支持多比特加密的全同态加密体制设计*

陈 莉[1]，周 扬[1]，段 然[2]
(1. 河南财经政法大学 网络信息安全研究所，郑州 450046；2. 数学工程与先进计算国家重点实验室，江苏 无锡 214125)

摘 要： 现有全同态加密体制普遍存在密文尺寸较大和采用单比特加密所导致的效率较低问题。在 Gentry 等人提出的全同态加密体制(简称 GSW13 体制)的基础上，通过修改其展开方式，利用近似特征向量技术，提出了一种新的全同态加密体制。在随机喻示模型下，将新体制的安全性归约到判定性容错学习问题(decisional learning with errors，DLWE)的难解性，给出了其正确性和安全性的证明。又在不改变系统参数的条件下，采用多比特加密，对新体制进行优化。与 GSW13 体制相比，新体制的密文尺寸减小 61.47%，加密运算量减少 68.97%。新体制不仅减小密文扩张，而且减少同态运算计算次数，从而提高了体制效率。

关键词： 云计算；全同态加密；判定性容错学习问题；多比特加密；可证明安全
中图分类号： TP309 **文献标志码：** A **文章编号：** 1001-3695(2021)02-050-0579-05
doi:10.19734/j.issn.1001-3695.2019.10.0680

Design of fully homomorphic encryption scheme supporting multi-bit encryption

Chen Li[1], Zhou Yang[1], Duan Ran[2]
(1. *Institute of Network Information Security, Henan University of Economics & Law, Zhengzhou* 450046, *China*; 2. *State Key Laboratory of Mathematical Engineering & Advanced Computing, Wuxi Jiangsu* 214125, *China*)

Abstract: The existing fully homomorphic encryption schemes are faced with challenges like large ciphertext sizes or low efficiency in calculation due to single-bit encryption. Based on the fully homomorphic encryption scheme proposed by Gentry et al. (GSW13 scheme), this paper proposed a new fully homomorphic encryption scheme by modifying its expansion method and using the idea of approximate eigenvector. It reduced the security of the new scheme to the complexity of the DLWE problem under the random oracle model, and gave the proof of its correctness and security. It used the multi-bit encryption to optimize the new scheme without changing the scheme parameters. Compared with the GSW13 scheme, the ciphertext size of the proposed scheme is reduced by 61.47%, and the number of encryption operations is minimized by 68.97%. The proposed scheme not only further reduces the ciphertext size, but also greatly reduces the number of homomorphic operations, thus further improving the scheme efficiency.

Key words: cloud computing; fully homomorphic encryption; DLWE; multi-bit encryption; provable security

0 引言

随着云计算的快速发展与推广应用，云计算环境中的数据安全和隐私保护等问题成为云计算研究中的关键问题。由于传统数据加密技术无法支持云服务商在不解密的情况下，直接对加密的云用户数据进行任何形式的有效计算，所以对云用户的数据安全和隐私保护产生了极大的威胁，云计算的便利性与用户对于数据安全和隐私保护的需求成为一对难以调和的矛盾。

全同态加密(fully homomorphic encryption，FHE)允许任何人在无须解密的情况下，在加密数据上进行各种有意义的运算，因而为上述问题和矛盾提供了一条切实有效的解决途径，拥有广阔的应用前景。1978 年，Rivest 等人[1]提出了全同态加密的原始概念。由于全同态加密设计与实现的难度极大，其相关研究进展缓慢。直到 2009 年，全同态加密的研究出现了重要突破，Gentry[2]基于一种被称为理想格(ideal lattice)的代数结构，成功构造出第一个真正意义上的全同态加密体制(Gentry 体制)。自此，设计出实用化的全同态加密方案成为密码学界和业界孜孜以求的共同目标[3]。

2009 年之后，学术界陆续提出了基于不同代数结构的全同态体制[4~7]，对全同态体制的相关研究也在不断发展[8~24]。2011 年，Brakerski 等人[15]采用重线性化技术和维数模约减技术控制密文的维度和噪声的增长，基于容错学习问题(learning with errors，LWE)[16]构造出一套全同态加密方案。2013 年，文献[17]提出了一种基于近似特征向量的全同态加密体制 GSW13，其最大特点是在同态运算中无须使用运算密钥，但缺点是密文尺寸较大。2014 年，Brakerski 等人[18]提出针对 GSW13 体制改进的 BootStrapping 方法，但该方法效率不高。Alperin-Sheriff 等人[19]修改 GSW13 的密文矩阵，提出一种在同态解密时快速计算内积的方法，并辅以 BootStrapping 技术，构造了一套误差项多项式级别增长的全同态加密方案。2015 年，古春生[20]通过扩展近似 GCD 到近似理想格的方法，构造了一个基于整数上部分近似理想格问题(PAILP)的有点同态加密方案，又基于 PAILP 的批全同态加密方案和基于近似理想格(AILP)构造了一个全同态加密方案。Halevi 等人[21]利用 HElib 库实现密文的重加密，支持密文在扩展域上的 BootStrap-

收稿日期：2019-10-28；修回日期：2019-12-05 基金项目：国家自然科学基金资助项目(61170234，61309007)；河南省高校科技创新人才支持计划项目(13HASTIT043)；河南省高等学校重点科研项目(20A520001)

作者简介：陈莉(1968-)，女，江苏如皋人，教授，博士，主要研究方向为密码学、信息安全(chlit123@aliyun.com)；周扬(1978-)，女，河南周口人，讲师，硕士，主要研究方向为信息安全；段然(1989-)，男，北京人，博士，主要研究方向为密码学、信息安全.

ping 过程。2016 年，Brakerski 等人[22]提出一个支持无限次同态操作的多密钥全同态加密体制。密文的长度和同态操作的空间复杂度随着参与计算群体数量的增多呈线性增长。利用 Gentry 的 BootStrapping 技术，在标准 LWE 假设下获得一个全同态加密方案。陈智罡等人[23]提出一个 LWE 上的短公钥多位全同态加密方案，该方案从离散高斯分布上选取 LWE 样例，将高斯噪声与之相加，导致 LWE 样例从 $2n\log q$ 下降到 $n+1$，使得方案的公钥长度变短。2017 年，姬晨等人[24]在 GSW13 全同态加密方案的基础上重新设计密钥生成、加密、解密、同态操作等函数，提出了一种基于布尔电路的改进同态加密方案，改进方案的同态加法和同态乘法对应矩阵加法和矩阵乘法，不会造成密文维度扩张。

