基于多比特全同态加密的安全多方计算

唐春明 胡业周

(广州大学数学与信息科学学院 广州 510006)

摘 要 本文中,我们首先证明了李增鹏等人提出的多比特多密钥全同态加密方案(MFHE)满足密钥同态性质,利用此性质,可以通过门限解密得到最终解密结果.使用该方案,我们设计了一个在 CRS 模型下和半恶意攻击者模型下安全的三轮多方计算协议(MPC).该安全多方计算协议的安全性是基于容错学习问题(LWE)的两个变种问题 Ferr-LWE 和 Some-are-errorless. LWE,而且,通过非交互的零知识证明,我们可以把半恶意攻击者模型下安全的三轮多方计算协议转变为在恶意模型下安全的三轮多方计算协议.

关键词 全同态加密;多密钥多比特;门限解密;LWE 及其变种问题;安全多方计算

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2021.00836

Secure Multi-Party Computation Based on Multi-Bit Fully Homomorphic Encryption

TANG Chun-Ming HU Ye-Zhou

(*School of Mathematics and Information Sciences, Guangzhou University, Guangzhou* 510006)

Abstract In this paper, we study secure multi-party computation based on multi-bit fully homomorphic encryption. In the previous work, a lot of research has been done on the secure multi-party computing protocol based on single-bit full homomorphic encryption. Although this protocol can be naturally extended to multi-bit version, it needs to be encrypted repeatedly, which greatly reduces efficiency. On the other hand, we know that in the full homomorphic encryption schemes based on ring-LWE such as BGV, multi-bits can be encrypted simultaneously by using the Chinese remainder theorem, namely SIMD operation. However, in those schemes, the dimension of ciphertext expands too fast, so the evaluated key is needed to perform re-linearization to reduce the dimension of ciphertext. Therefore, we choose GSW full homomorphic encryption scheme as the basis to build a secure multi-party computation protocol. In 2017, Li et al. used dual LWE to convert GSW full homomorphic encryption into multi-bit version, which could encrypt t bits at the same time. Based on this scheme, we construct a three-round secure multi-party computation. We first prove that the multi bit multi key fully homomorphic encryption scheme (MFHE) satisfies the key homomorphic property, because in the public key generation phase, each party uses a common random matrix. With this property, the final decryption result can be obtained by threshold decryption, namely each participant can use its own private key to decrypt the evaluated ciphertext. In combination with the partial decryption of all parties, the plaintext data can be recovered. Using this scheme, we design a three-round secure multi-party

收稿日期:2020-01-16;在线发布日期:2020-05-15.本课题得到国家自然科学基金项目(61772147)、"十三五"国家密码发展基金项目(MMJJ20170117)、广东省重大基础研究培育项目(2015A030308016)、密码科学技术国家重点实验室开放课题项目(MMKFKT201913)、广州市教育局协同创新重大项目(1201610005)、广州大学全日制研究生"基础创新"和项目(2019GDJC-M28)资助.

唐春明,博士,教授,博士生导师,主要研究领域为密码学及其应用. E-mail: ctang@gzhu.edu.cn. **胡业周**,硕士研究生,主要研究方向为全同态加密与安全多方计算.

computation protocol (MPC) in the CRS model and semi-malicious adversary model. The number of rounds of three is optimal, because at the ciphertext generation stage, each participant needs at least one round to encrypt the private message using the public key of all to be calculated as the joint public key. Then, in the second round, each party publishes the ciphertext that encrypts its own private data to calculate evaluated ciphertext, and in the last round, all parties publish their own partial decryption to reconstruct the final message. We compare it with the existing secure multi-party computation protocol based on GSW full homomorphic encryption scheme, because we can encrypt multiple bits at the same time, so the efficiency is the highest. The security of the secure multi-party computing protocol is based on the variants of the Learning with Errors Problem (LWE) called Ferr-LWE and Some-are-errorless.LWE problem, the difficulty is the same as solving the LWE problem. We can use ideal vs real models to prove this, namely using a simulator to simulate the input of the honest party, and finally a series of hybrid games are defined to prove that the ideal and the real are computation indistinguishable, which is hold when there is only one honest party, also we can prove the security against those who corrupt the arbitrary number of parties using only pseudorandom functions. On the other hand, based on non-interactive zero knowledge proof, we can transform the Three-round secure multiparty computation protocol under the semi-malicious adversary model into the Three-round secure multiparty computation protocol under the malicious model.

Keywords　fully homomorphic encryption; multi bit multi key; threshold decryption; LWE and its variants; secure multi-party computation

1　引　言

随着大数据行业的兴起与云计算的发展，数据的隐私保护越来越受到人们的关心，其中安全多方计算和全同态加密在数据的隐私保护中发挥着重要的作用.安全多方计算最先由姚期智在 1982 年解决“百万富翁”问题时提出[1].通常来说，安全多方计算协议是指在 n 个不同的参与方 $\{p_1,p_2,\cdots,p_n\}$ 之间，协同计算某一个函数 $(y_1,y_2,\cdots,y_n)=f(x_1,x_2,\cdots x_n)$，计算完毕后，每个参与者 P_i 仅仅知道自己的输入 x_i 和输出 y_i，但对于其他人的输入和输出得不到任何信息.全同态加密的概念最先由 Rivest[2] 在 1978 年提出，旨在不解密的情况下，对密文进行运算，其结果和直接在明文上进行操作相同.即

$$dec(f(Enc(m_1),Enc(m_2),\cdots,Enc(m_n)))=f(m_1,m_2,\cdots m_n).$$

目前，对多比特的全同态加密以及单比特的安全多方计算做了大量的研究，但如何构造一个基于多比特 GSW 全同态加密方案的安全多方计算协议，而不是采用逐比特加密，仍然是个未解决问题.本文利用文献[3]中多比特全同态加密方案以及其密钥同态的性质，构造了一个基于多比特全同态加密方案的安全多方计算协议，并与近些年同类的方案做横向对比，发现其性能是最优的.

本文第 2 节综述相关工作；第 3 节给出一些与本文相关的定义及定理并简要叙述文献[3]提出的多比特全同态加密方案和该方案的正确性及安全性；第 4 节证明该方案的密钥同态性；第 5 节利用该方案构造一个多比特的安全多方计算协议，证明其安全性并分析其性能；第 6 节总结全文.

2　相关工作

1987 年，Goldreich 等人提出一个安全多方计算协议，该协议可以计算任意函数，并在下一年给出了安全多方计算的安全性定义[4].目前常用安全多方计算协议的构造方法有如下几类：基于混淆电路的安全多方计算协议；基于不经意传输的安全多方计算协议[5]；基于可验证秘密共享的安全多方计算协议[6]；基于混合匹配的安全多方计算协议[7]；基于 HE 的安全多方计算协议[8-10].

全同态加密的发展较为缓慢，直到 2009 年，才由 Gentry 提出了第一个基于理想格的全同态加

密方案[11].随后,众多的全同态加密方案也应运而生.可以将其发展阶段分成三个阶段,第一阶段是基于 Gentry 所提的全同态加密方案,代表的方案有 SV10[12]、SS10[13]、LMSV11[14] 等.第二阶段是 Brakerski 和 Vaikuntanathan 利用 LWE 和 ring-LWE 的假设实现了 FHE.其代表方案有 BGV12[15]、Bra12[16]、BV14[17] 等.第三阶段是基于 LWE 假设,利用近似特征向量构造的 FHE 方案,其代表的方案有 GSW(13)[18]、CM(15)[8]、MW(16)[9] 等.

