TANGO WITH QUANTUM

- NIST PQC STANDARDIZATION UPDATE

LILY CHEN AND DUSTIN MOODY

CRYPTOGRAPHIC TECHNOLOGY GROUP

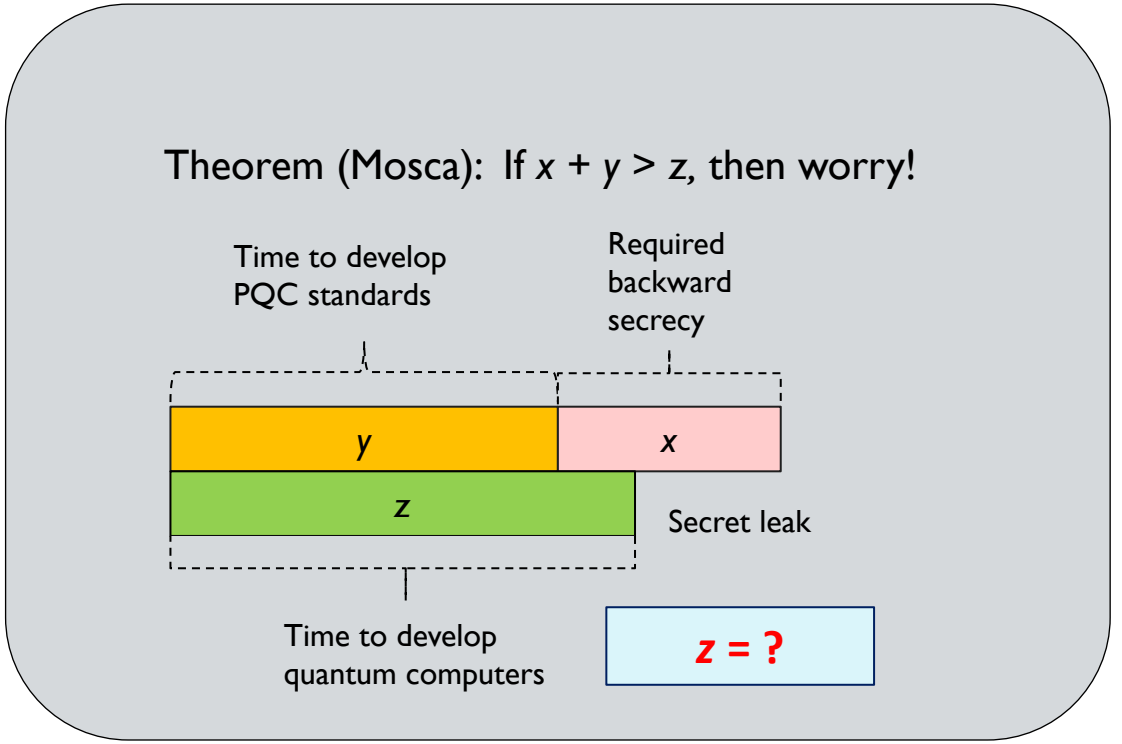
COMPUTER SECURITY DIVISION, INFORMATION TECHNOLOGY LAB

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

POST-QUANTUM CRYPTOGRAPHY AND QUANTUM COMPUTERS

- The debating about whether it is too early to look into PQC standardization will never end
  - **"There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031."**

