FINAL全同态加密方案盲旋转优化技术

赵秀凤，吴蒙，宋巍涛
（网络空间部队信息工程大学密码工程学院，河南 郑州 450001）

摘　要：针对密文同态计算的盲旋转密钥规模过大的问题，引入了环自同构技术，对基于MNTRU的FINAL全同态加密方案进行优化，提出新的盲旋转算法。该算法的盲旋转密钥规模减小为原来的50%，盲旋转产生的噪声减少为原来的55%。在此基础上，利用动态调整分解基技术，对该算法的参数进行优化。最终，优化后的盲旋转算法在计算代价增加约7%的情况下，盲旋转密钥规模优化67%。

关键词：全同态加密；自举；盲旋转
中图分类号：TP309.7
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025213

Blind rotation optimization technique for the FINAL fully homomorphic encryption scheme

ZHAO Xiufeng, WU Meng, SONG Weitao
School of Cryptographic Engineering, Cyberspace Force Information Engineering University, Zhengzhou 450001, China

Abstract: To address the issue of excessive blind rotation key size in ciphertext homomorphic evaluations, ring automorphism techniques were introduced to optimize the MNTRU-based FINAL fully homomorphic encryption scheme, and a new blind rotation algorithm was proposed. The blind rotation key size was reduced by 50% and the noise generated by blind rotation was cut by 55%. Furthermore, the parameters of the algorithm were optimized via the employment of dynamic adjustment of decomposition bases.Ultimately, the optimized blind rotation algorithm achieves a 67% reduction in key size with only a 7% increase in computational cost.

Keywords: fully homomorphic encryption, bootstrapping, blind rotation

0　引言

随着大数据、云计算时代的到来，数据安全与隐私保护问题日益凸显。传统的加密手段只能保证数据在通信以及存储时是安全的，并不能保证在计算时的安全性，而全同态加密能够保证数据全生命周期的安全性，其在云计算、隐私计算等领域均存在着广泛的应用需求。全同态加密目前的实现路径主要基于自举。FHEW[1]全同态加密方案的自举通常由盲旋转、模转换和密钥转换3个模块组成。其中，盲旋转操作在整个密文同态计算时钟周期的占比最大。全同态加密技术在实际应用中的主要瓶颈在于自举的高昂计算开销。

FHEW全同态加密方案及其TFHE[2]变体是对加密数据进行同态布尔运算的主要方法。2022年，亚密会提出FINAL[3]全同态加密方案，作为TFHE变体的一种，其自举采用NGS加密方案，与TFHE方案相比，自举速度快28%，自举密钥以及密钥转换密钥的尺寸减小45%。

收稿日期：2025–09–12；**修回日期：**2025–11–14
通信作者：赵秀凤，zhao_xiu_feng@163.com
基金项目：国家密码科学基金资助项目（No.2025NCSF02044）
Foundation Item：The National Cryptologic Science Fund of China (No.2025NCSF02044)

FHEW 类全同态加密方案[1-4]的自举采用两种方法：AP[5]自举方法和 GINX[6]方法。两种自举方法的性能依赖密钥分布：AP/FHEW[1,5]适用于高斯/均匀分布密钥，GINX/TFHE[2,6]在密钥空间为二进制或三元时表现更好。2022 年，Bonte 等[3]提出 FINAL 方案，其自举 NGS 方案是基于 NTRU 问题的 GSW 变体，自举效率优于 TFHE 方案。同年，Kluczniak[7]提出了一种基于 NTRU 的 TFHE 变体全同态加密方案 NTRU-ν-um，支持对有限域上的任何函数进行同态计算且在效率上优于 TFHE 方案。2023 年，Lee 等[8]在 TFHE 方案上提出密钥分块技术以及密钥复用技术，分别对自举的盲旋转算法以及密钥转换算法进行了优化，在相同的安全级别下，TFHE 自举的执行时间以及自举密钥尺寸得到了优化。2023 年欧密会，Lee 等[9]还利用环自同构技术进行盲旋转，进而提出了一种针对 FHEW 类全同态加密方案的新自举，该自举兼具 AP、GINX 两种自举方法的最佳特性：在不额外增加运行时间成本的情况下支持任意密钥分布，同时使用较小的评估密钥。FHEW 类全同态加密方案由两层框架构成，第一层为容错学习（LWE, learning with error）加密方案，第二层为 GSW 加密方案。2023 年美密会，Xiang 等[10]同样利用环自同构技术构建了具有快速自举算法的全同态加密方案，与 Lee 等[9]提出的方案第二层加密为基于 RLWE 的类 GSW 方案的不同在于，Xiang 等[10]提出的方案第二层加密为基于 NTRU 的类 GSW 方案，评估密钥尺寸优化为 Lee 等方案的约 $\frac{1}{3}$，计算效率提升约 3 倍。2024 年，Wang 等[11]提出新型稀疏同构，改进了 LMKC+盲旋转算法[9]，将自同构次数减少 10.4%~26.4%。

基于 MNTRU 的 FINAL 全同态加密方案（第一层为 MNTRU 加密方案，第二层为 NGS 加密方案）的密钥采用三元密钥，通过引入环自同构技术，对 FINAL 全同态加密方案的盲旋转进行优化。本文主要工作如下。

1) 引入了环自同构以及密钥转换对 FINAL 盲旋转进行优化，给出了 NGS 密文的自同构以及密钥转换，并将其应用于 FINAL 盲旋转，提出了密文经过模转换后分量都为奇数情况下核心的盲旋转算法。

2) 结合核心的盲旋转算法，给出普适性的存储高效的盲旋转优化算法，即不限制密文的条件，且评估密钥规模减小。

3) 引入动态调整分解基技术，对存储高效的盲旋转算法进行优化，并与原 FINAL 盲旋转算法进行性能对比分析。优化后的盲旋转算法在计算代价增加约 7% 的情况下，盲旋转密钥规模优化约 67%。

1 背景知识

1.1 全同态加密

全同态加密的关键在于密文同态运算，即明文的计算结果与加密后密文的计算并解密后的结果等价。

一个同态加密方案包含 4 个算法：密钥生成算法、加密算法、解密算法和评估算法。

KeyGen(λ)：输入安全参数 λ，输出公钥 pk、用于密文计算的评估密钥 evk 和私钥 sk，其中，评估密钥 evk 包括盲旋转密钥以及密钥转换密钥。

Enc(pk,m)：给定 $m\in\{0,1\}$，使用公钥对消息 m 进行加密，并输出密文 c。

Dec(sk,c)：使用私钥 sk 对密文 c 进行解密，以恢复消息 m。

Eval$(\mathrm{evk},F,c_1,\cdots,c_l)$：使用评估密钥 evk，输入 $c_1,\cdots,c_l$ 和功能函数 F，其中 $F\colon\{0,1\}^l\to\{0,1\}$，并输出密文 c。

1.2 NTRU 问题

设 $N>0$，$Q>1$ 是整数，$R:=\mathbb{Z}[X]/<X^N+1>$，$R_Q:=\mathbb{Z}_Q[X]/<X^N+1>$，实数 $\sigma>0$。定义 NTRU 分布为 $h=g\cdot f^{-1}\bmod Q$，其中，$g,f\leftarrow\chi_\sigma^N$ 且 f 在 R_Q 上是可逆的，χ_σ 是均值为 0、方差为 σ^2 的高斯分布。

