From:	Alperin-Sheriff, Jacob (Fed)
To:	Apon, Daniel C. (Fed); Moody, Dustin (Fed)
Subject:	Re: Hardware evals of NIST candidates -- thoughts?
Date:	Friday, February 1, 2019 12:17:49 PM

It would be helpful to have all the Round 2 candidates implemented on some specific set of devices and/or report that it won't work on some constrained devices (at least using their streamlined methodology)

From: "Apon, Daniel C. (Fed)" <daniel.apon@nist.gov>
Date: Friday, February 1, 2019 at 11:58 AM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Subject: Hardware evals of NIST candidates -- thoughts?

Hey Jacob, Dustin,

https://eprint.iacr.org/2019/047.pdf

I've spoken briefly with the authors of this paper. (Basically, "Hey, neat paper.")
I thought we should take a look at it..
They also were interested in any feedback we might have.

I think they currently have about 1/2 of our Round 2 candidates implemented in their hardware lab,
and might be open to any direction we have in terms of what data we would like them to gather..

--Daniel