现有全同态加密体制普遍存在因密文尺寸较大和采用单比特加密所导致的效率较低的问题，本文结合 GSW13 体制，通过修改其展开方式，利用近似特征向量技术，提出了一种支持多比特加密[25,26]的基于 DLWE 的全同态加密体制（记为 NFHE 体制）。与 GSW13 体制相比，NFHE 体制的密文尺寸和同态运算计算次数均显著减小，使得其效率得到高效提升。在随机喻示模型下，基于判定性 LWE 问题（简称 DLWE 问题）的难解性，证明 NFHE 体制在选择明文攻击下具有不可区分性（IND-CPA 安全）。

1 基础知识

1.1 符号定义

本文符号统一如下：$\mathbb{Z}^+$、$\mathbb{Z}$、$\mathbb{Q}$、$\mathbb{R}$、$\mathbb{Z}_q$ 分别表示正整数集、整数集、有理数集、实数集、整数模 q 剩余类环。对于 2 的方幂 n，R 表示多项式环 $\mathbb{Z}[x]/(x^n+1)$，R' 表示多项式环 $\mathbb{Q}[x]/(x^n+1)$，R_q 表示 $\mathbb{Z}_q[x]/(x^n+1)$。定义 n 维向量 $\boldsymbol{a}$ 的长度为其欧几里德范数 $\|\boldsymbol{a}\|=\sqrt{\sum_{i=0}^{n-1}a_i^2}$，定义向量集 S 的长度 $\|S\|=\max_{\boldsymbol{a}\in S}\|\boldsymbol{a}\|$。$\boldsymbol{a}\leftarrow D$ 表示从概率分布 D 中随机选取变量 $\boldsymbol{a}$，$\boldsymbol{a}\xleftarrow{R}A$ 表示从集合 A 中随机均匀选取变量 $\boldsymbol{a}$。向量 $\boldsymbol{a}\in\mathbb{Z}_q^n$ 可表示为 $\boldsymbol{a}=(a_0,\cdots,a_{n-1})$；多项式 $b\in R_q$ 可表示为 $b=(b_0,\cdots,b_{n-1})$，R_q 上的多项式和 $\mathbb{Z}_q^n$ 上的向量可以通过系数对应的方式相互转换。c_i 表示矩阵 $\boldsymbol{C}$ 的第 i 行，$\boldsymbol{I}_n$ 表示 n 维单位矩阵，$\varphi(y)$ 表示概率 $Pr[y\leqslant x\mid y\sim N(0,1)]$。对于多项式 b，$c\in R$，定义 $b\times c=bc \bmod (x^n+1)$。$\log n$ 表示 $\log_2 n$。

除了常用的计算复杂度符号 O、o、Θ 以外，本文还定义了 $\mathrm{poly}(\cdot)$ 和 $\mathrm{negl}(\cdot)$。如果 $f(n)=O(n^c)$，则 $f(n)$ 可表示为 $\mathrm{poly}(n)$。若对于任意的常数 c，都存在 $f(n)=o(n^{-c})$，则 $f(n)$ 可表示为 $\mathrm{negl}(n)$，称为 n 的可忽略函数。

1.2 LWE 和判定性 LWE 问题

容错学习问题[16]是从带噪声奇偶性学习问题（learning parity with noise，LPN）一般化扩展而来。Peikert[27]、Brakerski 等人[28]分别给出了从最短向量问题（shortest vector problem，SVP）、最短独立向量问题（shortest independent vectors problem，SIVP）的最坏情况归约到 LWE 问题的平均情况，因此 LWE 问题的难解性得到了很好的保证。2011 年，Brakerski 等人[15]提出第一种基于 LWE 问题的全同态加密体制，具备较高的计算效率和可靠的安全性归约，迅速成为全同态加密设计领域的研究热点[29,30]。

定义 1 LWE。对于正整数 n、$q=q(n)$，$\mathbb{Z}_q^n$ 上的向量 $\boldsymbol{s}$ 以及 $\mathbb{Z}_q$ 上的错误分布 χ，定义一个 $\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上的概率分布 $A_{\boldsymbol{s},\chi}$，其变量具备 $(\boldsymbol{a},\boldsymbol{a}^{\mathrm{T}}\cdot\boldsymbol{s}+x)$ 的形式，其中 $\boldsymbol{a}$ 是 Z_q^n 上均匀分布的变量，x 取自错误分布 χ，加法和向量乘法运算均在模 q 意义下进行。容错学习问题 $LWE_{m,n,q,\chi}$（寻找问题）定义为：给出 m 个 $A_{\boldsymbol{s},\chi}$ 上相互独立的变量，求出向量 $\boldsymbol{s}$ 的值。

定义 2 DLWE。在平均情况难解性条件下，将判定性 LWE 问题记为 $DLWE_{m,n,q,\chi}$，当向量 $\boldsymbol{s}$ 取自 $\mathbb{Z}_q^n$ 上的均匀分布时，要求攻击者以不可忽略的概率区分各包含 m 个样本的两组随机变量，两组变量分别取自分布 $A_{\boldsymbol{s},\chi}$ 和 $\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上的均匀分布。

$DLWE_{m,n,q,\chi}$ 的一种变形是攻击者不事先确定参数 m 的值，而是以多项式次数访问 $A_{\boldsymbol{s},\chi}$ 喻示，得到不定数量的两组变量并进行区分，称为 $DLWE_{n,q,\chi}$ 问题。

