From: Moody, Dustin (Fed)
To: Kerman, Sara J. (Fed)
Subject: RE: PQC forum
Date: Thursday, March 3, 2016 1:21:06 PM

Sara,

How about we replace it with the following text:

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of *post-quantum cryptography* (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.

The question of when a large-scale quantum computer will be built is a complicated one. While in the past it was less clear that large quantum computers are a physical possibility, many scientists now believe it to be merely a significant engineering challenge. Some engineers even predict that within the next twenty or so years sufficiently large quantum computers will be built to break essentially all public key schemes currently in use. Historically, it has taken almost two decades to deploy our modern public key cryptography infrastructure. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing.

NIST is taking the following steps to initiate a standardization effort in post-quantum cryptography. NIST plans to specify preliminary evaluation criteria for quantum-resistant public key cryptography standards. The criteria will include security and performance requirements. The draft criteria will be released for public comments in 2016 and hopefully finalized by the end of the year. At that time NIST will begin accepting proposals for quantum-resistant public key encryption, digital signatures, and key exchange algorithms. NIST intends to select at least one algorithm providing each of these functionalities for standardization. NIST will establish a submission deadline late in 2017 for algorithms to be considered, allowing the proposals to be subject to 3 to 5 years of public scrutiny before they are standardized.

Dustin

From: Kerman, Sara J. (Fed)
Sent: Thursday, March 03, 2016 12:29 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: PQC forum

Dustin,

I've put together a start for the PQC project web pages. Do you want to get together to view at some point today? It's on my local machine, so……. You can swing by my office and have a look or I can bring my laptop to you. Let me know.

Attached is the text I used for the index.html page (taken directly from http://csrc.nist.gov/groups/ST/crypto-research-projects/#PQC). You may want to review and update.

Sara

From: Moody, Dustin (Fed)
Sent: Monday, February 29, 2016 11:38 AM

To: Kerman, Sara J. (Fed)
Cc: Chen, Lily (Fed); Foti, James (Fed)
Subject: RE: PQC forum

Sara,

Thanks. As for the webpage, I agree we can incorporate the research-project info into the new page. There's no rush on creating the webpage, as we are only at the beginning stage. As for what should be on it, We can have a link to our previous workshop. We have NISTIR 8105 that's out for public comment right now. We can have a link to the pqc-forum archives (and instructions how to subscribe). I gave a presentation at PQCrypto that is basically our announcement and outline of our Call for Submissions that we will be doing later this year. So we could put those slides (attached), or take information off of them and include it. We can have our email (pqc-comments@nist.gov) for contact. We will host a workshop in 2018, but we don't have all the details for that yet.

Dustin

From: Kerman, Sara J. (Fed)
Sent: Monday, February 29, 2016 11:29 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>; Foti, James (Fed) <james.foti@nist.gov>
Subject: RE: PQC forum

Hey Dustin,

Yes, I can send an email out to last years attendees. Not a problem—I'll send it out today.

I can do the page too (I'm looping Jim Foti in for information). There is currently a "Post-Quantum Cryptography" informational blurb at: http://csrc.nist.gov/groups/ST/crypto-research-projects/#PQC. I'm assuming you want a page dedicated to PQC and upcoming work/events, in which case, I believe we should remove the information found at the link I provided and incorporate it into the new site. We should discuss what information you anticipate including on the site (workshops, documents, etc.).

Sara

From: Moody, Dustin (Fed)
Sent: Monday, February 29, 2016 11:12 AM
To: Kerman, Sara J. (Fed)
Cc: Chen, Lily (Fed)
Subject: PQC forum

Sara,

Two things for you related to PQC.

- First, I set up a pqc-forum mailing list, and announced that at the PQCrypto Workshop last week. Unfortunately, I didn't learn from my experience with the ecc-forum, and didn't correctly tell people outside of NIST how to subscribe. Can we send an email to all the participants of our PQC workshop and let them know about the forum and how to subscribe? I'll contact the PQCrypto workshop people and see if I can get them to do the same. The instructions we need to give are below.
- Second, we should probably have a web page that will be devoted to the PQCrypto project, since we will be doing something somewhat akin to the SHA-3 contest (albeit on a slightly smaller scale). Who do I work with to get one created?

Thanks,

Dustin

PQC Workshop Attendees,

NIST has set up an pqc-forum@nist.gov mail listserve. You must be subscribed to send email to the listserve. For those outside of NIST, please use the instructions below to subscribe.

> To join:
> mailto:pqc-forum-request@nist.gov?subject=subscribe
> You will receive a response message from pqc-forum-request@nist.gov. Please reply to that message to confirm your subscription request.
> To unsubscribe:
> mailto:pqc-forum-request@nist.gov?subject=unsubscribe

The pqc-forum@nist.gov will be used to discuss the standardization and adoption of secure, interoperable and efficient post-quantum algorithms. In particular, the listserve will facilitate discussions about our upcoming Call for Submissions (see http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf and https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf). The messages from the mailing list will be archived online, and available to everyone at: https://email.nist.gov/pipermail/pqc-forum/.