From:	Alperin-Sheriff, Jacob (Fed)
To:	Apon, Daniel C. (Fed); Moody, Dustin (Fed); Perlner, Ray A. (Fed)
Subject:	Re: [Ext] [pqc-forum] Re: 2 rounds? 3 rounds?
Date:	Monday, August 26, 2019 1:48:28 PM

We should legit give this comment an award

From: "'daniel.apon' via pqc-forum" <pqc-forum@list.nist.gov>
Reply-To: "Apon, Daniel C. (Fed)" <daniel.apon@nist.gov>
Date: Sunday, August 25, 2019 at 5:23 AM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Re: 2 rounds? 3 rounds?

Vadim wrote:

"...another reason for moving slowly is that this NIST standardization process spurred a lot of new Ph.D. students to come into the area. It would be good, then, to wait and see what novel cryptanalysis (or improvements to the schemes) this new generation can produce."

I hereby vote for this as a candidate for the most wholesome comment on this mailing list. :-)

--Daniel

--
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/ffb54212-08c1-4998-b2b5-c21b5036cf3f%40list.nist.gov.