

From: [Liu, Yi-Kai \(Fed\)](#)
To: [Moody, Dustin \(Fed\)](#)
Subject: Re: LAC
Date: Thursday, June 11, 2020 2:16:44 PM

Will do. Sorry, these few weeks are pretty crazy on my end. I'll try to say more about LAC, but it is a little tricky, because the worst attacks on LAC happened in round 1, and were arguably fixed in round 2. The attacks in round 2 seemed relatively minor. I think the attacks in round 1 just left a bad taste in everyone's mouths, and since we had lots of lattice KEMs, we didn't feel any need to keep LAC in the competition. I'll try to find a nicer way to say this.

--Yi-Kai

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Thursday, June 11, 2020 10:29 AM
To: Liu, Yi-Kai (Fed)
Subject: LAC

Yi-Kai,

Would you be able to expand on your write-up for LAC? If you check the report, you'll see it is noticeably shorter than most of the other ones. Thanks,

Dustin