From: Chen, Lily
To: Moody, Dustin
Subject: RE: Outline for PQC announcement
Date: Tuesday, January 19, 2016 9:35:00 AM

Dustin:

I think it is an good idea to tell NSA about our plan when they come.

Lily

From: Moody, Dustin
Sent: Tuesday, January 19, 2016 8:14 AM
To: Chen, Lily
Subject: Re: Outline for PQC announcement

Lily,
Thanks!! Your comments are extremely helpful as I'm preparing the slides.

By the way, our next meeting with the NSA PQC folks is Jan 26th. I plan on giving them a brief rundown of our plans, so they know what is happening. I don't want them to be the last to know.

Dustin

From: Chen, Lily
Sent: Friday, January 15, 2016 4:22 PM
To: Moody, Dustin; Liu, Yi-Kai; Perlner, Ray; Peralta, Rene; Bassham, Lawrence E; Jordan, Stephen P; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)
Subject: RE: Outline for PQC announcement

Hi, Dustin:

The outline is fine. Please see inserted suggestions/comments/discussions.

Lily

From: Moody, Dustin
Sent: Thursday, January 14, 2016 1:12 PM
To: Liu, Yi-Kai; Perlner, Ray; Peralta, Rene; Chen, Lily; Bassham, Lawrence E; Jordan, Stephen P; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)
Subject: Outline for PQC announcement

Everyone,
Sorry for yet another email, but we have much to get done this month. I’m going to start

working on the slides for our announcement at PQCrypto. I put together an outline to guide me. Please let me know if I'm missing something. Thanks,

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? (With Rene's statement in the front, we can move this part to the later portion of the presentation.)

b. Timeline

 i. Formal call out by late 2016. (We can select a month or season, say the fall of 2016)

 ii. Deadline for Submissions, late 2017 (DATE?)

 iii. Workshop ?? not too long after deadline [after the submission deadline, we will post the submissions. The first workshop is for the submitters to present. Right?]

 iv. Analysis phase, 3-5 years [we can have workshops during the analysis stage, not the end of the 3-5 years.]

1. Do we want rounds?? Announce workshops? [We may not be able to exclude many. But we can select. For example, among the submissions A, B, C, D, we select B, while A, C, D are still in the pool. No decision is made. Not like in a competition. If A, C, D are not selected, then A, C, D are out.]

2. We will issue report at end (or after round? Or halfway through? [It is likely that the report will focus on what we selected, not what we haven't selected.])

 v. Draft standard for public comment, 2 years later (DATE?)

 vi. Can accept submissions on ongoing basis (like modes), but…for the new submissions, it will take time for the analysis people to get into it. We cannot move forward until we have sufficient understanding about its security and performance.

c. Maybe here would be better to talk about difference from competition? (if we want to, I think we need to, probably here, not in the front.)

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

    v. Questions we have

    1. How is the timeline? Too fast? Too slow?
    2. Should all the proposals be on the same schedule, or should we try to "fast-track" those proposals that seem more mature? [An alternative of this question is how to determine a candidate is mature for standardization.]
    3. Should we just focus on encryption and signatures, or should we also consider other functionalities like stateful signatures and key establishment?
    4. How many "bits of security" do we need against quantum attacks?
    5. How can we encourage more work on quantum cryptanalysis? Maybe we could pose some more "challenge problems"?
    6. 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. [I think we shall encourage the submitters to provide any perspectives on "dropping" the proposed algorithms to the existing protocols such as TLS and IKE.]
    7. Etc….

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? (We need a new e-mail reflect. It will need some people who will in the team, not necessarily cryptographers.)

    i. Mention pqc – forum for discussion