)} \cdot [c_{2(l-2,l-2)}+m_2] + \\ & \quad \cdots + [c_{1(0,0)}+m_1] \cdot c_{2(0,l-2)} \\ & \quad \vdots \\ & c_{1(0,l-1)} \cdot c_{2(l-1,0)} + c_{1(0,l-2)} \cdot c_{2(l-2,0)} + \\ & \quad \cdots + [c_{1(0,0)}+m_1] \cdot [c_{2(0,0)}+m_2] \end{aligned} \tag{25}$$

对最后一行的元素应用 $BitDecomp^{-1}$,结果如下:

$$\begin{aligned} & 2^{l-1}c_{1(0,l-1)} \cdot c_{2(l-1,l-1)} + 2^{l-1}c_{1(0,l-2)} \cdot c_{2(l-2,l-1)} + \\ & \cdots + 2^{l-1}c_{1(0,0)} \cdot c_{2(0,l-1)} + 2^{l-2}c_{1(0,l-1)} \cdot c_{2(l-1,l-2)} \\ & + 2^{l-2}c_{1(0,l-2)} \cdot c_{2(l-2,l-2)} + \cdots + 2^{l-2}c_{1(0,0)} \cdot c_{2(0,l-2)} \\ & + \cdots + c_{1(0,l-1)} \cdot c_{2(l-1,0)} + c_{1(0,l-2)} \cdot c_{2(l-2,0)} \\ & + \cdots + c_{1(0,0)} \cdot c_{2(0,0)} + 2^{l-1}c_{1(0,l-1)} \cdot m_2 \\ & + 2^{l-1}c_{2(0,l-1)} \cdot m_1 \\ & + 2^{l-2}c_{1(0,l-2)} \cdot m_2 + 2^{l-2}c_{2(0,l-2)} \cdot m_1 \\ & + \cdots + c_{1(0,0)} \cdot m_2 + c_{2(0,0)} \cdot m_1 \\ & + m_1 \cdot m_2 \end{aligned}$$

$$\begin{aligned} 上式 = & \sum_{i=0}^{l-1} 2^i c_{1(0,l-1)} \cdot c_{2(l-1,i)} + \sum_{i=1}^{l-1} 2^i c_{1(0,l-2)} \cdot c_{2(l-2,i)} \\ & + \cdots + \sum_{i=0}^{l-1} 2^i c_{1(0,0)} \cdot c_{2(0,i)} + \sum_{i=0}^{l-1} 2^i c_{1(0,i)} \cdot m_2 \\ & + \sum_{i=0}^{l-1} 2^i c_{2(0,i)} \cdot m_1 + m_1 \cdot m_2 \\ = & c_{1(0,l-1)} \cdot c_{2(l-1)} + c_{1(0,l-2)} \cdot c_{2(l-2)} \\ & + \cdots + c_{1(0,0)} \cdot c_{2(0)} \\ & + c_{1(0)} \cdot m_2 + c_{2(0)} \cdot m_1 + m_1 \cdot m_2 \\ = & C_3 \end{aligned}$$

上式中的 $c_{1(i)}$ 和 $c_{2(i)}$ 均为 0 的加密,其中 $i=0,\cdots,l-1$. 即 $c_{1(i)} = hs_{1(i)} + pe_{1(i)}, c_{2(i)} = hs_{2(i)} + pe_{2(i)}$.

$$\begin{aligned} \lfloor C_3 f \rceil \bmod p = & [c_{1(0,l-1)} \cdot c_{2(l-1)} + c_{1(0,l-2)} \cdot c_{2(l-2)} + \\ & \cdots + c_{1(0,0)} \cdot c_{2(0)} + c_{1(0)} \cdot m_2 \\ & + c_{2(0)} \cdot m_1 + m_1 \cdot m_2] f \bmod p \end{aligned} \tag{26}$$

将 $c_{1(i)} = hs_{1(i)} + pe_{1(i)}, c_{2(i)} = hs_{2(i)} + pe_{2(i)}, h = pgf^{-1}, f \equiv 1 (\bmod p)$ 带入式(26),得:

$$\lfloor C_3 f \rceil \bmod p = m_1 \cdot m_2 \tag{27}$$

乘法同态性得证.

5.3 安全性分析

定理 在 $RLWE_{d,q,\chi}$ 的困难假设下,本文的全同态加密体制是 IND-CPA 安全的.

证明 定理证明采用基于游戏的 Game-Hopping 方法,游戏中包含一个多项式时间的敌手 A,用 $Adv_{IND-CPA}(A)$ 表示敌手 A 在游戏中获胜的概率.

