POST-QUANTUM CRYPTOGRAPHY

Lily Chen

Computer Security Division

Information Technology Lab, NIST

NIST

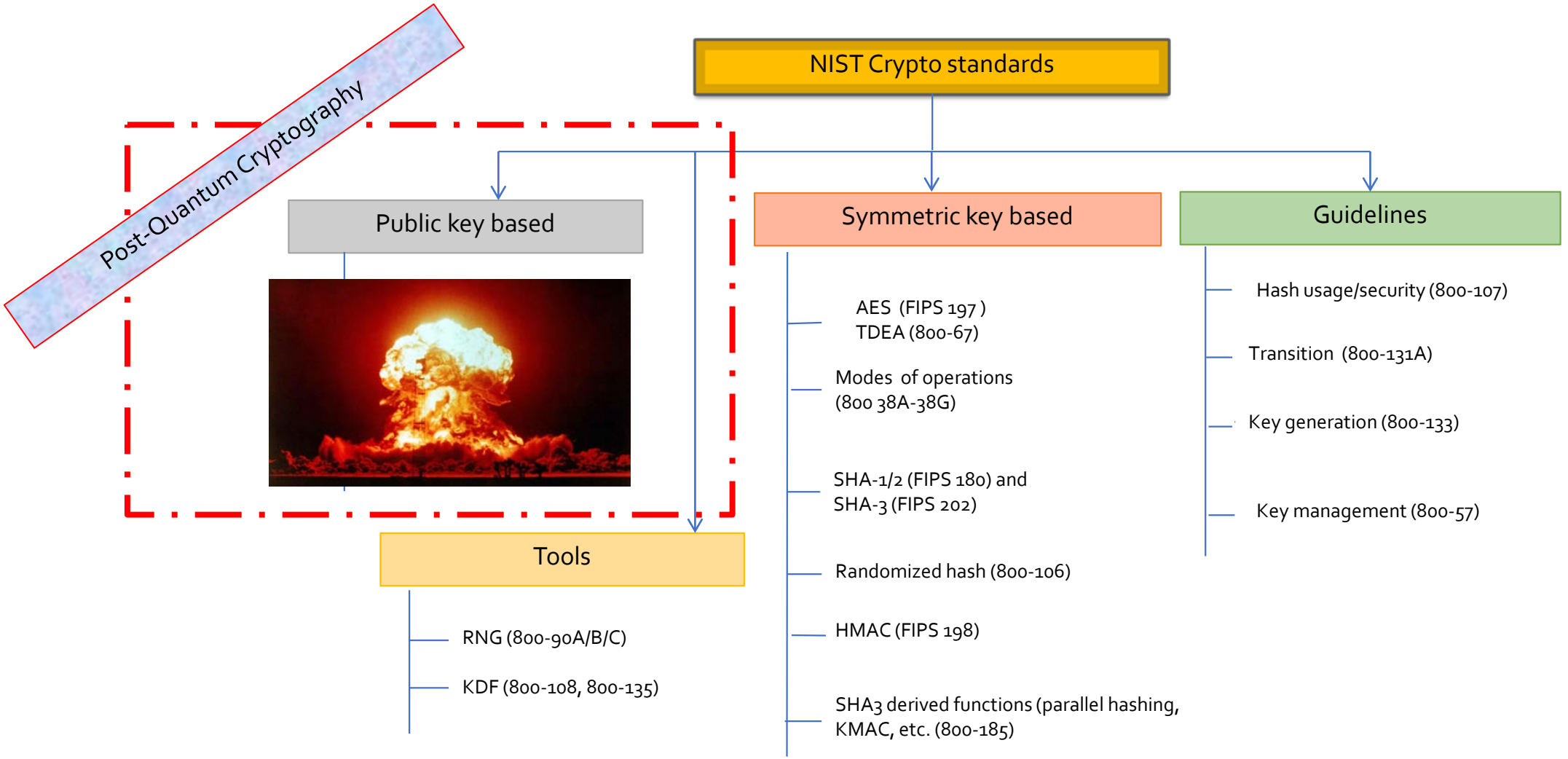
NIST Mission:
To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Information Technology Laboratory Mission:
Cultivating trust in IT and metrology.

Computer Security Division Mission:
Conduct research, development and outreach necessary to provide standards and guidelines, mechanisms, tools, metrics and practices to protect information and information systems.

