From: Moody, Dustin (Fed)
To: Liu, Yi-Kai (Fed); (b) (6) ; Perlner, Ray A. (Fed); Alperin-Sheriff, Jacob (Fed); (b) (6) ; daniel-c.smith@louisville.edu
Subject: 1st cut as Asiacrypt slides
Date: Monday, November 13, 2017 1:26:04 PM
Attachments: AsiaCrypt1.pptx

Yi-Kai, Ray, Jacob, Lily, Daniel,

I'm slated to give a 50 minute talk at Asiacrypt at the start of December. I figure it should be 45 minutes + 5 minutes for questions or so. I put together some slides for my first draft. Can you take a look and tell me what you think? I only have 36 slides, so I could certainly expand on some areas that I maybe only mentioned on one side. Let me know also if there are things I put in, that you don't think need to be there. Is there anything I didn't talk about that you think should get covered? Thanks,

Dustin

THE SHIP HAS SAILED

The NIST Post-Quantum Crypto "Competition"

Dustin Moody, NIST

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

BACKGROUND

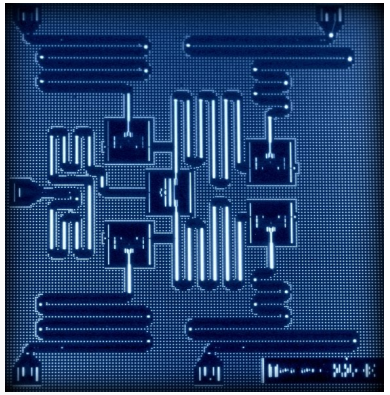
- The security of crypto relies on intractability of certain problems to modern computers
  - Example: RSA and factoring

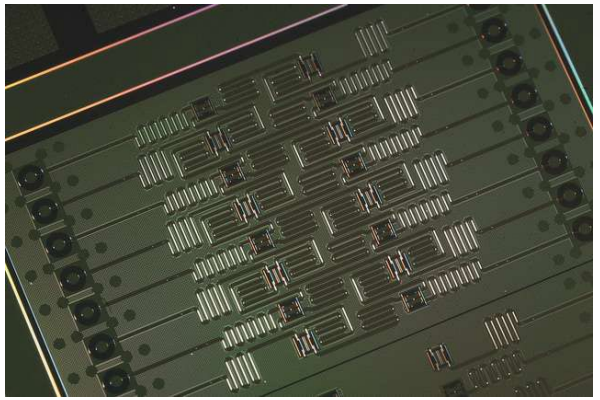
- Quantum computers
  - Exploit quantum mechanics to process information
  - Use quantum bits = "qubits" instead of 0's and 1's
  - Superposition – ability of quantum system to be in multiples states at the same time
  - Potential to vastly increase computational power beyond classical computing limit

QUANTUM COMPUTERS

- Difficulties
  - When a measurement is made on quantum system, superposition collapses
  - Quantum states are very fragile and must be extremely well isolated
  - Intersection of many developing fields: superconductors, nanotechnology, quantum electronics, etc…

- 1998 – 2 qubits
- 2000 – 4, 5, and then 7 qubits
- 2006 – 12 qubits
- 2011 – 14 qubits
- 2017 – 17, 49 qubits -> 56?
- Measuring qubits is not best metric



