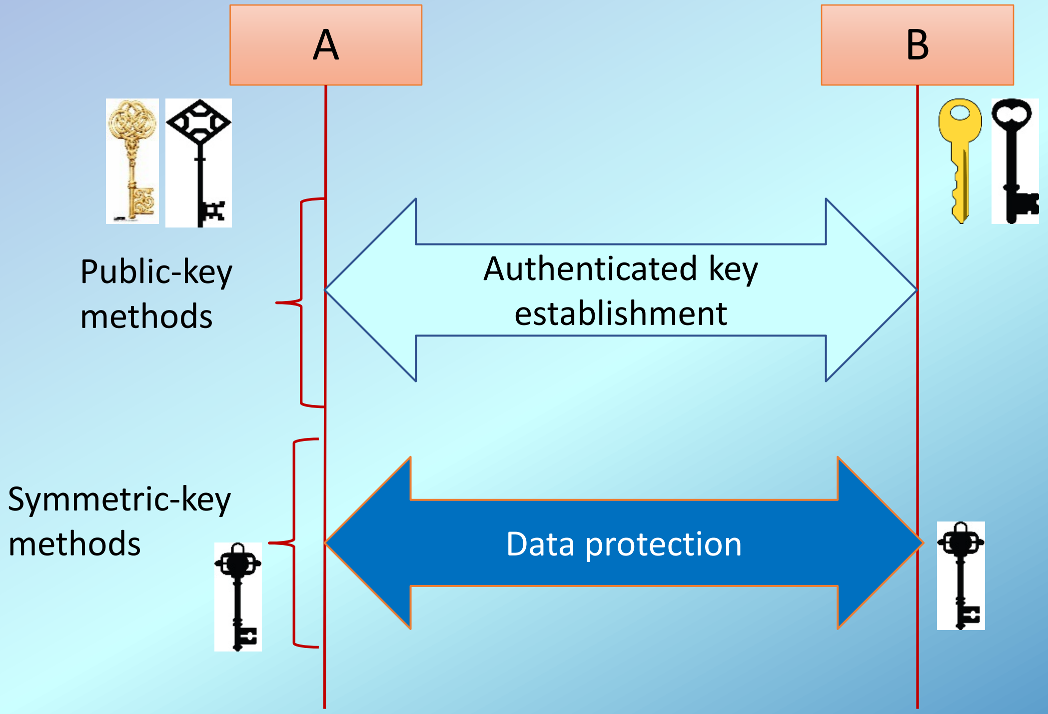
NIST Post-Quantum Cryptography Standardization

Lily Chen
Computer Security Division, Information Technology Lab
National Institute of Standards and Technology (NIST)

Cryptography for Secure Communications

- Use public key cryptography to establish keys and authenticate users through signatures
  - Diffie-Hellman Key Exchange
  - RSA and ECDSA signatures
- Use symmetric key cryptography to encrypt and authenticate bulk data
  - AES (CBC, GCM, etc.)
  - HMAC (SHA-2, SHA-3)
- Examples
  - Transport Layer Security (TLS)
  - Internet Key Exchange (IKE) + IPsec



Security of RSA, Diffie-Hellman, and ECDSA

- RSA encryption and RSA signature is based on the hardness of factorization
  - Given an integer n, find two primes p and q such that $n = pq$
- Diffie-Hellman key exchange and ECDSA is based on the hardness of discrete logarithm
  - Give y and a generator g of group G, find an x such as $g^x = y$

Hardness

- The hardness means that no algorithm on classical computers has been published that can factor all integers in polynomial time and the same for finding discrete logarithm
  - The complexity of factoring integer *n* is an exponential function of *ln n*