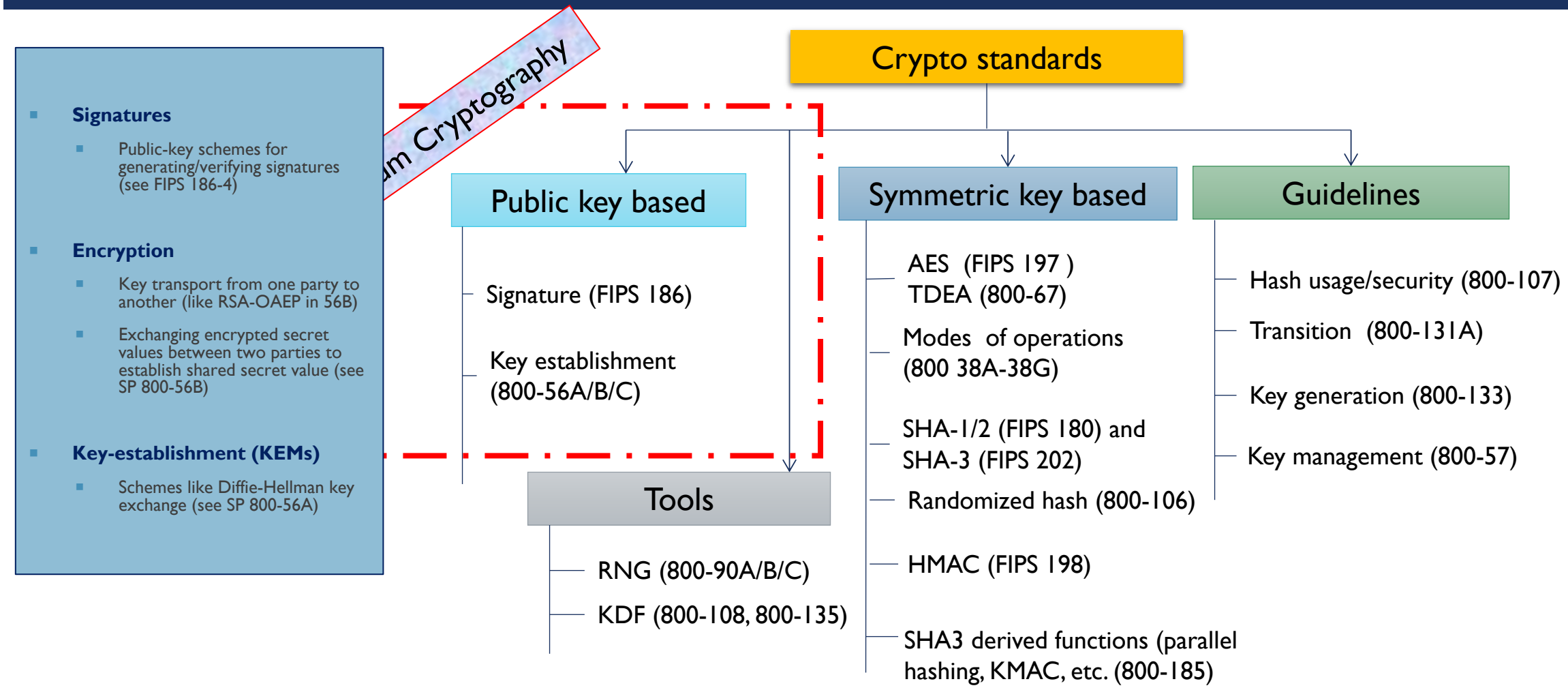
    – Dr. Michele Mosca, (April 2015)
- Progress has been made on quantum computers (*z* part) and so does PQC standardization (*y* part)
- This presentation focus on NIST PQC standardization
  - The scope and security requirements in Call For Proposals
  - The summary of the first round candidates
  - The 1st NIST PQC Standardization conference
  - What are the next steps
  - How should the application community be prepared



WHAT HAPPENED SO FAR?
- NIST PQC STANDARDIZATION REVIEW

- 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 call for proposals
  - Draft submission requirements and evaluation criteria released for public comments
- Dec 2016 – Announcement of finalized requirements and criteria(Federal Register Notice)
- Nov 2017 – Submission Deadline
- Dec 2017 – Announcement of the First Round Candidates
- April 2018 – The First NIST PQC Standardization Conference

SCOPE OF NIST PQC STANDARDIZATION



SECURITY CATEGORIES FOR SUBMISSIONS

Level	Security Description
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as SHA384 (collision search)
V	At least as hard to break as AES256 (exhaustive key search)

- Computational resources should be measured using a variety of metrics
- NIST asked submitters to focus on levels 1,2, and 3
  - Levels 4 and 5 for high security
- These are understood to be preliminary estimates
- Security definitions (proofs recommended, but not required) used to judge whether an attack is relevant
  - IND-CPA/IND-CCA2 for encryption, KEMS
  - EUF-CMA for signatures

SUBMISSIONS TO NIST CALL FOR PROPOSALS

- 82 total submissions received from 26 Countries, 6 Continents
  - The submitters in USA are from 16 States
- 69 accepted as "complete and proper" (5 since withdrawn)

	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate	7	2	9
Stateless Hash-based/Symmetric based	3		3
Other	2	5	7
Total	**19**	**45**	**64**

