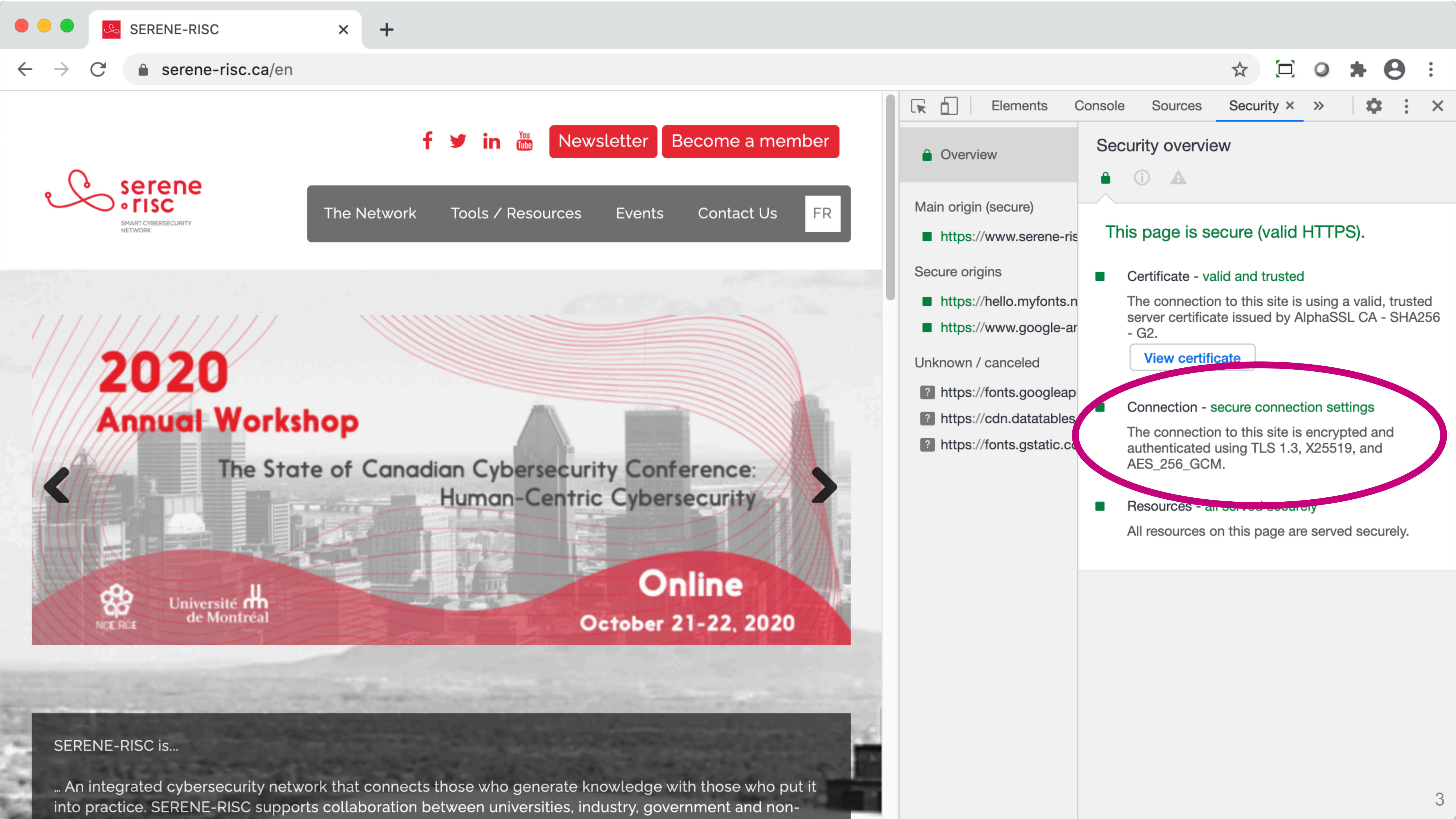
The current status of post-quantum cryptography

Douglas Stebila

SERENE-RISC 2020 Workshop • 2020-10-21

Why post-quantum?


SERENE-RISC
serene-risc.ca/en
Elements
Console
Sources
Security
Newsletter
Become a member
serene risc
SMART CYBERSECURITY NETWORK
The Network
Tools / Resources
Events
Contact Us
FR
Overview
Security overview
Main origin (secure)
https://www.serene-ris
Secure origins
https://hello.myfonts.n
https://www.google-ar
Unknown / canceled
https://fonts.googleap
https://cdn.datatables
https://fonts.gstatic.c
This page is secure (valid HTTPS).
Certificate - valid and trusted
The connection to this site is using a valid, trusted server certificate issued by AlphaSSL CA - SHA256 - G2.
View certificate
Connection - secure connection settings
The connection to this site is encrypted and authenticated using TLS 1.3, X25519, and AES_256_GCM.
Resources - all served securely
All resources on this page are served securely.
2020
Annual Workshop
The State of Canadian Cybersecurity Conference:
Human-Centric Cybersecurity
NCE RCE
Université de Montréal
Online
October 21-22, 2020
SERENE-RISC is...
.. An integrated cybersecurity network that connects those who generate knowledge with those who put it into practice. SERENE-RISC supports collaboration between universities, industry, government and non-

Cryptographic building blocks

Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.3, X25519, and AES_256_GCM.