1.3 全同态加密体制可证明安全

对于使用公钥加密模式的全同态加密体制的设计和分析而言，通过可证明安全理论进行安全性证明是目前被广泛接受和使用的分析手段。

定义 3 体制 IND-CPA 安全性。对于一个公钥加密体制 $\xi_{pub}=(Keygen,Enc,Dec)$ 和针对它的攻击 CPA，IND-CPA 攻击游戏的参与者包括一个挑战者 $\mathcal{C}$ 和一个攻击者 $\mathcal{A}$；挑战者 $\mathcal{C}$ 具备构造解密喻示 O_{Dec} 的能力，对于任意输入的密文 c_i，解密喻示 O_{Dec} 输出明文 $m_i\leftarrow\mathrm{Dec}(sk,c_i)$。游戏被分成五个阶段：

a) 初始化。挑战者 $\mathcal{C}$ 执行密钥生成算法 $(pk,sk)\leftarrow\mathrm{Keygen}(1^\lambda)$，将生成的公钥 pk 交给攻击者 $\mathcal{A}$。

b) 第一次喻示访问。$\mathcal{C}$ 为 $\mathcal{A}$ 构造一个喻示 $Oracle_1$，$\mathcal{A}$ 适应性地选择一组输入 $\{c_i,i=1,\cdots,t\}$ 对喻示 O_{Dec} 进行适应性访问，即第 i 次访问的输入可以依赖于从前 $i-1$ 次喻示访问中获取的信息。

c) 挑战。攻击者 $\mathcal{A}$ 选择一对挑战明文 $m_0^*,m_1^*\in\mathcal{P}$，两者长度相等，即 $|m_0^*|=|m_1^*|$，将其交给挑战者 $\mathcal{C}$，$\mathcal{C}$ 根据随机选择的 $b\xleftarrow{R}\{0,1\}$，对 m_b^* 进行加密，得到密文 $c^*\leftarrow\mathrm{Enc}(sk,m_b^*)$，并将其交给攻击者 $\mathcal{A}$。值得注意的是，此处不允许 $\mathcal{A}$ 使用上一阶段访问解密喻示时获得的输出反馈作为挑战明文。

d) 第二次喻示访问。$\mathcal{C}$ 为 $\mathcal{A}$ 构造出另一个喻示 $Oracle_2$ 供其访问，同样地，$\mathcal{A}$ 不允许使用将目标密文作为喻示 $Oracle_2$ 的输入。

e) 猜测。攻击者 $\mathcal{A}$ 猜测目标密文 c^* 所对应的明文，输出明文的角标 b' 作为其猜测结果，当 $b'=b$ 时，判定 $\mathcal{A}$ 在攻击游戏中获胜。

当 $Oracle_1=\perp$，$Oracle_2=\perp$；定义攻击者 $\mathcal{A}$ 在游戏中的优势为

$$\mathrm{Adv}_{\mathrm{CPA}}(\mathcal{A})=|\Pr[\mathcal{A}(pk,\mathrm{Enc}(pk,m_0^*)=1]-\Pr[\mathcal{A}(pk,\mathrm{Enc}(pk,m_1^*)=1]|$$

若任意多项式时间的攻击者 $\mathcal{A}$ 在 IND-CPA 攻击游戏中的优势均可忽略，则称公钥加密体制 ξ_{pub} 是 IND-CPA 安全的。对于使用公钥加密模式的全同态加密体制，Gentry[31]指出，其可以采用与公钥加密体制相同的安全性定义。

2 体制构造

本章针对 GSW13 体制现存的“因密文尺寸较大和采用单比特加密所导致的效率较低”的问题，在该体制的基础上，基于近似特征向量技术，通过修改 GSW13 体制的展开方式，提出一种使密文尺寸更小的全同态加密体制，称为 NFHE 体制。

NFHE 体制的构造思路如下，给定模数 q，维数 N，密文 $\boldsymbol{C}$ 为定义在 $\mathbb{Z}_p$ 上的 $N\times N$ 维矩阵，组成该矩阵的每个分量均远小于 q。$\boldsymbol{C}$ 的私钥 sk 为定义在 $\mathbb{Z}_p$ 上的 N 维向量，sk 中至少含有一个大的分量。令明文 μ 为小的整数，当 $\boldsymbol{C}\cdot sk=\mu\cdot sk+\boldsymbol{e}$ 时，则称 $\boldsymbol{C}$ 为 μ 的密文，其中 $\boldsymbol{e}$ 为小的误差向量。在解密过程中，先抽取 $\boldsymbol{C}$ 的第 i 行 C_i，接着计算 $x\leftarrow\langle C_i,sk\rangle=\mu\cdot sk_i+e_i$，

最后输出 $\mu = \lfloor x/sk_i \rceil$,其中 sk_i 为 sk 的第 i 个元素,e_i 为 e 的第 i 个元素,$i \in [0, N-1]$。在 NFHE 体制中,消息 μ 可被视为密文矩阵 C 的一个特征值,私钥 sk 为 C 对应于特征值 μ 的近似特征向量。

NFHE 体制的设计思路如下: 首先通过定义 mbDpt($\boldsymbol{a}$)、mbDpt^{-1}($\boldsymbol{a}'$)、mbFlatten($\boldsymbol{a}'$)、pofmb($\boldsymbol{b}$) 等函数,给出 NFHE 体制的展开方式; 接下来基于上述函数,设计 NFHE 体制包含的五个多项式时间算法,它们分别是密钥生成算法 NFHE. Keygen(n,q)、加密算法 NFHE. Encrypt(pk,μ)、解密算法 NFHE. Decrypt($\boldsymbol{sk}$,$\boldsymbol{C}$)、同态加法算法 NFHE. Add(C_1,C_2) 和同态乘法算法 NFHE. Mult(C_1,C_2)。

NFHE 体制的函数定义:

令 $\boldsymbol{a}$、$\boldsymbol{b}$ 为 $\mathbb{Z}_q^k$ 上的向量,k 为正整数,q 为模数,p 为 2 的方幂,$t = \lceil \log_p q \rceil$,$N = kt$。函数 mbDpt($\boldsymbol{a}$) 的结果为 N 维向量 $\boldsymbol{a}' = (a_{1,1}, \cdots, a_{1,t}, \cdots, a_{k,1}, \cdots, a_{k,t}) \in \mathbb{Z}_p^N$,其中 $a_i = \sum_{j=1}^{t} a_{i,j} p^{j-1}$,$a_{i,j} \in \mathbb{Z}_p$。

