AKCN-KEM 参数选取和算法特色补充说明

AKCN-KEM 团队

我们 AKCN-KEM 是一个模块化和一般化的算法结构，其既可以用 LWE 进行实例化（此时在 Frodo-KEM 相同的安全评测标准的基础上综合性能实质优于 NIST 第二轮的 Frodo-KEM），也可以用 MLWE 进行实例化。在第 5 章中，我们分别指定了 AKCN-LWE 的参数和 AKCN-MLWE 的参数。这体现了 AKCN-KEM 在模块化、灵活性、和兼容性上的算法的特色。

如果对 AKCN-KEM 仅仅指定一组唯一的参数，在从实现效率角度，我们指定如下 AKCN-MLWE 的参数（其在算法文档第 5 章已经给出）。

困难问题：	MLWE
（1）秘密向量维度 n	秘密为 $(\mathbf{x},\mathbf{e}) \in \mathcal{R}^3 \times \mathcal{R}^3$ 。 当把 $\mathbf{x},\mathbf{e}$ 理解为 $\mathcal{R}^3$ 中的元素时，维度为 3； 当把 $\mathbf{x},\mathbf{e}$ 理解为 $\mathbb{Z}[\zeta_{512}]^3$ 中的元素时，维度为 256*3=768；
（2）模数 q	7681
（3）秘密分布	当把 $\mathbf{x},\mathbf{e}$ 理解为 $\mathcal{R}^3$ 中的元素时， $\mathbf{x},\mathbf{e}$ 在幂基中的每个系数均服从中心二项分布。
（4）分布标准差 sd	1
（5）声称的经典安全强度	163
（6）声称的量子安全强度	148