Post-Quantum Cryptography

Douglas Stebila

UNIVERSITY OF WATERLOO

Why post-quantum?

Ho…e | Mathematics | Universit

uwat…rloo.ca/math/

UNIVERSITY OF WATERLOO

ADMISSIONS ABOUT WATERLOO FACULTIES & ACADEMICS OFFICES & SERVICES SUPPORT WATERLOO COVID-19 SEARCH

MATHEMATICS

Combinatorics and Optimization researchers use computational complexity to further understand the quantum partition function

Researchers collaborate with IBM researchers and publish new research from their work with the Institute for Quantum Computing

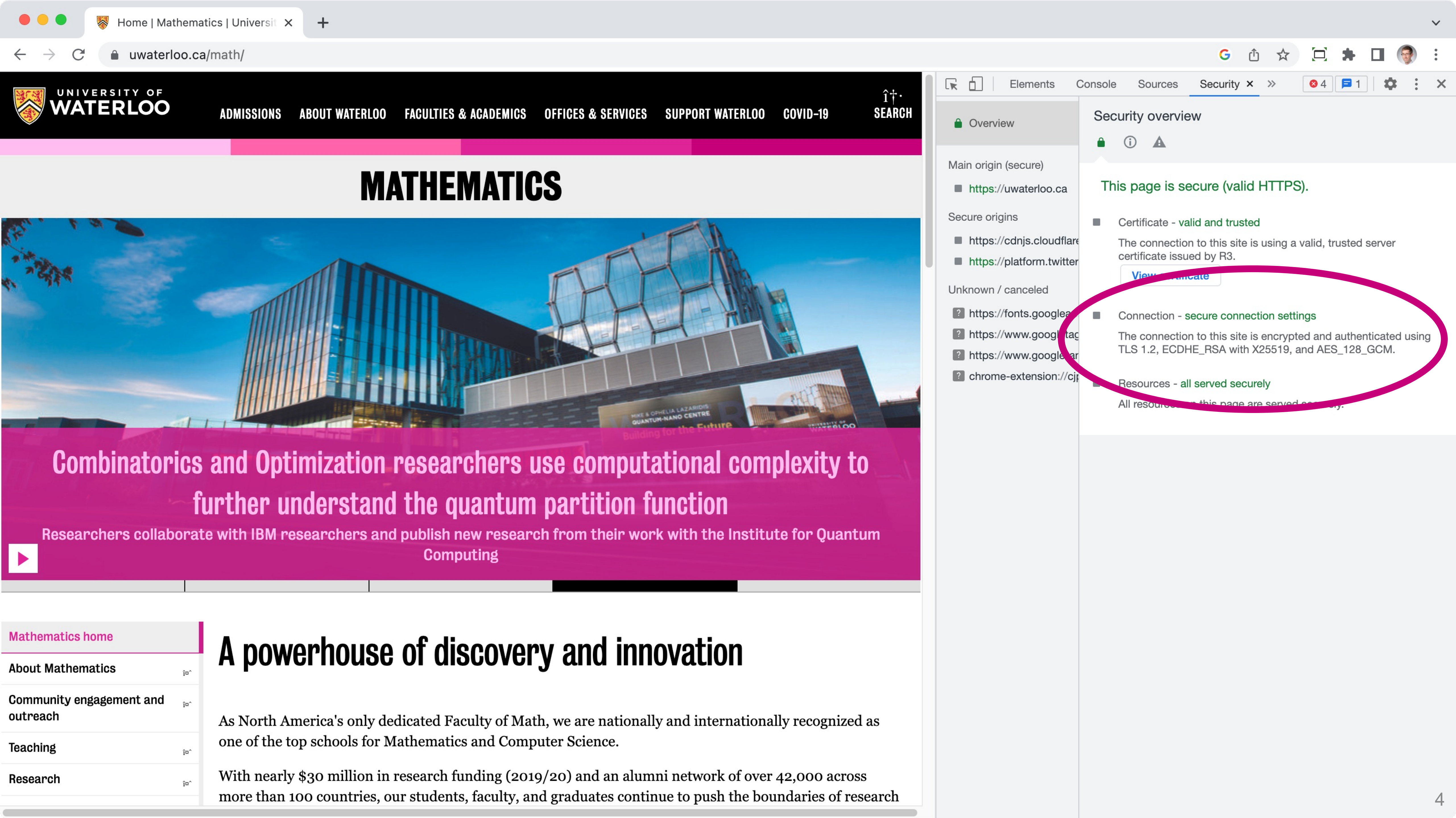
- Mathematics home
- About Mathematics
- Community engagement and outreach
- Teaching
- Research

A powerhouse of discovery and innovation

As North America's only dedicated Faculty of Math, we are nationally and internationally recognized as one of the top schools for Mathematics and Computer Science.

With nearly $30 million in research funding (2019/20) and an alumni network of over 42,000 across more than 100 countries, our students, faculty, and graduates continue to push the boundaries of research …scover new ways to harness the power of mathematics, computer science, and statistics

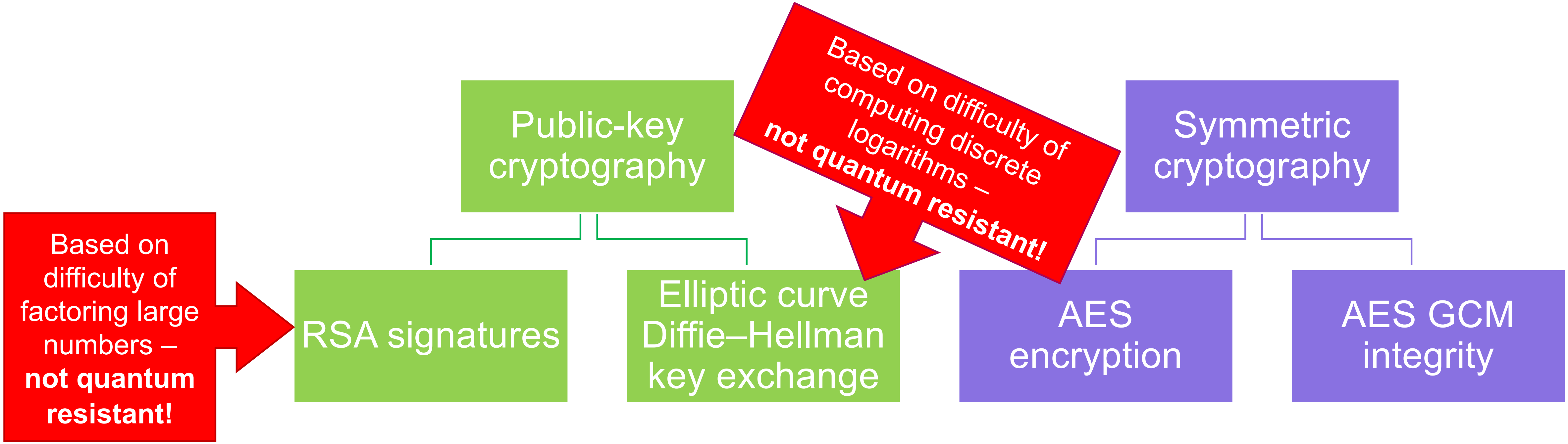
https://uwaterloo.ca/math/news/combinatorics-and-optimization-researchers-use-computational


