From: Miller, Carl A. (Fed)
To: Moody, Dustin (Fed)
Subject: Re: Reminder - Evaluate Round 2 submissions
Date: Monday, April 8, 2019 4:32:54 PM

Hi Dustin –

I looked at the two versions of qTESLA that I found on the sharepoint site, and they both seemed to mention the key compression technique – it's called "public key splitting," right? (Apologies if I'm mixing up the versions somehow.) Anyway, I believe qTESLA is complete. (I just checked off my part on the spreadsheet.)

-Carl

———

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

From: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Date: Thursday, April 4, 2019 at 4:36 PM
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Subject: Re: Reminder - Evaluate Round 2 submissions

Hi Dustin –

Ok, sure, I will take a look at both versions when I review qTESLA. I don't anticipate any problems finishing by the deadline. Thanks!

-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: Thursday, April 4, 2019 at 8:42 AM
To: internal-pqc <internal-pqc@nist.gov>

Subject: Reminder - Evaluate Round 2 submissions

Everyone,

Just a reminder to those who are going through the checklists for the Round 2 submissions -- we need to have them done before our meeting next Tuesday, 10am. If you need help, or don't think you can get it done, please let me know.

It'd be great if you could mark when you've completed one. You can do so here (on the sharepoint site):


Status of Round 2Submissions.xlsx

On another note, qTESLA submitted their updated revision with key compression in it. We'll have to decide if we'll accept it, or just their version submitted by the deadline. Jacob and Carl - I'll upload it to the sharepoint site, and maybe you can look at both versions?

Thanks everyone!

Dustin