基于CKKS函数型Bootstrapping的融合式同态LayerNorm方案设计

陈智罡[1]，宋新霞[2]，Liqun Chen[3]
（1.宁波财经学院人工智能学院，浙江 宁波 315175；2.浙江万里学院大数据与软件工程学院，浙江 宁波 315100；
3.英国萨里大学计算机科学系，吉尔福德 萨里 GU27XH）

摘要：针对CKKS同态Transformer中LayerNorm倒数平方根运算深度高的问题，提出了函数型Bootstrapping融合方案。在EvalMod阶段，以倒数平方根复合多项式替换反正弦多项式，结合预缩放和统计边界约束输入，在校准边界内实现零额外乘法深度。此外，采用Remez算法构造31阶极小极大逼近。实验结果表明，相较Goldschmidt（k=3），所提方案节省6层乘法深度，LayerNorm加速1.26倍，峰值内存降低16.7%。在BERT-Base的SST-2数据集上，获得92.1%的同态分类准确率，较明文低0.4个百分点。所提方案在保持精度的同时降低了同态LayerNorm的计算深度和资源开销。

关键词：全同态加密；CKKS；层归一化；函数型Bootstrapping；Transformer；隐私保护推理
中图分类号：TP309
文献标志码：A
doi：10.11959/j.issn.1000–436x.TXXB260263

Design of a fused homomorphic LayerNorm scheme based on CKKS functional Bootstrapping

Chen Zhigang[1], Song Xinxia[2], Liqun Chen[3]
1. College of Artificial Intelligence, Ningbo University of Finance and Economics, Ningbo 315175, China
2. School of Big Data and Software Engineering, Zhejiang Wanli University, Ningbo 315100, China
3. Department of Computer Science, University of Surrey, Surrey GU27XH, UK

Abstract: To address the high multiplicative depth required for inverse square root computation in LayerNorm for CKKS-based homomorphic Transformer inference, a fused functional Bootstrapping scheme was proposed. In the EvalMod stage, the arcsine polynomial was replaced with a composite polynomial that directly computed the inverse square root. Pre-scaling and statistical bounds were used to constrain the input, enabling zero additional multiplicative depth within the calibrated bound. In addition, the Remez algorithm was employed to construct a degree-31 minimax approximation. Experimental results show that, compared with the Goldschmidt iteration (k=3), the proposed scheme saves six levels of multiplicative depth, accelerates LayerNorm computation by 1.26 times, and reduces peak memory usage by 16.7%. BERT-Base achieves a homomorphic classification accuracy of 92.1% on the SST-2 dataset, only 0.4 percentage points lower than plaintext inference. The proposed scheme reduces the computational depth and resource overhead of homomorphic LayerNorm while maintaining classification accuracy.

Key words: fully homomorphic encryption, CKKS, LayerNorm, functional Bootstrapping, Transformer, privacy-preserving inference

---

收稿日期：2026–05–11；**修回日期：**2026–07–10
通信作者：宋新霞，sxxx@zwu.edu.cn
基金项目：国家自然科学基金资助项目（No.62571283）；浙江省自然科学基金资助项目（No.LMS26F020025）；宁波市自然科学基金资助项目（No.2025J185）；宁波财经学院高级别科研培育基金资助项目（No.1320263702）
Foundation Items: The National Natural Science Foundation of China (No.62571283), Zhejiang Provincial Natural Science Foundation of China (No.LMS26F020025), Ningbo Natural Science Foundation of China (No.2025J185), High-Level Scientific Research Incubation Project of Ningbo University of Finance & Economics (No.1320263702)

0　引言

随着人工智能技术在医疗诊断、金融风控、自然语言处理等领域的深入渗透，用户数据的隐私保护问题日益突出。传统的机器学习服务模式要求用户将原始数据上传至云端服务器进行模型推理，这不可避免地引发隐私泄露风险。全同态加密（fully homomorphic encryption, FHE）[1]为这一问题提供了理想的密码学解决方案，它允许在加密数据上直接执行任意计算，计算结果解密后与在明文上计算的结果一致，从而在整个推理过程中不需要暴露原始数据。

在现有FHE方案中，CKKS[2]因其对实数近似算术的原生支持而成为隐私保护机器学习的首选方案。与处理精确整数的BGV[3]和BFV[4]方案，以及处理布尔电路的TFHE[5]方案不同，CKKS方案将实数向量编码为多项式环元素，通过缩放因子控制精度，满足深度学习中大量浮点运算的需求。然而，CKKS方案的乘法运算会消耗模数链中的层级，当层级耗尽时必须通过自举（Bootstrapping）操作刷新密文，而Bootstrapping本身会消耗大量计算资源和乘法深度。

近年来，Transformer架构[6]已成为自然语言处理和计算机视觉领域的主导模型。从BERT[7]到GPT系列[8]，Transformer的应用范围不断扩展。在Transformer的每个注意力层和前馈层中，层归一化（LayerNorm）[9]是不可或缺的核心组件，其数学定义为$\hat{x}_i = \dfrac{x_i - \mu}{\sqrt{\sigma^2 + \epsilon}}$，其中$\mu$和$\sigma^2$分别为隐藏层向量的均值和方差，$\epsilon$为稳定性常数。其简化变体RMSNorm[10]省去均值计算但保留倒数平方根作为核心运算，近年来被LLaMA[11]等大语言模型（large language model, LLM）广泛采用。

在CKKS环境下，LayerNorm的大部分计算（如均值、残差、平方求和）均可通过低深度的同态加法、乘法和旋转操作高效实现。然而，其核心的倒数平方根运算却构成了严重的计算瓶颈。由于CKKS的乘法深度资源由Bootstrapping[12-13]刷新后的剩余层级决定，每一层乘法深度都弥足珍贵。目前计算倒数平方根的主流方法是采用Goldschmidt迭代[14]：每次迭代消耗两层乘法深度，达到足够精度通常需要$k \geqslant 3$次迭代，总计消耗6~8层乘法深度。这一开销在Bootstrapping后有限的深度预算中占比极高。对于12层的BERT-Base模型，仅LayerNorm中的倒数平方根计算就累计消耗数十层乘法深度，严重制约了推理效率。

近期，RBOOT[15]提出了一种函数型Bootstrapping方法，其核心思想是将非线性函数（如ReLU）的计算融入CKKS Bootstrapping的模约减（EvalMool）阶段。通过将恢复线性值的$P_{\arcsin}$多项式替换为直接计算目标函数的复合多项式，RBOOT实现了在Bootstrapping过程中“免费”获得ReLU的计算结果，避免了传统多项式近似[16]的高深度消耗。这一思想启发人们思考：能否将同样的融合策略应用于LayerNorm的倒数平方根计算？

与RBOOT中处理ReLU、Sign等分段函数不同，LayerNorm的倒数平方根函数并不能直接作为普通目标函数替换到EvalMod中。首先，$\dfrac{1}{\sqrt{x}}$在零点附近具有奇异性，且导数随x接近0而发散，若直接在包含零点或过近零点的区间上拟合，会导致多项式系数放大和噪声敏感性增强。其次，LayerNorm的输入是方差项，天然满足非负约束，而CKKS EvalMod的正弦域变量存在周期性和分支选择问题，若不约束输入范围，sin的周期别名会导致语义错误。最后，倒数平方根的输出尺度与预缩放后的方差尺度耦合，需要在复合函数中同时处理尺度恢复与稳定项。本文的贡献在于针对上述问题构造了带预缩放和统计边界的范围守卫，统一推导了正弦域复合目标函数，并分析了替换多项式对噪声传播的影响。

基于上述问题，本文提出了一种将$\dfrac{1}{\sqrt{\sigma^2 + \epsilon}}$融入CKKS Bootstrapping的新方法。本文的主要贡献如下。

（1）默认设置下零额外深度的融合式LayerNorm计算。本文在Bootstrapping的EvalMod阶段构造正弦域复合多项式$P_{\text{invsqrt}}(t) \approx \dfrac{1}{\sqrt{\dfrac{q_0}{2\pi}\arcsin(t) + \epsilon'}}$，将线性恢复与倒数平方根计算合并为一次多项式求值。在输入满足校准边界且不触发可选软裁剪的默认设置下，替换多项式与标准arcsin恢复多项式采用相同阶数和计算深度，因此不增加额外乘法深度。相比Goldschmidt迭代可节省6~8层乘法深度。

（2）低深度范围守卫机制。本文采用预缩放与

统计边界约束方差输入，使正弦域变量落在单调分支内，从而避免周期别名。对于分布外或统计保证不足的输入，本文进一步讨论可选软裁剪备用策略，该策略会额外消耗1~2层乘法深度，不计入本文默认零额外深度方案。

（3）极低的实现代价。本文方案仅需修改约50行代码（基于OpenFHEv1.1.2[17]），不改变Bootstrapping的整体结构。运行时计算量和内存占用与标准Bootstrapping完全一致。

