From: Bassham, Lawrence E (Fed)
To: Moody, Dustin (Fed); Alperin-Sheriff, Jacob (Fed); internal-pqc
Subject: Re: What Are We Doing About the Attacks That We"ve Been Given
Date: Thursday, December 28, 2017 7:33:00 AM

With previous " competitions" I think there were various outside groups - SHA Zoo as an example - that would create tables with breaks, etc. We already see people putting up tables now. I would let the community continue like that. All we need to do is eventually justify some decisions. It's still very soon after we announced the candidates. I bet that by the time the people give their presentations at the Workshop there will be plenty of sites up with that sort of information.

On: 27 December 2017 22:48, "Moody, Dustin (Fed)" <dustin.moody@nist.gov> wrote:

I think we should let the community discuss, and we can add comments if we like.

Maybe we should ask the submitters if they have any reply or if they would like to withdraw if they accept it as broken?

I think those paying attention know which algorithms are broken. We don't need to call extra attention to it.

From: Alperin-Sheriff, Jacob (Fed)
Sent: Wednesday, December 27, 2017 11:05:34 AM
To: internal-pqc
Subject: What Are We Doing About the Attacks That We've Been Given

Like I checked the RVB one in Sage and I'm convinced it's good. Are we telling them how apparently the mathematics have failed here?

—Jacob Alperin-Sheriff