对于多密钥的 FHE 是由 LÓPEZ-AltA、Tromere、Vaikuntanhanv 提出,他们利用改进的 NTRU 方案构造了一个 MFHE 方案,但该方案的复杂度太高,且复杂度随着用户的增长呈现出指数增长[19].在 CM(15)和 MW(16)中,提出了一个多密钥的全同态加密方案和一个在 CRS 模型中的 2 轮 MPC 协议.将一个密文矩阵通过扩展(Expand)操作,产生一个新的密文,并将密钥级联成组合密钥,用组合密钥解密扩展后的密文可以得到正确的解密结构.但是该方案的密文矩阵体积过大,且在 Expand 操作中,需要利用联合操作产生一个掩盖信息.在 BHP(17)中,提出了一个在平凡模型中基于多密钥全同态加密的 MPC 协议,且抵抗半恶意的敌手只需三轮通信,若想抵抗恶意敌手,只需增加一轮即可[10].这些全同态加密方案都是单比特加密的方案.

门限解密即每一方利用自己的私钥解密密文产生各自的部分解密,然后每一方结合其他人的部分解密可恢复出明文.上述提到的几种全同态加密方案都可以使用门限解密得到最终的结果.

3 多比特全同态加密(MFHE[3])方案

3.1 记 号

对于自然数 $n\in Z$,$[n]$代表$\{1,2,\cdots,n\}$.对于一个自然数 $x\in R$,$\lfloor x\rfloor$ 代表最接近 x 但小于 x 的整数.小写粗斜体字母代表向量,大写粗斜体字母代表矩阵.$[\boldsymbol{A}|\boldsymbol{Ax}]$表示矩阵和向量的水平连接,$(\boldsymbol{a},\boldsymbol{b})$,$(\boldsymbol{a}|\boldsymbol{b})$表示两个向量的水平连接,$(\boldsymbol{a}\cdot\boldsymbol{b})$表示两个向量的内积.对于向量 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$,$p\geq 1$,$l_p$ 范数指的是 $\|\boldsymbol{x}\|_p=\sqrt[p]{\sum_{i=1}^{n}|x_i|^p}$,$l_\infty$ 范数指的是 $\|\boldsymbol{x}\|_\infty=\max(|x_1|,|x_2|,\cdots,|x_n|)$,$l_1$ 范数指的是 $\|\boldsymbol{x}\|_1=\sum_{i=1}^{n}|x_i|$,$l_2$ 范数指的是 $\|\boldsymbol{x}\|_2=\sqrt{\sum_{i=1}^{n}|x_i|^2}$.对于一个矩阵 $\boldsymbol{A}$,$\boldsymbol{a}_i$代表的是矩阵 $\boldsymbol{A}$ 的第 i 列向量.$\|\boldsymbol{A}\|$表示矩阵$\boldsymbol{A}$ 中 l_2 范数最大列向量,即$\|\boldsymbol{A}\|=\max_i\|\boldsymbol{a}_i\|$.

3.2 定义与定理

定义 1. 算法 $BitDecomp^{-1}$ 指输入一个 $n=m\times q$ 维向量 $\boldsymbol{x}=(x_{1,0},\cdots,x_{1,q-1},\cdots,x_{m,1},\cdots,x_{m,q-1})$,输出一个 m 维向量 $\left(\sum_{j=0}^{q-1}2^j x_{1,j},\cdots,\sum_{j=0}^{q-1}2^j x_{m,j}\right)$.其中 $x_{1,0},\cdots,x_{1,q-1},\cdots,x_{m,1},\cdots,x_{m,q-1}$不必是$\{0,1\}$.

定理 1[20]. 对于任意的 $m>n\lceil\log q\rceil$,存在一个固定的矩阵 $\boldsymbol{G}\in Z_q^{n\times m}$,和一个确定性的"原像"函数 $\boldsymbol{G}^{-1}(\cdot)$,满足如下的情形:对于任意的 m',输入矩阵 $\boldsymbol{M}\in Z_q^{n\times m'}$,逆函数 $\boldsymbol{G}^{-1}(\boldsymbol{M})$输出一个$\{0,1\}$矩阵,即 $\boldsymbol{G}^{-1}(\boldsymbol{M})\in\{0,1\}^{m\times m'}$,使得 $\boldsymbol{G}\boldsymbol{G}^{-1}(\boldsymbol{M})=\boldsymbol{M}$.

定义 2. 一个基于整数上的分布$\{\chi_n\}_{n\in N}$,我们称该分布是 B-有界的,如果:

$$\Pr_{x\leftarrow\chi_n}[|x|\geq B]=negl(\lambda),$$

其中,$negl(\lambda)$是一个可忽略函数.

定理 2[21]. 对于服从 B-有界分布的一系列随机变量 $x_i(i\in N)$,则随机变量 $x=\frac{1}{N}\sum_{i=1}^{N}x_i$同样也服从该B-有界分布.

定理 3[22]. 对于 Z^m 中的向量 $\boldsymbol{x}$ 以及 $e\leftarrow D_{Z^m,r}$,当$|\boldsymbol{x}^{\mathrm{T}}\cdot\boldsymbol{e}|$的值被看作成$[0,\cdots,q-1]$里的一个整数,则满足:

$$|\boldsymbol{x}^{\mathrm{T}}\cdot\boldsymbol{e}|\leq\|\boldsymbol{x}\|r\omega\sqrt{\log m}+\|\boldsymbol{x}\|\sqrt{m}/2,$$

其中,$D_{Z^m,r}$是高斯分布,r 是高斯参数.

定义 3. 对于在有限域 Ω 上的两个分布 X 与 Y,X 与 Y 之间的统计距离指的是 $\Delta(X,Y)\overset{\text{def}}{=}\frac{1}{2}\sum_{\omega\in\Omega}|X(\omega)-Y(\omega)|$.如果 $\Delta(X,Y)$的值是可忽略的,则写作 $X\overset{\text{state}}{\approx}Y$.

定理 4[23]. 对 $\lambda\in Z$,$n\in N$,$q\in N$,$m\geq n\log q+2\lambda$.$\boldsymbol{A}\in Z_q^{n\times m}$是一个均匀随机矩阵,$r\overset{R}{\leftarrow}\{0,1\}^m$,以及 $\boldsymbol{y}\overset{R}{\leftarrow}Z_q^n$有:

$$\Delta((\boldsymbol{A},\boldsymbol{A}^{\mathrm{T}}\cdot r),(\boldsymbol{A},\boldsymbol{y}))\leq 2^{-\lambda}.$$

定义 4(Learning with Errors). 对于一个秘密向量 $\boldsymbol{s}\in Z_q^n$,在 $Z_q^n\times Z_q$上的 LWE 分布 $A_{s,\chi}$ 指的是均匀选取$\boldsymbol{a}\in Z_q^{n\times m}$,选取 $e\leftarrow\chi$,输出$(\boldsymbol{a},\boldsymbol{b}=\boldsymbol{a}\cdot\boldsymbol{s}+e \bmod q)$.

定义 5($Search.LWE_{n,q,\chi,m}$). 对于秘密向量

$\boldsymbol{s}\in Z_q^n$，给定 m 个从 $A_{s,\chi}$ 分布中选取的独立样本$(\boldsymbol{a}_i,\boldsymbol{b}_i)\in Z_q^n\times Z_q$，恢复出 $\boldsymbol{s}$.

定义 6($Decision.LWE_{n,q,\chi,m}$). 给定 m 个独立的样本$(\boldsymbol{a}_i,\boldsymbol{b}_i)\in Z_q^n\times Z_q$是从以下两个分布中选取：(1)从 $A_{s,\chi}$ 中选取；(2)从 $Z_q^n\times Z_q$中均匀选取. 能够区分这两种选取方式的优势可以忽略不记.