1 背景知识

1.1 CKKS Bootstrapping原理

目前，CKKS方案是应用最广泛的支持近似算术的全同态加密方案，其核心特征是将实数（或复数）向量编码为多项式环 $R_Q=\dfrac{\mathbb{Z}_Q[X]}{X^N+1}$ 中的元素，并通过缩放因子 Δ 控制编码精度。CKKS方案支持同态加法、同态乘法和旋转操作（实现槽位间的循环移位）。每次乘法运算消耗模数链中的一层（约 $\mathrm{lb}\,\Delta$ bit），当模数耗尽时需要通过Bootstrapping刷新密文以恢复计算能力。

CKKS Bootstrapping的目标是将密文的模数从接近耗尽的 q_{low} 提升回初始模数 Q，同时保持加密消息的正确性。其核心挑战在于：模数提升（ModRaise）会在明文中引入 q_{low} 的整数倍噪声，必须通过同态方式将其消除。标准CKKS Bootstrapping包含4个阶段：模数提升、系数–槽域转换（CoeffsToSlots/SlotsToCoeffs）、模约减EvalMod和输出阶段。其中，EvalMod阶段是Bootstrapping的核心阶段，目标是同态地计算模约减函数，消除ModRaise阶段引入的 $q_{\mathrm{low}}I$ 噪声项。由于模约减函数是不连续的，无法直接用多项式逼近，CKKS采用正弦逼近和反正弦恢复的两步策略来实现。表1给出了典型CKKS Bootstrapping的深度分解，其中 P_{arcsin} 为逼近arcsin的多项式（典型阶数31）。

表1 典型CKKS Bootstrapping的深度分解

步骤	消耗深度	说明
CoeffsToSlots	4	层级预算配置
Sine逼近+倍角公式	7~8	63阶 + 2~3次倍角
P_{arcsin} 计算	5	31阶，Estrin方案
SlotsToCoeffs	4	层级预算配置
总计	$L_{\mathrm{boot}}\approx 19\sim21$	—

1.2 函数型Bootstrapping（RBOOT）

RBOOT的核心思想是：既然Bootstrapping过程中必须计算一个多项式来恢复消息，为什么不将该多项式替换为直接输出目标函数值的多项式？具体而言，在EvalMod阶段的最后一步，标准Bootstrapping计算：$P_{\mathrm{arcsin}}(t)\approx\dfrac{q_0}{2\pi}\arcsin(t)\approx m$。RBOOT将其替换为：$P_f(t)\approx f\left(\dfrac{q_0}{2\pi}\arcsin(t)\right)=f(m)$，即输出 $f(m)$ 而非 m，其中 f 为目标函数（如ReLU、Sign等）。

RBOOT的实现非常简洁，仅需将EvalMod阶段最后一步的多项式系数从 P_{arcsin} 的系数替换为 P_f 的系数。Bootstrapping的其他所有步骤（ModRaise、CoeffsToSlots、Sine逼近和SlotsToCoeffs）均保持不变。这里的关键约束是替换多项式 P_f 的阶数不应超过原 P_{arcsin} 的阶数（典型阶数31），否则将增加额外的乘法深度。当目标函数 f 在拟合区间上足够平滑时，31阶多项式通常可以提供充足的逼近精度。

RBOOT对目标函数 f 有以下要求：①可多项式逼近：目标函数 f 在拟合区间上可被有限阶多项式以足够精度逼近；②与正弦域兼容：复合函数 $g(t)=f\left(\dfrac{q_0}{2\pi}\arcsin(t)\right)$ 在 $t\in[-1,1]$ 的子区间上可良好逼近；③阶数匹配：所需多项式阶数不超过深度预算（典型阶数≤31阶）。

1.3 LayerNorm与RMSNorm

LayerNorm[9]是Transformer架构中的核心归一化组件，定义为 $\mathrm{LayerNorm}(\boldsymbol{x})=\boldsymbol{\gamma}\odot\dfrac{\boldsymbol{x}-\mu}{\sqrt{\sigma^2+\epsilon}}+\boldsymbol{\beta}$，其中，$\boldsymbol{x}=(x_1,x_2,\cdots,x_H)\in\mathbb{R}^H$ 为隐藏层向量，$\mu=\dfrac{1}{H}\sum_{i=1}^{H}x_i$ 为均值，$\sigma^2=\dfrac{1}{H}\sum_{i=1}^{H}(x_i-\mu)^2$ 为方差，$\epsilon>0$ 为数值稳定性常数（通常取 10^{-5} 或 10^{-6}）。$\boldsymbol{\gamma},\boldsymbol{\beta}\in\mathbb{R}^{\mathrm{H}}$ 为可学习的缩放和偏移参数。

RMSNorm[10]是LayerNorm的简化变体，省去均值计算 $\mathrm{RMSNorm}(\boldsymbol{x})=\boldsymbol{\gamma}\odot\dfrac{\boldsymbol{x}}{\sqrt{\dfrac{1}{H}\sum_{i=1}^{H}x_i^2+\epsilon}}$，两者的核心计算瓶颈均为倒数平方根 $\dfrac{1}{\sqrt{\sigma^2+\epsilon}}$（或 $\dfrac{1}{\sqrt{\mathrm{RMS}^2+\epsilon}}$）。

在CKKS同态加密下，LayerNorm各步骤有不同的计算难度，如表2所示。

目前，在同态加密中计算$\frac{1}{\sqrt{x}}$的主流方法是Goldschmidt迭代（又称倒数平方根迭代），其迭代公式为$y_0 = x,\ \ h_0 = x \cdot c_0, h_{i+1} = h_i \cdot \frac{3 - y_i \cdot h_i}{2}$，$y_{i+1} = y_i \cdot \frac{3 - y_i \cdot h_i}{2}$，其中$c_0$为初始估计值（通常通过分段线性逼近获得），迭代收敛到$h_k \to \frac{1}{\sqrt{x}}$。

在每次Goldschmidt迭代中，$y_i h_i$消耗1层深度，$h_{i+1} = h_i \frac{3 - y_i h_i}{2}$依赖步骤1的结果，再消耗1层深度。因此，每次迭代消耗两层深度。达到足够精度通常需要$k \geqslant 3$次迭代（对应double精度范围内的收敛），总计消耗$2k \geqslant 6$层深度。

Goldschmidt迭代方法有局限性，其深度消耗高，6~8层深度在Bootstrapping后的剩余预算中占比显著。收敛依赖初值，初始估计c_0的质量影响收敛速度。此外，每次迭代需保存y_i、h_i等中间结果，增加内存开销。本文的核心动机正是消除Goldschmidt迭代的这些开销，通过将$\frac{1}{\sqrt{x}}$融入Bootstrapping实现“零额外深度”的倒数平方根计算。

1.4　相关工作

隐私保护神经网络推理是全同态加密的重要应用方向。CryptoNets[18]首次实现了基于FHE的神经网络推理，但仅支持浅层网络。Lee等[16]通过多路复用并行卷积和低阶最小极大近似多项式，在CKKS上实现了深层卷积神经网络（convolutional neural network, CNN）的高效推理，但ReLU的多项式近似仍需消耗大量乘法深度。Lee等[19]进一步优化了近似精度，但非线性层的深度瓶颈依然存在。RBOOT提出将ReLU函数融入Bootstrapping，实验表明可将每个ReLU的深度消耗从14~20层降至约8层，推理速度提升2.77倍，峰值内存降低81%。然而，RBOOT仅针对ReLU函数，尚未考虑Transformer中LayerNorm/RMSNorm的倒数平方根计算。本文面向Transformer LayerNorm/RMSNorm中的倒数平方根瓶颈，提出了一种适配CKKS函数型Bootstrapping的融合式计算方法。与已有RBOOT主要面向ReLU等激活函数不同，本文处理的是具有零点奇异性、非负定义域和尺度耦合特征的归一化函数，并给出了范围守卫、复合目标函数构造及噪声传播分析。

在CKKS Bootstrapping方面，Cheon等[12]首次提出了CKKS的Bootstrapping方法，Bossuat等[13]进一步优化了非稀疏密钥场景下的效率。CKKS领域近期的重要改进之一是Drucker等[20]提出的一种能够处理离散计算的CKKS变体。Discrete CKKS的核心是CKKS风格的函数型/可编程Bootstrapping[21-23]，它能够在Bootstrapping过程中计算任意函数。基于这一框架，已有多项研究工作[24-25]构建了整数计算单元，从而支持包括逻辑运算在内的高效高精度整数计算。本文方案是基于CKKS的Bootstrapping方法，可以直接集成到任何标准CKKS Bootstrapping实现中。

Transformer推理中的LayerNorm/RMSNorm需要计算$\frac{1}{\mathrm{sqrt}(x)}$，传统同态实现通常采用Goldschmidt或Newton-Raphson迭代，额外消耗多层乘法深度。与ReLU、Sign等函数不同，$\frac{1}{\mathrm{sqrt}(x)}$具有零

表2　CKKS同态加密下LayerNorm各步骤的计算难度

步骤	操作	同态实现方式	深度消耗
均值μ	$\sum \frac{x_i}{H}$	Rotate-and-Sum	lb H次旋转，0层深度
残差$x_i - \mu$	向量减法	同态减法	0层深度
方差σ^2	$\frac{\sum (x_i - \mu)^2}{H}$	同态平方+Rotate-and-Sum	1层深度
倒数平方根	$\frac{1}{\sqrt{\sigma^2 + \epsilon}}$	迭代算法	≥6层深度
归一化	$\frac{x_i - \mu}{\sqrt{\sigma^2 + \epsilon}}$	同态乘法	1层深度
仿射变换	$\gamma \cdot \hat{x} + \beta$	同态乘法和加法	1层深度

