同态明文−密文矩阵运算及其应用

刘洋[1]，杨林翰[1]，陈经纬[2,3]，吴文渊[2,3]，冯勇[2,3]

（1. 重庆交通大学信息科学与工程学院，重庆 400074；
2. 中国科学院重庆绿色智能技术研究院生物计算安全重庆市重点实验室，重庆 400714；
3. 中国科学院大学重庆学院，重庆 400714）

摘 要：支持单指令多数据操作的同态加密方案能有效提高密文计算的均摊效率，但密文结构导致矩阵运算复杂度高。在许多应用中，采用明文−密文矩阵操作可以在确保安全的同时实现隐私计算。基于此，提出一个适用于任意维数的明文−密文矩阵乘法方案。该方案通过明文矩阵编码和密文矩阵维数变换等步骤计算得到密文结果。与已知最好的 Jiang 等所提的密文方阵乘法算法相比，所提方案支持任意维数的矩阵乘法，并支持矩阵连乘；理论分析和实验结果均表明，所提方案具有更低的密文旋转复杂度和更高的计算效率。将所提方案应用在隐私保护的贝叶斯分类器中，能以更高安全参数和更少计算时间完成分类任务。

关键词：同态加密；矩阵运算；机器学习；贝叶斯分类器

中图分类号：TN92

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2024024

Matrix computation over homomorphic plaintext-ciphertext and its application

LIU Yang[1], YANG Linhan[1], CHEN Jingwei[2,3], WU Wenyuan[2,3], FENG Yong[2,3]

1. School of Information Science and Engineering, Chongqing Jiaotong University, Chongqing 400074, China
2. Chongqing Key Laboratory of Secure Computing for Biology, Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences, Chongqing 400714, China
3. Chongqing School, University of Chinese Academy of Sciences, Chongqing 400714, China

Abstract: Those homomorphic encryption schemes supporting single instruction multiple data (SIMD) operations effectively enhance the amortized efficiency of ciphertext computations, yet the structure of ciphertexts leads to high complexity in matrix operations. In many applications, employing plaintext-ciphertext matrix operations can achieve privacy-preserving computing. Based on this, a plaintext-ciphertext matrix multiplication scheme for matrices of arbitrary dimension was proposed. The resulting ciphertext was computed through steps such as encoding the plaintext matrix, transforming the dimensions of the encrypted matrix, etc. Compared to the best-known encrypted matrix multiplication algorithm for square matrices proposed by Jiang et al., the proposed scheme supported matrix multiplication of arbitrary dimension, and consecutive matrix multiplications. Both theoretical analysis and experimental results show that the proposed scheme requires less rotations on ciphertexts and hence features higher efficiency. When applied to a privacy-preserving Bayesian classifier, the proposed scheme can complete classification tasks with higher security parameters and reduced running time.

Keywords: homomorphic encryption, matrix computation, machine learning, Bayesian classifier

---

收稿日期：2023−11−02；**修回日期**：2023−12−14

通信作者：陈经纬，jingwei.chen@outlook.com

基金项目：国家重点研发计划基金资助项目（No.2020YFA0712303）；重庆市自然科学基金资助项目（No.CSTB2023NSCQ-MSX0441, No.cstc2021jcyj-msxmX0821, No.cstc2021yszx-jcyjX0004, No.2022YSZX-JCX0011CSTB, No.CSTB2023YSZX-JCX0008）

Foundation Items: The National Key Research and Development Program of China (No.2020YFA0712303), The Natural Science Foundation of Chongqing (No.CSTB2023NSCQ-MSX0441, No.cstc2021jcyj-msxmX0821, No.cstc2021yszx-jcyjX0004, No.2022YSZX-JCX0011CSTB, No.CSTB2023YSZX-JCX0008)

0　引言

机器学习领域的蓬勃发展，为众多领域提供了广泛的应用和服务。其中一个典型应用场景是供应商使用大量用户数据训练模型，并使用训练好的模型根据用户需求提供数据预测服务。虽然机器学习在提高社会生产力方面有着巨大的进步，但大量共享数据集也带来了严重的隐私安全问题。特别是当机器学习模型依赖于机密数据（如金融、医疗和个人数据）时，数据的安全性和隐私性尤其重要，因为模型拥有者不希望数据泄露与模型有关的信息，而数据拥有者也不希望模型泄露与数据相关的信息。为了解决这些矛盾，隐私保护机器学习已成为近年来的研究热点。

在绝大多数情况下，如果模型拥有者能够训练出大规模模型，那么通常该拥有者也能满足计算方的性能需求，因此，模型拥有者通常也是计算方。在密文计算的过程中，重点是确保数据拥有者的信息对计算方不可见，而不需要保证模型拥有者对计算方不可见。所以，在进行隐私保护机器学习的过程中，着重考虑计算方和客户端之间的隐私关系，即使模型数据以明文信息进行计算也能保证模型不被泄露。

常见的隐私保护机器学习方法包括差分隐私[1-4]、多方安全计算[5-7]、联邦学习[8-10]以及同态加密[11]等。差分隐私通过在处理数据之前添加随机噪声来保护个人数据隐私。多方安全计算实现多个参与者进行计算，但相互只能看见自己的输入和输出。联邦学习则通过共享机器学习过程中的部分参数，所有参与者共同训练获得全局最优的模型。同态加密是一种加密方案，它允许对加密的输入进行操作，且解密的结果与明文相应操作的结果匹配[11]。同态加密不仅可以提供可证安全和抗量子安全，而且理论上可以达到最优的交互次数，因此被认为是最有前途的隐私保护解决方案之一，已被成功应用于统计分析[10]、线性回归[12-16]、贝叶斯模型预测[17-21]、主成分分析[22-24]以及神经网络预测[25-27]和训练[28-30]等数据处理和分析中。

全同态加密方案的概念最早由 Rivest 等在 1978 年提出。自 2009 年 Gentry[31]开创性地提出自举的构想，并设计出第一个全同态加密方案以来，各种方案不断涌现。以 Gentry 为代表的第一代全同态加密方案效率低，并且基于非标准困难性假设，安全性不足。以 BGV（Brakerski-Gentry-Vaikuntanathan）[32]、BFV（Brakerski-Fan-Vercanteren）[33]为代表的第二代全同态加密方案适用于事先给定乘法深度的整数计算任务，支持自举，但代价昂贵。以 FHEW（fully homomorphic encryption of the west）[34]和 TFHE（fully homomorphic encryption over the Torus）[35]方案为代表的第三代全同态加密方案支持快速自举，因此可以实现任意深度的密文计算任务，尤其适用于基于门电路的计算任务。以 CKKS（Cheon-Kim-Kim-Song）[36]为代表的第四代全同态加密方案支持浮点运算，被广泛应用于隐私保护机器学习。目前，全同态加密的大规模应用仍然受到效率较低的瓶颈限制。

尽管引入了单指令多数据（SIMD, single instruction multiple data）的批处理[37]、快速自举[35, 38]等技术来优化同态加密方案的效率，但即使是当前最快的同态加密方案，其计算速度仍然远低于明文计算速度[39]。并且，这些同态加密方案都只提供了算术或逻辑的基本操作（如 BGV、BFV 提供密文加法和乘法运算，TFHE 提供与非门等逻辑门的密文赋值），更复杂的运算操作需要在这些基本操作的基础上来构建，例如向量内积、矩阵乘法等。矩阵乘法是最常见的运算操作之一，许多机器学习应用都涉及大量的矩阵乘法，因此同态密文矩阵乘法逐渐成为密文计算的重点。而考虑到模型和数据的实际关系，研究高效同态明文−密文矩阵乘法对同态加密应用到隐私保护机器学习具有深远的意义。

设 $\mathcal{R}$ 是一个环，$\boldsymbol{A}\in\mathcal{R}^{n\times m}$ 和 $\boldsymbol{B}\in\mathcal{R}^{m\times p}$ 为 $\mathcal{R}$ 的 2 个矩阵，$d=\max(n,m,p)$ 表示矩阵最大的维数。则计算 $\boldsymbol{X}=\boldsymbol{AB}\in\mathcal{R}^{n\times p}$ 本质上是一系列向量内积运算。若按照常规方式完成 2 个 $\boldsymbol{X}=\boldsymbol{AB}$ 的密文矩阵乘法，则总共需要 np 次密文乘法和 $np\log m$ 次密文旋转。Halevi 等[40]于 2014 年将矩阵对角线编码[41]与 SIMD 相结合，完成了对矩阵−向量乘法密文运算的加速。针对一个 $n\times m$ 的矩阵和一个 m 维向量相乘的情形，该方法需 n 次密文乘法和 n 次密文旋转，随后 Halevi 等[42]采用小步大步法将所需的密文旋转次数降低到 $2\sqrt{n}$。Rathee 等[24]提出了一种密文方阵的乘法方案，需要 d 次密文乘法和 $d\log d+d$ 次密文旋转；Huang 等[43]对其进行优化改进并提出了非方阵的版本，需要 d 次密文乘法和 $m\log d+m$ 次密文旋转。2018 年，Jiang 等[25]基于 Halevi 等[40]的矩阵−向量乘法提出了一种密文矩阵乘法的新方

