From: Moody, Dustin (Fed)
To: (b) (6)
Subject: RE: Review Request
Date: Thursday, November 30, 2017 2:01:00 PM

Daniel,

I’ve read the paper twice now. The second time at a deeper level, but I haven’t spent hours on it or anything. I’d definitely recommend acceptance. My review is super detailed, because the paper was well-written, without lots of errors.

Dustin

Review on: On the Equivalence of Torsion-Point Isogeny Problems

I think the abstract is a good summary of what the paper is about, and explains its importance accurately. More study is certainly needed on the security problems underlying SIDH, especially as the NIST PQC process is going on. This paper contributes much to the existing understanding.

The 3 problems of section 3 are more natural than the actual SIDH problem. It would be even better to be able to relate the security of SIDH to more general isogeny problems, as is described in Galbraith et. al.'s recent papers ([7,8]). Still, the reductions given are very helpful. Especially the connection to the Key Validation Problem.

I don't agree with the statement in the conclusion:
"The torsion-point isogeny problems underlying the security of SIDH and several proposals for isogeny-based signatures [8, 12, 17, 21] have thus far undergone little study. One could argue this lack of study is indicative of their difficulty."
It might be true, but it could just be that not enough experts in this area have looked at this problem.

Overall, I highly recommend acceptance.

From: Daniel Smith (b) (6)
Sent: Tuesday, November 28, 2017 3:52 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Review Request

Hi, Dustin,

Would you be willing to be a subreviewer for the following attached paper? "On the Equivalence of Torsion-Point Isogeny Problems"

If you can, please send me your review by Dec. 15. My deadline is Dec. 17th, and I may want to add some of my own comments.

If you can't (or, of course, don't want to), please let me know. I'm comfortable with this paper (and one I just asked Ray to help with), but it would be better for me to have an expert look at it to spot anything that may get past me. So if you can't, I think that I'll need to ask someone else.

Thanks.

Cheers,
Daniel