定义 7(Ferr-LWE). 对于 $q\geq 1$，$n>0$，$m>0$，在 Z 上的错误分布χ以及一个概率多项式时间算法 A，Ferr-LWE 问题是区分以下两种情形.

(1)从 $Z_q^n\times Z_q$中均匀选取所有样本.

(2)$\boldsymbol{s}\in\{0,1,\cdots,q-1\}^n$是一个秘密均匀随机向量，第一个样本从 $A_{s,0}$ 中选取，其余的所有样本从 $A_{s,\chi}$ 中选取. 即第一个样本为$(\boldsymbol{a},\boldsymbol{b}=\boldsymbol{a}\cdot\boldsymbol{s} \bmod q)$，没有引入错误 e，其余 $m-1$ 样本为$(\boldsymbol{a}_i,\boldsymbol{b}=\boldsymbol{a}_i\cdot\boldsymbol{s}+e_i \bmod q)$，$i\in\{2,\cdots,m\}$，每一样本引入一个小的错误 e_i.

定义 8(Some-are-errorless.LWE). 对于 $q\geq 1$，$n>0$，在R 上的错误分布χ'，$T_q=\left\{0,\frac{1}{q},\cdots,\frac{q-1}{q}\right\}$，其中 $q\in Z$. 在 $T_q^n\times T_q$上的分布 $A'_{s,\chi}$ 指的是均匀选取 $\boldsymbol{a}\in T_q^n$，选取 $e\leftarrow\chi'$，输出$(\boldsymbol{a},\boldsymbol{b}=\boldsymbol{a}\cdot\boldsymbol{s}+e)$. Some-are-errorless.LWE 是区分以下两种情况：

(1)从 $T_q^n\times T_q$中均匀选取所有样本.

(2)$\boldsymbol{s}\in T_q^n$是一个秘密均匀随机向量，前 l 个样本从 $A'_{s,0}$ 中选取. 其余的所有样本从 $A'_{s,\chi}$ 中选取. 即前 l 个样本为$(\boldsymbol{a}_i,\boldsymbol{b}=\boldsymbol{a}_i\cdot\boldsymbol{s})$，没有引入错误 e，其余样本为$(\boldsymbol{a}_i,\boldsymbol{b}=\boldsymbol{a}_i\cdot\boldsymbol{s}+e_i)$，$i>l$，每一样本引入一个小的错误 e_i.

容易看出 Ferr-LWE 以及 Some-are-errorless. LWE 是 LWE 问题的变种，差别在于 Ferr-LWE 第一个等式中没有错误，Some-are-errorless. LWE 前 l 个等式中没有错误.

定理 5[1]. 对于任意的 $n\geq 2$，$m\geq 1$，$q\geq 1$，以及错误分布 χ，存在一个从 $LWE_{n-1,q,m,\chi}$ 到 $LWE_{n,q,m,\chi}$ 变种问题 Ferr-LWE 多项式归约，该规约至多将问题的成功优势降低$\sum_p p^{-n}$，其中 p 过所有 q 的素因子.

定理 6[21]. 对于任意的 $n,l,q\geq 1(l\ll n)$，以及错误分布χ'，存在一个从 $LWE_{n-l,q,\chi}$ 到 $LWE_{n,q,\chi}$ 变种问题 Some-are-errorless. LWE 多项式归约，该规约至多将问题的成功优势降低$\sum_p p^{-n}$，其中 p 过所有 q 的素因子. 证明见文献[21]中定理二.

3.3 方案的构造

该方案是文献[3]基于对偶-LWE 的 MFHE[1] 方案. 其中对偶 LWE 是 Gentry 等人在 2008 年提出，其特点是方案的公钥中不含噪音. 方案中的 $t\in N$ 表示加密的比特数.

$-params\leftarrow MFHE.Setup(1^\lambda,1^d)$：$\lambda$ 为安全参数，d 为电路的最大深度. 模为 $q=q(\lambda)$，格的维数 $n=n(\lambda,d)$，错误分布$\chi=\chi(\lambda,d)$. 合适的选取参数使得 LWE 问题的困难性假设成立. 选取$\bar{m}=n\log q+2\lambda$，$m=m(\lambda,d,t)=\bar{m}+t=n\log q+2\lambda+t\approx O(n\log q)$. 使 $l=\lfloor\log q\rfloor+1$，$H=(m+1)\times l$，输出 $params=(n,q,\chi,m)$.

$-(pk,sk)\leftarrow MFHE.KeyGen(params)$：

$-sk\leftarrow MFHE.SecretKeyGen(params)$：

对于 $1\leq i\leq t$，随机选取向量 $\bar{\boldsymbol{e}}_i\xleftarrow{R}D_{Z_q^{\bar{m}},r}$，使得 $\boldsymbol{e}_i=[\bar{\boldsymbol{e}}_i|\boldsymbol{I}_i]$，其中 $\boldsymbol{I}_i=(\underbrace{0,\cdots,0}_{\text{共}i-1\text{个}0},1,0,\cdots,0)$表示一个 $t\times 1$ 维列向量，秘密矩阵为$[\boldsymbol{e}_1,\cdots,\boldsymbol{e}_t]=\begin{bmatrix}\bar{\boldsymbol{e}}_1 & & \bar{\boldsymbol{e}}_t\\ \boldsymbol{I}_1 & \cdots & \boldsymbol{I}_t\end{bmatrix}$，输出 t 个私钥 $sk_i=\bar{\boldsymbol{e}}_i=[1,\boldsymbol{e}_i]^{\mathrm{T}}\in Z_q^{(m+1)\times 1}$，$i=1,2,\cdots,t$.

$-pk\leftarrow MFHE.PublicKeyGen(params)$：

首先，选取随机矩阵 $\bar{\boldsymbol{A}}\in Z_q^{n\times\bar{m}}$，然后生成 $\boldsymbol{A}=[\bar{\boldsymbol{A}}|\boldsymbol{U}-\bar{\boldsymbol{A}}\cdot\bar{\boldsymbol{e}}_1|\cdots|\boldsymbol{U}-\bar{\boldsymbol{A}}\cdot\bar{\boldsymbol{e}}_t]$. $\boldsymbol{U}$ 从 $Z_q^{n\times 1}$ 中选取. 最后输出公钥 $pk=K=[\boldsymbol{U}|-\boldsymbol{A}]\in Z_q^{n\times(m+1)}$，易看出 $K\cdot\tilde{\boldsymbol{e}}_i=[\boldsymbol{U}|-\boldsymbol{A}]\cdot(1,\boldsymbol{e}_i)^{\mathrm{T}}=0$.

