From: Robinson, Angela Y. (Fed)
To: Moody, Dustin (Fed)
Subject: RE: PQC forum
Date: Thursday, August 29, 2019 3:25:00 PM

Okay, thanks! Some guy wrote something about side channel attacks on the FO transform. I wanted to ask for more details. I'm pretty sure it has less to do with the transform (since that only requires hashing and a random seed) and more to do with the decryption oracle.

I think I'll skip opinions altogether.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Thursday, August 29, 2019 3:23 PM
To: Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>
Subject: RE: PQC forum

You've been added. Feel free to post away!

In general – when you write, try to distinguish between your opinion and NIST's opinion . You can write for yourself. But any situation where it might seem you are writing as NIST, it's a good idea to send it first to internal-pqc@nist.gov and let people give feedback before posting. You're a good judge – I'm not worried about you!

Dustin

From: Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>
Sent: Thursday, August 29, 2019 1:25 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: PQC forum

Hi Dustin,

How can I be added to the PQC forum so I can reply to posts?