FIRST ROUND CANDIDATES

- Most submissions cover security levels 1,3, and 5
  - 10 submissions target only the lower levels 1,2,3
    - CFPKM, CompactLWE, Emblem/R.Emblem, NTRU-HRSS-KEM, PQRSA Enc/Sig, QC MDPC-KEM, Gravity-SPHINCS, HiMQ-3, RaCoSS
  - 7 submissions target only the high security levels 4,5
    - Classic McEliece, DME, GuessAgain, Hila5, Mersenne-756839, NTRUprime, KCL
- Most submitted schemes or previous versions of the submitted schemes have been published at the conferences or released through IACR eprint – In general, no big surprise
- Most submissions include proofs on the security CCA/CPA for Encryption/KEM and EUF-CMA for signatures
- Most submissions addressed the rationale for the selected parameters and mathematics structures as well as pros and cons for the schemes

ANALYSIS AND OFFICIAL COMMENTS

- Security analysis on submitted PQC schemes and related research topics have been active
  - Results have been published at conferences like PQCrypto 2018 and also release through IACR eprint
  - More analysis results have been announced through "Official Comments", which will lead to future publications
- At this stage, performance considerations will not play a major role in the evaluation process
  - In fact, it is even not possible to differentiate key size and performance as a general comparison among different families of submissions, say lattice-based vs. code-based
  - For a give family of submissions, e.g. lattice based family, the key sizes for different mathematics structures and different way to represent can be very different
- About 238 "Official Comments" received upon May 2nd, 2018
  - ~60% of these are on 10 submissions
- Comments can be questions to submitters or major attacks/breaks
  - 41 submissions have official comments
  - 23 submissions have none
  - 19 submissions have 2 or less

THE 1ST NIST PQC STANDARDIZATION CONFERENCE

- The 1st NIST PQC Standardization Conference was held in Ft. Lauderdale April 11-13, collocated with PQCrypto2018
- The conference accommodated 52 presentations covering 60 algorithms, attracted 345 attendees
  - We allow only 15 minutes for each submitted scheme (some even 10 minutes)
- We made a 30 minutes for discussions at the workshop on the following topics
  - measuring the complexity of quantum attacks
  - classical attack with super high memory,
  - the way to handle similar submissions, and
  - what constitutes unacceptable key sizes or performance
- Adi Shamir talked about his suggestions on NIST strategy on standardizing PQC at the discussion session
  - Developing new PKC is harder and riskier than SKC and there is no immediate need to widely deploy a winner
  - He suggested a three list approach: Research, Development, Production
    - The production list can remain empty until there is a real imminent threat from quantum computers

NIST TIMELINE AND REMARKS

- After the 1st NIST PQC Standardization Conference
  - Allow similar submissions to merge and submit before November 30
- 2018/2019 – 2nd Round begins (smaller number of submissions)
  - minor changes/tweaks allowed
- Aug 2019 – 2nd NIST PQC Workshop
- 2020/2021 - Select algorithms or start a 3rd Round
- 2022-2024 - Draft standards available

Some submitted algorithms may not be selected in the second round and neither be excluded for future consideration.

We may select one or two to standardize and leave others as 3rd round candidates and maintain a separate list for future consideration. It may not be the case to select winners and exclude all the others in one pass.

The standard development may last longer than two or three years based on the development of quantum computers and the maturity of the PQC algorithms.

FURTHER REMARKS ON THE STRATEGY AND TIMELINE

- We fully understand the complexity of developing PQC standards
- We need to deal with challenges including
  - Uncertainties in arrival of quantum computers (z = ?)
  - New attack techniques (classical and quantum)
  - New features/properties in PQC algorithms
  - …
- For an algorithm, some details may not be understood until put into a standard
  - How many times PKCS#1 padding schemes have changed due to attacks?
  - Every detail needs to be scrutinized before a standard can be deployed
  - The NIST timeline is not rushing to decisions but getting into the details

TRANSITION AND MIGRATION

- NIST will update guidance when PQC standards are available
  - Before that, follow the transition guideline as specified in NIST SP 800-131A
  - The future PQC transition shall not be an excuse to stay on weak crypto
  - The classical attacks can be efficient and can break your system – the pre-quantum security is equally important and more urgent
- A "hybrid mode" has been proposed as a transition/migration step towards PQC
  - Such a mode combines a classical algorithm with a post-quantum one
  - Besides "quantum resistant", it can provide some user experience for selected post quantum cryptography
  - Current FIPS 140 validation will validate the NIST-approved (classical) component
  - It is vendors/users decision whether to implement hybrid mode
- NIST plans to consider stateful hash-based signatures as an early candidates for standardization, but only for specific applications like code signing
  - Please let us know whether it is suitable for your application and how likely you will deploy it