(n,q,σ)-NTRU 计算问题是在给定 h 的情况下，恢复 f 和 g。

(n,q,σ)-NTRU 判定问题是区分 NTRU 分布和 R_Q 上的均匀随机分布[12]。

1.3 MNTRU 基本加密方案

MNTRU 基本加密方案[3]包含 5 个算法，具体描述如下。

MNTRU.ParamGen(1^λ)：输入安全参数 λ，输出 (n,q,σ)。

MNTRU.KeyGen：采样 $\boldsymbol{F}\leftarrow\chi_\sigma^{n\times n}$，且 $\boldsymbol{F}^{-1}$ 存在。密钥 sk: $=\boldsymbol{F}$，evk: $=\left(\boldsymbol{g}_{\mathrm{MNTRU}}+\lfloor\frac{5\cdot q}{8}\rceil\cdot(1,\boldsymbol{0})\right)\cdot$

$\boldsymbol{F}^{-1} \in \mathbb{Z}_q^n$，其中，$\boldsymbol{g}_{\text{MNTRU}} \leftarrow \chi_\sigma^n$，$\lfloor \rceil$为四舍五入符号。输出(evk,sk)。

MNTRU.Enc(m,sk)：输入明文m、密钥sk，输出密文 $\boldsymbol{c} = \left(\boldsymbol{g}_{\text{MNTRU}} + \Delta \cdot (m,\boldsymbol{0})\right) \cdot \boldsymbol{F}^{-1} \in \mathbb{Z}_q^n$，其中 $m \in \{0,1\}$，$\boldsymbol{g}_{\text{MNTRU}} \leftarrow \chi_\sigma^n$，$\Delta = \lfloor \frac{q}{4} \rceil$。

MNTRU.Dec($\boldsymbol{c}$,sk)：输入密文c、密钥sk，其中密文 $\boldsymbol{c} = \left(\boldsymbol{g}_{\text{MNTRU}} + \lfloor \frac{q}{2} \rceil \cdot (m,\boldsymbol{0})\right) \cdot \boldsymbol{F}^{-1} \in \mathbb{Z}_q^n$。计算$r = \boldsymbol{c} \cdot \text{col}_0(\boldsymbol{F}) \bmod q$，输出$\lfloor \frac{2r}{q} \rceil \bmod 2$。

MNTRU.Nand($\boldsymbol{c}_0$,$\boldsymbol{c}_1$,evk)：输入公钥evk以及两个形式为 $\left(\boldsymbol{g}_{\text{MNTRU}} + \lfloor \frac{q}{4} \rceil \cdot (m_i,\boldsymbol{0})\right) \cdot \boldsymbol{F}^{-1} \in \mathbb{Z}_q^n$ 的密文$\boldsymbol{c}_0$和$\boldsymbol{c}_1$，输出$\boldsymbol{c}_{\text{NAND}}$: = evk − $\boldsymbol{c}_0$ − $\boldsymbol{c}_1$。

1.4 NGS加密方案

NGS方案[3]是基于NTRU的GSW类方案，与GSW方案一样具有准加性噪声增长，被用作自举的累加器。NGS加密方案具有两个加密函数，一个加密的明文是R_Q上的三元多项式，另一个加密的明文是R_Q上的向量。为了简化噪声分析，该方案假设所有向量密文加密的消息都属于单项式集 $\mathbb{M} = \{\pm b \cdot X^k : b \in \{0,1\}, k \in \mathbb{N}\}$。

1.4.1 算法描述

NGS.ParamGen(1^λ)：输入安全参数λ，输出(N,Q,σ,B,l)，其中B是分解密文的分解基，$l = \log_B Q$。

NGS.KeyGen：输出sk: = $f = 1 + 4 \cdot f'$，设$f = 1 + 4 \cdot f'$，其中$f' \leftarrow \chi_\sigma^N$且$f^{-1}$在$R_Q$中存在。

NGS.EncS(m,sk)：输入(m,sk)，输出$c = g_{\text{NGS}} \cdot f^{-1} + \Delta \cdot m \in R_Q$，其中$m$是待加密的三元多项式明文，$g_{\text{NGS}} \leftarrow \chi_\sigma^N$，$\Delta = \lfloor \frac{Q}{4} \rceil$，$c$为$m$的NGS标量密文。

NGS.EncVec(m,sk)：输入(m,sk)，$m \in \mathbb{M}$。定义$\boldsymbol{g}_{\text{NGS}} = (g_0,\cdots,g_{l-1})$，$\mathfrak{g} = (B^0,\cdots,B^{l-1})$，其中，$g_i \leftarrow \chi_\sigma^N$ $(0 \leqslant i \leqslant l-1)$。输出 $\boldsymbol{c} = g_{\text{NGS}} \cdot f^{-1} + \mathfrak{g} \cdot m \in R_Q^\ell$，$\boldsymbol{c}$为$m$的NGS向量密文。

1.4.2 外积

设标量密文为$c = g_{\text{NGS}} \cdot f^{-1} + \Delta \cdot u \in R_Q$，向量密文为$\boldsymbol{c} = g_{\text{NGS}} \cdot f^{-1} + \mathfrak{g} \cdot v \in R_Q^\ell$，其中，$\mu$是一个三元多项式，$v \in \mathbb{M}$是一个单项式，定义$c$和$\boldsymbol{c}$的外积为

$$c \otimes \boldsymbol{c} = \left(\mathfrak{g}^{-1}(c) \cdot \boldsymbol{g}_{\text{NGS}} + g_{\text{NGS}} \cdot v \cdot f^{-1}\right) + \Delta \cdot \mu \cdot v \tag{1}$$

1.4.3 噪声分析

定义1 标量密文的噪声。设标量密文为$c = g_{\text{NGS}} \cdot f^{-1} + \Delta \cdot m \in R_Q$，定义$c$的噪声为$\text{err}(c) = c \cdot f - \Delta \cdot m \in R_Q$。

定义2 向量密文的噪声。设向量密文为$\boldsymbol{c} = g_{\text{NGS}} \cdot f^{-1} + \mathfrak{g} \cdot m \in R_Q^\ell$，定义$\boldsymbol{c}$的噪声为$\text{err}(\boldsymbol{c}) = \boldsymbol{c} \cdot f - \mathfrak{g} \cdot m \cdot f \in R_Q$，将其视为系数在$[-\frac{Q}{2},\frac{Q}{2}]$中的$\mathbb{Z}[X]$上的多项式。

引理1 标量密文的噪声。设标量密文为$c = g_{\text{NGS}} \cdot f^{-1} + \Delta \cdot m \in R_Q$，若$m$是形如$\pm b \cdot X^k$的单项式（其中$b \in \{0,1\}$），则

$$\text{Var}(\text{err}(c)) \leqslant \text{Var}(g_{\text{NGS}}) + 4 \cdot \sigma^2 \tag{2}$$

若m是$N-1$次的三元多项式，则

$$\text{Var}(\text{err}(c)) \leqslant \text{Var}(g_{\text{NGS}}) + 4 \cdot N \cdot \sigma^2 \tag{3}$$

引理2 向量密文的噪声。设向量密文为$\boldsymbol{c} = g_{\text{NGS}} \cdot f^{-1} + \mathfrak{g} \cdot m \in R_Q^\ell$，则

$$\text{err}(\boldsymbol{c}) = (g_{\text{NGS}} \cdot f^{-1} + \mathfrak{g} \cdot m) \cdot f - \mathfrak{g} \cdot m \cdot f = \boldsymbol{g}_{\text{NGS}} \tag{4}$$

