From: Moody, Dustin (Fed)
To: Peralta, Rene C. (Fed)
Subject: FW: new paper
Date: Monday, April 3, 2017 8:52:02 AM

FYI

From: Perlner, Ray (Fed)
Sent: Friday, March 31, 2017 5:06 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: new paper

Have you shown this to Rene? I think he'd be quite interested in the ZK proof aspects. (I think that part is much more interesting than the signature scheme, which appears to be unambiguously worse than SPHINCS. More advanced functionalities like EPID may be a more promising application, maybe, but I suspect this result is primarily of theoretical interest.)

From: Moody, Dustin (Fed)
Sent: Friday, March 31, 2017 11:17 AM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: new paper

Ray,
Here's the paper I was telling you about. Their keygen is actually fast enough, but signing and verifying are slow.

http://eprint.iacr.org/2017/279.pdf