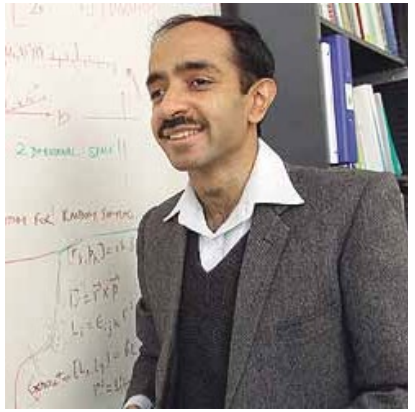


IBM's 5 qubit and 16 qubit processors

QUANTUM ALGORITHMS

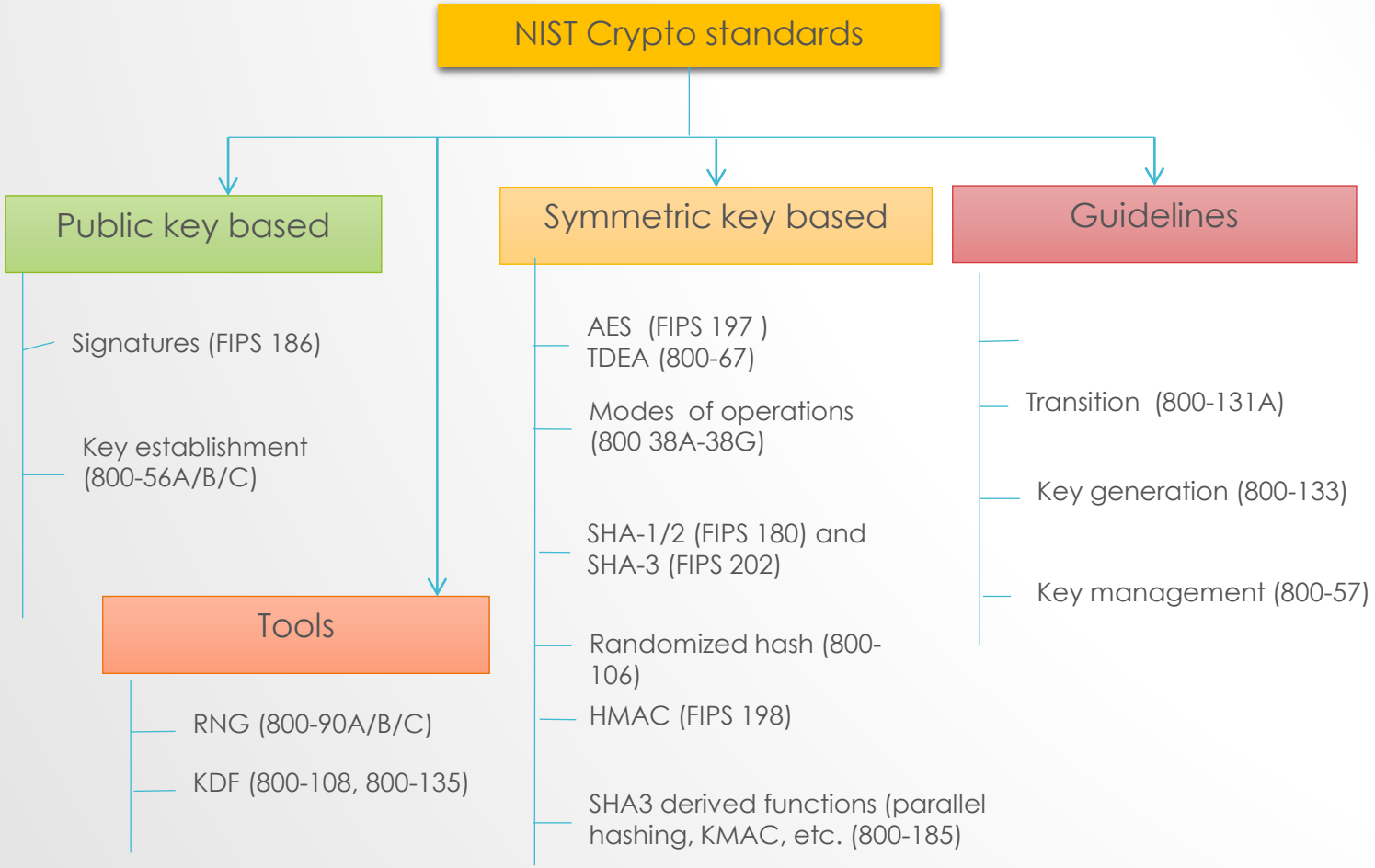
- 1994, Peter Shor created a quantum algorithm that would give an exponential speed-up over classical computers
  - Factoring large integers
  - Finding discrete logarithms

- Grover's algorithm – polynomial speed-up in unstructured search, from $O(N)$ to $O(\sqrt{N})$



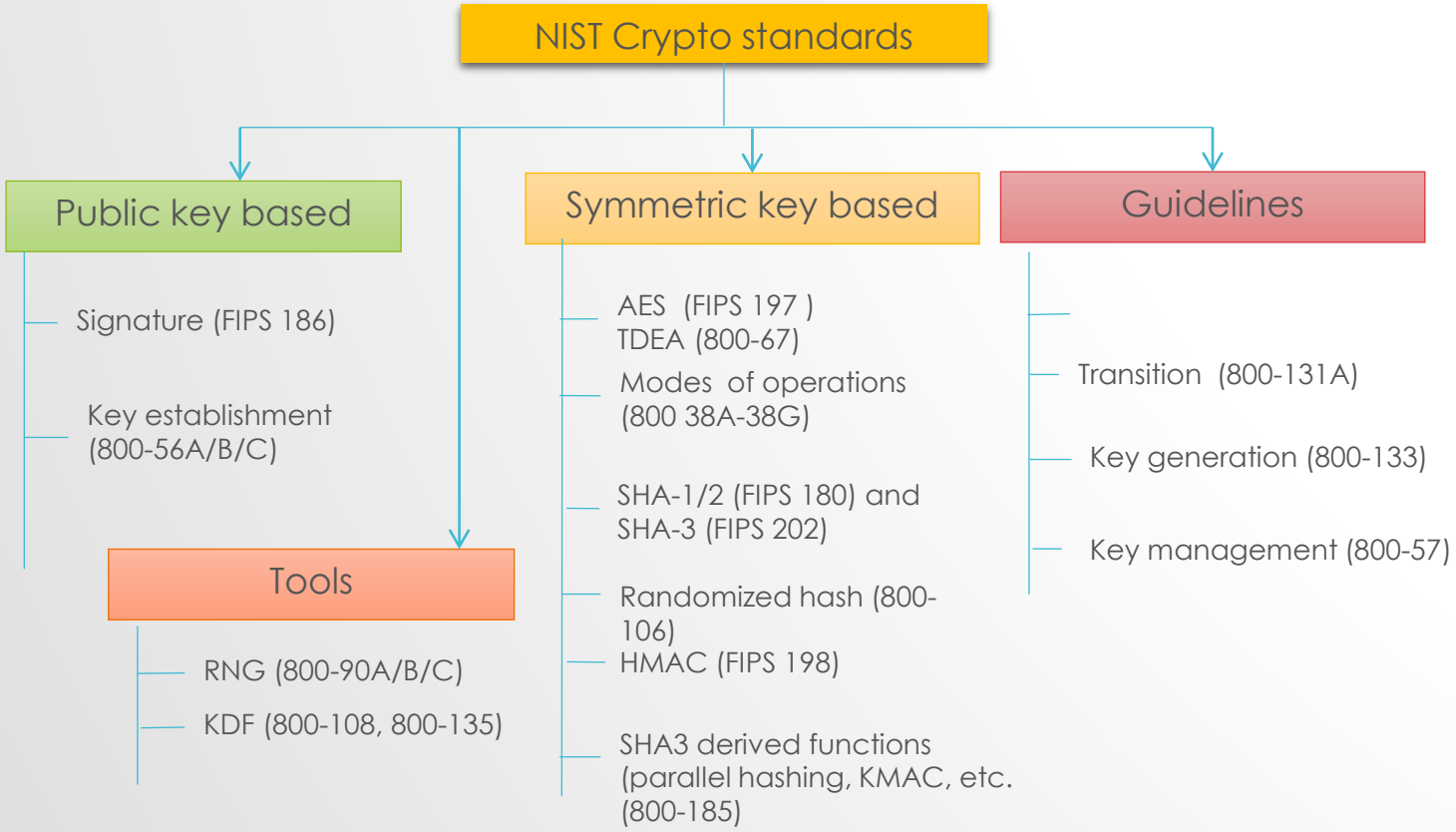
- Simulating the dynamics of molecules, superconductors, photosynthesis, among many, many others
  - see http://math.nist.gov/quantum/zoo