即

$$\text{Var}(\text{err}(\boldsymbol{c})) = \sigma_{g_{\text{NGS}}}^2 \tag{5}$$

引理3 外积的噪声。设标量密文为$c = g_{\text{NGS}} \cdot f^{-1} + \Delta \cdot m \in R_Q$，向量密文为$\boldsymbol{c} = g_{\text{NGS}} \cdot f^{-1} + \mathfrak{g} \cdot v \in R_Q^\ell$，$v \in \mathbb{M}$，定义$c_{\text{mult}} = c \otimes \boldsymbol{c}$，则

$$\begin{aligned}&\text{Var}(\text{err}(c_{\text{mult}})) \leqslant N \cdot \ell \cdot \gamma^2 \cdot \text{Var}(\boldsymbol{g}_{\text{NGS}}) + \\ &\|v\|_2^2 \cdot \text{Var}(g_{\text{NGS}}) + 4 \cdot \sigma^2 \leqslant \\ &N \cdot \ell \cdot B^2 \cdot \text{Var}(\text{err}(\boldsymbol{c})) + \text{Var}(c)\end{aligned} \tag{6}$$

引理4 连续外积的噪声。设标量密文$c = g_{\text{NGS}} \cdot f^{-1} + \Delta \cdot m \in R_Q$（$m$是一个三元多项式），向量密文$\boldsymbol{c}_i = \boldsymbol{g}_{\text{NGS},i} \cdot f^{-1} + \mathfrak{g} \cdot m_i \in R_Q^\ell$，$m_i \in \mathbb{M}$。若 $c' = c \otimes \prod_{i=1}^k \boldsymbol{c}_i$，则有

$$\begin{aligned}&\text{Var}(\text{err}(c')) \leqslant \\ &N \cdot \ell \cdot \gamma^2 \cdot \sum_{i=1}^k \text{Var}(\boldsymbol{c}_i) + \text{Var}(\text{err}(c)) \leqslant \\ &N \cdot \ell \cdot \gamma^2 \cdot \sum_{i=1}^k \text{Var}(\boldsymbol{g}_{\text{NGS},i}) + \text{Var}(g) + 4 \cdot \sigma^2\end{aligned} \tag{7}$$

1.5 基于环自同构的核心盲旋转算法

文献[9]针对LWE基本加密方案给出了利用自同构的核心盲旋转算法。设LWE密文$c = (\boldsymbol{a},b = -$

$<\boldsymbol{a},\boldsymbol{s}>+e+m$)，盲旋转算法的目标是将累加器旋转$X^{<\boldsymbol{a},\boldsymbol{s}>}$，其中$<\boldsymbol{a},\boldsymbol{s}>$对$2N$取模。核心盲旋转算法中，模转换后的$a_i$为奇数。对于$N\geqslant 8$，群$\mathbb{Z}_{2N}^*$与$\mathbb{Z}_{N/2}\otimes\mathbb{Z}_2$同构，其生成元为$\{\vartheta,-1\}$（如$\vartheta=5$），且每个$t\in\mathbb{Z}_{2N}^*$都可以表示为$\pm\vartheta^k$的形式，$t\in\mathbb{Z}_{\frac{N}{2}}$。设$a_i=\pm\vartheta^{k_i}(\mathrm{mod}2N),i=0,\cdots,n-1$，定义$I_\ell^+=\{i{:}a_i=\vartheta^\ell\}$和$I_\ell^-=\{i{:}a_i=-\vartheta^\ell\}$，其中$\ell\in[0,\frac{N}{2}-1]$。利用$\vartheta^{\frac{N}{2}}=1(\mathrm{mod}2N)$，可以得到以下分解

$$\begin{aligned}\langle\boldsymbol{a},\boldsymbol{s}\rangle=&\sum_{j\in I_0^+}s_j+\cdots+\vartheta\cdot\\&(\sum_{j\in I_{\frac{N}{2}-1}^+}s_j-\vartheta\cdot(\sum_{j\in I_0^-}s_j+\cdots+\\&\vartheta\cdot(\sum_{j\in I_{\frac{N}{2}-1}^-}s_j)))(\mathrm{mod}\,2N)\end{aligned}\tag{8}$$

定义$\mathrm{brk}_j:=\mathrm{RGSW}_z(X^{s_j})$。给定初始密文$\mathrm{ACC}=\mathrm{RLWE}_z^0(f'(X))$，首先将其与所有$j\in I_{\frac{N}{2}-1}^-$对应的$\mathrm{brk}_j$相乘，并对ACC应用自同构$\mathrm{Auto}_\vartheta$，得到

$$\mathrm{ACC}=\mathrm{RLWE}_z\left(f'\left(X^\vartheta\right)\cdot X^{\vartheta\cdot\sum\limits_{j\in I_{\frac{N}{2}-1}^-}f_j}\right)\tag{9}$$

然后，将累加器与$j\in I_{\frac{N}{2}-2}^-$对应的brk_j相乘，并再次对ACC应用自同构Auto_ϑ。对I_ℓ^+和I_ℓ^-重复此过程，$\ell=0,\cdots,\frac{N}{2}-1$。需要注意的是，在第$\frac{N}{2}$步（即与$I_0^-$对应的$\mathrm{brk}_j$相乘之后），应用自同构$\mathrm{Auto}_{-\vartheta}$，且（为了减少运算）跳过了与$I_0^+$的乘法。最后结果为

$$\mathrm{ACC}=\mathrm{RLWE}_z\left(f'\left(X^{-\vartheta^{\frac{N}{2}-1}}\right)\cdot X^{\sum_i a_i\cdot s_i}\right)\tag{10}$$

设$f'(X)=f(X^{-\vartheta})\cdot X^{-\vartheta b}$，则结果变为$\mathrm{ACC}=\mathrm{RLWE}_z\left(f(X)\cdot X^{\beta+<\boldsymbol{a},\boldsymbol{s}>}\right)$。

2 NGS密文的环自同构技术

基于FHEW方案的盲旋转算法[9]，本节给出了NGS密文的环自同构算法及其用到的密钥转换算法。

根据定义1可知，NGS标量密文$c_1=g_{\mathrm{NGS}}\cdot f_1^{-1}+\Delta\cdot m\in R_Q$的噪声为

$$\mathrm{err}(c_1)=c_1\cdot f_1-\Delta\cdot m=g_{\mathrm{NGS}}+4\varepsilon m f_1'\in R_Q$$

其中，$\Delta=\frac{Q}{4}+\varepsilon$，$|\varepsilon|\leqslant\frac{1}{2}$。

KeySwitchGen(f_1,f)：输入待转换的密钥f_1以及目标密钥f，输出密钥转换密钥

$$\begin{aligned}&\mathrm{ksk}:=\mathrm{NGS.EncVec}\left(f_1,f_2\right)=\\&g_{\mathrm{NGS}}\cdot f_2^{-1}+\mathfrak{g}\cdot f_1\in R_Q^l\end{aligned}\tag{11}$$

KeySwitch$_{f_1\to f_2}(c_1,\mathrm{ksk})$：输入NGS标量密文$c_1=g\cdot f_1^{-1}+\Delta\cdot m\in R_Q$，密钥转换密钥ksk，输出

$$\begin{aligned}&c_1\otimes\mathrm{ksk}=\mathfrak{g}^{-1}(c_1)\cdot\mathrm{ksk}=\\&(g^{-1}(c_1)\cdot\boldsymbol{g}_{\mathrm{NGS}})\cdot f_2^{-1}+c_1\cdot f_1=\\&(g^{-1}(c_1)\cdot\boldsymbol{g}_{\mathrm{NGS}}+\mathrm{err}(c_1)\cdot f_2)\cdot f_2^{-1}+\Delta\cdot m=\\&\mathrm{NGS.EncS}\left(m,f_2\right)=c_1'\end{aligned}\tag{12}$$