$-\boldsymbol{C}\leftarrow MFHE.Enc(params,pk,\boldsymbol{M})$：

选取 $\boldsymbol{X}=\begin{pmatrix}\boldsymbol{X}_0\leftarrow\{0\}^{1\times H}\\ \boldsymbol{X}_1\leftarrow\boldsymbol{\chi}^{m\times H}\end{pmatrix}\in Z_q^{(m+1)\times H}$，令 $\boldsymbol{M}=\begin{pmatrix}\boldsymbol{E}_{(\bar{m}+1)\times(\bar{m}+1)} & 0_{(\bar{m}+1)\times t}\\ 0_{t\times(\bar{m}+1)} & \boldsymbol{M}'_{t\times t}\end{pmatrix}\in\{0,1\}^{(m+1)\times(m+1)}$，其中 $\boldsymbol{E}$ 为单位矩阵，$\boldsymbol{M}'_{t\times t}$为对角矩阵，其对角线上的元素 $m'_{i,i}=m_i$.

$$\boldsymbol{C}=\boldsymbol{M}\boldsymbol{G}+\boldsymbol{K}^{\mathrm{T}}\boldsymbol{R}+\boldsymbol{X}(\bmod q)\in Z_q^{(m+1)\times H},$$

其中，$\boldsymbol{G}=BitDecomp^{-1}(\boldsymbol{I}'_{m+1})=(\boldsymbol{g}^{\mathrm{T}}\otimes\boldsymbol{I}'_{m+1})\in Z_q^{(m+1)\times H}$，$\boldsymbol{g}^{\mathrm{T}}=[2^0,\cdots,2^{l-1}]\in Z_q^l$，$l=\lceil\log q\rceil$. $\boldsymbol{R}\leftarrow\{0,1\}^{n\times H}$. 其中 $\boldsymbol{I}'_{m+1}$为 $m+1$ 维单位矩阵.

$-m'_i\leftarrow MFHE.bitDec(params,sk_i,\boldsymbol{C})$：

(1)假设解密第 $i(1\leq i\leq t)$个比特，输入 $sk_i\in Z_q^{(m+1)\times 1}$，定义向量：

$$\boldsymbol{w}^{\mathrm{T}}=[0,\cdots,0|\lceil q/2\rceil,\cdots,\lceil q/2\rceil]$$

其中前$\bar{m}+1$ 个元素为 0，后 t 个元素为$\lceil q/2\rceil$.

(2) 计算 $\tilde{\boldsymbol{e}}_i^{\mathrm{T}}\cdot\boldsymbol{C}=\tilde{\boldsymbol{e}}_i^{\mathrm{T}}\cdot\boldsymbol{K}^{\mathrm{T}}\cdot\boldsymbol{R}+\tilde{\boldsymbol{e}}_i^{\mathrm{T}}\cdot\boldsymbol{X}+\tilde{\boldsymbol{e}}_i^{\mathrm{T}}\cdot\boldsymbol{M}\cdot\boldsymbol{G}=error+\tilde{\boldsymbol{e}}_i^{\mathrm{T}}\cdot\boldsymbol{M}\cdot\boldsymbol{G}$. 令 $\boldsymbol{v}_i=\tilde{\boldsymbol{e}}_i^{\mathrm{T}}\cdot\boldsymbol{C}\cdot\boldsymbol{G}^{-1}(\boldsymbol{w}^{\mathrm{T}})$.

(3) 计算 $\frac{\boldsymbol{v}_i}{q/2}$, 如果接近 0, 则 m_i' 为 0, 反之为 1.

$-m'\leftarrow MFHE.Dec(params,sk,\boldsymbol{C})$:

(1) 假设同时解密 t 个比特, 输入 $sk=\boldsymbol{S}=[\tilde{\boldsymbol{e}}_1,\cdots,\tilde{\boldsymbol{e}}_t]$, 向量 $\boldsymbol{w}$ 与上面相同.

(2) 计算 $\boldsymbol{S}^{\mathrm{T}}\cdot\boldsymbol{C}=\boldsymbol{S}^{\mathrm{T}}\cdot\boldsymbol{K}^{\mathrm{T}}\cdot\boldsymbol{R}+\boldsymbol{S}^{\mathrm{T}}\cdot\boldsymbol{X}+\boldsymbol{S}^{\mathrm{T}}\cdot\boldsymbol{M}\cdot\boldsymbol{G}=\boldsymbol{S}^{\mathrm{T}}\cdot\boldsymbol{M}\cdot\boldsymbol{G}+error$. 令 $\boldsymbol{v}_i=\boldsymbol{S}^{\mathrm{T}}\cdot\boldsymbol{C}\cdot\boldsymbol{G}^{-1}(\boldsymbol{w}^{\mathrm{T}})$.

(3) 输出 $\frac{\boldsymbol{v}_i}{q/2}$.

$-MFHE.Eval(params,\boldsymbol{C}_1,\cdots,\boldsymbol{C}_l)$

$-MFHE.Add(\boldsymbol{C}_1,\boldsymbol{C}_2)$: 输出 $\boldsymbol{C}_1+\boldsymbol{C}_2\in Z_q^{(m+1)\times H}$;

$-MFHE.Mult(\boldsymbol{C}_1,\boldsymbol{C}_2)$: 输出 $\boldsymbol{C}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2)\in Z_q^{(m+1)\times H}$.

3.3.1 方案的正确性

由定理 3 知, 当解密单比特时, $\tilde{\boldsymbol{e}}_i^{\mathrm{T}}\cdot\boldsymbol{C}$ 噪音 $\|error\|\leq B_\chi(r\cdot w\sqrt{\log\bar{m}}+\sqrt{\bar{m}}/2+1)=E$, 当同时解密多比特, $\boldsymbol{S}^{\mathrm{T}}\cdot\boldsymbol{C}$ 噪音 $\|Error\|\leq\max_i\|error_i\|\leq B_\chi(r\cdot w\sqrt{\log\bar{m}}+\sqrt{\bar{m}}/2+1)=E$. 称该密文是 E-$noisy$ 密文. 令 $E_{\mathrm{init}}=B_\chi(r\cdot w\sqrt{\log\bar{m}}+\sqrt{\bar{m}}/2+1)$. 当计算 $\boldsymbol{v}_i$ 时, 噪音 $\|error^{\mathrm{dec}}\|\leq(m+1)\cdot E$, 为能正确解密, 需满足 $\|error^{\mathrm{dec}}\|_\infty\leq q/4$, 即 $E<\frac{q}{4(m+1)}$. 令 $E_{\max}=\frac{q}{4(m+1)}$. 假设 $\boldsymbol{C}_1$ 是 E_1-$noisy$ 密文, $\boldsymbol{C}_2$ 是 E_2-$noisy$ 密文, 则 $\boldsymbol{C}^{\mathrm{Add}}=\boldsymbol{C}_1+\boldsymbol{C}_2$ 是 (E_1+E_2)-$noisy$ 密文. $\boldsymbol{C}^{\mathrm{mult}}=\boldsymbol{C}_1\cdot\boldsymbol{G}^{-1}(\boldsymbol{C}_2)$ 是 $((m+1)E_1+E_2)$-$noisy$ 密文. 对深度为 d 的 NAND 门布尔电路, 一个为 E_{init}-$noisy$ 的密文, 最终密文噪音为 $E_{\mathrm{finnal}}=(m+1)^d\cdot E_{\mathrm{init}}$. 为能达到正确解密, 需满足 $E_{\mathrm{finanl}}\leq E_{\max}$, 通过参数选取可以保证. 详见文献[1].

3.3.2 方案的安全性

选取参数 $params=(n,q,m,\chi,t)$ 满足 $LWE_{n,m,q,\chi}$ 问题的困难性假设, $m=O(n\log q)$, 则该方案是选择明文(IND-CPA)安全.

证明.

(1) 第一, 公钥 $\boldsymbol{K}=[\boldsymbol{U},-\boldsymbol{A}]$ 和从 Z_q 中均匀选取的 $n\times(m+1)$ 阶矩阵统计不可区分.

(2) 第二, 密文 $\boldsymbol{C}$ 和从 Z_q 均匀选取的 $(m+1)\times H$ 阶矩阵计算不可区分. 详细证明见文献[3].

4 该 MFHE 方案的密钥同态性

4.1 密钥同态性定义[24]

设 $F:K\times X\rightarrow Y$ 是一个伪随机函数(PRF), 密钥空间 K 具有群结构并在群上有某种$\oplus$运算; X 与 Y 分别为明文空间与密文空间. 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 $F(k_1\oplus k_2,x)$.

