From: Moody, Dustin (Fed)
To: Dang, Quynh H. (Fed)
Subject: RE: 1st Round Report
Date: Monday, December 10, 2018 3:17:02 PM

Thanks. I've made the changes

From: Dang, Quynh (Fed)
Sent: Monday, December 10, 2018 2:46 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: 1st Round Report

Hi Dustin,

See my proposed changes in the NTRU and NTRU Prime sections.

One more thing: you skipped the sentence about security property of being a large Galois group. It seems to me that Mike Hamburg kinda implicitly agreed that being a large Galois group might have security benefit.

If an attack is based on the Galois group (all of the automorphisms), a large Galois group would be computationally expensive to be computed. For the size of 4500!, it is around 10^14,5000.

Quynh.

From: Moody, Dustin (Fed)
Sent: Monday, December 10, 2018 1:36:42 PM
To: Alagic, Gorjan (Assoc); Alperin-Sheriff, Jacob (Fed); Apon, Daniel C. (Fed); Cooper, David A. (Fed); Dang, Quynh (Fed); Liu, Yi-Kai (Fed); Miller, Carl A. (Fed); Perlner, Ray (Fed); Robinson, Angela Y. (Fed); Smith-Tone, Daniel (Fed); (b) (6)
Subject: 1st Round Report

I did a revision on some of the write-ups to make them more uniform. I think we want to try and make sure they are all written about the same level of detail, and include the important characteristics, strengths, and weaknesses. Please take a look and let me know of any suggested revisions. I put some comments in a few places where I thought changes might be good.

Thanks,

Dustin