Build Quantum-Safe 6G Network

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

Technology and Security Evolutions – 1G to 5G

1G - Analog, circuit switched networks, and only carry voice traffic, almost no security protection

2G: Digital communications, high bit rate voice, limited data communications, allow SIM subscriber authentication and encryption (proprietary algorithms)

3G: Voice, high speed data, co-existed IP packet switch and legacy circuit switch, multimedia, mandatory subscriber authentication, encryption and integrity by AKA (symmetric-key)

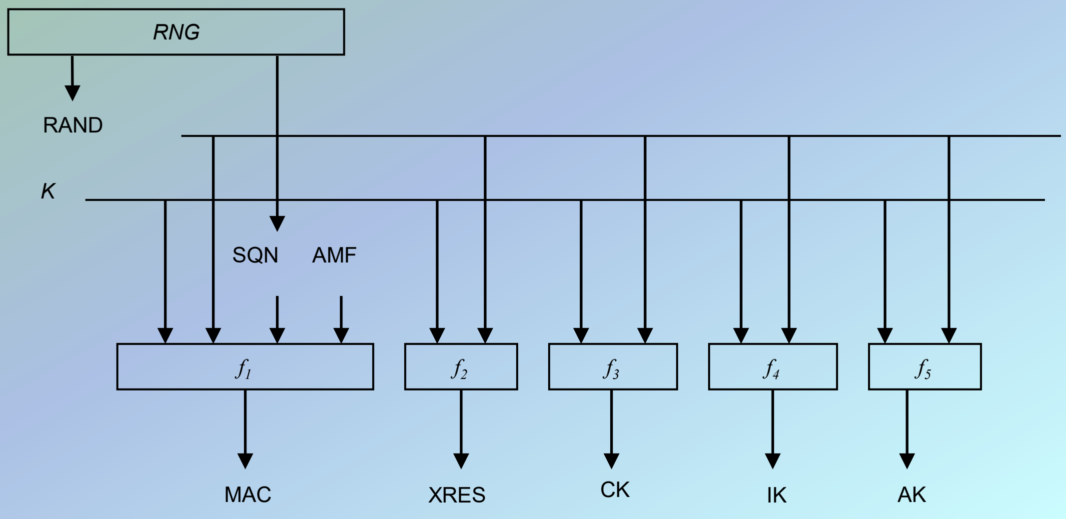
4G: Higher speed, all IP packet switch network, interoperation with non-cellular networks, AKA +introduce IP network security

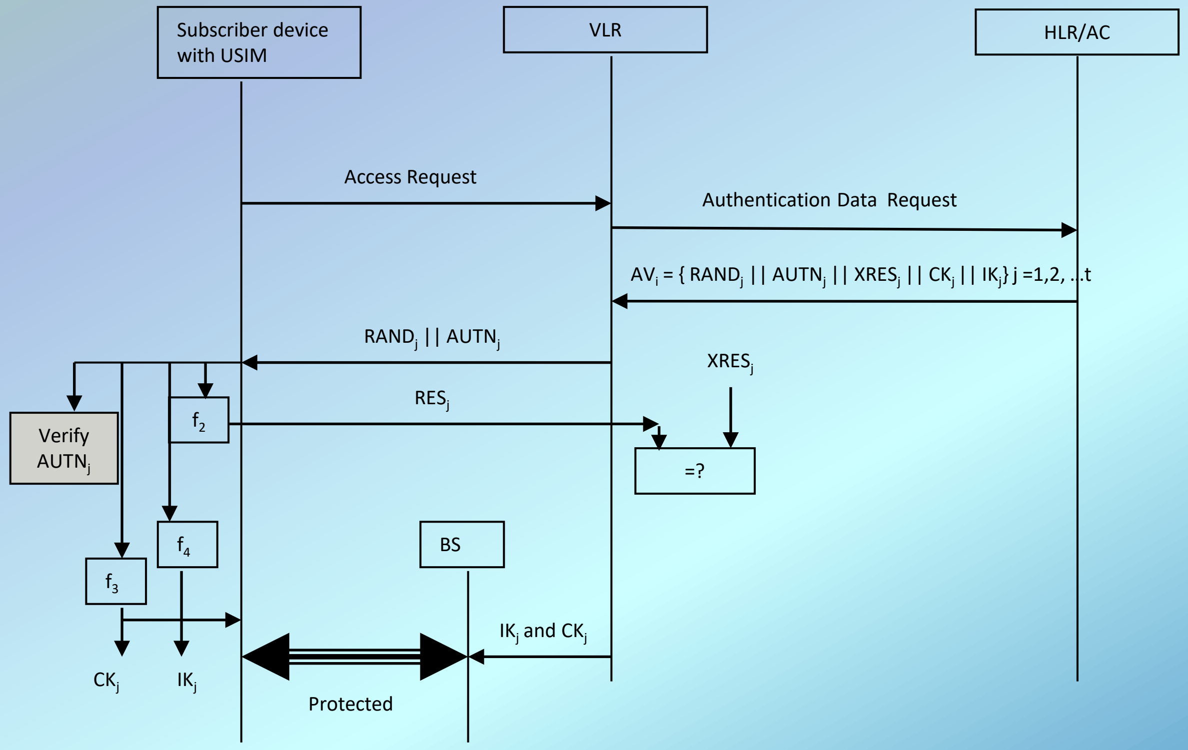
5G: more capacity, lower latency, better mobility, more accuracy of terminal location, 5G AKA or EAP-AKA + use PKC for privacy + TLS + IKEv2