Public-key cryptography

- RSA or elliptic curve signatures
- Elliptic curve Diffie–Hellman key exchange

Symmetric cryptography

- AES encryption
- AES GCM integrity

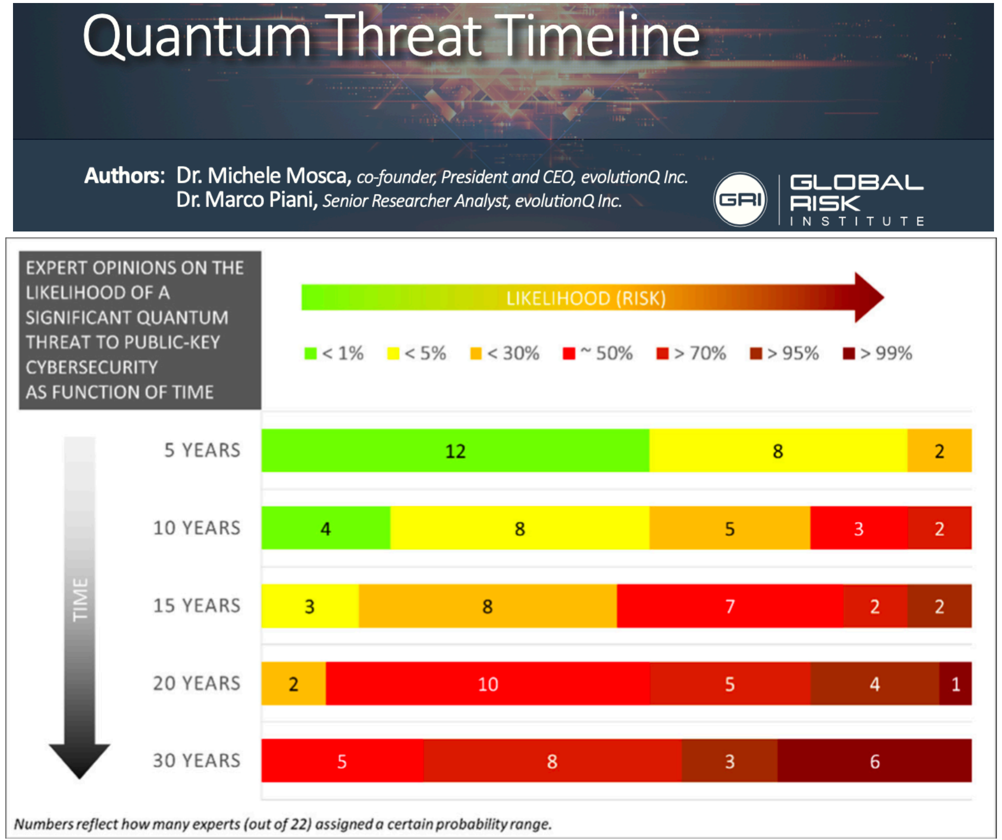
Based on difficulty of factoring large numbers – not quantum resistant!

Based on difficulty of computing discrete logarithms – not quantum resistant!

When will a large-scale quantum computer be built?

"I estimate a 1/7 chance of breaking RSA-2048 by 2026 and a 1/2 chance by 2031."

— Michele Mosca, University of Waterloo



https://eprint.iacr.org/2015/1075
http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf
https://globalriskinstitute.org/publications/quantum-threat-timeline/