法，该方法仅需要 d 次密文乘法和 $3d+5\sqrt{d}$ 次密文旋转就可以完成 $\boldsymbol{X}=\boldsymbol{AB}$ 的密文计算，但只讨论了方阵相乘（即 $n=m=p$ ）的情形并且明确要求加密方案的参数需要选取得足够大，以使 SIMD 操作对应的明文槽大于 n^2，但这势必会影响方案的计算效率。近些年，Huang 等[44]优化了 Jiang 等[25]方法中的分块方法，有效提高大规模矩阵的运算效率。Jang 等[45]则针对张量结构通过修改 CKKS 方案，优化 Jiang 等[25]方法中的密文旋转和乘法次数，但在明文−密文乘法下的开销与 Jiang 等[25]方法相同。尽管如此，在最近的研究中[46]，Jiang 等[25]提出的方法仍然是目前最快的密文矩阵乘法方法之一。

另一些研究则将明文信息编码到多项式系数上。Duong 等[47]推广了 Yasuda 等[48-49]安全内积的方法，将明文信息编码到多项式系数上，仅需一次同态乘法就能完成密文矩阵乘法。随后 Mishra 等[50]进行了改进，提高了明文槽的利用率。然而这种方法在计算过程中会产生无意义的项，导致对空间的利用率低，并对连续矩阵乘法不友好等。

本文主要的研究工作如下。

1) 提出一种适用于明文−密文矩阵乘法的编码方法，该编码支持任意维数的明文−密文矩阵乘法。在这种编码方式下，矩阵 $\boldsymbol{X}=\boldsymbol{AB}$ 的密文计算（算法 4）只考虑矩阵 $\boldsymbol{A}$ 为明文方阵（即 $n=m$ ）和矩阵 $\boldsymbol{B}$ 为密文矩阵（ $m\times p$ ）的情况。算法 4 完成单次明文−密文矩阵乘法需要 $3\sqrt{m}$ 次旋转操作和 $2m-1$ 次乘法操作。本文将 Halevi 等[42]方案和 Jiang 等[25]方案在明文−密文矩阵乘法的情况下与所提方案的计算开销进行比较，结果如表 1 所示。其中，$d=\max\{n,m,p\}$ 表示按照其中最大的维数进行矩阵到方阵的变换，CMult 表示进行明文−密文乘法的深度。

2) 提出了算法 5，实现对密文矩阵进行维数变换。在计算 $\boldsymbol{X}=\boldsymbol{AB}$ 时，算法 4 需要将编码后的矩阵 $\boldsymbol{B}$ 加密为一条密文。当明文矩阵 $\boldsymbol{A}$ 中 $n>m$ 时，在进行矩阵到方阵转换时会变成 $n\times n$ 的方阵，因此需要将密文矩阵 $\boldsymbol{B}$ 也从 $m\times p$ 转换成 $n\times p$ 的矩阵，将单条密文的信息进行对齐，以便进行下一步的明文−密文矩阵乘法操作。算法 5 完成一次维数变换需要 $2\sqrt{p}$ 次旋转操作和 p 次乘法操作。实验结果表明，当 $m\geqslant n$ 时，完成明文−密文矩阵乘法计算只需执行算法 4，由于算法 4 的计算开销与 p 无关，因此当 $p>m\geqslant n$ 时，计算明文−密文矩阵乘法更加高效。

3) 基于 SEAL 同态加密库中的 CKKS 方案，本文实现了的算法 4 和算法 5，并将其应用于隐私保护的贝叶斯分类器中，与 Chen 等[17]的相关工作相比，对于来自 UCI 机器学习库中的几个数据集，在分类精度并无明显降低的前提下，本文方案可以以更高的安全参数和更低的计算时间完成分类任务。

1 预备知识

首先对本文一些常用的记号说明如下。对于 2 个正整数 i 和 k，用 $[i]_k$ 表示 i 模 k 的非负剩余。所有的向量都用斜粗体的小写字母表示，如 $\boldsymbol{a}$、$\boldsymbol{b}$，其分量的下标从 0 开始，使用 $\rho(\boldsymbol{a};\ell)$ 表示对向量 $\boldsymbol{a}$ 进行移位。矩阵用斜粗体的大写字母表示，如 $\boldsymbol{A}$、$\boldsymbol{B}$。对于环 $\mathcal{R}$ 上的 $n\times m$ 矩阵 $\boldsymbol{A}=(a_{i,j})$，其下标范围为 $0\leqslant i<n, 0\leqslant j<m$。

1.1 同态加密

同态加密允许在不进行解密的条件下对密文直接计算得到与明文对应的计算结果。令 $\mathcal{M}$ 和 $\mathcal{C}$ 分别表示明文空间和密文空间。一个同态加密方案 HE 由如下随机算法组成。Setup(1^λ)：输入安全参数 λ，输出公钥 pk、公开的计算密钥 ek 和私钥 sk。$\mathrm{Enc}_{\mathrm{pk}}(\boldsymbol{m})$：使用公钥 pk 加密消息 $\boldsymbol{m}\in\mathcal{M}$，输出密文 $\boldsymbol{c}\in\mathcal{C}$。$\mathrm{Dec}_{\mathrm{sk}}(\boldsymbol{c})$：使用私钥 sk 解密密文 $\boldsymbol{c}\in\mathcal{C}$，输出明文 $\boldsymbol{m}\in\mathcal{M}$。$\mathrm{Eval}_{ek}(f;(\boldsymbol{c}_1,\cdots,\boldsymbol{c}_k))$：输入电路 $f:\mathcal{M}^k\to\mathcal{M}$ 和密文 $\boldsymbol{c}_1,\cdots,\boldsymbol{c}_k$，使用计算密钥 ek 计算并输出密文 $\boldsymbol{c}\in\mathcal{C}$。

当同态加密方案 HE 具有如下性质时，称其是

表 1 一次明文−密文矩阵乘法方案计算开销比较

方案	密文加法	明文−密文乘法	密文旋转	密文条数	密文深度
Halevi 等[42]	$2p\sqrt{n}$	pn	$2p\sqrt{n}$	p	1CMult
Jiang 等[25]	$4d$	$2d$	$d+2\sqrt{d}$	1	2CMult
本文算法 4	$2m-1$	$2m-1$	$3\sqrt{m}$	1	1CMult
本文算法 4+算法 5	$p+m+n-1$	$p+m+n-1$	$2(\sqrt{p}+\sqrt{m+n-1})$	1	2CMult

正确的。对于任意的 $\boldsymbol{m}\in\mathcal{M}$ 及其对应的任意密文 $\boldsymbol{c}\leftarrow\mathrm{Enc}_{\mathrm{pk}}(\boldsymbol{m})$，都有 $\Pr[\mathrm{Dec}_{\mathrm{sk}}(c)\neq\boldsymbol{m}]=\mathrm{negl}(\lambda)$ 中的结果，其中 $\mathrm{negl}(\lambda)$ 表示一个关于 λ 可忽略的函数。对于任意的电路 $f:\mathcal{M}^k\to\mathcal{M}$、密文 $\boldsymbol{c}_i\leftarrow\mathrm{Enc}_{\mathrm{pk}}(\boldsymbol{m}_i)$，以及相应的计算结果密文 $\boldsymbol{c}\leftarrow\mathrm{Eval}_{\mathrm{ek}}(f;(\boldsymbol{c}_1,\cdots,\boldsymbol{c}_k))$，有 $\Pr[\mathrm{Dec}_{\mathrm{sk}}(\boldsymbol{c})\neq f(\boldsymbol{m}_1,\cdots,\boldsymbol{m}_k)]=\mathrm{negl}(\lambda)$。

由于 pk 和 ek 都是公开的，为了方便起见，下面用 pk 表示公钥和计算密钥等所有公开的密钥，并且如无特殊说明，将在基本操作中省略不写。例如，本文将用到密文加法、密文乘法、明文−密文乘法等基本操作。$\mathrm{Add}(c_1\in\mathcal{C},c_2\in\mathcal{C})$：输出密文 $\boldsymbol{c}$，使 $\Pr[\mathrm{Dec}_{\mathrm{sk}}(\boldsymbol{c})\neq\mathrm{Dec}_{\mathrm{sk}}(\boldsymbol{c}_1)+\mathrm{Dec}_{\mathrm{sk}}(\boldsymbol{c}_2)]=\mathrm{negl}(\lambda)$。$\mathrm{Mult}(c_1\in\mathcal{C},c_2\in\mathcal{C})$：输出密文 $\boldsymbol{c}$，使 $\Pr[\mathrm{Dec}_{\mathrm{sk}}(\boldsymbol{c})\neq\mathrm{Dec}_{\mathrm{sk}}(\boldsymbol{c}_1)\mathrm{Dec}_{\mathrm{sk}}(\boldsymbol{c}_2)]=\mathrm{negl}(\lambda)$。$\mathrm{CMult}(\boldsymbol{m}\in\mathcal{M},\boldsymbol{c}\in\mathcal{C})$：输出密文 $\boldsymbol{c}'$，使 $\Pr[\mathrm{Dec}_{\mathrm{sk}}(\boldsymbol{c}')\neq\boldsymbol{m}\mathrm{Dec}_{\mathrm{sk}}(\boldsymbol{c})]=\mathrm{negl}(\lambda)$。

