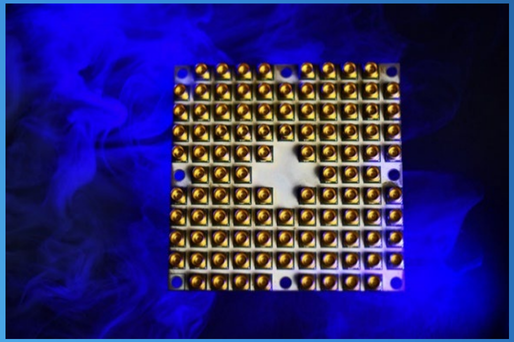
Preparing for Quantum: Understand How Quantum Computing Will Change Cyber Attacks

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

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 multiple states at the same time
- Potential to vastly increase computational power beyond classical computing limit
- Limitations:
  - When a measurement is made on quantum system, superposition collapses
  - Only good at certain problems
  - Quantum states are very fragile and must be extremely well isolated
  - Intersection of many developing fields: superconductors, nanotechnology, quantum electronics, etc…

IBM's 50-qubit quantum computer
November 2017

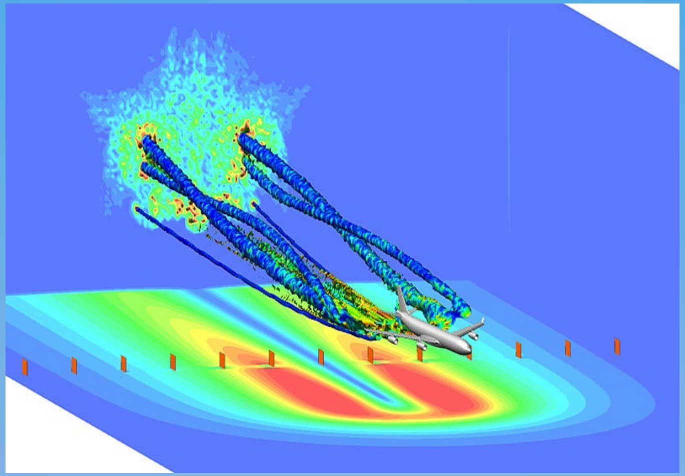


Intel's 49-qubit chip "Tangle-Lake"
January 2018

Google's 72-qubit chip "Bristlecone"
March 2018

Quantum Computers – New Paradigm

Design new materials and drugs



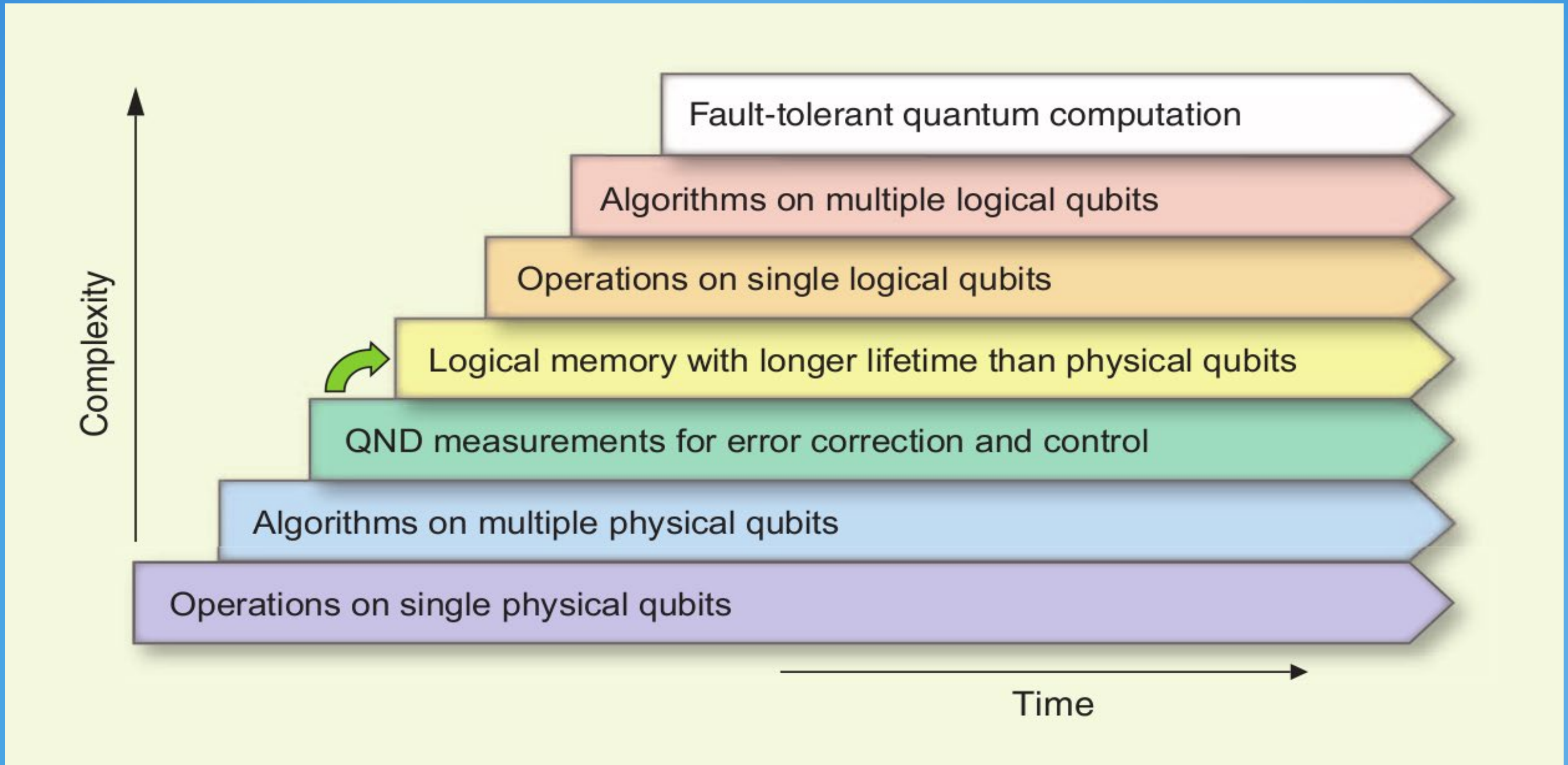
Simulation and data processing

Sensing and measuring

- Known to solve many problems previously thought to be intractable

