From:	Chen, Lily (Fed)
To:	Scholl, Matthew A. (Fed)
Subject:	FW: Slides for RWC talk
Date:	Monday, January 9, 2017 9:36:14 AM
Attachments:	RWC2017.pptx

From: Rene Peralta <rene.peralta@nist.gov>
Date: Tuesday, January 3, 2017 at 8:17 AM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, Daniel Smith (b) (6), "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>, Lily Chen <lily.chen@nist.gov>, Stephen Jordan <stephen.jordan@nist.gov>, Yi-Kai Liu <yi-kai.liu@nist.gov>, "Miller, Carl A. (Fed)" <carl.miller@nist.gov>, Dustin Moody <dustin.moody@nist.gov>, Ray Perlner <ray.perlner@nist.gov>, "Smith-Tone, Daniel (Fed)" <daniel.smith@nist.gov>
Cc: "Regenscheid, Andrew (Fed)" <andrew.regenscheid@nist.gov>, Rene Peralta <rene.peralta@nist.gov>
Subject: Slides for RWC talk

Dear all,

I managed to delete all copies of my talk in Hanoi, so I made a new set of slides for tomorrow's talk at RWC (attached).

Any comments are most welcome.

Happy New Year, Rene.

NIST's Post-Quantum Cryptography Project

Rene Peralta
NIST PQC team

Real World Cryptography 2017

The Problem

- “Large” quantum computers would break most of our public-key crypto
  - RSA, Diffie-Hellman key exchange, elliptic curve crypto
- Symmetric crypto would be affected, but not broken
  - Keys will have to be longer.
- Full transition to alternatives takes a long time (possibly > 10 years).
- Long-term privacy and security implications …

NIST's PQC project

- To monitor progress in quantum computers and quantum algorithms.
- To find and standardize quantum-resistant alternatives for PKC, key-exchange, and digital signatures.
- To ensure transparency of the process and legitimacy of the outcome.

Not a Competition

- We hope at the end of the day there will be significant community consensus.
- We may standardize several algorithms.
- The evaluation criteria is not set in stone, it will probably evolve during the next few years.

The Call For Proposals

- Nominations for post-quantum candidate algorithms may now be submitted http://csrc.nist.gov/groups/ST/post-quantum-crypto/cfp-announce-dec2016.html

- Deadline is November 30, 2017

The PQC Forum

- The wording of the CFP followed public discussion on the pqc-forum (pqc-forum@nist.gov).
- This is also where submissions and germane issues - such as evaluation criteria - will be discussed.
- To join send mail to pqc-forum-request@nist.gov with subject=subscribe

How Things Look Like Now

- Signatures: hash-based , lattice-based, multivariate…
- PKE : lattice-based, code-based, multivariate, …
- Key agreement: PKE, isogeny-based, …

How Things Look Like Now

- Speed looks good.
- Key sizes may increase significantly.
- Some signature sizes look big.
- Possible significant increase in ciphertext size for short plaintexts.
- **We need industry to do an impact assessment.**

Public Discussion

- Ongoing discussion regarding “security-levels” and derived parametrization.
- Suspicion that NIST is just doing NSA’s bidding.
- Demands that future standards make bad implementations harder.

TIMELINE

Dec 20, 2016	Formal Call for Proposals 
Nov 30, 2017	Deadline for submissions
Early 2018	Workshop - Submitter's Presentations
3-5 years	Analysis Phase - NIST will report findings *1-2 workshops during this phase*
2 years later	Draft Standards ready

THANKS