From:	Moody, Dustin (Fed)
To:	Miller, Carl A. (Fed)
Subject:	RE: 1st Round Report
Date:	Wednesday, December 12, 2018 11:11:18 AM

Got it. Thanks Carl.

From: Miller, Carl A. (Fed)
Sent: Wednesday, December 12, 2018 10:55 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: 1st Round Report

Hi Dustin –

I took another look at the qTesla submission, and I think it might be better / more accurate if I just focus on the quantum random oracle model in my summary. If it sounds correct to you, please replace:

"The authors of qTESLA have claimed tight security proofs for the schemes in the random oracle model and the quantum random oracle model. These security proofs have some challenges: the original security proof had a bug that needed an adjustment in parameters, and the proof in the quantum random oracle model assumes (among other things) a conjecture about the distribution of random elements in the ring."

With:

"The authors of qTESLA have claimed a tight security proof for the schemes in the quantum random oracle model. The security proof has some challenges: the original submission had a bug that needed an adjustment in parameters, and the security argument assumes (among other things) a conjecture about the distribution of random elements in the ring."

Otherwise the qTesla section looks good. Thanks for putting this together!

-Carl

———
Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Tuesday, December 11, 2018 at 3:08 PM

To: internal-pqc <internal-pqc@nist.gov>
Subject: 1st Round Report

Everyone,
I've incorporated comments in from our meeting this morning. Please review. Send back suggestions/edits by Friday.

Thanks!

Dustin