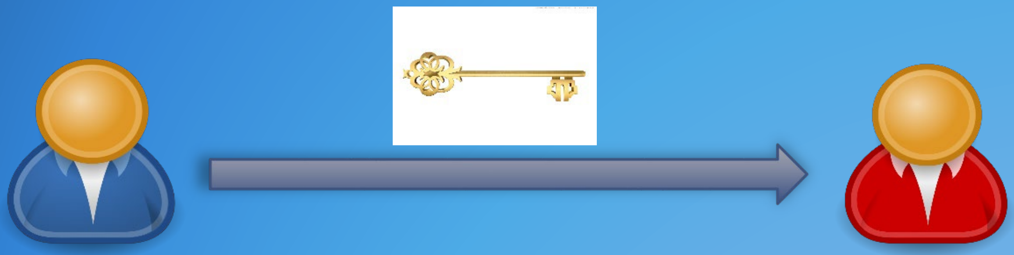
Quantum Computing Progress

- A lot of progress, but still a long way to go

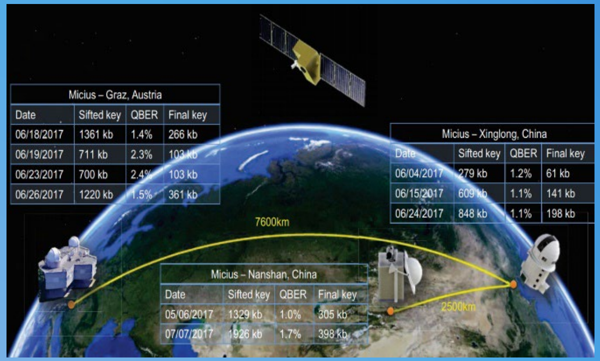

Fault-tolerant quantum computation
Algorithms on multiple logical qubits
Operations on single logical qubits
Logical memory with longer lifetime than physical qubits
QND measurements for error correction and control
Algorithms on multiple physical qubits
Operations on single physical qubits
Complexity
Time

[Image credit: M. Devoret and R. Schoelkopf]

Quantum Key Distribution



- Using quantum mechanics to enable two parties to share a random secret key
- It can solve key distribution problem when quantum interface is available in a pairwise manner
- Today's many-to-many network such as Internet uses public key cryptography to establish keys for data protection



Micius – Graz, Austria

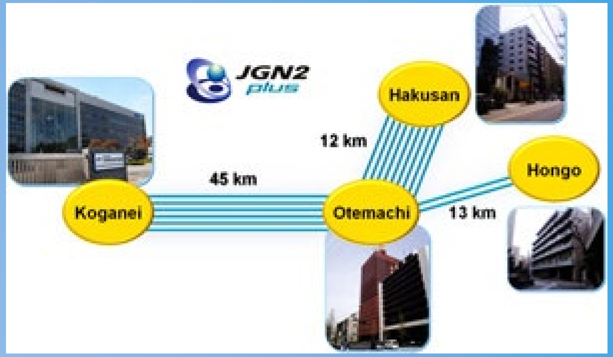
Date	Sifted key	QBER	Final key
06/18/2017	1361 kb	1.4%	266 kb
06/19/2017	711 kb	2.3%	103 kb
06/23/2017	700 kb	2.4%	103 kb
06/26/2017	1220 kb	1.5%	361 kb