将其定义扩展到多密钥. 假设对某公钥加密方案 E, (pk_i,sk_i) 为该方案的有效公钥/私钥对, 若对 $pk=f(pk_1,pk_2,\cdots,pk_N)$, 能找到 $sk=h(sk_1,sk_2,\cdots,sk_N)$, 使得 (pk,sk) 也是 E 的有效公钥/私钥对, 则称 E 具有密钥同态性质, 其中, f,h 都为概率多项式时间可计算函数. 特别的, 如果 f,h 都为求和函数, 则称 E 具有密钥加同态性质, 如果 f,h 都为乘积函数, 则称 E 具有密钥乘同态性质, 如果 f,h 都为线性函数, 则称 E 具有密钥线性同态性质.

4.2 方案密钥同态性

在该MFHE方案中, 公钥 $pk_i=\boldsymbol{K}_i=[\boldsymbol{U}_i|-\boldsymbol{A}_i]=[\boldsymbol{U}_i|\bar{\boldsymbol{A}}|\boldsymbol{U}_i-\bar{\boldsymbol{A}}\cdot\bar{\boldsymbol{e}}_{i,1}|\cdots|\boldsymbol{U}_i-\bar{\boldsymbol{A}}\cdot\bar{\boldsymbol{e}}_{i,t}]\in Z_q^{n\times(m+1)}$, 其中 $i\in[N]$. 私钥 $\boldsymbol{t}_i=[\tilde{\boldsymbol{e}}_{i,1}^{\mathrm{T}},\cdots,\tilde{\boldsymbol{e}}_{i,t}^{\mathrm{T}}]=\left[\begin{pmatrix}1\\ \bar{\boldsymbol{e}}_{i,1}\\ \boldsymbol{I}_1\end{pmatrix},\cdots,\begin{pmatrix}1\\ \bar{\boldsymbol{e}}_{i,t}\\ \boldsymbol{I}_t\end{pmatrix}\right]\in Z_q^{(m+1)\times t}$. 记 $pk=\boldsymbol{K}=\frac{1}{N}\sum_{i=1}^N\boldsymbol{K}_i$, 用 pk 对明文 $\boldsymbol{M}$ 进行加密得到 $\boldsymbol{C}=\boldsymbol{M}\boldsymbol{G}+\boldsymbol{K}^{\mathrm{T}}\boldsymbol{R}+\boldsymbol{X}$, $\boldsymbol{M},\boldsymbol{X}$ 如上定义. 令 $sk=\boldsymbol{t}=\frac{1}{N}\sum_{i=1}^N\boldsymbol{t}_i$, 用该私钥对密文进行解密. 如果保持公钥 $\boldsymbol{K}_i$ 中 $\bar{\boldsymbol{A}}$ 是不变的, 则该方案具有密钥同态性质.

证明.

$$\begin{aligned}\boldsymbol{t}\cdot\boldsymbol{K}&=\frac{1}{N}\sum_{i=1}^N\boldsymbol{t}_i\cdot\frac{1}{N}\sum_{i=1}^N\boldsymbol{K}_i\\&=\left[\begin{pmatrix}1\\ \frac{1}{N}\sum_{i=1}^N\bar{\boldsymbol{e}}_{i,1}\\ \boldsymbol{I}_1\end{pmatrix},\cdots,\begin{pmatrix}1\\ \frac{1}{N}\sum_{i=1}^N\bar{\boldsymbol{e}}_{i,t}\\ \boldsymbol{I}_t\end{pmatrix}\right]\cdot\\&\quad\left[\frac{1}{N}\sum_{i=1}^N\boldsymbol{U}_i,-\bar{\boldsymbol{A}},-\frac{1}{N}\sum_{i=1}^N(\boldsymbol{U}_i-\bar{\boldsymbol{A}}\cdot\bar{\boldsymbol{e}}_{i,1}),\cdots,\right.\\&\quad\left.\frac{1}{N}\sum_{i=1}^N(\boldsymbol{U}_i-\bar{\boldsymbol{A}}\cdot\bar{\boldsymbol{e}}_{i,t})\right]^{\mathrm{T}}\\&=\sum_{j=1}^t\left(\frac{1}{N}\sum_{i=1}^N\boldsymbol{U}_i-\frac{1}{N}\sum_{i=1}^N\bar{\boldsymbol{A}}\cdot\bar{\boldsymbol{e}}_{i,j}-\right.\end{aligned}$$

$$\frac{1}{N}\sum_{i=1}^{N}\boldsymbol{U}_i+\frac{1}{N}\sum_{i=1}^{N}\bar{\boldsymbol{A}}\cdot\bar{\boldsymbol{e}}_{i,j}\Big)=0,$$

故仍有 $\boldsymbol{t}^{\mathrm{T}}\cdot\boldsymbol{C}=\boldsymbol{t}^{\mathrm{T}}\cdot\boldsymbol{K}^{\mathrm{T}}\cdot\boldsymbol{R}+\boldsymbol{t}^{\mathrm{T}}\cdot\boldsymbol{X}+\boldsymbol{t}^{\mathrm{T}}\cdot\boldsymbol{M}\cdot\boldsymbol{G}=\boldsymbol{t}^{\mathrm{T}}\cdot\boldsymbol{M}\cdot\boldsymbol{G}+error$. 因此仍然可以恢复出明文. 因此在 $\bar{\boldsymbol{A}}$ 不变的情况下，该方案是密钥线性同态的. 接下来证明 $pk=\frac{1}{N}\sum_{i=1}^{N}\boldsymbol{K}_i$ 是安全的，即该公钥不会泄露私钥的任何信息.　　证毕.

证明.　由文献[3]定理 3 知每一个 $\boldsymbol{K}_i, i\in[N]$ 与在 Z_q 中均匀选取的 $n\times(m+1)$ 阶矩阵统计不可区分，故该公钥不会泄露每一个参与方的私钥. 下证该公钥不会泄露联合私钥.

因为，$\sum_{i=1}^{N}\boldsymbol{U}_i\in Z_q^n,\sum_{i=1}^{N}\bar{\boldsymbol{e}}_{i,1},\cdots,\sum_{i=1}^{N}\bar{\boldsymbol{e}}_{i,t}\in Z_q^n$，故该联合公钥仍满足定理 4 以及 LWE 问题，即 $\sum_{i=1}^{N}\boldsymbol{U}_i$ 与均匀选取的向量 $\boldsymbol{\alpha}\in Z_q^n$ 统计不可区分；$\Big[\bar{\boldsymbol{A}}\Big|\sum_{i=1}^{N}\boldsymbol{U}_i-\bar{\boldsymbol{A}}\cdot(\sum_{i=1}^{N}\bar{\boldsymbol{e}}_{i,1})\Big|\cdots\Big|\sum_{i=1}^{N}\boldsymbol{U}_i-\bar{\boldsymbol{A}}\cdot(\sum_{i=1}^{N}\bar{\boldsymbol{e}}_{i,t})\Big]$ 与均匀选取的 $n\times m$ 阶矩阵计算不可区分. 所以联合公钥 $\sum_{i=1}^{N}\boldsymbol{K}_i$ 与均匀选取的 $n\times(m+1)$ 阶矩阵统计不可区分.　证毕.