点奇异性、非负定义域和尺度耦合等特征，不能直接平凡替换到EvalMod中。本文的主要工作在于：通过稳定项、预缩放和统计边界构造范围守卫，统一推导正弦域目标函数$h(t)=\frac{1}{\mathrm{sqrt}\left(\frac{\arcsin(t)}{\alpha s}\right)}$，并给出噪声传播和参数敏感性分析，从而在默认设置下实现零额外深度的融合式同态LayerNorm。

2 方案设计

2.1 核心思想

LayerNorm的核心计算式为$\hat{x}_i=\frac{x_i-\mu}{\sqrt{\sigma^2+\epsilon}}$，其中，$\sigma^2=\frac{1}{H}\sum j=1^H(x_j-\mu)^2$为方差。在同态加密环境下，$\frac{1}{\sqrt{\sigma^2+\epsilon}}$为计算瓶颈，传统Goldschmidt迭代方法通常需要至少消耗6层乘法深度。

核心洞察：CKKS Bootstrapping在EvalMod阶段需要计算一个高阶多项式来逼近$\arcsin(\sin(\theta))$，以实现模约减。本文观察到，通过将该多项式替换为直接输出$\frac{1}{\sqrt{x}}$的复合多项式，可以在自举过程中“免费”获得倒数平方根的计算结果。

关于复合函数的构造，本文首先统一变量定义。设LayerNorm的原始方差为$v=\sigma^2$，稳定项后输入为$u=v+\epsilon$。范围守卫对u进行预缩放，得到$z=su=s(\sigma^2+\epsilon)$，其中$s$为由方差上界$V_{\max}$和安全边界$\delta$决定的缩放因子。在CKKS Bootstrapping的EvalMod阶段，正弦逼近和倍角步骤产生正弦域变量$t=\sin(\alpha z)$，其中α为由CKKS模约减尺度决定的常数。

标准Bootstrapping的恢复步骤可理解为利用$P_{\arcsin}(t)$近似恢复z。本文将该恢复多项式替换为复合多项式$P_{\mathrm{invsqrt}}(t)$，直接输出LayerNorm所需的倒数平方根值。由于在范围守卫保证的单调区间内有$\arcsin(t)=\alpha z=\alpha s(\sigma^2+\epsilon)$，目标函数可统一写为$h(t)=\frac{1}{\mathrm{sqrt}\left(\frac{\arcsin(t)}{\alpha s}\right)}$。

因此，本文实际拟合的是正弦域变量t上的复合函数$h(t)$，而不是直接在方差变量v上拟合$\frac{1}{\mathrm{sqrt}(v+\epsilon)}$。该多项式将arcsin线性恢复与倒数平方根计算合并为一次多项式求值，不需要自举后的额外迭代计算。

为更清晰地描述本文的融合式同态LayerNorm方案，算法1给出默认设置下的完整计算流程。默认方案仅包含预缩放、统计边界和EvalMod替换多项式，不启用可选软裁剪；软裁剪仅用于分布外输入或校准统计不足时的备用场景。

算法1 默认设置下的融合式同态LayerNorm方案

输入 密文向量$\mathrm{ct}_x=\mathrm{Enc}(x)$，隐藏维度$H$，稳定项$\epsilon$，校准方差上界$V_{\max}$，安全边界$\eta$，缩放因子$s=\frac{\frac{q_0}{4}-\delta}{V_{\max}+\epsilon}$，替换多项式$P_{\mathrm{invsqrt}}(t)$

输出 密文归一化结果$\mathrm{ct}_y\approx\mathrm{Enc}\left(\frac{x-\mu}{\mathrm{sqrt}(\sigma^2+\epsilon)}\right)$

1) 通过Rotate-and-Sum计算均值$\mathrm{ct}_\mu=\mathrm{Enc}\left(\frac{1}{H\sum x_i}\right)$

2) 计算残差$\mathrm{ct}_r=\mathrm{ct}_x-\mathrm{ct}_\mu$

3) 通过同态平方和旋转求和计算方差$\mathrm{ct}_v=\mathrm{Enc}(\sigma^2)=\mathrm{Enc}\left(\frac{1}{H\sum(x_i-\mu)^2}\right)$

4) 加入稳定项并预缩放：$\mathrm{ct}_z=s(\mathrm{ct}_v+\epsilon)$

5) 对ct_z执行CKKS Bootstrapping。在EvalMod阶段，将标准恢复多项式$P_{\arcsin}(t)$替换为$P_{\mathrm{invsqrt}}(t)$，其中目标函数为$h(t)=\frac{1}{\mathrm{sqrt}\left(\frac{\arcsin(t)}{\alpha s}\right)}$

6) Bootstrapping输出$\mathrm{ct}_q\approx\mathrm{Enc}\left(\frac{1}{\mathrm{sqrt}(\sigma^2+\epsilon)}\right)$

7) 计算归一化结果$\mathrm{ct}_y=\mathrm{ct}_r\mathrm{ct}_q$；若模型包含可学习参数$\gamma$、$\beta$，则进一步计算$\mathrm{ct}_y=\gamma\mathrm{ct}_y+\beta$

在输入满足$\sigma^2\leqslant V_{\max}$且不触发可选软裁剪的默认设置下，步骤5)中的$P_{\mathrm{invsqrt}}$与标准$P_{\arcsin}$采用相同阶数和多项式求值深度，因此倒数平方根计算不引入额外乘法深度。

2.2 技术挑战与解决方案

（1）挑战1：零点奇异性

问题描述：函数$f(x)=\frac{1}{\sqrt{x}}$在$x=0$处无定义，且当$x\to 0$时趋向无穷大，多项式无法逼近此行为。

解决方案：在进入自举前，对方差施加偏移$\sigma'^2=\sigma^2+\epsilon,\ \epsilon>0$，其中$\epsilon$为LayerNorm的标准稳

定性常数（通常为10^{-5}或10^{-6}）。这确保逼近定义域为$[\epsilon, V_{\max}+\epsilon]$，严格避开零点。

（2）挑战2：周期别名风险

问题描述：EvalMod阶段使用$\sin(\theta)$进行模约减。正弦函数是周期函数，如果输入x超出单调区间$\left[-\frac{q_0}{4},\frac{q_0}{4}\right]$，正弦函数将发生“折返”（即两个不同的$x$值映射到相同的$\sin(x)$值），导致语义错误而非仅仅是精度损失。该问题很严重，因为这是正确性问题，任何越界都将导致完全错误的输出。

解决方案：本文采用默认范围守卫机制限制输入落入正弦函数的单调区间。默认方案由预缩放和统计边界两部分构成。此外，针对分布外输入或统计边界不足的场景，本文讨论可选软裁剪备用策略。

① 预缩放：设原始方差为$v=\sigma^2$，稳定项后输入为$u=v+\epsilon$。本文对u而非单独的v进行预缩放，即$z=s(\sigma^2+\epsilon)$，其中缩放因子$s=\frac{\frac{q_0}{4}-\delta}{V_{\max}+\epsilon}$，$V_{\max}$为统计确定的方差上界，$\delta$为安全边界。这样，当$0\leqslant\sigma^2\leqslant V_{\max}$时，有$0<s(\sigma^2+\epsilon)\leqslant\frac{q_0}{4}-\delta$，从而保证进入EvalMod阶段的正弦域变量对应的角度位于单调区间内。

② 统计边界：在模型校准阶段，收集每层的方差统计信息，计算99.9%分位数作为$V_{\max}$。

③ 可选软裁剪备用策略：若部署场景中输入分布可能明显偏离校准集，导致统计边界$V_{\max}$不再可靠，可在自举前应用低阶多项式逼近的软裁剪函数，将异常方差压回安全区间。需要强调的是，软裁剪不是本文默认实验和定理分析中的必选步骤；一旦启用软裁剪备用策略，将额外消耗1~2层乘法深度，因此该备用策略不再满足严格的零额外深度声明。

默认范围守卫的核心目标可归结为以下形式化约束，以确保缩放后的输入角度始终落在正弦函数的单调区间内：$\forall\sigma^2\in[0,V_{\max}]:\cdots\in\left(0,\frac{\pi}{2}\right)$。

定理 1　范围守卫正确性。设输入方差$\sigma^2\in[0,V_{\max}]$，缩放因子定义为$s=\frac{\frac{q_0}{4}-\delta}{V_{\max}+\epsilon}$，其中$\delta>0$为安全边界，$\epsilon>0$为LayerNorm稳定性常数。则对于任意$\sigma^2\in[0,V_{\max}]$，有$\theta=\frac{2\pi}{q_0}s(\sigma^2+\epsilon)\in\left[\frac{2\pi s\epsilon}{q_0},\frac{\pi}{2}-\frac{2\pi\delta}{q_0}\right]\subset\left(0,\frac{\pi}{2}\right)$。因此，$\sin(\theta)$在该区间内严格单调递增，不存在周期别名。