Home | Mathematics | Universit
uwaterloo.ca/math/
UNIVERSITY OF WATERLOO
ADMISSIONS
ABOUT WATERLOO
FACULTIES & ACADEMICS
OFFICES & SERVICES
SUPPORT WATERLOO
COVID-19
SEARCH
MATHEMATICS
Combinatorics and Optimization researchers use computational complexity to further understand the quantum partition function
Researchers collaborate with IBM researchers and publish new research from their work with the Institute for Quantum Computing
Mathematics home
About Mathematics
Community engagement and outreach
Teaching
Research
A powerhouse of discovery and innovation
As North America's only dedicated Faculty of Math, we are nationally and internationally recognized as one of the top schools for Mathematics and Computer Science.
With nearly $30 million in research funding (2019/20) and an alumni network of over 42,000 across more than 100 countries, our students, faculty, and graduates continue to push the boundaries of research
Elements
Console
Sources
Security
Overview
Main origin (secure)
https://uwaterloo.ca
Secure origins
https://cdnjs.cloudflare
https://platform.twitter
Unknown / canceled
https://fonts.googlea
https://www.googl tag
https://www.google ar
chrome-extension://cj
Security overview
This page is secure (valid HTTPS).
Certificate - valid and trusted
The connection to this site is using a valid, trusted server certificate issued by R3.
Connection - secure connection settings
The connection to this site is encrypted and authenticated using TLS 1.2, ECDHE_RSA with X25519, and AES_128_GCM.
Resources - all served securely

Cryptographic building blocks

Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.2, ECDHE_RSA with X25519, and AES_128_GCM.



Post-quantum cryptography

a.k.a. quantum-resistant algorithms

Cryptography based on computational assumptions believed to be resistant to attacks by quantum computers

Uses only classical (non-quantum) operations to implement

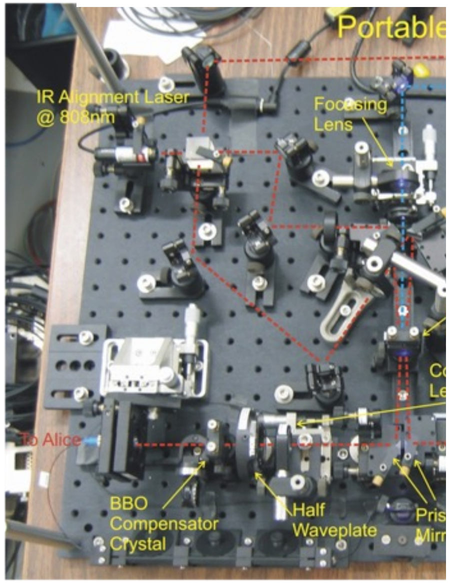
Quantum key distribution

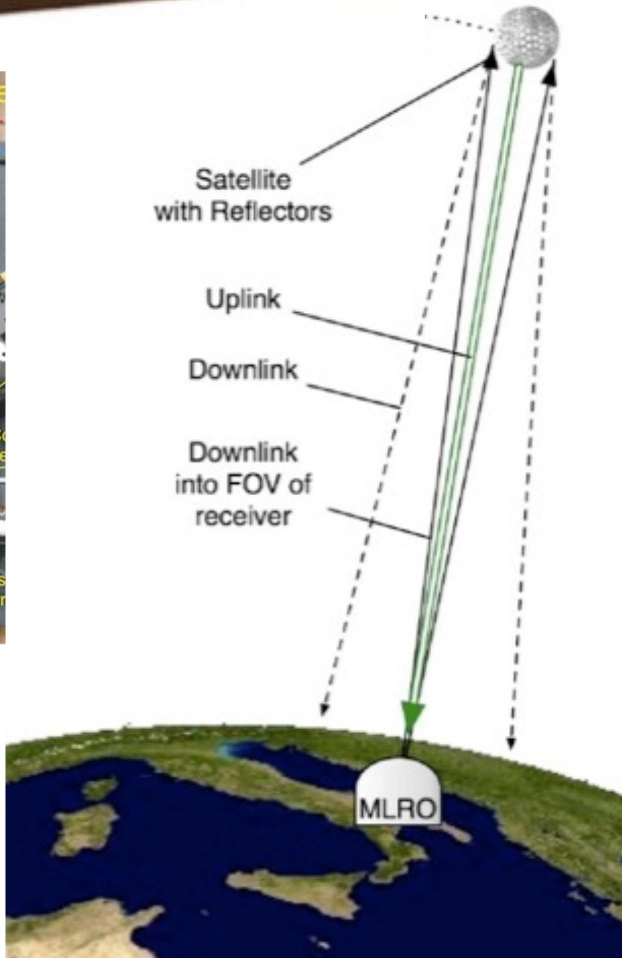
Also provides quantum-resistant confidentiality

Uses quantum mechanics to protect information

Doesn't require a full quantum computer

=> Not the subject of this talk



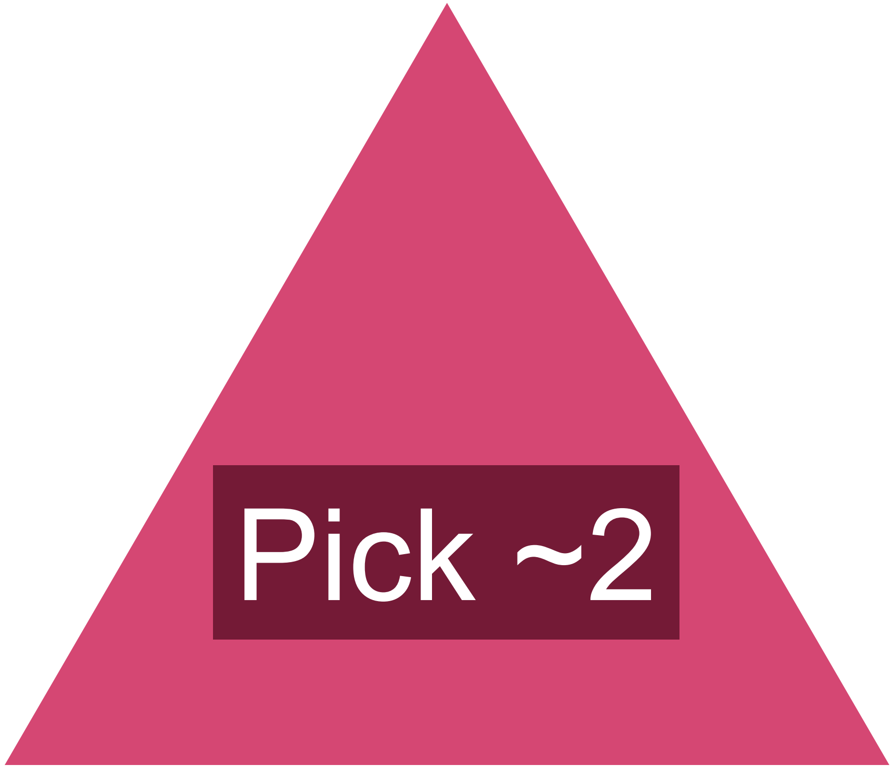


Post-quantum	QKD
Security depends on computational assumptions	Can be information-theoretically secure
Works on existing infrastructure	Requires new devices and communication channels
No limitations on communication distance	Limits on communication distance without new technology (repeaters) or additional trusts assumptions

