
From: Moody, Dustin (Fed)
Sent: Tuesday, June 23, 2020 2:30 PM
To: Kerman, Sara J. (Fed)
Subject: Fw: [pqc-forum] Rainbow parameter update

Sara,

The rainbow team would like this to be an official comment on Rainbow. Thanks!

Dustin

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of Jintai Ding <jintai.ding@gmail.com>
Sent: Monday, June 22, 2020 4:31 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Rainbow parameter update

Due to recent progress in security analysis, we would like to propose some minor modifications on the Rainbow signature parameters.

Details can be found in the link below:

<https://sites.google.com/site/jintaiding/nist-papers>

Rainbow Team

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.

To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visit <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/4b739dea-439f-45f5-ad89-f6d6c7c1f2f6o%40list.nist.gov>.