NIST Post-Quantum Cryptography Standardization Status Report

René Peralta

Cryptographic Technology Group
National Institute of Standards and Technology
(Gaithersburg, Maryland, USA)

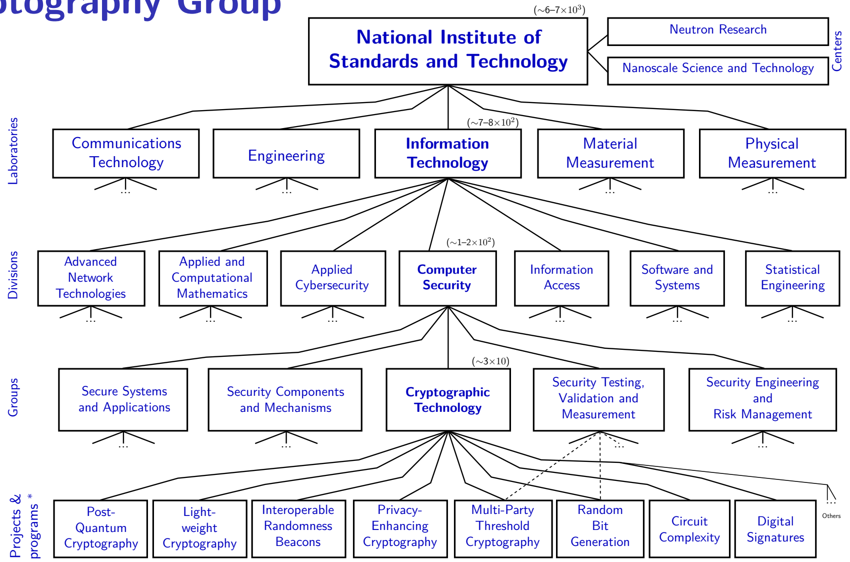
Presentation at Post-Quantum Cryptography
PKI Consortium Conference
March 3, 2023 @ Ottawa, Canada

National Institute of Standards and Technology (NIST)

- **Mission** (keywords): innovation, industrial competitiveness, measurement science, standards and technology, economic security, quality of life.

Aerial photo of Gaithersburg campus (source: Google Maps, August 2019)

The Cryptography Group



* Source: Luís Brandão

(In parenthesis: approximate range # workers, inc. associates and fed. employees)

Why PQC?

- In the early 1980s Feynman, Manin and others lay the theoretical foundation for quantum computing;
- In 1994 Peter Shor developed a quantum computer algorithm that can factor integers and compute discrete logs;
- Quantum circuits are fragile. They easily collapse into random classical states. In 1995 it was discovered (Shor again) that quantum error-correction is theoretically possible;
- It is expected that in the 2020s significant advances will occur in building (a few) logical qbits.

Why PQC?

- Around 2014 NIST decided that quantum resistant cryptography would eventually have to replace current public-key cryptography standards;
- The process was formally launched in 2016;

Why Now?

Quantum computers capable of breaking current cryptography are (likely) decades away.

But:

Why Now?

Quantum computers capable of breaking current cryptography are (likely) decades away.

But:

- There could be some surprise breakthrough.

Why Now?

Quantum computers capable of breaking current cryptography are (likely) decades away.

But:

- There could be some surprise breakthrough.
- Migration to new cryptography is complicated and takes a long time.

Why Now?

Quantum computers capable of breaking current cryptography are (likely) decades away.

But:

- There could be some surprise breakthrough.
- Migration to new cryptography is complicated and takes a long time.
- There are applications in which we need long-time secrecy.

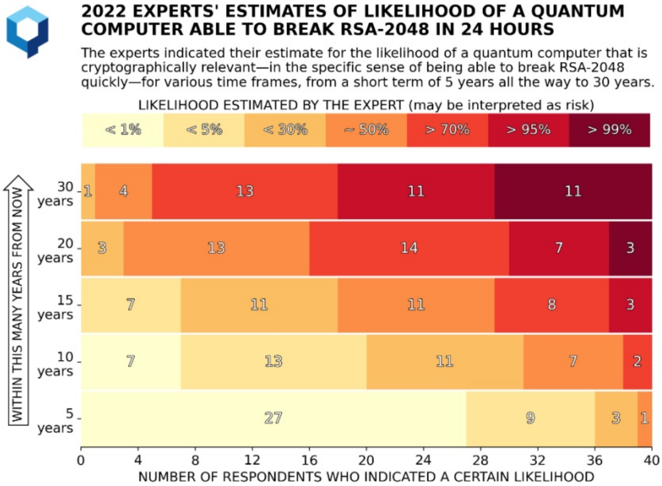
Why Now?

Quantum computers capable of breaking current cryptography are (likely) decades away.