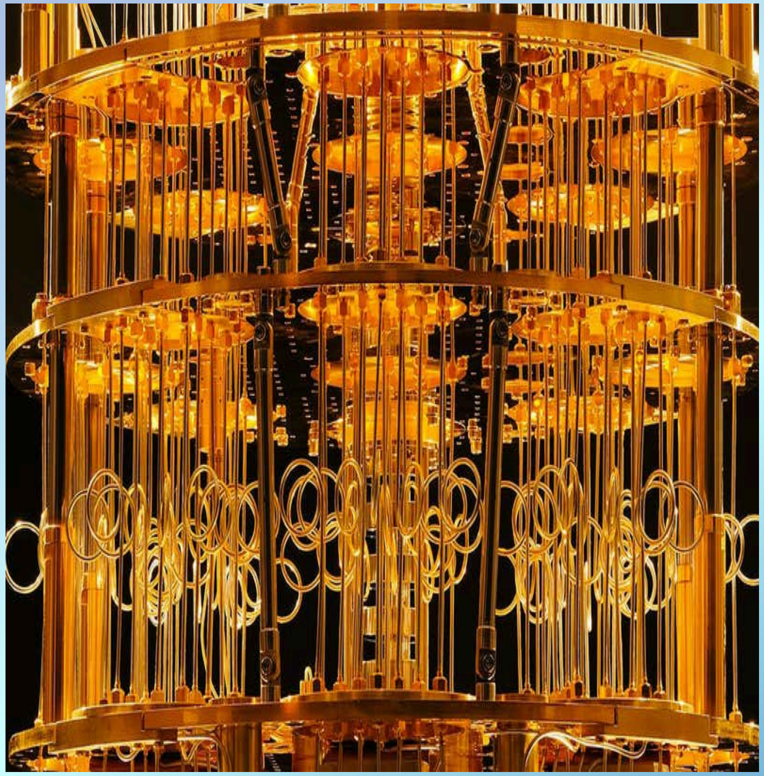
$$\exp\left(\left(\sqrt[3]{\frac{64}{9}} + o(1)\right) (\ln n)^{\frac{1}{3}} (\ln \ln n)^{\frac{2}{3}}\right)$$

6 = 2 x 3
143 = 11 x 13
2021 = 47 x 43
19043 = 137 x 139
… …

RSA-250: *2700 core-years using Intel Xeon Gold 6130 at 2.1 GHz to factor an 829-bit integer - February 2020.*

Quantum Impact to Cybersecurity

- Quantum computing changed what we have believed about the hardness of discrete log and factorization problems
  - By Shor’s algorithm, they can be solved by quantum computers in polynomial time
- The well-deployed public - key cryptosystems, RSA, Diffie-Hellman, ECDSA, will need to be replaced to prepare for quantum era
- Quantum computing also impacted security strength of symmetric key based cryptography algorithms – manageable by increasing key size

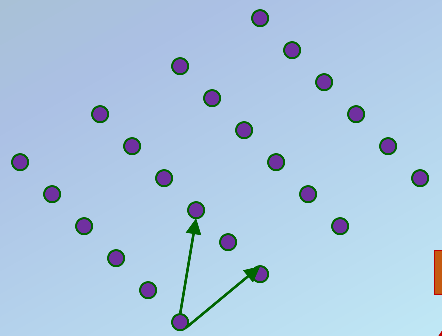


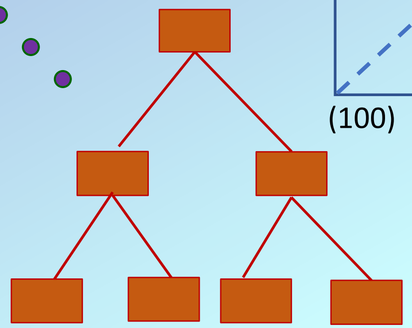
How to Deal with Quantum Attacks?

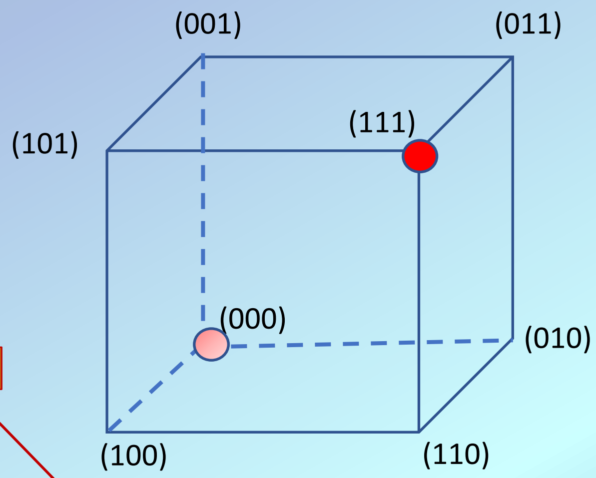
- Need to find cryptographic algorithms which are secure against attacks by both classical and quantum computers
  - The algorithms must be based on hard problems which are hard for both classical and quantum computers
- In other words, we need quantum resistant cryptography, named by the researchers as post-quantum cryptography (PQC)
- Clarification
  - Post-quantum cryptographic algorithms are supposed to be implemented in "classical" computers in the same way as RSA, DH, and ECDSA
  - It is different from Quantum Key Distribution (QKD), which relies on quantum mechanics to distribute keys