Micius – Xinglong, China

Date	Sifted key	QBER	Final key
06/04/2017	279 kb	1.2%	61 kb
06/15/2017	609 kb	1.1%	141 kb
06/24/2017	848 kb	1.1%	198 kb

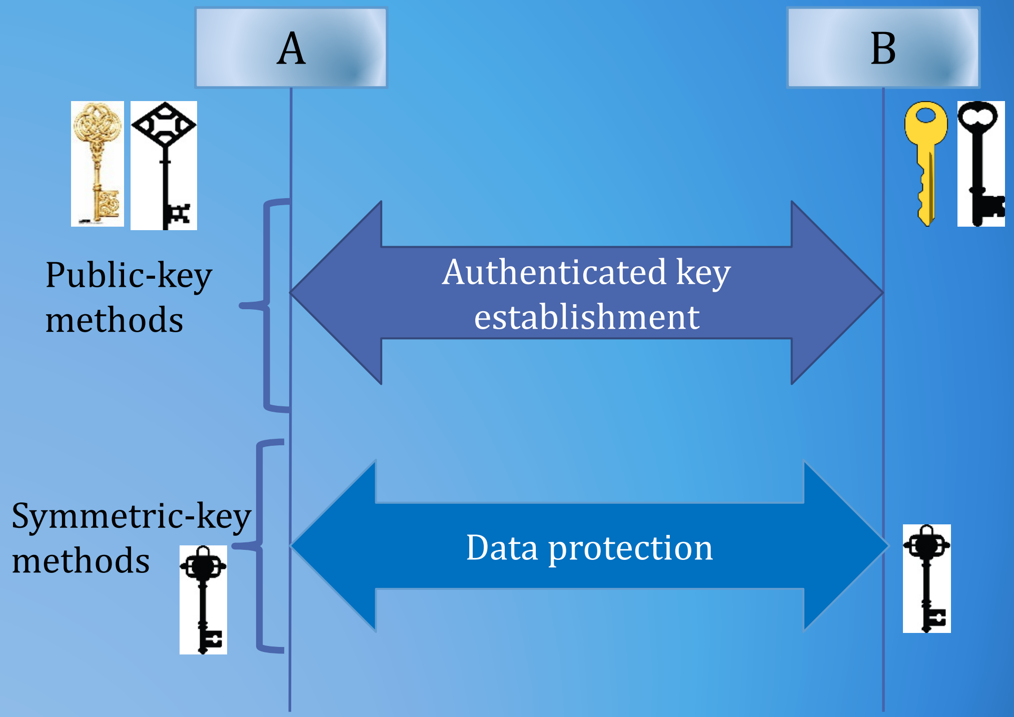
Micius – Nanshan, China

Date	Sifted key	QBER	Final key
05/06/2017	1329 kb	1.0%	305 kb
07/07/2017	1926 kb	1.7%	398 kb



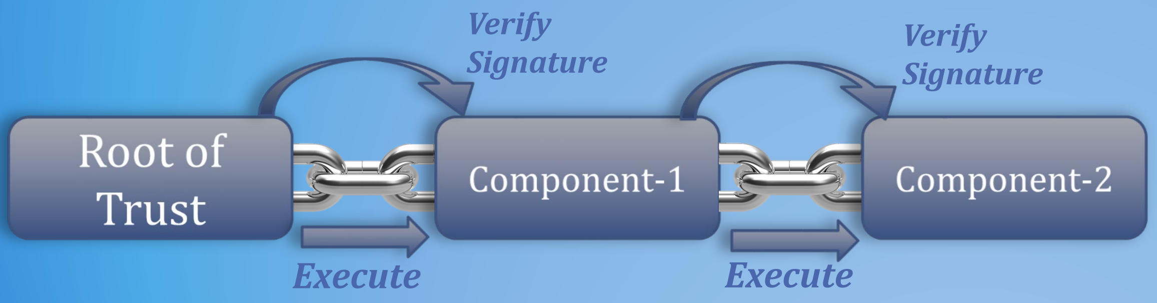
Today's Usage of Public-Key and Symmetric-Key Crypto — For Secure Communications

- In communication protection, public key and symmetric key cryptography schemes are used together, e.g. TLS, IPsec, etc.
  - Use public key cryptography to establish keys and authenticate users through signatures
  - Use symmetric key cryptography to encrypt and authenticate bulk data



Today’s Usage of Public-Key and Symmetric-Key Crypto — In Trusted Platform in Digital Device

- Use public-key cryptography to establish a root of trust
  - Form a trust chain starting from the root of trust
  - The root is protected through hardware technologies
- They are trusted to perform security-critical functions, e.g.,
  - Verify signed software for authenticity to prevent malware attacks
  - Protect cryptographic keys
  - Perform device authentication



