From: 쫍킌쩸 <ylzhao@fudan.edu.cn>
To: pqc-comments <pqc-comments@nist.gov>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: ROUND 3 OFFICIAL COMMENT: NTRU
Date: Thursday, May 12, 2022 05:35:00 AM ET
Attachments: CTRU-comparisons.jpg

Dear NTRU team and dear all in PQC community:

Recently, we proposed compact NTRU-based KEM with scalable ciphertext compression, referred to CTRU. The paper is available from: https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Farxiv.org%2Fabs%2F2205.05413&data=05%7C01%7Candrew.regenscheid%40nist.gov%7C15476a69f917489eeba008da33faac3f%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637879449004480090%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000%7C%7C%7C&sdata=vljhJtrv%2Fd5rCspD5ikFCkoV0%2Be2jeRdLTSg%2FOxH%2Bww%3D&reserved=0

CTRU has very concise ciphertext size, and to our knowledge it is the first NTRU-based KEM with a single polynomial ciphertext compression. Another interesting point is that it combines NTRU and RLWE, and in turn unifies RLWE and RLWR within the same scheme structure. Specifically, we also proposed compact NTRU based on RLWR, referred to CNTR that is just a simplified version of CTRU. The technique used in this work can also be applied to other NTRU variants. CTRU has remarkable performance, which is summarized in the attached table with details referred to the paper.

Any feedbacks and suggestions are appreciated from you.

All the best
Yunlei