关于木兰签名参数选取和算法特色的进一步说明

木兰签名算法团队

令 t=As+e，其中 s 取自[-η, … , η]的中心二项分布，e 取自[-η', … , η']的中心二项分布。在木兰第一轮的算法说明中，我们取的是 q=4191233，$(\eta, \eta') =$ （3,2)。在木兰第二轮的算法说明中，通过测试更多的参数，我们取的是 q=1952257，$\eta = \eta' = 2$，即标准的（对称版本的）LWE。这主要是因为这组参数可以在安全性和性能上取得更好的表现，并从利于和 NIST 第二轮的 Dilithium 签名算法兼容适配以及便于比较的角度来设置。

我们最近也测试了针对 q=1952257 的非对称参数，下表是$(\eta, \eta') =$ （1,4)的非对称参数及性能。简要地说，在保持木兰第二轮指定的对称参数的性能数据的前提下，非对称参数可以进一步实质降低签名循环次数（从而进一步提升签名效率），并进一步减少私钥尺寸。我们未来也计划实现这组参数。

我们提供这组非对称参数主要是用来进一步说明木兰签名在参数选取灵活性、签名性能进一步提升空间等方面的算法特色。

	木兰-非对称参数	木兰-对称参数（第二轮提交）	Dilithium
q	1952257	1952257	8380417
n	256	256	256
(h, ℓ)	（5,4）	(5,4)	(5,4)
(η, η')	(4,1)	（2,2）	（5,5）
公钥长度（字节）	1312	1312	1472
私钥长度（字节）	3024	3056	3504
签名长度（字节）	2573	2573	2701
重复次数	4.9	5.67	6.6
抗密钥恢复攻击的量子比特开销	128	128	128
抗伪造签名的量子比特开销	131	131	125