From: Moody, Dustin (Fed)
To: (b) (6)
Subject: RE: Reviews
Date: Monday, December 18, 2017 7:59:00 AM

I agree with you.

From: Daniel Smith (b) (6)
Sent: Monday, December 18, 2017 7:58 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Reviews

Yeah. I think that part of the issue is that Bo-Yin is an expert at hacks that make the code as fast as possible. I'm not sure if they are trying to get away with cheating or not, but to me the main point is that it is clear that they can do it properly and get it to us. Jacob's email set a hard deadline that sounds scary (which makes perfect sense to me, considering out meeting and Jacob's situation), but these are not schemes that we should be rejecting because of a technicality. There are other schemes that had errors in the science that I am willing to forgive because of the possible promise of the schemes done properly, and that is a much more serious error, I think, than buggy code that we know can be fixed. The reason it is buggy is because they want to be as tricky as possible within the framework to be efficient. They should just drop this and get something working. Of course we will consider better implementations later in the process, but they don't know that.

Cheers,
Daniel

On Mon, Dec 18, 2017 at 7:42 AM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

> It’s been a pain getting their implementations checked. I’m working with Jacob and Larry on it today. We did get the KATs to work for one parameter set.
>
> We’ll work with them.
>
> **From:** Daniel Smith (b) (6)
> **Sent:** Monday, December 18, 2017 7:33 AM
> **To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
> **Subject:** Re: Reviews
>
> I'll try to email you later today.
>
> I got a call from Jintai yesterday. He was frightened by an email from Jacob. He is having trouble getting ahold of Bo-Yin to make the implementation platform independent. He said that they were confused before about that since we said something about the testing platform and since the instruction set they were using is across modern intel platforms they thought what they did was okay. Jintai is worried that they can't finish by 5pmEST tomorrow (the deadline Jacob gave them).

> Just a head's up. I'll write more about it or talk to you later.
>
> Cheers,
> Daniel
>
> On Mon, Dec 18, 2017 at 7:29 AM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:
>
> > Daniel,
> > Thanks – I will send out a summary sheet today, and you can add any comments. I'll add the two you wrote below.
> >
> > Dustin
> >
> > **From:** Daniel Smith (b) (6) [redacted]
> > **Sent:** Friday, December 15, 2017 6:25 PM
> > **To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
> > **Subject:** Reviews
> >
> > Hi, Dustin,
> >
> > I finished the reviews. Of the ones I did today, a couple of issues stand out. First, NTRU Prime seems to be incomplete, unless I overlooked the data. I see no timing values for the NTRULPrime scheme. It seems fine for the SNTRUP scheme with everything complete.
> >
> > Second, I'm not moved by the reply from the submitters of STRPI and TPSig that the decryption/signing function is linear "only" for the legitimate user. What nonsense is that? Is y=2x quadratic for me if I don't look at it? The submission is complete, but not proper.
> >
> > I will not be able to attend the meeting on Tuesday, but I'll write more for you on the schemes that I reviewed so that you can have notes if they are necessary. I will probably be able to send it on Monday. I'm pretty busy this weekend.
> >
> > Cheers!
> > Daniel