6G: more heterogeneous, everything for 5G security + heterogeneous network and media protections

Authentication and key agreement (AKA)

- AKA is a symmetric-key based scheme using a key stored in USIM and authentication server
- Authentication vectors (AVs) are provided for local access authentication
- An AV includes authentication token and session keys
  - Session keys are used to protect airlink
- AKA was specified for UMTS and used for LTE and 5G with extended key hierarchy



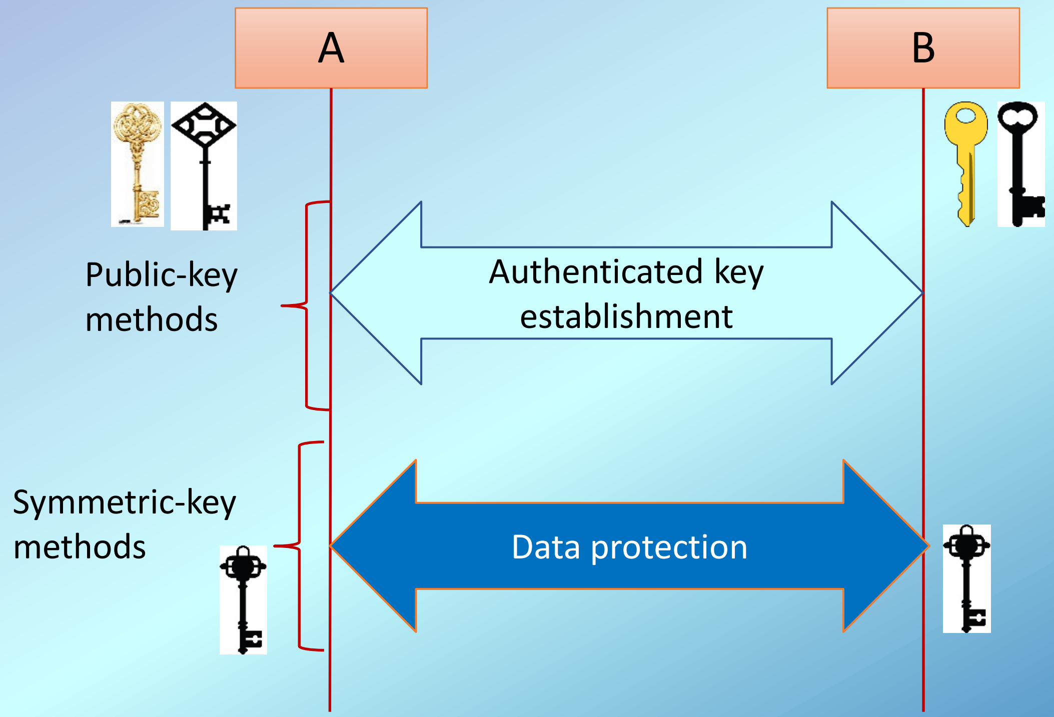


Security for 6G – Beyond what AKA provides

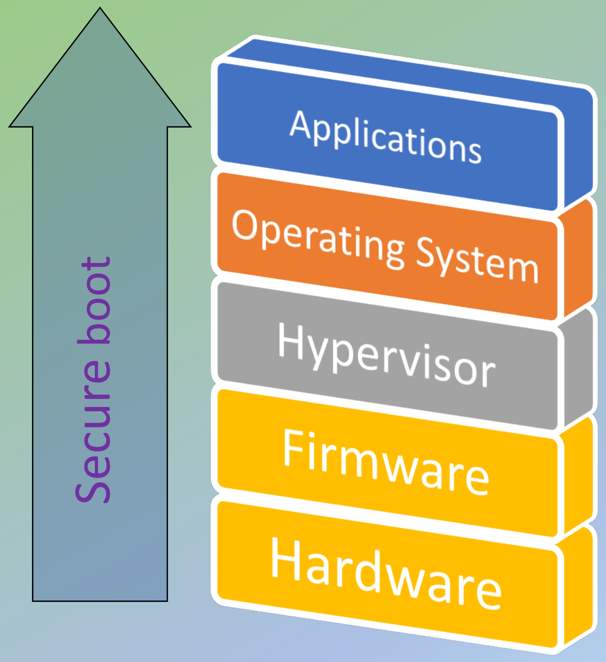
- TLS is supported by all network functions in the 5G architecture in service-based interface, while IKEv2 is used to establish a shared secret in non-service-based interface
  - Private networks using the 5G system may use EAP TLS for authentication and key agreement
  - An ephemeral Diffie-Hellman or ECDH key exchange may be added to 5G-AKA in future releases of 5G