THE IMPACT ON CRYPTO



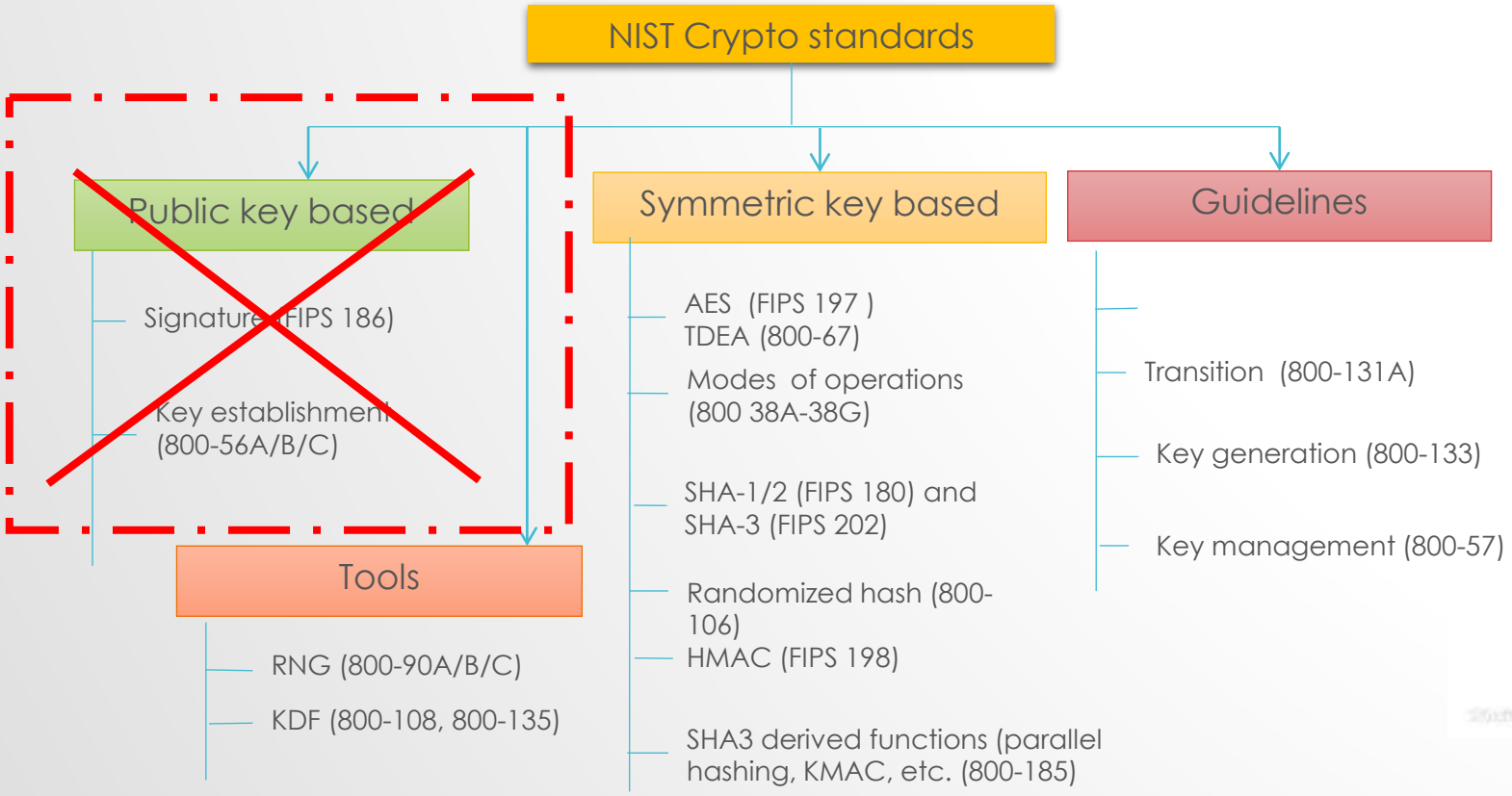
THE SKY IS FALLING?