Post-quantum cryptography

a.k.a. quantum-resistant algorithms

Cryptography believed to be resistant to attacks by quantum computers

Uses only classical (non-quantum) operations to implement

Not as well-studied as current encryption

- Less confident in its security
- More implementation tradeoffs

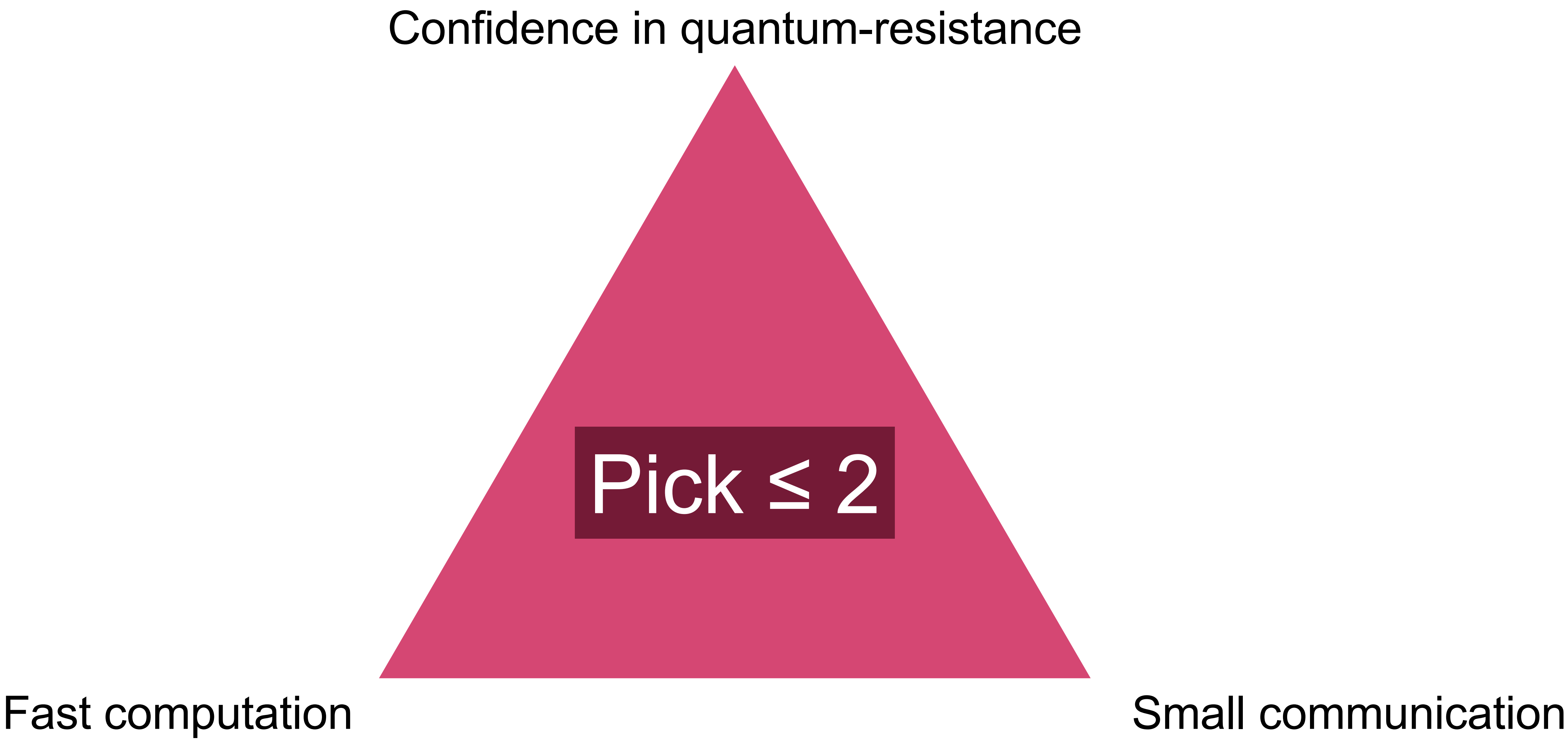
Hash-based & symmetric

Multivariate quadratic

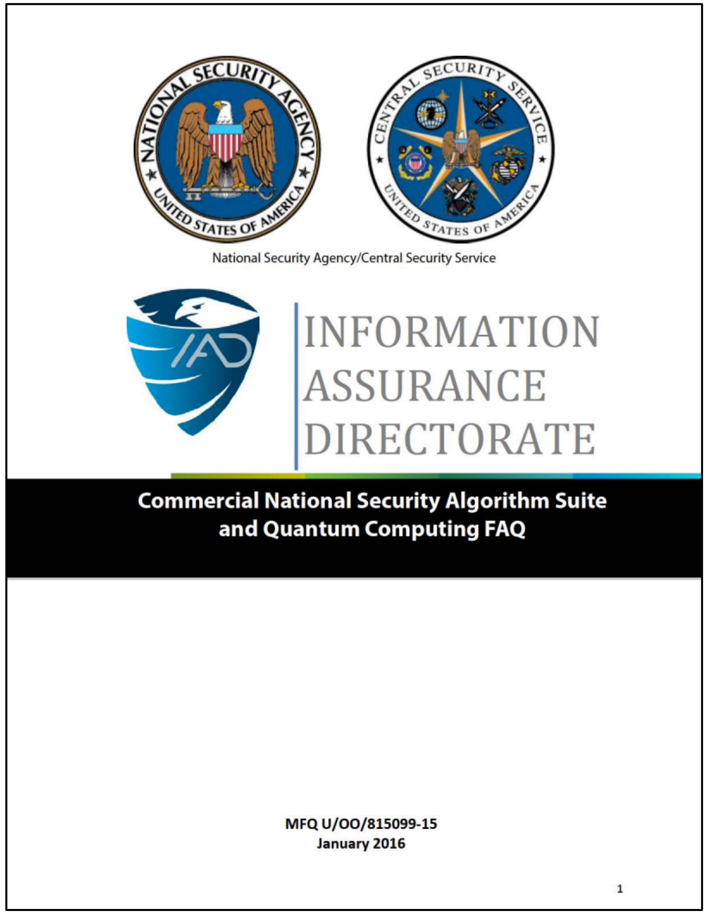
Code-based

Lattice-based

Elliptic curve isogenies


Confidence in quantum-resistance
Pick ≤ 2
Fast computation
Small communication

Standardizing post-quantum cryptography


National Security Agency/Central Security Service

INFORMATION
ASSURANCE
DIRECTORATE

Commercial National Security Algorithm Suite and Quantum Computing FAQ

MFQ U/OO/815099-15
January 2016

1

Aug. 2015 (Jan. 2016)

"IAD will initiate a transition to quantum resistant algorithms in the not too distant future."

– NSA Information Assurance Directorate, Aug. 2015


NIST

CSRC MENU

Search CSRC

COMPUTER SECURITY
RESOURCE CENTER

CSRC

Post-Quantum Cryptography

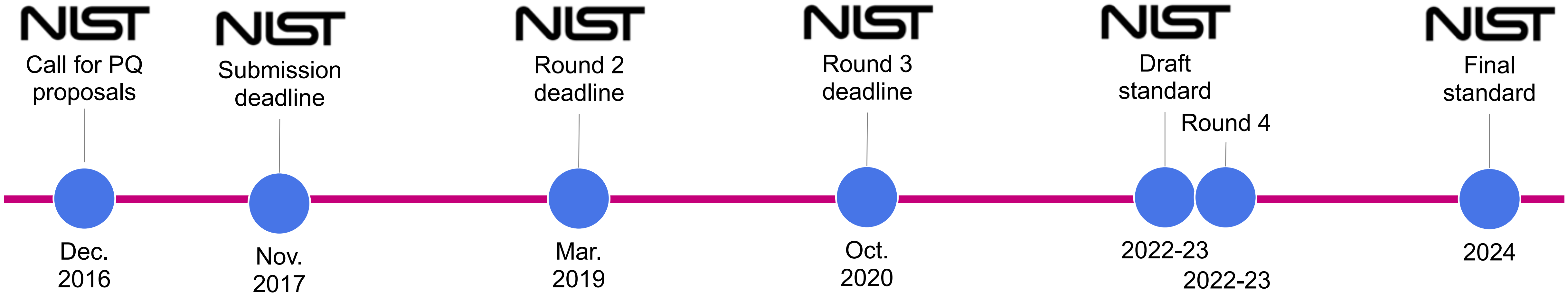
Post-Quantum Cryptography Standardization

Post-quantum candidate algorithm nominations are due November 30, 2017.
Call for Proposals

Call for Proposals Announcement

NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Currently, public-key cryptographic algorithms are specified in FIPS 186-4, *Digital Signature Standard*, as well as special publications SP 800-56A Revision 2, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography* and SP 800-56B Revision 1, *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer*