证明　首先看下界：当$\sigma^2=0$时，$\theta_{\min}=\frac{2\pi s\epsilon}{q_0}>0$（因$s,\epsilon>0$）。上界是：当$\sigma^2=V_{\max}$时，$\theta_{\max}=\frac{2\pi}{q_0}s(V_{\max}+\epsilon)=\frac{2\pi}{q_0}\frac{\frac{q_0}{4}-\delta}{V_{\max}+\epsilon}(V_{\max}+\epsilon)=\frac{\pi}{2}-\frac{2\pi\delta}{q_0}$。由于$\delta>0$，有$\theta_{\max}<\frac{\pi}{2}$。结合$\theta_{\min}>0$，整个区间$(\theta_{\min},\theta_{\max})\subset\left(0,\frac{\pi}{2}\right)$，在此区间内$\sin(\theta)$严格单调递增。证毕。

（3）挑战3：定义域不匹配

问题描述：首先是输入方差σ^2恒为非负：$\sigma^2\in[0,+\infty)$。其次是EvalMod阶段输出$\sin(\theta)\in[-1,1]$，理论上包含负值。在计算流程中，数据经历3个阶段的变换：输入方差σ^2经过Bootstrapping变为正弦域中间值$\sin(\theta)$，再经复合多项式$P_{\text{invsqrt}}(\cdot)$映射为最终输出$\frac{1}{\sqrt{\sigma^2+\epsilon}}$。该流程可表示为$\sigma^2\xrightarrow{\text{范围守卫 + Bootstrapping}}\sin(\theta)\xrightarrow{P_{\text{invsqrt}}(\cdot)}\frac{1}{\sqrt{\sigma^2+\epsilon}}$。

解决方案：利用范围守卫机制保证正区间。由定理1可知，范围守卫机制确保$\theta\in\left(0,\frac{\pi}{2}\right)$。在此区间内，当$\sin(\theta)\in(0,1)$时，始终为正，与方差的非负性匹配；当$\sin(\theta)$严格单调递增时，满足arcsin反函数的存在性。

因此，虽然CKKS自举天然同时产生$\sin(\theta)$和$\cos(\theta)$（源于复数槽结构），但本文设计中使用sin通道即可，因为范围守卫已将输入约束到sin的“安全区域”。那么为何不选择cos通道？二者对比如表3所示。

表3　sin通道与cos通道的对比

特性	$\sin(\theta)$（本文采用）	$\cos(\theta)$
$\theta\in(0,\frac{\pi}{2})$的值域	(0, 1)，单调递增	(0, 1)，单调递减
反函数	arcsin（与标准CKKS实现一致）	arccos（需修改EvalMod）
实现复杂度	低（复用现有代码）	高（需定制）

选择 sin 通道可直接复用现有 CKKS 库的 arcsin 多项式，降低实现复杂度。

2.3 多项式拟合

Remez 算法的目标函数定义为正弦域复合函数 $h(t)$，而不是方差域函数。根据 2.1 节的定义，有 $t=\sin(\alpha s(\sigma^2+\epsilon))$。在范围守卫保证 $\alpha s(\sigma^2+\epsilon)$ 位于正弦单调区间时，有 $\arcsin(t)=\alpha s(\sigma^2+\epsilon)$，因此 $h(t)=\dfrac{1}{\mathrm{sqrt}\left(\dfrac{\arcsin(t)}{\alpha s}\right)}$。拟合区间由方差范围 $0\leqslant\sigma^2\leqslant V_{\max}$ 映射得到：$t\in[t_{\min},t_{\max}]=[\sin(\alpha s\epsilon),\sin(\alpha s(V_{\max}+\epsilon))]$。

本文采用切比雪夫多项式基表示 $P_{\mathrm{invsqrt}}(t)$，并在上述区间上使用 Remez 算法求解 $h(t)$ 的 31 阶极小极大逼近。

使用 Remez 算法求解极小极大逼近：$P^*=\arg\min_{P\in\mathcal{P}d}\max t\in[a,b]|P(t)-f_{\mathrm{target}}(t)|$。算法的流程是输入目标函数 $f(t)$，区间 $[a,b]$，阶数 d，容差 ϵ，输出是最优系数 $\{c_0,\cdots,c_d\}$。

引理 1 Remez 最优性。设 $P^{(t)}$ 为 Remez 算法在区间 $[a,b]$ 上对目标函数 $f_{\mathrm{target}}(t)$ 的 d 阶输出，则 $\|P^*-f_{\mathrm{target}}\|_\infty=E_d(f_{\mathrm{target}})=\inf_{p\in\mathcal{P}d}\|f_{\mathrm{target}}-p\|_\infty$，即 Remez 算法输出的多项式达到该阶数下的最佳逼近误差。

证明 Remez 算法的输出满足 Chebyshev 等振性质。误差函数 $e(t)=P^*(t)-f(t)$ 在区间 $[a,b]$ 上至少有 $d+2$ 个交替符号的极值点，且极值绝对值相等。由 Chebyshev 定理可知，这是最佳逼近的充要条件。证毕。

引理 2 解析函数的指数衰减。若 f_{target} 在包含区间 $[a,b]$ 的 Bernstein 椭圆 $\mathcal{E}\rho$（$\rho>1$）内解析，且 $|f(z)|\leqslant M$ 对所有 $z\in\mathcal{E}\rho$ 成立，则 $E_d(f_{\mathrm{target}})\leqslant\dfrac{2M\rho^{-d}}{\rho-1}$。

证明 这是 Bernstein 逼近定理的直接结论。

对于本文统一后的目标函数 $h(t)=\dfrac{1}{\mathrm{sqrt}\left(\dfrac{\arcsin(t)}{\alpha s}\right)}$，潜在奇点主要来自两类：一是 $\arcsin(t)$ 在 $t=\pm1$ 附近存在分支点；二是当 $\dfrac{\arcsin(t)}{\alpha s}=0$ 时，倒数平方根项存在零点奇异性。本文通过范围守卫将拟合区间限制为 $[\sin(\alpha s\epsilon),\sin(\alpha s(V_{\max}+\epsilon))]$，其下界对应 $\sigma^2=0$ 时的稳定项 ϵ，因此 $\dfrac{\arcsin(t)}{\alpha s}\geqslant\epsilon>0$；同时上界与正弦折返点保持安全边界 δ。因此，$h(t)$ 在所选闭区间及其邻域内解析，Remez 多项式可稳定逼近该目标函数。证毕。

在多项式计算策略方面，为减少同态计算的深度消耗，采用 Estrin 方法进行并行计算：$P(t)=(c_0+c_1t)+t^2(c_2+c_3t)+t^4(\cdots)$。与 Horner 方法的对比，如表 4 所示。

表 4 多项式计算方法对比

方法	乘法深度	并行性
Horner	d（必须串行）	无
Estrin	$\lceil\mathrm{lb}(d+1)\rceil$	高

对于 63 阶多项式，Estrin 方法将乘法深度从 63 降至 6。

2.4 噪声传播分析

本文将标准 CKKS Bootstrapping 中的 $P_{\arcsin}$ 替换为 P_{invsqrt}。虽然替换前后多项式阶数相同，但倒数平方根目标函数在小值附近曲率较大，可能影响 EvalMod 阶段的噪声传播。因此，本节从误差分解角度分析替换多项式对输出误差的影响，并结合实验数据说明本文方案的误差主要由 CKKS Bootstrapping 的固有噪声主导，而非由 Remez 算法逼近误差主导。

设原始方差为 $v=\sigma^2$，稳定项后输入为 $u=v+\epsilon$，预缩放后输入为 $z=su=s(\sigma^2+\epsilon)$。在 EvalMod 阶段，正弦域变量记为 $t=\sin(\alpha z)$，其中 α 为由 CKKS Bootstrapping 模约减尺度决定的常数。在范围守卫保证 αz 位于正弦单调区间时，有 $\arcsin(t)=\alpha z$，因此本文替换多项式的理想目标函数为 $h(t)=\dfrac{1}{\mathrm{sqrt}\left(\dfrac{\arcsin(t)}{\alpha s}\right)}$。

在实际同态计算中，由正弦逼近、倍角公式、重缩放和密文噪声共同引入的误差会使正弦域输入变为 $\tilde{t}=t+e_t$，其中 e_t 表示进入最后一步多项式求值前的正弦域误差。设 $P_{d(t)}$ 为 d 阶 Remez 多项式，本文中 $d=31$。最终输出误差可分解为 $|\tilde{y}-y|=|P_d(\tilde{t})-h(t)|\leqslant|P_d(\tilde{t})-P_d(t)|+|P_d(t)-h(t)|+e_{\mathrm{eval}}$，其中 e_{eval} 表示多项式同态求值过程中的系数舍入、重缩放和 CKKS 近似噪声。由均值定理可得 $|P_d(\tilde{t})-P_d(t)|\leqslant L_P|e_t|$，其中 $L_P=\max_\{\xi\in I\}|P'_d(\xi)|$，$I=[t_\min,t_\max]=[\sin(\alpha s\epsilon),\sin(\alpha s(V_{\max}+\epsilon))]$ 为 Remez

