周报 向嘉豪(2026-02-09)

摘要: 本周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的撰写工作，提出了自适应线程分配（ATA）和函数级并行化（FLP）策略，在 NVIDIA RTX 4090 上实现 AES-128-CTR 模式 1842 Gb/s 的加密吞吐量。同时对第四篇小论文中 ML-DSA 的格密码学基础进行系统梳理，完成了格几何、短向量问题（SVP）、最近向量问题（CVP）、短整数解问题（SIS）以及 ML-DSA 签名方案三阶段流程的图解。

下周计划: 1) 继续修改第四篇小论文 2) 完成硕士学位论文的撰写工作

1 硕士学位论文撰写

1.1 第五章面向 GPU 的 AES 算法线程自适应并行优化实现

完成了第五章面向 GPU 的 AES 算法线程自适应并行优化实现的撰写工作，该章节包括 AES 算法与 GPU 计算模型、线程自适应 GPU 优化方法、GPU 实现结果与吞吐量评估三个主要部分。本章提出了自适应线程分配（ATA）策略，通过建立执行时间性能模型$T(g_i, t) = \alpha_i + \beta_i/t + \gamma_i \cdot t$，针对 AES 不同操作动态确定最优线程配置$t_i^* = \sqrt{\beta_i/\gamma_i}$，并结合函数级并行化（FLP）方法将 AES 核心操作（SubBytes、ShiftRows/MixColumns、AddRoundKey）分解为可并发执行的细粒度计算任务。

性能评估部分在 NVIDIA RTX 4090 GPU 上进行测试，AES-128-CTR 模式达到 1842 Gb/s（230.3 GB/s）的吞吐量，AES-128-ECB 模式达到 1596 Gb/s（199.5 GB/s）。延迟分解分析表明 SubBytes 操作占总执行时间的 68.7%，ShiftRows/MixColumns 贡献 23.8%，AddRoundKey 仅占 7.5%。AES-256 相比 AES-128 的性能下降约 16 – 17%，主要原因是轮数增加（14 轮 vs 10 轮）和密钥扩展的额外计算开销。

2 第四篇小论文——ML-DSA 格密码学基础梳理

本周对第四篇小论文中 ML-DSA 的格密码学理论基础进行系统梳理与可视化图解，涵盖格基础概念、核心困难问题与 ML-DSA 方案流程。

2.1 格的基本概念与基变换

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$\mathcal{L}(B) = \{Bz : z \in \mathbb{Z}^m\}$。同一格可由不同基描述，密码学利用“好基”（短且近正交）与“坏基”（长且倾斜）之间的计算不对称性构建安全方案。

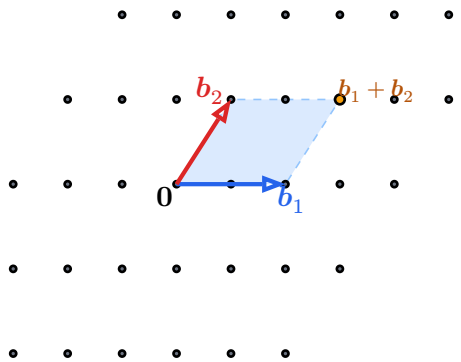

图 1　二维格及其基本平行四边形。

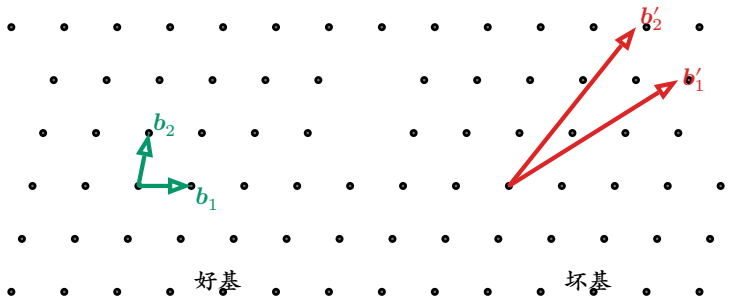

图 2　同一格的好基（左）与坏基（右）。

2.2 格上核心困难问题

格密码学的安全性建立在三个核心困难问题之上。SVP 要求找到格中最短非零向量，在高维下具有指数级复杂度且无已知量子加速。CVP 要求找到距目标点最近的格点，ML-DSA 签名本质上是有界距离解码问题。SIS 要求找到满足$\boldsymbol{A}\boldsymbol{x} = \boldsymbol{0} \bmod q$且$\|\boldsymbol{x}\|_\infty \le \beta$的短向量，ML-DSA 验证依赖于该问题的困难性。

