From: Liu, Yi-Kai
To: Moody, Dustin
Subject: Re: Outline for PQCrypto announcement
Date: Thursday, January 14, 2016 1:57:24 AM

Hi Dustin,

Thanks for putting that together! I think it looks pretty good. One suggestion is to make a slide with a list of questions that we would like to ask the PQCrypto community:

- How is the timeline? Too fast? Too slow?

- Should all the proposals be on the same schedule, or should we try to "fast-track" those proposals that seem more mature?

- Should we just focus on encryption and signatures, or should we also consider other functionalities like stateful signatures and key establishment?

- How many "bits of security" do we need against quantum attacks?

- How can we encourage more work on quantum cryptanalysis? Maybe we could pose some more "challenge problems"?

- If we want to standardize some post-quantum cryptosystem that has worse parameters (such as key length) than our currently-deployed crypto, this may have consequences for higher-level protocols and applications. How can we encourage people to study these issues? For instance, I would feel more confident if we had some more prototype implementations of post-quantum TLS and IKE protocols.

- And probably lots of other questions...

Thanks,

--Yi-Kai

From: Moody, Dustin
Sent: Wednesday, January 13, 2016 2:28 PM
To: Liu, Yi-Kai
Subject: Outline for PQCrypto announcement

Yi-Kai,

Sorry for sending lots of emails to you. I thought I'd run things by you first, before sending them around to the group. Here's an outline I created for the PQcrypto announcement. I haven't worried about if this all fits in 30 minutes, or how much time to spend on what parts, or anything like

that. I just tried to think of everything we might want to mention. I think if we come up with a good outline, it will help us make sure our plan for the process is missing anything, and we can write section 4 of the NISTIR better.

Anyway, this is pretty rough, but a place to start.

Dustin

1) Motivation (not a lot needed for this audience)
a. Quote estimate of time til quantum computers, "Mosca's Theorem" (as to why we need to start now)
b. Impact on PKC / (NIST) standards
i. Can mention our NISTIR
c. Mention NSA's statement? (not sure about this) EU's project?
2) NIST Call
a. Idea of Rene's statement (we want to manage process, hopefully help community to identify good choices…)
i. Talk about similarities/differences between this and AES/SHA-3 competitions? (not sure about this)
b. Timeline
i. Formal call out by late 2016. (SHOULD WE PICK A DATE?)
ii. Deadline for Submissions, late 2017 (DATE?)
iii. Workshop ?? not too long after deadline
iv. Analysis phase, 3-5 years
1. Do we want rounds?? Announce workshops?
2. We will issue report at end (or after round? Or halfway through?)
v. Draft standard for public comment, 2 years later (DATE?)
vi. Can accept submissions on ongoing basis (like modes), but…
c. Maybe here would be better to talk about difference from competition? (if we want to)
3) More details
a. Detailed instructions will be similar to SHA-3
i. Parameter sets, target security levels
ii. Specification/code
1. API instructions?
2. Call approved symmetric primitives?
3. Implementations
a. C code
b. Known answer / Monte-Carlo tests
b. Evaluation criteria (will be open for public comment?)
i. Security analysis
1. What are the right security definitions?
2. Algorithm complexity definitions
3. Security proofs not required?
4. Quality of prior cryptanalysis
ii. Performance analysis

1. Parameters & key sizes
2. Time to perform operations

iii. Practical deployment

1. Ease of implementation, ease of use, misuse resistance

iv. IPR stuff (not sure if here or in 3a)

1. If can make license free than it's a big advantage, but not required

4) Conclusion

a. Restate our role in managing process
b. We don't have all the answers. We want feedback
c. Contact info (pqc@nist.gov – NSA gets this email as well. Need new email?)

i. Mention pqc – forum for discussion