NGS密文下的密钥转换的噪声分析如下。

令$g_{\mathrm{mult}}=(\mathfrak{g}^{-1}(c_1)\cdot\boldsymbol{g}_{\mathrm{NGS}}+\mathrm{err}(c_1)\cdot f_2)$，由引理1标量密文的噪声可得，$c_1\otimes\mathrm{ksk}$外积的噪声为

$$\mathrm{Var}(\mathrm{err}(c_{\mathrm{mult}}=c_1\otimes\mathrm{ksk}))\leqslant\mathrm{Var}(g_{\mathrm{mult}})+4\cdot\sigma^2\tag{13}$$

$g_{\mathrm{mult}}=(\mathfrak{g}^{-1}(c_1)\cdot\boldsymbol{g}_{\mathrm{NGS}}+\mathrm{err}(c_1)\cdot f_2)$的噪声为

$$\mathrm{Var}(\mathrm{err}(g_{\mathrm{mult}}))\leqslant\mathrm{Var}(\mathfrak{g}^{-1}(c_1)\cdot\boldsymbol{g})+\mathrm{Var}(\mathrm{err}(c_1)\cdot f_2)\tag{14}$$

结合1.4.3节噪声分析可得

$$\begin{aligned}&\mathrm{Var}(\mathrm{err}(c_{\mathrm{mult}}=c_1\otimes\mathrm{ksk}))\leqslant\\&N\cdot\ell\cdot\gamma^2\cdot\mathrm{Var}(\mathrm{ksk})+\\&16\cdot N\cdot\sigma^2\cdot\mathrm{Var}(\mathrm{err}(c_1))+4\cdot\sigma^2\end{aligned}\tag{15}$$

与原FINAL盲旋转方案外积噪声$\mathrm{Var}(\mathrm{err}(c_{\mathrm{mult}}=c\otimes\boldsymbol{c}))\leqslant N\cdot\ell\cdot\gamma^2\cdot\mathrm{Var}(\mathrm{err}(\boldsymbol{c}))+\mathrm{Var}(c)$相比较，式(15)噪声增长较大。因此，FINAL方案中的原NGS加密方案与环自同构技术不适配，为解决此问题，本文引入文献[10]的基于NTRU的类GSW方案，给出NGS密文的环自同构算法以及相关的密钥转换算法。

2.1 NGS密文下的密钥转换

引入文献[10]的基于NTRU的类GSW方案，即改进NGS标量密文的形式为

$$c_1=g_{\mathrm{NGS}}\cdot f_1^{-1}+\Delta\cdot m\cdot f_1^{-1}\in R_Q\tag{16}$$

该密文形式可视为加密了密钥相关消息$m\cdot f_1^{-1}$的原NGS密文。NGS标量密文形式修改后，噪声分析如下。

标量密文噪声的方差为

$$\mathrm{err}(c)=c\cdot f-\Delta\cdot m=g_{\mathrm{NGS}}\in R_Q\tag{17}$$

标量密文c与向量密文$\boldsymbol{c}=\boldsymbol{g}_{\mathrm{NGS}}\cdot f^{-1}+\mathfrak{g}\cdot$

$v \in R_Q^l, v \in \mathbb{M}$的外积为

$$c_{\text{mult}} = (\mathfrak{g}^{-1}(c_1) \cdot \boldsymbol{g}_{\text{NGS}} + g_{\text{NGS}} \cdot v) \cdot f^{-1} + \Delta \cdot m \cdot v \cdot f^{-1} \tag{18}$$

外积的噪声方差为

$$\begin{aligned} &\text{Var}(\text{err}(c_{\text{mult}})) = \\ &\text{Var}(\text{err}(\mathfrak{g}^{-1}(c_1) \cdot \boldsymbol{g}_{\text{NGS}} + g_{\text{NGS}} \cdot v)) \leqslant \\ &N \cdot \ell \cdot \gamma^2 \cdot \text{Var}(\text{err}(\boldsymbol{c})) + \text{Var}(c) \end{aligned} \tag{19}$$

NGS密文的密钥转换算法定义如下。

KeySwitchGen$(f_1 \cdot f^{-1}, f)$：输入$f_1 \cdot f^{-1}$和f，其中，f_1为待转换的密钥，f为目标密钥，输出密钥转换密钥

$$\begin{aligned} &\text{ksk} := \text{NGS.EncVec}(f_1, f) = \\ &\boldsymbol{g}_{\text{NGS}} \cdot f^{-1} + g \cdot f_1 \cdot f^{-1} \in R_Q^l \end{aligned} \tag{20}$$

KeySwitch$_{f_1 \to f}(c_1, \text{ksk})$：输入NGS标量密文$c_1 = \boldsymbol{g}_{\text{NGS}} \cdot f^{-1} + \Delta \cdot m \cdot f_1^{-1} \in R_Q$和密钥转换密钥ksk，输出

$$\begin{aligned} &c_1 \otimes \text{ksk} = \mathfrak{g}^{-1}(c_1) \cdot \text{ksk} = \\ &(\mathfrak{g}^{-1}(c_1) \cdot \boldsymbol{g}_{\text{NGS}}) \cdot f^{-1} + c_1 \cdot f_1 \cdot f^{-1} = \\ &(\mathfrak{g}^{-1}(c_1) \cdot \boldsymbol{g}_{\text{NGS}} + g) \cdot f^{-1} + \Delta \cdot m \cdot f^{-1} = \\ &\text{NGS.EncS}(m, f) \end{aligned} \tag{21}$$

密钥转换算法的噪声方差为

$$\begin{aligned} &\text{Var}(\text{err}(c_{\text{mult}} = c_1 \otimes \text{ksk})) = \\ &\text{Var}(\text{err}(\mathfrak{g}^{-1}(c_1) \cdot \boldsymbol{g}_{\text{NGS}} + g_{\text{NGS}})) \leqslant \\ &N \cdot \ell \cdot \gamma^2 \cdot \text{Var}(\text{err}(\text{ksk})) + \text{Var}(c) \end{aligned} \tag{22}$$

该方差与密钥相同情况下的标量密文和向量密文外积产生噪声的方差相同。因此，连续外积的噪声方差同样相同。

根据引理4，若$c' = c \otimes \overset{k}{}_{i=1} \boldsymbol{c}_i$，则连续外积的噪声方差为

$$\begin{aligned} &\text{Var}(\text{err}(c')) \leqslant \\ &N \cdot \ell \cdot \gamma^2 \cdot \sum_{i=1}^{k} \text{Var}(\boldsymbol{c}_i) + \text{Var}(\text{err}(c)) \leqslant \\ &N \cdot \ell \cdot \gamma^2 \cdot \sum_{i=1}^{k} \text{Var}(\boldsymbol{g}_{\text{NGS},i}) + \text{Var}(g_{\text{NGS}}) \end{aligned} \tag{23}$$

2.2 NGS密文下的环自同构

定义R上的自同构映射$\psi_t: c(X) \to c(X^t)$，$t \in \mathbb{Z}_{2N}^*$。

Auto$_t$(NGS.Enc$_f(m)$, ak$_t$)：输入密钥f加密下的NGS标量密文NGS.Enc$_f(m(X)) = c(X)$以及转换密钥 ak$_t$ = NGS.EncVec$(f(X^t) \cdot f(X)^{-1}, f(X))$，对$c(X)$应用自同构映射$\Psi_t$得到$c(X^t)$，其中$c(X^t)$是明文$m(X^t)$在密钥$f(X^t)$加密下的NGS标量密文。然后应用密钥转换KeySwitch$_{f(X^t) \to f(X)}(c(X^t), \text{ksk})$，最后输出明文$m(X^t)$在密钥$f(X)$加密下的NGS标量密文。

3 基于环自同构的盲旋转优化算法

本节给出了基于MNTRU的FINAL全同态加密方案的盲旋转优化算法，该算法通过一系列NGS.EncS ⊗ NGS.EncVec外积更新累加器。NGS.EncS密文存储着累加器ACC的值，NGS.EncVec密文为盲旋转密钥brk$_i$，加密的明文信息为MNTRU密钥f_i。

