计算机科学
COMPUTER SCIENCE

**基于高效全同态加密的安全多方计算协议**

朱宗武，黄汝维

引用本文

朱宗武，黄汝维. 基于高效全同态加密的安全多方计算协议[J]. 计算机科学, 2022, 49(11): 345-350.

ZHU Zong-wu, HUANG Ru-wei. Secure Multi-party Computing Protocol Based on Efficient Fully Homomorphic Encryption[J]. Computer Science, 2022, 49(11): 345-350.

---

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210900047

# 基于高效全同态加密的安全多方计算协议

朱宗武　黄汝维
广西大学计算机与电子信息学院　南宁 530004
(zongwuzhu@st.gxu.edu.cn)

**摘　要**　针对目前基于全同态加密的安全多方计算协议存在的密文尺寸大、效率较低的问题,文中证明了 Chen 等提出的支持多比特加密的全同态加密方案满足密钥同态性,基于该方案和门限解密设计了一个在公共随机串模型下的 3 轮交互的高效安全多方计算协议。该协议由非交互的零知识证明可以得出协议在恶意模型下是安全的,其安全性可归结为容错学习问题的变种问题 Some-are-errorless LWE。与现有的在 CRS 模型下的协议相比,该协议支持多比特加密,能有效降低与非门复杂度;同时密文尺寸较小,减少了运算量,从而提高了时间与空间效率。

**关键词**:全同态加密;安全多方计算;多比特加密;门限解密;容错学习问题
**中图法分类号**　TP309

## Secure Multi-party Computing Protocol Based on Efficient Fully Homomorphic Encryption

ZHU Zong-wu and HUANG Ru-wei
School of Computer and Electronic Information,Guangxi University,Nanning 530004,China

**Abstract**　In view of the problem of large ciphertext size and low efficiency of the current secure multi-party computation protocol based on fully homomorphic encryption,this paper proves that the fully homomorphic encryption scheme that supports multi-bit encryption proposed by Chen et al. satisfies the key homomorphism. Based on this scheme and threshold decryption,an efficient and secure multi-party computation protocol with three rounds of interaction under the common random string(CRS) model is designed. The protocol can be concluded from the non-interactive zero knowledge proof that the protocol is safe under the malicious model,and its security can be boiled down to the variants of the learning with errors problem(LWE). Compared with the existing protocol of the CRS model,the protocol supports multi-bit encryption,which can effectively reduce the complexity of the NAND gate. At the same time,the size of the ciphertext is smaller,the amount of calculation is reduced,and the time and space efficiency are improved.

**Keywords**　Fully homomorphic encryption,Secure multi-party computation,Multi-bit encryption,Threshold decryption,Learning with errors

随着云计算的迅速发展,用户数据的隐私安全问题日益突出,全同态加密(Fully Homomorphic Encryption,FHE)的出现正好解决了数据的隐私计算问题。全同态加密最早由 Rivest 等[1]于 1978 年提出,它可以在不知道密钥的情况下对密文进行各种有意义的计算,即对任意明文 $m$ 和函数 $f$,有 $f(Enc(m))=Enc(f(m))$。从 2009 年 Gentry[2]提出第一个 FHE 方案开始,先后出现了众多 FHE 方案,如 BV11[3],BGV12[4],Bra12[5],GSW13[6],CKKS17[7]等。由于 FHE 方案能够直接对密文进行运算,在多个用户想要进行安全的联合计算场景中能够有效地保护数据不被泄露和篡改,因此利用 FHE 方案来构造安全多方计算(Secure Multi-party Computation,SMC)协议具有天然的优势。安全多方计算的概念来源于 Yao[8]提出的百万富翁问题,其一般形式化定义[9]可以描述为:假设有 $N$ 个参与方 $\{P_1,P_2,\cdots,P_N\}$,$x_i(i\in[N])$ 是每个参与方 $P_i$ 拥有的私人数据,所有参与方共同计算某个有效函数 $y=f(x_1,x_2,\cdots,x_N)$。计算结束后,每个 $P_i$ 都能够得到 $y$,但无法得到其他参与者的私人数据。

近年来,国内外学者对基于全同态加密方案的安全多方计算协议展开了大量的研究。2012 年,López-Alt 等[9]基于改进的 NTRU 方案[10]构造了一个多密钥全同态加密(Multi-key Fully Homomorphic Encryption,MFHE)的方案,该方案能够对在多个无关密钥下加密的输入进行操作,但是复杂度太高。2016 年,Mukherjee 等(MW16 方案)[11]基于 LWE 假设实现在公共随机串(Common Random String,CRS)模型下仅进行 2 轮交互的多密钥安全多方计算协议,达到最佳的交互轮次,但密文矩阵体积过大。2017 年,Wang 等[12]基于 GSW13 方案构造了一个在 CRS 模型下简单的 3 轮层次型多密钥安全多方计算协议,该协议相比 MW16 方案虽然增加了

到稿日期:2021-09-06　返修日期:2022-03-11
基金项目:国家自然科学基金(62062009);广西科技重大专项资助项目(AA17204058-17,AA18118047-7)
This work was supported by the National Natural Science Foundation of China(62062009)and Guangxi Innovation-Driven Development Project(AA17204058-17,AA18118047-7).
通信作者:黄汝维(ruweih@gxu.edu.cn)

一轮交互，但加解密复杂度低，密文膨胀率小并且不需要运行密钥。2018 年，针对 CRS 模型下的安全多方计算协议削弱了用户独立生成自己的密钥的能力问题，Kim 等（KLP18 方案）[13]构建了一个无 CRS 的 3 轮安全多方计算协议，该协议对半恶意对手是安全的，但无法对抗完全恶意敌手。2020 年，Tang 等[14]利用 Li 的方案[15]中的编码操作改进了 KLP18 方案的密文扩展方式，设计了一个基于多密钥全同态加密的无 CRS 模型的 3 轮安全多方计算协议，该协议提高了效率，降低了解密噪音，但同样无法证明在全恶意环境下是安全的。2021 年，Tang 等[16]证明了 Li 提出的多比特全同态加密方案[17]的密钥同态性，基于该方案设计了一个在 CRS 模型下的能够支持多比特加密的 3 轮安全多方计算协议，进一步降低了与非门复杂度。