5　基于该 MFHE 方案的安全多方计算协议

5.1　安全多方计算定义

假设有 N 个参与方，分别记作 $\{P_1,P_2,\cdots,P_N\}$，对于每一个参与方 $\{P_i\}_{i\in[N]}$ 都有一个秘密数据 $\{x_i\}_{i\in[N]}$，一个单输出的安全多方计算协议指的是所有的参与方可以合作计算某个任意概率多项式时间可计算函数 $y=f(x_1,x_2,\cdots,x_N)$，其中 $x_1,x_2,\cdots,x_N$ 分别为 $P_1,P_2,\cdots,P_N$ 的私有数据. 计算结束后，每一个参与方都可以得到计算结果 y，但得不到其他参与方的秘密数据.

在本文中，假设每一个参与方 $\{P_i\}_{i\in[N]}$ 的秘密数据为 $\boldsymbol{x}_i=\{\boldsymbol{x}_{i,1},\boldsymbol{x}_{i,2},\cdots,\boldsymbol{x}_{i,t}\}\in\{0,1\}^t$，与之前逐比特加密相比，我们通过多比特同态加密得到 $\{\boldsymbol{C}_i\}_{i\in[N]}$，做为函数 f 的输入. 最后通过门限解密得到最终的计算结果 $\boldsymbol{y}=f(\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_N)$.

5.2　安全多方计算中敌手模型

在多方安全计算中，通常存在以下的敌手类型. 第一种是半诚实模型，指的是所有的参与方都会严格遵守协议运行，不会主动更改协议或数据，但可能会保留协议间的中间结果以推算其他参与方的秘密数据；第二种是半恶意模型，指的是敌手根据输入和一定的随机性来决定是否忠实履行协议；第三种是恶意模型指的是参与方可以任意篡改、泄露协议和数据，甚至可以阻止协议正常运行.

如果一个安全多方计算协议在半恶意模型下是安全的，在 CRS 模型中则可以通过非交互的零知识证明(NIZKs)转换为恶意模型下也是安全的. 故我们仅考虑该 MPC 协议在半恶意模型下是否安全即可.

本文的基础 MFHE 方案是层次型的，只能做有限次的同态与运算，通过自举可达到任意次的同态运算，但自举会破坏该方案的大部分优势，故本文将构造基于层次型的 MFHE 方案的安全多方计算协议.

π_f：在 CRS 模型下，安全计算单值函数 f 的协议，该协议可以抵抗一个半诚实的敌手或一个半恶意的敌手. 具体如下：

预处理：运行 $params\leftarrow MFHE.Setup(1^\lambda,1^d)$，所有参与方共享参数设置.

输入：共有 N 个参与方，第 i 个参与方记作 P_i；每个参与方拥有私有数据 $\boldsymbol{x}_i=\{\boldsymbol{x}_{i,1},\cdots,\boldsymbol{x}_{i,t}\}\in\{0,1\}^t$. 把 $\boldsymbol{x}_i$ 转变成 $\boldsymbol{M}_i$(与上文一致). 一个多项式时间可计算的确定性函数 $f:(\{0,1\}^{(m+1)\times(m+1)})^N\rightarrow\{0,1\}^{l_{\mathrm{out}}}$，$d$ 为 f 的电路深度.

第一轮。每一个参与方 P_i 执行以下操作.

(1) 生成 $(pk_i,sk_i)\leftarrow MFHE.KeyGen(params)$.

(2) 发布公钥 $\{pk_i\}_{i\in[N]}$.

第二轮. 每一个参与方 P_i 接收他人公钥 $\{pk_j\}_{j\in[N]\setminus\{i\}}$ 并执行以下操作.

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

(2) 利用 pk 计算密文 $\boldsymbol{C}_i=\boldsymbol{K}^{\mathrm{T}}\cdot\boldsymbol{R}_i+\boldsymbol{M}_i\cdot\boldsymbol{G}+\boldsymbol{X}_i$，发布密文 $\{\boldsymbol{C}_i\}_{i\in[N]}$.

第三轮. 每一个参与方 P_i 接收他人密文 $\{\boldsymbol{C}_j\}_{j\in[N]\setminus\{i\}}$ 并执行以下操作.

(1) 进行同态运算 $\boldsymbol{C}\leftarrow Evaluate(pk,f,\boldsymbol{C}_1,\cdots,\boldsymbol{C}_N)$.

(2) 进行门限解密. P_i 选取随机向量 $\boldsymbol{\gamma}_i'\leftarrow\boldsymbol{\chi}^{(\bar{m}+1)l}$，令 $\boldsymbol{\gamma}_i=(\boldsymbol{\gamma}_i',0,\cdots,0)\in\chi^H$，计算 $\boldsymbol{\eta}_i=\boldsymbol{t}_i\cdot\boldsymbol{C}+\boldsymbol{\gamma}_i\in Z_q^H$，然后公布 $\boldsymbol{\eta}_i$.

输出：每一方 P_i 接受他人解密 $\{\boldsymbol{\eta}_j\}_{j\in[N]\setminus\{i\}}$，计

算：$\boldsymbol{\eta}=\frac{1}{N}\sum_{i=1}^{N}\boldsymbol{\eta}_i=t\boldsymbol{C}+\frac{1}{N}\sum_{i=1}^{N}\boldsymbol{\gamma}_i=t\boldsymbol{C}+\boldsymbol{\gamma}$，然后计算 $v=\boldsymbol{\eta}\boldsymbol{G}^{-1}(\boldsymbol{w}^{\mathrm{T}})$，其中 $\boldsymbol{w}^{\mathrm{T}}$ 和上文中一样.

5.3 协议的正确性

首先，该 MFHE 方案在进行 d 层 NAND 门计算之后，最终密文的噪音为 $(m+1)^d E_{\text{init}}$，通过我们的参数选取，可使 $(m+1)^d E_{\text{init}}\leq\frac{q}{4(m+1)}$. 方案可以正确解密.

其次，通过对该方案密钥同态性进行分析，协议 π_f 中所用的密钥对是有效的. 由定理 2 可知，协议 π_f 中的联合误差也是服从 B-有界分布的.

最后证明联合解密的正确性.

证明. 由 $\boldsymbol{\eta}=\frac{1}{N}\sum_{i=1}^{N}\boldsymbol{\eta}_i=t\boldsymbol{C}+\frac{1}{N}\sum_{i=1}^{N}\boldsymbol{\gamma}_i=t\boldsymbol{C}+\boldsymbol{\gamma}$ 可得：

$$\begin{aligned}\boldsymbol{\eta}\boldsymbol{G}^{-1}(\boldsymbol{w}^{\mathrm{T}})&=(t\boldsymbol{C}+\boldsymbol{\gamma})\boldsymbol{G}^{-1}(\boldsymbol{w}^{\mathrm{T}})\\&=t\boldsymbol{C}\boldsymbol{G}^{-1}(\boldsymbol{w}^{\mathrm{T}})+\boldsymbol{\gamma}\boldsymbol{G}^{-1}(\boldsymbol{w}^{\mathrm{T}})\\&=\boldsymbol{\mu}\left\lceil\frac{q}{2}\right\rceil+(\boldsymbol{\gamma}_1^*,\cdots,\boldsymbol{\gamma}_{(\bar{m}+1)\times l}^*,0,\cdots,0)\boldsymbol{G}^{-1}\begin{pmatrix}0\\\vdots\\\left\lceil\frac{q}{2}\right\rceil\\\vdots\\\left\lceil\frac{q}{2}\right\rceil\end{pmatrix}\\&=\boldsymbol{\mu}\left\lceil\frac{q}{2}\right\rceil.\end{aligned}$$

因为 $\boldsymbol{G}^{-1}\left(\left\lceil\frac{q}{2}\right\rceil\right)$ 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，故上式中最后一个等式成立. 证毕.

