

From: [Senseney, Justin S. \(Fed\)](#)
To: [Kerman, Sara J. \(Fed\)](#); [Moody, Dustin \(Fed\)](#)
Cc: [Mohamoud, Zak \(Fed\)](#)
Subject: Re: Help with pqc-forum Google Group Mail List
Date: Tuesday, November 7, 2017 4:34:18 PM

Thanks, I'm seeing those messages in the archives. There is a message within Septmeber that is incompatible with Google Groups, and it's causing my program to jump over all of the September messages. While I'm fixing that, you can continue to use the new list, it's easy for me to push in old messages even when newer ones are being created.

-Justin

From: "Kerman, Sara J. (Fed)" <sara.kerman@nist.gov>
Date: Tuesday, November 7, 2017 at 4:00 PM
To: "Senseney, Justin S. (Fed)" <justin.senseney@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Cc: "Mohamoud, Zak (Fed)" <abdirizak.mohamoud@nist.gov>
Subject: RE: Help with pqc-forum Google Group Mail List

Hi Justin,

I think there are a lot missing. The ones below were sent between September 6-October 15. I did a "search for messages" (in archive) for the "subject" words and these didn't show up (which is the biggest gap, date-wise, in the archive).

- Large Submission Files
- Proposal Format
- Reminder and minor bug fixes updated
- List of announced submissions
- Pqskeleton (multiple topics—different dates included in subject)
- Statements and Disclosures
- Random Bytes
- Website link to the NIST PQC page
- API issues; also website down
- The API is final. No more changes
- KAT values for reference and optimized implementations
- KAT, rng.c, rng.h and others
- Additional Implementations
- KAT Call File Explainer
- Structure
- Will a proposal be abandoned if its author cannot attend conferences?
- KAT scripts
- Security categories
- Ask about the instruction set supported by the Intel platform

- Regarding Sept 30 deadline
- Updated API *(included on list with 10 posts, but it had 15 included original message)*

From: Senseney, Justin S. (Fed)
Sent: Tuesday, November 07, 2017 3:43 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Cc: Mohamoud, Zak (Fed) <abdirizak.mohamoud@nist.gov>
Subject: Re: Help with pqc-forum Google Group Mail List

I just did the transfer again, can you let me know if you see a specific message missing? I'm still seeing 55 topics + the 1 you posted today.

-Justin

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Tuesday, November 7, 2017 at 3:33 PM
To: "Senseney, Justin S. (Fed)" <justin.senseney@nist.gov>, "Kerman, Sara J. (Fed)" <sara.kerman@nist.gov>
Cc: "Mohamoud, Zak (Fed)" <abdirizak.mohamoud@nist.gov>
Subject: RE: Help with pqc-forum Google Group Mail List

Justin,

Today I'm sending a message to all our mailing list members updating them on the changes. Can you try re-uploading all the messages so that none will be missing? It still seemed to me that the last time you did there were some missing. Thanks,

Dustin

From: Senseney, Justin S. (Fed)
Sent: Monday, November 06, 2017 2:18 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Mohamoud, Zak (Fed) <abdirizak.mohamoud@nist.gov>
Subject: Re: Help with pqc-forum Google Group Mail List

You're right, some email did not upload from September. I re-uploaded it, and everything should be there now.

-Justin

From: "Kerman, Sara J. (Fed)" <sara.kerman@nist.gov>
Date: Monday, November 6, 2017 at 1:25 PM
To: "Senseney, Justin S. (Fed)" <justin.senseney@nist.gov>
Cc: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Mohamoud, Zak (Fed)" <abdirizak.mohamoud@nist.gov>
Subject: RE: Help with pqc-forum Google Group Mail List

Justin,
Thanks for your help with the website verbiage. I really appreciate that!

I guess I did get a NIST Google account because I was able to access the archives. ☺ It still appears that a lot of the discussion between Sept 6 and Oct 14 is missing. I've tried searching on some of the subjects and it's not finding those messages in the google archive. Thoughts?

Again, thank you for all your help with this.
-Sara

From: Senseney, Justin S. (Fed)
Sent: Monday, November 06, 2017 12:37 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Mohamoud, Zak (Fed) <abdirizak.mohamoud@nist.gov>
Subject: Re: Help with pqc-forum Google Group Mail List

Sara, I pushed the rest of the archives, and edited the attached document to clarify how to subscribe, unsubscribe, and view archives.

-Justin

From: "Kerman, Sara J. (Fed)" <sara.kerman@nist.gov>
Date: Monday, November 6, 2017 at 11:16 AM
To: "Senseney, Justin S. (Fed)" <justin.senseney@nist.gov>
Cc: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Subject: Help with pqc-forum Google Group Mail List

Hi Justin,
I still don't have a google account tied to my NIST account so I'm having a little trouble helping out with the recently migrated pqc-forum mailing list. We need to update our website to include new subscription instructions and information regarding the archive (see attached with questions).

Also, I've been told that the last (most recent) message showing in the archive is dated September 6; however, there has been a lot of discussion on the list over the last two months. Do you know what would cause this? The list was activated October 5 if that helps. Thanks for any guidance you can provide,

Sara J. Kerman

NIST

301-975-4634

sara@nist.gov