From: Moody, Dustin (Fed)
To: Kelsey, John M. (Fed)
Subject: RE: fips 186
Date: Friday, June 17, 2016 8:18:29 AM

John,
Andy probably knows as much as I do, but here's my take. We opened FIPS 186 for comments, received several, and have had several meetings about what revisions to make. There are some pretty minor ones involving things like prime generation, which nobody seemed to have a problem with. The two more substantive issues were: are we going to add new curves, and if so how/which ones? And also, there seemed support for adding a deterministic signature scheme (but which one?).
It seems we've decided that we will add the two curves the CFRG is going to standardize (Curve 25519 and Ed448). For now, that's what we know for sure. We've been slowly trying to feel out people's opinion if that is sufficient. The other thing that we might do is decide to add some pseudorandom curves (like the Brainpool ones, or generate new ones). We don't yet know if we will do that or not.
As for which signature scheme to add, I don't think our discussions ever settled that. I think several of us wanted to know what you thought, but you were gone when we had a few of the meetings. The main possibilities seem to be a deterministic ECDSA, or a Schnorr-type scheme (of which there are a few). We should probably decide on that.
Right now, Andy and Lily are in the process of trying to hire a contractor to help us out with the actual writing. They seem to feel this is necessary. I think the hope is that we can get that finalized sometime this year. It feels to me we are moving pretty slow on all this, but I regularly ask Andy and Lily, who seem okay with the pace. I think some of the wind has gone out of the sails of all this, due to PQC, and the NSA's pronouncements about ECC. It feels to me a lot of the urgency and animated conversation about new curves seems to have died down a bit, which might explain our slow pace somewhat. Anyway, that's where things stand with FIPS 186 as I know it. Let me know if you have any other questions about it. Thanks,
Dustin

From: Kelsey, John M. (Fed)
Sent: Thursday, June 16, 2016 5:23 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: fips 186
Dustin,
I'm giving a talk on Sunday in Colorado in which I'm going to talk about what we're doing w.r.t. crypto standards. I've talked with Lily about PQ stuff, but I'd also like to know what's going on with the FIPS 186 revision. (I talked with Andy about it, but I think you're the main guy working on it.) Can you just give me a paragraph or two about what's going on right now, what our plans are, what our timetable is, etc?
Thanks,
--John