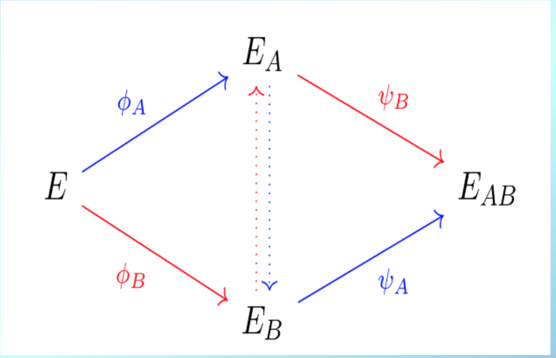
Post Quantum Cryptography (PQC)

- PQC has been a very active research area in the past decade
- Some actively researched PQC categories include
  - Lattice-based
  - Code-based
  - Multivariate
  - Hash/Symmetric key -based signatures
  - Isogeny-based schemes



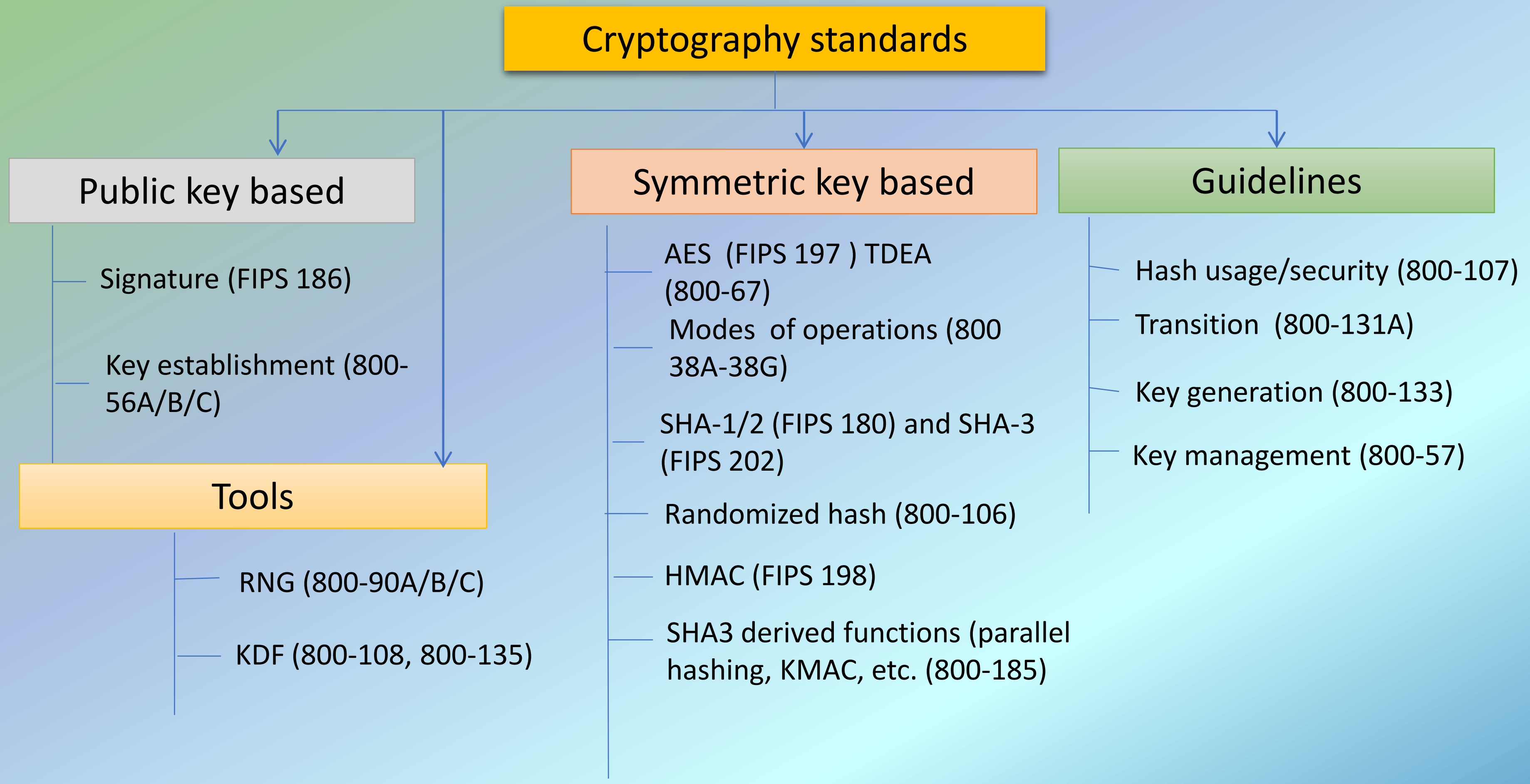






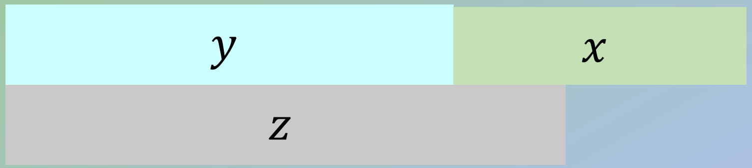
$$
\begin{aligned}
p^{(1)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)}\cdot x_i + p_0^{(1)}\\