<table>
<tr><th colspan="2">Post-quantum</th><th>Traditional public key crypto</th></tr>
<tr><td colspan="2">Computational assumptions studied since</td><td rowspan="2">Computational assumptions studied since 1970s / 1980s</td></tr>
<tr><td>1970s</td><td>1990s/2000s/2010s</td></tr>
<tr><td colspan="2">Conjecturally resistant to quantum attacks</td><td>Vulnerable to quantum attacks</td></tr>
<tr><td colspan="2">Medium to large communication sizes (700–30000+ bytes)</td><td>Small communication sizes (32–384 bytes)</td></tr>
<tr><td colspan="2">Sub-millisecond computation times</td><td>Sub-millisecond computation times</td></tr>
<tr><td colspan="2">Less flexible for building fancy cryptography</td><td>Flexible for building fancy crypto</td></tr>
</table>

Trade-offs with post-quantum crypto

Long standing confidence in quantum-resistance



Fast computation

Small communication

Families of post-quantum cryptography

Hash- & symmetric-based

- Can only be used to make signatures, not public key encryption
- Very high confidence in hash-based signatures, but large signatures required for many signature-systems

Code-based

- Long-studied cryptosystems with moderately high confidence for some code families
- Challenges in communication sizes

Multivariate quadratic

- Variety of systems with various levels of confidence and trade-offs
- Substantial break of Rainbow algorithm in Round 3

Lattice-based

- High level of academic interest in this field, flexible constructions
- Can achieve reasonable communication sizes

Elliptic curve isogenies

- Newest mathematical construction
- Small communication, slower computation
- Substantial break of SIKE in Round 4

Primary goals for post-quantum crypto

Confidentiality in the public key setting

- **Public key encryption schemes**
- Alternatively: key encapsulation mechanisms
  - KEMs are a generalization of two-party Diffie–Hellman-style key exchange
  - Easy to convert KEM into PKE and vice versa

Authentication & integrity in the public key setting

- **Digital signature schemes**

Standardization of PQ cryptography

The path to standardization

Principles

- Legislation
- Regulators

Policies

- Standards organizations: ISO, …
- Industry bodies:
  - PCI-DSS, ANSI, NIST, …

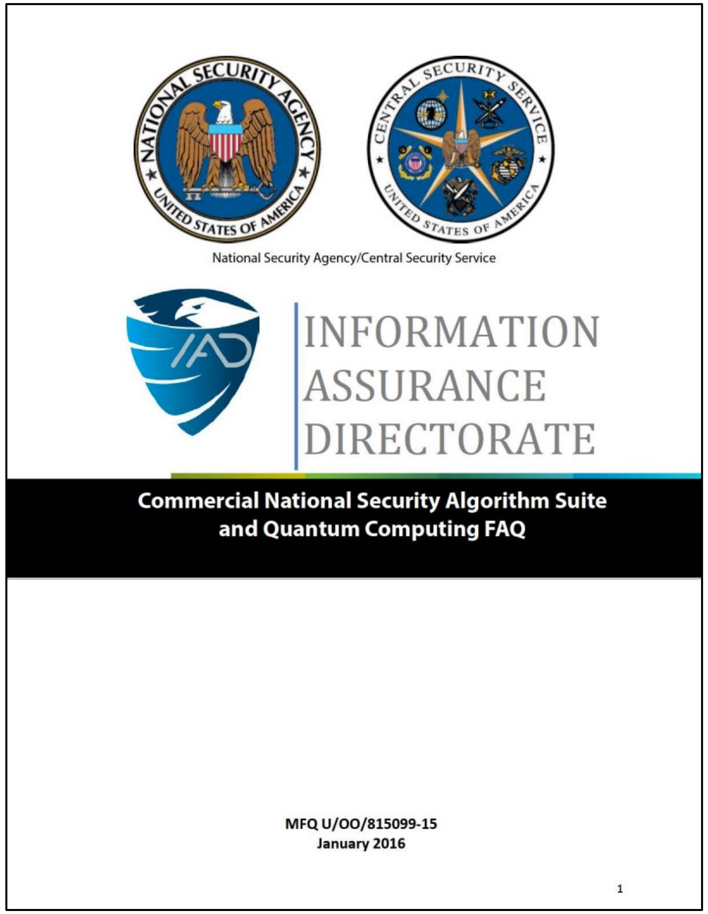
Protocols

- Technology standards organizations
  - IETF, ANSI, ...