由上述相关工作可知，虽然无 CRS 模型下的安全多方计算协议允许多密钥全同态加密用户独立生成自己的密钥，但该模型下的安全多方计算协议安全性不够高，无法抵抗完全恶意敌手。而目前 CRS 模型下基于全同态加密的安全多方计算协议存在密文尺寸过大、效率不高等问题。本文针对以上问题，利用 Chen 等[18]提出的 NFHE 方案和门限式解密，设计一个在 CRS 模型下可抵抗恶意敌手的 3 轮安全多方计算协议。该协议支持多比特加密，与现有的在 CRS 模型下的安全多方计算协议相比，协议密文尺寸较小，整体性能优于现有协议。

## 1 基础知识

### 1.1 符号与基础概念

相关符号及其意义如表 1 所列，其中，加粗斜体小写字母代表向量，加粗斜体大写字母代表矩阵。

表 1 符号及其含义

Table 1 Symbols and their meanings

| 符号 | 意义 |
|---|---|
| $\mathbb{R}$ | 实数集 |
| $\mathbb{Z}$ | 整数集 |
| $\mathbb{Z}_q$ | 整数模 $q$ 剩余类环 |
| $\|\boldsymbol{a}\|$ | $n$ 维向量 $\boldsymbol{a}$ 的长度为其欧几里德范数 $\|\boldsymbol{a}\|=\sqrt{\sum_{i=0}^{n-1}\boldsymbol{a}_i^2}$ |
| $\|S\|$ | 向量集 $S$ 的长度 $\|S\|=\max_{a\in S}\|\boldsymbol{a}\|$ |
| $\boldsymbol{a}\leftarrow D$ | 从概率分布 $D$ 中随机选取变量 $\boldsymbol{a}$ |
| $\boldsymbol{a}\xleftarrow{R}A$ | 从集合 $A$ 中随机均匀选取变量 $\boldsymbol{a}$ |
| $\boldsymbol{C}_i$ | 矩阵 $\boldsymbol{C}$ 的第 $i$ 行 |
| $\mathbf{I}_n$ | $n$ 维单位矩阵 |
| $\varphi(y)$ | 概率 $Pr[y\leqslant x\|yN(0,1)]$ |

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 $b=(b_0,\cdots,b_{n-1})$。对于多项式 $b,c\in R$，定义 $b\times c=bc \bmod (x^n+1)$。

在本文中，$\log n$ 表示 $\log_2 n$。$O$ 和 $o$ 表示计算复杂度，同时对于 $poly(\cdot)$ 和 $negl(\cdot)$，如果 $f(n)=O(n^c)$，则 $f(n)$ 可表示为 $poly(n)$。若对于任意的常数 $c$，都存在 $f(n)=o(n^{-c})$，则 $f(n)$ 可表示为 $negl(n)$，$n$ 为可忽略函数。

**定义 1** 称一个基于整数集的分布序列 $\{\chi_n\}_{n\in N}$ 为 $B_\chi$ 有界的，如果满足：

$$\Pr_{x\leftarrow\chi_n}[|x|\geqslant B]=negl(\lambda) \tag{1}$$

其中，每一个分布 $\chi_n$ 都被称为一个 $B_\chi$ 有界分布。

**定理 1** 设 $e_i(i\in[N])$ 为一系列服从某个 $B_\chi$ 有界分布的独立随机变量，则随机变量 $e=\frac{1}{N}\sum_{i=1}^{N}e_i$ 也服从该 $B_\chi$ 有界分布。

### 1.2 Some-are-errorless LWE 问题

Regev[19]提出容错学习问题（Learning With Errors，LWE）的一个量子规约，Wang 等[12]将该概念进行了扩展，考虑了带有多个等式约束的 LWE 问题的困难性，提出了 Some-are-errorless LWE 问题。

**定义 2** Some-are-errorless LWE

设 $n\geqslant 1$ 为维数，$q\geqslant 2$ 为模，$l\geqslant 1$ 为整数，$\chi$ 为 $R$ 上的误差分布。$A_{s,\chi}$ 是 $\boldsymbol{T}_q^n\times\boldsymbol{T}_q$ 上按照如下方式构造的概率分布：均匀随机选取 $\boldsymbol{a}\in T_q^n$，依分布 $\chi$ 选择误差 $\boldsymbol{e}\leftarrow\chi$，然后输出 $(\boldsymbol{a},\langle\boldsymbol{a},\boldsymbol{s}\rangle+\boldsymbol{e})$。

搜索版本的 Some-are-errorless LWE 问题是：给定 $l$ 个来自分布 $A_{s,0}$ 的独立样本和任意个来自 $A_{s,\chi}$ 的独立样本，输出秘密向量 $\boldsymbol{s}\in\boldsymbol{T}_q^n$。

判定版本（表示为 $DLWE_{n,l,q,\chi}$）的目标是以不可忽略的优势区分以下两种情况：在第一种情况中，均匀随机选择向量 $\boldsymbol{s}\in\boldsymbol{T}_q^n$，从分布 $A_{s,0}$ 中选取 l 个样本，然后从 $A_{s,\chi}$ 中选取随意的多个样本。在第二种情况中，从 $\boldsymbol{T}_q^n\times\boldsymbol{T}_q$ 中均匀随机选取所有样本。

