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, December 16, 2022 07:24:41 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] Implicit Rejection in Kyber
From: Mike Hamburg <mike@shiftleft.org>
Date: Dec 16 12:40PM +0100

Hi Tobias,

Part of the point of implicit rejection is that it enables security proof techniques which are
otherwise unavailable in the quantum random oracle model. I'm not up-to-date on the latest
security proofs of Kyber's Fujisaki-Okamoto

Approve: https://groups.google.com/a/list.nist.gov/group/pqc-forum/pendmsg?view=full&pending_id=5990809766612098411

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%7Cdustin.moody%40nist.gov%7Cc1ea6fab6da9492ce55808dadf6080d2%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C638067902816184080%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=flS%2FQjHzZqmPLrhbfuq0WhmfF24FXAP6wMd2zN0SQdY%3D&reserved=0