NIST Post-quantum Crypto Project timeline



Round 1:
69 schemes
1/3 signatures
2/3 PKE

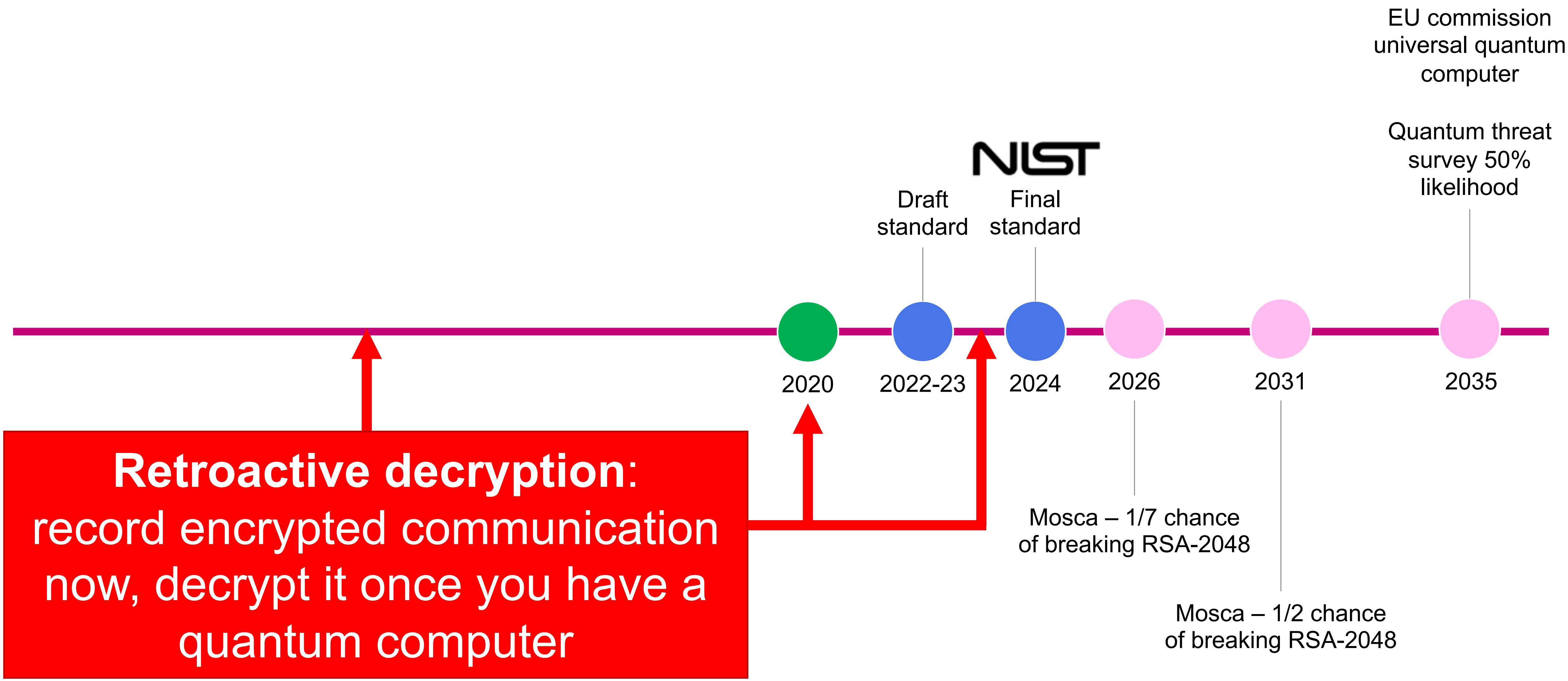
Round 2:
26 schemes
9 signatures
17 PKE

Round 3:
Finalists:
- 3 signatures
- 4 PKE

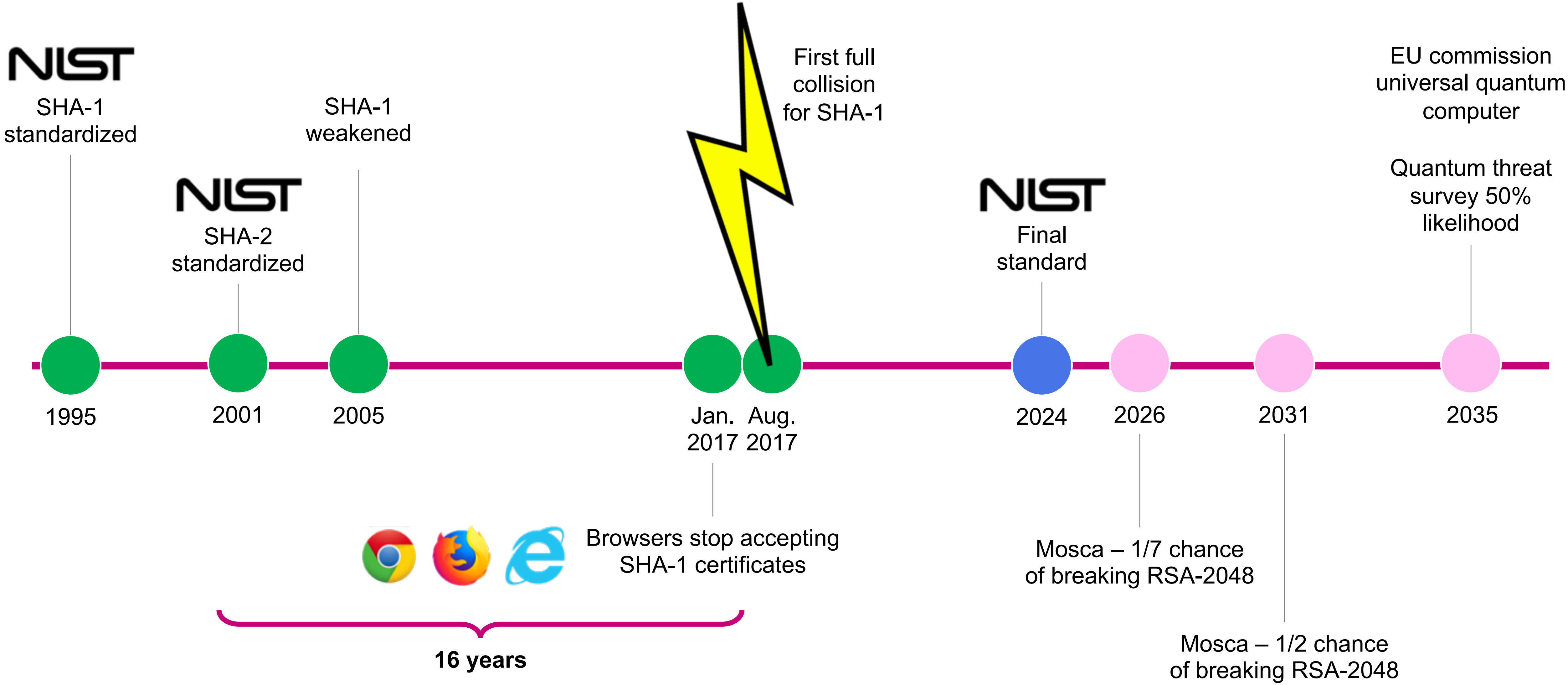
Alternates:
- 3 signatures
- 5 PKE

http://www.nist.gov/pqcrypto

Will we be ready in time?