- If a large-scale quantum computer could be built then….



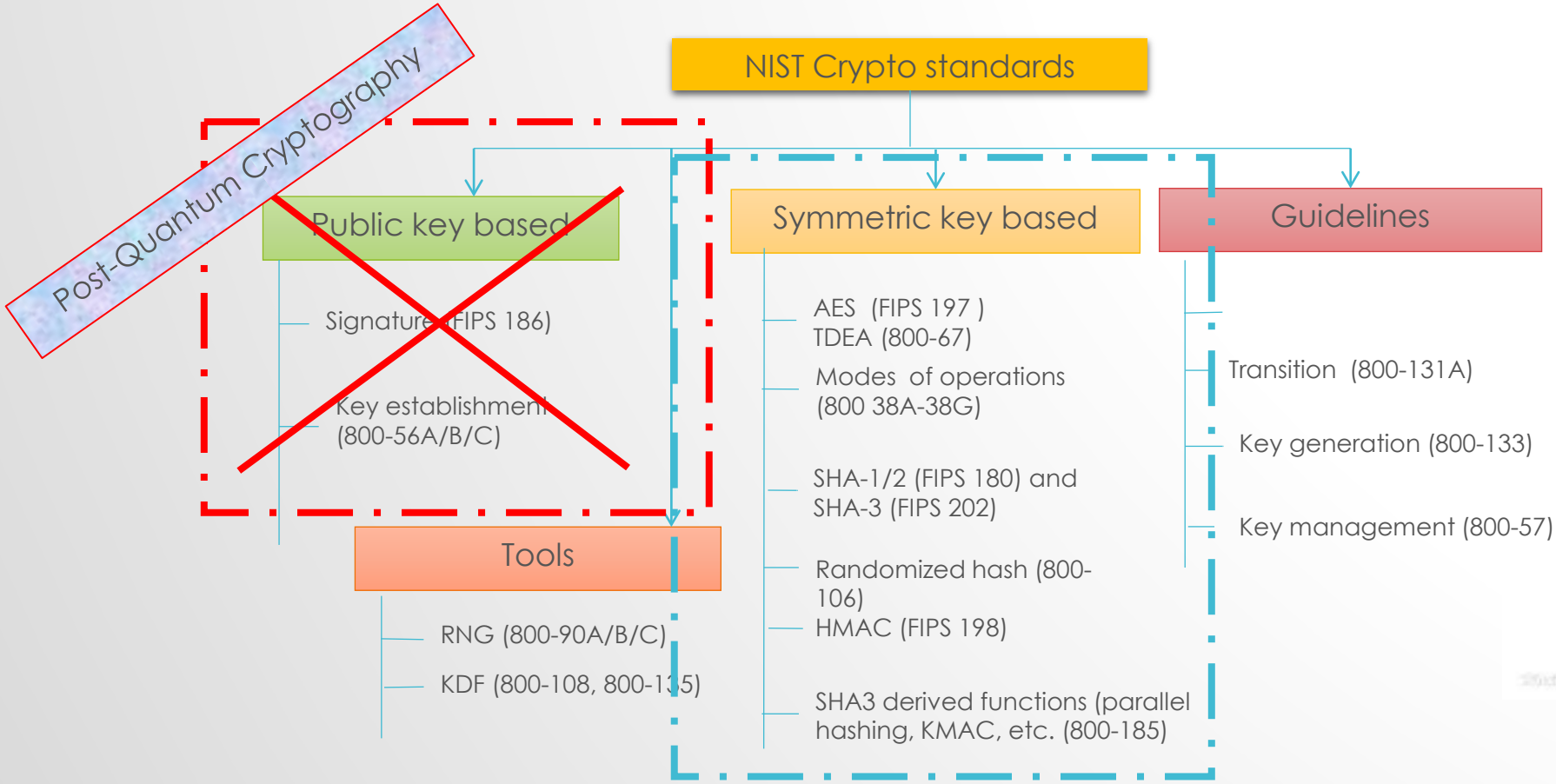
THE SKY IS FALLING?

- If a large-scale quantum computer could be built then….



THE SKY IS FALLING?

- If a large-scale quantum computer could be built then….