### 1.3 安全多方计算模型

在安全多方计算协议中，根据参与者执行协议和被腐败者篡改协议的情况，有半诚实模型、半恶意模型和恶意模型 3 种计算模型。

(1)半诚实模型：所有参与者将严格遵守协议，不会主动改变协议或数据，但是可能会保留中间计算结果并用于计算其他参与者的私人数据。

(2)半恶意模型：敌手可以根据输入和一定的随机性来决定是否忠实地执行原始协议。

(3)恶意模型：所有计算参与者能够随意篡改、泄露协议和数据，甚至阻止协议的正常执行。

## 2 高效全同态加密方案

该方案是文献[18]基于 GSW13 进行改进的 NFHE 方案。该方案的构造如下：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 $\boldsymbol{sk}$ 为定义在 $\mathbb{Z}_p$ 上的 $N$ 维向量。令明文 $\mu$ 为小的整数，当 $\boldsymbol{C}\cdot\boldsymbol{sk}=\mu\cdot\boldsymbol{sk}+\boldsymbol{e}$ 时，则称 $\boldsymbol{C}$ 为 $\mu$ 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 $\boldsymbol{C}_i$，接着计算 $x\leftarrow\langle\boldsymbol{C}_i,\boldsymbol{sk}\rangle=\mu\cdot sk_i+e_i$，最后输出 $\mu=\lfloor x/sk_i\rfloor$，其中 $sk_i$ 为 $\boldsymbol{sk}$ 的第 $i$ 个元素，$e_i$ 为 $\boldsymbol{e}$ 的第 $i$ 个元素，$i\in[0,N-1]$。消息 $\mu$ 可被视为密文矩阵 $\boldsymbol{C}$ 的一个特征值，私钥 $\boldsymbol{sk}$ 为 $\boldsymbol{C}$ 对应于特征值 $\mu$ 的近似特征向量。

构造思路如下：首先定义 $mbDpt(\boldsymbol{a})$，$mbDpt^{(-1)}(\boldsymbol{a}')$，$mbFlatten(\boldsymbol{a}')$，$pofmb(\boldsymbol{b})$等函数，给出 NFHE 方案的展开方式；基于上述函数设计 NFHE 方案包含的 5 个多项式时间算法，分别为密钥生成算法 NFHE.Keygen$(n,q)$、加密算法 NFHE.Encrypt$(\boldsymbol{pk},\mu)$、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$(C_1,C_2)$。

令 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 为 $\mathbb{Z}_q^k$ 上的向量，$k$ 为正整数，$q$ 为模数，$p$ 为 2 的方幂，$t=\lceil \log_p q \rceil$，$N=kt$。各个函数的定义如下式所示：

$$mbDpt(\boldsymbol{a})=\boldsymbol{a}'=(a_{1,1},\cdots,a_{1,t},\cdots,a_{k,1},\cdots,a_{k,t})\in \mathbb{Z}_p^N \tag{2}$$

$\boldsymbol{a}'$ 为 $N$ 维向量，其中 $a_i=\sum_{j=1}^{t} a_{i,j}p^{j-1}$，$a_{i,j}\in \mathbb{Z}_p$。

$$mbDpt^{(-1)}(\boldsymbol{a}')=(\sum p^j\cdot a_{1,j},\cdots,\sum p^j\cdot a_{k,j}) \tag{3}$$

$$mbFlatten(\boldsymbol{a}')=mbDpt(mbDpt^{(-1)}(\boldsymbol{a}')) \tag{4}$$

$$pofmb(\boldsymbol{b})=(b_1,pb_1,\cdots,p^{t-1}b_1,\cdots,b_k,pb_k,\cdots,p^{t-1}b_k) \tag{5}$$

(1)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 $\boldsymbol{pk}=(\boldsymbol{A},\boldsymbol{b}=\boldsymbol{A}\cdot\boldsymbol{s}+\boldsymbol{e})\in\mathbb{Z}_q^{n\times n}\times\mathbb{Z}_q^n$，私钥为 $\boldsymbol{sk}=\begin{pmatrix}-\boldsymbol{s}\\1\end{pmatrix}\in\mathbb{Z}_q^{n+1}$。

(2)加密算法 NFHE.Encrypt($\boldsymbol{pk},\mu$)。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 $\boldsymbol{C}=mbFlatten(\boldsymbol{\mu}\cdot\mathbf{I}_N+mbDpt(\boldsymbol{C}'))\in\mathbb{Z}_p^{m\times m}$。

(3)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 $\boldsymbol{s}'=pofmb(\boldsymbol{sk})$，计算并输出明文 $\mu=\left\lfloor\langle\boldsymbol{s}',C_{m-1}\rangle/(q/2p)+\frac{1}{2}\right\rfloor \bmod 2$。

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

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

### 2.1 方案正确性

首先，对方案的同态加法和乘法的正确性进行分析。对同态加法，有：

$$\boldsymbol{C}=mbFlatten((\mu_1+\mu_2)\cdot\mathbf{I}_N+mbDmp(C_1+C_2)) \tag{6}$$

$$NFHE.Dec(\boldsymbol{sk},\boldsymbol{C})=(\mu_1+\mu_2)\bmod 2 \tag{7}$$

每次方案执行同态加法后，噪声不超过原密文的两倍。对同态乘法，有 $\boldsymbol{C}\cdot\boldsymbol{sk}=\mu_1\cdot\mu_2\cdot\boldsymbol{sk}+\mu_2\cdot\boldsymbol{e}_1+C_1\cdot\boldsymbol{e}_2$，$NFHE.Dec(sk,C)=\mu_1\cdot\mu_2$（其中 $\boldsymbol{e}_1$ 和 $\boldsymbol{e}_2$ 表示密文 $C_1$ 和 $C_2$ 中的噪声）。由于 $\mu_2$ 的系数为 $\{0,1\}$，$C_1$ 的系数受限于 $\mathbb{Z}_p$，故每次执行同态乘法后，噪声不超过原密文的 $pN+1$ 倍。

**定理 2** 对于 NFHE 方案，在未进行同态运算的情况下，如果 $\boldsymbol{C}$ 是加密 0 得到的密文，那么当 $|\langle C_{m-1},\boldsymbol{s}'\rangle|<q/[4p(pN+1)^L]$ 时，方案是正确的，详细证明见参考文献[18]。对于加密 0 所得的密文，有：

$$\langle C_{m-1},\boldsymbol{s}'\rangle=\langle\boldsymbol{r},\boldsymbol{s}\rangle+e_{m-1,2}-\langle e_{m-1,1},\boldsymbol{e}\rangle \tag{8}$$

因此，只要选取适当的参数 $q$，令其足够大便可满足其正确性。

### 2.2 方案安全性

**定理 3** 设参数 $n=poly(\lambda)$ 和 $q=poly(\lambda)$ 为安全参数 $\lambda$ 的多项式，假设攻击者能以不可忽略的优势区分 NFHE 方案的密文和 $\mathbb{Z}_p^{m\times m}$ 上的均匀分布，则同样能求解 $DLWE_{q,n,2n+1,\chi}$ 问题。故假设该问题是困难的，那么 NFHE 方案就可以达到选择明文(IND-CPA)的安全性，详细证明见参考文献[18]。