Mathematics

- Specialist organizations
  - NIST, CFRG

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

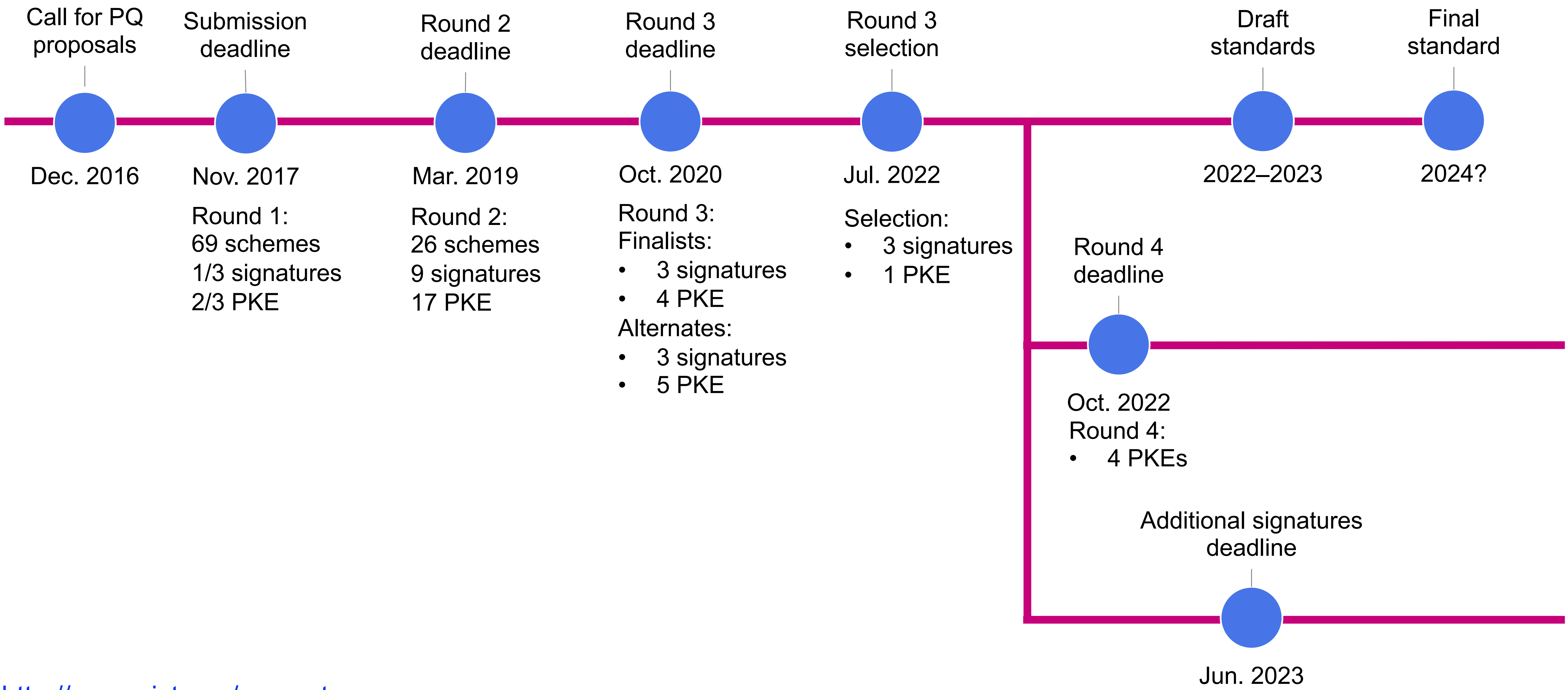
1

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 Post-quantum Crypto Project timeline



