# SaTC 2019 PI meeting breakout group report summary: Post-Quantum Cryptography

Co-leads: Jonathan Katz and Brian LaMacchia

# Problem/domain summary

- What is the topic?
  - How to ensure security of cryptosystems if large-scale quantum computers are built

- Why is it important to society? to a secure and trustworthy cyberspace? in other ways?
  - Existing public-key cryptosystems would be broken if large-scale, general-purpose quantum computers are built; several countries have large investments directed toward building quantum computers; limited understanding of security of existing cryptosystems against quantum adversaries
  - Post-quantum crypto also broadens the range of assumptions on which we can base cryptography
  - It is worth thinking about the relative importance of this problem (e.g., via a cost/benefit analysis) compared to other problems in cybersecurity

- Is there is an existing body of research and/or practice? What are some highlights or pointers?
  - NIST post-quantum standardization effort
  - There is a need for accessible material on PQC (and, to a lesser extent, quantum computing) so researchers can more easily enter the field
  - Tutorials at PQCrypto 2017

# Key research challenges

- What are important challenges that remain?  Are there new challenges that have arisen based on new models, new knowledge, new technologies, new uses, etc?
  - Expanding beyond lattice-based crypto, e.g., code-based crypto; tighter collaboration between math and crypto communities to study PQ assumptions
  - Reducing keysize in McEliece encryption
  - Looking beyond public-key crypto, e.g., info-theoretic cryptography (e.g., PIR), symmetric-key crypto (Kerberos), trusted hardware
  - Quantum cryptography (e.g., QKD); what else might be possible with quantum computers that is not possible classically (e.g., no-cloning, randomness verification)
  - Analysis of NIST candidates; (quantum) cryptanalysis of underlying hard problems; concrete security parameters
  - Performance evaluation of NIST candidates, given that there are many and they will be used for multiple applications
  - Faster evaluation methods, e.g., using hardware/software co-design, automatic hardware synthesis, …
  - Subversion resistance of PQ standards
  - “Fully-quantum” security proofs; “fully-quantum” perspective on foundational cryptography; quantum RO model, etc.
  - Quantum cryptanalysis of symmetric-key cryptography
  - Side-channel resistance of PQ schemes
  - “Advanced” PQC beyond the NIST standards (e.g., FHE, other applications)

# Key research challenges

- Formal verification techniques for (post-)quantum crypto/quantum adversaries; verification using quantum computers?
- Protocol level
  - Integrating PQ algorithms with, e.g., TLS, DNS, code signing, certificate hierarchies, …
  - "Hybrid" modes that couple post-quantum crypto with existing classical algorithms
  - Choosing a "diverse" set of standards (e.g., optimizing security, key size, computational efficiency, etc.) for different applications
- Systems level
  - Side-channel resistance
  - Crypto agility; making sure that it does not weaken security
  - How to write code supporting frequent changes in the underlying crypto
  - Automated code patching
  - How to design/build a "quantum internet," how to understand interactions between quantum and classical systems
- Quantum side channels(?)
- Estimations of running time/cost/timeline for quantum computers
- Hardware design for efficient post-quantum crypto

# Potential approaches

- Are there promising directions to addressing them?
  - Yes, many…

- What kinds of expertise and collaboration is needed (disciplines and subdisciplines)?
  - Collaborating between math and crypto communities
  - Collaborating between cryptographers and crypto engineers/implementers
  - Collaboration between cryptographers and quantum-computing experts/physicists for quantum cryptanalysis, and "fully quantum" security proofs
  - Hardware experts and cryptographers to ensure resistance to side-channel attacks
  - PL researchers and cryptographers to enable formally verified implementations, and ensuring constant-time code
  - Industry and academia
  - Building expertise through better educational offerings

# Long-term significance

- Will this domain/problem remain relevant in 10 years? if so, why?
    - Yes
        - Currently, large-scale quantum computers appear feasible (even if timeframe is unclear)
        - Even if large-scale quantum computers are never built (or shown to be infeasible), diversifying crypto assumptions is important and crypto agility will remain an issue (e.g., in IoT)
    - Even once NIST candidates are chosen, transition period is long (10+ years)
    - Even once NIST candidates are chosen, several important short-term and long-term questions remain
    - If quantum computing becomes a reality, how does CS/crypto education change?