拟合区间。因此，总误差满足上界 $|\tilde{y}-y| \leqslant L_P|e_t| + e_{\text{poly}} + e_{\text{eval}}$，其中 $e_{\text{poly}} = \max_{t\in I}|P_d(t)-h(t)|$ 为 Remez 逼近误差，其表明替换多项式是否导致额外噪声放大，主要由两个量决定：一是 Remez 逼近误差 e_{poly}；二是多项式导数上界 L_P。

进一步，若直接考察理想目标函数 $h(t)$ 的导数，可得 $h'(t) = -\dfrac{1}{2\alpha s\sqrt{1-t^2}}\left(\dfrac{\arcsin(t)}{\alpha s}\right)^{-\frac{3}{2}}$，其说明 $\dfrac{1}{\text{sqrt}(x)}$ 在 x=0 附近的导数发散会反映为 $h(t)$ 在区间下界附近的较大斜率。本文通过两点控制该风险：一是 LayerNorm 的稳定项 ϵ 使 $\dfrac{\arcsin(t)}{\alpha s} \geqslant \epsilon$，避免目标函数在使用区间内触及零点；二是范围守卫将 t 限制在正弦函数单调区间内，并保留安全边界 δ，使 $\text{sqrt}(1-t^2)$ 不接近 0。因此，在本文拟合区间 I 内，$h(t)$ 和 $P_{d(t)}$ 的导数均有界，噪声放大因子可由 L_P 显式度量。

在实验层面，本文进一步汇总多项式逼近误差、倒数平方根密文计算误差以及最终 LayerNorm 输出误差，如表 5 所示。

表 5　替换多项式的误差传播与密文执行误差

指标	数值	说明
Remez 逼近误差 e_{poly}	8.6×10^{-11}	d=31 时 P_{invsqrt} 的离线最大逼近误差
$\dfrac{1}{\text{sqrt}(\sigma^2+\epsilon)}$ 平均相对误差	3.2×10^{-7}	密文端倒数平方根平均相对误差
$\dfrac{1}{\text{sqrt}(\sigma^2+\epsilon)}$ 最大相对误差	1.8×10^{-6}	密文端倒数平方根最大相对误差
$\dfrac{1}{\text{sqrt}(\sigma^2+\epsilon)}$ 平均绝对误差	4.5×10^{-7}	密文端倒数平方根平均绝对误差
LayerNorm 输出平均绝对误差	6.8×10^{-6}	逐元素统计
LayerNorm 输出最大绝对误差	4.2×10^{-5}	逐元素统计
LayerNorm 输出 RMSE	8.3×10^{-6}	逐元素统计

表 5 表明，d=31 时 P_{invsqrt} 的离线 Remez 逼近误差为 8.6×10^{-11}，而密文端 $\dfrac{1}{\text{sqrt}(\sigma^2+\epsilon)}$ 的平均绝对误差为 4.5×10^{-7}，二者相差约 4 个数量级。这说明在当前参数下，系统误差主要来自 CKKS Bootstrapping 和后续同态运算中的近似噪声，而不是来自 P_{invsqrt} 的多项式逼近误差。进一步，最终 LayerNorm 输出的平均绝对误差为 6.8×10^{-6}，最大绝对误差为 4.2×10^{-5}，均方根误差（root mean square error, RMSE）为 8.3×10^{-6}，仍处于深度学习推理可接受范围内。因此，虽然 P_{invsqrt} 的目标函数曲率高于标准 arcsin 恢复函数，但在稳定项 ϵ 和范围守卫约束下，该替换并未造成不可控的噪声放大。

综上所述，本文替换多项式的误差可分解为正弦域输入误差放大项、Remez 逼近误差和同态求值误差三部分。稳定项 ϵ 和范围守卫使目标函数在拟合区间内远离零点奇异性和正弦折返点，从而保证误差放大因子有限。实验结果表明，Remez 逼近误差远低于密文端实际误差，最终 LayerNorm 输出误差也保持在可接受范围内。因此，P_{invsqrt} 替换不会成为本文方案的主要精度瓶颈。

2.5　复杂度分析

复杂度对比如表 6 所示。

表 6　　复杂度对比

方法	乘法深度	内存占用	正确性保证
Goldschmidt 迭代	$L_{\text{boot}}+2k$（$k\geqslant3$）	高（需更大 Q）	依赖收敛性
本文方案	$L_{\text{boot}}+\Delta_{\text{本文方案}}$	低	依赖范围守卫

定理 2　默认方案下的深度节省。设 Goldschmidt 迭代需要 k 次迭代收敛（典型 $k\geqslant3$），设自举深度为 L_{boot}，替换后的 P_{invsqr} 与原 P_{arcsin} 采用相同阶数和多项式求值策略，则 $D_{\text{Goldschmidt}} = L_{\text{boot}} + 2k$，$D_{\text{本文方案}} = L_{\text{boot}} + \Delta_{\text{本文方案}}$，本文默认方案相对于标准 Bootstrapping 的额外深度 $\Delta_{\text{本文方案}} = 0$。相比 Goldschmidt 迭代方法，本文方法节省 $2k$ 层乘法深度，当 k=3 时节省 6 层。

证明　本文默认方案仅采用预缩放与统计边界，不启用软裁剪。因此，范围守卫不引入额外乘法深度，其作用仅是常数缩放与明文参数配置。首先计算 Goldschmidt 迭代深度。Goldschmidt 算法计算 $\dfrac{1}{\sqrt{x}}$ 的每次迭代包含 $h_i = \dfrac{3-y_i x}{2}$，需要先计算 $y_i x$，因此消耗 1 层深度。然后包含 $y_{i+1} = y_i h_i$，其依赖 h_i，需要串行执行，因此再消耗 1 层深度。所以每次迭代消耗 2 层深度。另外达到所需精度需 $k\geqslant3$ 次迭代，总计 $2k\geqslant6$ 层。

本文方案是将 $\frac{1}{\sqrt{x}}$ 融入 Bootstrapping 的 EvalMod阶段。当替换后的多项式 P_{invsqrt} 的计算深度不超过原 EvalMod 恢复步骤的深度预算时，$\Delta_{\text{本文方案}} = 0$。因此，$D_{\text{Goldschmidt}} - D_{\text{本文方案}} = 2k - \Delta_{\text{本文方案}} \geqslant 6$。证毕。

推论 设每层深度对应的模数位数为 Δq bit。本文方案允许减少总模数链长度，从而可能降低所需 Q，并在满足同等安全级别的条件下潜在允许选择更小的 N 或更快的 Bootstrapping 参数配置，从而实现系统级加速。

3 方案实现

表 7 列出了 CKKS 全同态加密的核心参数配置。

表 7 CKKS 核心参数配置

参数	符号	推荐值	说明
多项式度数	N	2^{16}	支持足够的深度和槽位数量
槽位数量	$\frac{N}{2}$	2^{15}	全打包模式
基础模数	q_0	$\approx 2^{51}$	Bootstrapping 后的精度保证
模数链总长	$\text{lb}Q_{\text{boot}}$	≈1 500 bit	由 Bootstrapping 消耗深度决定
缩放因子	Δ	2^{45}	平衡精度与溢出风险

注意，本节中 q_0 均指模数的数值（约 2^{51}），而非位长。参数选择依据如下：根据文献[26]，在 $N=2^{16}$ 的设置下，128 位安全级别允许的最大模数约为 1 747 位。本文采用的主模数链总长约为 1 500 位，低于该上限，因此在上述安全估计模型和计入总模数范围下满足 128 位安全级别。若实现中 Bootstrapping 或 key switching 使用辅助模数，则安全估计应以实际计入的总模数为准。$N = 2^{16}$ 满足 128 位安全级别下支持 Bootstrapping 的最小需求；$q_0 \approx 2^{51}$ 确保 Bootstrapping 后有足够精度进行后续 LayerNorm 计算；$\Delta = 2^{45}$ 在典型 LLM 激活值范围内避免溢出。

对于 Transformer 模型，本文采用行优先展平的槽位布局策略：将二维张量 [Batch,Hidden$_{\text{D}}$im] 按行优先顺序展平为一维向量，依次填入密文的各个槽位。即先填入第 0 个样本的全部 H 个隐藏维度分量，再紧接着填入第 1 个样本，以此类推。

范围守卫参数配置如表 8 所示。

表 8 范围守卫参数配置

参数	符号	典型值	说明
稳定性常数	ϵ	10^{-5}	LayerNorm 标准值
安全边界比例	η	5%	预留安全余量
安全边界	δ	$\eta\left(\frac{q_0}{4}\right)$	安全缓冲距离
方差上界	$V_{\max}$	模型校准获得	99.9% 分位数
缩放因子	s	$\frac{\frac{q_0}{4} - \delta}{V_{\max} + \epsilon}$	由定理 1 确定