Verify Signature

Verify Signature

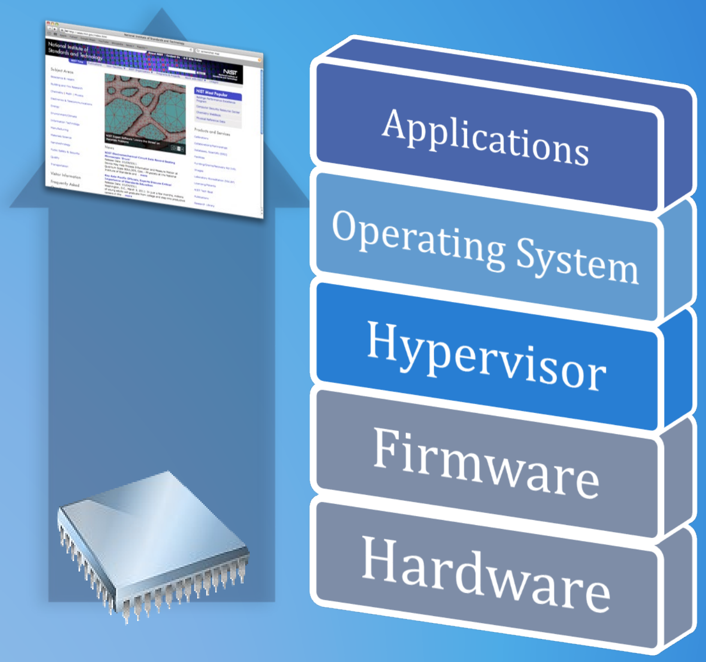
Root of Trust

Component-1

Component-2

Execute

Execute



Applications

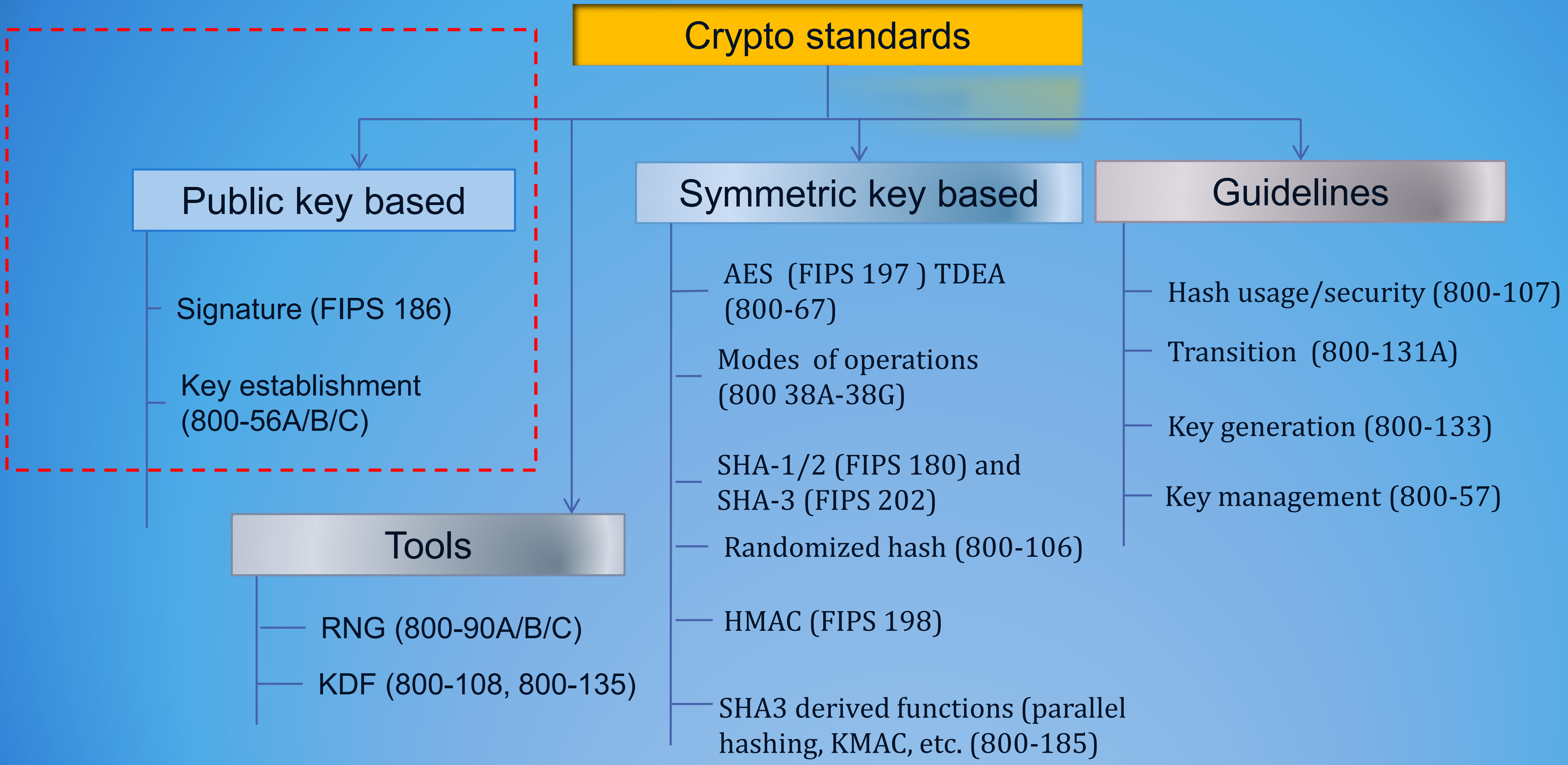
Operating System

Hypervisor

Firmware

Hardware

NIST Cryptographic Standards



Crypto standards

Public key based

- Signature (FIPS 186)
- Key establishment (800-56A/B/C)

Tools

- RNG (800-90A/B/C)
- KDF (800-108, 800-135)

Symmetric key based

- AES (FIPS 197) TDEA (800-67)
- Modes of operations (800 38A-38G)
- SHA-1/2 (FIPS 180) and SHA-3 (FIPS 202)
- Randomized hash (800-106)
- HMAC (FIPS 198)
- SHA3 derived functions (parallel hashing, KMAC, etc. (800-185)

Guidelines

- Hash usage/security (800-107)
- Transition (800-131A)
- Key generation (800-133)
- Key management (800-57)

Why Public-Key Cryptography is Secure?

- A problem is hard if no polynomial time algorithm is known to solve it

- The hardness is categorized by computing complexity - generally expressed as a function $n \rightarrow f(n)$, where n is the size of the input, e.g.
  - If $f(n)$ is a polynomial, then the problem is not hard
  - If $f(n) = c \cdot e^{h(n)}$ then, the problem is hard

- Practically, it means that it is infeasible to solve it with the currently available computing resource

- The hardness on certain problems is used as the basic assumptions for some cryptographic schemes, e.g.
  - RSA is based on the hardness of integer factorization, given integer n $(= p \cdot q)$ find p and q
  - Diffie-Hellman key agreement is based on the hardness of discrete logarithm problem, given y $\in$ GF(p)* and generator g , find x , such that $y = g^{x}$

NIST Public Key Cryptography Standards

- NIST standardized public key cryptographic schemes are based two "hard problems"

Integer Factorization

- RSA encryption (SP 800-56B for key establishment)
- RSA signatures (FIPS 186)

