From: Dang, Quynh (Fed)
To: internal-pqc
Subject: Re: Some notes from the discussion
Date: Monday, August 26, 2019 10:08:07 AM

Hi everyone,

John had a nice list of many important points. I would like to discuss a bit more about several of those points inlines of John's email.

Another question: Should we keep the current schedule or extend it to get more reviews and analysis ?

It seems that vast majority of the community thinks that more time than what we planed is needed.

There is a comment saying that the intelligence community may want to have a standard soon because it takes a long time for new crypto to be deployed and those devices might be in the field for a long time and in many cases, it is very costly or impossible to update them to pq crypto later. However, it would be much worse when the crypto is broken.

The intelligence community makes their own decision on what crypto to use I think. I think they are not mandated by any laws to use NIST's standards. It could be that internally some of them has a policy of using NIST-standards only (When I make a change, I am reliable for that change. If I take advice from someone, I could have some defense for something wrong).

But, we standardize crypto only when we have strong confidence that it is secure and usable.

Regards,
Quynh.

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Saturday, August 24, 2019 11:59:13 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Some notes from the discussion

Everyone,

Congratulations on what seemed like a quite successful conference! I think the final discussion went very well, especially given how tired everyone was.

I took a few notes from the discussion today, and related them to some conversations I had during

the workshop.

a. We need to think about how to add support in our KDFs for extra randomness (from any source). If there's a simple way to do this for a given KDF, then it will be easy to use a hybrid scheme even before we've approved any PQ algorithms—feed the agreed key from the PQ scheme in as the extra randomness. I think we can do this in a pretty minimally-invasive way.
b. There's basically no good mechanism in our community for making sure things have been carefully checked out—it's common that something has been public for years, is in widespread use, but nobody's ever really closely looked at some critical part of it. Some ways I can see to try to do a better job with this are:
    a. Maybe we could make a kind of public checklist of what needs to be looked at in each design, and try to fill in each checklist with a reference to a paper or something? (Maybe that would make it easier to make the case for getting a paper published based on analysis that filled one of the spaces in the checklist?)
    b. Would it make sense to hire some contractors (or fund some grad students) to spend a few months checking specific stuff we want checked?
    c. Can we read through the submissions and try to list the critical assumptions? Or get someone else to do so?
    d. Is there some way to fund some effort to actually do automated proof checking? I doubt it, but it would be kinda cool.
    e. Is there some way we can help people get some kind of academic/tenure credit for filling in gaps/checking proofs in our competition?

Quynh: Often, checking proofs is a very hard job, especially when it is 30 or 40 pages long. So, my guess is that when the author is a very respected one, readers tend to skip his or her lengthy proofs.
Edoardo Persichetti's comment and another in Yi-Kai's summary suggested that we should find ways to support proof verification works such as the work Dan Berstien did of pointing out some gaps or unclear points in several schemes' security proofs. Proof verifications by software seems to be very complicated because in order to use software to verify a proof, it seems that one must understand exactly how the proof works in details. But, if one understands the proof in details, then it seems that no software verification is needed.

So, proof verification works require experts in the specific fields to understand all the details of the proofs. Funding should help this effort.

a. We need a way to get people to tell us about negative cryptanalysis—"I spent a month looking at this and didn't get anywhere." This is hard, because nobody wants to do that and then have someone else find a problem they missed, but it's frustrating how much effort is duplicated and how much is lost because it didn't end up with a publishable result.

Quynh. Exactly. we would need to give these people some rewards for their efforts with the hope that

they'll talk about what they have gone through. Grad students are more likely to do this than the established researchers. We could hold workshops and fund the students who provide details of what they are doing/thinking which are relevant to us, for their travels to come to talk to us at workshops or private meetings.

a. A lot of the problems on which PQC is based are very unfamiliar even to most older cryptographers. (I sympathize!). This means it's hard for people who want to understand these schemes to get up to speed.
    a. We should try to link to good tutorials for various PQ schemes. There was a very nice summer school organized by Dan and Tanja a couple years ago that has some videos—that's not a bad place to start.
    b. I had a couple people suggest to me that we should have a couple days of tutorials before the next PQ workshop, so people could refresh their memories about what was going on in the schemes.

Quynh: This is a great idea. A lot of grad students would appreciate this. One commenter said she had a hard time to understand many candidates. People only like, analyze and work on the things that they understand. So, more people understand, more people will analyze the schemes for us.

a. The proposal for workshops on specific classes of schemes seemed reasonable.

Quynh: Another good idea.

a. How can we get better information on performance limitations. Some of this information might be available from the lightweight project, but I think for a lot of it, we need to try to get some people in industry to talk to us at some depth. I'm not sure how to go about this.
b. Daniel the Elder brought up NSF funding lines. Can we follow up on this?

I hope this is helpful.

Thanks,

--John