### 2.3 基于多比特加密的优化

在 GSW13 方案和前面构造的 NFHE 方案中，虽然明文消息均为 $\mu\in\{0,1\}$，但在系统参数不变的情况下，GSW13 方案无法支持多比特加密[17]。NFHE 方案将加密算法 NFHE.Encrypt($pk,\mu$)中明文的取值由原来的 $\mu\in\{0,1\}$ 修改为 $\mu\in\mathbb{Z}_p$，同时将解密算法 NFHE.Decrypt($\boldsymbol{sk},\boldsymbol{C}$)中输出的明文。

$$\mu=\left\lfloor\langle\boldsymbol{s}',C_{m-1}\rangle/(q/2p)+\frac{1}{2}\right\rfloor \bmod 2 \tag{9}$$

修改为：

$$\mu=\left\lfloor\langle\boldsymbol{s}',C_{m-1}\rangle/(q/2p)+\frac{1}{2}\right\rfloor \bmod p \tag{10}$$

在不改变系统参数的情况下实现多比特加密。具体的实现多比特加密的 NFHE 方案的加解密算法如下。

(1)加密算法 NFHE.Encrypt($\boldsymbol{pk},\mu$)。对于明文 $\mu\in\mathbb{Z}_p$，均匀随机选取 $\boldsymbol{r}_i,e_{i,1}\leftarrow\chi^n,e_{i,2}\leftarrow\chi,i=1,\cdots,(n+1)\cdot t$，计算 $C_{i,1}=\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{r}_i+e_{i,1}\in\mathbb{Z}_q^n,C_{i,2}=\boldsymbol{b}^{\mathrm{T}}\cdot\boldsymbol{r}_2+e_{i,2}\in\mathbb{Z}_q$。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：

$$\boldsymbol{C}=mbFlatten(\boldsymbol{\mu}\cdot\mathbf{I}_N+mbDpt(\boldsymbol{C}'))\in\mathbb{Z}_p^{m\times m} \tag{11}$$

(2)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 $\boldsymbol{s}'=pofmb(\boldsymbol{sk})$，计算并输出明文 $\mu=\left\lfloor\langle\boldsymbol{s}',C_{m-1}\rangle/(q/2p)+\frac{1}{2}\right\rfloor \bmod p$。

当未进行同态运算时，若明文消息为 $\mu'$，根据加/解密流程，解密后有：

$$\mu=\left\lfloor\langle\boldsymbol{s}',C_{m-1}\rangle/(q/2p)+\frac{1}{2}\right\rfloor \bmod p=\left\lfloor\mu'+e/(q/2p)+\frac{1}{2}\right\rfloor \bmod p \tag{12}$$

当 $|e/(q/2p)<1/2|$ 时，有 $\mu=\mu'$，可以正确解密。

对于同态加法，有：

$$\boldsymbol{C}=mbFlatten((\mu_1+\mu_2)\cdot\mathbf{I}_N+mbDmp(C_1+C_2)) \tag{13}$$

$$NFHE.Dec(\boldsymbol{sk},\boldsymbol{C})=(\mu_1+\mu_2)\bmod p \tag{14}$$

对于同态乘法，有：

$$\boldsymbol{C}\cdot\boldsymbol{sk}=\mu_1\cdot\mu_2\cdot\boldsymbol{sk}+\mu_2\cdot\boldsymbol{e}_1+C_1\cdot\boldsymbol{e}_2 \tag{15}$$

$$NFHE.Dec(\boldsymbol{sk},\boldsymbol{C})=\mu_1\cdot\mu_2 \tag{16}$$

因此可以做到正确解密。

在进行同态乘法后，由于 $\mu_2$ 和 $C_1$ 的系数都限制在 $\mathbb{Z}_p$ 上，噪声不超过原密文的 $pN+p$ 倍，因此，当进行多比特加密时，定理 2 对噪声的限制变为：

$$|\langle C_{m-1},\boldsymbol{s}'\rangle|<q/[4p(pN+p)^L] \tag{17}$$

由于 $pN=pkt\gg p$，因此这一变动对于模数 $q$ 的影响可以忽略不计。

在实际的应用中，仅支持单比特加密的方案需要进行 $\log^2 p$ 次同态乘法运算，才能够实现 $\log p$ 比特的同态乘法运算。相比之下，优化后的基于多比特加密的 NFHE 方案能够在很大程度上减少同态运算的计算次数，促进了方案效率的提升。

## 3 NFHE 方案的密钥同态性

### 3.1 密钥同态性定义

设 $F:K\times X\to Y$ 是一个伪随机函数(PRF)[20],$K$ 为密钥空间,具备群结构并且在群上满足某种$\oplus$运算;$X$ 为明文空间;$Y$ 为密文空间。若对任意的 $k_1,k_2\in K$,能找到有效的算法由 $F(k_1,x)$和 $F(k_2,x)$计算出 $F(k_1\oplus k_2,x)$。

现将其定义扩展到多密钥,假设密钥数量为 $N$。对某公钥加密方案 $E$,如果$(pk_i,sk_i)$为该方案的有效公钥或私钥对,若对 $pk=f(pk_1,pk_2,\cdots,pk_N)$,能找到 $sk=f(sk_1,sk_2,\cdots,sk_N)$,能令$(pk,sk)$也是 $E$ 的有效公钥或私钥对,则称 $E$ 为具备密钥同态性质,其中,$f,h$ 都为有效可计算函数。特别地,如果 $f,h$ 都为求和(乘积/线性)函数,则称 $E$ 具有密钥加(乘/线性)同态性质。