若同态加密方案 HE 支持 SIMD[37]操作，则其明文空间 $\mathcal{M}$ 可以看作环 $\mathcal{R}$ 上的 n 维向量形成的集合 $\mathcal{R}^n$。此时，$\mathcal{R}^n$ 中的任意元素 $\boldsymbol{m}$ 在编码后可以被加密成一条密文，在进行密文计算时，相当于对 $\boldsymbol{m}$ 的每个分量（明文槽）并行地进行相应的计算，从而使 HE 达到更好的均摊性能。在计算过程中，可能需要对 $\boldsymbol{m}$ 的明文槽间的数据进行操作，例如密文旋转。$\mathrm{Rot}(\boldsymbol{c}\in\mathcal{C};\ell\in\mathbb{Z})$：输入明文信息 $\boldsymbol{m}=(m_0,m_1,\cdots,m_{n-1})\in\mathcal{M}=\mathcal{R}^n$ 的一个密文 $\boldsymbol{c}\in\mathcal{C}$ 和一个整数 ℓ，输出 $\boldsymbol{c}'$ 使 $\Pr[\mathrm{Dec}_{\mathrm{sk}}(\boldsymbol{c}')\neq\rho(\boldsymbol{m};\ell)]=\mathrm{negl}(\lambda)$，其中 $\rho(\boldsymbol{m};\ell)=(m_\ell,\cdots,m_{n-1},m_0,\cdots,m_{\ell-1})$ 表示将 $\boldsymbol{m}$ 的分量依次向左旋转 ℓ 个明文槽得到的新明文。

由于密文旋转后需要进行代价昂贵的密钥交换操作，因此其开销比密文乘法和密文加法都大，而密文乘法的开销又远大于密文加法。除此之外，同态密文计算的乘法深度会影响参数的选取，从而影响计算性能。因此，本文仅统计密文乘法次数、密文旋转次数以及密文乘法深度，并以这些指标作为衡量计算性能的关键指标。

1.2　Halevi 等的矩阵−向量乘法

作为矩阵乘法的一种特殊情形，矩阵−向量乘法已研究得比较成熟[40]。

设 $\boldsymbol{A}\in\mathcal{R}^{n\times m}$，$\boldsymbol{v}\in\mathcal{R}^{m\times1}$，记 $\boldsymbol{u}=\boldsymbol{A}\boldsymbol{v}\in\mathcal{R}^n$。Halevi 等[40]算法的基本思想是对矩阵采用对角线编码。文献[40]只给出了 $m=n$ 的情形，这里给出更为一般的 n 整除 m 的情形描述。设 $m=nq$。则矩阵 $\boldsymbol{A}=(a_{i,j})_{0\leqslant i<n,0\leqslant j<m}$ 的对角线编码方式为对于 $0\leqslant\ell<n$，定义 $\boldsymbol{A}$ 的第 ℓ 个对角向量为

$$\begin{aligned}d_\ell(\boldsymbol{A})=(&a_{0,\ell},\cdots,a_{n-1,n+\ell-1},a_{0,n+\ell},\cdots,a_{n-1,2n+\ell-1},\cdots,\\&a_{0,[(q-1)n+\ell]_m},\cdots,a_{n-1,[m+\ell-1]_m})\in\mathcal{R}^m\end{aligned}\tag{1}$$

在得到这样的对角线编码之后，$\boldsymbol{u}=\boldsymbol{A}\boldsymbol{v}$ 的计算可以分为如下 2 个步骤。

1) 计算

$$\boldsymbol{u}=\sum_{0\leqslant\ell<n}(\rho(\boldsymbol{v};\ell)\odot\boldsymbol{d}_\ell)\tag{2}$$

其中，$\odot$ 表示矩阵的 Hadamard 乘积，即按分量对应相乘。

2) 更新

$$\boldsymbol{u}=\sum_{0\leqslant i<q}\rho(\boldsymbol{u};in),\quad q=\frac{m}{n}\tag{3}$$

显然，式(2)的计算需要对向量 $\boldsymbol{v}$ 进行 n 次旋转操作。若 $n=kl$，则可以采用小步大步法进一步将旋转操作的次数降至 $k+l$ 次。这是因为式(2)可以重写为

$$\begin{aligned}\boldsymbol{u}=&\sum_{i=0}^{l-1}\sum_{j=0}^{k-1}(\rho(\boldsymbol{v};ki+j)\odot\boldsymbol{d}_{ki+j})=\\&\sum_{i=0}^{l-1}\rho\left(\sum_{j=0}^{k-1}\Big(\rho(\boldsymbol{v};j)\odot\rho(\boldsymbol{d}_{ki+j};-ki)\Big);ki\right)\end{aligned}\tag{4}$$

在事先计算好 $\rho(\boldsymbol{d}_{ki+j};-ki)$ 的情况下（即将矩阵 $\boldsymbol{A}$ 按此编码成 n 个向量），仅需对向量 $\boldsymbol{v}$ 进行 $k+l$ 次[42]旋转操作便能够完成 $\boldsymbol{u}$ 的计算。根据式(3)和式(4)，将明文向量对应到密文向量，ρ 对应密文旋转 Rot 操作，$\odot$ 对应明文−密文乘法 CMult 操作，得到如算法 1 所示的密文矩阵−向量乘法算法。

算法 1　矩阵−向量乘法算法

对所有 $0\leqslant i<l$，$0\leqslant j<k$ 的 $\boldsymbol{c}_{i,j}$ 初始化，其中 $\boldsymbol{c}_{i,j}$ 对应明文 $\rho(\boldsymbol{d}_{ki+j};-ki)$ 的密文，$\boldsymbol{d}_\ell$ 是矩阵 $\boldsymbol{A}\in\mathcal{R}^{n\times m}$ 的第 ℓ 个对角向量，且 $n=kl$，m 是 n 的整数倍；初始化密文向量 $\boldsymbol{c}\in\mathcal{C}$，对应明文 $\boldsymbol{v}\in\mathcal{R}^{m\times1}$ 的密文；初始化密文向量 $\boldsymbol{c}'=\mathrm{Enc}_{\mathrm{pk}}(\boldsymbol{0})$。

1) 根据式(4)中 $\boldsymbol{u}$ 在密文下计算 $\boldsymbol{c}'$；

2) 根据式(3)中 $\boldsymbol{u}$ 在密文下更新 $\boldsymbol{c}'$；

3) 返回 $\boldsymbol{c}'$；

步骤 1) 需要 n 次密文乘法和 $k+l$ 次密文旋转（当 $k\approx l$ 时，$k+l\approx2\sqrt{n}$）。尽管式(3)表面上需要 q 次旋转，但采用二分法容易证明 $\log q$ 次旋转便足够了。因此，步骤 2) 至多需要 $\log q=\log\frac{m}{n}$ 次密文旋转。设 $\boldsymbol{A}\in\mathcal{R}^{n\times m}$，$\boldsymbol{B}\in\mathcal{R}^{m\times p}$，若将计算 $\boldsymbol{X}=\boldsymbol{A}\boldsymbol{B}$ 归

约为 p 次矩阵−向量乘法，本文将密文计算使用明文−密文计算来代替，计算开销如表 1 所示。

1.3 Jiang 等的密文矩阵乘法算法

设待相乘的矩阵是 2 个方阵 $\boldsymbol{A}\in\mathcal{R}^{n\times n}$ 和 $\boldsymbol{B}\in\mathcal{R}^{n\times n}$，在 Jiang 等[25]给出的同态密文乘法算法中，其核心思想就是将 $\boldsymbol{X}=\boldsymbol{AB}$ 的计算式重写为

$$\boldsymbol{X}=\sum_{i=0}^{n-1}\boldsymbol{A}_i\odot\boldsymbol{B}_i$$

其中，$\boldsymbol{A}_0\in\mathcal{R}^{n\times n}$ 的第 j 列就是矩阵 $\boldsymbol{A}$ 的第 j 个对角向量 $\boldsymbol{d}_j(\boldsymbol{A})$，$0\leqslant j<n$；$\boldsymbol{B}_0\in\mathcal{R}^{n\times n}$ 的第 j 行就是矩阵 $\boldsymbol{B}^{\mathrm{T}}$ 的第 j 个对角向量 $\boldsymbol{d}_j(\boldsymbol{B}^{\mathrm{T}})$，$0\leqslant j<n$；$\boldsymbol{A}_i\in\mathcal{R}^{n\times n}$ 是将 $\boldsymbol{A}_0$ 的列向左旋转 i 列得到的矩阵，记作 $\boldsymbol{A}_i=\mathrm{ColRot}(\boldsymbol{A}_0,i)$，$1\leqslant i<n$；$\boldsymbol{B}_i\in\mathcal{R}^{n\times n}$ 是将 $\boldsymbol{B}_0$ 的行向上旋转 i 行得到的矩阵，记作 $\boldsymbol{B}_i=\mathrm{RowRot}(\boldsymbol{B}_0,i)$，$1\leqslant i<n$。

