From: Dang, Thinh H. (Fed)
To: (b) (6)
Subject: Fw: Suggestion- we should meet sometime over the new CLZ21 paper
Date: Monday, August 30, 2021 2:58:10 PM

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Monday, August 30, 2021 12:24 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Suggestion- we should meet sometime over the new CLZ21 paper

https://eprint.iacr.org/2021/1093.pdf

It doesn't impact candidates, but you get the feeling that they took their shot at Dilithium and only just missed.

It's not obvious that it will quickly extend to a serious quantum attack against Dilithium (because it's using Arora-Ge as a subroutine, and inherits all of the limitations related to #samples), but it seems worth understanding the techniques well enough to stay informed about where things are.

Bonus points for this paper: They make big claims, and immediately provide verifiable analysis to support those claims. (I know that's been in short supply lately.)

--Daniel