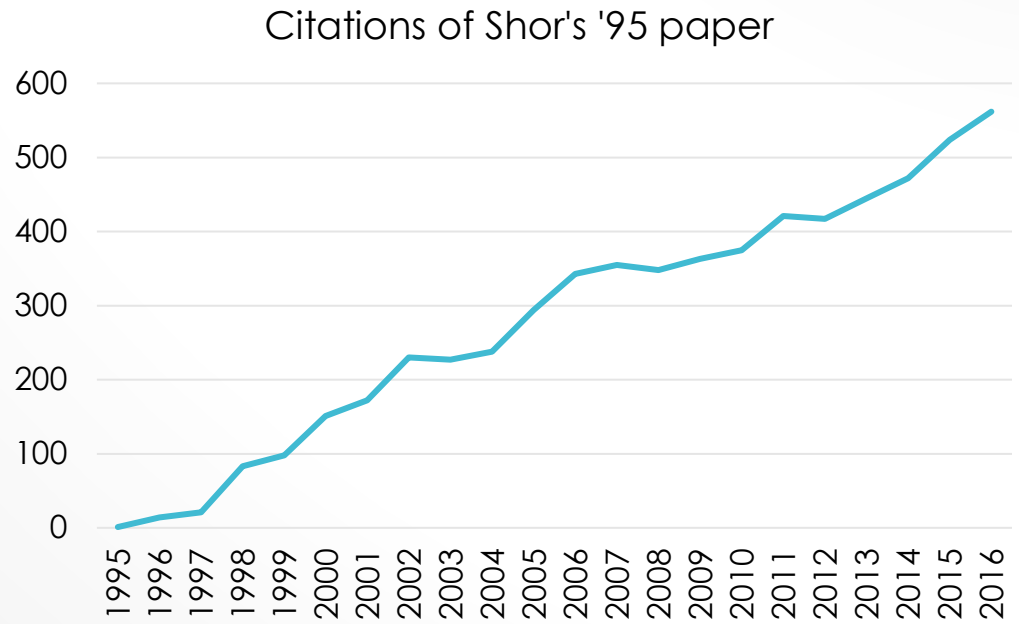


POST-QUANTUM CRYPTOGRAPHY (PQC)

- Cryptosystems which run on classical computers, and are considered to be resistant to quantum attacks

- PQC needs time to be ready
  - Efficiency
  - Confidence – cryptanalysis
  - Standardization
  - Usability and interoperability

    (IKE, TLS, etc… use public key crypto)

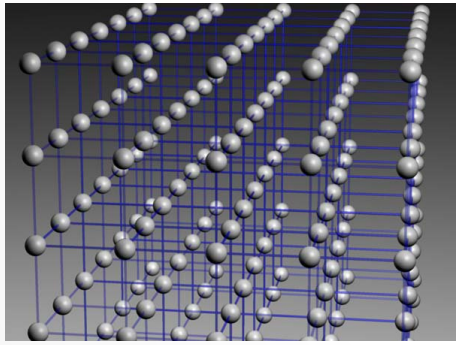


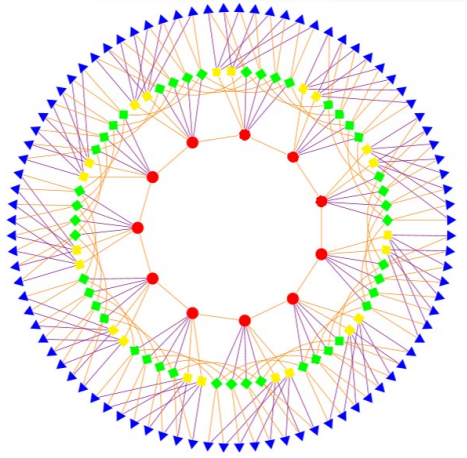
POSSIBLE REPLACEMENTS

- Lattice-based
- Code-based
- Multivariate
- Others
  - Hash-based signatures
  - Isogeny-based
  - Etc….

- All have their pros and cons

01010111 01101001 01101011
01101001 01110000 01100101
01100100 01101001 01100001





$$
\begin{aligned}
f_1(x_1,\ldots,x_n) &= \sum_{1\le i\le j\le n} a_{ij}^{(1)} x_i x_j + \sum_{1\le i\le n} b_i^{(1)} x_i + c^{(1)} = d_1,\\
f_2(x_1,\ldots,x_n) &= \sum_{1\le i\le j\le n} a_{ij}^{(2)} x_i x_j + \sum_{1\le i\le n} b_i^{(2)} x_i + c^{(2)} = d_2,\\
&\vdots\\
f_m(x_1,\ldots,x_n) &= \sum_{1\le i\le j\le n} a_{ij}^{(m)} x_i x_j + \sum_{1\le i\le n} b_i^{(m)} x_i + c^{(m)} = d_m,
\end{aligned}
$$

PQC STANDARDIZATION - TOO EARLY?

- There has been much debate whether it is too early to look into PQC standardization
- When will a (large-scale) quantum computer be built?
  - **"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."**

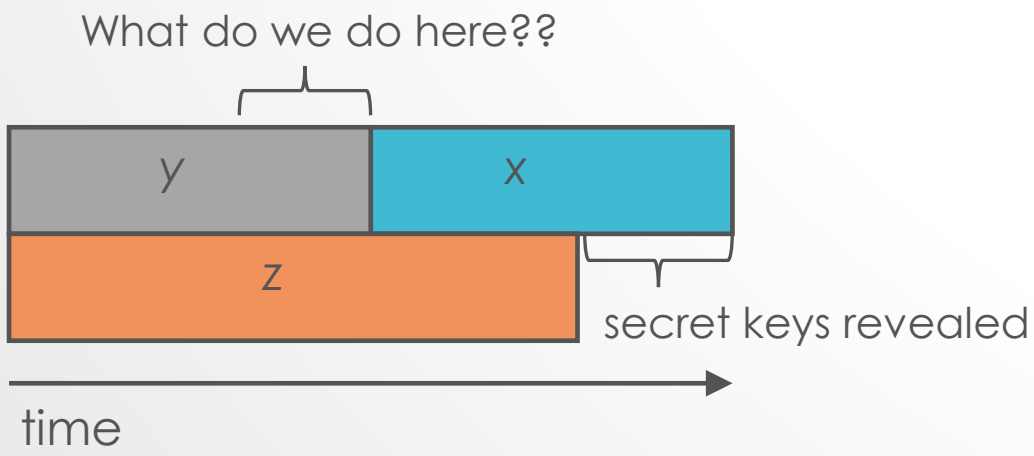
  – Dr. Michele Mosca, U. of Waterloo

- Our experience tells that we need (at least) several years to develop and deploy PQC standards

HOW SOON DO WE NEED TO WORRY?