另外，Jiang 等给出的同态密文乘法算法将一个 $n\times n$ 的矩阵都按行依次排列，编码成一个 n^2 维的向量。将矩阵 $\boldsymbol{A}$、$\boldsymbol{B}$ 和 $\boldsymbol{X}$ 照此编码后得到的向量分别记为 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{x}\in\mathcal{R}^{n^2}$，得到算法 2。

算法 2 Jiang 等的密文矩阵乘法

初始化明文向量 $\boldsymbol{a}$，对应矩阵 $\boldsymbol{A}\in\mathcal{R}^{n\times n}$ 的明文；初始化密文向量 $\boldsymbol{c}_b$，对应矩阵 $\boldsymbol{B}\in\mathcal{R}^{n\times n}$ 的明文向量 $\boldsymbol{b}$。

1) 从 $\boldsymbol{c}_b$ 构造 $\boldsymbol{c}_{b_0}$，对应向量 $\boldsymbol{b}_0$ 和矩阵 $\boldsymbol{B}_0$；
2) 从 $\boldsymbol{a}$ 构造 $\boldsymbol{a}_0$，对应矩阵 $\boldsymbol{A}_0$；
3) 计算 $\boldsymbol{c}_x\leftarrow\mathrm{CMult}(\boldsymbol{a}_0,\boldsymbol{c}_{b_0})$
4) for $1\leqslant i<n$
5) 计算 $\boldsymbol{a}_i\leftarrow\mathrm{ColRot}(\boldsymbol{a}_0,i)$；
6) 计算 $\boldsymbol{c}_{b_i}\leftarrow\mathrm{RowRot}(\boldsymbol{c}_{b_0},i)$；
7) 更新 $\boldsymbol{c}_x\leftarrow\mathrm{Add}(\boldsymbol{c}_x,\mathrm{CMult}(a_i,\boldsymbol{c}_{b_i}))$；
8) end for
9) 返回 $\boldsymbol{c}_x$。

考虑明文−密文的情况，只统计 $\boldsymbol{B}$ 的密文操作，根据文献[25]，算法 2 共需要 d 次明文−密文乘法和 $d+2\sqrt{d}$ 次密文旋转，其中 $d=\max\{n,m,p\}$ 表示按照其中最大的维数进行矩阵到方阵的变换，计算开销如表 1 所示。

2 明文−密文矩阵乘法方案

本节提出了一种新的密文矩阵乘法，适用于任意的 $\boldsymbol{A}=(a_{i,j})\in\mathcal{R}^{n\times m}$ 和 $\boldsymbol{B}=(b_{i,j})\in\mathcal{R}^{m\times p}$ 的矩阵乘法 $\boldsymbol{X}=\boldsymbol{AB}\in\mathcal{R}^{n\times p}$。该方法解除了矩阵 $\boldsymbol{B}$ 对方阵的限制，但是需要满足 $\boldsymbol{A}$ 为方阵。本文考虑模型拥有方和计算方相同的情形，提出了明文−密文矩阵乘法。该方案相较于其他方案在明文−密文矩阵乘法时具有较好的优越性，特别是当 $p>m\geqslant n$ 时，该方案只需进行算法 4，且计算开销与 p 无关，因而该方案的效率最高。

2.1 矩阵编码

设 $\boldsymbol{A}\in\mathcal{R}^{m\times m}$ 和 $\boldsymbol{B}\in\mathcal{R}^{m\times p}$ 是 2 个待相乘的矩阵。定义如下元素提取方式

$$U_k^{m\times m}(a_{0,j})=\begin{cases}a_{k,j+k}, & 0\leqslant j+k<m\\ 0, & \text{其他}\end{cases}\tag{5}$$

这里需要注意的是，式(5)的目的是从 $a_{0,j}$ 起，取对角线的元素，当下标超过矩阵维数时，取值为 0，最终结果是一个 k 维向量。

同样定义另一种元素提取方式为

$$V_k^{m\times m}(a_{i,0})=\begin{cases}a_{k,k-i}, & 0\leqslant k-i<m\\ 0, & \text{其他}\end{cases}\tag{6}$$

需要注意的是，同式(5)类似，式(6)最终得到的也是一个 k 维向量。接下来，引入一种编码方式，将矩阵 $\boldsymbol{A}\in\mathcal{R}^{m\times m}$ 编码成 $(2m-1)\times(mp)$ 的矩阵，记为 $\underline{\boldsymbol{A}}$。

算法 3 矩阵编码算法

输入明文矩阵 $\boldsymbol{A}=(a_{i,j})\in\mathcal{R}^{m\times m}$；初始化全 0 明文编码矩阵 $\underline{\boldsymbol{A}}\in\mathcal{R}^{2m\times m}$，向量 $\underline{\boldsymbol{a}}_i$ 表示编码矩阵 $\underline{\boldsymbol{A}}$ 的第 i 行。

1) for $0\leqslant i<2m-1$
2) if $i\leqslant m$
3) 计算 $\underline{\boldsymbol{a}}_i\leftarrow\mathrm{repeat}(p,V_m(a_{m-i,0}))$；
4) else
5) 计算 $\underline{\boldsymbol{a}}_i\leftarrow\mathrm{repeat}(p,U_m(a_{0,i-m}))$；
6) end if
7) end for
8) 返回 $\underline{\boldsymbol{A}}$。

当执行完式(5)和式(6)操作时，得到一个 m 维的向量，repeat 函数将该向量重复 p 次，所以在循环结束时 $\underline{\boldsymbol{a}}_i\in\mathcal{R}^{mp}$，最终编码矩阵 $\underline{\boldsymbol{A}}\in\mathcal{R}^{(2m-1)\times(mp)}$。

对于矩阵 $\boldsymbol{B}\in\mathcal{R}^{m\times p}$，根据式(6)定义矩阵变换 $\tau:\mathcal{R}^{m\times p}\rightarrow\mathcal{R}^{m\cdot p}$，将矩阵转换成向量

$$\tau(\boldsymbol{B})=(\varphi^m(b_{0,0}),\varphi^m(b_{0,1}),\cdots,\varphi^m(b_{0,p-1}))\tag{7}$$

通过上述变化，可以将一个矩阵变成一个向量，向量的长度是原来矩阵行列数的乘积。接下来将描述如何通过 $\underline{\boldsymbol{A}}$ 和 $\tau(\boldsymbol{B})$ 进行矩阵乘法计算。

2.2　明文−密文矩阵乘法

现将上述编码结果在密文上进行计算，实现矩阵乘法计算。

算法 4　明文−密文矩阵乘法

矩阵 $\boldsymbol{A}=(a_{i,j})\in\mathcal{R}^{m\times m}$；矩阵 $\boldsymbol{B}=(b_{i,j})\in\mathcal{R}^{m\times p}$；初始化 k 和 l，其中 $kl=2m-1$ 且尽可能相等；初始化密文向量 $\boldsymbol{v}_{\text{cip}}$，长度为 k；初始化密文 $\boldsymbol{c}_x$ 和 $\boldsymbol{c}_{\text{tmp}}$；初始化公钥 pk。

1) 使用算法 3 通过 $\boldsymbol{A}$ 得到 $\underline{\boldsymbol{A}}$；
2) 计算 $\boldsymbol{b}\leftarrow\tau(\boldsymbol{B})$；
3) 加密 $\boldsymbol{c}_B=\text{Enc}_{\text{pk}}(\boldsymbol{b})$；
4) for $0\leqslant j<k$
5) $\quad\boldsymbol{v}_{\text{cip}}[j]\leftarrow\text{Rot}(\boldsymbol{c}_{\boldsymbol{B}},j-m)$；
6) end for
7) for $0\leqslant i<l$
8) $\quad$for $0\leqslant j<k$
9) $\quad\quad$如果 $\underline{\boldsymbol{A}}_{ik+j}$ 元素全 0，跳过；
10) $\quad\quad$更新 $\underline{\boldsymbol{A}}_{ik+j}\leftarrow\rho(\underline{\boldsymbol{A}}_{ik+j},-ki)$；
11) $\quad\quad$更新 $\boldsymbol{c}'\leftarrow\text{CMult}(\underline{\boldsymbol{A}}_{ik+j},\boldsymbol{v}_{\text{cip}}[j])$；
12) $\quad$end for
13) $\quad$更新 $\boldsymbol{c}_x\leftarrow\text{Add}(\boldsymbol{c}_x,\text{Rot}(\boldsymbol{c}',ki))$；
14) end for
15) 返回 $\boldsymbol{c}_x$

