关于 AKCN-E8 参数选取、错误率分析、算法特色的进一步说明

AKCN-E8-KEM 团队

2019 年 10 月 31 日

一、 AKCN-E8-3329 参数

我们第二轮提交的 AKCN-E8 文档，给的的参数为了便于和 NIST 第二轮的 NewHope 兼容和比较，采用了和 NewHope 相同的 q=12289。我们注意到，使用[1,2]发展的 preprocess-then-NTT 技术，我们可以也可以采用 q=3329。下表是我们给出的 AKCN-E8-3329 参数，未来我们给予实现。使用这种技术，AKCN-E8 的带宽可以进一步实质降低。

	$\lvert K\rvert$	n	q	η	g	t	c-sec	pq-sec	err	pk (B)	cipher (B)
NewHope-1024-CPA	256	1024	12289	8	2^3	0	257	233	2^{-216}	1824	2176
AKCN-E8-3329-1024-E-CPA	512	1024	3329	2	2^4	2	254	230	2^{-303}	1568	1792
AKCN-E8-3329-1024-C-CPA	512	1024	3329	2	2^3	2	254	230	2^{-178}	1568	1664
NewHope-1024-CCA	256	1024	12289	8	2^3	0	257	233	2^{-216}	1824	2208
AKCN-E8-3329-1024-E-CCA	512	1024	3329	2	2^4	2	254	230	2^{-303}	1568	1824
AKCN-E8-3329-1024-C-CCA	512	1024	3329	2	2^3	2	254	230	2^{-178}	1568	1696

当然，NewHope 也可以采用同样的技术和 q=3329。但是由于我们 E8 编码相对于 D4 编码在纠错能力上的优越性。在 q=3329 时，AKCN-E8 仍可以在共享密钥长度、安全性、错误率、和带宽上全面超越 NewHope。

这进一步突出了 AKCN-E8 由于底层 E8 格编码创新和（相对于格编码技术路线而言）几乎最优的纠错能力，导致的 AKCN-E8 在参数选取方面的灵活性，以及在共享密钥长度、安全性、错误率和带宽方面更优的表现。

二、 关于指定参数和算法实现

如果从和 NewHope 兼容并具有相同安全性的角度考虑，我们在文档第 18 页表格中指定的是 AKCN-E8-1024-E，其中 eta=8,标准差为$\sqrt{4}$（文档第 18 页表格中的$\sqrt{8}$为笔误）。这组参数满足算法竞赛第二轮的要求。

在我们算法文档的第 20 页，第 5.2.1 节，我们明确指出了我们实现的参数是：AKCN-E8-1024-C，其中 eta=4。因此我们文档描述和算法实现代码是一致和对应的。如果强制指定参数和实现参数一致，则我们采用 AKCN-E8-1024-C。未来版本我们也计划实现上述的 AKCN-E8-3329。

三、 关于错误率分析脚本

在我们文档第 18 页，第 4.1 节，我们分析了 AKCN-E8 的错误率，并在 4.1 节的最后明确指出了错误率分析脚本可以在 http://github.com/AKCN-E8 获得。

参考文献：

1. Y. Zhu, Y. Pan and Z. Liu. When NTT Meets Karatsuba: Preprocess-then-NTT Technique Revisited. https://eprint.iacr.org/2019/1079
2. S. Zhou, H. Xue, D. Zhang, K. Wang, X. Lu, B. Li, and J. He. Preprocess-then-NTT Technique and Its Applications to Kyber and Newhope. Inscrypt 2018: 117-137.