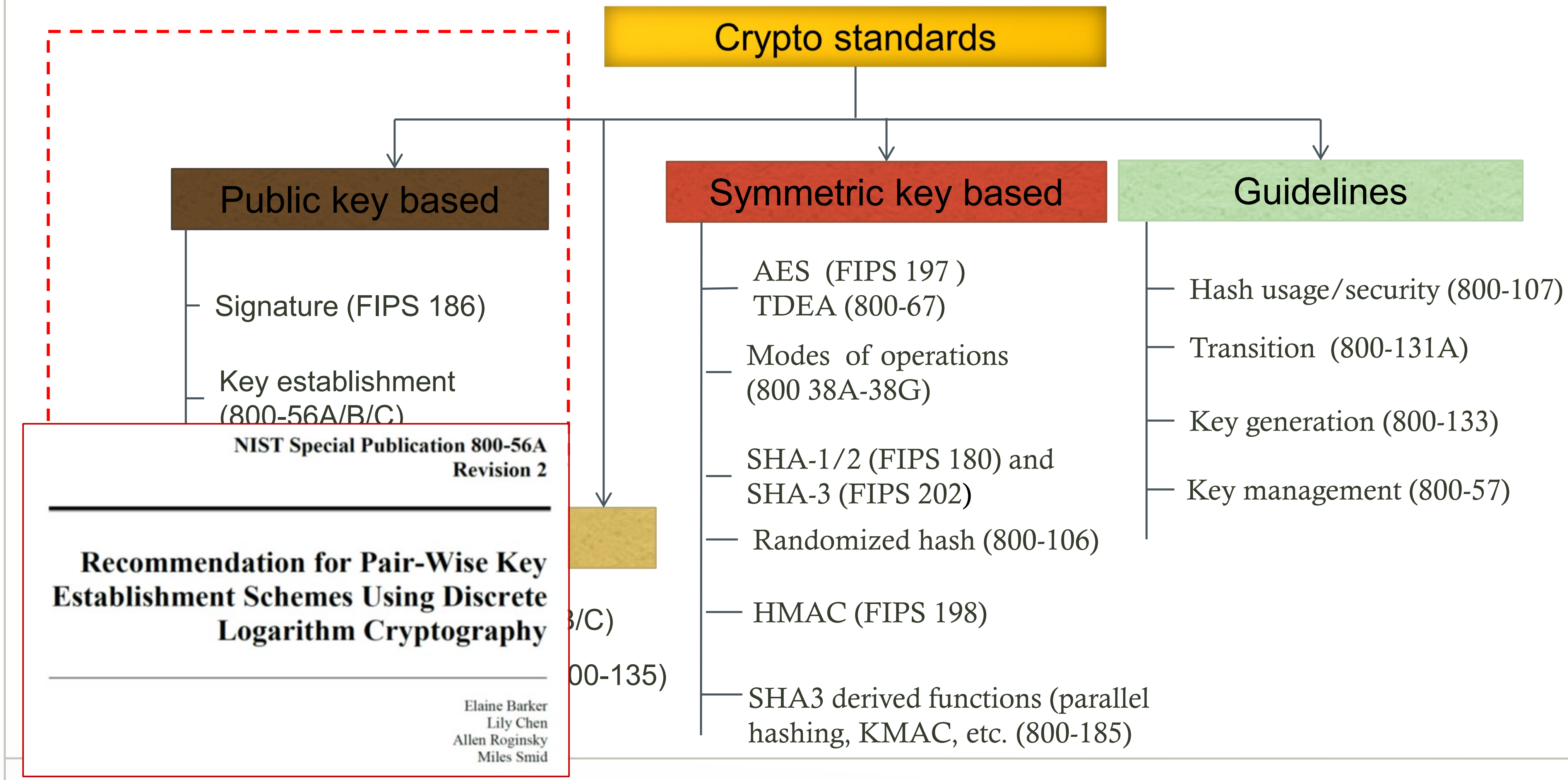
Post-Quantum Cryptography and Standardization

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

NIST Cryptographic Standards



Crypto standards

Public key based

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

/C)

00-135)

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)

