From: noreply-spamdigest@google.com via pqc-forum <pqc-forum@list.nist.gov>
To: Spam moderators <pqc-forum+managers@list.nist.gov>
Subject: [pqc-forum] Moderator's spam report for pqc-forum@list.nist.gov
Date: Friday, August 12, 2022 08:25:26 AM ET

This message is being sent to you because you are a moderator of the group pqc-forum.

The following suspicious messages were sent to your group, but are being held in your moderation queue because they are classified as likely spam messages.

If you take no action, all the messages below will be discarded automatically as spam.

However, if you see any messages that are not spam below, you may approve them individually by going to:

https://groups.google.com/a/list.nist.gov/group/pqc-forum/pendmsg

Please do not mark this notification as spam; this is a service for group moderators. If you do not wish to receive these notifications in the future, you may change your preferences by going to:

https://groups.google.com/a/list.nist.gov/group/pqc-forum/manage_post

————— 1 of 1 —————
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
From: Mike Hamburg <mike@shiftleft.org>
Date: Aug 11 12:56PM +0200

Hi all,

> Uri Blumenthal wrote
> >I think NIST standards are orthogonal to use of hybrids, and it won't make any
sense for NIST to require them. NIST standardizes KEMs. You want to combine/
concatenate several of the standardized KEMs, and maybe

Approve: https://groups.google.com/a/list.nist.gov/group/pqc-forum/pendmsg?
view=full&pending_id=3430660943006643841

For more information about this message, please visit:
https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Fsupport.google.com%2Fgroups%2Fanswer%2F2466386&data=05%7C01%7Cd
ustin.moody%40nist.gov%7C4658b13328554dd6cc7e08da7c5dbba3%7C2ab5d82fd8fa4797a93e05465
5c61dec%7C1%7C0%7C637959039262097625%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQ
IjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=73BmguzWfqg%2Fr7
Vl8biAjhxcKr59V12CFDOdks3GPho%3D&reserved=0