From:	Moody, Dustin (Fed)
To:	Robinson, Angela Y. (Fed)
Subject:	RE: Idea for talk
Date:	Wednesday, December 11, 2019 8:56:00 AM

Angela,

That sounds great. When would you like to talk?

Dustin

From: Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>
Sent: Tuesday, December 10, 2019 3:45 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Idea for talk

Hi Dustin,

Dan and Tanja recently posted a scheme on eprint that solves the problem of how to split up the very large McEliece keys in a way that prevents denial-of-service attacks. Although I just saw the article only appeared on eprint Dec. 2nd, Ray says Dan has talked about this before. Here is the paper: https://eprint.iacr.org/2019/1395 . I am thinking I could present this to the group.

Thank you,
Angela