Timeline to replace cryptographic algorithms



NIST Round 3

NIST Round 3

Finalists

Key encapsulation mechanisms

- Code-based: Classic McEliece
- Lattice-based: Kyber, NTRU, Saber
    - At most one of these 3 will be standardized

Signatures

- Lattice-based: Dilithium, Falcon
    - At most one of these 2 will be standardized
- Multivariate: Rainbow

Alternate candidates

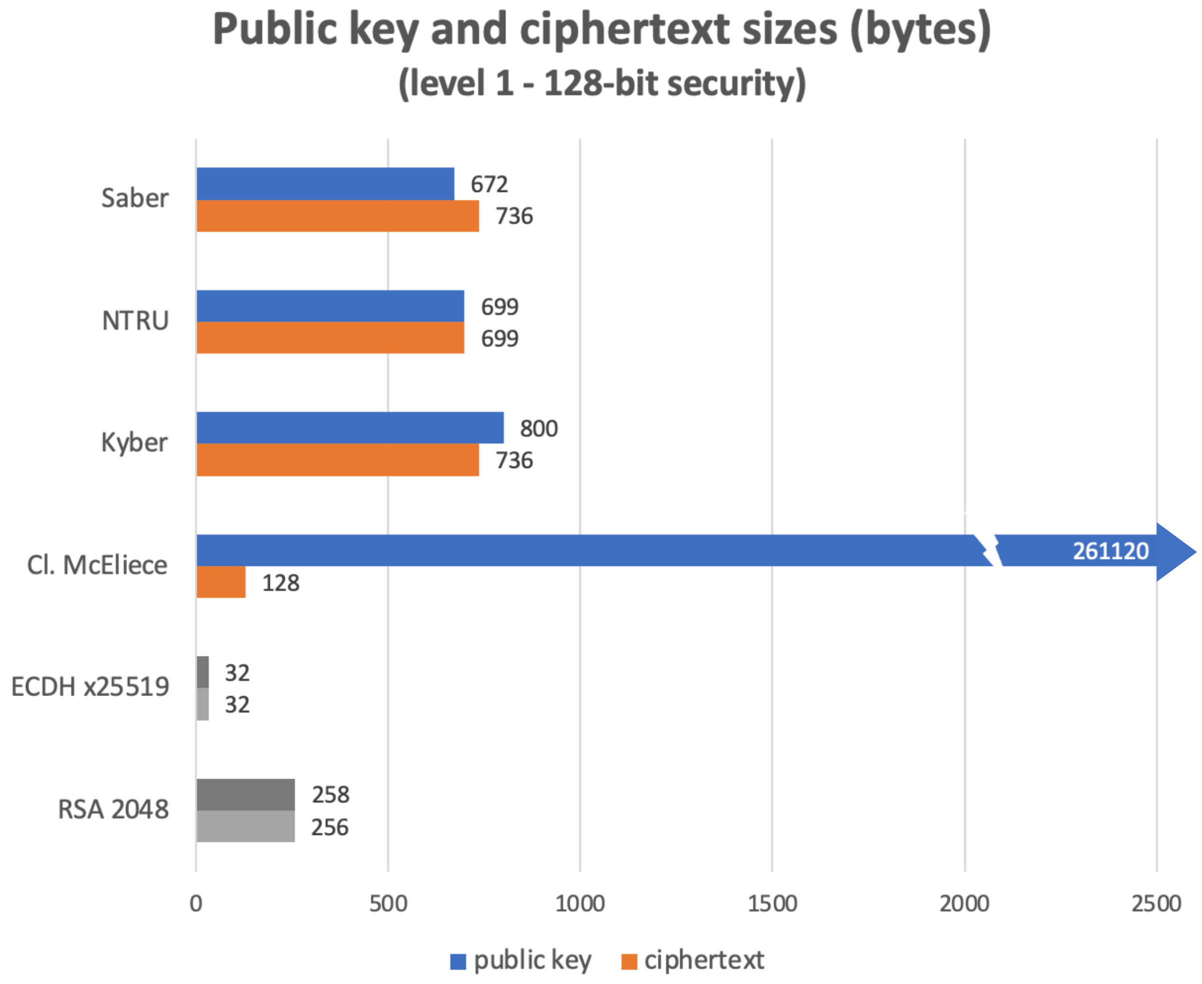
Key encapsulation mechanisms

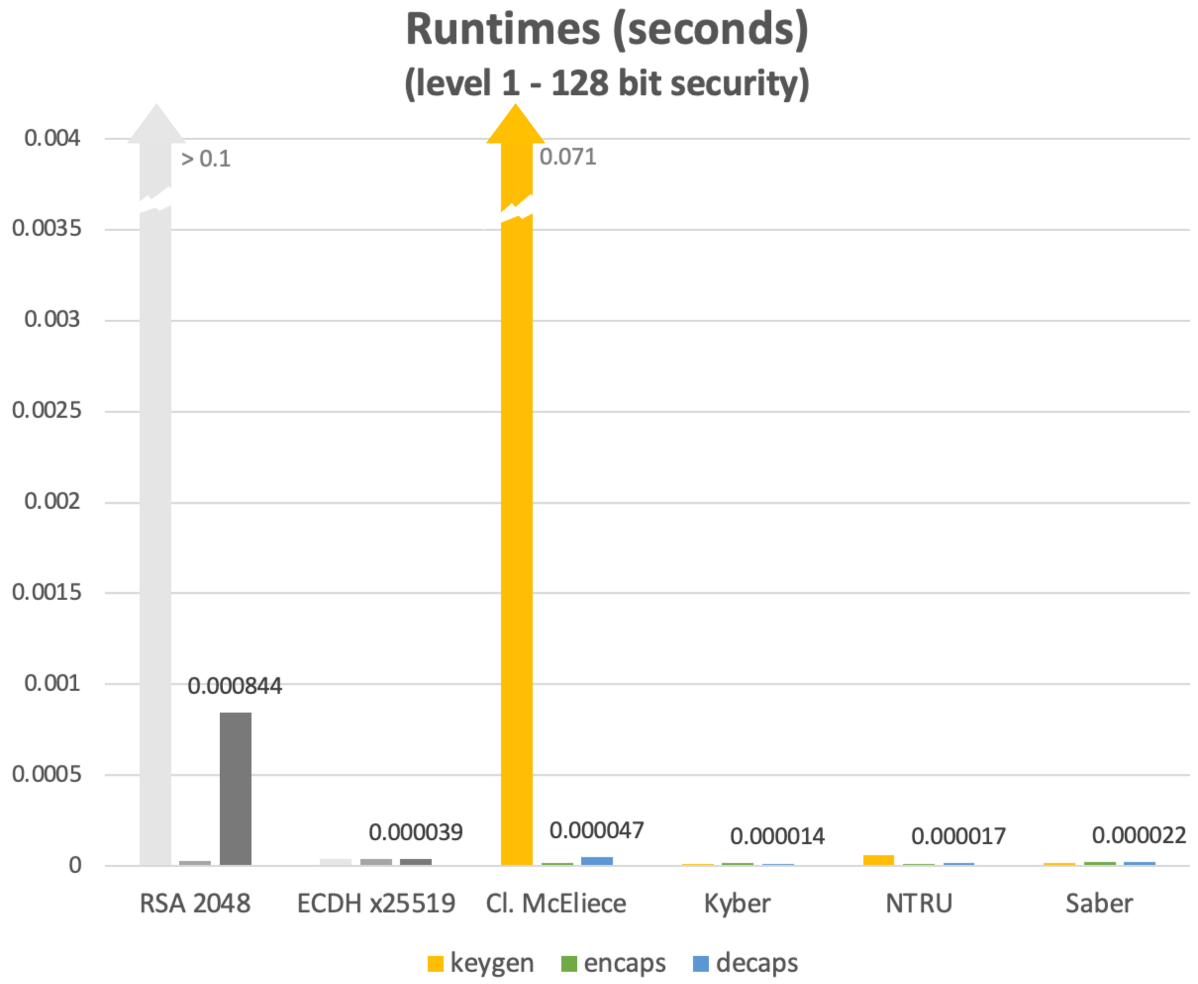
- Code-based: BIKE, HQC
- Lattice-based: FrodoKEM, NTRU Prime
- Isogeny-based: SIKE