与原FINAL方案的盲旋转算法不同，本节提出的优化算法不是通过一系列ACC与CMux门的外积来替代累加器指数上的乘法，而是使用了环自同构ψ_t及其相关的转换密钥ak$_t$。

首先给出核心的盲旋转算法，该算法用于基于MNTRU的FINAL全同态加密方案且所有c_i均为奇数的特定场景，这是因为环自同构ψ_t在t为奇数时才具有数学意义。然后，对核心的盲旋转算法进行优化，提出普适的优化盲旋转算法。

3.1 核心的盲旋转算法

基于MNTRU基本加密方案的核心盲旋转算法的目标是将累加器旋转$X^{\boldsymbol{c} \cdot \text{col}_0(\boldsymbol{F})}$，其中$\boldsymbol{c} \cdot \text{col}_0(\boldsymbol{F})$对$2N$取模，$\text{col}_0(\boldsymbol{F}) = (f_0, f_1, \cdots, f_{n-1})$。$\boldsymbol{c} \cdot \text{col}_0(\boldsymbol{F})$可以分解为

$$\begin{aligned} &\boldsymbol{c} \cdot \text{col}_0(\boldsymbol{F}) = \sum_{j \in I_0^+} f_j + \cdots + \vartheta \cdot \\ &(\sum_{j \in I_{\frac{N}{2}-1}^+} f_j - \vartheta \cdot (\sum_{j \in I_0^-} f_j + \cdots + \\ &\vartheta \cdot (\sum_{j \in I_{\frac{N}{2}-1}^-} f_j))) \, (\text{mod}\, 2N) \end{aligned} \tag{24}$$

定义brk$_j$: = NGS.EncVec(X^{f_j})。给定初始密文ACC = NGS.EncS$(f'(X))$，首先将其与所有$j \in I_{\frac{N}{2}-1}^-$对应的brk$_j$相乘，再对ACC应用自同构Auto$_\vartheta$，得到

$$\text{ACC} = \text{NGS.EncS}\left(f'(X^\vartheta) \cdot X^{\vartheta \cdot \sum\limits_{j \in I_{\frac{N}{2}-1}^-} f_j}\right) \tag{25}$$

然后，将累加器与$j \in I_{\frac{N}{2}-2}^{-}$对应的$\mathrm{brk}_j$相乘，并再次对ACC应用自同构$\mathrm{Auto}_{\vartheta}$。对$I_{\ell}^{+}$和$I_{\ell}^{-}$重复此过程，$\ell = 0,\cdots,\frac{N}{2}-1$。需要注意的是，在第$\frac{N}{2}$步（即与$I_0^{-}$对应的$\mathrm{brk}_j$相乘之后），应用自同构$\mathrm{Auto}_{-\vartheta}$，且（为了减少运算）跳过了与$I_0^{+}$的乘法。最后结果为

$$\mathrm{ACC} = \mathrm{NGS.EncS}\left(f'\left(X^{-\vartheta^{\frac{N}{2}-1}}\right)\cdot X^{\boldsymbol{c}\cdot \mathrm{col}_0(\boldsymbol{F})}\right) \tag{26}$$

设$f'(X) = f\left(X^{-\vartheta}\right)$，则结果变为

$$\mathrm{ACC} = \mathrm{NGS.EncS}\left(\left\lfloor\frac{Q}{8}\right\rceil\cdot X^{\frac{N}{2}}\cdot\sum_{i=0}^{N-1}X^i\cdot X^{\boldsymbol{c}\cdot \mathrm{col}_0(\boldsymbol{F})}\right) = \mathrm{NGS.EncS}\left(f(X)\cdot X^{\boldsymbol{c}\cdot \mathrm{col}_0(\boldsymbol{F})}\right) \tag{27}$$

计算过程中需要n个自举密钥brk_i（$i \in [0,n-1]$）和两个自同构密钥ak_{ϑ}、$\mathrm{ak}_{-\vartheta}$。优化的盲旋转算法包括两种类型的同态运算，即NGS.EncS ⊗ NGS.EncVec的外积运算以及自同构运算，其中，NGS.EncS ⊗ NGS.EncVec外积运算的数量为n，自同构运算的数量为$N-1$。由于存在一部分$I_{\ell}^{\pm}$为空集，因此可以通过将这部分之间的自同构由多个自同构ak_{ϑ}组合替换为单个自同构$\mathrm{ak}_{\vartheta^u}$，减少自同构次数。存储方面则需要额外存储所有$u$可能值对应的自同构密钥$\mathrm{ak}_{\vartheta^u}$，为了提高存储效率，可以仅存储少量的$\{\mathrm{ak}_{\vartheta^u}\}_{u\in[1,w]}$，其中$w$为窗口大小。具体算法描述如算法1所示。

算法1 核心的盲旋转算法（$\boldsymbol{c}_i$为奇数）

$\mathrm{BlindRotateCore}(\mathrm{ACC},\mathrm{ct},\{\mathrm{brk}_i\}_{0\leqslant i\leqslant n-1},\left\{\mathrm{ak}_{\vartheta^u}\right\}_{u\in[1,w]},\mathrm{ak}_{-\vartheta})$

输入 MNTRU基本加密方案的密文$\mathrm{ct} = (c_0,\cdots,c_n)\in\mathbb{Z}_q^n$，加密的明文$m\in\{0,1\}$；初始化的累加器ACC；盲旋转密钥$\{\mathrm{brk}_i\}_{0\leqslant i\leqslant n-1}$，其中$\mathrm{brk}_j := \mathrm{NGS.EncVec}\left(X^{f_j}\right)\in R_{Q,N}^{\ell}$；自同构的转换密钥$\{\mathrm{ak}_{\vartheta^u}\}_{u\in[1,w]},\mathrm{ak}_{-\vartheta}$

输出 $\mathrm{NGS.EncS}\left(f(X)\cdot X^{\boldsymbol{c}\cdot \mathrm{col}_0(\boldsymbol{F})}\right)$，即累加器旋转$X^{\boldsymbol{c}\cdot \mathrm{col}_0(\boldsymbol{F})}$，$\boldsymbol{c}\cdot\mathrm{col}_0(\boldsymbol{F})$对$2N$取模

1) $(c_0,\cdots,c_{n-1})\leftarrow\left\lfloor\frac{2\cdot N\cdot \mathbf{ct}}{q}\right\rceil$，其中$c_i$为奇数

2) 初始化$\mathrm{ACC}\leftarrow\left\lfloor\frac{Q}{8}\right\rceil\cdot X^{\frac{N}{2}}\cdot\sum_{i=0}^{N-1}X^i$

3) $v\leftarrow 0$

4) 对于ℓ从$\frac{N}{2}-1$到1：

5) 　对于$j\in I_{\ell}^{-}$，计算$\mathrm{ACC}\leftarrow\mathrm{ACC}\otimes\mathrm{brk}_j$

6) 　$v\leftarrow v+1$

7) 　若$I_{\ell-1}^{-}\neq\varnothing$或者$v=w$或者$\ell=1$，则

8) 　　$\mathrm{ACC}\leftarrow\mathrm{Auto}_{\vartheta^v}\left(\mathrm{ACC},\mathrm{ak}_{\vartheta^v}\right)$

9) 　　$v\leftarrow 0$

10) 对于$j\in I_0^{-}$，计算$\mathrm{ACC}\leftarrow\mathrm{ACC}\otimes\mathrm{brk}_j$

11) $\mathrm{ACC}\leftarrow\mathrm{Auto}_{-\vartheta}\left(\mathrm{ACC},\mathrm{ak}_{-\vartheta}\right)$