定义 mbDpt^{-1}($\boldsymbol{a}'$) $= (\sum p^j \cdot a_{1,j}, \cdots, \sum p^j \cdot a_{k,j})$;

定义 mbFlatten($\boldsymbol{a}'$) $=$ mbDpt(mbDpt^{-1}($\boldsymbol{a}'$));

定义 pofmb($\boldsymbol{b}$) $= (b_1, pb_1, \cdots, p^{t-1} b_1, \cdots, b_k, pb_k, \cdots, p^{t-1} b_k)$。

NFHE 体制包含的五个多项式时间算法具体描述如下:

a) 密钥生成算法 NFHE. Keygen(n,q)。对于正整数 n,同态运算的深度 l,从 $\mathbb{Z}_q^{n \times n}$ 上随机均匀选取 $\boldsymbol{A} \xleftarrow{R} \mathbb{Z}_q^{n \times n}$,从 $\mathbb{Z}^{n \times l}$ 上的离散高斯分布 $\chi^{n \times l}$ 上采样 $\boldsymbol{s}, \boldsymbol{e} \leftarrow \chi^n$。计算公钥 $pk = (\boldsymbol{A}, \boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}) \in \mathbb{Z}_q^{n \times n} \times \mathbb{Z}_q^n$,私钥为 $\boldsymbol{sk} = \begin{pmatrix} -\boldsymbol{s} \\ 1 \end{pmatrix} \in \mathbb{Z}_q^{n+1}$。

b) 加密算法 NFHE. Encrypt(pk,μ)。对于要加密的明文 $\mu \in \{0,1\}$,随机选取 $\boldsymbol{r}_i, e_{i,1} \leftarrow \chi^n, e_{i,2} \leftarrow \chi, i = 1, \cdots, (n+1) \cdot t$,计算 $C_{i,1} = \boldsymbol{A}^{\mathrm{T}} \cdot \boldsymbol{r}_i + e_{i,1} \in \mathbb{Z}_q^n$,$C_{i,2} = \boldsymbol{b}^{\mathrm{T}} \cdot \boldsymbol{r}_2 + e_{i,2} \in \mathbb{Z}_q$。其中,$e_{ij}$ 为 e_i 的第 j 个元素,C_{ij} 为 C_i 的第 j 个元素。令 $\boldsymbol{C}'$ 为由 $m = (n+1) \cdot t$ 个密文作为列向量排列而成的矩阵,其维数为 $(n+1) \times m$,输出密文 $\boldsymbol{C} = \mathrm{mbFlatten}(\mu \cdot \boldsymbol{I}_N + \mathrm{mbDpt}(\boldsymbol{C}')) \in \mathbb{Z}_p^{m \times m}$。

c) 解密算法 NFHE. Decrypt($\boldsymbol{sk}$,$\boldsymbol{C}$)。对于密文 $\boldsymbol{C} \in \mathbb{Z}_p^{m \times m}$ 和私钥 $\boldsymbol{sk} = \begin{pmatrix} -\boldsymbol{s} \\ 1 \end{pmatrix} \in \mathbb{Z}_q^{n+1}$,令 $\boldsymbol{s}' = \mathrm{pofmb}(\boldsymbol{sk})$,计算并输出明文 $\mu = \lfloor \dfrac{\langle \boldsymbol{s}', \boldsymbol{C}_{m-1} \rangle}{(q/2p)} + \dfrac{1}{2} \rfloor \bmod 2$。

d) 同态加法算法 NFHE. Add(C_1,C_2)。输入密文 C_1、C_2,输出进行同态加法运算后得到的新密文 $C = \mathrm{mbFlatten}(C_1 + C_2)$。

e) 同态乘法算法 NFHE. Mult(C_1,C_2)。输入密文 C_1、C_2,输出进行同态乘法运算后得到的新密文 $C = \mathrm{mbFlatten}(C_1 \cdot C_2)$。

3　体制分析

3.1　正确性分析

首先,对同态加法和乘法的正确性进行分析。对同态加法,有 $\boldsymbol{C} = \mathrm{mbFlatten}((\mu_1 + \mu_2) \cdot \boldsymbol{I}_N + \mathrm{mbDmp}(\boldsymbol{C}_1 + \boldsymbol{C}_2))$,NFHE. Dec($\boldsymbol{sk}$,$\boldsymbol{C}$) $= (\mu_1 + \mu_2) \bmod 2$。每次同态加法运算后,噪声不超过原密文的两倍。

对同态乘法,有 $\boldsymbol{C} \cdot \boldsymbol{sk} = \mu_1 \cdot \mu_2 \cdot \boldsymbol{sk} + \mu_2 \cdot \boldsymbol{e}_1 + \boldsymbol{C}_1 \cdot \boldsymbol{e}_2$,NFHE. Dec($\boldsymbol{sk}$,$\boldsymbol{C}$) $= \mu_1 \cdot \mu_2$(其中 $\boldsymbol{e}_1$、$\boldsymbol{e}_2$ 表示密文 $\boldsymbol{C}_1$、$\boldsymbol{C}_2$ 中的噪声)。由于 μ_2 的系数为 $\{0,1\}$,$\boldsymbol{C}_1$ 的所有系数都限制在 $\mathbb{Z}_p$ 上,所以每次同态乘法后,噪声不超过原密文的 $pN+1$ 倍。

对于体制的正确性,有如下结论。

定理 1　对于 NFHE 体制,如果 $\boldsymbol{C}$ 是未进行同态运算的情况下加密 0 得到的密文,那么当 $|\langle \boldsymbol{C}_{m-1}, \boldsymbol{s}' \rangle| < q/[4p(pN+1)^l]$ 时,体制的正确性可以得到满足。

