Do we know what we think we know?
- A possible plan for standardizing PQC

Lily Chen
Computer Security Division, NIST
October 21, 2015
Publish a NIST Interagency Report (NISTIR) in FY16
  - Inform the government agencies and industry for the “upcoming” migration to Quantum Resistant Cryptography
  - Summarize the major results and progress in the area
  - Discuss challenges and potential issues in the migration

Challenges
  - May not be able to provide a definite timeline for the migration – Need constant update
  - May discourage the deployment of stronger cryptography in general – Need more detailed guidance on the strategy
Promote security analysis on existing PQC schemes through
- Research funding (FY15-16)
- Collaboration
- Workshop (FY17)
- Grow NIST research team

Challenges
- Many algorithm candidates – the set is too large
- Constant improvements – quite dynamic
- Lack of resource/motivation working on practical security in the research community
- **Call for proposals (FY16-17)**
  - Generate requirements and evaluation criteria for PQC standards proposals
  - Attract more resource to analyze a smaller pool

- **Challenges**
  - May not get consensus on requirements - Need constant updates on requirements
  - May not be able to make a time table – Need phased selection and standardization
  - May end up to select the “most promising” at the time and turn out something is even better afterward

---

**Move towards PQC standards**
- Research community
  - Security analysis, performance data

- Industry
  - Practical impact on each specific implementation

- Government agencies
  - Understand government needs

- Standard bodies
  - “Drop-in” case study, e.g. hash-based signature for code signing in TCG, TLS cipher-suite with post-quantum schemes in IETF, etc.

- International community
  - For general acceptance of PQC standards

Collaborations