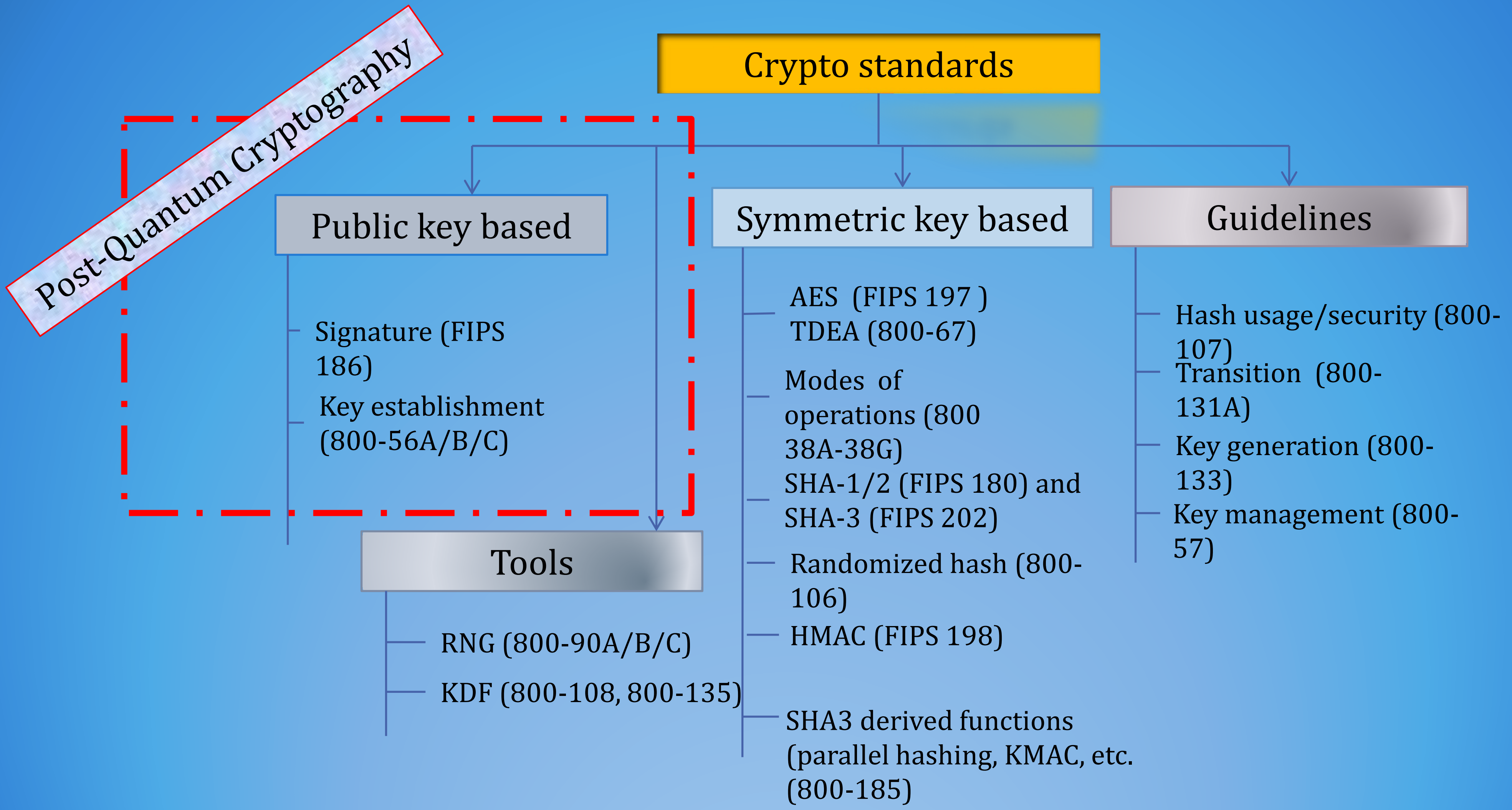
Discrete Logarithm

- DH/ECDH and MQV/ECMQV (SP 800-56A for key establishment)
- DSA and ECDSA (FIPS 186)

Quantum Impact

- Emerging quantum computers changed what we have believed about the hardness of discrete log and factorization problems
  - Using quantum computers, an integer n can be factored in polynomial time using Shor's algorithm
  - The discrete logarithm problem can also be solved by Shor's algorithm in polynomial time
- As a result, the public key cryptosystems deployed since the 1980s will need to be replaced
  - RSA signatures, DSA and ECDSA (FIPS 186-4)
  - Diffie-Hellman Key Agreement over finite fields and elliptic curves(NIST SP 800-56A)
  - RSA encryption (NIST SP 800-56B)
- We have to look for quantum-resistant counterparts for these cryptosystems
- Quantum computing also impacted security strength of symmetric key based cryptography algorithms