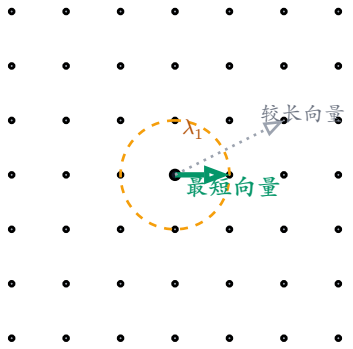

图 3　SVP：虚线圆半径λ_1内无非零格点。

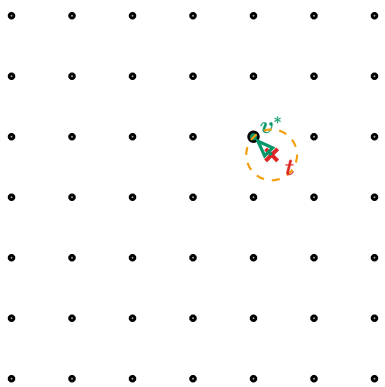

图 4　CVP：找到距目标$\boldsymbol{t}$最近的格点$\boldsymbol{v}^*$。

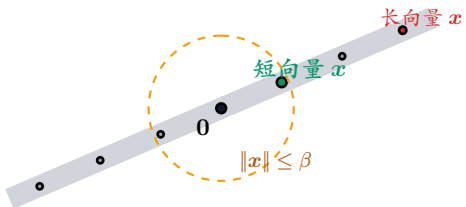

图 5　SIS：解空间中仅少数格点为短向量。

2.3 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$\boldsymbol{s}_1, \boldsymbol{s}_2$，计算$\boldsymbol{t} = \boldsymbol{A}\boldsymbol{s}_1 + \boldsymbol{s}_2$并分割为公钥$\boldsymbol{t}_1$和私钥$\boldsymbol{t}_0$，安全性基于 Module-LWE 困难性。

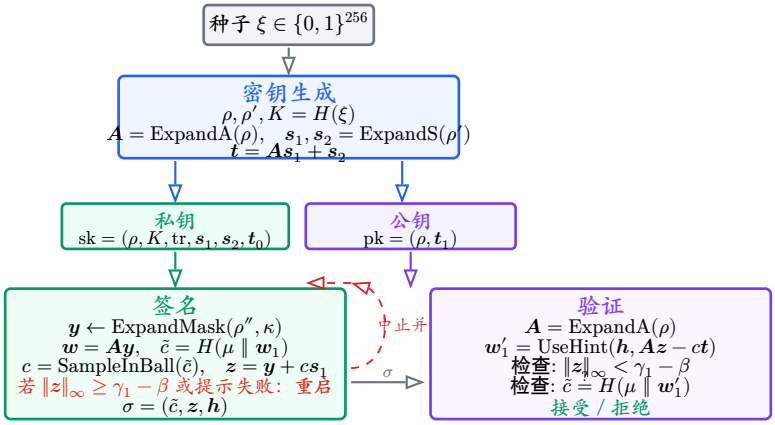

图 6　ML-DSA 三阶段流程概览。

签名阶段采用拒绝采样：选取掩码$\boldsymbol{y}$，计算$\boldsymbol{z} = \boldsymbol{y} + c\boldsymbol{s}_1$，若$\|\boldsymbol{z}\|_\infty \geq \gamma_1 - \beta$则重启，确保$\boldsymbol{z}$分布与$\boldsymbol{s}_1$无关。

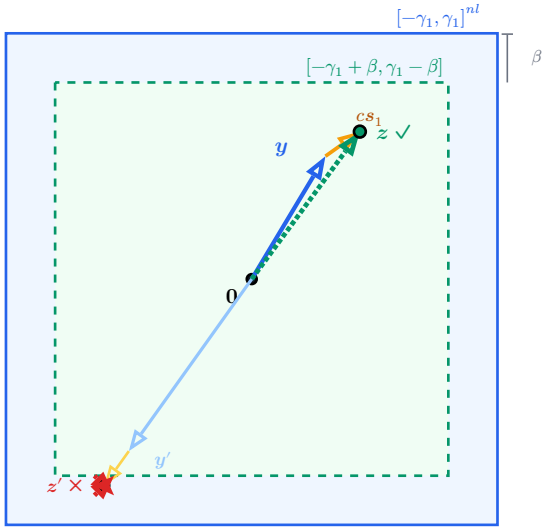

图 7　签名几何：$\boldsymbol{z} = \boldsymbol{y} + c\boldsymbol{s}_1$须落在接受区域内。

验证阶段利用$\boldsymbol{A}\boldsymbol{z} - c\boldsymbol{t} = \boldsymbol{w} - c\boldsymbol{s}_2$重构$\boldsymbol{w}'_1$，由于$c\boldsymbol{s}_2$为短向量，高位比特匹配$\boldsymbol{w}_1$，提示$\boldsymbol{h}$修正舍入误差后验证哈希一致性。

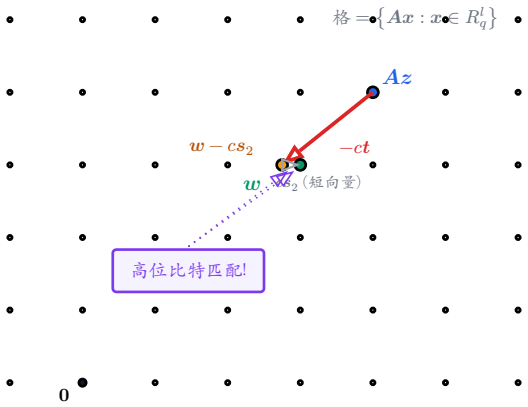

图 8　验证代数：$\boldsymbol{A}\boldsymbol{z} - c\boldsymbol{t} = \boldsymbol{w} - c\boldsymbol{s}_2$，短向量$c\boldsymbol{s}_2$保证高位匹配。