首先对 $\tau(\boldsymbol{B})$ 向量进行加密记为 $\boldsymbol{c}_{\boldsymbol{B}}=\text{Enc}_{\text{pk}}(\tau(\boldsymbol{B}))$，然后计算 $\underline{\boldsymbol{A}}_i$ 与 $\text{Rot}(\boldsymbol{c}_{\boldsymbol{B}};i-m)$ 明文−密文乘积结果；按照一般方式，需要进行 $2m-1$ 次密文乘法和 Rot 操作。注意到，式(4)适用于任意连续变化的密文。因此将式(4)应用到算法 4 中，可以将密文旋转操作从原来的 $2m-1$ 次降低到 $2\sqrt{2m-1}\leqslant3\sqrt{m}$ 次。

根据算法 4，计算得到明文−密文矩阵乘法的结果。如果将 $\boldsymbol{A}\in\mathcal{R}^{m\times m}$ 和 $\boldsymbol{B}\in\mathcal{R}^{m\times p}$ 矩阵乘法结果表示为 $\boldsymbol{X}\in\mathcal{R}^{m\times p}$，那么计算结果其实是 $\text{Enc}_{\text{pk}}(\tau(\boldsymbol{X}))$。可以观察到，矩阵 $\boldsymbol{B}$ 和矩阵 $\boldsymbol{X}$ 有类似的性质，因此可以直接将计算结果作为算法 4 的输入，实现多次乘法计算。

2.3　正确性验证

对算法 4 过程用公式描述为

$$\boldsymbol{X}=\text{Add}(\text{CMult}(\underline{\boldsymbol{A}}_i,\text{Rot}(c_{\boldsymbol{B}};i-m)))_{0\leqslant i\leqslant2m-1}\tag{8}$$

将密文操作对应到明文，可以得到如下结果

$$\boldsymbol{X}=\sum_{i=0}^{2m-1}\underline{\boldsymbol{A}}_i\odot\rho(\tau(\boldsymbol{B});i-m)\tag{9}$$

根据旋转的方向将式(9)分成两部分，用 $\boldsymbol{X}^{(1)}$ 和 $\boldsymbol{X}^{(2)}$ 表示，即 $\boldsymbol{X}=\boldsymbol{X}^{(1)}+\boldsymbol{X}^{(2)}$，其中 $\boldsymbol{X}^{(1)}$ 和 $\boldsymbol{X}^{(2)}$ 分别为

$$\boldsymbol{X}^{(1)}=\sum_{i=0}^{m}\underline{\boldsymbol{A}}_i\odot\rho(\tau(\boldsymbol{B});i-m)\tag{10}$$

$$\boldsymbol{X}^{(2)}=\sum_{i=m}^{2m-1}\underline{\boldsymbol{A}}_i\odot\rho(\tau(\boldsymbol{B});i-m)\tag{11}$$

因此，分别对 $\boldsymbol{X}^{(1)}$ 和 $\boldsymbol{X}^{(2)}$ 的计算结果进行验证，验证计算的正确性。

首先，对式(10)中矩阵 $\boldsymbol{A}$ 的编码进行分析，得到如下结果

$$\underline{\boldsymbol{A}}_i=(\underbrace{V_m(a_{m-i,0}),\cdots,V_m(a_{m-i,0})}_{p})=$$
$$(\underbrace{0,\cdots,0,a_{m-i,0},\cdots,a_{m-1,i-1}}_{m},\cdots,\underbrace{0,\cdots,0,a_{m-i,0},\cdots,a_{m-1,i-1}}_{m})$$

对 $\tau(\boldsymbol{B})$ 进行移位的过程中有如下结果

$$\rho(\tau(\boldsymbol{B});i-m)=(\underbrace{b_{i,p-1},\cdots,b_{m-1,p-1},b_{0,0},\cdots,b_{i-1,0}}_{m},\cdots,$$
$$\underbrace{b_{i,p-2},\cdots,b_{m-1,p-2},b_{0,p-1},\cdots,b_{i-1,p-1}}_{m})$$

所以，可以将式(10)中第 i 条乘积重写成如下形式

$$\underline{\boldsymbol{A}}_i\odot\rho(\tau(\boldsymbol{B});i-m)=$$
$$(\underbrace{0,\cdots,0,a_{m-i,0}b_{0,0},\cdots,a_{m-1,i-1}b_{i-1,0}}_{m},\cdots,$$
$$\underbrace{0,\cdots,0,a_{m-i,0}b_{0,p-1},\cdots,a_{m-1,i-1}b_{i-1,p-1}}_{m})$$

得到 $\boldsymbol{X}^{(1)}$ 的结果如下所示

$$\boldsymbol{X}^{(1)}=(\underbrace{0,\sum_{i=0}^{0}a_{1,i}b_{i,0},\cdots,\sum_{i=0}^{m-2}a_{m-1,i}b_{i,0}}_{m},\cdots,$$
$$\underbrace{0,\sum_{i=0}^{0}a_{1,i}b_{i,p-1},\cdots,\sum_{i=0}^{m-2}a_{m-1,i}b_{i,p-1}}_{m})$$

通过上述分析，最终计算得到 $\boldsymbol{X}^{(1)}$ 的结果。

同理，在式(11)中有 $m\leqslant i<2m-1$，对矩阵 $\boldsymbol{A}$ 的编码进行分析，得到如下结果

$$\underline{\boldsymbol{A}}_i=(\underbrace{U_m(a_{0,i-m}),\cdots,U_m(a_{0,i-m})}_{p})=$$
$$(\underbrace{a_{0,i-m},\cdots,a_{2m-1-i,m-1},0,\cdots,0}_{m},\cdots,$$
$$\underbrace{a_{0,i-m},\cdots,a_{2m-1-i,m-1},0,\cdots,0)}_{m}$$

对 $\tau(B)$ 进行移位的过程中有如下结果

$$\rho(\tau(\boldsymbol{B});i-m)=(\underbrace{b_{i-m,0},\cdots,b_{m-1,0},b_{0,1},\cdots,b_{i-m-1,1}}_{m},\cdots,$$
$$\underbrace{b_{i-m,p-1},\cdots,b_{m-1,p-1},b_{0,0},\cdots,b_{i-m-1,0}}_{m})$$

所以，可以将式(11)中第 i 条乘积重写成如下形式

$$\underline{\boldsymbol{A}}_i\odot(\rho(\tau(\boldsymbol{B});i-m)=$$
$$(\underbrace{a_{0,i-m}b_{i-m,0},\cdots,a_{2m-1-i,m-1}b_{m-1,0},0,\cdots,0}_{m},\cdots,$$
$$\underbrace{a_{0,i-m}b_{i-m,p-1},\cdots,a_{2m-1-i,m-1}b_{m-1,0},0,\cdots,0)}_{m}$$

所以，式(11)的结果为以下形式

$$\boldsymbol{X}^{(2)}=(\underbrace{\sum_{i=0}^{m-1}a_{0,i}b_{i,0},\sum_{i=1}^{m-1}a_{1,i}b_{i,0},\cdots,\sum_{i=m-1}^{m-1}a_{m-1,i}b_{i,0}}_{m},\cdots,$$
$$\underbrace{\sum_{i=0}^{m-1}a_{0,i}b_{i,p-1},\sum_{i=1}^{m-1}a_{1,i}b_{i,p-1},\cdots,\sum_{i=m-1}^{m-1}a_{m-1,i}b_{i,p-1}}_{m})$$

经过上述过程，最终计算得到 $\boldsymbol{X}^{(2)}$ 的结果。

将 $\boldsymbol{X}^{(1)}$ 和 $\boldsymbol{X}^{(2)}$ 的结果进行相加，可以得到 $\boldsymbol{X}$ 的表达式为

$$\boldsymbol{X}=\boldsymbol{X}^{(1)}+\boldsymbol{X}^{(2)}=$$
$$(\underbrace{\sum_{i=0}^{m-1}a_{0,i}b_{i,0},\sum_{i=0}^{m-1}a_{1,i}b_{i,0},\cdots,\sum_{i=0}^{m-1}a_{m-1,i}b_{i,0}}_{m},\cdots,$$
$$\underbrace{\sum_{i=0}^{m-1}a_{0,i}b_{i,p-1},\sum_{i=0}^{m-1}a_{1,i}b_{i,p-1},\cdots,\sum_{i=0}^{m-1}a_{m-1,i}b_{i,p-1}}_{m})\tag{12}$$

通过上述推导过程可以得到 $\boldsymbol{X}$ 的结果。通过观察发现，式(12)中每一项都是内积，实际上就是矩阵一般乘法，从而证明计算的正确性。

2.4 性能分析

算法 3 实现了对密文矩阵的乘法。通过将算法 3 用式(9)进行表示可以发现，用原始方法进行明文矩阵计算需要分别进行 $2m-1$ 次密文加法、明文–密文乘法以及密文旋转操作。在优化之后，能将密文旋转操作减少至 $3\sqrt{m}$ 次。同时可以观察到，密文计算的次数与 p 无关，只与 m 的大小相关，因此当 p 远大于 m 时，在不改变计算效率的情况下，能同时处理更大数据量。