  - Grover's algorithm can find AES key with approximately $\sqrt{2^n}$ operations where n is the key length
  - Intuitively, we should double the key length, if 2^{64} quantum operations cost about the same as 2^{64} classical operations

Quantum Impact to NIST Standards



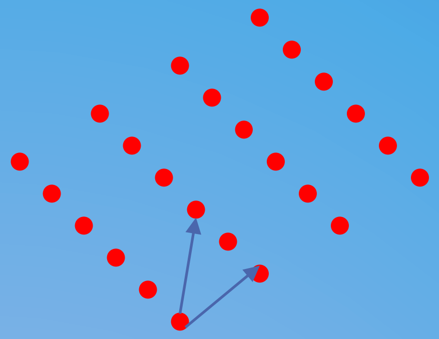
Post-Quantum Cryptography

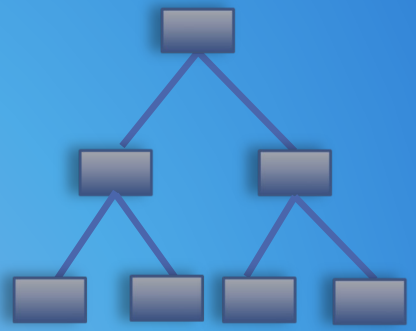
Crypto standards

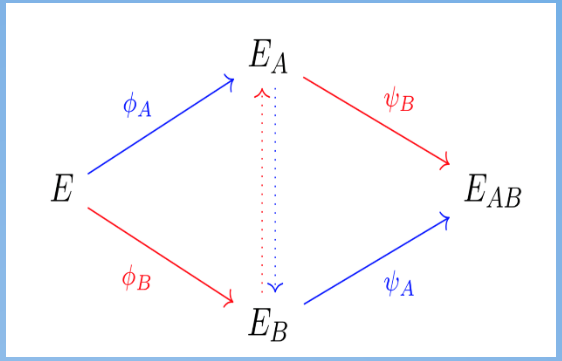
- Public key based
  - Signature (FIPS 186)
  - Key establishment (800-56A/B/C)
- Tools
  - RNG (800-90A/B/C)
  - KDF (800-108, 800-135)
- Symmetric key based
  - AES (FIPS 197)
    TDEA (800-67)
  - Modes of operations (800 38A-38G)
  - SHA-1/2 (FIPS 180) and SHA-3 (FIPS 202)
  - Randomized hash (800-106)
  - HMAC (FIPS 198)
  - SHA3 derived functions (parallel hashing, KMAC, etc. (800-185)
- Guidelines
  - Hash usage/security (800-107)
  - Transition (800-131A)
  - Key generation (800-133)
  - Key management (800-57)