证明　根据对同态加法、乘法正确性的分析,每次同态运算后,噪声不超过原密文的 $pN+1$ 倍。因此当 $|\langle \boldsymbol{C}_{m-1}, \boldsymbol{s}' \rangle| < q/[4p(pN+1)^l]$ 时,在进行不超过 L 次同态运算后,$|\langle \boldsymbol{C}_{m-1}, \boldsymbol{s}' \rangle| < q/(4p)$。根据解密算法,当 $|\langle \boldsymbol{C}_{m-1}, \boldsymbol{s}' \rangle| < q/(4p)$ 时,有 $\langle \boldsymbol{s}', \boldsymbol{C}_{m-1} \rangle / (q/2p) < 1/2$。因此,如果加密的消息为 0,那么 $\langle \boldsymbol{C}_{m-1}, \boldsymbol{s}' \rangle$ 离 0 比 $q/(2p)$ 近,$\mu = \lfloor \langle \boldsymbol{s}', \boldsymbol{C}_{m-1} \rangle / (q/2p) + 1/2 \rfloor \bmod 2 < \lfloor 1/2 + 1/2 \rfloor \bmod 2 = 0$; 否则情况相反,即可保证体制解密的正确性。

接下来,验证 NFHE 体制是否满足以上结论。正确性,对于加密 0 所得的密文,有

$$\langle \boldsymbol{C}_{m-1}, \boldsymbol{s}' \rangle = \langle \boldsymbol{r}, \boldsymbol{s} \rangle + e_{m-1,2} - \langle \boldsymbol{e}_{m-1,1}, \boldsymbol{e} \rangle$$

因此,只要在参数选取时,令 q 足够大,即可满足正确性。

3.2　安全性分析

定理 2　设系统参数 $n = \mathrm{poly}(\lambda)$、$q = \mathrm{poly}(\lambda)$ 为安全参数 λ 的多项式,如果攻击者可以区分 NFHE 体制的密文和 $\mathbb{Z}_p^{m \times m}$ 上的均匀分布。那么攻击者就可以求解 $DLWE_{q,n,2n+1,\chi}$ 问题。因此如果假设该问题是困难的,那么 NFHE 体制就可以达到 IND-CPA 安全。

证明　本节通过如下的游戏序列证明该定理。

a) Game0。

初始化: 挑战者运行 NFHE. Keygen(n,q) 生成公私钥对 (pk,$\boldsymbol{sk}$),并将公钥给攻击者 A。

步骤 1: 攻击者可以自行或通过挑战者对消息 $\mu \in \{0,1\}$ 进行加密。若通过挑战者加密,则挑战者需正确返回密文。

挑战: 在某个时间点,攻击者向挑战者发起挑战,并发送挑战明文 $\mu_1, \mu_2 \in \{0,1\}$。挑战者随机选取 $b \in \{0,1\}$,运行 NFHE. Encrypt(pk,μ_b) 计算挑战密文 $\boldsymbol{C}$ 并发送给攻击者。

步骤 2: 同步骤 1 一样,攻击者可以自行或通过挑战者对消息 $\mu \in \{0,1\}$ 进行加密。

猜测: 攻击者对从挑战步骤中选取的挑战明文进行猜测,输出 $b' \in \{0,1\}$。

Game0 即为标准的 IND-CPA 攻击游戏,将攻击者的优势记做

$$\mathrm{Adv}_{\mathrm{CPA}}(A) = |Pr[A(pk, \mathrm{NFHE.Encrypt}(pk, \mu_0)) = 1] - Pr[A(pk, \mathrm{NFHE.Encrypt}(pk, \mu_1)) = 1]|$$

b) Game1。

在 Game1 中,挑战者在除初始化以外的阶段都与在 Game0 中相同。

初始化: 挑战者随机均匀选取 $A \xleftarrow{R} \mathbb{Z}_q^{(n+1) \times n}$ 作为公钥给攻击者 A。

将 Game1 中攻击者的优势记做 $\mathrm{Adv}_{\mathrm{Game1}}(A)$。

在 Game1 中,公钥不再通过私钥生成。由于 Game0 中的公钥可以看做 $n \times 1$ 个 $LWE_{q,n,\chi}$ 实例,Game1 中的公钥随机取自均匀分布,所以以不可忽略的优势区分 Game0 和 Game1 和以不可忽略的优势求解 $DLWE_{q,n,n,\chi}$ 问题是等价的。如果 $DLWE_{q,n,n,\chi}$ 假设成立,则攻击者区分 Game0 和 Game1 的优势可忽略,有

$$\mathrm{Adv}_{\mathrm{CPA}}(A) = \mathrm{Adv}_{\mathrm{Game1}}(A) + \mathrm{negl}(\lambda)$$

c) Game2。

在 Game2 中,挑战者在除挑战以外的阶段都与在 Game1 中相同。

挑战: 在某个时间点,攻击者向挑战者发起挑战,并发送挑战明文 $\mu_1, \mu_2 \in \{0,1\}$。挑战者随机选取 $b \in \{0,1\}$,

$\boldsymbol{C} \xleftarrow{R} \mathbb{Z}_q^{n+1}$，将 $\boldsymbol{c}' = \boldsymbol{c} + (\boldsymbol{o}, \mu \cdot \lfloor q/2 \rfloor)$ 作为挑战密文发送给攻击者。

将 Game2 中攻击者的优势记做 $\mathrm{Adv}_{\mathrm{Game2}}(A)$。

在 Game2 中，挑战密文不再通过公钥计算。由于 Game1 中的挑战密文可以看做 $n+1$ 个 $LWE_{q,n,\chi}$ 实例，Game2 中的挑战密文随机取自均匀分布，所以以不可忽略的优势区分 Game1 和 Game2 与以不可忽略的优势求解 $DLWE_{q,n,n+1,\chi}$ 问题是等价的。如果 $DLWE_{q,n,n+1,\chi}$ 假设成立，那么攻击者区分 Game1 和 Game2 的优势可忽略，则有

$$\mathrm{Adv}_{\mathrm{Game1}}(A) \leqslant \mathrm{Adv}_{\mathrm{Game2}}(A) + \mathrm{negl}(\lambda)$$

d) Game3。

在 Game3 中，挑战者在除挑战以外的阶段都与在 Game2 中相同。

挑战：在某个时间点，攻击者向挑战者发起挑战，并发送挑战明文 $\mu_1, \mu_2 \in \{0,1\}$。挑战者随机选取 $b \in \{0,1\}$，$\boldsymbol{C} \xleftarrow{R} \mathbb{Z}_q^{n+1}$，将 $\boldsymbol{C}$ 作为挑战密文发送给攻击者。

