

From: [Moody, Dustin \(Fed\)](#)
To: (b) (6) [internal-pqc](#)
Subject: Re: [pqc-forum] A few (minor) corrections
Date: Friday, December 22, 2017 9:48:56 AM

I don't know that we want to provide a comment on every paper/posting/etc that breaks something/does something else. That gets to be a lot of acknowledging, and then we have to judge whether the paper is correct or not, which others might not agree with us.

We do want to generally thank people for all the work and analysis that they have done/will do.

Dustin

From: Jacob Alperin-Sheriff (b) (6)
Sent: Friday, December 22, 2017 7:58:36 AM
To: Moody, Dustin (Fed); internal-pqc
Subject: Re: [pqc-forum] A few (minor) corrections

Are we acknowledging and thanking people for doing the brute work in actually breaking things (especially things that we felt were broken but posted anyway because submitters disputed?) We probably should.

On Dec 22, 2017 7:50 AM, "Jacob Alperin-Sheriff" (b) (6) wrote:
Oops (I'm out today since we gotta be in NJ by sunset and not worth coming in for 2-3 hours).

On Dec 22, 2017 7:39 AM, "Moody, Dustin (Fed)" <dustin.moody@nist.gov> wrote:
Everyone,
We have been notified of several mistakes, mostly dealing with typos on our page listing the submissions accepted for the first round. These will be corrected, although we ask for a little bit of patience as it is the holiday season here.

Of a bit more importance, it seems we did not post the latest version of the specification for two schemes: Lotus and Titanium. I have attached the correct versions, although I'm not sure how the Mailing List will handle these attachments. The correct version of the Titanium submission is also available via their website:

<http://users.monash.edu.au/~rste/Titanium.html>

The correct versions will be updated soon on our webpage, although again, I ask for a bit of patience. We apologize for these mistakes.

Dustin Moody

--

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.

Visit this group at <https://groups.google.com/a/list.nist.gov/group/pqc-forum/>.