- 6G is going to be more heterogeneous
  - Interoperate with other networks – protocols and layered protections
  - Trusted platform is critical – protection from malware attacks
- Public key cryptography will be extensively used for
  - Key establishment between network entities (e.g., key agreement, public-key encryption, key encapsulation mechanisms, and authenticate with digital signatures)
  - Firmware and software verification with digital signatures

Cryptography for Secure Communications

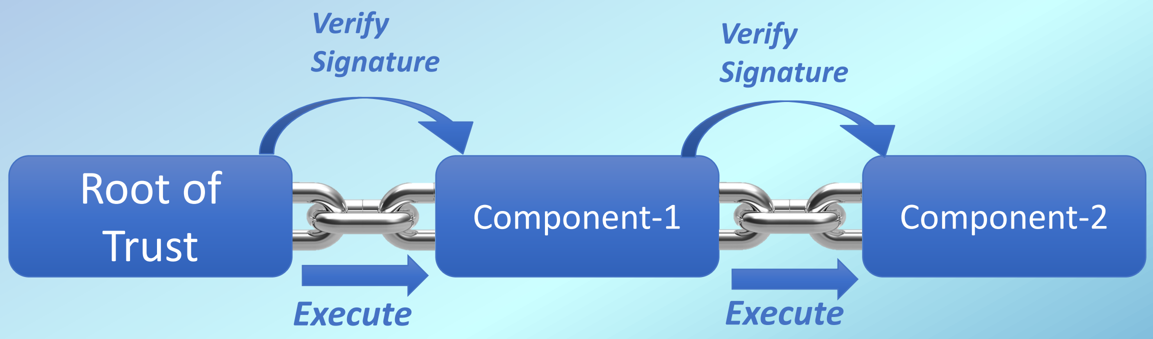
- Use public key cryptography to establish keys and authenticate users through signatures
  - Diffie-Hellman Key Exchange
  - RSA and ECDSA signatures
- Use symmetric key cryptography to encrypt and authenticate bulk data
  - AES (CBC, GCM, etc.)
  - HMAC (SHA-2, SHA-3)
- Examples
  - Transport Layer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