校准流程：在明文数据集上运行模型前向传播；收集每层 LayerNorm 的方差统计；计算 99.9% 分位数作为 $V_{\max}$；计算对应的缩放因子 s。

标准 CKKS Bootstrapping 的 EvalMod 阶段执行以下步骤。

（1）正弦逼近：计算 $t = \sin\left(\frac{2\pi}{q_0}x'\right)$。

（2）倍角迭代：通过倍角公式扩展频率。

（3）反正弦恢复：计算 $P_{\arcsin}(t)$ 恢复线性值。

注意，不同 CKKS 方案实现可能采用不同的恢复策略（如 EvalExp 变种）。

本文对 EvalMod 的修改仅涉及最后一步。标准的 EvalMod 是：$\sin(\theta) \to P_{\arcsin}(t) \to x'$（恢复线性）。而本文修改的 EvalMod 是：$\sin(\theta) \to P_{\text{invsqrt}}(t) \to \frac{1}{\sqrt{\sigma^2 + \epsilon}}$（直接输出结果）。其中，$P_{\text{invsqrt}}$ 的输入不是方差 σ^2，而是 EvalMod 中的正弦域变量 $t=\sin(\alpha s \cdot (\sigma^2+\epsilon))$；其拟合目标为 $h(t)=\frac{1}{\text{sqrt}\left(\frac{\arcsin(t)}{\alpha s}\right)}$。

使用 Remez 算法离线生成 P_{invsqrt} 的系数。输入–输出关系推导如下。Bootstrapping 前的方差输入记为 $v = \sigma^2$，加入稳定项后得到 $u = v+\epsilon$，并经范围守卫预缩放为 $z=su=s(\sigma^2+\epsilon)$。EvalMod 的正弦域变量记为 $t=\sin(\alpha z)$。由于范围守卫保证 αz 位于正弦函数的单调区间内，因此有 $\arcsin(t)=\alpha z=\alpha s(\sigma^2+\epsilon)$。于是 LayerNorm 所需的倒数平方根可写为 $\frac{1}{\text{sqrt}(\sigma^2 + \epsilon)} = \frac{1}{\text{sqrt}\left(\frac{\arcsin(t)}{\alpha s}\right)}$。

因此，Remez 算法的目标函数统一为 $h(t)=$

$\frac{1}{\mathrm{sqrt}\left(\frac{\arcsin(t)}{\alpha s}\right)}$，并在区间$[t_{\min}, t_{\max}]=[\sin(\alpha s\epsilon), \sin(\alpha s(V_{\max}+\epsilon))]$上求解31阶极小极大逼近$P_{\mathrm{invsqrt}}(t)$。由于尺度因子$\alpha s$已包含在目标函数定义中，$P_{\mathrm{invsqrt}}(t)$的输出为$\frac{1}{\mathrm{sqrt}(\sigma^2+\epsilon)}$，不需要在自举后再进行额外迭代或尺度校正。拟合区间由定理1确定：$t\in[\sin(\theta_{\min})+\tau, \sin(\theta_{\max})-\tau]$，其中$\theta_{\min}=\frac{2\pi s\epsilon}{q_0}$，$\theta_{\max}=\frac{\pi}{2}-\frac{2\pi\delta}{q_0}$，$\tau$是数值稳定冗余量（典型值$10^{-6}$），避免边界处的数值不稳定。

表9中的Remez配置均针对正弦域目标函数$h(t)=\frac{1}{\mathrm{sqrt}\left(\frac{\arcsin(t)}{\alpha s}\right)}$，而非直接针对方差变量$v$上的$\frac{1}{\mathrm{sqrt}(v+\epsilon)}$。Remez算法配置如表9所示。

表9　　Remez算法配置

配置项	值
多项式度数	31（参考表10量化分析）
基函数	Chebyshev多项式
收敛精度	10^{-10}
系数精度	long double（避免精度损失）
输出格式	Chebyshev系数（直接用于EvalChebyshevSeries）

关于多项式度数，选择31阶Chebyshev多项式的量化依据如表10所示。

表10　　多项式度数选择的量化依据

阶数d	Remez L_∞误差
15	~ 10^{-4}
23	~ 10^{-7}
31	**~ 10^{-10}**
47	~ 10^{-14}

误差来源分析。方案的总误差由三部分组成：$\epsilon_{\mathrm{total}}=\epsilon_{\mathrm{approx}}+\epsilon_{\mathrm{coeff}}+\epsilon_{\mathrm{CKKS}}$，其中$\epsilon_{\mathrm{approx}}$是多项式逼近误差（Remez误差），$\epsilon_{\mathrm{coeff}}$是系数舍入误差（long double存储），$\epsilon_{\mathrm{CKKS}}$是CKKS噪声（rescale、Bootstrapping固有噪声）。

关于Lipschitz误差传播，对于$f(x)=x^{-\frac{1}{2}}$，在区间$x\in[\epsilon, V_{\max}+\epsilon]$上的Lipschitz常数为$L=\max_x|f'(x)|=\frac{1}{2}\epsilon^{-\frac{3}{2}}$。因此，多项式逼近误差$\epsilon_{\mathrm{approx}}$对最终输出的影响满足$|P(t)-f(x)|\le\epsilon_{\mathrm{approx}}$，这是绝对误差而非相对误差。对于典型值$\epsilon=10^{-5}$，$f(x)\in[1,316]$（对应$x\in[10^{-5},10]$），相对误差范围为$\frac{\epsilon_{\mathrm{approx}}}{f(x)}\in[3\times10^{-13},10^{-10}]$。

量化结论：31阶多项式的逼近误差$\epsilon_{\mathrm{approx}}\approx10^{-10}$远小于CKKS Bootstrapping的典型精度损失（~10^{-6}），因此多项式逼近不是精度瓶颈。

关于常数因子，虽然P_{invsqrt}与$P_{\arcsin}$度数相同，但由于目标函数在$t\to t_{\min}$处曲率较大（$\frac{1}{\sqrt{\arcsin(t)}}$的导数发散），系数幅度略大。替换多项式对噪声传播的影响已在第2.4节进行了详细分析。

4　实验评估

本节对本文方案进行全面的实验评估，从多项式逼近精度、深度消耗、运行时间和端到端推理性能4个维度进行验证，并与基于Goldschmidt迭代的传统方案进行对比。

4.1　实验分析

表11对比了本文方案与标准Bootstrapping的实现开销。数据基于Intel Xeon Gold6248R@3.0 GHz、256 GB内存的服务器，运行Ubuntu22.04LTS，使用GCC11.4.0编译OpenFHE v1.1.2，单线程模式执行。

表11　本文方案与标准Bootstrapping的实现开销对比

指标	标准Bootstrapping	本文方案	增量
代码修改量	—	~50行	极低
预计算（Remez）	无	一次性，小于1 s	可忽略
运行时内存（实测峰值）/GB	~6.5	~6.5	无变化
单次Bootstrapping时间/s	~12	~12	无变化

内存由剩余数系（residue number system, RNS）分解的临时缓冲区、数论变换（number

theoretic transform, NTT）变换、密钥等共同决定。本文方案不改变这些结构，因此内存占用与标准 Bootstrapping 一致。在时间方面，多项式度数相同（31 阶），Chebyshev 计算的乘法次数一致，因此计算量无变化。结论表明，本文方案的实现代价极低，主要工作是离线生成多项式系数，运行时与标准 Bootstrapping 完全等价。

为覆盖不同规模的推理场景，本文选取以下模型与数据集，如表 12 所示。

表 12　　模型与数据集

模型	隐藏维度 H	层数	数据集	用途
BERT-Tiny	128	2	SST-2	轻量场景验证
BERT-Base	768	12	SST-2	标准对比基准
GPT-2 单层 Block	768	1	WikiText-2	生成任务验证

在明文环境下，对 SST-2 验证集的 1 000 条样本运行前向传播，收集每层 LayerNorm 的方差统计。实验观察到，BERT-Tiny 模型方差分布集中在 [0.01, 3.5]，99.9% 分位数 $V_{\max} \approx 5.2$；BERT-Base 模型方差分布集中在 [0.02, 8.1]，99.9% 分位数 $V_{\max} \approx 12.7$；GPT-2 单层 Block 模型方差分布集中在 [0.05, 6.3]，99.9% 分位数 $V_{\max} \approx 9.8$。

本文方案与基线方案对比如下。

（1）Goldschmidt 迭代：标准 CKKS Bootstrapping 与 k 次 Goldschmidt 迭代计算 $\frac{1}{\sqrt{x}}$。取 $k = 3$（典型配置）和 $k = 4$（高精度配置）。

（2）Newton-Raphson 迭代：标准 CKKS Bootstrapping 与 Newton 迭代，$k = 4$ 次。

（3）明文 LayerNorm（Baseline）：未加密的 PyTorch 实现，作为精度参考。

首先验证 Remez 算法生成的 $P_{\text{invsqrt}}(t)$ 的逼近质量。表 13 给出了不同阶数下的最大绝对误差（L_∞ 误差）。

从表 13 可以看到，d=23 时最大逼近误差为 4.1×10^{-7}，已达到可用精度；当阶数提高到 d=31 时，最大逼近误差进一步降至 8.6×10^{-11}，显著低于 CKKS Bootstrapping 的固有近似噪声。31 阶多项式的逼近误差（$\sim10^{-11}$）远小于 CKKS Bootstrapping 的固有精度损失（$\sim10^{-6}$），因此多项式逼近不构成系统精度瓶颈，本文采用 d=31 作为默认多项式阶数。继续提高 d 至 47 或 63 虽可将离线逼近误差分别降低至 3.2×10^{-15} 和 1.8×10^{-19}，但会增加多项式求值深度，综合收益有限。因此，10^{-7} 量级主要对应阶数 d=23 的情形，而 d=31 及以上阶数的实测逼近误差已明显低于该量级。

