From: Liu, Yi-Kai (Fed)
To: Moody, Dustin (Fed); Alperin-Sheriff, Jacob (Fed)
Subject: Re: Number of Papers to Add?
Date: Friday, August 26, 2016 4:16:24 PM

Thanks Jacob! That is very helpful!

Actually, one more thing: could you add links to some of the mailing lists that you find useful? There seem to be some useful discussions there that never get published anywhere else, and we (or at least I) haven't been great at remembering those.

Also, feel free to add a few papers on implementation to our list, too. We're not that interested in embedded systems, but it doesn't hurt to know a little about what people are doing there.

Thanks very much!

--Yi-Kai

_____

From: Moody, Dustin (Fed)
Sent: Wednesday, August 24, 2016 9:04:26 AM
To: Alperin-Sheriff, Jacob (Fed); Liu, Yi-Kai (Fed)
Subject: Re: Number of Papers to Add?

Maybe do a search on eprint.iacr.org over the past several months using the search terms post-quantum cryptography, and see if any there is anything recent that would be good to discuss. Could also look at PQCrypto 2016 in Japan to see if there are any from there as well.

Thanks!

_____

From: Alperin-Sheriff, Jacob (Fed)
Sent: Tuesday, August 23, 2016 4:24:56 PM
To: Moody, Dustin (Fed); Liu, Yi-Kai (Fed)
Subject: Number of Papers to Add?

I added about 10 (including adding a section on the various recent key-exchange proposals) that I think get many of the more important works over the last 3-4 years (as relates to standardization). There are a number of implementation papers (including some optimized to embedded hardware) that I could've added but didn't, and I of course didn't put anything from the multitude of lattice-based cryptography papers that I can't think are at all relevant to PQC standardization.

I suppose there may be a few other signature papers that could be relevant.
—Jacob Alperin-Sheriff