From: Daniel Smith
To: Chen, Lily (Fed)
Cc: Perlner, Ray A. (Fed); Liu, Yi-Kai (Fed); Moody, Dustin (Fed); Jordan, Stephen P; Peralta, Rene C. (Fed); Regenscheid, Andrew R. (Fed); Smith-Tone, Daniel C. (Fed)
Subject: Re: PQCrypto slides
Date: Tuesday, February 2, 2016 12:08:25 PM

The meeting today reinforces what I think that Ray and I feel that we learned in Dagstuhl in September. ETSI's process is sort of a "path of least resistance" to establishing a consensus on post-quantum technologies. By this, I mean that is seems they are wanting to support in as reasonable a way as possible the types of schemes that industry would like to hear are viable options, even at the expense of rigor.

I think that this is a perfectly reasonable think to do, and I believe that it is valuable, but I'm concerned about how their suggestions might impact the perception on our choices later on. We may be (probably will be) more or less forced to make recommendations that fall far short of theirs in certain metrics. My own self-serving recommendation to us as a team interacting with them would be to recommend that they disclose the gap between the assurance of security between various schemes that they are recommending (and not recommending).

An example of this would be my comment about the gap between theory and practice in the state-of-the-art lattice reduction algorithms. If we face a situation in which we choose lattice signatures but choose parameter sizes that have a more concrete justification, it would be nice (for political reasons) to be able to refer to an ETSI document admitting that the discrepancy between their recommended parameters and justified parameters exists.

Do you agree? Perhaps my opinion is unjustified. Is it less justified than certain lattice signature parameters? :/

I notice that in the table in the draft sent to us that most of the parameters for the multivariate schemes seem to not match the figures I am familiar with. (I may be confusing the 128 bit parameters with 80 bit parameters, but I think that I'm not.) Perhaps someone better qualified in our group could take a similar look at some of the parameters for other families to see if they reflect the current cryptonomy (;D). This discrepancy makes me wonder about ETSI's process and how politically motivated it is.

I'm sorry to be so paranoid, but I am skeptical that ETSI's process is accurately reflecting the state of knowledge in PQ, even though I think that the recommendations they are making are reasonable from their claimed standpoint.

What do you think?

Cheers,
Daniel

On Tue, Feb 2, 2016 at 11:33 AM, Chen, Lily <lily.chen@nist.gov> wrote:

> I think that is a good point.

> Lily
>
> ---
>
> **From:** Daniel Smith <dcs.xmr@gmail.com>
> **Sent:** Tuesday, February 2, 2016 11:32 AM
> **To:** Chen, Lily
> **Cc:** Perlner, Ray; Liu, Yi-Kai; Moody, Dustin; Jordan, Stephen P; Peralta, Rene; Regenscheid, Andrew
> **Subject:** Re: PQCrypto slides
>
> We should extend the timeline beyond draft standards. As mentioned in our meeting, this invites tough questions. Do you agree?
>
> On Thu, Jan 28, 2016 at 9:03 AM, Chen, Lily <lily.chen@nist.gov> wrote:
>
>> Here is an aspect we might need to think about: How are we going to collaborate with other standards organizations?
>>
>> This has never been a problem for AES and SHA-3. For the existing Public Key Cryptography standards, there exist certain inconsistences between NIST standards and other standards. For example, for Diffie-Hellman key agreement in 56A and in IKE and TLS.
>>
>> In the next 5-7 years, when we are working on PQC standards, I am sure other standards will work on PQC as well. What we can do to collaborate with other standards organizations.
>>
>> We do not have to include an answer to the slides. But people will ask. We need to know how to respond. We need to plan ahead.
>>
>> Lily
>>
>> ---
>>
>> **From:** Perlner, Ray
>> **Sent:** Wednesday, January 27, 2016 9:35 AM
>> **To:** Liu, Yi-Kai; Daniel Smith; Moody, Dustin
>> **Cc:** Chen, Lily; Jordan, Stephen P; Peralta, Rene; Regenscheid, Andrew
>> **Subject:** RE: PQCrypto slides
>>
>> Here are my comments
>>
>> ---
>>
>> **From:** Liu, Yi-Kai
>> **Sent:** Monday, January 25, 2016 4:30 PM
>> **To:** Daniel Smith; Moody, Dustin
>> **Cc:** Chen, Lily; Jordan, Stephen P; Peralta, Rene; Perlner, Ray; Regenscheid, Andrew
>> **Subject:** Re: PQCrypto slides
>>
>> Hi Dustin,

> > Thanks for putting together those slides! I think they look fine. Here are a few suggestions:
> >
> > Slides 1 and 2: Edit "When will a quantum computer be built?" to say "When will a quantum computer be built that can break RSA-1024?"
> >
> > Between slides 6 and 7: I think it might be helpful to add a slide saying that there is no "silver bullet" for post-quantum cryptography, i.e., there is no one candidate that will satisfy everyone. Every candidate has some disadvantages: McEliece has giant keys, hash based signatures are prone to accidental misuse, NTRUSign leaks some information, etc. And, above all, there hasn't been enough research on quantum algorithms to be really confident about the security of some of these schemes.
> >
> > As a result, I think that post-quantum cryptography is a much more complicated situation than AES or SHA-3. It may be impossible to achieve consensus on which candidate is "the best." Instead, I think our goal should be to pick a candidate that is "well rounded" in the sense that it meets everyone's minimum requirements. (This is elaborating on some of your comments on slide 7.)
> >
> > Maybe instead of calling this a "competition," we could say that this is a "standards development process"?
> >
> > On slide 8: Under "minimal acceptability requirements," I would add "theoretical and empirical evidence that provides justification for claims about security."
> >
> > On slide 15: Under the question "How is the timeline? Too fast? Too slow?" maybe add another question "Should we do this only once, or have an ongoing process to standardize technologies as they become mature?"
> >
> > Cheers,
> >
> > --Yi-Kai
> >
> > ---
> >
> > **From:** Daniel Smith <dcs.xmr@gmail.com>
> > **Sent:** Sunday, January 24, 2016 1:52 AM
> > **To:** Moody, Dustin
> > **Cc:** Chen, Lily; Liu, Yi-Kai; Jordan, Stephen P; Peralta, Rene; Perlner, Ray; Regenscheid, Andrew
> > **Subject:** Re: PQCrypto slides
> >
> > I don't like the line:
> >
> > "Algorithms could be submitted later, but may not get the same scrutiny"
> >
> > I don't think it is inappropriate exactly; I just don't like the way it sounds. I think that it would be better to leave out the second bullet point there altogether. Narrowing the focus already implies this idea without stating it so bluntly.
> >
> > Cheers,

> > Daniel
> >
> > On Thu, Jan 21, 2016 at 5:15 PM, Moody, Dustin <dustin.moody@nist.gov> wrote:
> >
> > Everyone,
> >
> > Next Tuesday (1/26) we'll go over our PQC plans with the NSA. I've been working on slides for our PQCrypto announcement in February. My first attempt at the slides is attached. Please make corrections/suggestions, etc... before Tuesday. Thanks!
> >
> > Dustin