WORK WITH OTHER STANDARD ORGANIZATIONS

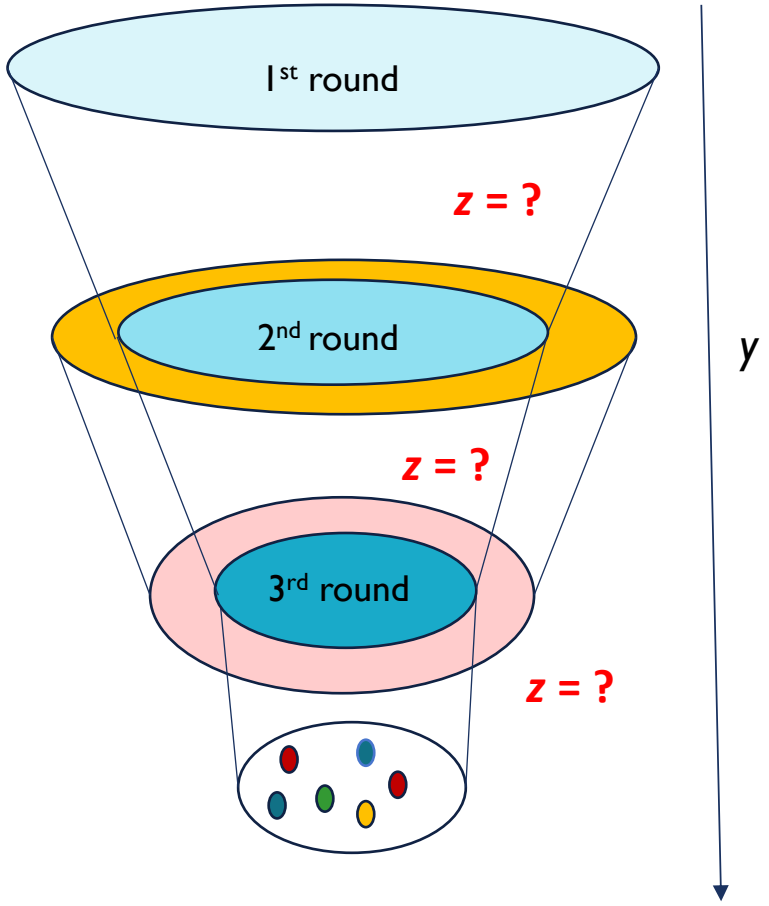
- We are aware that many standards organizations and expert groups are working on PQC
  - IEEE P1363.3 has standardized some lattice-based schemes
  - IETF is taking action in specifying stateful hash-based signatures
  - ETSI has released quantum-safe cryptography reports
  - EU expert groups PQCrypto and SafeCrypto made recommendations and released reports
  - ISO/IEC JTC 1 SC27 has already had 24 months study periods for quantum-resistant cryptography
- NIST is interacting and collaborating with these organizations and groups
  - Participate in X9 quantum risk study group
  - Lead the effort to developing a standing document (SD8) in ISP/IEC JTC 1 SC27 WG2 to prepare the group for future standardization activities

INPUT FROM APPLICATION COMMUNITY

- We need input from the application community about PQC candidates
- Tell us what you can or cannot handle in your applications with regard to key size, ciphertext size, signature size, key generation, decryption failure, processing complexity, etc.
- Discuss what is the possible barrier to migrate to post-quantum cryptography in your application
- Tell us your concerns with regard to the product cycle for implementing new cryptography algorithms
- Raise issues you can see on deploying post-quantum cryptography in your application environment
- Ask questions if you have any

SUMMARY

- Handling the uncertainties is the major challenge
- We will constantly check what is the progress on z=? and re-adjust our strategy?
- This is indeed a "competition" because we do compete with the progress in developing quantum computers
- We ask for input from application community to tell us what will make the applications work or not work
- Developing future proof cryptographic standards is the goal for the whole community



FOR FURTHER INFORMATION

- Join the discussion group pqc-forum at http://www.nist.gov/pqcrypto
- The 1st round candidates are posted at http://www.nist.gov/pqcrypto with presentations under the 1st NIST PQC Standardization Conference
- For comments, questions, or suggestions, send e-mail to pqc-comments@nist.gov