NIST – Post Quantum Cryptography

Next session: Lily Chen and Dustin Moody from NIST

December 2016 Call for PQC proposals
November 2017 Round 1 submissions due
April 2018 1st Post Quantum Cryptography Standardization Workshop
January 2019 Round 2 announcement
April 2019 Round 2 re-submission deadline
August 2019 2nd Post Quantum Cryptography Standardization Workshop
September 2019 Projected a Round 3 announcement ~June 2020
American Standards Committee X9

  Background on quantum computing, its impact on cryptography, and in particular to financial information systems.

ASC X9 TR 50–2019 Quantum Techniques in Cryptographic Message Syntax (CMS), January 2019
  Focus on the impact to CMS, digital signatures and the use of hybrid methods.
NSF – Quantum Leap Challenge Institutes

Preliminary Proposals for $94 Million NSF QLCI Program

Conceptual Grants (CG): 12 – 15 awards for 12 months/max $150,000
Challenge Institute (CI): 1 – 3 awards for 5 years/max $5M/year

Round 1
3 June 2019: CG Proposals due
1 August 2019: CI preliminary proposals
2 January 2020: CI full proposal (invite only)

Round 2
1 September 2020: CI preliminary proposals
1 February 2021: CI full proposal (invite only)
Funding announcements

**August 2019:** Department of Energy announced $60.7* million to advance quantum computing.

- University of Maryland’s QuICS Receives $3.8 Million Award for QC Research
- Argonne National Laboratory Awarded $4.15 Million for Quantum Research
- ...

NSF Provides $4M Funding to Brown and Dartmouth for Quantum Research

NSF funds Quantum Foundry at UCSB with a $25 Million Grant
Computing Community Consortium (CCC)

Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility

Organizing Committee: David Ott (VMWare), Christopher Peikert (University of Michigan), and CCC personnel.

Migration
- Performance, security, minimize disruption and formal modeling

Agility needs
- Architectural frameworks, application, context, hardware acceleration

New capabilities
- MPC, partial homomorphic encryption, etc.
Host: Mozilla
Organizers: Dan Bernstein, Karthik Bhargavan, and Douglas Stebila

Focus on software implementations suitable for microcontrollers hybridization, experiments, verification, novel protocol implementations.

Outcomes: pqclean library, IETF draft Design issues for hybrid KEX for TLS 1.3
Quantum algorithms for analysis of public-key crypto

**Host:** American Institute of Mathematics

**Organizers:** Daniel J. Bernstein, Dan Boneh, Tanja Lange, and Michele Mosca

- Exact security of ECC and RSA under quantum attacks
- Quantum algorithms for generic post-quantum systems
- Quantum algorithms for post-quantum systems with extra structure

[https://aimath.org/pastworkshops/quantumalgrep.pdf](https://aimath.org/pastworkshops/quantumalgrep.pdf)
Simons Institute – Berkeley

Lattices: Algorithms, Complexity and Cryptography
14 January – 15 May 2020
https://simons.berkeley.edu/programs/lattices2020

Workshops:
- Lattices: Geometry, Algorithms and Hardness, 18 – 21 Feb 2020
- Quantum Cryptanalysis of Post-Quantum Cryptography, 22 – 24 Feb 2020
- Lattices: New Cryptographic Capabilities, 23 – 26 Mar 26 2020
- Lattices: From Theory to Practice, 27 Apr – 1 May 2020
Simons Institute – Berkeley

The Quantum Wave in Computing
14 January – 15 May 2020
https://simons.berkeley.edu/programs/quantum2020

Workshops:
  - Quantum Cryptanalysis of Post-Quantum Cryptography, 22 – 24 Feb. 2020
  - Quantum Algorithms, 25 – 28 Feb 2020
  - Quantum Protocols: Testing & Quantum PCPs, 30 Mar – 3 Apr 2020
  - Quantum Devices: Simulation, Supremacy, and Optimization, 4 – 8 May 2020
Experiments in hybrid post quantum

AWS
Deployed pq-TLS on AWS Key Management Service worldwide
Previously open sourced an OpenSSH pq-hybrid (via libOQS)

Cloudflare
Deployed a pq-hybrid TLS 1.3 with NTRU-HRSS and SIKEp434
https://blog.cloudflare.com/the-tls-post-quantum-experiment/

Microsoft
OpenSSH pq-hybrid with signatures (via libOQS)
OpenVPN pq-hybrid https://github.com/microsoft/PQCrypto-VPN
OpenSSL pq-hybrid with signatures (via libOQS)
Notable announcements

January 2019: IBM’s Q System One a 20-qubit (productionizing previous Q-system).

September 2019: IBM announced a new 53-qubit (Rochester Device)

October 2019: Google’s Nature Quantum Supremacy article about Sycamore, a 54-qubit processor to produce certifiably random numbers.
Thank you!

Matthew Campagna
campagna@amazon.com