Post-Quantum Cryptography (PQC)

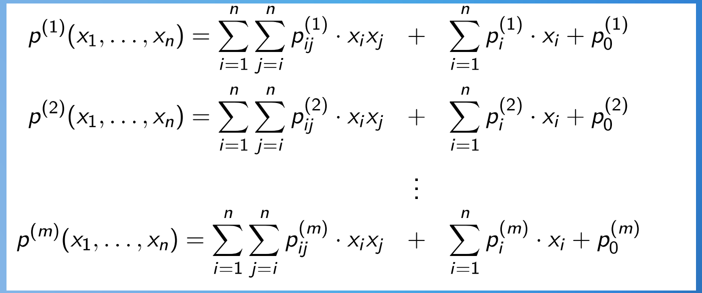
- Post-quantum cryptography algorithms are classical cryptographic algorithms which are considered to be able to resist quantum attacks
  - They must be based on hard problems which are still hard even when large scale quantum computers become available
- Some actively researched PQC categories
  - Lattice-based
  - Code-based
  - Multivariate
  - Hash based signatures
  - Isogeny-based schemes







$$\begin{tikzcd}
 & E_A \arrow[dr, "\psi_B"] \arrow[dd, dotted, bend left=10] & \\
E \arrow[ur, "\phi_A"] \arrow[dr, "\phi_B"'] & & E_{AB} \\
 & E_B \arrow[ur, "\psi_A"'] \arrow[uu, dotted, bend left=10] &
\end{tikzcd}$$



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

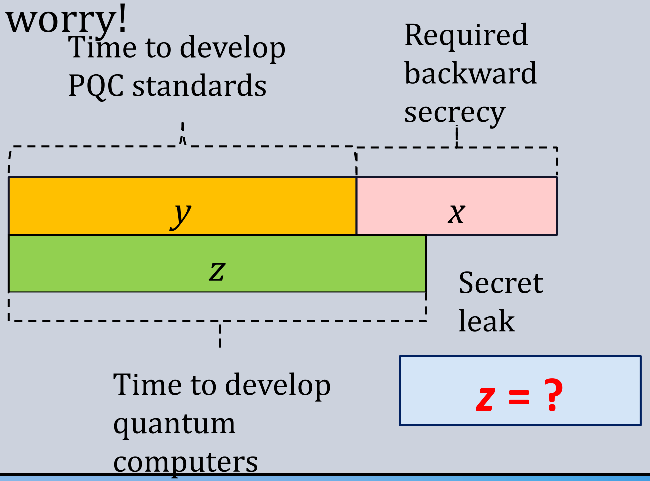
Is it too early to start?

"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)

- It takes time to develop and deploy PQC standards (y years)
- Considering backward secrecy and product cycle, it is the time to start

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


Time to develop PQC standards
Required backward secrecy
y
x
z
Secret leak
Time to develop quantum computers
z = ?

NSA IAD Announcement August 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

Scope

- Digital signature
  - Replace the schemes specified in FIPS 186-4 (RSA, DSA, ECDSA)
- Encryption
  - Replace key transport specified in SP 800-56B (currently using RSA encryption like OAEP and Key-Encapsulation Mechanism)
- Key agreement
  - Replace DH/ECDH, MQV/ECMQV in SP 800-56A
  - If no good replacement, use public key encryption to exchange selected secret values (as in 56B)
  - For perfect forward secrecy, use one-time public key to encrypt the selected secret values, assuming key pair generation is fast

Understand the Challenges

- Much broader scope – three crypto primitives, compared to AES and SHA-3 – single primitive
- Both classical and quantum attacks
  - Security strength assessment on specific parameter selections
- Consider various theoretical security models and practical attacks
  - Provably security and security against instantiation or implementation related security flaws and pitfalls
- Multiple tradeoff factors
  - Security, performance, key size, signature size, side-channel attack countermeasures
- Migrations into new and existing applications
  - TLS, IKE, code signing, PKI infrastructure, and much more

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
- The draft requirements and criteria were announced in August 2016 to call for public comments

Security Strength Categories

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
- 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 or Symmetric based	3		3
Other	2	5	7
Total	**19**	**45**	**64**