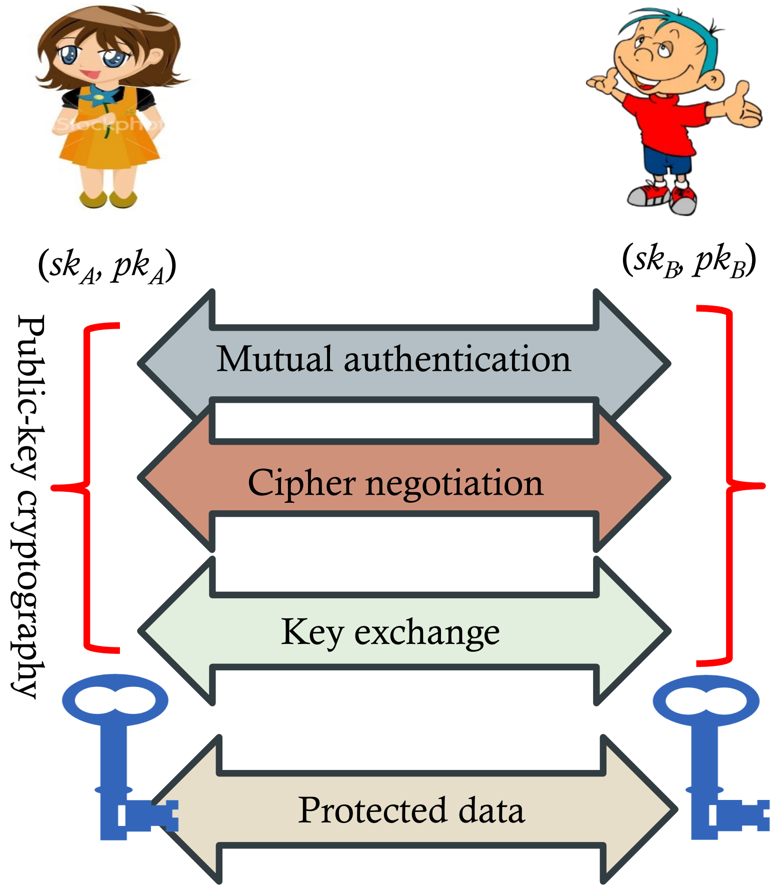
NIST Special Publication 800-56A
Revision 2

Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography

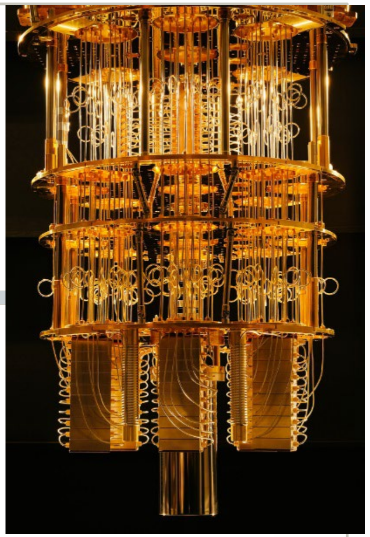
Elaine Barker
Lily Chen
Allen Roginsky
Miles Smid

NIST Public-Key Cryptography Standards Usage

- Public-key cryptography has been used in
  - network protocols to establish symmetric keys and also to conduct mutual authentication such as in Internet Key Exchange (IKE) Protocol
  - web access to establish security sessions for such as Transport Layer Security (TLS) protocol (handshake for key establishment, cipher-suite negotiation, and authentication
  - software authentication and authorization for secure boot and application update (code signed by digital signatures); and
  - many other places
- Need quantum resistant cryptography to provide security for computation, communication and storage in quantum era



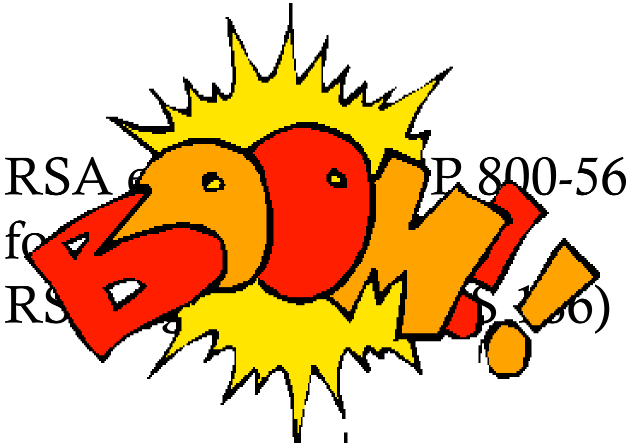
NIST PK Crypto Standards and Quantum Impact