需要注意的是，这种方法需要限制矩阵 $\boldsymbol{A}$ 为方阵，但是对于矩阵为以下情况时 $\boldsymbol{A}=(a_{i,j})\in\mathcal{R}^{n\times m}$，$n>m$，如果转换矩阵，则需要将 $\boldsymbol{A}$ 变成 $n\times n$ 的矩阵，相应地需要将矩阵 $\boldsymbol{B}\in\mathcal{R}^{m\times p}$ 变换为 $\boldsymbol{B}\in\mathcal{R}^{n\times p}$，才能进行矩阵乘法。一种解决办法是对矩阵 $\boldsymbol{A}$ 以 m 进行切割，再分别进行矩阵乘法。但同时也提供了一种算法，即可以在密文上进行维数变换，以满足待相乘的 2 个矩阵的维数匹配要求。

3 维数变换算法

本节为了解决转换矩阵的维数变化问题，提出了一种算法，即在密文上能够转换维数，将矩阵在密文上进行 $\mathcal{R}^{m\times p}\to\mathcal{R}^{n\times p}$ 变换。维数变换的提出使得方案能支持任意维数矩阵连乘。

首先对式(4)进行改写，注意到，如果同时乘以一个倍数，那么等式仍然成立。

$$\boldsymbol{u}=\sum_{i=0}^{\frac{l}{r}}\sum_{j=0}^{k-1}(\rho(\boldsymbol{v};r[ki+j])\odot\boldsymbol{d}_{r[ki]+j})=$$
$$\sum_{i=0}^{\frac{l}{r}}\rho\left(\sum_{j=0}^{k-1}\left(\rho(\boldsymbol{v};r[j])\odot\rho(\boldsymbol{d}_{ki+j};-r[ki])\right);r[ki]\right)\tag{13}$$

可以看到，式(13)减少了外层的操作次数，这种方式适用于有规律的稀疏矩阵，能有效减少操作次数。

因此，可以将维数变换看成矩阵和向量的乘法。根据式(3)或式(13)，将明文向量对应到密文向量，ρ 对应密文旋转 Rot 操作，$\odot$ 对应明文–密文乘法 CMult 操作，在密文上实现维数变换。维数变换算法如算法 5 所示。

算法 5 维数变换算法

输入密文 $\boldsymbol{c}_b$ 对应明文 v 的密文，以及新的行数 n_1，旧的行数 n_2；初始化 k 和 l，其中 $kl=p$ 且尽可能相等，$r=n_1-n_2$；初始化密文 $\boldsymbol{c}'=\mathrm{Enc}_{\mathrm{pk}}(\boldsymbol{0})$。

1) for $0\leqslant i<p$
2) 生成向量 $\mathbf{diag}_{i(n_1-n_2)}=[]$，其中从 $n_2 i$ 到 $n_2(i+1)$ 位置为 1，其余为 0，对应 $\rho(\boldsymbol{d}_{ki+j};-r[ki])$；
3) end for
4) 根据式(13)中 $\boldsymbol{u}$ 在密文下计算 $\boldsymbol{c}'$；
5) 根据式(3)中 $\boldsymbol{u}$ 在密文下更新 $\boldsymbol{c}'$；
6) 返回 $\boldsymbol{c}'$。

算法 5 将原本需要 p 次的密文旋转减少到只需要 $2\sqrt{p}$ 次密文旋转，提高了运算效率。当然算法 5 不仅能够扩张矩阵的行数，也能够降低矩阵的行数。计算开销比较如表 2 所示。注意到，通过算法 5 进行转换之后，单独考虑算法 4 需要进行 $2m-1$ 次密文加法、$2m-1$ 次明文−密文乘法和 $3\sqrt{m}$ 次密文旋转。但是在扩张维数时，矩阵 $\boldsymbol{A}$ 通过填 0 进行升维，变换维数后的矩阵会十分稀疏，由于这种稀疏性在对矩阵 $\boldsymbol{A}$ 编码时产生 $n-m$ 个全 0 向量，而这些向量在算法 4 中不需要进行计算，因此，当算法 4 和算法 5 一起使用时，算法 4 的密文旋转次数会降低到 $2(\sqrt{p}+\sqrt{m+n-1})$ 次。此外，并不是每次计算都需要进行维数变换，只需要在 $m>n$ 时进行维数变换即可。

4　实验及实施

本节将详细描述同态矩阵运算的性能，并将其应用到贝叶斯分类器上进行分析和比较。本节基于 Microsoft SEAL 版本 4.1.0 中的 CKKS 方案实现相关功能。所有的实验都在具有 2.8 GHz 额定的 4 个内核运行的英特处理器 i7 笔记本计算机上运行。

4.1　参数设置

在进行实验时，首先设置 CKKS 方案参数，其中分圆多项式模数设置为 8 192，多项式系数模链设置为 $\{60,40,40,60\}$，此时多项式模数 $q=200$ bit，（在给定误差标准差 $\sigma=3.19$ 的情况下，参照格估计器（Lattice Estimator）[51]中给出的攻击方式，最低可以达到 137 bit 的安全性。

4.2　矩阵运算效率

表 3 中设置了 4 种规模的矩阵进行明文−密文矩阵乘法，分别统计每种规模下加密时间、解密时间、算法 4 和算法 5 的时间以及总时间，所有结果是对 10 次运算取平均值。

对实验结果进行如下分析。

1) 通过比较表 3 中 1、2 行结果可以发现，随着 p 增加，总时间基本相差无几，可以说明算法 4 的运行效率和 p 的大小无关。

2) 通过比较表 3 中 1、3 行结果可以发现，在 $\mathcal{R}^{16\times16}\times\mathcal{R}^{16\times128}$ 中算法 4 的时间大于 $\mathcal{R}^{16\times4}\times\mathcal{R}^{4\times128}$ 中算法 4 的时间，这是因为进行维数变换后的矩阵需要通过添加 0 元素来改变矩阵大小，对矩阵 $\boldsymbol{A}$ 进行编码时会出现许多全 0 行，而这些编码不需要进行计算，因此实际上的运算时间会减少。

3) 通过比较表 3 中 3 行和第 4 行的结果可以发现，$\mathcal{R}^{16\times4}\times\mathcal{R}^{4\times256}$ 相比于 $\mathcal{R}^{16\times4}\times\mathcal{R}^{4\times128}$ 在算法 5 上的时间差距明显，而其他运算的时间几乎相等。这说明算法 5 的运行效率和 p 的大小有关，p 越大进行维数变换所需的时间越长。

表 4 中设置了 3 组规模下的方阵进行明文−密文矩阵乘法的时间结果。在实验中，Halevi 等[42]将密文矩阵的每一列加密成一条密文；Jiang 等[25]的方案是根据文献[25]中算法 2 实现的明文−密文矩阵乘法。在这种规模下，所提方案实现计算只需要进行算法 4。通过比较可以发现，所提方案在时间上优于 Jiang 等[25]的方案，详细结果如表 4 所示。

表 2　　**计算开销比较**

算法	密文加法	明文−密文乘法	密文旋转	密文条数	密文深度
算法 4	$2m-1$	$2m-1$	$3\sqrt{m}$	1	1CMult
算法 5	p	p	$2\sqrt{p}$	1	1CMult
算法 4+算法 5	$p+m+n-1$	$p+m+n-1$	$2(\sqrt{p}+\sqrt{m+n-1})$	1	2CMult

表 3　　**4 种规模的矩阵的运算时间**

矩阵规模	加密时间/ms	解密时间/ms	算法 4 的时间/ms	算法 5 的时间/ms	总时间/ms
$\mathcal{R}^{16\times16}\times\mathcal{R}^{16\times128}$	3.08	0.51	62.16	—	65.75
$\mathcal{R}^{16\times16}\times\mathcal{R}^{16\times256}$	2.81	0.52	48.10	—	51.43
$\mathcal{R}^{16\times4}\times\mathcal{R}^{4\times128}$	2.51	0.22	24.92	148.04	175.69
$\mathcal{R}^{16\times4}\times\mathcal{R}^{4\times256}$	3.07	0.22	21.38	257.42	282.09

表 4 矩阵运算效率

矩阵规模	方案	加解密时间/ms	矩阵乘法时间/ms	密文个数/个	总时间/ms
$\mathcal{R}^{16\times16}\times\mathcal{R}^{16\times16}$	Halevi 等[42]	50.82	343.80	16	394.62
	Jiang 等[25]	3.20	64.24	1	67.44
	算法 4	3.35	66.83	1	70.18
$\mathcal{R}^{32\times32}\times\mathcal{R}^{32\times32}$	Halevi 等[42]	112.40	1393.50	32	1 505.9
	Jiang 等[25]	3.48	143.85	1	147.33
	算法 4	4.02	112.74	1	116.76
$\mathcal{R}^{64\times64}\times\mathcal{R}^{64\times64}$	Halevi 等[42]	225.85	4747.44	64	4 973.29
	Jiang 等[25]	3.48	234.70	1	238.18
	算法 4	3.46	168.28	1	171.74