http://www.nist.gov/pqcrypto

NIST Round 3 selections and Round 4

Selections

Key encapsulation mechanisms

- Lattice-based: Kyber

Signatures

- Lattice-based: Dilithium, Falcon
- Hash-based: SPHINCS+

Round 4

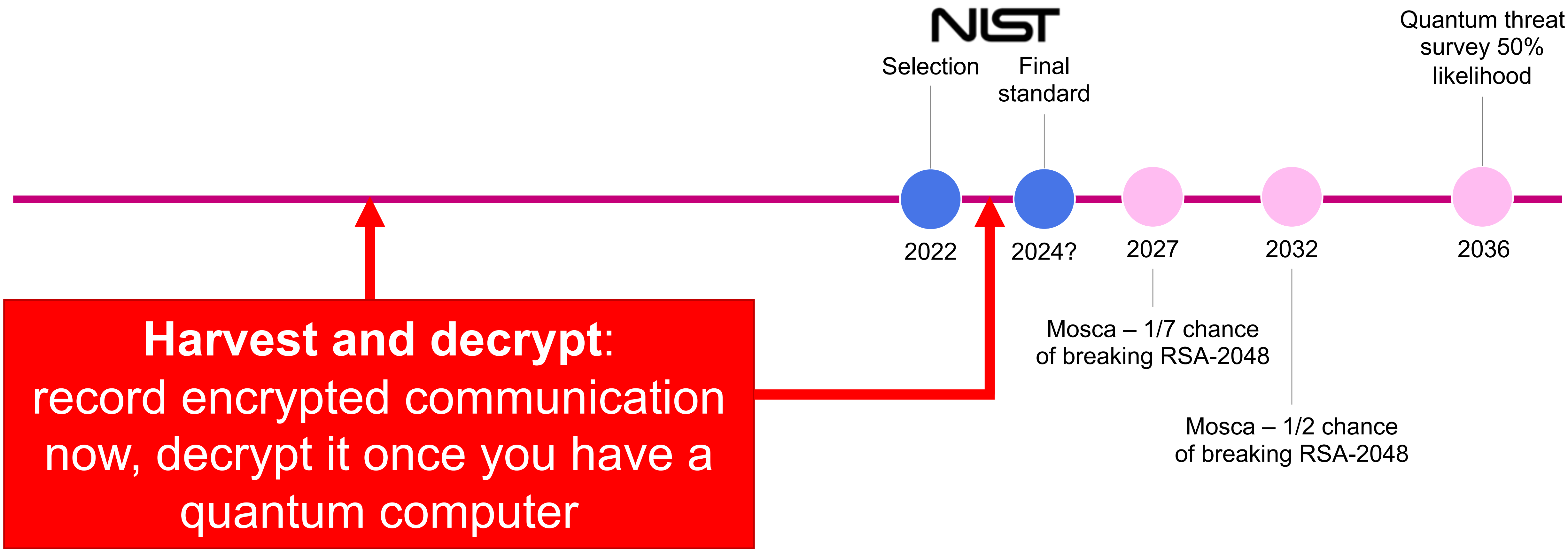
Key encapsulation mechanisms

- Code-based: BIKE, Classic McEliece, HQC
- ~~Isogeny-based: SIKE~~

Signatures

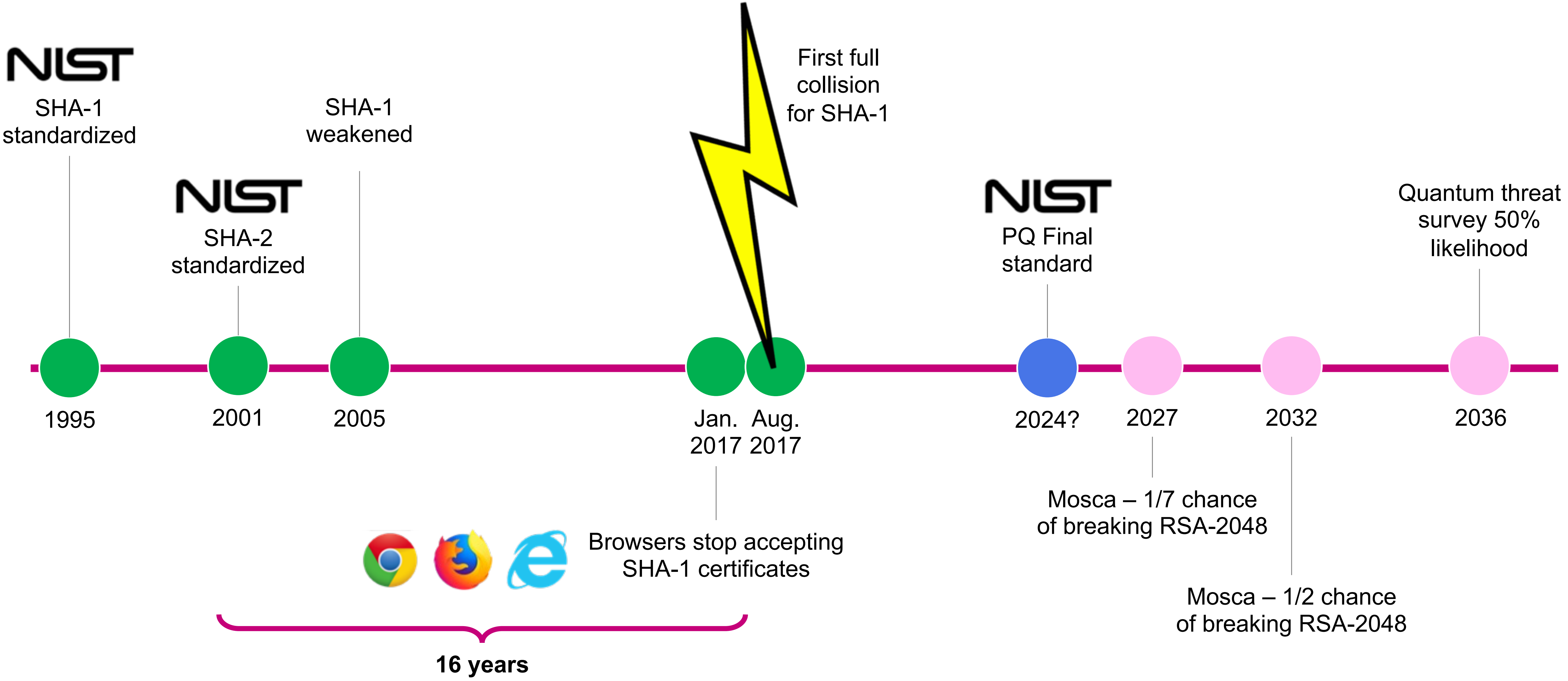
- There will be an "on-ramp" for new signature schemes

Will we be ready in time?

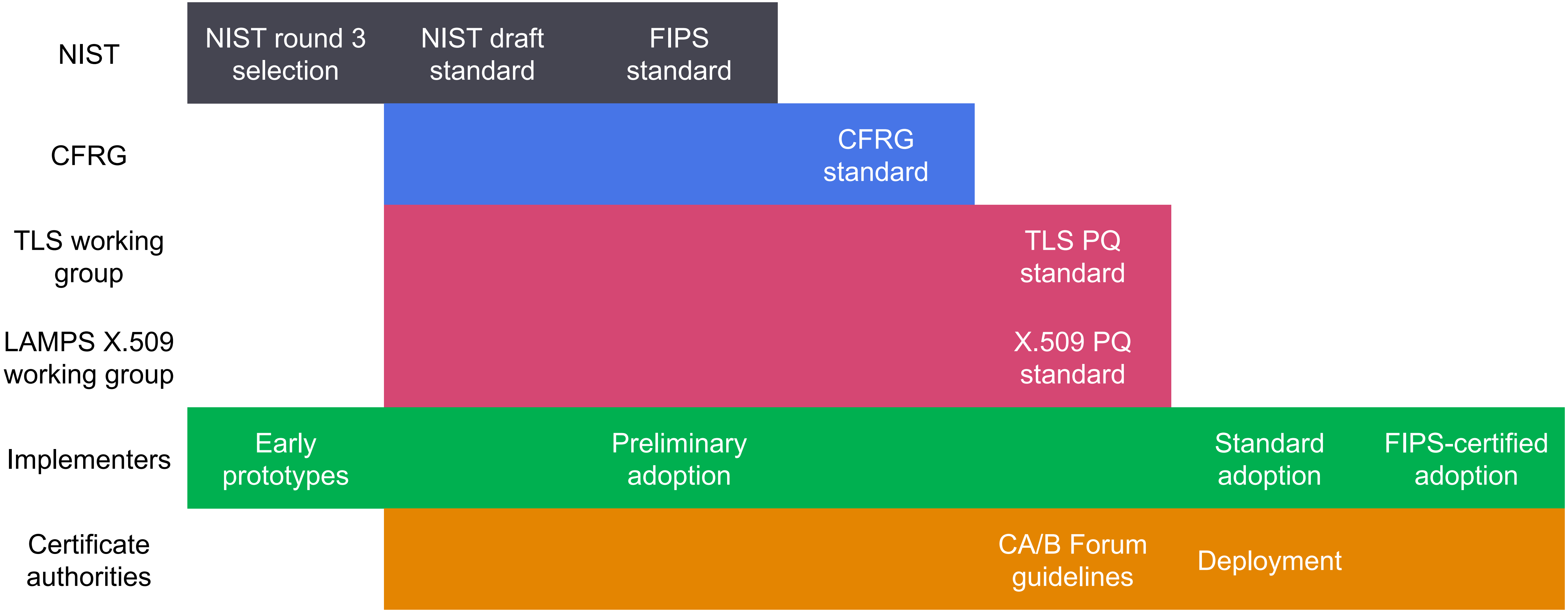


[Mosca] IEEE Security & Privacy 16(5):38–41, Sep/Oct 2018. https://doi.org/10.1109/MSP.2018.3761723
[Quantum threat] https://evolutionq.com/quantum-threat-timeline-2021.html