表 13　Remez 逼近误差与多项式阶数（BERT-Base 参数）

阶数 d	L_∞ 误差	计算深度（Estrin）	备注
15	2.7×10^{-4}	4	精度不足
23	4.1×10^{-7}	5	可用
31	$\mathbf{8.6\times10^{-11}}$	**5**	**本文采用**
47	3.2×10^{-15}	6	过高，增加深度
63	1.8×10^{-19}	6	远超需求

将本文方案输出的 $\frac{1}{\sqrt{\sigma^2+\epsilon}}$ 与明文计算的真实值进行逐样本对比。对 BERT-Base 模型的 SST-2 验证集执行完整推理，记录每层 LayerNorm 的输出误差，如表 14 所示。

表 14　　$\frac{1}{\sqrt{\sigma^2+\epsilon}}$ 计算误差对比

方法	平均相对误差	最大相对误差	平均绝对误差
本文方案（d= 31）	3.2×10^{-7}	1.8×10^{-6}	4.5×10^{-7}
Goldschmidt（k= 3）	5.7×10^{-7}	3.1×10^{-6}	7.8×10^{-7}
Goldschmidt（k= 4）	2.1×10^{-8}	9.4×10^{-8}	3.6×10^{-8}
Newton-Raphson（k= 4）	4.3×10^{-8}	2.5×10^{-7}	5.9×10^{-8}

本文方案的精度与 Goldschmidt 处于同一量级，均满足深度学习推理的精度需求（相对误差 $< 10^{-5}$）。Goldschmidt 和 Newton 可达到更高精度，但需额外消耗 2 层乘法深度。本文方案的误差主要源于 CKKS Bootstrapping 的固有噪声（ϵ_{CKKS}），而非多项式逼近误差（ϵ_{approx}）。更重要的是 LayerNorm 最终输出 $\hat{x}_i = \frac{x_i - \mu}{\sqrt{\sigma^2+\epsilon}}$ 的精度。表 15 展示了归一化后每个元素的误差统计。

本文方案的 LayerNorm 输出精度略优于 Goldschmidt，且完全满足下游分类/生成任务的需求。

需要说明的是，表 14 和表 15 反映的是单次倒数平方根计算和单次 LayerNorm 输出误差，而端到端分类准确率还受到模型分类边界、样本分布

和后续非线性传播的影响，不应被理解为与单步数值误差严格单调对应。为观察多层LayerNorm调用下的累积效应，本文进一步在BERT-Base的12层Transformer结构上进行端到端同态推理实验。该设置每个样本包含24次LayerNorm调用，100条样本共包含2 400次LayerNorm调用；实验结果如表19所示，本文方案在多层累积后仍保持92.1%的分类准确率，与明文推理相差0.4个百分点，说明当前数值误差没有在多层调用中造成明显的任务级退化。

表15　LayerNorm输出误差（BERT-Base，逐元素统计）

方法	平均绝对误差	最大绝对误差	均方根误差（RMSE）
本文方案	6.8×10^{-6}	4.2×10^{-5}	8.3×10^{-6}
Goldschmidt（k= 3）	9.1×10^{-6}	5.7×10^{-5}	1.1×10^{-5}
Goldschmidt（k= 4）	2.4×10^{-7}	1.6×10^{-6}	3.1×10^{-7}

乘法深度是CKKS方案中最关键的资源，表16详细对比了各方案的乘法深度分解。

表16　　乘法深度分解对比

步骤	本文方案	Goldschmidt（k=3）	Goldschmidt（k=4）
Bootstrapping（L_{boot}）	19	19	19
EvalMod替换多项式（$\Delta_{\text{本文方案}}$）	0	—	—
Goldschmidt迭代	—	6	8
方差计算 + 归一化	3	3	3
总深度	**22**	**28**	**30**
节省深度	基准	—	—
相对节省	—	6层（21%）	8层（27%）

深度节省的量化意义：节省6~8层乘法深度意味着模数链总长缩短约$6 \times 50 = 300$位（每层≈ 50位）。在相同安全级别下，可选择更小的N，或在相同N下支持更多后续计算。对于多层Transformer模型，深度节省具有累积效应

表17展示了执行单次LayerNorm计算的运行时间分解，所有实验在单线程模式下重复10次，取平均值。

Bootstrapping操作在各方案中均为主要耗时部分（> 60%），与方案选择无关。本文方案省去了Goldschmidt迭代的4.2~5.6 s开销，但引入了范围守卫预处理（0.3 s），净节省3.9~5.3 s。相对于Goldschmidt，本文方案实现1.26×加速；相对于k = 4，实现1.36×加速。

表17　　单次LayerNorm运行时间分解

步骤	本文方案/s	Goldschmidt（k=3）/s	Goldschmidt（k=4）/s
方差计算（Rotate-Sum）	1.8	1.8	1.8
范围守卫（预缩放+偏移）	0.3	—	—
Bootstrapping	12.1	12.1	12.1
Goldschmidt/Newton迭代	—	4.2	5.6
归一化乘法	0.6	0.6	0.6
LayerNorm总计	**14.8**	**18.7**	**20.1**
加速比	基准	1.26×	1.36×

表18记录了各方案在执行LayerNorm时的峰值内存占用。

表18　　峰值内存占用

方案	峰值内存/GB	相对本文方案的内存增量/GB	本文方案相对该方案的内存节省/GB
本文方案	6.5	基准	基准
Goldschmidt（k=3）	7.8	+20%	16.7%
Goldschmidt（k=4）	8.4	+29%	22.6%

本文方案的内存占用与标准Bootstrapping一致（6.5 GB），因为不需要存储Goldschmidt迭代过程中的中间密文。Goldschmidt方法在迭代过程中需要额外保存y_i、h_i等中间结果密文，导致内存开销增大。

将本文方案集成到BERT-Base的完整同态推理流程中，在SST-2数据集上进行评估。本文评估样本数为1 000条，并报告准确率的95%置信区间，如表19所示。

表19　BERT-Base在SST-2上的同态推理性能

方案	分类准确率	95%置信区间	单样本推理时间/s	总深度消耗/层
明文推理（Baseline）	92.5%	[90.70%, 93.97%]	0.02	—
本文方案	92.1%	[90.26%, 93.62%]	178.2	22 × 12
Goldschmidt（k=3）	91.8%	[89.94%, 93.34%]	225.6	28 × 12
Goldschmidt（k=4）	92.3%	[90.48%, 93.80%]	242.4	30 × 12

所有同态方案的准确率与明文推理差距均小于1%，表明加密域LayerNorm的精度足够。本文方案准确率（92.1%）介于Goldschmidt（91.8%）和$k = 4$（92.3%）之间，接近$k = 4$的精度但时间开销远小于后者。在推理时间上，本文方案比Goldschmidt快21%，比$k = 4$快26%。

需要说明的是，表14中的倒数平方根误差、表15中的LayerNorm输出误差与表19中的端到端分类准确率并不构成严格单调关系。其根本原因在于，前两者是连续数值误差指标，衡量的是中间计算结果与明文结果之间的平均或最大偏差；分类准确率是离散任务指标，只有当数值扰动最终改变预测类别时才会发生变化。因此，较小的连续误差通常有助于提高稳定性，但并不必然对应严格更高的分类准确率。

从误差传播机理看，LayerNorm误差对最终分类结果的影响还取决于误差的分布位置、符号方向以及样本距离分类边界的远近。对于分类置信度较高、logit margin较大的样本，即使LayerNorm输出存在小幅扰动，后续注意力层、前馈层和分类头通常仍会保持相同预测；而对于接近决策边界的样本，较小但方向不利的扰动也可能改变最终类别。换言之，端到端分类准确率不仅与误差幅值有关，还与误差是否集中作用于分类边界附近样本、误差方向是否削弱正确类别logit有关。

因此，Goldschmidt(k=4)虽然在表14和表15中具有更小的连续数值误差，但其端到端分类准确率仅比本文方案略高，并不矛盾。这说明在当前实验设置下，本文方案的数值误差已经低于任务输出对LayerNorm扰动的敏感阈值。继续降低倒数平方根近似误差只能带来有限的任务级收益，却需要额外乘法深度、运行时间和内存开销。本文的主要结论并不是声称端到端分类准确率严格优于Goldschmidt(k=4)，而是在保持接近任务精度的同时显著降低乘法深度和系统开销。

表20展示了本文方案在不同模型规模下的性能表现。

本文方案的加速比在不同模型规模下保持稳定（1.25~1.28×），表明该方案具有良好的可扩展性。对于轻量模型（BERT-Tiny），由于Rotate-Sum的旋转次数减少（lb128 = 7与lb768 ≈ 10），单次LayerNorm时间略短。

表20　不同模型规模下的本文方案性能

模型	LN层数	单次LN耗时/s	总LN耗时/s	相对Goldschmidt (k=3)加速比
BERT-Tiny（H=128）	4	13.6	54.4	1.28×
BERT-Base（H=768）	24	14.8	355.2	1.26×
GPT-2单层（H=768）	2	14.9	29.8	1.25×

