From: 赵运磊 <ylzhao@fudan.edu.cn> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-comments <pqc-comments@nist.gov>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] ROUND 3 OFFICIAL COMMENT: SABER
Date: Thursday, May 12, 2022 05:42:04 AM ET
Attachments: CNTR-Saber.JPG

Dear Saber team and dear all in PQC community:

Recently, we proposed compact NTRU based on RLWR, referred to CNTR. 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%7C0b31b0d07e45468be1ba08da33fbab6c%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637879453246096650%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C2000%7C%7C%7C&sdata=3xZLKzL3S63II5aqA%2BjzNfM%2FgF5QN10mm33fgMV5%2FB4%3D&reserved=0

To our knowledge, CNTR has almost the smallest ciphertext size. Compared with Saber, it has smaller ciphertext size, stronger security, and lower error probabilities. By combining NTRU and RLWR, it could eliminate most of the existing patent threats. In addition, CNTR has flexible plaintext message space that is ${0,1}^{n/2}$ where n is the polynomial dimension, compared to the fixed message size of 256 bits of Saber. The comparison between CNTR and Saber is summarized in the attached table.

Any feedbacks and suggestions are appreciated from you.

All the best
Yunlei