From: Moody, Dustin (Fed)
To: Chen, Lily (Fed)
Subject: Re: side-channel and NIST standards
Date: Monday, August 16, 2021 9:14:43 AM

Thanks. I understand.

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Saturday, August 14, 2021 7:14 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: side-channel and NIST standards

Hi, Dustin,

We do not have any fund for FY21. We cannot predict funding situation for FY22. They can submit application. Our call for proposals is open regardless whether we have fund or not. If they submit, we must review, also regardless whether we have fund or not.

If we have funding in FY22, we may consider those applications based on the review. But they can choose to submit proposals in FY22, which starts October 1, 2021.

Lily

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Friday, August 13, 2021 9:19 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: side-channel and NIST standards

The University of Florida team asked if there is ITL grant money right now.

I guess they want to know if there is a reason to apply (or if there is no money right now then no need to apply for an ITL grant).

Do you know?

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Tuesday, August 10, 2021 2:48 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: side-channel and NIST standards

Dustin,

I think we can have a meeting with our team to discuss. About side-channel security, I think we might think them at two levels.

1. Consider side-channel secure feature when selecting algorithms to be standardized, e.g. whether the algorithm can be implemented efficiently with countermeasures for side-channel

attacks.

2. Include some guidance on side-channel resistance implementations.

I think we have factored in side-channel in PQC candidates. But addressing side-channel in standards may need some considerations. A standard specifies an algorithm. It seems that there are not much space to “discuss” side-channel resistance. For security, we can provide requirements on key length, parameters, etc. Can we provide solid requirements for side-channel security? Actually, side-channel resistance is a secure measure for FIPS 140 crypto module validation for level 4 security. Those have been specified in the testing. But it is not specified in the standards for algorithm specification.

Maybe these have been discussed at the meeting. In any case, let’s have a meeting.

Lily

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Tuesday, August 10, 2021 1:18 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: side-channel and NIST standards

Lily,

On Monday, a few of us had a meeting with a team from the University of Florida. They had been doing some side-channel analysis work on SABER, and plan to continue to do more work on the other finalists. They gave us an update on their work, and it was pretty good. They would like funding, so I'm going to point them to the ITL grants as the best way to do this. Apparently he's worked with Apostol on some grants before.

Anyway, after the meeting the NIST people had a discussion about the importance of side-channel analysis. We were talking about how our standards address side-channel attacks. I think some of our standards have a few comments about side-channels, but no extensive discussion. Daniel Apon and Apostol seemed to think that we should start having much more in our standards, perhaps starting with the pqc standard. They would like to have a meeting with a larger audience (the crypto team) to discuss this. Do you have any thoughts on this?

Dustin