### 3.2 方案密钥同态性证明

在该 NFHE 方案中,$\boldsymbol{s}\in\mathbb{Z}^{n\times l}$,私钥 $\boldsymbol{sk}=\begin{pmatrix}-\boldsymbol{s}\\1\end{pmatrix}\in\mathbb{Z}_q^{n+1}$,公钥 $\boldsymbol{pk}=(\boldsymbol{A},\boldsymbol{b}=\boldsymbol{A}\cdot\boldsymbol{s}+\boldsymbol{e})\in\mathbb{Z}_q^{n\times n}\times\mathbb{Z}_q^{n}$,记 $\boldsymbol{pk}=\boldsymbol{K}=\frac{1}{N}\sum_{i=1}^{N}\boldsymbol{K}_i$,若用 $\boldsymbol{pk}$ 对明文 $\mu$ 加密得到:

$$\begin{aligned}\boldsymbol{C}&=mbFlatten(\boldsymbol{\mu}\cdot\mathbf{I}_N+mbDpt(\boldsymbol{C}'))\\&=mbFlatten(\boldsymbol{\mu}\cdot\mathbf{I}_N+mbDpt(\boldsymbol{r}\cdot\boldsymbol{K}))\end{aligned}\tag{18}$$

可用 $\boldsymbol{sk}=\bar{t}=\frac{1}{N}\sum_{i=1}^{N}\bar{t}_i$ 对该密文解密,即如果保持 $\boldsymbol{A}$ 不变,则该方案满足密钥线性同态性。

证明:

$$\begin{aligned}\bar{\boldsymbol{t}}\boldsymbol{K}&=\frac{1}{N}\sum_{i=1}^{N}\bar{\boldsymbol{t}}_i\cdot\frac{1}{N}\sum_{i=1}^{N}\boldsymbol{K}_i\\&=\begin{pmatrix}-\frac{1}{N}\sum_{i=1}^{N}\boldsymbol{s}_i\\1\end{pmatrix}\left(\boldsymbol{A},\frac{1}{N}\sum_{i=1}^{N}b_i\right)\\&=\frac{1}{N}\sum_{i=1}^{N}e_i\approx0\end{aligned}\tag{19}$$

成立。因此仍然有:

$$\begin{aligned}\bar{\boldsymbol{t}}\boldsymbol{C}&=mbFlatten(\boldsymbol{\mu}\cdot\mathbf{I}_N+mbDpt(\boldsymbol{r}\cdot\boldsymbol{K}))\bar{\boldsymbol{t}}\\&=\mu\cdot\bar{\boldsymbol{t}}+\boldsymbol{r}\cdot\boldsymbol{K}\cdot\bar{\boldsymbol{t}}=\mu\cdot\bar{\boldsymbol{t}}+\boldsymbol{r}\cdot\boldsymbol{e}=\mu\cdot\bar{\boldsymbol{t}}+\bar{\boldsymbol{e}}\end{aligned}\tag{20}$$

其中,$\bar{\boldsymbol{e}}=\boldsymbol{r}\cdot\boldsymbol{e}$。因此,按原方案解密可得到明文 $\mu$。故在 $\boldsymbol{A}$ 不变的情况下,该方案满足密钥线性同态性质。

## 4 基于 NFHE 方案的安全多方计算

### 4.1 基于层次型 NFHE 方案的安全多方计算协议

与文献[11-12,16]相同(构造的协议基础方案为层次型的 GSW13 方案),本文的基础 NFHE 方案是层次型的,只能做有限次的同态运算。虽然可以通过自举去除这个限制,达到任意次的同态运算,但该方案的大部分优势也会因此被破坏,进而使得构造的安全多方计算协议复杂度增加、效率降低,与本文提出的高效全同态加密目标相背。故本文将构造基于层次型的 NFHE 方案的安全多方计算协议。

$\pi_f$:在 CRS 模型下,安全计算单值函数 $f$ 的协议,该协议在半诚实模型和半恶意模型下是安全的。具体如下。

(1)Preprocessing:进行参数设置,确保所有参与方共享参数设置,选择公共随机串矩阵 $\boldsymbol{A}\xleftarrow{R}\mathbb{Z}_q^{n\times n}$。

(2)Input:对于 $i\in[N]$,输入每个参与者 $P_i$ 输入私有数据 $x_i\in\{0,1\}$,一个参与者想要计算的单值函数 $f:(\{0,1\}^N\to\{0,1\})$,$d$ 为 $f$ 的电路深度。

Round 1 每一个 $P_i$ 执行以下操作:

1)生成$(pk_i,sk_i)\leftarrow NFHE.Keygen(n,q)$;

2)发布公钥$\{pk_i\}_{i\in[N]}$。

Round 2 每一个 $P_i$ 接收他人公钥$\{pk_i\}_{i\in[N]\setminus\{i\}}$并执行以下操作:

1)计算联合公钥 $\boldsymbol{pk}=\boldsymbol{K}=\frac{1}{N}\sum_{i=1}^{N}\boldsymbol{K}_i$;

2)利用 $\boldsymbol{pk}$ 计算密文 $\boldsymbol{C}=mbFlatten(\boldsymbol{\mu}\cdot\mathbf{I}_N+mbDpt(\boldsymbol{C}'))$,发布密文$\{C_i\}_{i\in[N]}$。

Round 3 每一方 $P_i$ 接收他人密文$\{C_i\}_{i\in[N]\setminus\{i\}}$并执行以下操作:

1)进行同态运算;

2)进行门限解密。

$P_i$ 选取随机向量 $\boldsymbol{\gamma'}_i\leftarrow\boldsymbol{\chi}^{m-l}$,令 $\boldsymbol{\gamma}_i=(\boldsymbol{\gamma}_i',0,\cdots,0)\in\boldsymbol{\chi}^m$,计算 $\boldsymbol{\eta}_i=\boldsymbol{t}_i\cdot\boldsymbol{C}+\boldsymbol{\gamma}_i\in\mathbb{Z}_q^m$,然后公布 $\boldsymbol{\eta}_i$。

(3)Output:每一个参与者 $P_i$ 接受他人解密$\{\boldsymbol{\eta}_i\}_{i\in[N]\setminus\{i\}}$,计算 $\boldsymbol{\eta}=\frac{1}{N}\sum_{i=1}^{N}\boldsymbol{\eta}_i=\boldsymbol{tC}+\frac{1}{N}\sum_{i=1}^{N}\boldsymbol{\gamma}_i=\boldsymbol{tC}+\boldsymbol{\gamma}$,然后计算 $\boldsymbol{v}=\boldsymbol{\eta}\boldsymbol{G}^{-1}(\boldsymbol{w}^{\mathrm{T}})$,其中 $\boldsymbol{w}=\left(0,0,\cdots,\left\lceil\frac{q}{2}\right\rceil\right)$。若 $\boldsymbol{v}$ 的值接近 0,则取 $\mu=0$;若 $\boldsymbol{v}$ 的值接近$\left\lceil\frac{q}{2}\right\rceil$,则取 $\mu=1$。