- How long does your information need to be secure (x years)
- How long to re-tool with a quantum safe solution (y years)
- How long until a large-scale quantum computer is built (z years)

Theorem (Mosca): If x + y > z, then worry!



NSA ANNOUNCEMENT

- Aug 2015 - NSA's Information Assurance Directorate updated its list of Suite B cryptographic algorithms

  - **"IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms."**

- Standardization is the first step towards the transition

THE DECISION TO MOVE FORWARD

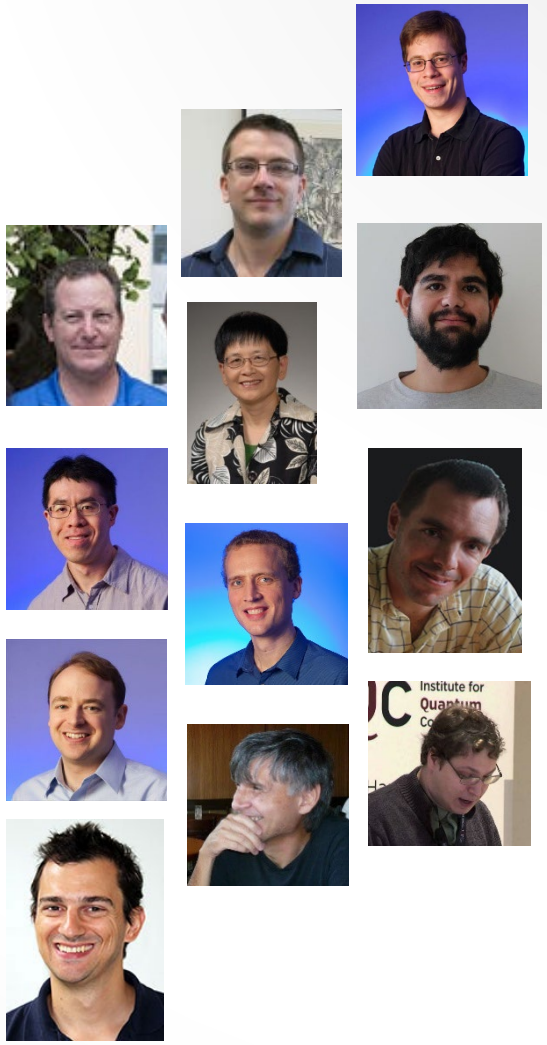
- NIST decided **it is the time** to look into standardization
- We see our role as managing a process of achieving community consensus in a **transparent** and **timely** manner
- We do not expect to "pick a winner"
  - Ideally, several algorithms will emerge as 'good choices'

WHAT WE HAVE DONE SO FAR – THE FIRST MILE IN A LONG JOURNEY

- ~ 2012 – NIST begins PQC project
  - Research and build NIST team
- April 2015 – 1st NIST PQC workshop
- Aug 2015 – NSA statement
- 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 ended
- Dec 2016 – Finalized requirements and criteria (Federal Register Notice)
- Nov 2017 – Deadline for submissions

THE NIST PQC TEAM

- Consists of 12+ NIST researchers in crypto, quantum information, quantum algorithms
- Hold bi-weekly seminars (internal and invited speakers)
- Publish results in journals/conferences
- Engage with research community
- Work with industry and standards organizations (ETSI, IETF, ISO/IEC SC27)
- Reach government agencies for raising awareness of upcoming cryptography transition
- Collaborate with QuiCS at the Univ. of Maryland, as well as Univ. of Waterloo



NIST'S PQC ~~CONTEST~~ STANDARDIZATION PLAN

Timeline	
Nov. 30, 2017	Submission deadline
April 2018	Workshop – Submitters' presentations
3-5 years	Analysis phase - NIST reports on findings and more workshops/conferences
2 years later	Draft standards available for public comments

- NIST will post "complete and proper" submissions - Dec 2017
- 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

SCOPE

- Signatures
  - Public-key signature schemes for generating and verifying digital signatures (FIPS 186-4)
- Encryption
  - Key transport from one party to another
  - Exchanging encrypted secret values between two parties to establish shared secret value (see SP 800-56B)
- Key-establishment (KEMs)
  - Schemes like Diffie-Hellman key exchange (see SP 800-56A)

DIFFERENCES WITH AES/SHA-3 COMPETITIONS

- Post-quantum cryptography is more complicated than AES or SHA-3
  - No silver bullet - each candidate has some disadvantage
  - Not enough research on quantum algorithms to ensure confidence for some schemes
- We do not expect to "pick a winner"
  - Ideally, several algorithms will emerge as "good choices"
- We will narrow our focus at some point
  - This does not mean algorithms are "out"
- Requirements/timeline could potentially change based on developments in the field