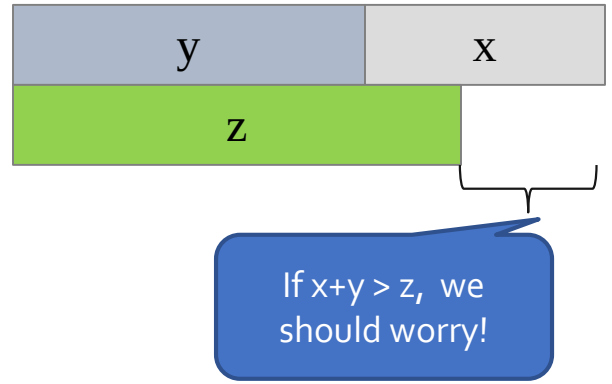
Crypto Technology Group Mission:
Research, develop, engineer, and standardize cryptographic algorithms, methods, and protocols.

Quantum Impact and NIST Standards



Timeline – Why Now?

- It has been a long debate among researchers and practitioners on whether it is too early to look into PQC standardization
- "A one-in-seven chance that some fundamental public-key crypto will be broken by quantum by 2026, and a one-in-two chance of the same by 2031" – Michele Mosca, U. of Waterloo)
- The experience tells that we need at least several years to developing and deploying PQC standards
- If we require 5-year backward secrecy, we certainly need to start standardization now



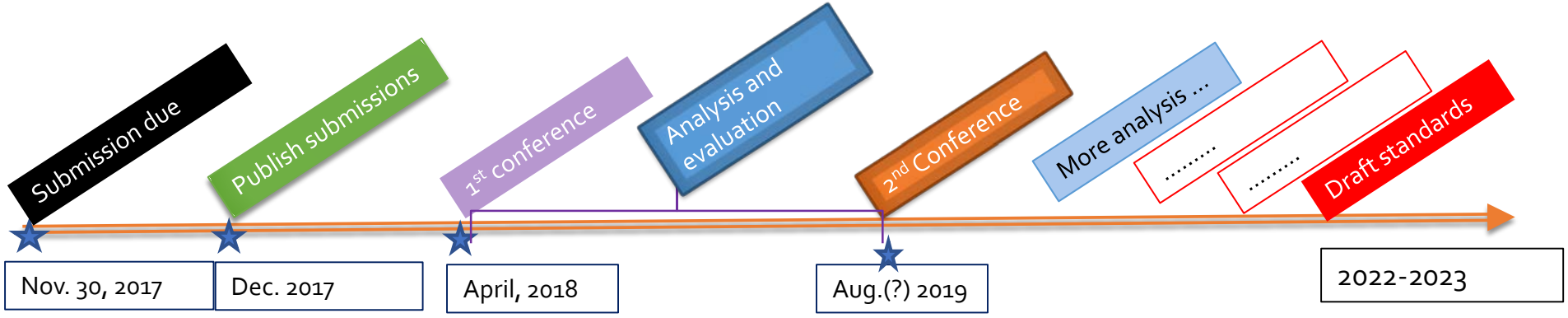
- y is the time taken for developing and deploying PQC standards
- x is the time for "backward secrecy" (maintain secrecy for the information encrypted x years ago)
- z is the time before quantum computers are available

NIST Milestones

- 2012 – NIST begins PQC project
  - Research and build NIST team
- April 2015 – 1st NIST PQC workshop
- Feb 2016 – NIST Report on PQC (NISTIR 8105)
- Feb 2016 – NIST preliminary announcement of standardization plan
- Aug 2016 – Draft submission requirements and evaluation criteria released for public comments
- Sep 2016 – Comment period ends
- Dec 2016 – Announcement of finalized requirements and criteria(Federal Register Notice)
- Nov. 30, 2017 - Submission deadline

NIST Plan in Developing PQC Standards

- NIST will post "complete and proper" submissions
- NIST PQC Standardization Conference (with PQCrypto, Apr. 2018)
- Initial phase of evaluation (12-18 months)
  - Internal and public review
  - No modifications allowed
- Narrowed pool will undergo a second round (12-18 months)
  - Second conference to be held
  - Minor changes allowed
- Possible third round of evaluation, if needed
- NIST will release reports on progress and selection rationale



National Quantum Initiative and Cybersecurity

- Cryptography is the corner stone of cybersecurity
- Transition from current deployed cryptosystems to quantum resistant systems is challenging
- Security analysis and performance assessment are extremely critical
- National quantum initiative should provide strong support for research in quantum resistant cryptography, a.k.a. post-quantum cryptography