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

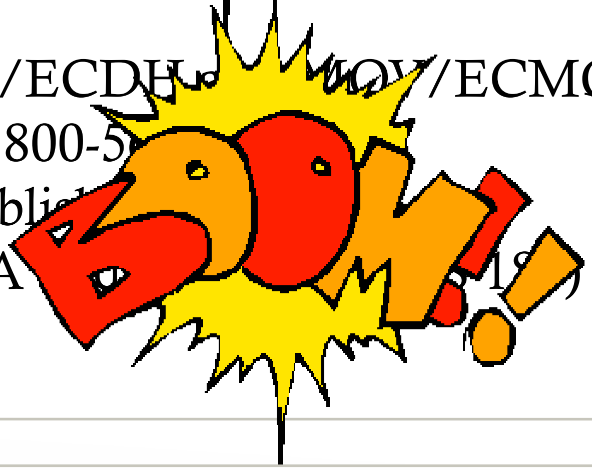
Integer Factorization

- RSA P 800-56B fo
- RS 6)



Discrete Logarithm

- DH/ECDH QV/ECMQV (SP 800-5 establi
- DSA)



- 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

What and where researchers have looked for?

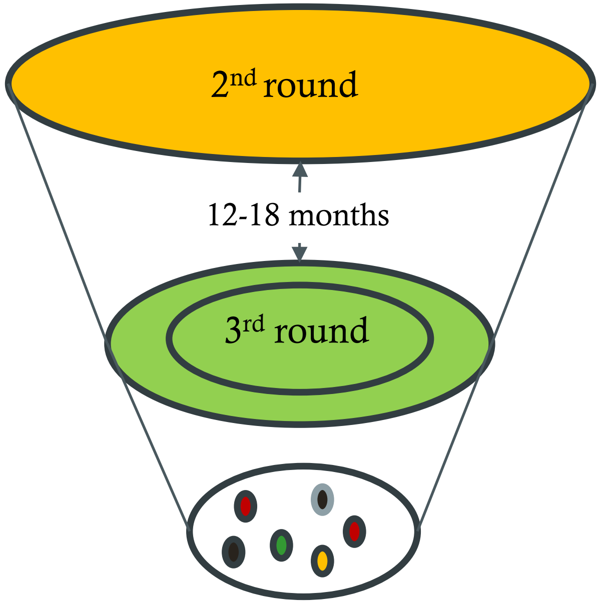
- Hard problems which are hard even with quantum computers, e.g.
  - Shortest vector problem in the lattice
  - Random decoding
  - Etc.
- Cryptosystems based on the hard problems and resistant to quantum computers
  - Some cryptosystems proposed many years ago, e.g. McEliece (1970s) and got improved
  - Others, e.g. NTRU (1990s), evolved to many variations

What NIST has done so far on PQC standardization?

- NIST has started to grow expertise in post-quantum cryptography since 2009
- Engaged with research community through workshops, technical reports, etc.
- Announced call for proposals with requirements and criteria(Federal Register Notice) in Dec. 2016
- Received 82 submissions and 69 were "proper and complete as the first round candidates Nov/Dec 2017
- Announced the 26 second round candidates Jan. 30, 2019

What will be the next?

- Analyze and evaluate the PQC candidates
  - Second analysis phase 12-18 month
- May take third analysis phase if needed
- Make selections and release draft standards in 2022-2023



Message to Application Community

- NIST leads a new initiative to develop PQC standards
- The PQC standards will be used in existing and new applications
- Identify possible barrier to migrate to PQC standards
- Raise issues you can see on deploying PQC standards
- Follow us at www.nist.gov/pqcrypto and join discussion pqc-forum@nist.gov
- Questions/comments sent to comments-pqc@nist.gov