将 Game3 中攻击者的优势记做 $\mathrm{Adv}_{\mathrm{Game3}}(A)$。

在 Game3 中，公钥和挑战密文都取自均匀分布，且不包含明文的任何信息，所以 $\mathrm{Adv}_{\mathrm{Game3}}(A) = 0$。由于 Game2 和 Game3 中的 $\boldsymbol{C}$ 均取自 $\mathbb{Z}_q^{n+1}$ 上的均匀分布，所以 Game2 的 $\boldsymbol{C}'$ 和 Game3 的 $\boldsymbol{C}$ 是统计不可区分的，即

$$\mathrm{Adv}_{\mathrm{Game2}}(A) \leqslant \mathrm{Adv}_{\mathrm{Game3}}(A) + \mathrm{negl}(\lambda)$$

由于 $\mathrm{Adv}_{\mathrm{Game3}}(A) = 0$，所以，若 $DLWE_{q,n,2n+1,\chi}$ 假设成立，那么 $\mathrm{Adv}_{\mathrm{CPA}}(A) = \mathrm{negl}(\lambda)$，NFHE 体制是 IND-CPA 安全的。

3.3 基于多比特加密的优化

由于 GSW13 体制是针对单个比特进行加密，所以导致该体制效率较低。为了进一步提高本文 NFHE 体制的效率，本节采用多比特加密模式对 NFHE 体制进行优化。

在 GSW13 体制和第 2 章构造的 NFHE 体制中，虽然明文消息均为 $\mu \in \{0,1\}$，但 GSW13 体制无法在系统参数不变的情况下支持多比特加密[17]。本文可以在不改变系统参数的情况下，通过如下修改使得 NFHE 体制实现多比特加密。

加密算法 NFHE.Encrypt(pk, μ)：对于要加密的明文 $\mu \in \mathbb{Z}_p$，随机选取 $\boldsymbol{r}_i, \boldsymbol{e}_{i,1} \leftarrow \chi^n, e_{i,2} \leftarrow \chi, i = 1, \cdots, (n+1) \cdot t$，计算 $C_{i,1} = \boldsymbol{A}^{\mathrm{T}} \cdot \boldsymbol{r}_i + \boldsymbol{e}_{i,1} \in \mathbb{Z}_q^n$，$C_{i,2} = \boldsymbol{b}^{\mathrm{T}} \cdot \boldsymbol{r}_2 + e_{i,2} \in \mathbb{Z}_q$。令 $\boldsymbol{C}'$ 为由 $m = (n+1) \cdot t$ 个密文作为列向量排列而成的矩阵，其维数为 $(n+1) \times m$，输出密文 $\boldsymbol{C} = \mathrm{mbFlatten}(\mu \cdot \boldsymbol{I}_N + \mathrm{mbDpt}(\boldsymbol{C}')) \in \mathbb{Z}_p^{m \times m}$。

解密算法 NFHE.Decrypt$(\boldsymbol{sk}, \boldsymbol{C})$：对于密文 $\boldsymbol{C} \in \mathbb{Z}_p^{m \times m}$ 和私钥 $\boldsymbol{sk} = \begin{pmatrix} -\boldsymbol{s} \\ 1 \end{pmatrix} \in \mathbb{Z}_q^{n+1}$，令 $\boldsymbol{s}' = \mathrm{pofmb}(\boldsymbol{sk})$，计算并输出明文 $\mu = \lfloor \langle \boldsymbol{s}', \boldsymbol{C}_{m-1} \rangle / (q/2p) + 1/2 \rfloor \bmod p$。

在未进行同态运算的情况下，若明文消息为 μ'，根据加/解密流程，解密后有 $\mu = \lfloor \langle \boldsymbol{s}', \boldsymbol{C}_{m-1} \rangle / (q/2p) + 1/2 \rfloor \bmod p = \lfloor \mu' + \boldsymbol{e}/(q/2p) + 1/2 \rfloor \bmod p$，当 $|\boldsymbol{e}/(q/2p)| < 1/2$ 时，有 $\mu = \mu'$，可以正确解密。

对同态加法，有 $\boldsymbol{C} = \mathrm{mbFlatten}((\mu_1 + \mu_2) \cdot \boldsymbol{I}_N + \mathrm{mbDmp}(\boldsymbol{C}_1 + \boldsymbol{C}_2))$，NFHE.Dec$(\boldsymbol{sk}, \boldsymbol{C}) = (\mu_1 + \mu_2) \bmod p$。

对同态乘法，有 $\boldsymbol{C} \cdot \boldsymbol{sk} = \mu_1 \cdot \mu_2 \cdot \boldsymbol{sk} + \mu_2 \cdot \boldsymbol{e}_1 + \boldsymbol{C}_1 \cdot \boldsymbol{e}_2$，NFHE.Dec$(\boldsymbol{sk}, \boldsymbol{C}) = \mu_1 \cdot \mu_2$。

因此在进行同态运算后，同样可以做到正确解密。

在进行同态乘法后，由于 μ_2 的系数属于 $\mathbb{Z}_p$，$\boldsymbol{C}_1$ 的所有系数都限制在 $\mathbb{Z}_p$ 上，所以噪声不超过原密文的 $pN + p$ 倍。因此在进行多比特加密的情况下，定理 1 对噪声的限制变为 $|\langle \boldsymbol{C}_{m-1}, \boldsymbol{s}' \rangle| < q/(4p(pN+p)^L)$。由于 $pN = pkt >> p$，所以这一变动对于模数 q 的影响可以忽略不计。

