From: 쬽킌쩸 <ylzhao@fudan.edu.cn>
To: pqc-comments <pqc-comments@nist.gov>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: ROUND 3 OFFICIAL COMMENT: CRYSTALS-KYBER
Date: Thursday, May 12, 2022 06:19:11 AM ET

Dear Kyber team and dear all in PQC community:

Recently, we made a systematic optimization of the Kyber algorithm, and proposed an optimized version referred to as OSKR.

We note that with the AKCN mechanism proposed in the KCL proposal (in the first round submissions of NIST-PQC), on the same parameters, OSKR has more efficient decryption process and has lower error probability simultaneously.

We study how to encapsulate 512-bit key with OSKR-1024. By proposing a hybrid-NTT (HNTT) technique, OSKR-1024 not only encapsulates 512-bit key, but its implementation can be more efficient than Kyber-1024. Also thanks to the HNTT technique, all the three parameter sets can be implemented in modular and unified way.

The paper is available from: https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Farxiv.org%2Fabs%2F2109.02893&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cc3f816dfa6e6449b4fc708da3400d8a1%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637879475512717344%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C2000%7C%7C%7C&sdata=P37yizXD10SXggXmKfeLH9GdF3doVY%2FwBgkOXjGoNXo%3D&reserved=0

All my best
Yunlei