But:

- There could be some surprise breakthrough.
- Migration to new cryptography is complicated and takes a long time.
- There are applications in which we need long-time secrecy.
- Encrypted data and communications could be stored today and decrypted once possible to do so.

Asking the Experts



Source: Mosca and Piani, Quantum Threat Timeline Report 2022

The Process

- Somewhat different from the AES and SHA competitions.
- Community consensus building.
- Transparency a central objective.

The Process

- Somewhat different from the AES and SHA competitions.
- Community consensus building.
- Transparency a central objective.
- Have concluded three phases, each involving the world community.

NIST PQC Milestones and Timelines

2016

Determined criteria and requirements, published NISTIR 8105

Announced call for proposals

2017

Received 82 submissions

Announced 69 1st round candidates

2018

Held the 1st NIST PQC standardization Conference

2019

Announced 26 2nd round candidates, NISTIR 8240

Held the 2nd NIST PQC Standardization Conference

2020

Announced 3rd round 7 finalists and 8 alternate candidates. NISTIR 8309

2021

Hold the 3rd NIST PQC Standardization Conference

2022 Make 3rd round selection and draft standards – NISTIR 8413

2023 Release draft standards and call for public comment

2024 Publish the 1st set of PQC Standards

Chosen Algorithms

- Kyber KEM : (structured) lattice-based.
- Dilithium Signature : (structured) lattice-based.
- Falcon Signature : (structured) lattice-based.
- SPHINCS+ : hash-function based.

Chosen Algorithms

- Kyber KEM : (structured) lattice-based.
- Dilithium Signature : (structured) lattice-based.
- Falcon Signature : (structured) lattice-based.
- SPHINCS+ : hash-function based.

KEM Algorithms Still Under Consideration

- Classic McEliece : code-based, conservative security, VERY LARGE public keys.
- Bike and HQC : based on structured codes, useful performance profiles.

An On-Ramp for Signatures

NIST has issued a new Call for Signatures:

- the deadline for submission is June 1, 2023.
- looking to diversify the signature portfolio.
- we are **most interested** in a general-purpose signature which is not based on structured lattices.

Parametrization for Various Security Levels

Submitters were asked for parameter sets that correspond to various security levels.

Algorithms required to be hard(er) to break than AES inversion or SHA collision (by exhaustive search).

- Level I: AES128
- Level II: SHA256
- Level III: AES192
- Level IV: SHA384
- Level V: AES256

Legend:

AES = Advanced Encryption Standard

SHA = Secure Hash Algorithm

KEM Performance Profile

Algorithm	Security level	Public key	Private key	Ciphertext
Kyber512	I	800	1632	768
Kyber768	III	1184	2400	1088
Kyber1024	V	1568	3168	1568

Sizes in bytes

KEM Performance Profile

Algorithm	Security level	Public key	Private key	Ciphertext
Kyber512	I	800	1632	768
Kyber768	III	1184	2400	1088
Kyber1024	V	1568	3168	1568

Sizes in bytes

Algorithm	keygen/s	encap/s	decap/s
Kyber768	53K	46K	60K

OpenSSL performance (source)

Signature Performance Profile

Algorithm	Security level	Public key	Private key	Signature
Dilithium	II	1312	2528	2420
Dilithium	III	1952	4000	3293
Dilithium	V	2592	4864	4595
Falcon-512	I	897	7553	666
Falcon-1024	V	1793	13953	1280
SPHINCS+(s)	I	32	64	7856
SPHINCS+(f)	I	32	64	17088
SPHINCS+(s)	III	48	96	16224
SPHINCS+(f)	III	48	96	35664
SPHINCS+(s)	V	64	128	29792
SPHINCS+(f)	V	64	128	49856

Sizes in bytes

Signature Performance Profile

Algorithm	Security level	Keygen/s	Sign/s	Verify/s
Dilithium	II	27K	10.6K	29K
Dilithium	III	16K	6.5K	17.5K
Dilithium	V	10K	5.3K	10.8K
Falcon512	I	113	2.8K	17.5K
Falcon1024	V	40	1.4K	8.6K
SPHINCS+ (f)	I	1K	35	220
SPHINCS+ (s)	I	16	2	670
SPHINCS+ (f)	III	700	23	150
SPHINCS+ (f)	V	140	7	110

OpenSSL performance (source)

Other...

- Rationale for hybrid modes.
- Patents statements.
- Side-channel vulnerabilities in implementations.
- For migration guidance see NCCOE documents.
- Impact of Grover's algorithm on private-key cryptography.

Thanks

- NIST is grateful for everybody's efforts
- Check out NIST'S PQC WEB PAGE
- Sign up for the PQC-Forum for announcements & discussion
- Send email to PQC-comments@nist.gov