3.4 效率分析

NFHE 与 GSW13 体制相比，虽然两者使用的都是近似特征向量技术，但是本文通过修改 GSW13 体制的展开方式，对其密文尺寸 $(n+1)^2 \lceil \log q \rceil^2$ 进行改进，得到 NFHE 体制的密文尺寸为 $(n+1)^2 \lceil \log q \rceil^2 / \lceil \log p \rceil$。

表 1 给出了 NFHE 与 GSW13 体制的效率对比。令 $n = 512$，GSW13 体制的公钥尺寸为 $n(n+1) \lceil \log q \rceil \approx 7.26$ MB，私钥尺寸为 $(n+1) \lceil \log q \rceil \approx 14.53$ KB，密文尺寸为 $(n+1)^2 \lceil \log q \rceil^2 \approx 211.07$ MB，加密运算量为 $n \lceil \log q \rceil \approx 18848$；NFHE 体制的公钥尺寸为 $n(n+1) \lceil \log q \rceil \approx 9.02$ MB，私钥尺寸为 $(n+1) \lceil \log q \rceil \approx 18.04$ KB，密文尺寸为 $(n+1)^2 \times \lceil \log q \rceil^2 / \lceil \log p \rceil \approx 81.32$ MB，加密运算量为 $n \lceil \log q \rceil / \lceil \log p \rceil \approx 4608$。

表 1 全同态加密体制效率对比

Tab. 1 Comparison of the efficiency of the fully homo-morphic encryption schemes

体制	n	$\log q$	公钥尺寸/MB	私钥尺寸/KB	密文尺寸/MB	加密运算量/次	解密运算量/次	支持多比特加密
GSW13	512	29	7.26	14.53	211.07	14 848	512	否
NFHE	512	36	9.02	18.04	81.32	4 608	512	是

通过表 1 中两种体制的对比可以看出，虽然 NFHE 体制的密钥尺寸略微增大，但是其密文尺寸比 GSW13 体制大幅度减小了 61.47%，其加密运算量比 GSW13 体制大幅度降低了 68.97%。由于体制的密文尺寸远大于密钥尺寸，所以 NFHE 体制通过大幅度压缩密文尺寸，有效减少了体制的存储开销，提高了体制效率。

与 GSW13 体制相比，基于多比特加密的优化 NFHE 体制进一步减小了密文扩张。此外，在实际应用中，采用单比特加密的 GSW13 体制需要进行 $\log^2 p$ 次同态乘法运算，才可以实现 $\log p$ 比特的同态乘法运算，而 NFHE 体制则通过采用多比特加密，大幅度减少了同态运算计算次数，从而进一步提高了体制效率。

4 结束语

针对全同态加密体制 GSW13 存在的因密文尺寸较大和采用单比特加密所导致的效率较低问题，本文提出了一种支持多比特加密的、基于 DLWE 的全同态加密体制 NFHE，将 NFHE 体制的安全性经典归约到 DLWE 问题的难解性，并在随机喻示模型下给出了严格的体制安全证明。下一步工作将围绕现有全同态加密体制普遍存在的公钥尺寸大的缺陷，综合利用基于身份加密和全同态加密这两种密码体制的优势[32~36]，研究更高效的基于身份的全同态加密体制，旨在有效克服公钥尺寸对于全同态加密体制实际应用效率的影响。

参考文献：

[1] Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms [J]. Foundations of Secure Computation, 1978, 4: 169-179.

[2] Gentry C. Fully homomorphic encryption using ideal lattices [C] // Proc of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 169-178.

[3] 李增鹏，马春光，周红生. 全同态加密研究 [J]. 密码学报，2017，4(6)：561-578. (Li Zengpeng, Ma Chunguang, Zhou Hongsheng. Overview on fully homomorphic encryption [J]. Journal of Cryptologic Research, 2017, 4(6): 561-578.)

[4] Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and security for key dependent messages [C] // Proc of the 31st Annual International Cryptology Conference. Berlin: Springer, 2011: 505-524.

[5] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from(standard) LWE [J]. SIAM Journal on Computing, 2014, 43(2) : 831-871.

[6] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) Fully homomorphic encryption without BootStrapping [J]. ACM Trans on Computation Theory, 2011, 18(3) : 169-178.

[7] 汤殿华,祝世雄,王林,等. 基于 RLWE 的全同态加密方案 [J]. 通信学报, 2014, 35(1) : 173-182. (Tang Dianhua, Zhu Shixiong, Wang Lin, *et al*. Fully homomorphic encryption scheme from RLWE [J]. Journal on Communications, 2014, 35(1) : 173-182.)

[8] Naehrig M, Lauter K, Vaikuntanathan V. Can homomorphic encryption be practical? [C] //Proc of the 3rd ACM Workshop on Cloud Computing Security Workshop. New York: ACM Press, 2011: 113-124.

[9] Gentry C, Halevi S, Smart N P. Homomorphic evaluation of the AES circuit [C] //Proc of the 32nd Annual International Cryptology Conference. Berlin: Springer, 2012: 850-867.

[10] Gentry C, Groth J, Ishai Y, *et al*. Using fully homomorphic hybrid encryption to minimize non-interatcive zero-knowledge proof [J]. Journal of Cryptology, 2015, 28(4) : 820-843.

[11] Ducas L, Micciancio D. FHEW: BootStrapping homomorphic encryption in less than a second [C] //Proc of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2015: 617-640.

[12] Peikert C, Shiehian S. Multi-key FHE from LWE, revisited [C] //Proc of the 13th IACR Theory of Cryptography Conference. Berlin: Springer, 2016: 217-238.

[13] Benhamouda F, Lepoint T, Mathieu C, *et al*. Optimization of BootStrapping in circuits [C] //Proc of the 28th Annual ACM-SIAM Symposium on Discrete Algorithms. New York: ACM Press, 2017: 2423-2433.

[14] 李子臣,张卷美,杨亚涛,等. 基于 NTRU 的全同态加密方案 [J]. 电子学报, 2018, 46(4) : 938-944. (Li Zichen, Zhang Juanmei, Yang Yatao, *et al*. A fully homomorphic encryption scheme based on NTRU [J]. Acta Electronica Sinica, 2018, 46(4) : 938-944.)