### 4.2 协议正确性

协议的正确性主要依赖两个方面。

(1)协议所使用的 NFHE 方案的正确性已经在前面得到证明,因此只需要验证所用的参数是否正确。由该方案可知,通过上述参数设置,每次进行同态运算后,噪声不超过原密文的 $pN+p$ 倍。因此当$|\langle C_{m-1},\boldsymbol{s}'\rangle|<q/\lceil 4p(pN+p)^L\rceil$时,在不超过 $L$ 次同态运算后,$|\langle C_{m-1},\boldsymbol{s}'\rangle|<q/(4p)$,方案可以正确解密。

(2)协议的加解密正确性。对前面该方案的密钥同态性进行分析可知,协议 $\pi_f$ 中所用的密钥对是有效的。由定理 1 可知,协议 $\pi_f$ 中的联合误差也是服从 $B_\chi$有界分布的。接下来证明协议联合解密的正确性。

证明:由 $\boldsymbol{\eta}=\frac{1}{N}\sum_{i=1}^{N}\boldsymbol{\eta}_i=\boldsymbol{tC}+\frac{1}{N}\sum_{i=1}^{N}\boldsymbol{\gamma}_i=\boldsymbol{tC}+\boldsymbol{\gamma}$

可得:

$$\begin{aligned}\boldsymbol{\eta}\boldsymbol{G}^{-1}(\boldsymbol{w}^{\mathrm{T}})&=(\boldsymbol{tC}+\boldsymbol{\gamma})\boldsymbol{G}^{-1}(\boldsymbol{w}^{T})\\&=\boldsymbol{tC}\boldsymbol{G}^{-1}(\boldsymbol{w}^{\mathrm{T}})+\boldsymbol{\gamma}\boldsymbol{G}^{-1}(\boldsymbol{w}^{\mathrm{T}})\\&=\mu\left\lceil\frac{q}{2}\right\rceil+(\boldsymbol{\gamma}_1',\cdots,\boldsymbol{\gamma}'_{(m-l)},0,\cdots,0)\boldsymbol{G}^{-1}\begin{pmatrix}0\\\vdots\\\left\lceil\frac{q}{2}\right\rceil\end{pmatrix}\\&=\mu\left\lceil\frac{q}{2}\right\rceil\end{aligned}\tag{21}$$

因为 $\boldsymbol{G}^{-1}\left\lceil\frac{q}{2}\right\rceil$是对$\left\lceil\frac{q}{2}\right\rceil$的比特分解,而$\left\lceil\frac{q}{2}\right\rceil$最大的分解长度为$\lfloor\log q\rfloor+1$,又由 $l=\lfloor\log q\rfloor+1$ 以及共有 $t$ 个$\left\lceil\frac{q}{2}\right\rceil$可知,$\boldsymbol{G}^{-1}\begin{pmatrix}\left\lceil\frac{q}{2}\right\rceil\\\vdots\\\left\lceil\frac{q}{2}\right\rceil\end{pmatrix}$最大长度为 $tl$。又因为在 $\boldsymbol{\gamma}$ 中后 $tl$ 位全部为

0，故协议可以正确进行联合解密。

### 4.3 议安全性

#### 4.3.1 半诚实模型下的安全性

在 CRS 模型中，该协议的安全性基于以下几个问题。

(1)在上述设置下，该 NFHE 方案的安全性可以归结为 LWE 问题。

(2)在 $\boldsymbol{\eta}_i=\boldsymbol{t}_i\cdot\boldsymbol{C}+\boldsymbol{\gamma}_i$ 和 $\boldsymbol{\eta}=\boldsymbol{tC}+\boldsymbol{\gamma}$ 中，由于 $\boldsymbol{\gamma}_i$ 与 $\boldsymbol{\gamma}$ 中前 $l$ 个分量是服从 $B_\chi$ 有界分布的，因此这两个等式使得本协议安全性可以归结为 Some-are-errorless LWE 问题。因而在 Round 3 中每一方公布自己的 $\boldsymbol{\eta}_i$ 后，自己的私钥以及联合密钥不会泄露，所以该协议在半诚实模型下是安全的。

#### 4.3.2 半恶意模型下的安全性

为了方便表示，用 $\boldsymbol{\rho}_i=\boldsymbol{\eta}_i\boldsymbol{G}^{-1}(\boldsymbol{w}^{\mathrm{T}})+\boldsymbol{\varepsilon}_i=\boldsymbol{v}_i+\boldsymbol{\varepsilon}_i,\boldsymbol{\varepsilon}_i\leftarrow\chi$ 代替 $\boldsymbol{\eta}_i$ 作为 $P_i$ 的部分解密。如果通过模拟得到的 $\boldsymbol{\rho}_i$ 与解密 $\boldsymbol{\eta}_i$ 得到的真实 $\boldsymbol{\rho}_i$ 不可区分，则通过模拟得到的 $\boldsymbol{\eta}_i$ 与真实的 $\boldsymbol{\eta}_i$ 也是不可区分的。

**定理 4** 设 $f$ 是一个确定性多项式时间(PPT)的可计算函数，具有 $N$ 个输入，1 个输出。上述的协议式 $\pi_f$ 能够实现 $f$ 在面对一个恰好俘获 $N-1$ 个参与者的半恶意敌手时是安全的。

证明：我们构造一个 PPT 模拟器 $S$ 用来针对一个俘获 $N-1$ 个用户的半恶意敌手，记该静态的半恶意敌手为 $A$，设 $P_h$ 为剩下的唯一诚实方。模拟器 $S$ 代表 $P_h$ 执行以下操作。

