周报

2026-02-10

本周研究摘要

完成硕士学位论文第五章面向 GPU 的 AES 算法线程自适应并行优化实现撰写

对第四篇小论文中 ML-DSA 的格密码学基础进行系统梳理与图解

第五章：AES 线程自适应并行优化

提出自适应线程分配（ATA）策略与函数级并行化（FLP）方法

- 性能模型：$T(g_i, t) = \alpha_i + \beta_i/t + \gamma_i \cdot t$，最优线程$t_i^* = \sqrt{\beta_i/\gamma_i}$
- AES 核心操作分解为 SubBytes、ShiftRows/MixColumns、AddRoundKey 三类细粒度任务
- NVIDIA RTX 4090 上 AES-128-CTR 达 1842 Gb/s，AES-128-ECB 达 1596 Gb/s

ML-DSA 格密码学基础：格的基本概念

格是由m个线性无关向量的整数线性组合构成的离散点集$\mathcal{L}(B) = \{Bz : z \in \mathbb{Z}^m\}$，密码学利用“好基”与“坏基”之间的计算不对称性构建安全方案。

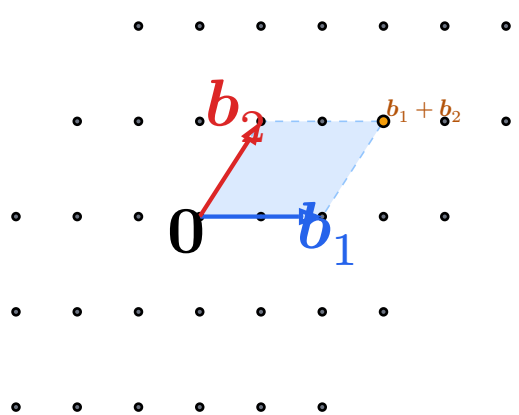

Figure 1: 二维格及其基本平行四边形。

好基与坏基对比

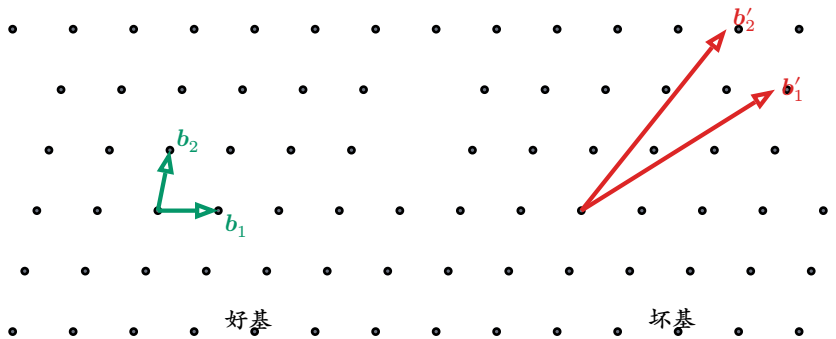

Figure 2: 同一格的好基（左）与坏基（右）。

格上核心困难问题

SVP 要求找到格中最短非零向量，CVP 要求找到距目标点最近的格点，SIS 要求找到满足$\boldsymbol{A}\boldsymbol{x} = \boldsymbol{0} \bmod q$且$\|\boldsymbol{x}\|_\infty \leq \beta$的短向量。ML-DSA 的安全性建立在这三个问题之上。

SVP：最短向量问题

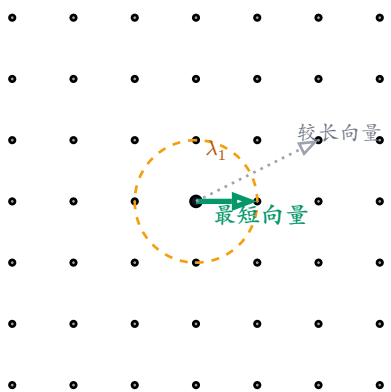

Figure 3: SVP：虚线圆半径λ_1内无非零格点。

CVP：最近向量问题

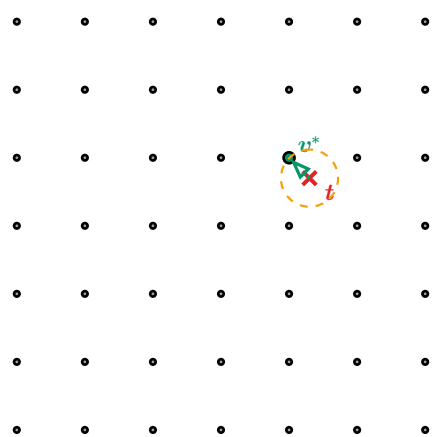

Figure 4: CVP：找到距目标t最近的格点v^*。

SIS：短整数解问题

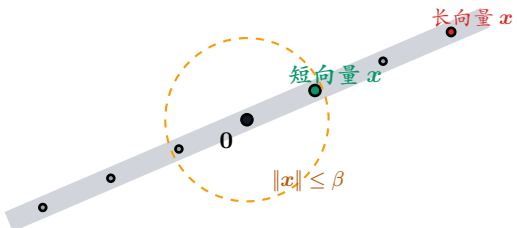

Figure 5: SIS：解空间中仅少数格点为短向量。

ML-DSA 签名方案三阶段流程

ML-DSA 基于 Fiat-Shamir with Aborts 范式，包含密钥生成、签名和验证三个阶段。密钥生成从种子ξ派生$\boldsymbol{A}$和短秘密$\boldsymbol{s}_1, \boldsymbol{s}_2$，签名采用拒绝采样确保$\boldsymbol{z}$分布与$\boldsymbol{s}_1$无关。