[15] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from(standard) LWE [C] //Proc of the 52nd Annual Symposium on Foundations of Computer Science. Piscataway, NJ: IEEE Press, 2011: 97-106.

[16] Regev O. On lattices, learning with errors, random linear codes, and cryptography [C] //Proc of the 37th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2005: 84-93.

[17] Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based [C] //Proc of the 33rd Annual International Cryptology Conference. Berlin: Springer, 2013: 75-92.

[18] Brakerski Z, Vaikuntanathan V. Lattice-based FHE as secure as PKE [C] //Proc of the 5th Conference on Innovations in Theoretical Computer Science. New York: ACM Press, 2014: 1-12.

[19] Alperin-Sheriff J, Peikert C. Faster BootStrapping with polynomial error [C] //Proc of the 34th Annual International Cryptology Conference. Berlin: Springer, 2014: 297-314.

[20] 古春生. 近似理想格上的全同态加密方案 [J]. 软件学报, 2015, 26(10) : 2696-2719. (Gu Chunsheng. Fully homomorphic encryption from approximate ideal lattices [J]. Journal of Software, 2015, 26(10) : 2696-2719.)

[21] Halevi S, Shoup V. BootStrapping for HElib [C] //Proc of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2015: 641-670.

[22] Brakerski Z, Perlman R. Lattice-based fully dynamic multi-key FHE with short ciphertexts [C] //Proc of the 36th Annual International Cryptology Conference. Berlin: Springer, 2016: 190-213.

[23] 陈智罡,宋新霞,赵秀凤. 一个 LWE 上的短公钥多位全同态加密方案 [J]. 计算机研究与发展, 2016, 53(10) : 2216-2223. (Chen Zhigang, Song Xinxia, Zhao Xiufeng. A multi-bit fully homomorphic encryption with better key size from LWE [J]. Journal of Computer Research and Development, 2016, 53(10) : 2216-2223.)

[24] 姬晨,蔡斌,向宏,等. 一种基于 LWE 问题的布尔电路同态加密方案 [J]. 密码学报, 2017, 4(3) : 229-240. (Ji Chen, Cai Bin, Xiang Hong, *et al*. A Boolean circuit homomorphic encryption scheme based on LWE problem [J]. Journal of Cryptologic Research, 2017, 4(3) : 229-240.)

[25] Brakerski Z, Gentry C, Halevi S. Packed ciphertexts in LWE-based homomorphic encryption [C] //Proc of International Conference on Practice and Theory in Public-Key Cryptography. Berlin: Springer, 2013: 1-13.

[26] Li Zengpeng, Ma Chunguang, Eduardo M, *et al*. Multi-bit leveled homomorphic encryption via dual. LWE-based [C] //Proc of the 12th International Conference on Information Security and Cryptology. Berlin: Springer, 2016: 221-242.

[27] Peikert C. Public-key cryptosystems from the worst-case shortest vector problem [C] //Proc of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 333-342.

[28] Brakerski Z, Langlois A, Peikert C, *et al*. Classical hardness of learning with errors [C] //Proc of ACM Symposium on Theory of Computing. New York: ACM Press, 2013: 575-584.

[29] 吕海峰,丁勇,代洪艳,等. LWE 上的全同态加密方案研究 [J]. 信息网络安全, 2015, 15(1) : 32-38. (Lyu Haifeng, Ding Yong, Dai Hongyan, *et al*. Survey on LWE-based fully homomorphic encryption scheme [J]. Netinfo Security, 2015, 15(1) : 32-38.)

[30] 王志刚,马春光,史晓倩. 基于 binary LWE 的全同态加密方案研究 [J]. 信息网络安全, 2015, 15(7) : 41-50. (Wang Zhigang, Ma Chunguang, Shi Xiaoqian. Research on full homomorphic encryption scheme based on binary LWE [J]. Netinfo Security, 2015, , 15(7) : 41-50.)

[31] Gentry C. A fully homomorphic encryption scheme [D]. Stanford: Stanford University, 2009.

[32] 辛丹,顾纯祥,郑永辉,等. 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) : 2887-2893. (Xin Dan, Gu Chunxiang, Zheng Yonghui, *et al*. Identity-based fully homomorphic encryption from ring learning with errors problem [J]. Acta Electronica Sinica, 2016, 44(12) : 2887-2893.)

[33] 康元基,顾纯祥,郑永辉,等. 利用特征向量构造基于身份的全同态加密体制 [J]. 软件学报, 2016, 27(6) : 1487-1497. (Kang Yuanji, Gu Chunxiang, Zheng Yonghui, *et al*. Identity-based fully homomorphic encryption from eigenvector [J]. Journal of Software, 2016, 27(6) : 1487-1497.)

[34] 汤永利,胡明星,刘琨,等. 新的格上基于身份的全同态加密方案 [J]. 通信学报, 2017, 38(5) : 39-47. (Tang Yongli, Hu Mingxing, Liu Kun, *et al*. Novel identity-based fully homomorphic encryption scheme from lattice [J]. Journal on Communications, 2017, 38(5) : 39-47.)

[35] 叶青,胡明星,汤永利,等. 基于 LWE 的高效身份基分级加密方案 [J]. 计算机研究与发展, 2017, 54(10) : 2193-2204. (Ye Qing, Hu Mingxing, Tang Yongli, *et al*. Efficient hierarchical identity-based encryption scheme from learning with errors [J]. Journal of Computer Research and Development, 2017, 54(10) : 2193-2204.)

[36] 段然,顾纯祥,祝跃飞,等. 一种 NTRU 格上基于身份全同态加密体制设计 [J]. 电子学报, 2018, 46(10) : 2410-2417. (Duan Ran, Gu Chunxiang, Zhu Yuefei, *et al*. An identity-based fully homomorphic encryption over NTRU lattice [J]. Acta Electronica Sinica, 2018, 46(10) : 2410-2417.)