Security Analysis and Evaluations

- NIST team has been reviewing and evaluating the first round candidates through internal seminars
- NIST team members monitored and participated in the discussions on pqc-forum
- The NIST PQC Standardization has greatly promoted research
  - Analysis results on candidates have been published at conferences like PQCrypto 2018 and also released through IACR eprint
  - More analysis results were announced through “Official Comments”, which will lead to future publications
- Each design team submitted reference implementations and preliminary estimations on the performance
  - NIST team has verified the reference implementations as the first round review
  - At this stage, even performance considerations will not play a major role in the evaluation process, need to understand extreme cases and show stoppers

Evaluation of the 1st Round

- NIST team had seminars to present each candidate by team members to understand how it works, look into security analysis provided by the submitters, raise questions, discuss pros and cons, etc.

- Security analysis
  - Research publications at conferences and journals (e.g. PQCrypto)
  - Official comments - Over 300 official comments
  - E-mail discussions at pqc-forum – 926 posts

- Performance
  - Evaluation resources include
    - NIST's internal testing with submitters' code
    - Preliminary benchmarks – SUPERCOP, OpenQuantumSafe, etc.

Selection of second round candidates

- Security
  - Candidates which were broken, significantly attacked, or difficult to establish confidence in their security were left out
  - Candidates which provided clear design rationale and reasonable security proofs to established reasonable confidence in security are advanced
- Performance
  - Candidates with obvious performance or key/signature/ciphertext size issues for existing applications were not advanced - even though they might have been well prepared with good ideas

NIST announced second round candidates in January 31, 2019

The 2nd round candidates

KEM/Enc

Lattice –based (9):
Crystals-Kyber; FrodoKEM; LAC; NewHope; NTRU; NTRU Prime; Round 5; Saber; Three Bears

Code –based (7):
Classic McEliece; NTS-KEM; BIKE; HQC; Rollo; LEDAcrypt; RQC

Isogeny –based (1):
SIKE

Signature

Lattice –based (3):
Crystals-Dilithium; Falcon; qTESLA

Symmetric –based (2) :
Sphincs+; Picnic

Multivariate (4):
GeMSS; LUOV; MQDSS; Rainbow

* See NISTIR 8240 for a summary of each of the 2nd round candidates

Transition and Migration

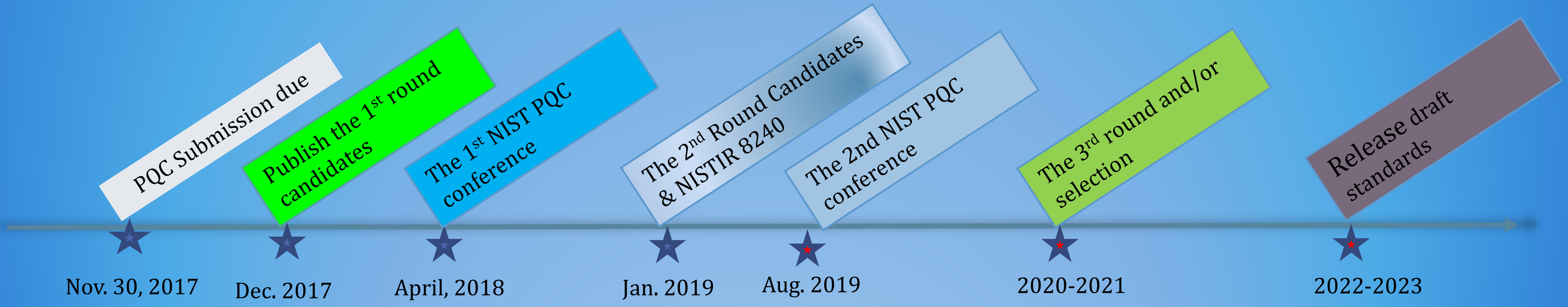
- NIST will update guidance when PQC standards are available
  - Before that, follow the transition guideline as specified in NIST SP 800-131A
  - The future PQC transition shall not be an excuse to stay on weak crypto
  - The classical attacks can be efficient and can break your system – the pre-quantum 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

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

Future plans

- The 2nd PQC Standardization Conference will be held in August 2019
- Spend 12-18 months to analyze and evaluate the 2nd round candidates
- Start a 3rd round and/or select algorithms to standardize 2020-2021
- Release draft standards in 2022-2023 for public comments



PQC Submission due

Nov. 30, 2017

Publish the 1st round candidates

Dec. 2017

The 1st NIST PQC conference

April, 2018

The 2nd Round Candidates & NISTIR 8240

Jan. 2019

The 2nd NIST PQC conference

Aug. 2019

The 3rd round and/or selection

2020-2021

Release draft standards

2022-2023

Information on NIST PQC Standardization

- For NIST PQC project, please follow us at
  https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

- Join discussion mailing list pqc-forum@nist.gov