MINIMAL ACCEPTABILITY REQUIREMENTS

- Publicly disclosed and freely available during the process
  - Signed statements, disclose patent info
- Implementable in wide range of platforms
- Provides at least one of: signature, encryption, or key exchange
- Theoretical and empirical evidence providing justification for security claims
- Concrete values for parameters meeting target security levels

THE SELECTION CRITERIA

- Security - against both classical and quantum attacks
- Performance - measured on various "classical" platforms
- Other properties
  - Drop-in replacements - Compatibility with existing protocols and networks
  - Perfect forward secrecy
  - Resistance to side-channel attacks
  - Simplicity and flexibility
  - Misuse resistance, and
  - More

COMPLEXITIES OF PQC STANDARDIZATION

- Much broader scope – three crypto primitives
  - Signatures, Encryption, Key agreement
- Both classical and quantum attacks
  - Security strength assessment on specific parameter selections
- Consider various theoretical security models and practical attacks
  - Provably security vs. security against instantiation or implementation related security flaws and pitfalls
- Multiple tradeoff factors
  - Security, performance, key size, signature size, side-channel resistance countermeasures
- Migrations into new and existing applications
  - TLS, IKE, code signing, PKI infrastructure, and much more
- Not exactly a competition – it is and it isn't

SECURITY ANALYSIS

- Security definitions
  - IND-CPA/IND-CCA2 for encryption, KEMS and EUF-CMA for signatures
  - Used to judge whether an attack is relevant
- Quantum/classical algorithm complexity
  - Classical computers are not going away, and may have the cheapest attacks in practice
  - Stability of best known attack complexity
  - Precise security claim against quantum computation
  - Parallelism?
- Security proofs (not required but considered as support material)
- Quality and quantity of prior cryptanalysis

QUANTUM SECURITY – HOW TO ASSESS IT?

- No clear consensus on best way to measure quantum attacks
- Uncertainties
  - The possibility that new quantum algorithms will be discovered, leading to new attacks
  - The performance characteristics of future quantum computers, such as their cost, speed and memory size
- Currently, NIST crypto standards specify parameters for classical security levels at 112, 128, 192, 256 bits
- For PQC standardization, need to specify concrete parameters with security estimates

QUANTUM SECURITY STRENGTH CATEGORIES

	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
  - Number of classical elementary operations, quantum circuit size, etc…
  - Consider realistic limitations on circuit depth (e.g. 2^{40} to 2^{80} logical gates)
  - May also consider expected relative cost of quantum and classical gates.
- These are understood to be preliminary estimates
  - Submitters need not provide parameters for all levels

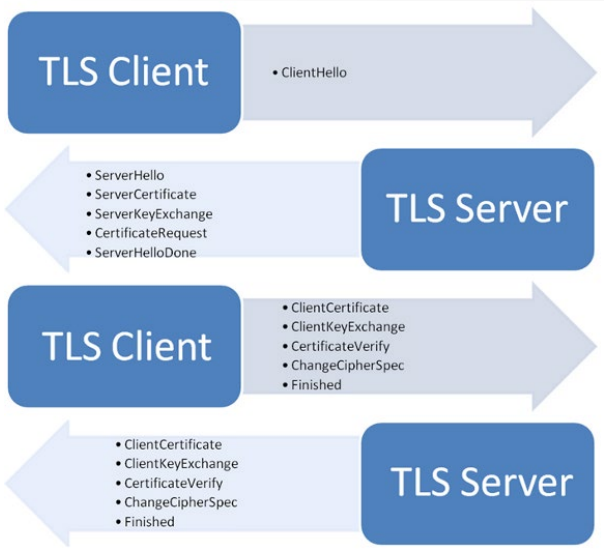
COST AND PERFORMANCE

- Standardized post-quantum cryptography will be implemented in "classical" platforms
- Ideally, implementable on wide variety of platforms and applications
- May need to standardize more than one algorithm for each function to accommodate different application environments
    - from extremely processing constrained devices to limited communication bandwidth
- Allowing parallel implementation for improving efficiency is certainly a plus

- Preliminary conclusions: efficiency likely OK, but key sizes may pose a significant challenge

DROP-IN REPLACEMENTS

- We're looking for drop-in replacements for existing applications, e.g. IKE and TLS
  - Key establishment
    - Ideally, we'd like to have something to replace Diffie-Hellman key exchange
    - Practically, we have to look into some schemes such as encryption with one-time public key, which are not quite drop-in replacements
  - Signatures
    - We'd like to have signatures with reasonable public key size, signature size, and fast signature verification
    - Practically, we shall prepare to handle probably larger public keys, or/and larger signatures, (and to handle a stateful situation)
- We need to be realistic about what we can get



CHALLENGES

- Uncertainties – Quantum Security
- Assess classical security
  - Most of PQC schemes are relatively new
  - It'll take years to understand their classical security
- We need to deal with new situations which we haven't considered before, e.g.
  - Decryption failure
  - State management for hash based signatures
  - Public-key encryption vs. key-exchange issues
    - Public-key encryption IND-CCA2
    - Ephemeral key exchange (no key-pair reuse, consider passive attacks, IND-CPA)
  - Auxiliary functions/algorithms, e.g.
    - Gaussian simulation
- We have to move away from many things we have been used with existing schemes