Timeline to replace cryptographic algorithms



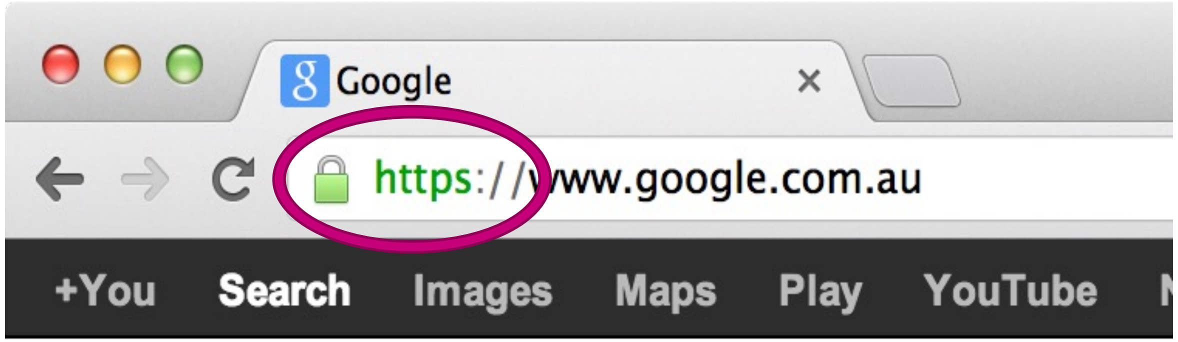
Paths to standardization and adoption



Making TLS post-quantum

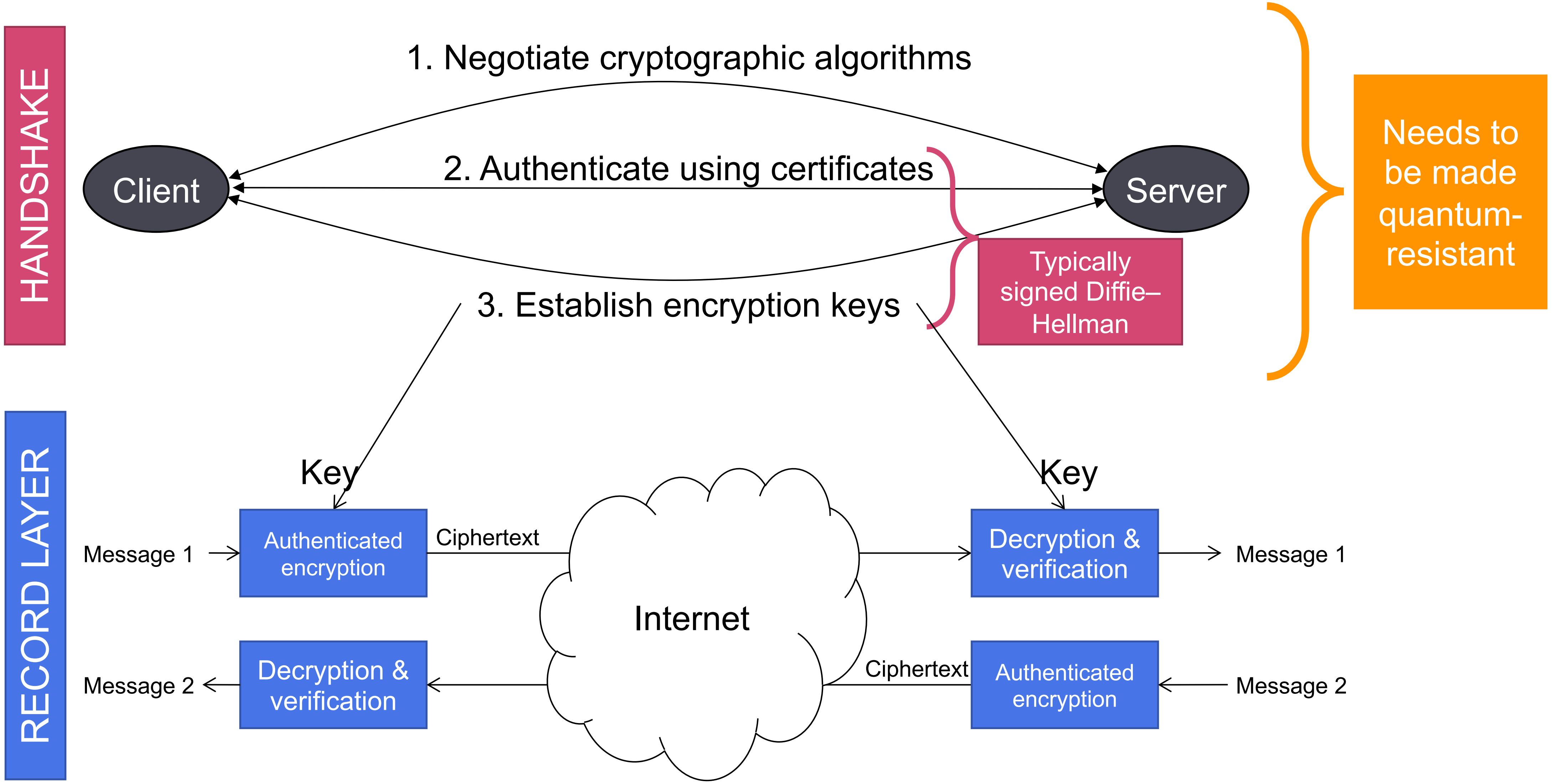
Transport Layer Security (TLS) protocol

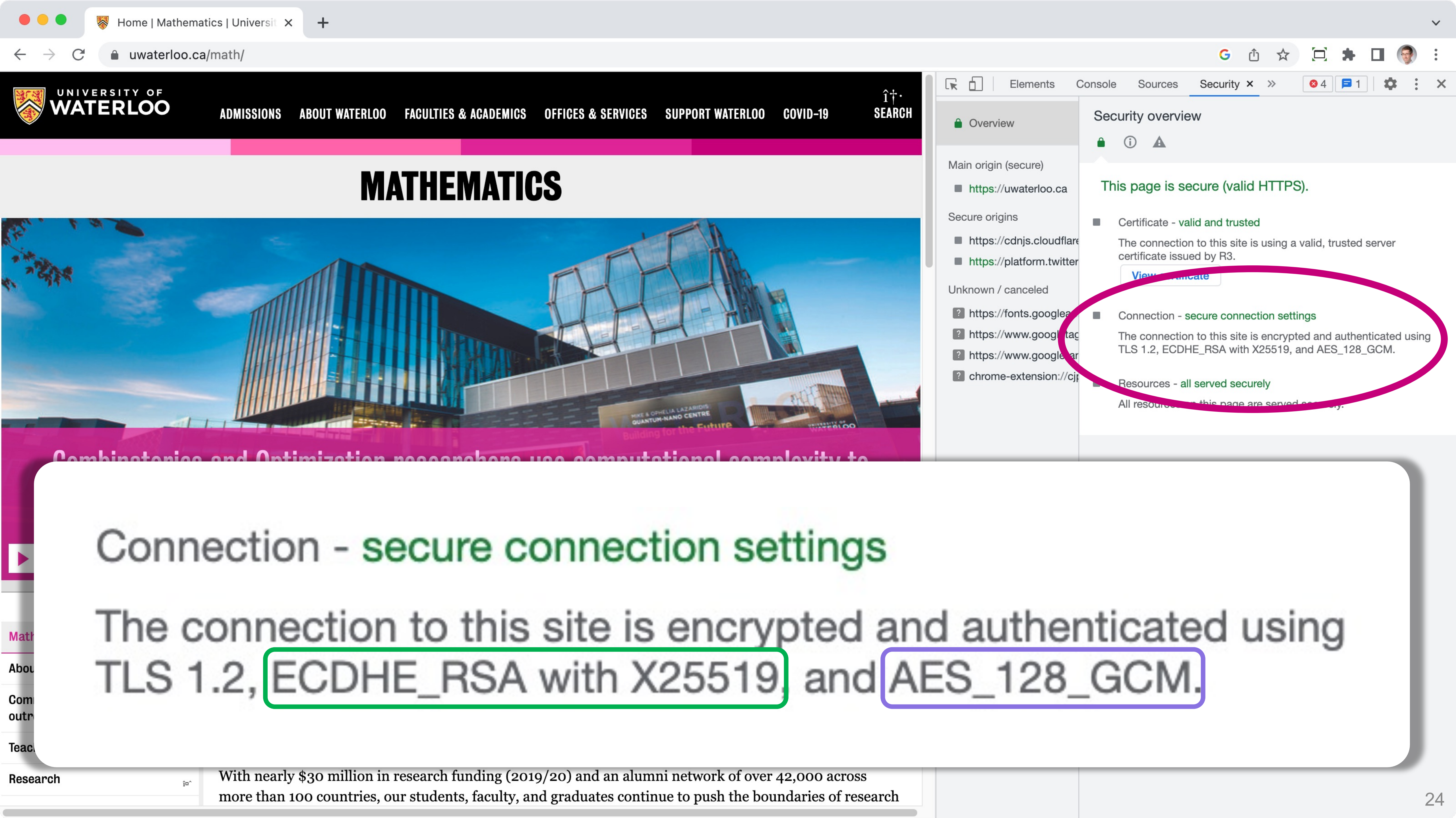
- Most important cryptographic protocol on the Internet
- The “S” in HTTPS