12) 对于ℓ从$\frac{N}{2}-1$到1：

13) 　对于$j\in I_{\ell}^{+}$，计算$\mathrm{ACC}\leftarrow\mathrm{ACC}\otimes\mathrm{brk}_j$

14) 　$v\leftarrow v+1$

15) 　若$I_{\ell-1}^{+}\neq\varnothing$或者$v=w$或者$\ell=1$，则

16) 　　$\mathrm{ACC}\leftarrow\mathrm{Auto}_{\vartheta^v}\left(\mathrm{ACC},\mathrm{ak}_{v^v}\right)$

17) 　　$v\leftarrow 0$

18) 对于$j\in I_0^{+}$，计算$\mathrm{ACC}\leftarrow\mathrm{ACC}\otimes\mathrm{brk}_j$

19) 返回$\mathrm{ACC} = \mathrm{NGS.EncS}\left(f(X)\cdot X^{\boldsymbol{c}\cdot \mathrm{col}_0(\boldsymbol{F})}\right)$

分析算法1所需的自同构数量，易知非空集合$I_l^{\pm}=\varnothing$的数量最多为$\min(N,n)$，下面计算标准假设下，即c_i是随机且独立的情况下，非空集合$I_l^{\pm}$的平均数量。在算法1中，所有c_i为奇数，若所有c_i都不属于某个固定的集合$I_l^{\pm}$，则该集合为空。由于c_i是随机且独立的，则$P\left(I_l^{\pm}=\varnothing\right)=\left(1-\frac{1}{N}\right)^n\approx \mathrm{e}^{-\frac{n}{N}}$，$P\left(I_l^{\pm}\neq\varnothing\right)=1-\left(1-\frac{1}{N}\right)^n\approx 1-\mathrm{e}^{-\frac{n}{N}}$，非空集合的数量为$N\left(1-\left(1-\frac{1}{N}\right)^n\right)\approx N\left(1-\mathrm{e}^{-\frac{n}{N}}\right)$。

计算集合$I_l^{\pm}=\varnothing$的数量有助于估计优化算法执行的自同构次数，因为非空集合间的自同构可以通过$\left\{\mathrm{ak}_{\vartheta^u}\right\}_{u\in[1,w]}$中自同构（给定窗口大小$w$）组合和替换而成。设$k$为非空集合的数量，最坏情况下$K=\min(N,n)$，平均情况下$k=N\left(1-\mathrm{e}^{-\frac{n}{N}}\right)$。设$v_1,\cdots,v_k$为算法需要应用的$k$个自同构$\vartheta^{v_i}$的指数，将每个指数表示为$v_i=v_i'+w\cdot v_i''$，其中$v_i'=$

$v_i \bmod w \in \{1,\cdots,w-1\}$，$v_i'' = \dfrac{v_i'}{w}$。在算法 1 中，基本自同构 ϑ 的 v_i 次可以被一个自同构 $\vartheta^{v_i'}$ 和 v_i'' 个自同构 ϑ^w 所替代。自同构 ϑ^{v_i} 应用的次数为 κ，其中 $\kappa \leqslant k$。为了限制自同构 ϑ^w 应用的次数，利用 $\sum\limits_i v_i \leqslant N$，则 $\sum\limits_i v_i'' \leqslant \dfrac{N-\kappa}{w}$。总之，通过存储 w 个自同构密钥 $\left\{\mathrm{ak}_{\vartheta^u}\right\}_{u\in[1,w]}$，可以将自同构应用的次数减少到 $\kappa + \dfrac{N-\kappa}{w} = \left(1-\dfrac{1}{w}\right)\kappa + \left(\dfrac{1}{w}\right)N$。因此，自同构应用的总次数总是受到 $\left(1-\dfrac{1}{w}\right)k + \dfrac{N}{w}$ 的限制。平均情况下，即 $k = N\left(1-\mathrm{e}^{-\frac{n}{N}}\right)$，自同构应用的预期次数减少到 $N\left(1-\left(1-\dfrac{1}{w}\right)\cdot \mathrm{e}^{-\frac{n}{N}}\right)$。

3.2　普适的存储高效的盲旋转算法

针对 c_i 存在偶数的情况，本节提出了普适的存储高效的盲旋转算法。

该算法的设计是如果 c_i 是偶数，则设置 $\omega_i = c_i - 1$；如果 c_i 是奇数，则设置 $\omega_i = c_i$。然后，对向量 $\boldsymbol{\omega} = (\omega_0,\cdots,\omega_{n-1})$ 应用核心盲旋转算法，得到密文 $\mathrm{NGS.EncS}\left(f(X)\cdot X^{\boldsymbol{c}\cdot \mathrm{col}_0(\boldsymbol{F})}\right)$。最后，针对每个偶数 c_i 重复乘以对应的密钥 brk_i。该算法平均额外需要 $\dfrac{n}{2}$ 次外积运算。

此外，该算法额外存储一个密钥 $\mathrm{brk}_{\mathrm{nsum}} := \mathrm{NGS.EncVec}\left(X^{-\sum_i f_i}\right)$，当偶数 c_i 的数量大于 $\dfrac{n}{2}$ 时，则计算 $\mathrm{ACC} \otimes \mathrm{brk}_{\mathrm{nsum}}$ 外积更新累加器，并更新 $c_i \leftarrow c_i + 1$。这使奇数 c_i 的数量超过一半，从而缓解最坏情况的发生。完整算法描述如算法 2 所示。

算法 2　存储高效的盲旋转算法

$\mathrm{BlindRotateMe}(\mathrm{ACC},\mathrm{ct},\{\mathrm{brk}_i\}_{0\leqslant i\leqslant n-1},\mathrm{brk}_{\mathrm{nsum}},\left\{\mathrm{ak}_{\vartheta^u}\right\}_{u\in[1,w]},\mathrm{ak}_{-\vartheta})$

输入　MNTRU 基本加密方案的密文 $\mathrm{ct}\in\mathbb{Z}_q^n$，加密的明文 $m\in\{0,1\}$；初始化的累加器 ACC；盲旋转密钥 $\mathrm{brk}_{\mathrm{nsum}}$，$\{\mathrm{brk}_i\}_{0\leqslant i\leqslant n-1}$，其中 $\mathrm{brk}_{\mathrm{nsum}} := \mathrm{NGS.EncVec}\left(X^{-\sum_i f_i}\right)$；自同构的转换密钥 $\left\{\mathrm{ak}_{\vartheta^u}\right\}_{u\in[1,w]},\mathrm{ak}_{-\vartheta}$

输出　$\mathrm{NGS.EncS}\left(f(X)\cdot X^{\boldsymbol{c}\cdot \mathrm{col}_0(\boldsymbol{F})}\right)$，即累加器旋转 $X^{\boldsymbol{c}\cdot \mathrm{col}_0(\boldsymbol{F})}$，$\boldsymbol{c}\cdot\mathrm{col}_0(\boldsymbol{F})$ 对 $2N$ 取模

1) $(c_0,\cdots,c_{n-1}) \leftarrow \left\lfloor \dfrac{2\cdot N\cdot \mathbf{ct}}{q} \right\rceil$

2) 初始化 $\mathrm{ACC} \leftarrow \left\lfloor \dfrac{Q}{8} \right\rceil \cdot X^{\frac{N}{2}} \cdot \sum\limits_{i=0}^{N-1} X^i$

3) 若 c_i 为偶数的数量大于 $\dfrac{n}{2}$，则

4) $\begin{cases} \mathrm{ACC} \leftarrow \mathrm{ACC} \otimes \mathrm{brk}_{\mathrm{nsum}} \\ (c_0,\cdots,c_{n-1}) \leftarrow (c_0+1,\cdots,c_{n-1}+1)(\mathrm{mod}2N) \end{cases}$