p^{(2)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(2)}\cdot x_i + p_0^{(2)}\\
&\vdots\\
p^{(m)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(m)}\cdot x_i + p_0^{(m)}
\end{aligned}
$$

NIST Cryptographic Standards – A Glance



Why Should We Start to Develop PQC Standards Now?

If $y + x > z$, then we should worry.
- Michele Mosca



y – time for PQC standardization and adoption

x – time of maintaining data security

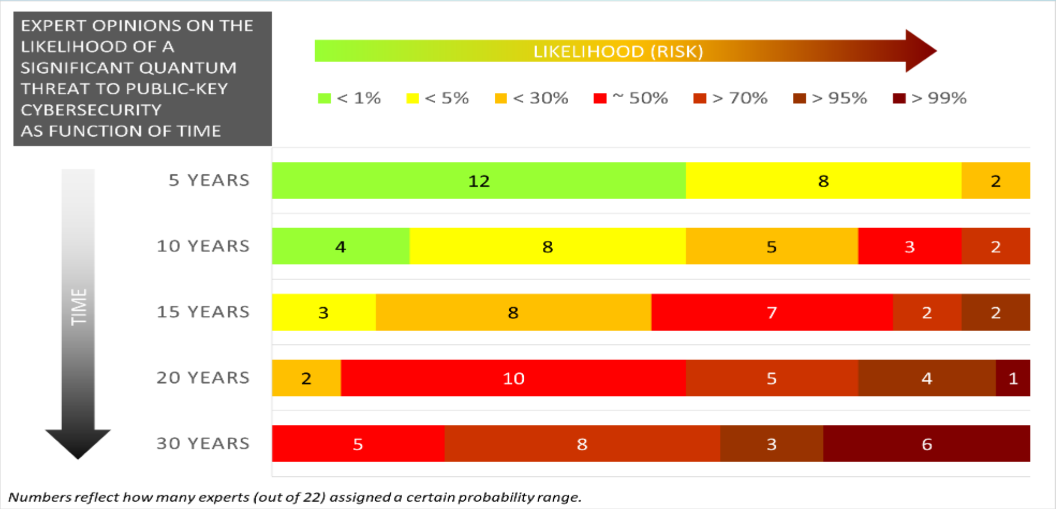
z – time for quantum computers to be developed

What is z?

