From: Bassham, Lawrence E. (Fed)
To: Apon, Daniel C. (Fed)
Subject: Re: Interested in a group phone call with an FPGA team, perhaps interested in implementing PQC candidates?
Date: Thursday, February 7, 2019 2:30:17 PM

Sure

From: "Apon, Daniel C. (Fed)" <daniel.apon@nist.gov>
Date: Thursday, February 7, 2019 at 2:29 PM
To: "Bassham, Lawrence E. (Fed)" <lawrence.bassham@nist.gov>
Subject: Fw: Interested in a group phone call with an FPGA team, perhaps interested in implementing PQC candidates?

Larry--

Dustin, Jacob, Ray, and I are interested in setting up a call with Dr. Andrews. Would you be interested in joining?

--Daniel

From: Apon, Daniel C. (Fed)
Sent: Thursday, February 7, 2019 2:24 PM
To: Moody, Dustin (Fed); Chen, Lily (Fed); Alperin-Sheriff, Jacob (Fed); Perlner, Ray (Fed)
Subject: Interested in a group phone call with an FPGA team, perhaps interested in implementing PQC candidates?

Hi all,

I've been briefly looking around for additional hardware research teams, which might be interested in independently implementing our 2nd Round PQC candidates on either Cortex-M4 or Artix-7, so that we can incorporate some type of external, comparative hardware performance data into our 2nd Round decisions..

The first, serious response I've gotten back is from David Andrews at the University of Arkansas. His FPGA team has, for instance, sent multiple graduate students into careers at Xilinx. He is, in his words, "heavily involved in the design of FPGAs," and he appears interested in directing resources towards hardware evaluations of our candidate-algorithms.

I am intending to schedule a voice chat / call with him in the next week or so. Would any of you be interested in joining this call with Dr. Andrews?

--Daniel