在第二轮时，模拟器 $S$ 用 0 代替诚实方 $P_h$ 的真实输入进行加密，而后模拟器 $S$ 从“证据磁带”中得到 $N-1$ 个被俘获方的输入和私钥，这些输入由 $S$ 发送一个理想机得到输出 $y$，同时可以得到同态计算后的密文 $\boldsymbol{C}$，然后 $S$ 为 $P_h$ 计算模拟的部分解密 $\boldsymbol{\rho}_h'\leftarrow S(\boldsymbol{y},\boldsymbol{C},h,\{sk_i\}_{i\in[N]\setminus\{h\}})$，并在第三轮中公布模拟的部分解密结果，代替真实解密结果。

本文通过一系列混合攻击游戏来证明真实结果和模拟结果的不可区分，即 $IDEAL_{F,S,Z}\overset{\text{comp}}{\approx}REAL_{\pi,A,Z}$，其中 $Z$ 代表特定环境。

(1)游戏 $REAL_{\pi,A,Z}$：在真实环境 $Z$ 中，存在一个半恶意的敌手，执行协议 $\pi_f$。

(2)游戏 $HYB_{\pi,A,Z}$：与游戏 $REAL_{\pi,A,Z}$ 基本相同，不同之处在于假定 $P_h$ 在第二轮之后得到所有的私钥 $\{sk_i\}_{i\in[N]\setminus\{h\}}$，并在第三轮用模拟的部分解密 $\boldsymbol{\rho}_h'\leftarrow S(\boldsymbol{y},\boldsymbol{C},h,\{sk_i\}_{i\in[N]\setminus\{h\}})$ 代替真实解密发布出去。

(3)游戏 $IDEAL_{F,S,Z}$：和游戏 $HYB_{\pi,A,Z}$ 基本相同，除了在第二轮 $P_h$ 用 0 代替真实输入加密并发布出去。

**引理 1** $REAL_{\pi,A,Z}\overset{\text{stat}}{\approx}HYB_{\pi,A,Z}$

证明：两个游戏的区别在于 $P_h$ 的真实部分解密 $\boldsymbol{\rho}_h$ 用模拟解密 $\boldsymbol{\rho}_h'$ 代替。因此设 $\boldsymbol{v}=\boldsymbol{\mu}\left\lceil\frac{q}{2}\right\rfloor+\boldsymbol{e}'$，其模拟解密的算法为：

$$\begin{aligned}\boldsymbol{\rho}_h'&=N\boldsymbol{\mu}\left\lceil\frac{q}{2}\right\rfloor+N\boldsymbol{e}'-\sum_{i\neq h}\boldsymbol{t}_i\boldsymbol{C}\boldsymbol{G}^{-1}(w^{\mathrm{T}})+\boldsymbol{\varepsilon}_h'\\&=N\boldsymbol{\mu}\left\lceil\frac{q}{2}\right\rfloor+N\boldsymbol{e}'+\boldsymbol{\varepsilon}_h'-\sum_{i\neq h}\boldsymbol{v}_i\end{aligned}\tag{22}$$

其中，$\boldsymbol{e}'\leftarrow\chi,\boldsymbol{\varepsilon}_h'\leftarrow\chi$。

$P_h$ 的真实解密结果为：由于 $\boldsymbol{e}=\frac{1}{N}\sum_{i\in[N]}\boldsymbol{v}_i=\boldsymbol{\mu}\left\lceil\frac{q}{2}\right\rfloor+\boldsymbol{e}'\Rightarrow N\boldsymbol{e}'=\sum_{i\in[N]}\boldsymbol{v}_i-N\boldsymbol{\mu}\left\lceil\frac{q}{2}\right\rfloor$，则：

$$\begin{aligned}\boldsymbol{\rho}_h&=\boldsymbol{\eta}_h\boldsymbol{G}^{-1}(\boldsymbol{w}^{\mathrm{T}})+\boldsymbol{\varepsilon}_h=\boldsymbol{v}_h+\boldsymbol{\varepsilon}_h\\&=\sum_{i\in[N]}\boldsymbol{v}_i-\sum_{i\neq h}\boldsymbol{v}_i+\boldsymbol{\varepsilon}_h\\&=\sum_{i\in[N]}\boldsymbol{v}_i-N\boldsymbol{\mu}\left\lceil\frac{q}{2}\right\rfloor+N\boldsymbol{\mu}\left\lceil\frac{q}{2}\right\rfloor-\sum_{i\neq h}\boldsymbol{v}_i+\boldsymbol{\varepsilon}_h\\&=N\boldsymbol{e}'+N\boldsymbol{\mu}\left\lceil\frac{q}{2}\right\rfloor-\sum_{i\neq h}\boldsymbol{v}_i+\boldsymbol{\varepsilon}_h\end{aligned}\tag{23}$$

其中，$\boldsymbol{\varepsilon}_h\leftarrow\chi$。

易得 $\boldsymbol{\varepsilon}_h$ 和 $\boldsymbol{\varepsilon}_h'$ 在统计上不可区分，从而证明了 $\boldsymbol{\rho}_h$ 与 $\boldsymbol{\rho}_h'$ 的不可区分性，故结论得证。

**引理 2** $HYB_{\pi,A,Z}\overset{\text{comp}}{\approx}IDEAL_{F,S,Z}$

证明：$P_h$ 所产生的密文是这两个游戏的唯一不同之处。由该 NFHE 方案的加密方式的语义安全性可知密文在计算上具有不可区分性，因此这两个游戏在计算上也是不可区分的。

由引理 1 和引理 2 可得 $IDEAL_{F,S,Z}\overset{\text{comp}}{\approx}REAL_{\pi,A,Z}$。

证毕。

根据文献[21]，若在 CRS 模型下的 SMC 协议在半恶意环境下被证明是安全的，则该协议可以通过非交换的零知识证明(NIZKs)等工具转换为恶意环境下的协议。因此，本文设计的 SMC 协议在恶意模型下也是安全的。