5 应用

本节首先对贝叶斯分类器进行改进，使其适于进行密文计算；然后将算法 4 应用到明文–密文矩阵乘法上；最后将结果和文献[17]进行对比，取得更优的结果。

5.1 贝叶斯分类器

朴素贝叶斯分类器是一种基于贝叶斯定理和特征独立假设的简单、快速、高效的分类算法。它的基本思想是首先计算每个特征在不同类别下的概率，然后通过预测数据特征的概率去比较所有类别的可能性，最后取概率最大的类别为预测结果。对于 $1,2,\cdots,s$ 共 s 个分类和 $X_1,X_2,\cdots,X_n$ 共 n 个特征，每个特征包含 $1,2,\cdots,t$ 种取值的贝叶斯模型。假设对 $\boldsymbol{x}=(x_1,\cdots,x_n)$ 进行分类预测，表示为

$$\hat{y}=\arg\max_{i=1,\cdots,s}\Pr[Y=i]\prod_{k=1}^{n}\Pr[X_k=x_k\mid Y=i]$$

其中，$\Pr[Y=i]$ 为先验概率，表示 $Y=i$ 类别的概率；$\Pr[X_k=x_k\mid Y=i]$ 为条件概率，表示在 $Y=i$ 的条件下 X_k 取 $x_k\in(x_1,\cdots,x_n)$ 的概率。预测过程实际上可理解为计算后验概率，也就是计算当 $X_k=x_k$ 时，$Y=i$ 类别的概率，最后通过比较得到概率最大的类别，即预测结果。

5.2 隐私保护朴素贝叶斯

为了在密文上应用矩阵运算时减少比较操作带来的计算开销，需要对贝叶斯模型进行改进，即对所有特征取值，取特征值对应的序号为 1，其余全部为 0。通过这种编码，将每条预测数据扩展成 kt 长度的预测数据。

$$X_i=\begin{cases}1, X_i=x_i\\ 0, X_i\neq x_i\end{cases}$$

为了减少同态比较带来的计算开销，考虑如图 1 所示的隐私保护贝叶斯分类器框架，对 m 条数据进行预测，在服务器端只需对 $s\times nk$ 和 $nk\times m$ 大小的矩阵进行同态密文矩阵乘法，对每个样本添加随机选取的相同噪声之后，将密文结果传输给客户端解密，经过比较得到最终的预测结果。

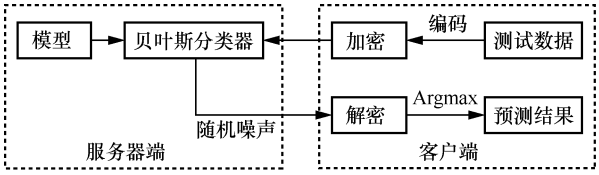


图 1 隐私保护贝叶斯分类器框架

5.2.1 安全性

对于客户端来说，客户端将预测数据进行编码，然后通过 CKKS 方案进行加密，传输给服务器端。从服务器端来看，它没有私钥，不能对密文数据进行解密运算，因此只能看见加密后的预测数据，从而保证了客户端的安全性。

对于服务器端来说，服务器端在计算出后验概率之后，在模型结果每个样本中引入一个相同的噪声。从客户端来看，依然能够正确比较后验概率的大小，保证预测结果的正确性，同时由于噪声是随机选取的，客户端不能根据预测结果去推测模型中的相关参数，从而保证了服务器端的安全性。

5.2.2 性能评估

本文使用 UCI 机器学习库中的 Iris 数据集和 WBC（Wisconsin Breast Cancer）数据集进行实验，使用文献[17]中的模型进行运算，2 种模型的实验精度在 97%左右，这和明文上运算的精度没有区别。

实验过程中，参数设置参照 5.1 节中的参数设置，实现至少 137 bit 的安全性。

在 Iris 数据集中，总共有 150 个样本，被分为 3 类，其中每个样本含有 4 个特征。将样本中连续的特征类型变成离散型数据，通过将每种特征值最大最小值的区间平均分成 5 段，可以得到 5 个不同的取值。使用其中 80%（120 个）的数据进行模型训练，使用 20%（30 个）的数据进行模型预测。所以，密文计算实际上是 2 个 3×20 和 20×30 的矩阵相乘。本节将所提方案与 Jiang 等[25]方案以及文献[17]方案进行比较，需要注意的是，首先，Jiang 等[25]的方案在计算时，需要按照最大维数将 2 个矩阵变换成方阵，即 30×30 与 30×30 的矩阵乘法，因此会增加密文计算的时间；其次，文献[17]方案中取最大值的操作是在密文上进行的，所以在统计结果中应忽略掉这部分时间。详细结果如表 5 所示。

在 WBC 数据集中，总共有 683 个样本，被分为 2 类，其中每个样本含有 9 个特征，每个特征有 10 个不同的取值。使用其中 70%（487 个）的数据进行模型训练，使用 30%（205 个）的数据进行预测。对本文数据来说，实际上是 2 个 2×90 和 90×205 的矩阵相乘，在这种维度下，单条密文无法装下所有数据，因此需要分组进行计算。将 205个数据拆成9组22个和一组7个 共10组预测分别进行计算。本节也将所提方案与 Jiang 等[25]方案以及文献[17]方案进行比较，在统计文献[17]方案的结果时也忽略密文上取最大值的操作。需要注意的是，在 WBC 数据集中，使用 Jiang 等[25]方案涉及的分块方式和所提方案不同，需要按照方阵进行切分。详细结果如表 6 所示。

对比实验结果表明，使用所提方案更具有优势，每个样本最低只需要 2.14 ms 就能进行预测，同时方案的传输开销也更小。总体而言，所提方案在时间和空间上更具有优势。

表 5　　Iris 数据集实验结果

方案	加解密时间/ms	密文计算时间/ms	总时间/ms	样本平均时间/ms	密文大小/KB
算法 4	3.57	60.75	64.32	2.14	385
Jiang 等[25]	3.08	177.42	180.50	6.02	385
文献[17]	580	1272	1852	61.7	40 980

表 6　　WBC 数据集实验结果

方案	加解密时间/ms	密文计算时间/ms	总时间/ms	样本平均时间/ms	密文大小/KB
算法 4	32.93	1 300.23	1 333.16	6.50	3856
Jiang 等[25]	25.62	1 786.45	1 812.07	8.84	3085
文献[17]	2 773	2 680	5 453	26.6	180 875

6　结束语

本文首先提出了明文−密文矩阵乘法方案，然后通过维数变换算法将明文方阵扩展到任意维数的明文矩阵。相对于先前的技术，所提方案降低了密文旋转的复杂度，提高了运算效率。当矩阵维数 $p>m\geqslant n$ 时，完成矩阵乘法计算只需算法 4 且算法 4 的开销和 p 无关，因而明文−密文矩阵乘法的表现更出色。最后将明文−密文矩阵乘法方案应用到贝叶斯分类器中，取得了更好的实验结果。

明文−密文矩阵乘法方案也能支持密文−密文矩阵乘法，但密文矩阵乘法与之前方案相比，通信开销（密文数量）更大，因此本文不考虑密文−密文的情况。其次，尽管能实现任意维数的矩阵乘法，但是方案的本质是明文方阵−密文矩阵乘法，这可能会限制方案广泛的应用。最后，面对更大规模的矩阵，需要对矩阵分块进行计算。所以在接下来的工作中，首先需要进一步改进所提方案，使该方案能解除对方阵的限制，并能够胜任更复杂的密文−密文矩阵乘法。其次对矩阵分块进行分析，针对所提方案提出相应的分块方案，并将其应用到更多的机器学习模型中去。

参考文献：

[1] LIN G B, LI H, ZHANG Y Y, et al. Dynamic momentum for deep learning with differential privacy[C]//International Conference on Machine Learning for Cyber Security. Berlin: Springer, 2023: 180-190.

[2] DWORK C, KENTHAPADI K, MCSHERRY F, et al. Our data, ourselves: privacy via distributed noise generation[C]//Proceedings of the

24th Annual International Conference on The Theory and Applications of Cryptographic Techniques. New York: ACM Press, 2006: 486-503.

[3] DWORK C, ROTH A. The algorithmic foundations of differential privacy[J]. Foundations and Trends® in Theoretical Computer Science, 2013, 9(3/4): 211-407.

[4] DWORK C. Differential privacy: a survey of results[C]//International Conference on Theory and Applications of Models of Computation. Berlin: Springer, 2008: 1-19.

[5] DU W L, ATALLAH M J. Secure multi-party computation problems and their applications: a review and open problems[C]//Proceedings of the Workshop on New Security Paradigms. New York: ACM Press, 2001: 13-22.

[6] YAO A C C. How to generate and exchange secrets[C]//Proceedings of the 27th Annual Symposium on Foundations of Computer Science (SFCS 1986). Piscataway: IEEE Press, 1986: 162-167.

[7] MOHASSEL P, ZHANG Y P. SecureML: a system for scalable privacy-preserving machine learning[C]//Proceedings of IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2017: 19-38.

[8] YANG Q, LIU Y, CHEN T J, et al. Federated machine learning: concept and applications[J]. arXiv Preprint, arXiv: 1902.04885, 2019.

