From:	Alperin-Sheriff, Jacob (Fed)
To:	Moody, Dustin (Fed)
Cc:	internal-pqc
Subject:	Re: next project for you
Date:	Wednesday, April 10, 2019 11:34:54 AM

Looks like FALCON, ntruprime, ROLLO and RQC are the ones who didn't

---

From: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Date: Wednesday, April 10, 2019 at 10:47 AM
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Re: next project for you

Yeah, let's make them publish them on their own webpage, I agree. And I think a concrete deadline is good, if you want to move it back a bit farther that might be okay though.

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Wednesday, April 10, 2019 at 10:46 AM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Re: next project for you

What will we do when we get back such implementations? Obviously we will review them internally, but will we post them on our webpage or anything? Or just have the submitters post them on their own websites? Do we need a concrete deadline?

Perhaps we should modify C) to not say "if we don't receive them" to just say something like "if these implementations are not published..."

From: Alperin-Sheriff, Jacob (Fed)
Sent: Wednesday, April 10, 2019 10:41 AM
To: Moody, Dustin (Fed)
Cc: internal-pqc
Subject: Re: next project for you

I also noticed several teams didn't have AVX2/vector /assembly implementations. If you're okay with that, I will email those teams today or tomorrow noting

A. That we do not appear to have received an AVX2/vector /assembly implementations from them
B. While these implementations were not strictly mandatory, they have been strongly recommended for over a year, and given that performance will play a very large role in Round 2, teams without such an implementation are likely to be at a very distinct disadvantage.

C. Should we not receive such an implementation by (I dunno, May 1st), we will be forced to compare their mandatory optimized implementations to the other submission's AX2/vector/assembly implementations in our analysis

---

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Wednesday, April 10, 2019 at 10:26 AM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Subject: Re: next project for you

From: Alperin-Sheriff, Jacob (Fed)
Sent: Wednesday, April 10, 2019 10:26 AM
To: Moody, Dustin (Fed)
Subject: Re: next project for you

I was going to do that shortly with the machine Larry gave me.

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Wednesday, April 10, 2019 at 10:24 AM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Subject: next project for you

Jacob,

No immediate rush, but can you generate numbers for the submissions like you did for the 1st Round? The ones you put in the spreadsheet that show key sizes, as well as the cycle counts from your machine? Thanks,

Dustin