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, June 17, 2022 08:24:48 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] HertzBleed : power side channel attacks on SIKE
From: Taylor R Campbell <campbell+nist-pqc-forum@mumble.net>
Date: Jun 17 10:11AM

> prone to abuse (NISTPQC should be protected against being manipulated
> through choices of demos). How is this different from penalizing SIKE
> for HertzBleed?

This misfeature isn't merely hypothetical -- on Intel SGX, four

Approve: https://groups.google.com/a/list.nist.gov/group/pqc-forum/pendmsg?view=full&pending_id=1294068937321290090

For more information about this message, please visit:

https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsupport.google.com%2Fgroups%2Fanswer%2F2466386&amp;data=05%7C01%7Cdustin.moody%40nist.gov%7C6a0227cf1c674d7b57e908da505c5d6e%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637910654884202759%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&amp;sdata=hFMhFe4gNgjUbldQ7tYUMU0ulG4NWbnB0q4e%2Bj8OFNo%3D&amp;reserved=0