- Originally SSL (Secure Sockets Layer) by Netscape in 1995
- Standardized by IETF as TLS 1.0 in 1999; current version is TLS 1.3 (2018)
- Required by default for all web browsers since ~2021

SSL/TLS Protocol




Home | Mathematics | Universit
uwaterloo.ca/math/
UNIVERSITY OF WATERLOO
ADMISSIONS
ABOUT WATERLOO
FACULTIES & ACADEMICS
OFFICES & SERVICES
SUPPORT WATERLOO
COVID-19
SEARCH
MATHEMATICS
Elements
Console
Sources
Security
Overview
Main origin (secure)
https://uwaterloo.ca
Secure origins
Unknown / canceled
Security overview
This page is secure (valid HTTPS).
Certificate - valid and trusted
The connection to this site is using a valid, trusted server certificate issued by R3.
Connection - secure connection settings
The connection to this site is encrypted and authenticated using TLS 1.2, ECDHE_RSA with X25519, and AES_128_GCM.
Resources - all served securely
Connection - secure connection settings
The connection to this site is encrypted and authenticated using TLS 1.2, ECDHE_RSA with X25519 and AES_128_GCM.
Research
With nearly $30 million in research funding (2019/20) and an alumni network of over 42,000 across more than 100 countries, our students, faculty, and graduates continue to push the boundaries of research

Four TLS 1.3 modes

Signed Diffie–Hellman, server-only authentication

Signed Diffie–Hellman, mutual authentication

Pre-shared key (PSK)

Already PQ!

Pre-shared key with ephemeral Diffie–Hellman (PSK-ECDHE)

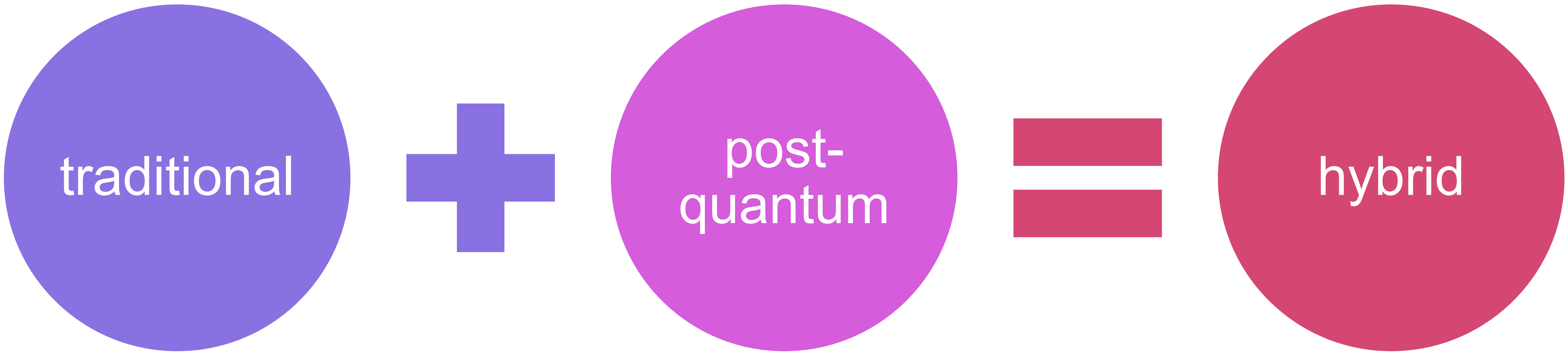
Three dimensions of "post-quantum TLS"

What is “post-quantum TLS”?

Pre-shared key (PSK) mode	Post-quantum key exchange	Classical+PQ key exchange	Post-quantum signatures	Classical+PQ signatures	Alternative protocol designs
• Already supported! • Still has the key distribution problem • No PQ forward secrecy	• Easiest to implement • Easy backwards compatibility • Needed soonest: harvest now & decrypt later with quantum computer	• “Hybrid” • Easy to implement • Possibly in demand during pre-FIPS-certification period			

Cautious “hybrid” approach

Hybrid approach: use traditional and post-quantum simultaneously such that successful attack needs to break both



Why use two (or more) algorithms?

1. Reduce risk from break of one algorithm

2. Ease transition with improved backwards compatibility

3. Standards compliance during transition

What is “post-quantum TLS”?

Pre-shared key (PSK) mode

- Already supported!
- Still has the key distribution problem
- No PQ forward secrecy

Post-quantum key exchange

- Easiest to implement
- Easy backwards compatibility
- Needed soonest: harvest now & decrypt later with quantum computer

Classical+PQ key exchange

- “Hybrid”
- Easy to implement
- Possibly in demand during pre-FIPS-certification period

Post-quantum signatures

- On the web: requires coordination with certificate authorities
- Less urgently needed: can’t retroactively break channel authentication

Classical+PQ signatures

- “Hybrid” or “Composite”
- May not make sense in the context of a negotiated protocol like TLS