Signatures

- Symmetric-based: Picnic, SPHINCS+
- Multivariate: GeMSS

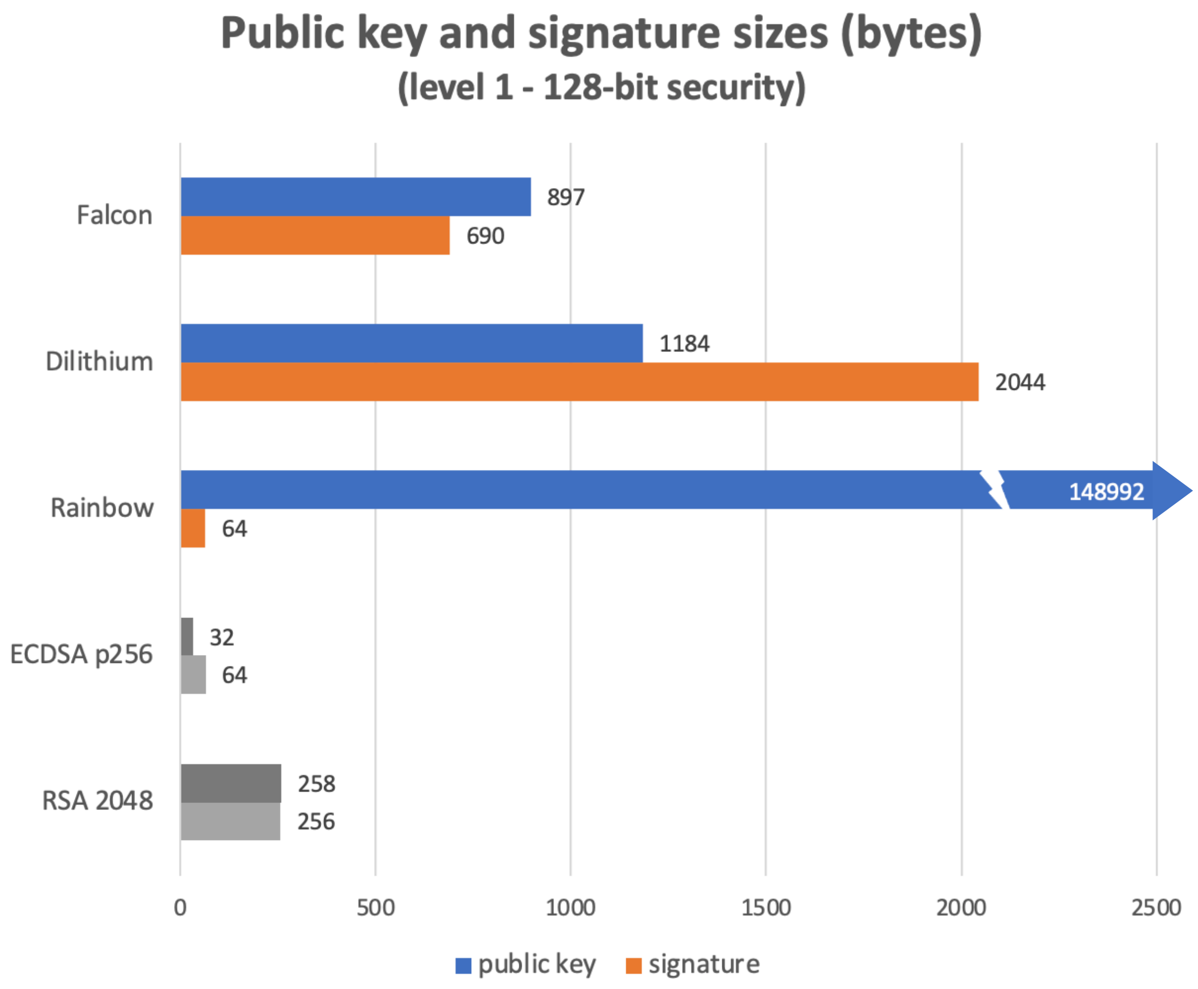
NIST Round 3 KEM Finalists

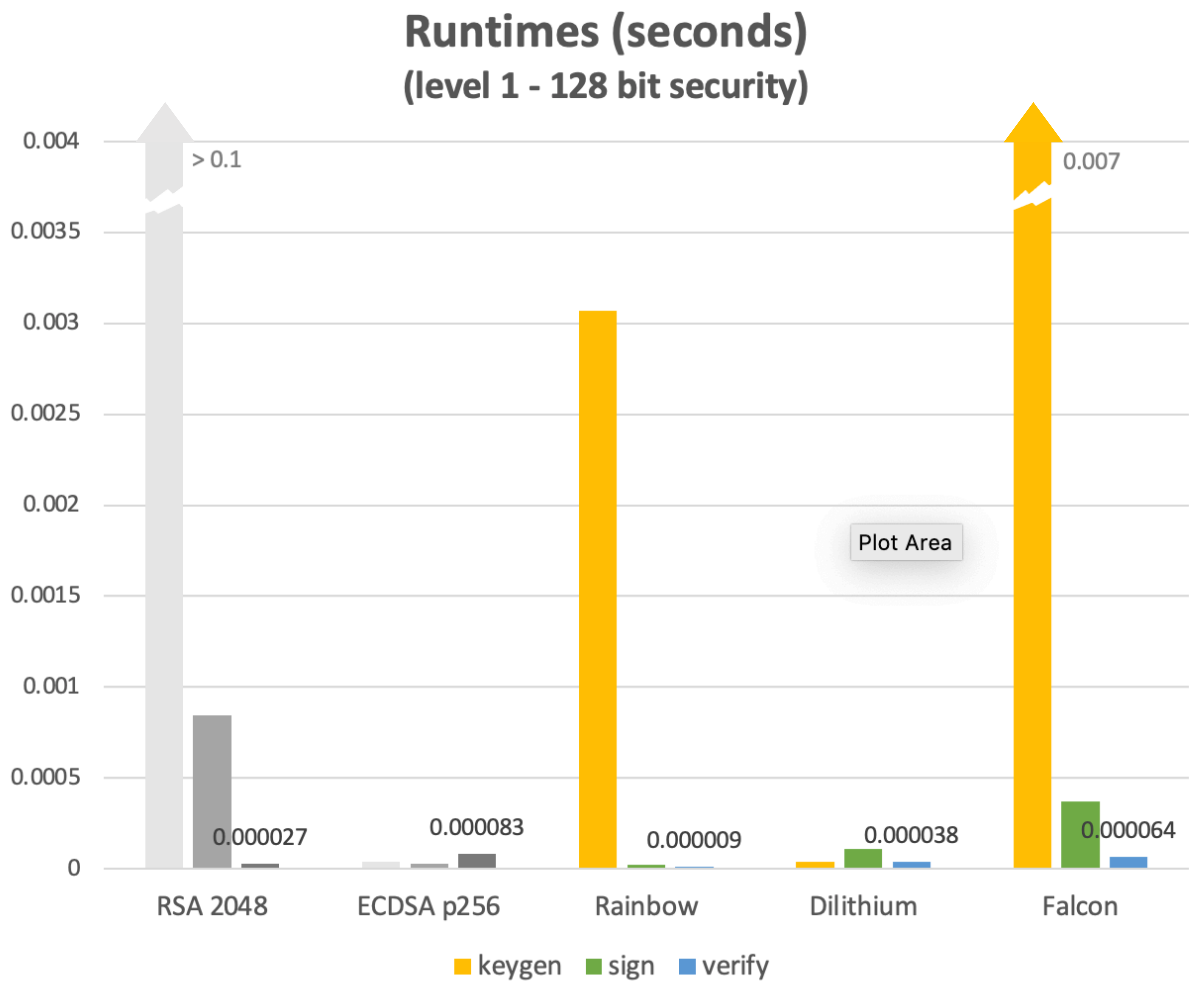




Based on Round 2 submission documents; AVX2 runtimes normalized

NIST Round 3 Signature Finalists





Based on Round 2 submission documents; AVX2 runtimes normalized

NIST's priorities for Round 3 analysis

Cryptanalysis

- Better understand CoreSVP hardness of lattice-based schemes
- Does choice of lattice structure matter?
- Decide between Kyber, NTRU, Saber
- Decide between Dilithium and Falcon

Implementations

- Side-channel resistant implementations
- Easy of implementation
- Performance data in Internet protocols
- Performance data for hardware implementations

Transitioning to post-quantum crypto

Open Quantum Safe Project

Use in applications

Apache httpd · nginx · curl, links · Open VPN · Chromium

Integration into forks of widely used open-source projects

OpenSSL
S/MIME, TLS 1.3, X.509

BoringSSL

Open SSH

Language SDKs
C#, C++, Go, Java, Python, Rust

C language library, common API
- x86/x64 (Linux, Mac, Windows)
- ARM (Android, Linux)

liboqs

key exchange / KEMs

signatures

isogenies · code-based · lattice-based · multi-variate polynomial · hash-based / symmetric

Industry partners:
- Amazon Web Services
- evolutionQ
- IBM Research
- Microsoft Research