[9] LI L, FAN Y X, TSE M, et al. A review of applications in federated learning[J]. Computers & Industrial Engineering, 2020, 149: 106854.

[10] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[J]. arXiv Preprint, arXiv: 1602.05629, 2016.

[11] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169-180.

[12] GIACOMELLI I, JHA S, JOYE M, et al. Privacy-preserving ridge regression with only linearly-homomorphic encryption[C]// International Conference on Applied Cryptography and Network Security. Berlin: Springer, 2018: 243-261.

[13] HALL R, FIENBERG S E, NARDI Y. Secure multiple linear regression based on homomorphic encryption[J]. Journal of Official Statistics, 2011, 27(4): 669-691.

[14] HAN K, JEONG J, SOHN J H, et al. Efficient privacy preserving logistic regression inference and training[J]. IACR Cryptology ePrint Archive, 2020, 2020: 1396.

[15] YU X P, ZHAO W, HUANG Y F, et al. Privacy-preserving outsourced logistic regression on encrypted data from homomorphic encryption[J]. Security and Communication Networks, 2022, 1396: 1321198.

[16] 吕由, 吴文渊. 两方参与的隐私保护岭回归方案与应用[J]. 密码学报, 2023, 10(2): 276-288.
LYU Y, WU W Y. Two-party privacy-preserving ridge regression scheme with applications[J]. Journal of Cryptologic Research, 2023, 10(2): 276-288.

[17] CHEN J W, FENG Y, LIU Y, et al. Non-interactive privacy-preserving Naïve Bayes classifier using homomorphic encryption[C]//International Conference on Security and Privacy in New Computing Environments. Berlin: Springer, 2022: 192-203.

[18] SUN X Q, ZHANG P, LIU J K, et al. Private machine learning classification based on fully homomorphic encryption[J]. IEEE Transactions on Emerging Topics in Computing, 2020, 8(2): 352-364.

[19] TANG W R, ZHOU Y H, LI M S, et al. Differential privacy preserving naive Bayes classification via wavelet transform[C]//Proceedings of International Conference on Networking and Network Applications (NaNA). Piscataway: IEEE Press, 2020: 81-85.

[20] WOOD A, SHPILRAIN V, NAJARIAN K, et al. Private naive Bayes classification of personal biomedical data: application in cancer data analysis[J]. Computers in Biology and Medicine, 2019, 105: 144-150.

[21] YASUMURA Y, ISHIMAKI Y, YAMANA H. Secure Naïve Bayes classification protocol over encrypted data using fully homomorphic encryption[C]//Proceedings of the 21st International Conference on Information Integration and Web-based Applications & Services. New York: ACM Press, 2019: 45-54.

[22] PANDA S. Principal component analysis using CKKS homomorphic scheme[C]//International Symposium on Cyber Security Cryptography and Machine Learning. Berlin: Springer, 2021: 52-70.

[23] MA X R. Improved privacy-preserving PCA using optimized homomorphic matrix multiplication[J]. arXiv Preprint, arXiv: 2305.17341, 2023.

[24] RATHEE D, MISHRA P K, YASUDA M. Faster PCA and linear regression through hypercubes in HElib[C]//Proceedings of the Workshop on Privacy in the Electronic Society. New York: ACM Press, 2018: 42-53.

[25] JIANG X Q, KIM M, LAUTER K, et al. Secure outsourced matrix computation and application to neural networks[C]//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 1209-1222.

[26] LEE J W, KANG H, LEE Y, et al. Privacy-preserving machine learning with fully homomorphic encryption for deep neural network[J]. IEEE Access, 2022, 10: 30039-30054.

[27] LEE E, LEE J W, LEE J, et al. Low-complexity deep convolutional neural networks on fully homomorphic encryption using multiplexed parallel convolutions[C]//Proceedings of the International Conference on Machine Learning. New York: PMLR, 2022: 1-20.

[28] MIHARA K, YAMAGUCHI R, MITSUISHI M, et al. Neural network training with homomorphic encryption[J]. arXiv Preprint, arXiv: 2012.13552, 2020.

[29] LOU Q, FENG B, FOX G C, et al. Glyph: fast and accurately training deep neural networks on encrypted data[J]. arXiv Preprint, arXiv: 1911.07101, 2019.

[30] PODSCHWADT R, TAKABI D. Non-interactive privacy preserving recurrent neural network prediction with homomorphic encryption[C]//Proceedings of IEEE 14th International Conference on Cloud Computing (CLOUD). Piscataway: IEEE Press, 2021: 65-70.

[31] GENTRY C. A fully homomorphic encryption scheme [D]. State of California: Stanford University, 2009.

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

[33] FAN J F, VERCAUTEREN F. Somewhat practical fully homomorphic encryption[J]. IACR Cryptology ePrint Archive, 2012, 144: 1-19.

[34] DUCAS L, MICCIANCIO D. FHEW: bootstrapping homomorphic encryption in less than a second[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2015: 617-640.

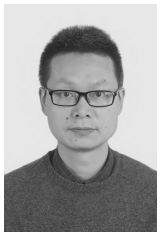
[35] CHILLOTTI I, GAMA N, GEORGIEVA M, et al. TFHE: fast fully homomorphic encryption over the torus[J]. Journal of Cryptology,

2020, 33(1): 34-91.
[36] 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. Berlin: Springer, 2017: 409-437.
[37] SMART N P, VERCAUTEREN F. Fully homomorphic SIMD operations[J]. Designs, Codes and Cryptography, 2014, 71(1): 57-81.
[38] LIU F H, WANG H. Batch bootstrapping II: bootstrapping in polynomial modulus only requires O~(1) the multiplications in amortization[C]//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2023: 353-384.
[39] KIM D, GUYOT C. Optimized privacy-preserving CNN inference with fully homomorphic encryption[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 2175-2187.
[40] HALEVI S, SHOUP V. Algorithms in HElib[C]//Proceedings of the Advances in Cryptology–CRYPTO 2014: 34th Annual Cryptology Conference. Berlin: Springer, 2014: 554-571.
[41] LEIGHTON F T. Introduction to parallel algorithms and architectures: arrays, trees, hypercubes[M]. San Francisco: Morgan Kaufmann Publishers Inc., 1991.
[42] HALEVI S, SHOUP V. Bootstrapping for HElib[J]. Journal of Cryptology, 2021, 34(1): 7.
[43] HUANG H, ZONG H R. Secure matrix multiplication based on fully homomorphic encryption[J]. The Journal of Supercomputing, 2023, 79(5): 5064-5085.
[44] HUANG Z C, HONG C, WENG C K, et al. More efficient secure matrix multiplication for unbalanced recommender systems[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(1): 551-562.
[45] JANG J, LEE Y, KIM A, et al. Privacy-preserving deep sequential model with matrix homomorphic encryption[C]//Proceedings of ACM on Asia Conference on Computer and Communications Security. New York: ACM Press, 2022: 377-391.
[46] BABENKO M, GOLIMBLEVSKAIA E, TCHERNYKH A, et al. A comparative study of secure outsourced matrix multiplication based on homomorphic encryption[J]. Big Data and Cognitive Computing, 2023, 7(2): 84.
[47] DUONG D H, MISHRA P K, YASUDA M. Efficient secure matrix multiplication over LWE-based homomorphic encryption[J]. Tatra Mountains Mathematical Publications, 2016, 67(1): 69-83.
[48] YASUDA M, SHIMOYAMA T, KOGURE J, et al. Secure statistical analysis using RLWE-based homomorphic encryption[C]//Australasian Conference on Information Security and Privacy. Berlin: Springer, 2015: 471-487.
[49] YASUDA M, SHIMOYAMA T, KOGURE J, et al. New packing method in somewhat homomorphic encryption and its applications[J]. Security and Communication Networks, 2015, 8(13): 2194-2213.
[50] MISHRA P K, DUONG D H, YASUDA M. Enhancement for secure multiple matrix multiplications over ring-LWE homomorphic encryption[C]//International Conference on Information Security Practice and Experience. Berlin: Springer, 2017: 320-330.
[51] ALBRECHT M R, PLAYER R, SCOTT S. On the concrete hardness of learning with errors[J]. Journal of Mathematical Cryptology, 2015, 9(3): 169-203.

[作者简介]

刘洋（1984− ），女，湖北咸宁人，博士，重庆交通大学副教授、硕士生导师，主要研究方向为形式化验证、网络信息安全等。

杨林翰（2000− ），男，重庆人，重庆交通大学硕士生，主要研究方向为信息安全、密文计算等。



陈经纬（1984− ），男，四川巴中人，博士，中国科学院重庆绿色智能技术研究院副研究员、硕士生导师，主要研究方向为信息安全、格算法及其应用等。

吴文渊（1976− ），男，四川成都人，博士，中国科学院重庆绿色智能技术研究院研究员、博士生导师，主要研究方向为符号数值计算、信息安全。

冯勇（1965− ），男，四川宁南人，博士，中国科学院重庆绿色智能技术研究院研究员、博士生导师，主要研究方向为符号数值计算、信息安全。