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 $pk=h$ 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 $c = Enc_{pk}(m_b)$,敌手 A 尝试区分 c 所对应的明文 $m_b, b \in \{0,1\}$. Game0 中敌手 A 的优势为

$$Adv_{IND-CPA}(A) = \left| \begin{matrix} \Pr[A(pk, \mathrm{Enc}_{pk}(m_0)=1)] \\ -\Pr[A(pk, \mathrm{Enc}_{pk}(m_1)=1)] \end{matrix} \right| \tag{28}$$

Game1:Game1 与 Game0 的区别在于公钥 pk 的生成方式. Game1 中的公钥 pk 不通过私钥 $sk=f$ 和高斯抽样算法得到,而是直接从 R_q^* 中随机均匀选取. 文献[20]中指出,根据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. 因此,敌手 A 无法区分 Game0 与 Game1,有

$$|Adv_{\mathrm{Game1}}(A) - Adv_{IND\text{-}CPA}(A)| = 0 \tag{29}$$

Game2:Game2 与 Game1 的区别在于 Game2 中的加密算法不再按照全同态加密体制中的改进后的 NTRU 加密算法进行加密,而是直接从 $\{0,1\}^{l\times l}$ 中随机均匀选取. 由文献[19]可知,$BitDecomp, BitDecomp^{-1}, Flatten$ 操作并不会对方案的安全性产生影响. 根据文献[23]中 NTRU 加密体制到 RLWE 问题的规约,可知 Game2 与 Game1 中,敌手 A 的优势差在于解决 RLWE 问题的优势

$$|Adv_{\mathrm{Game2}}(A) - Adv_{\mathrm{Game1}}(A)| = RLWE_{d,q,\chi}Adv(A) \tag{30}$$

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

$$|Adv_{\mathrm{Game3}}(A) - Adv_{\mathrm{Game2}}(A)| = RLWE_{d,q,\chi}Adv(A) \tag{31}$$

至此,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 $m_b, b \in \{0,1\}$ 没有关系. 因此,敌手 A 在 Game3 中的优势为 0,即

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

综上,由式(28)~(32)可得

$$Adv_{IND-CPA}(A) = RLWE_{d,q,\chi}Adv(A) + RLWE_{d,q,\chi}Adv(A)$$

因此,在 $RLWE_{d,q,\chi}$ 的困难假设下,$Adv_{IND-CPA}(A)$ 可忽略,本文的全同态加密体制是 IND-CPA 安全的.

6 小结

NTRU 加密体制是后量子加密算法中最受青睐的算法,以其高速的加解密速度得到了十分广泛的应用,而且,目前并没有发现 NTRU 算法不能抵抗的量子攻击.但是,它的可证明安全问题一直是一个悬而未决的问题.全同态加密是目前密码学研究的热点问题,在云计算、密文检索、安全多方计算等方面都有广泛应用.本文基于原始的 NTRU 加密体制,提出一种新的 NTRU 加密体制.基于改进后的加密体制,利用 Flattening 技术,提出一种基于 NTRU 加密体制的全同态加密算法,在标准模型下证明了全同态加密方案选择明文攻击的不可区分性 IND-CPA 安全.

参考文献

[1] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[A]. Foundations of Secure Computation[C]. USA: Academia Press, 1978. 169-179.

[2] GAMAL T E. A public key cryptosystem and a signature scheme based on discrete logarithms[A]. Proceedings of CRYPTO 84 on Advances in Cryptology[C]. New York: Springer-Verlag, 1985. 10-18.

[3] GOLDWASSER S, MICALI S. Probabilistic encryption & how to play mental poker keeping secret all partial information[A]. Proceedings of Fourteenth ACM Symposium on Theory of Computing[C]. New York: ACM, 1982. 365-377.

[4] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[J]. Lecture Notes in Computer Science, 1999, 547(1): 223-238.

[5] RIVEST R, SHAMIR A, ADLEMAN L M. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 26(2): 96-99.

[6] GENTRY C. A Fully Homomorphic Encryption Scheme[D]. USA: Stanford University, 2009.

[7] DIJK M V, GENTRY C, HALEVI S, et al. Fully homomorphic encryption over the integers[J]. Lecture Notes in Computer Science, 2009, (4): 24-43.

[8] BRAKERSKI Z, VAIKUNTANATHAN V. Efficient fully homomorphic encryption from (standard) LWE[A]. Proceedings of Foundations of Computer Science[C]. USA: IEEE, 2010. 97-106.