5) 对于 i 从 0 到 $n-1$：

6)　若 c_i 为偶数，则

7)　　$\omega_i = c_i - 1$

8)　否则

9)　　$\omega_i = c_i$

10) $\mathrm{BlindRotateCore}(\mathrm{ACC},\mathrm{ct},\{\mathrm{brk}_i\}_{0\leqslant i\leqslant n-1},\left\{\mathrm{ak}_{\vartheta^u}\right\}_{u\in[1,w]},\mathrm{ak}_{-\vartheta})$

11) 对于 i 从 0 到 $n-1$：

12)　若 c_i 为偶数，则

13)　　$\mathrm{ACC} \leftarrow \mathrm{ACC} \otimes \mathrm{brk}_i$

14) 返回 $\mathrm{ACC} = \mathrm{NGS.EncS}\left(f(X)\cdot X^{\mathbf{c}\cdot \mathrm{col}_0(\boldsymbol{F})}\right)$

算法 2 性能分析如下。盲旋转所需的密钥为 $\{\mathrm{brk}_i\}_{0\leqslant i\leqslant n-1},\mathrm{brk}_{\mathrm{nsum}},\left\{\mathrm{ak}_{\vartheta^u}\right\}_{u\in[1,w]},\mathrm{ak}_{-\vartheta}$，即密钥规模为 $n+w+2$ 个 NGS 向量密文。盲旋转所需的外积次数为 $\dfrac{3}{2}n + \dfrac{w-1}{w}k + \dfrac{N}{w}$，其中，$n$ 为 BlindRotateCore 算法需要的外积次数，$\dfrac{1}{2}n$ 为 c_i 是偶数的情况下需要额外进行的外积次数，$\dfrac{w-1}{w}k + \dfrac{N}{w}$ 是自同构运算时需要的外积次数。对于噪声的比较，根据文献[3]，FINAL 方案盲旋转算法产生的噪声方差为 $\mathrm{Var}(\mathrm{err}) \leqslant n\cdot N\cdot l\cdot B^2\cdot \mathrm{Var}\left(\mathrm{err}\left(c_{\mathrm{Mux}}\right)\right) + 4\cdot N\cdot \sigma^2$。其中，$\mathrm{Var}\left(\mathrm{err}\left(c_{\mathrm{Mux}}\right)\right)$ 为

$$\mathrm{Var}\left(\mathrm{err}\left(c_{\mathrm{Mux}}\right)\right) \leqslant X^{c_i} - 1_2^2\cdot \mathrm{Var}\left(\mathrm{err}\left(\mathrm{bsk}_{i,0}\right)\right) + X^{-c_i} - 1_2^2\cdot \mathrm{Var}\left(\mathrm{err}\left(\mathrm{bsk}_{i,1}\right)\right) \leqslant 4\cdot \mathrm{Var}\left(\mathrm{err}(\mathrm{bsk})\right) = 4\cdot\sigma^2 \tag{28}$$

其中，$\mathrm{Var}(\mathrm{err}(\mathrm{bsk}))$ 是 NGS 密文的噪声方差，σ 为

NGS加密方案中g以及f'的标准差，n为盲旋转需要的外积次数。

算法2的盲旋转密钥brk_j: = NGS.EncVec$\left(X^{f_j}\right) \in R_{Q,N}^{\ell}$，相较于FINAL的外积ACC $\otimes$ c_{Mux}，算法2的外积变为ACC $\otimes$ brk_j，因此，盲旋转算法产生的噪声方差变为

$$\begin{aligned}&\mathrm{Var}(\mathrm{err}) \leqslant \\ &\left(\frac{3}{2}n+\frac{w-1}{w}k+\frac{N}{w}\right)\cdot N\cdot l\cdot B^2\cdot \mathrm{Var}\left(\mathrm{err}\left(\mathrm{brk}_j\right)\right)+ \\ &\mathrm{Var}\left(\mathrm{err}\left(\frac{Q}{8}\cdot X^{\frac{N}{2}}\cdot\sum_{i=0}^{N-1}X^i\right)\right)\leqslant \\ &\left(\frac{3}{2}n+\frac{w-1}{w}k+\frac{N}{w}\right)\cdot N\cdot l\cdot B^2\cdot \mathrm{Var}\left(\mathrm{err}\left(\mathrm{brk}_j\right)\right)\end{aligned} \tag{29}$$

其中，$\mathrm{Var}(\mathrm{err}\left(\mathrm{brk}_j\right)=\mathrm{Var}\left(\mathrm{err}(\mathrm{bsk})\right)=\sigma_g{}^2$。

在$w=20$（文献[9]中当$w \geqslant 10$，盲旋转运行时间接近，因此，本文中选取$w=20$）以及FINAL原方案参数设置下，盲旋转所需的平均自同构数量为$\left(1-\frac{1}{w}\right)k+\frac{N}{w}=579$。表1对比了不同盲旋转方案的密钥规模、外积次数以及噪声方差。

表1 密钥规模、外积次数以及噪声方差对比

方案	密钥规模/个	外积次数/次	噪声方差
FINAL	1 600	800	$3\,200NlB^2\sigma_g{}^2$
算法2	822	1 779	$1\,779NlB^2\sigma_g{}^2$

由表1可以看出，算法2与原方案相比，密钥规模以及噪声方差降低，外积次数增多。

外积运算主要由FFT运算以及Hadamard向量积运算构成。算法2噪声方差降低，因此，本文可以在噪声限度内，动态调整NGS加密方案的分解基，减少盲旋转需要的FFT运算以及Hadamard向量积运算的总次数。

3.3 安全性分析

参数$n,q,Q,\sigma_f,\sigma_g,\sigma_s,\sigma_e,N$影响基于MNTRU的FINAL全同态加密方案的安全级别。本文仅对盲旋转算法进行了优化，即从环同构的角度实现盲旋转，得到盲旋转优化算法，第4节引入动态调整分解基技术也仅仅改变FINAL全同态加密方案第二层加密结构（NGS）的分解基及对应维数的值，参数$n,q,Q,\sigma_f,\sigma_g,\sigma_s,\sigma_e,N$的值均不变，因此，方案的安全级别与原方案基本相同。

4 动态调整分解基

自举产生的噪声需要小于噪声界限才可以正常解密，算法2大大减小了盲旋转算法产生的噪声，因此，扩大了参数优化的空间，即可以通过采用较大的分解基B_1和B_2进一步降低外积所需的FFT次数以及多项式环上的乘法次数。由于本文是对FINAL方案的盲旋转进行改进，因此不妨只对盲旋转进行分析，即以原方案盲旋转产生的噪声为界限，动态调整优化算法的分解基，减少盲旋转需要的FFT运算以及Hadamard向量积运算的总次数。

基于MNTRU的FINAL方案的参数设置为：$n=800$，$q=2^{17}-1$，$N=2^{10}$，$Q=912829$。因为$q=2^{17}-1$，本文中可以将q近似为2^{17}，则$\mathbb{Z}_{2^{17}}^{*} \cong \mathbb{Z}_{2^{15}} \otimes \mathbb{Z}_2$。