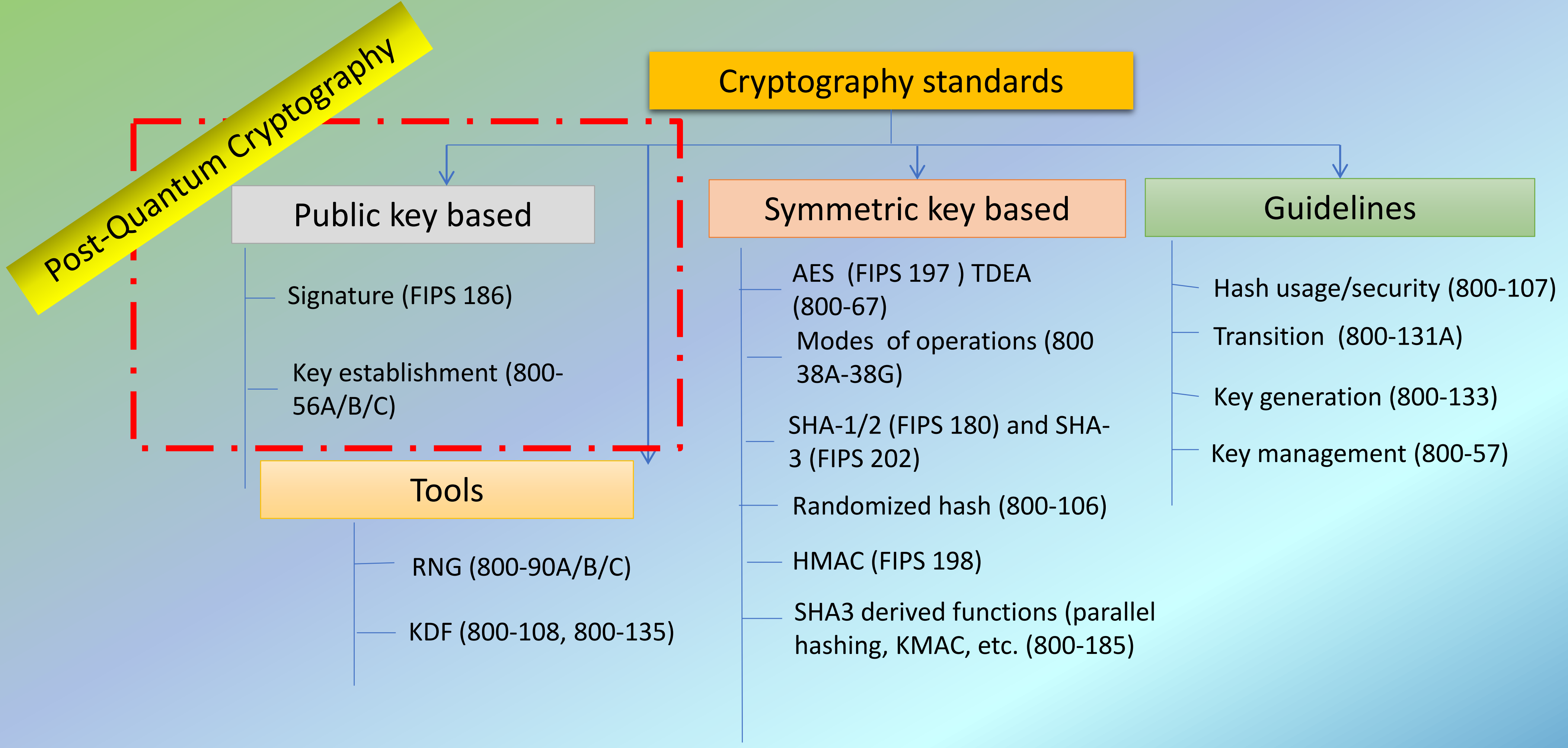
- **2020**, M. Mosca: "There is a 1 in 5 chance that some fundamental public-key crypto will be broken by quantum by 2029."

Quantum Threat Timeline

See survey at
https://globalriskinstitute.org/publications/quantum-threat-timeline/



NIST PQC Standards - Scope



NIST PQC Standards – Milestones and Timeline

2016 Criteria and requirements and call for proposals

2017 Received 82 submissions and announced 69 1st round candidates

2018 The 1st NIST PQC standardization Conference

2019
Announced 26 2nd round candidates

The 2nd NIST PQC Standardization Conference

2020 Announced 3rd round 7 finalists and 8 alternate candidate

2021
The 3rd NIST PQC Standardization Conference

2022-2023 Release draft standards and call for public comments

2024 Publish PQC Standards

The First, Second, and Third Round Candidates

1st round	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-bas			
Multi-var			
Stateless Hash/Sym			
Other			
Total			

2nd round	Signatures	KEM/Encryption	Overall
Lattice-based	3	9	12
Code-based		7	7
Multi-va			
Stateles based			
Isogeny			
Total			