ML-DSA 三阶段流程图

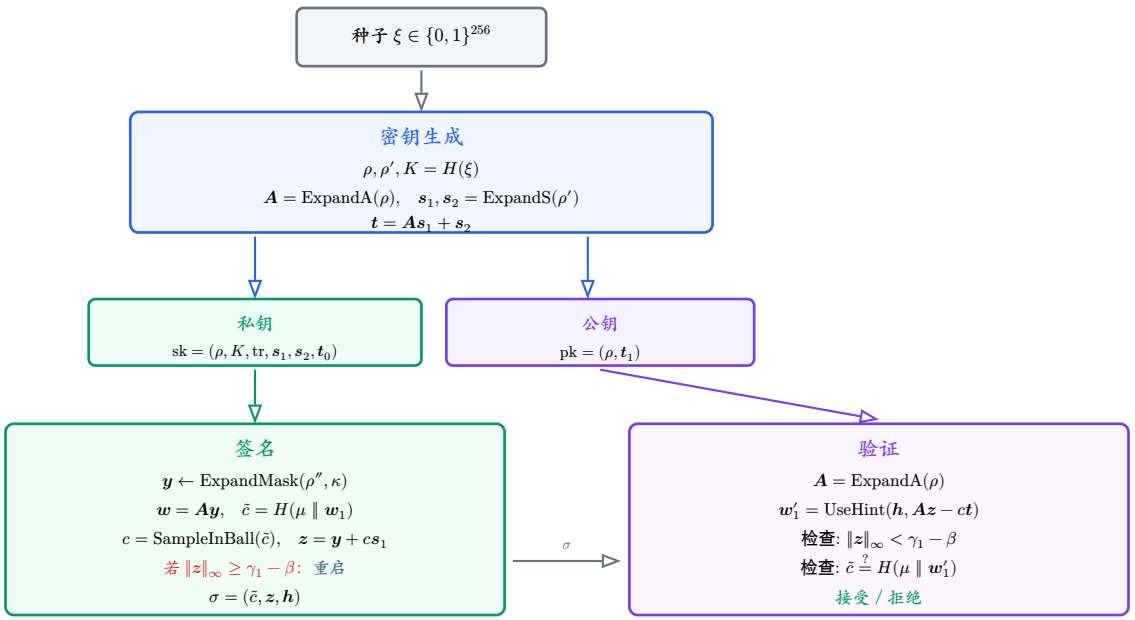

Figure 6: ML-DSA 三阶段流程概览。

签名几何：拒绝采样

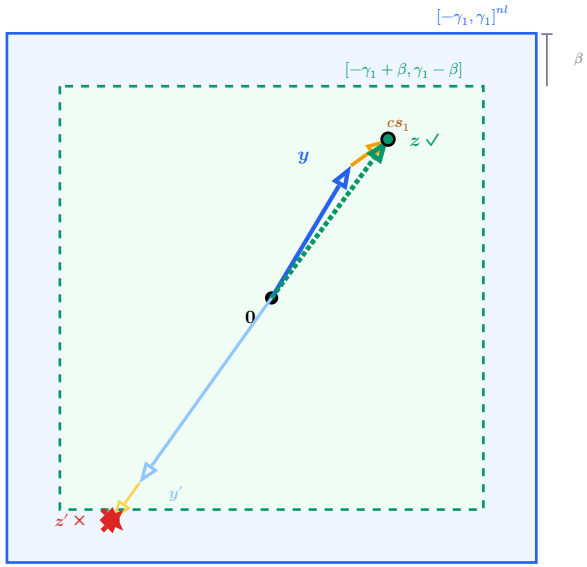

Figure 7: 签名几何：$\boldsymbol{z} = \boldsymbol{y} + c\boldsymbol{s}_1$须落在接受区域内。

验证

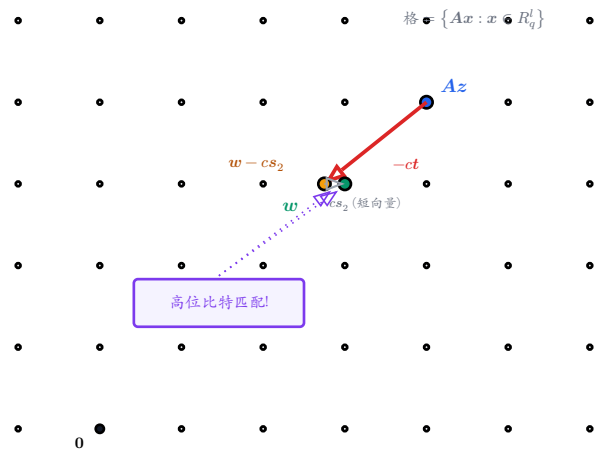

Figure 8: 验证：$\boldsymbol{Az - ct = w - cs_2}$，短向量$\boldsymbol{cs_2}$保证高位匹配。

总结

下周计划

- 找可优化的算子
- 完成硕士学位论文的撰写工作

老师评语

我不理解这第 4 篇小论文从 29 页到现在的 5 页了？中间出现重大错误推倒重来了？

旧的创新点没有理论分析，只能发三四区。目前计划优化模格中的算子，提升论文层次。