### 4.4 性能分析及对比

文献[11]和文献[12]中均为单比特的安全多方计算协议，设 $t$ 为参与方输入的比特数量，这两个方案则需要重复执行 $t$ 次；文献[16]与本文中的 SMC 协议由于都支持多比特加密，故只需执行一次。而本文基于的 NFHE 方案[18]通过修改 GSW13 方案的展开方式，对其密文尺寸 $(n+1)^2\lceil\log q\rceil^2$ 进行改进，得到的密文尺寸为 $\frac{(n+1)^2\lceil\log q\rceil^2}{\lceil\log q\rceil}$。在进行多比特加密的情况下，密文尺寸为 $\frac{(n+t)^2\lceil\log q\rceil^2}{\lceil\log q\rceil}$，如表 2 所列，故在时间效率上，在已有的 CRS 模型下的协议的性能最优。在空间效率上，由于文中的 SMC 协议基于的 NFHE 方案密文是矩阵，因此密文膨胀率同样为 $O(1)$；同时因为密文尺寸远大于密钥尺寸，所以本文的协议通过大幅度压缩密文尺寸，有效减少了体制的存储开销，提高了整体协议的效率。现有的在 CRS 模型下的基于全同态加密的安全多方计算协议主要性能对比如表 2 所列，其中，“Basic”表示协议所使用的基础全同态加密方案，“*Rd*”代表协议的交互轮次，“*CTE Ratio*”表示密文膨胀率，“*Depth*”代表与非门复杂度，最后一栏“*Ciphertext Size*”代表密文的尺寸大小。

表 2 基于 FHE 的 SMC 协议性能对比

Table 2 Performance comparison of SMC protocol based on FHE

| Protocol | Basic | *Rd* | *CTE Ratio* | *Depth* | *Ciphertext Size* |
|---|---|---|---|---|---|
| Mukherjee et al.[11] | GSW13 | 2 | $O(1)$ | $\widetilde{O}(tN(nd^{\omega}))$ | $(n+1)^2\lceil\log q\rceil^2$ |
| Wang et al.[12] | GSW13 | 3 | $O(1)$ | $\widetilde{O}(t(nd^{\omega}))$ | $(n+1)^2\lceil\log q\rceil^2$ |
| Tang et al.[16] | GSW13 | 3 | $O(1)$ | $\widetilde{O}((nd^{\omega}))$ | $(n+t)^2\lceil\log q\rceil^2$ |
| Ours | GSW13 | 3 | $O(1)$ | $\widetilde{O}((nd^{\omega}))$ | $\frac{(n+t)^2\lceil\log q\rceil^2}{\lceil\log p\rceil}$ |

**结束语** 本文基于高效的全同态加密方案，在公共随机串模型下构造了一个层次型的多比特多密钥安全多方计算协议。该协议共3轮通讯，且在半诚实与半恶意环境下被证明是安全的，其安全性基于DLWE和Some-are-errorless LWE。与现有的协议相比，本文协议密文膨胀率小，多比特加密大幅度减少了同态运算计算次数，与非门复杂度低，密文尺寸小，整体性能在已有的基于全同态加密的安全多方计算协议中最优。下一步的工作会研究在协议的执行过程中，如何采取合适的方法来确保数据能够安全传输以及满足会话的协同性要求，同时也会进一步改善协议，进而达到实用标准。

## 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(11): 169-180.

[2] GENTRY C. Fully homomorphic encryption using ideal lattices [C]// Proceedings of the forty-first Annual ACM Symposium on Theory of Computing. 2009: 169-178.

[3] 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. 2011: 97-106.

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

[5] BRAKERSKI Z. Fully homomorphic encryption without modulus switching from classical GapSVP[C]// Annual Cryptology Conference. Berlin: Springer, 2012: 868-886.

[6] GENTRY C, SAHAI A, WATERS B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based [C] // Annual Cryptology Conference. Berlin: Springer, 2013: 75-92.

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

[8] YAO A C. Protocols for secure computations[C]// 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982). IEEE, 1982: 160-164.

[9] LÓPEZ-ALT A, TROMER E, VAIKUNTANATHAN V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption[C]// Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing. 2012: 1219-1234.

[10] HOFFSTEIN J, PIPHER J, SILVERMAN J H. NTRU: A ring-based public key cryptosystem[C]// International Algorithmic Number Theory Symposium. Berlin: Springer, 1998: 267-288.

[11] MUKHERJEE P, WICHS D. Two round multiparty computation via multi-key FHE[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2016: 735-763.

[12] WANG H Y, FENG Y, ZHAO L Z, et al. A Secure Multi-Party Computation Protocol on the Basis of Multi-Key Homomorphism [J]. Journal of South China University of Technology (Natural Science Edition), 2017, 45(7): 69-76.

[13] KIM E, LEE H S, PARK J. Towards round-optimal secure multiparty computations: Multikey FHE without a CRS[C]// Australasian Conference on Information Security and Privacy. Cham: Springer, 2018: 101-113.

[14] TANG C M, HU Y Z, LI X X. Three Round Secure Multiparty Computation Based on Multi-key Full-Homomorphic Encryption without CRS[J]. Journal of Cryptography, 2021, 8(2): 273-281.

[15] LI Z P. Lattice-based Fully Homomorphic Encryption and Its Applications [D]. Harbin: Harbin Engineering University.

[16] TANG C M, HU Y Z. Secure multi-party computing based on multi-bit fully homomorphic encryption [J]. Chinese Journal of Computers, 2021, 44(4): 836-845.

[17] LI Z, MA C, MORAIS E, et al. Multi-bit Leveled Homomorphic Encryption via Dual. LWE-Based[C]// Information Security and Cryptology: 12th International Conference(Inscrypt 2016). Beijing, China, 2016: 4-6.

[18] CHEN L, ZHOU Y, DUAN R. Design of fully homomorphic encryption scheme supporting multi-bit encryption [J]. Application Research of Computer, 2021, 38(2): 579-583.

[19] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM(JACM), 2009, 56(6): 1-40.

[20] BONEH D, LEWI K, MONTGOMERY H, et al. Key homomorphic PRFs and their applications[C]// Annual Cryptology Conference. Berlin: Springer, 2013: 410-428.

[21] ASHAROV G, JAIN A, LÓPEZ-ALT A, et al. Multiparty computation with low communication, computation and interaction via threshold FHE[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2012: 483-501.


**ZHU Zong-wu**, born in 1997, postgraduate, is a member of China Computer Federation. His main research interests include homomorphic encryption and secure multi-party computing.

**HUANG Ru-wei**, born in 1978, Ph. D, professor, is a member of China Computer Federation. Her main research interests include cloud computing and homomorphic encryption.

（责任编辑：何杨）