5.4 协议的安全性

首先考虑在 CRS 模型中，存在一个半诚实的敌手，该协议的安全性.

证明.

(1) 该 MFHE 方案的安全性可以归结为 Ferr-LWE 问题.

(2) 在 $\boldsymbol{\eta}_i=\boldsymbol{t}_i\cdot\boldsymbol{C}+\boldsymbol{\gamma}_i$ 和 $\boldsymbol{\eta}=\boldsymbol{t}\cdot\boldsymbol{C}+\boldsymbol{\gamma}$ 中，由于 $\boldsymbol{\gamma}_i$ 与 $\boldsymbol{\gamma}$ 中前 $(\bar{m}+1)l$ 个分量是服从 B_χ-有界的，故这两个等式构成了 Some-are-errorless. LWE 问题. 因此在第三轮中每一方公布自己的 $\boldsymbol{\eta}_i$ 不会泄露自己的私钥以及联合密钥. 故该协议可以抵抗一个半诚实的敌手.

下面考虑存在半恶意敌手该协议的安全性. 为方便表示，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. 下面给出该协议在半恶意环境中的安全性定理及证明.

定理 6. 设 f 是一个多项式时间可计算的确定性函数，具有 N 个输入，一个输出. 上述的协议 π_f 能够实现 f 在面对一个恰好腐败 $N-1$ 个参与方的半恶意敌手协议是是安全的.

证明. 为针对一个恰好腐败 $N-1$ 个参与方的半恶意敌手，我们构造一个 PPT 模拟器 S，让 A 代表一个静态的半恶意敌手，P_h 代表唯一的诚实方. 模拟器 S 代表诚实方执行以下操作.

在第二轮，模拟器 S 用 0 代替 P_h 的真实输入进行加密. 然后 S 从“证据磁带”中得到 $N-1$ 个腐败方的输入和私钥，S 把这些输入给一个“理想机”并得到输出 $\boldsymbol{y}$，同时可以得到同态计算后密文 $\hat{\boldsymbol{C}}$. 然后 S 为诚实方 P_h 计算模拟部分解密 $\boldsymbol{\rho}_h'\leftarrow S(\boldsymbol{y},\hat{\boldsymbol{C}},h,\{sk_i\}_{i\in[N]\setminus\{h\}})$ 并在第三轮中用模拟部分解密代替真实解密发布出去.

我们定义一系列混合游戏来证明真实和模拟的不可区分，即 $IDEAL_{F,S,Z}\overset{\text{comp}}{\approx}REAL_{\pi,A,Z}$. 其中 Z 代表特定环境.

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 π_f.

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 $\boldsymbol{\rho}_h'\leftarrow S(\boldsymbol{y},\hat{\boldsymbol{C}},h,\{sk_i\}_{i\in[N]\setminus\{h\}})$ 代替真实解密发布出去.

游戏 $IDEAL_{F,S,Z}$：和游戏 $HYB_{\pi,A,Z}$ 基本一样除了在第二轮 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. 两个游戏的不同之处在于 P_h 的真实部分解密 $\boldsymbol{\rho}_h$ 用模拟解密 $\boldsymbol{\rho}_h'$ 所代替. 因此设 $\boldsymbol{v}=\boldsymbol{\mu}\left\lceil\frac{q}{2}\right\rceil+\boldsymbol{e}'$，其模拟解密的算法为

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

$$=N\boldsymbol{\mu}\left\lceil\frac{q}{2}\right\rfloor+\boldsymbol{N}\boldsymbol{e}'+\boldsymbol{\varepsilon}_h'-\sum_{i\neq h}\boldsymbol{v}_i,$$

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

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

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

其中 $\boldsymbol{\varepsilon}_h\leftarrow\chi$.

易知 $\boldsymbol{\varepsilon}_h$ 和 $\boldsymbol{\varepsilon}_h'$ 统计不可区分，故证明了 $\boldsymbol{\rho}_h$ 与 $\boldsymbol{\rho}_h'$ 是不可区分的，结论得证. 证毕.

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

证明. 两个游戏的唯一不同之处在于 P_h 所产生的密文. 由该 MFHE 方案的语义安全性可知密文是计算不可区分的，故这两个游戏也是计算不可区分的. 证毕.

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

接下来根据上述安全协议 π_f 构造一个扩展协议 $\hat{\pi}_f$，该协议能够实现 f 在面对一个能够腐败任意 $t\in[N]$ 个参与方的半恶意敌手协议是安全的.

定义 9. 一个多项式时间可计算的函数 $f:(\{0,1\}^{(m+1)\times(m+1)})^N\rightarrow\{0,1\}^{l_{\text{out}}}$，$l_{\text{out}}\in N$，一个伪随机函数 $PRF:\{0,1\}^{\lambda\times\lambda}\times[N]\rightarrow\{0,1\}^{(m+1)\times(m+1)}$. 我们定义一个扩展函数 $\hat{f}:\{\{0,1\}^{(m+1)\times(m+1)}\times\{\{\underbrace{1,\cdots,1}_{m+1}\}^{\mathrm{T}},\{\underbrace{2,\cdots,2}_{m+1}\}^{\mathrm{T}},\{\underbrace{3,\cdots,3}_{m+1}\}^{\mathrm{T}}\}\times\{0,1\}^{(m+1)\times\lambda}\}\rightarrow\{0,1\}^{l_{\text{out}}}$，$\hat{f}$ 的输入为 $((x_1,\text{mode}_1,z_1),\cdots,(x_N,\text{mode}_N,z_N))$，其中：

(1) 如果对任意 $i\in N$ 有 $\text{mode}_i=\underbrace{\{1,\cdots,1\}}_{m+1}$，输出 $f(x_1,\cdots,x_n)$.

(2) 如果有唯一的 $i\in N$ 使得 $\text{mode}_i=\underbrace{\{2,\cdots,2\}}_{m+1}$，令 $K:=Z_i$. 对所有的 $j\in[N]$：

① 如果 $\text{mode}_j=\underbrace{\{3,\cdots,3\}}_{m+1}$，令 $x_j':=PRF(K,j)\oplus x_j$.

② 否则令 $x_j':=x_j$.

(3) 其余情况输出 $0^{l_{\text{out}}}$.

最后描述扩展协议 $\hat{\pi}_f$，实际上就是运行协议 $\pi_{\hat{f}}$，其中 $\hat{f}$ 为扩展函数，其输入为扩展输入 $((x_1,\text{mode}_1,z_1),\cdots,(x_N,\text{mode}_N,z_N))$. 该扩展协议 $\hat{\pi}_f$ 与原协议 π_f 的不同之处在于输入阶段，在协议 $\hat{\pi}_f$ 中，每个参与方 P_k 的输入为 $\hat{x}_k:=(x_k,\text{mode}_k,z_k)$，其中 $\text{mode}_k:=\underbrace{\{1,\cdots,1\}}_{(m+1)}$，$z_k:=\boldsymbol{0},\boldsymbol{0}$ 表示合适尺寸的全为 0 的字符串. 参与方使用 $\{\hat{x}_k\}_{k\in N}$ 运行协议 $\pi_{\hat{f}}$，最后输出结果.

定理 7. 扩展协议 $\hat{\pi}_f$ 能够实现 f 在面对一个能够腐败任意 $t\in[N]$ 个参与方的半恶意敌手协议是安全的. 详见文献[9].

5.5 协议的性能

文献[9]与文献[21]中都为单比特的安全多方计算，若参与方的输入为 t 比特，上述两方案需重复执行 t 次，本文只需一次，故在时间效率上优于已有的方案，如表 1 所示. 在空间效率上，本文的密文同样不会发生膨胀.