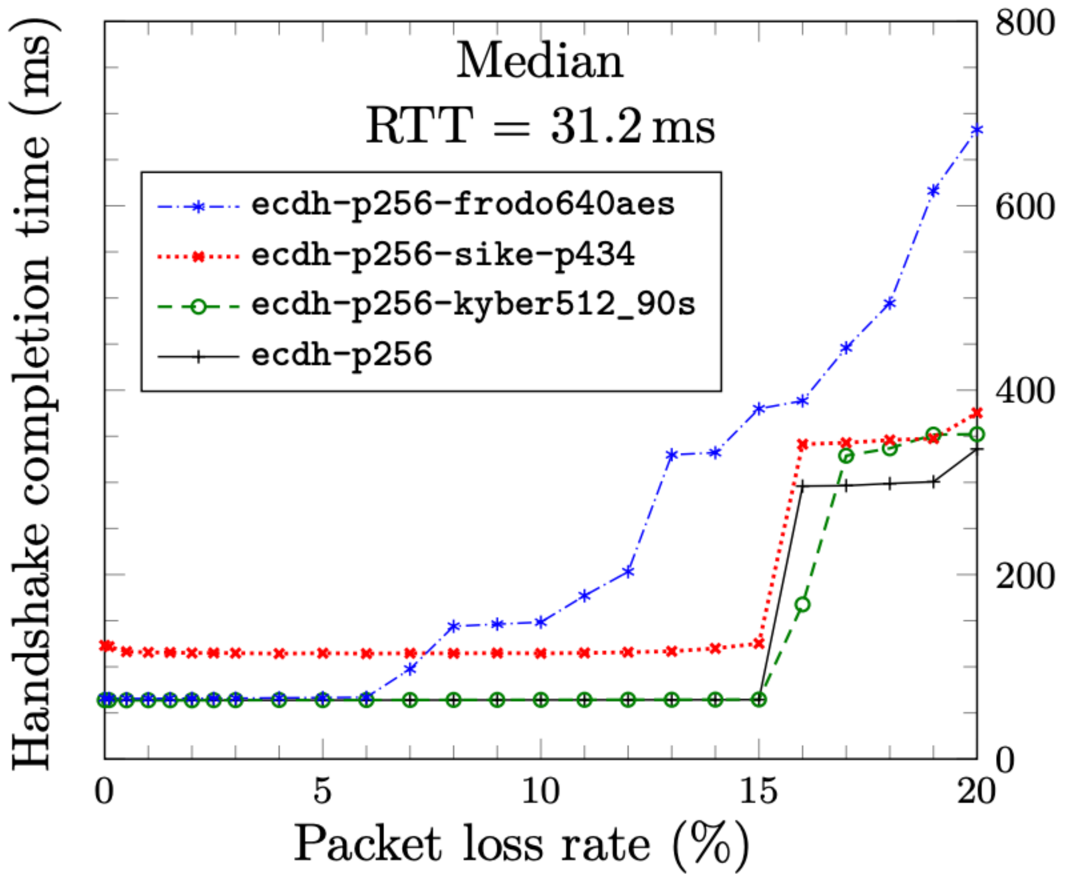
Additional contributors:
- Cisco
- Senetas
- PQClean project
- Individuals

Financial support:
- AWS
- Canadian Centre for Cyber Security
- NSERC

https://openquantumsafe.org/ • https://github.com/open-quantum-safe/

Prototyping PQ crypto in network protocols

- Designs for PQ and hybrid signatures in X.509 [1]
- Assess whether PQ algorithms satisfy TLS and SSH protocol size constraints [2]
- Measure network performance of PQ algorithms in TLS [3]
- IETF Internet-Drafts specifying hybrid post-quantum + traditional key exchange in TLS [4] and SSH



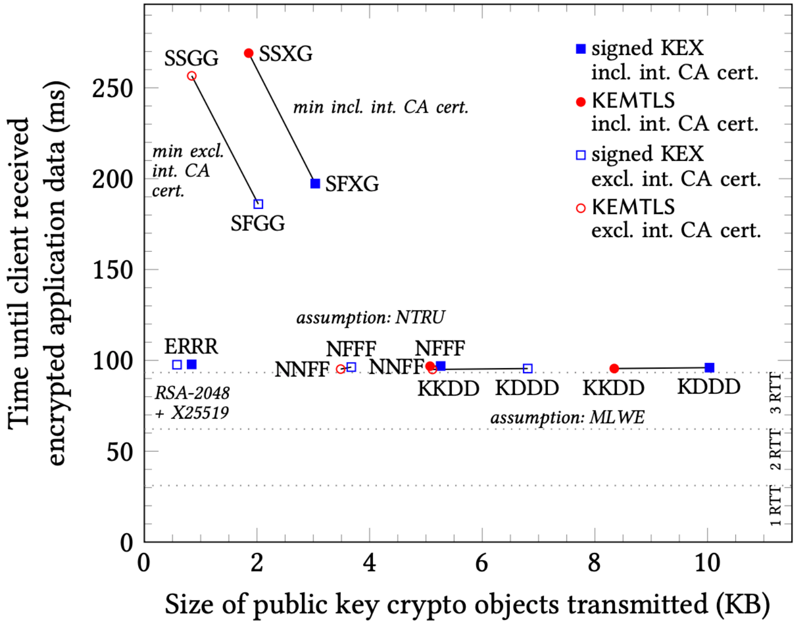
[1] https://eprint.iacr.org/2017/460 • [2] https://eprint.iacr.org/2019/858 • [3] https://eprint.iacr.org/2019/1447
[4] https://tools.ietf.org/html/draft-ietf-tls-hybrid-design-01

New approaches to protocols: PQ TLS without signatures

Problem: Post-quantum signatures are bigger than post-quantum KEMs.

Idea: Use KEMs for authenticated key exchange in the TLS handshake to save space.

- Simple to implement
- With isogenies, can get handshake size very close to current sizes
- Implicit rather than explicit authentication
- Different forward secrecy and downgrade resilience properties
- Increased benefits when caching intermediate CA certificates
- Interesting questions about certificate lifecycle management
- Working with Cloudflare to test within their infrastructure



Post-quantum crypto @ UWaterloo

- UW involved in two NIST Round 3 finalists (Kyber, NTRU) and two Round 3 alternate candidates (FrodoKEM, SIKE)
- Large team led by David Jao working on isogeny-based crypto
- Quantum cryptanalysis led by Michele Mosca
- CryptoWorks21 training program for quantum-resistant cryptography
- + quantum key distribution, quantum computing, …

The current status of post-quantum cryptography

Douglas Stebila

UNIVERSITY OF WATERLOO

NIST Round 3:
https://nist.gov/pqcrypto

Quantum threat timeline:
https://globalriskinstitute.org/publications/quantum-threat-timeline/

Open Quantum Safe project:
https://openquantumsafe.org/
https://github.com/open-quantum-safe/

Prototyping PQ crypto in network protocols:
https://eprint.iacr.org/2017/460 (X.509 certs)
https://eprint.iacr.org/2019/858 (SSH/TLS compat.)
https://eprint.iacr.org/2019/1447 (TLS perf.)
https://tools.ietf.org/html/draft-ietf-tls-hybrid-design-01
(TLS hybrid spec)

New protocol designs:
https://eprint.iacr.org/2020/534 (PQ TLS without sigs)
https://eprint.iacr.org/2019/1356 (other key exchange)