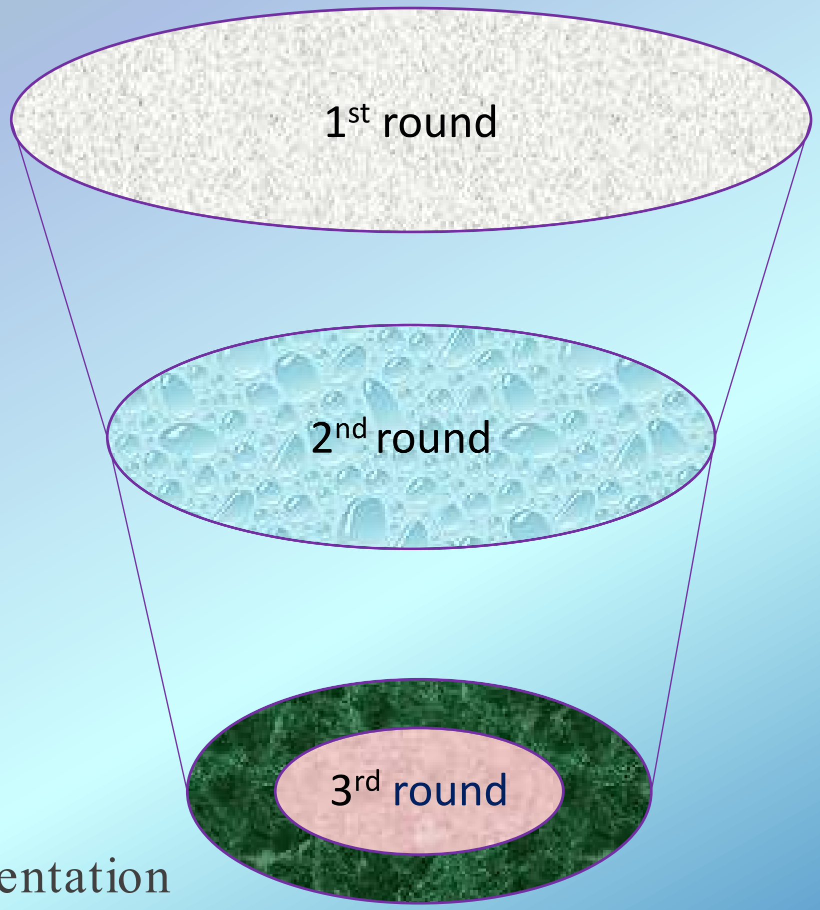
3rd round	Signatures		KEM/Encryption		Overall	
Lattice-based	2		3	2	5	2
Code-based			1	2	1	2
Multi-variate	1	1			1	1
Stateless Hash or Symmetric based		2				2
Isogeny				1		1
Total	3	3	4	5	7	8

Considerations in Selecting Algorithms

- Security
  - Classical and quantum complexity
    - security levels offered
  - (confidence in) security proof
  - Any attacks

- Performance
  - Size of parameters
  - Speed of KeyGen, Enc/Dec, Sign/Verify
  - Tradeoffs

- Other characteristics
  - IP issues
  - Side-channel resistance
  - Simplicity and clarity of documentation
  - Flexible



Community effort

- NIST received 82 submissions from 25 countries and 6 continents
  - A lot design teams consist of researchers from multiple countries
  - Academic and industry researchers collaborate
- Evaluate and analyze candidates
  - Research publications at conferences and journals (e.g. PQCrypto, Crypto, Eurocrypt, CHES, etc. each has multiple sessions on PQC)
  - Official comments - Over 300 official comments in the first round evaluation
  - E-mail discussions at pqc-forum – 926 posts in the first round
  - Benchmarks – community contributions e.g. SUPERCOP, OpenQuantumSafe, etc.
- Prepare for transition
  - Many implementations of PQC candidates in well deployed protocols, e.g. TLS
  - International and industry standards initiatives (e.g. ISO/IEC JTC1 SC27, IEEE-SA, IETF, ETSI, etc.)
  - The National Cybersecurity Center of Excellence (NCCoE) has a project for Migration to PQC - work with industry partners

Thanks

- Check out www.nist.gov/pqcrypto
- Sign up for the pqc-forum for announcements & discussion
- Contact us at: pqc-comments@nist.gov