为验证范围守卫机制的鲁棒性，本文统计了各模型在推理过程中方差值落入安全区间的比例。表21显示了范围守卫覆盖率统计。

表21　范围守卫覆盖率统计

模型	总LayerNorm调用次数	$\sigma^2 \leqslant V_{\max}$比例	超出安全区间次数
BERT-Tiny	400	100%	0
BERT-Base	2 400	100%	0
GPT-2单层	200	100%	0

所有测试样本的方差均落在99.9%分位数确定的$V_{\max}$范围内，未出现超出安全区间的情况，验证了统计边界方法的有效性。表21中BERT-Base的2 400次LayerNorm调用均满足范围守卫约束，说明在本文实验分布下，范围守卫在多层、多样本调用中没有出现安全区间外输入。

4.2　范围守卫参数敏感性消融

为验证范围守卫默认参数选择的合理性，本文在BERT-Tiny模型上补充轻量参数敏感性实验。实验固定模型、数据集和多项式阶数不变，仅改变方差上界$V_{\max}$的校准分位数和安全边界η，统计不同配置下LayerNorm方差输入的覆盖率、软裁剪触发次数和端到端分类准确率参考值。实验使用SST-2验证集前100条样本，并统计Transformer block内部4个LayerNorm模块，共400次LayerNorm调用记录。需要说明的是，端到端分类准确率为明文范围限制模拟结果，即当某次LayerNorm的方差超过当前$V_{\max}$时，将归一化中使用的方差按$V_{\max}$进行上限截断。该列用于观察范围守卫参数变化对任务输出的影响趋势。

表22显示，当$V_{\max}$分位数由99.9%降至99.5%和99.0%时，覆盖率分别下降至99.75%和99.25%，并分别出现1次和3次软裁剪触发。这说明较低分

表22　　范围守卫参数敏感性消融结果

配置	V_{max}分位数	η	V_{max}	覆盖率	软裁剪触发次数	明文范围限制模拟准确率
较低分位数	99.0%	5%	14.021 4	99.25%	3	83.00%
中等分位数	99.5%	5%	14.793 2	99.75%	1	83.00%
无安全边界	99.9%	0	15.286 0	100.00%	0	83.00%
本文默认	99.9%	5%	15.286 0	100.00%	0	83.00%
更大安全边界	99.9%	10%	15.286 0	100.00%	0	83.00%

位数会增加分布尾部样本超界风险。对于固定的99.9%分位数，η=0、5%和10%均可实现100%覆盖和0次软裁剪触发，但η=0不保留额外安全边界，对校准误差和CKKS近似噪声更敏感。η=10%则使缩放更加保守，进一步压缩有效输入动态范围。相比之下，η=5%在保持100%覆盖率和0次软裁剪触发的同时，保留了适中的正弦单调区间安全余量。因此，本文采用V_{max}=99.9%分位数和η=5%作为默认配置，该选择不是单一配置下的偶然成功，而是在覆盖率、鲁棒性和零额外深度约束之间的折中。

5　结束语

本文提出了一种基于CKKS函数型Bootstrapping的融合式同态LayerNorm方案。该方案在EvalMod阶段将标准arcsin恢复多项式替换为倒数平方根复合多项式$P_{\mathrm{invsqrt}}(t)$，从而将$\dfrac{1}{\mathrm{sqrt}\,(\sigma^2+\epsilon)}$的计算融入Bootstrapping过程。通过稳定项、预缩放和统计边界构成默认范围守卫，本文使输入方差落在正弦函数单调区间内，并在不触发可选软裁剪的默认设置下实现倒数平方根计算的零额外乘法深度。实验结果表明，本文方案在保持与Goldschmidt方法相近精度的同时，可节省6层乘法深度，并降低LayerNorm运行时间和峰值内存开销。

本文仍存在进一步改进空间。首先，当前范围守卫依赖离线校准得到的V_{max}，未来可研究面向分布外输入的自适应范围守卫机制。其次，本文主要验证LayerNorm场景，后续可进一步扩展到RMSNorm及其他归一化函数。最后，本文实验以单密钥CKKS设置为主，未来可探索与多方FHE或MPC-FHE混合推理框架的结合。

参考文献：

[1] Gentry C. Fully homomorphic encryption using ideal lattices[C]//Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 169-178.

[2] Cheon J H, Kim A, Kim M, et al. Homomorphic encryption for arithmetic of approximate numbers[C]//Advances in Cryptology-ASIACRYPT 2017. Berlin: Springer, 2017: 409-437.

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

[4] Kupcova E, Pleva M, Khavan V, et al. A comparative study of partially, somewhat, and fully homomorphic encryption in modern cryptographic libraries[J]. Electronics, 2025, 14(23): 4753.

[5] 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.

[6] Vaswani A, Shazeer N, Parmar N, et al. Attention is all you need[C]//Advances in Neural Information Processing Systems(NeurIPS). Massachusetts: MIT Press, 2017: 5998-6008.

[7] Devlin J, Chang M W, Lee K, et al. BERT: pre-training of deep bidirectional transformers for language understanding[C]//Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers). Kerrville: Association for Computational Linguistics, 2019: 4171-4186.

[8] Brown T B, Mann B, Ryder N, et al. Language models are few-shot learners[C]//Proceedings of the 34th International Conference on Neural Information Processing Systems. New York: ACM Press, 2020: 1877-1901.

[9] Ba J L, Kiros J R, Hinton G E. Layer normalization[PP]. V1. (2016-07-21)[2026-05-11]. arXiv: arXiv.1607.06450.

[10] Niu J T, Wang J S, Liu X L, et al. Micro-suction and micro-blowing on channel flow: large eddy simulation of velocity normalization, root-mean-square velocity fluctuations, and Reynolds stress[J]. International Journal of Green Energy, 2025, 22(9/12): 1947-1964.

[11] Touvron H, Lavril T, Izacard G, et al. LLaMA: open and efficient foundation language models[PP]. V1. (2023-02-27) [2026-05-11]. arXiv:

arXiv.2302.13971.

[12] Cheon J H, Han K, Kim A, et al. Bootstrapping for approximate homomorphic encryption[C]//Advances in Cryptology-EUROCRYPT 2018. Berlin: Springer, 2018: 360-384.

[13] Bossuat J P, Mouchet C, Troncoso-Pastoriza J, et al. Efficient bootstrapping for approximate homomorphic encryption with non-sparse keys[C]//Advances in Cryptology-EUROCRYPT 2021. Berlin: Springer, 2021: 587-617.

[14] Goldschmidt R E. Applications of division by convergence[D]. Cambridge: Massachusetts Institute of Technology, 1964.

[15] Yang Z M, Niu C, Wei B Q, et al. RBOOT: accelerating homomorphic neural network inference by fusing ReLU within bootstrapping[J]. Cryptology ePrint Archive, 2025.

[16] Lee E, Lee J W, Lee J, et al. Low-complexity deep convolutional neural networks on fully homomorphic encryption using multiplexed parallel convolutions[J]. Cryptology ePrint Archive, 2022.

[17] Badawi A A, Bates J, Bergamaschi F, et al. OpenFHE: open-source fully homomorphic encryption library[C]//Proceedings of the 10th Workshop on Encrypted Computing & Applied Homomorphic Cryptography. New York: ACM Press, 2022: 53-63.

[18] Dowlin N, Gilad-Bachrach R, Laine K, et al. CryptoNets: applying neural networks to encrypted data with high throughput and accuracy[C]//Proceedings of the33rd International Conference on Machine Learning (ICML). 2016: 201-210.

[19] Lee J, Lee E, Lee J W, et al. Precise approximation of convolutional neural networks for homomorphically encrypted data[J]. IEEE Access, 2023, 11: 62062-62076.

[20] Drucker N, Moshkowich G, Pelleg T, et al. BLEACH: cleaning errors in discrete computations over CKKS[J]. Journal of Cryptology, 2024, 37: 3.

[21] Bae Y, Cheon J H, Kim J, et al. Bootstrapping bits with CKKS[C]//Advances in Cryptology-EUROCRYPT 2024. Berlin: Springer, 2024: 94-123.

[22] Bae Y, Kim J, Stehlé D, et al. Bootstrapping small integers with CKKS[C]//Advances in Cryptology-ASIACRYPT 2024. Berlin: Springer, 2024: 330-360.

[23] Alexandru A, Kim A, Polyakov Y. General functional bootstrapping using CKKS[C]//Advances in Cryptology-CRYPTO 2025. Berlin: Springer, 2025: 304-337.

[24] Kim J. Efficient homomorphic integer computer from CKKS[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025(4): 873-898.

[25] Boneh D, Kim J. Homomorphic encryption for large integers from nested residue number systems[C]//Advances in Cryptology-CRYPTO 2025. Berlin: Springer, 2025: 338-370.

[26] Bossuat J P, Cammarota R, Chillotti I, et al. Security guidelines for implementing homomorphic encryption[J]. IACR Communications in Cryptology, 2025, 1(4): 1-40.

[作者简介]



陈智罡（1972– ），男，博士，宁波财经学院教授，主要研究方向为全同态加密与格密码。



宋新霞（1973– ），女，浙江万里学院教授，主要研究方向为代数与编码。



Liqun Chen（1956– ），女，博士，英国萨里大学教授，主要研究方向为应用密码学。