假设自举密钥提前进行了FFT预处理，则每次外积需要进行l_i+1次FFT以及$2\cdot l_i$次Hadamard向量积，即原FINAL方案需要进行的FFT运算次数和Hadamard向量积运算次数分别为

$$\left(l_1+1\right)\cdot n_1+\left(l_2+1\right)\cdot n_2 \tag{30}$$

$$2\cdot\left(l_1\cdot n_1+l_2\cdot n_2\right) \tag{31}$$

其中，n_1和n_2将n分为两部分，即$n_1+n_2=n$，B_1、B_2和l_1、l_2分别为这两部分的分解基和分解长度。

算法2需要进行的FFT运算次数和Hadamard向量积运算次数分别为

$$\left(\left(l_1'+1\right)\cdot n_1'+\left(l_2'+1\right)\cdot n_2'\right)\cdot\frac{3}{2}+\left(L'+1\right)\cdot\left(\frac{w-1}{w}k+\frac{N}{w}\right) \tag{32}$$

$$\left(l_1'\cdot n_1'+l_2'\cdot n_2'\right)\cdot\frac{3}{2}+L'\cdot\left(\frac{w-1}{w}k+\frac{N}{w}\right) \tag{33}$$

其中，算法2生成盲旋转密钥时可能采用更大的分解基B_1'和B_2'，使$l_1' \leqslant l_1, l_2' \leqslant l_2$，$L'$为自同构运算时密钥转换密钥的分解长度。

原FINAL方案的盲旋转噪声公式为

$$\mathrm{Var}(\mathrm{err}) \leqslant 4\cdot N\cdot\sigma_g{}^2\cdot\left(n_1\cdot l_1\cdot B_1^2+n_2\cdot l_2\cdot B_2^2\right) \tag{34}$$

算法2的盲旋转噪声公式为

$$\mathrm{Var}(\mathrm{err}) \leqslant N \cdot {\sigma_g}^2 \cdot \left(n_1' \cdot l_1' \cdot B_1'^2 + n_2' \cdot l_2' \cdot B_2'^2\right) \cdot \frac{3}{2} + \left(\frac{w-1}{w} k + \frac{N}{w}\right) \cdot L' \cdot B_{\mathrm{ksk}}'^2 \cdot N \cdot {\sigma_g}^2 \quad (35)$$

5　性能分析

利用动态调整分解基技术，取$B'_{\mathrm{ksk}} = 32$，$B_1' = 16$，$B_2' = 32$，$n_1' = 310$，$n_2' = 490$。不同算法的具体性能对比如表2所示，其中，密钥规模用R_Q上元素的数量来表示，FFT和内积分别表示方案需要进行的FFT运算次数和内积运算次数。

经过参数优化，分解基B_1和B_2对应的n_1和n_2与原FINAL方案不同。因此，表1所示的以NGS向量密文的数量表示盲旋转密钥的规模不再适用，考虑到盲旋转密钥形式为NGS.EncVec $\in R_Q^l$，不妨以R_Q上元素的数量表示盲旋转密钥规模，即原FINAL方案盲旋转密钥规模为$2 \cdot (l_1 \cdot n_1 + l_2 \cdot n_2) = 11\,000$，本文优化方案（算法2）盲旋转密钥规模为$l_1 \cdot n_1 + l_2 \cdot n_2 + L \cdot (w+2) = 3\,598$。

在Inter Core i7-13700F处理器、64 GB DDR4内存以及Ubuntu 20.04虚拟机的环境下，FINAL原方案盲旋转耗时为0.093 s，一次FFT的耗时为7 μs，一次内积的耗时为4.5 μs，结合表2，FINAL算法的盲旋转计算耗时为$6\,300 \times 7 + 11\,000 \times 4.5 = 9.36 \times 10^4 \mu\mathrm{s} = 0.093\,6$ s，与测试结果0.093 s相近。同理，计算利用动态调整分解基技术调整参数后的算法2盲旋转耗时约为0.1 s。算法2在计算代价增加约7%的情况下，将盲旋转密钥规模优化67%。

6　结束语

本文利用环自同构以及密钥转换技术优化了MNTRU型FINAL全同态加密方案的盲旋转算法，减少了自举所需的盲旋转密钥规模以及盲旋转产生的噪声，同时使优化算法在分解基的选取上有更多的选择。再通过动态调整分解基技术对参数的选取进一步优化，使最终优化后的盲旋转算法在计算代价增加约7%的情况下，盲旋转密钥规模优化67%。

参考文献：

[1] DUCAS L, MICCIANCIO D. FHEW: bootstrapping homomorphic encryption in less than a second[C]//Advances in Cryptology- EUROCRYPT 2015. Berlin: Springer, 2015: 617-640.

[2] CHILLOTTI I, GAMA N, GEORGIEVA M, et al. TFHE: fast fully homomorphic encryption over the torus[J]. Journal of Cryptology, 2020, 33(1): 34-91.

[3] BONTE C, ILIASHENKO I, PARK J, et al. FINAL: faster FHE instantiated with NTRU and LWE[C]//Advances in Cryptology-ASIACRYPT 2022. Berlin: Springer, 2022: 188-215.

[4] MICCIANCIO D, POLYAKOV Y. Bootstrapping in FHEW-like cryptosystems[C]//Proceedings of the 9th on Workshop on Encrypted Computing & Applied Homomorphic Cryptography. New York: ACM Press, 2021: 17-28.

[5] ALPERIN-SHERIFF J, PEIKERT C. Faster bootstrapping with polynomial error[C]//Advances in Cryptology-CRYPTO 2014. Berlin: Springer, 2014: 297-314.

[6] GAMA N, IZABACHÈNE M, NGUYEN P Q, et al. Structural lattice reduction: generalized worst-case to average-case reductions and homomorphic cryptosystems[C]//Advances in Cryptology-EUROCRYPT 2016. Berlin: Springer, 2016: 528-558.

[7] KLUCZNIAK K. NTRU-v-um: secure fully homomorphic encryption from NTRU with small modulus[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2022: 1783-1797.

[8] LEE C M, MIN S, SEO J, et al. Faster TFHE bootstrapping with block binary keys[C]//Proceedings of the ACM Asia Conference on Computer and Communications Security. New York: ACM Press, 2023: 2-13.

[9] LEE Y, MICCIANCIO D, KIM A, et al. Efficient FHEW bootstrapping with small evaluation keys, and applications to threshold homomorphic encryption[C]//Advances in Cryptology-EUROCRYPT 2023. Berlin: Springer, 2023: 227-256.

[10] XIANG B W, ZHANG J, DENG Y, et al. Fast blind rotation for bootstrapping FHEs[C]//Advances in Cryptology-CRYPTO 2023. Berlin: Springer, 2023: 3-36.

[11] WANG R D, WEN Y D, LI Z H, et al. Circuit bootstrapping: faster and

表2　具体计算性能对比

方案	(B_1,n_1,l_1)	(B_2,n_2,l_2)	(B_{ksk},L)	密钥规模	FFT	内积	耗时/s
FINAL	(8,750,7)	(16,50,5)	(3,16)	11 000	6 300	11 000	0.093
算法2	(8,750,7)	(16,50,5)	(3,16)	5 852	19 293	17 514	0.21
	(16,310,5)	(32,490,4)	(32,4)	3 598	9 360	7 581	0.1

smaller[C]//Advances in Cryptology - EUROCRYPT 2024. Berlin: Springer, 2024: 342-372.

[12] KIRCHNER P, FOUQUE P A. Revisiting lattice attacks on overstretched NTRU parameters[C]//Advances in Cryptology - EUROCRYPT 2017. Berlin: Springer, 2017: 3-26.

[作者简介]

赵秀凤（1977– ），女，山东梁山人，博士，网络空间部队信息工程大学副教授，主要研究方向为全同态密码、格密码、密码协议等。

吴蒙（2000– ），男，河北保定人，网络空间部队信息工程大学硕士生，主要研究方向为全同态密码。

宋巍涛（1989– ），男，河南中牟人，博士，网络空间部队信息工程大学副教授，主要研究方向为全同态密码及应用。