[9] MANDAL A, TIBOUCHI M. Fully homomorphic encryption over the integers with shorter public keys[A]. Proceedings of Conference on Advances in Cryptology[C]. New York: Springer-Verlag, 2011. 487-504.

[10] CORON J, NACCACHE D, TIBOUCHI M. Public key compression and modulus switching for fully homomorphic encryption over the integers[A]. Proceedings of International Conference on Theory and Applications of Cryptographic Techniques[C]. New York: Springer-Verlag, 2012. 446-464.

[11] YAGISAWA M. Fully homomorphic encryption without bootstrapping[J]. ACM Transactions on Computation Theory, 2015, 6(3): 1-36.

[12] HALEVI S, SHOUP V. HElib, Homomorphic Encryption Library[OL]. http://shaih.github.io/HElib/, 2012.

[13] 李顺东,王道顺. 基于同态加密的高效多方保密计算[J]. 电子学报, 2013, 41(4): 798-803.
LI Shun-dong, WANG Dao-shun. Efficient secure multiparty computation based on homomorphic encryption[J]. Acta Electronica Sinica, 2013, 41(4): 798-803. (in Chinese)

[14] 辛丹,顾纯祥,郑永辉,光焱,康元基. 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): 442887-2893.
XIN Dan, GU Chun-xiang, ZHENG Yong-hui, GUANG Yan, KANG Yuan-ji. Identity-based fully homomorphic encryption from ring learning with errors problem[J]. Acta Electronica Sinica, 2016, 44(12): 2887-2893. (in Chinese)

[15] CHEN H, YUPU H, LIAN Z. Double batch for RLWE-based leveled fully homomorphic encryption[J]. Chinese Journal of Electronics, 2015, 24(3): 661-666.

[16] HOFFSTEIN J, PIPHER J, SILVERMAN J H. NTRU: a ring-based public key cryptosystem[A]. Proceedings of the 3rd International Symposium on Algorithmic Number Theory[C]. Berlin: Springer, 1998. 267-288.

[17] 杨铭,曹云飞. NTRU 的应用前景分析及展望[J]. 信息安全与通信保密, 2007, (8): 36-38.
YANG Ming, CAO Yun-fei. Application prospect and analysis of NTRU[J]. Information Security and Communications Privacy, 2007, (8): 36-38. (in Chinese)

[18] TROMER E, VAIKUNTANATHAN V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption[A]. Proceedings of Forty-Fourth ACM Symposium on Theory of Computing[C]. New York, ACM, 2012. 1219-1234.

[19] GENTRY C, SAHAI A, WATERS B. Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based[M]. Berlin: Springer, 2013. 75-92.

[20] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[A]. Proceedings of DBLP[C]. Germany: DBLP, 2008. 197 – 206.

[21] LYUBASHEVSHY V, PEIKERT C, REGEV O. On ideal lattice and learning with errors over rings[A]. Proceedings of Eurocrypt 2010[C]. New York: Springer-Verlag, 2010. 1 – 23.

[22] 张建航, 贺健, 胡予濮. 基于 R-LWE 问题的新型 NTRU 加密方案[J]. 电子科技, 2012, 25(5): 76 – 78.
ZHANG Jian-hang, HE Jian, HU Yu-pu. A novel NTRU encryption scheme based on R-LWE problem[J]. Electronic Science and Technology, 2012, 25(5): 76 – 78. (in Chinese)

[23] STEINFELD R. Making NTRU as secure as worst-case problems over ideal lattices[A]. Proceedings of International Conference on Theory and Applications of Cryptographic Techniques: Advances in Cryptology[C]. New York: Springer-Verlag, 2011. 27 – 47.

作者简介

李子臣 男, 1965 年 9 月出生, 河南焦作人. 现为北京印刷学院教授. 研究领域为公钥密码学、同态加密.
E-mail: lizichen@bigc.edu.cn

张卷美(通信作者) 女, 1963 年 3 月出生, 河南新乡人. 现为北京电子科技学院副教授. 研究方向为密码计算方法、同态密码.
E-mail: zhangjm@besti.edu.cn

杨亚涛(通信作者) 男, 1978 年 2 月出生, 河南平顶山人. 现为北京电子科技学院副教授, 研究方向为密码学与信息安全、无线通信安全.
E – mail: yy2008@163.com

张峰娟 女, 1992 年 1 月出生, 河南濮阳人. 2017 年毕业于西安电子科技大学, 获得硕士学位. 研究方向为密码学、信息安全、同态密码.
E-mail: 1185238590@qq.com