SUMMARY OF COMMENTS RECEIVED

- 26 comments submitted
  - Clarifications in the text of the Call For Proposals
  - Require constant-time implementations?
  - More implementation platforms
  - Intellectual Property requirements
  - Decryption failure threshold
  - Public-key encryption and key-exchange issues (KEMs)
  - Quantum security and target security levels
  - API suggestions

PRELIMINARY SUBMISSIONS

- Submitters who sent us their algorithms by Sept. 30th were able to have their submissions checked for "completeness"
- 37 submissions received
  - 10 signature schemes
  - 27 Encryption/KEM schemes

  - 15 were lattice-based
  - 7 were code-based
  - 5 were multivariate
  - The rest were a mix (hash-based, isogenies, ….)

- From 15 states, 18 countries, and 5 continents

FINAL SUBMISSIONS RECEIVED

- The deadline is past – no more submissions
- X submissions received
  - X signature schemes
  - X Encryption/KEM schemes

  - X were lattice-based
  - X were code-based
  - X were multivariate
  - The rest were a mix (hash-based, isogenies, ….)

- From X states, Y countries, and Z continents

TRANSITION AND MIGRATION

- NIST will update guidance when PQC standards are available
  - SP 800-57 specifies classical security levels 128, 192, and 256 bits are acceptable through 2030
- Even with the upcoming PQC transition, anything with classical security less than 112 bits should NOT be used anymore
- 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
  - Current FIPS 140 validation will only validate the NIST-approved (classical) component
  - The PQC standardization will only consider the post-quantum component

INTERACTIONS WITH STANDARDS 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 three six months study periods for quantum-resistant cryptography

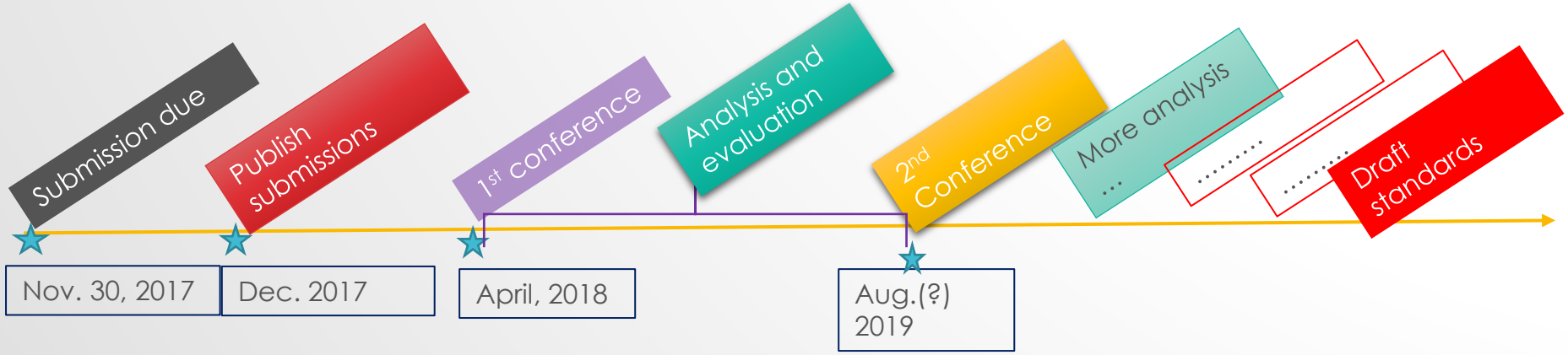
- NIST is interacting and collaborating with these organizations and groups
- NIST plans to consider hash-based signatures as an early candidates for standardization, but probably just for specific applications like code signing

DISCUSSIONS AND QUESTIONS

- Since the draft call for proposals was announced, the NIST team has actively interacted with submitters and researchers
- The questions include
  - APIs to support different ancillary functions
  - Using third party libraries
  - Submission format
  - etc.
- The topics discussed at pqc-forum@nist.gov include
  - Quantum vs. classical security strength
  - Security notions (IND-CCA2, IND-CPA, etc.)
  - Random number generator
  - Key exchange vs. key encapsulation
  - Implementation details, etc…..
- Answers to the common questions and summaries on the major discussion topics were added to the FAQ at www.nist.gov/pqcrypto

WHAT TO EXPECT NEXT?

- NIST will post "complete and proper" submissions for analysis at www.nist.gov/pqcrypto as soon as possible
- The 1st NIST PQC Standardization Conference (co-located with PQCrypto, April 2018)
  - For submitters to present their algorithms and design rationale
  - For researchers and practitioners to ask questions on the submitted algorithms
- Evaluation and analysis continue (16~18 months)
- The 2nd NIST PQC Standardization Conference will likely be Aug/Sept 2019



SUMMARY

- Quantum computers have HUGE potential
- Post-quantum cryptography standardization is going to be a long journey
- We have already observed many complexities and challenges, with more to come.
- Be prepared to transition to new algorithms in 10 years
- We will continue to work with the community towards PQC standardization

See www.nist.gov/pqcrypto

Sign up for the pqc-forum for announcements and discussion