Cryptography for Trusted Platform



- Today's digital devices adopt open-platforms and allow constant update and installation
- Public-key based digital signatures are used for establishing trusted platform
- Symmetric-key algorithms are used to protect data stored in the devices



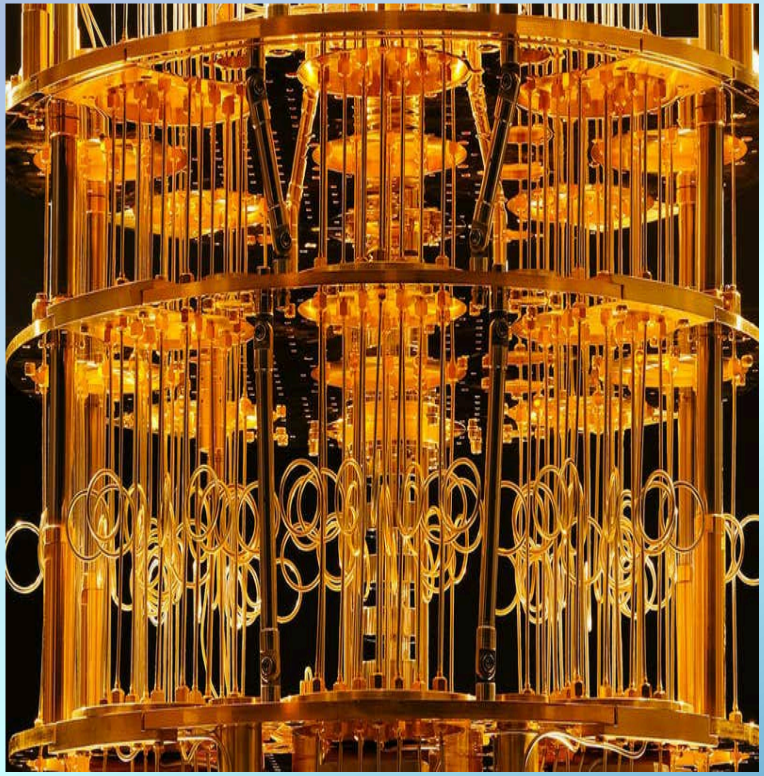
- TS 33.117: "the network product shall support software package integrity validation via cryptographic means", e.g. digital signature.

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 $g^x = y$

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

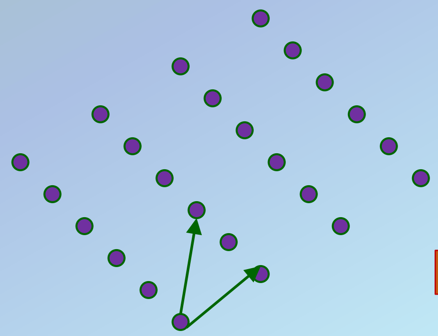


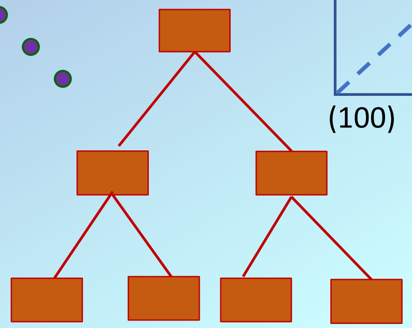
How to Deal with Quantum Attacks?

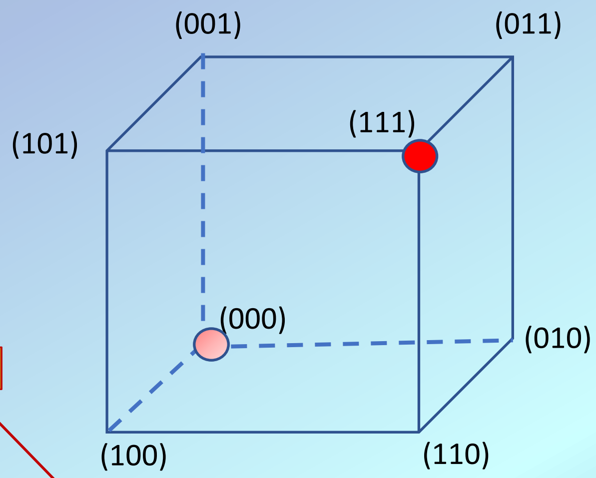
- Need to find cryptographic algorithms which are secure against attacks by both classical and quantum computers
  - The algorithms must be based on hard problems which are hard for both classical and quantum computers
- In other words, we need quantum resistant cryptography, named by the researchers 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