表 1　基于全同态加密方案的安全多方计算性能对比

方案	轮数	密文膨胀率	基础方案	与非门复杂度
文献[9]	2	$O(1)$	GSW(13)	$\tilde{O}(tN(nd)^{\omega})$
文献[21]	3	$O(1)$	GSW(13)	$\tilde{O}(t(nd)^{\omega})$
本文	3	$O(1)$	GSW(13)	$\tilde{O}((nd)^{\omega})$

6　结　论

基于多比特的全同态加密方案构造了一个层次型的多密钥多比特安全多方计算协议，该协议在半诚实环境下的安全性可以归结到 Ferr-LWE 问题以及 Some-are-errorless.LWE 问题；在半恶意环境下，通过定义一系列混合游戏证明了 $IDEAL_{F,S,Z}\approx REAL_{\pi,A,Z}$，从而证明了该协议的安全性. 该协议构造简单，只需三轮通信，且是第一个同时加密多比特的安全多方计算协议.

该协议还有需要改进之处. 首先，该 MFHE 方案的效率不高，无法达到实用的标准，需要通过一些处理来提高效率. 其次，在协议执行的过程当中，需保证数据的安全传输及会话的协同性.

致　谢　感谢审稿专家的宝贵意见！

参　考　文　献

[1] Yao A. Protocols for secure computations//Proceedings of the 23rd Annual Symposium on Foundations of Computer

Science. New York, USA, 1982: 160-164
[2] Rivest R L, Adieman L, Dertouzos M L. On data banks and privacy homomorphisms//Foundations of Secure Computation, Richard Lipton. USA, 1978: 169-180
[3] Li Z, Ma C, Morais E, et al. Multi-bit leveled homomorphic encryption via Dual. LWE-based//Proceedings of the International Conference on Information Security and Cryptology. Seoul, Korea, 2017: 221-242
[4] Goldreich O, Micali S, Widgerson A. How to play a mental game//Proceedings of the 19th Annual ACM Conference on Theory of Computing. New York, USA, 1998: 218-229
[5] Goldreich O. Secure multi-party computation (working draft, Version 1.1)//van Tilborg H C A, Jajodia S, eds. Encryption of Cryptography and Security. Fairfax, USA, 2010: 47-59
[6] Gennaro R, Rabin M, Rabin T. Simplified VSS and fast-track multiparty computation with application to threshold cryptography//Proceedings of the 17th Annual ACM Symposium on Principles of Distributed Computing, Puerto Vallarta, Mexico, 1998: 101-111
[7] Jakobsson M, Juels A. Mix and match: Secure function evaluation via ciphertexts//Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology-ASIACRYPT 2000. Kyoto, Japan, 2000: 162-177
[8] Clear M, McGoldrick C. Multi-identity and multi-key leveled FHE from learning with errors//Gennaro R, Robshaw M J B, eds. CRYPTO 2015, Part II. Heidelberg, Germany: Springer, 2015, 9216: 630-656
[9] Mukherjee P, Wichs D. Two round multiparty computation via multi-key FHE//Fischlin M, Coron J-S, eds. EUROCRYPT 2016, Part II. Heidelberg, Germany: Springer, 2016, 9666: 735-763
[10] Brakerski Z, Halevi S, Polychroniadou A. Four round secure computation without setup//Proceedings of the Theory of Cryptography. Baltimore, USA, 2017: 678-710
[11] Gentry C. Fully homomorphic encryption using ideal lattices//Proceedings of the 41st Annual ACM Symposium on Theory of Computing. Bethesda, USA, 2009: 169-178
[12] Smart N P, Vercauteren F. Fully homomorphic encryption with relatively small key and ciphertext sizes//Nguyen P Q, Pointcheval D, eds. PKC 2010. Heidelberg, Germany: Springer, 2010, 6056: 420-443
[13] Stehle D, Steinfeld R. Faster fully homomorphic encryption//Abe M ed. ASIACRYPT 2010. Heidelberg, Germany: Springer, 2010, 6477: 377-394
[14] Loftus J, May A, Smart N P, et al. On CCA-secure somewhat homomorphic encryption//Miri A, Vaudenay S, eds. SAC 2011. Heidelberg, Germany: Springer, 2012, 7118: 55-72
[15] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping//Innovations in Theoretical Computer Science (ITCS 2012). Cambridge, Massachusetts, 2012: 309-325
[16] Brakerski Z. Fully homomorphic encryption without modulus switching from classical GapSVP//Safavi-Naini R, Canetti R, eds. CRYPTO 2012. Heidelberg, Germany: Springer, 2012, 7417: 868-886
[17] Brakerski Z, Vaikuntanathan V. Lattice-based FHE as secure as PKE//Innovations in Theoretical Computer Science (ITCS 2014). Princeton New Jersey, USA, 2014: 1-12
[18] Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors conceptually-simpler, asymptotically-faster, attribute-based//Canetti R, Garay J A, eds. CRYPTO 2013, Part I. Heidelberg, Germany: Springer, 2013, 8042: 75-92
[19] Stehle D, Steinfe R. Making NTRU as secure as worst-case problems over ideal lattices//Proceedings of the Advances in Cryptology-EUROCRYPT 2011. Tallinn, Estonia, 2011: 27-47
[20] Micciancio D, Peikert C. Trapdoors for lattices: Simpler, tighter, faster, smaller//Proceedings of the EUROCRYPT 2012. Cambridge, UK, 2012: 700-718
[21] Wang Hui-Yong, Feng Yong, Zhao Ling-Zhong, Tang Shi-jie. A secure multi-party computation protocol on the basis of multi-key homomorphism. Journal of South China University of Technology (Natural Science Edition), 2017, 45(7): 69-76
[22] Agrawal S, Boneh D, Boyen X. Efficient lattice (H)IBE in the standard model//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Riviera, France, 2010:553-572
[23] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic Eencryption from (Standard) LWE. SIAM Journal on Computing, 2014, 43(2):831-871
[24] Boneh D, Lewi K, Montgomery H, et al. Key homomorphic PRFs and their Applications//Proceedings of the Annual Cryptology Conference. Santa Barbara, USA, 2013: 410-428

TANG Chun-Ming, Ph. D., professor, Ph. D. supervisor. His research interests include cryptography and its applications.

HU Ye-Zhou, M. S. candidate. His research interests include fully homomorphic encryption and secure multi-party computation protocol.

Background

With the development of cloud computing, people pay more and more attention to privacy protection. The emergence of fully homomorphic encryption allows people to operate on ciphertext, thus it protects individuals' private data. Secure multi-party computation allows participants to compute a function together without revealing any private information about themselves, It has been a research hotspot.

This paper constructs the first three-round multi-bit secure multi-party computation protocol using a multi-bit fully homomorphic encryption. Unlike previous protocols, the protocol in this article allows participants to enter more than one bit of data at a time, we prove shat the security of the secure multi-party computing protocol is based on the variants of the Learning with Errors Problem (LWE) called Ferr-LWE and Some-are-errorless. LWE.

This research was supported in part by the National Natural Science Foundationof China (61772147), in part by the Guangdong province Natural Science Foundation of Major Basic Research and Cultivation Project (2015A030308016), in part by the National Cryptography Development Fund (MMJJ20170117), in part by the Open Project of State Key Laboratory of Cryptography Science and Technology (MMKFKT201913), in part by the Collaborative Innovation Major Projects of Bureau of Bureau of Education of Guangzhou City (1201610005), and in part by the Basic Innovation Program of Graduate Students of Guangzhou University (2019GDJC-M28).