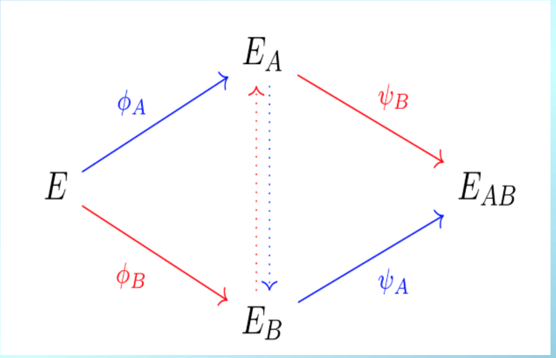
Post Quantum Cryptography (PQC)

- 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









$$p^{(1)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)}\cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(1)}\cdot x_i + p_0^{(1)}$$

$$p^{(2)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)}\cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(2)}\cdot x_i + p_0^{(2)}$$

$$\vdots$$

$$p^{(m)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)}\cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(m)}\cdot x_i + p_0^{(m)}$$

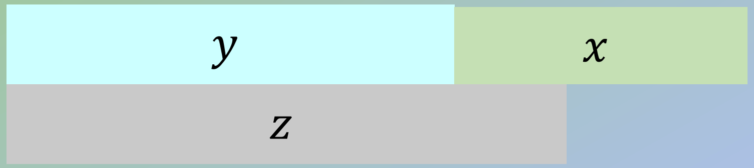
NIST Cryptographic Standards – A Glance

Cryptography 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 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

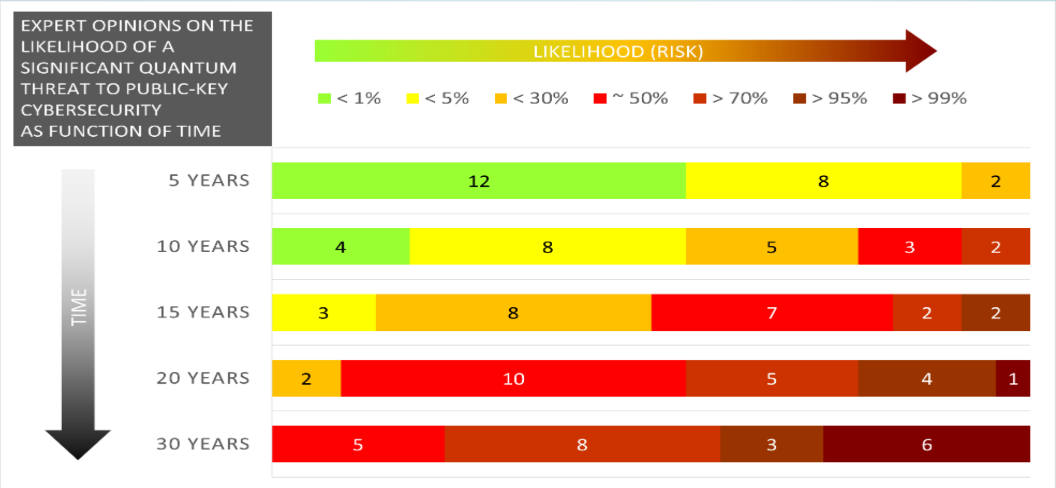
z – time for quantum computers to be developed

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/



Numbers reflect how many experts (out of 22) assigned a certain probability range.

NIST PQC Standards - Scope

Post-Quantum Cryptography

Cryptography 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)

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

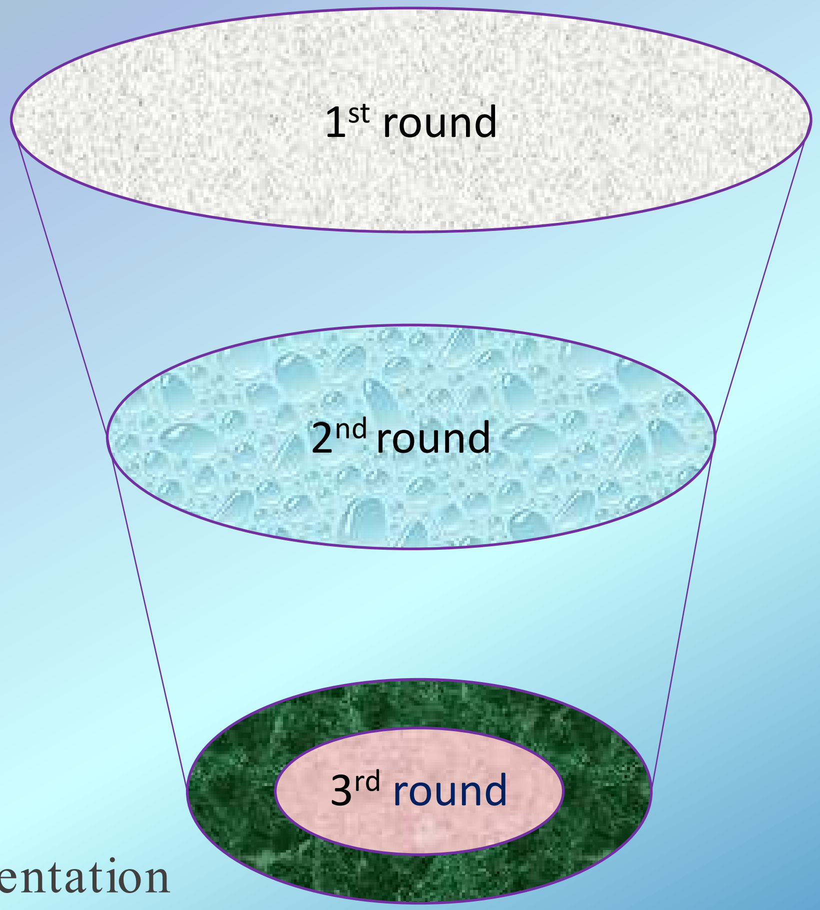
2024 Publish PQC Standards

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



The First Round Candidates

1st round	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate	7	2	9
Stateless Hash/Symmetric based	3		3
Other	2	5	7
Total	19	45	64

The Second Round Candidates

2nd round	Signatures	KEM/Encryption	Overall
Lattice-based	3	9	12
Code-based		7	7
Multi-variate	4		4
Stateless Hash/Symmetric based	2		2
Isogeny		1	1
Total	10	16	26

The Third Round Candidates

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

Prepare for PQC Adoption in 6G

- Understand the new features of PQC and their applications in 6G networks
  - ETSI TR 103 616 V1.1.1 (2021-09) "Quantum-Safe Signatures" https://www.etsi.org/deliver/etsi_tr/103600_103699/103616/01.01.01_60/tr_103616v010101p.pdf
  - ETSI TR 103 823 V1.1.1 (2021-09) "Quantum-Safe Public Key Encryption and Key Encapsulation" https://www.etsi.org/deliver/etsi_tr/103800_103899/103823/01.01.01_60/tr_103823v010101p.pdf
- Assess the impact of PQC in 6G network on demanded bandwidth and processing power
  - Experimental implementations of PQC candidates to obtain the firsthand experience;
  - Identify barriers, limitations, showstoppers, and necessary justifications – Feedback is extremely important for NIST standardization
- Collaborate with other standards organizations for a smooth transition
  - PQC adoption in Internet protocols e.g. TLS, IKE, etc.
  - Post-quantum digital signatures for trusted platform, e.g. code signing

Thanks

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