Alternative protocol designs

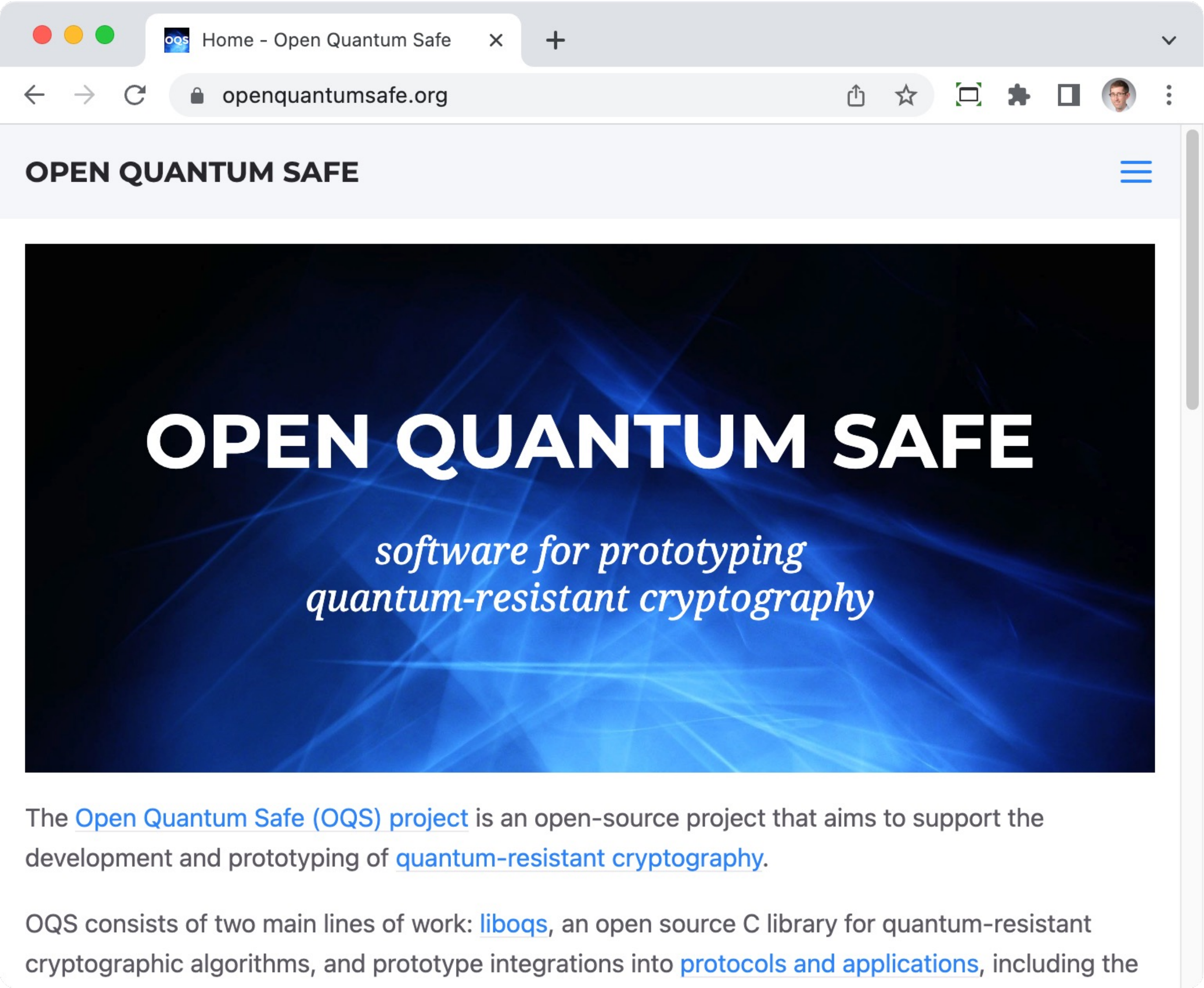
- Harder to implement; may require state machine or architecture changes
- Lots of interesting research to do!

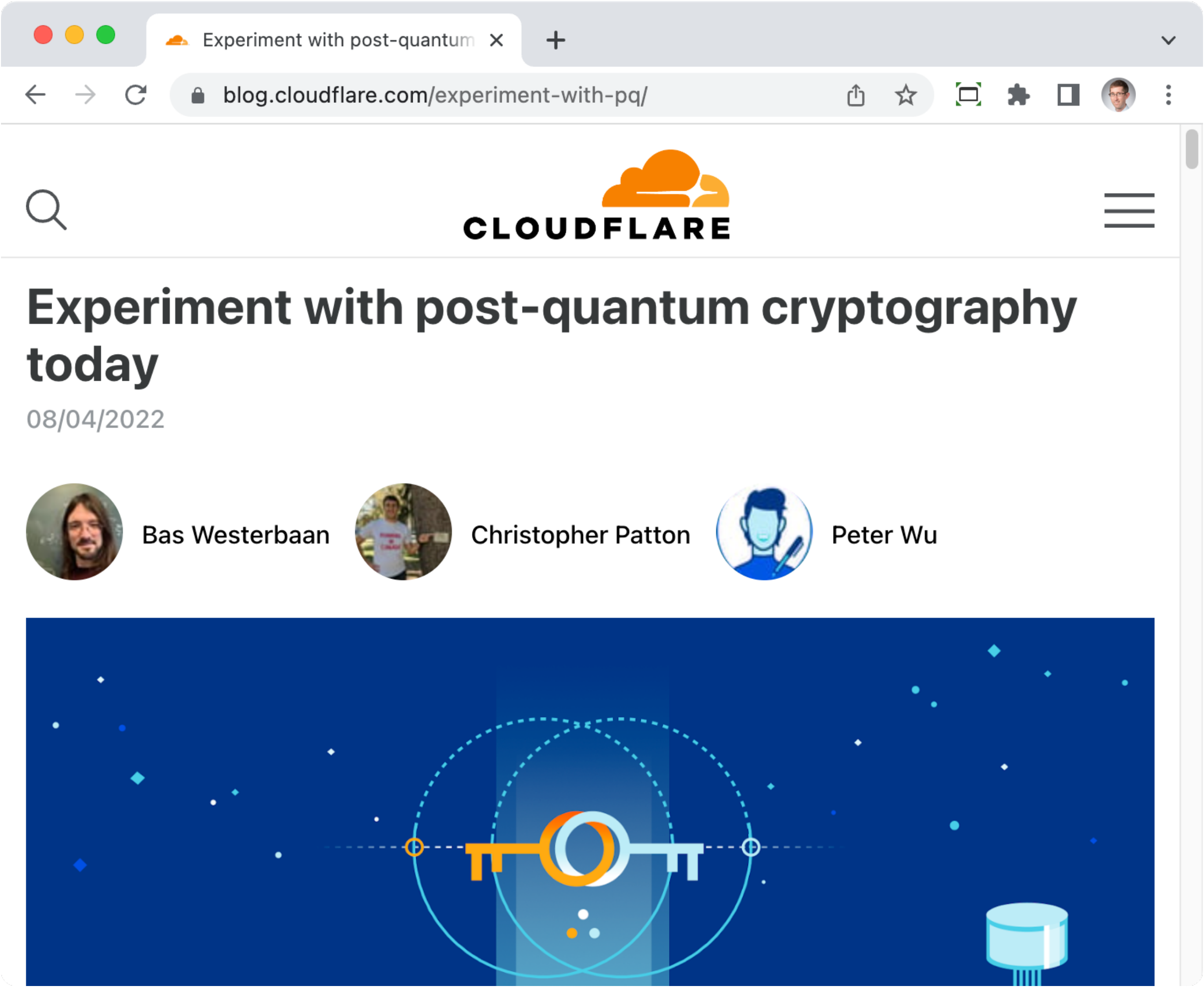
Hybrid key exchange in TLS 1.3

- General structures for hybrid post-quantum + classical key exchange in TLS 1.3
- No algorithm specifications included – to be defined elsewhere via NIST and CFRG
- Standardization paused until algorithms ready
- Preliminary implementations available

Stebila, Fluhrer, Gueron. https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/

Preliminary PQ TLS experiments





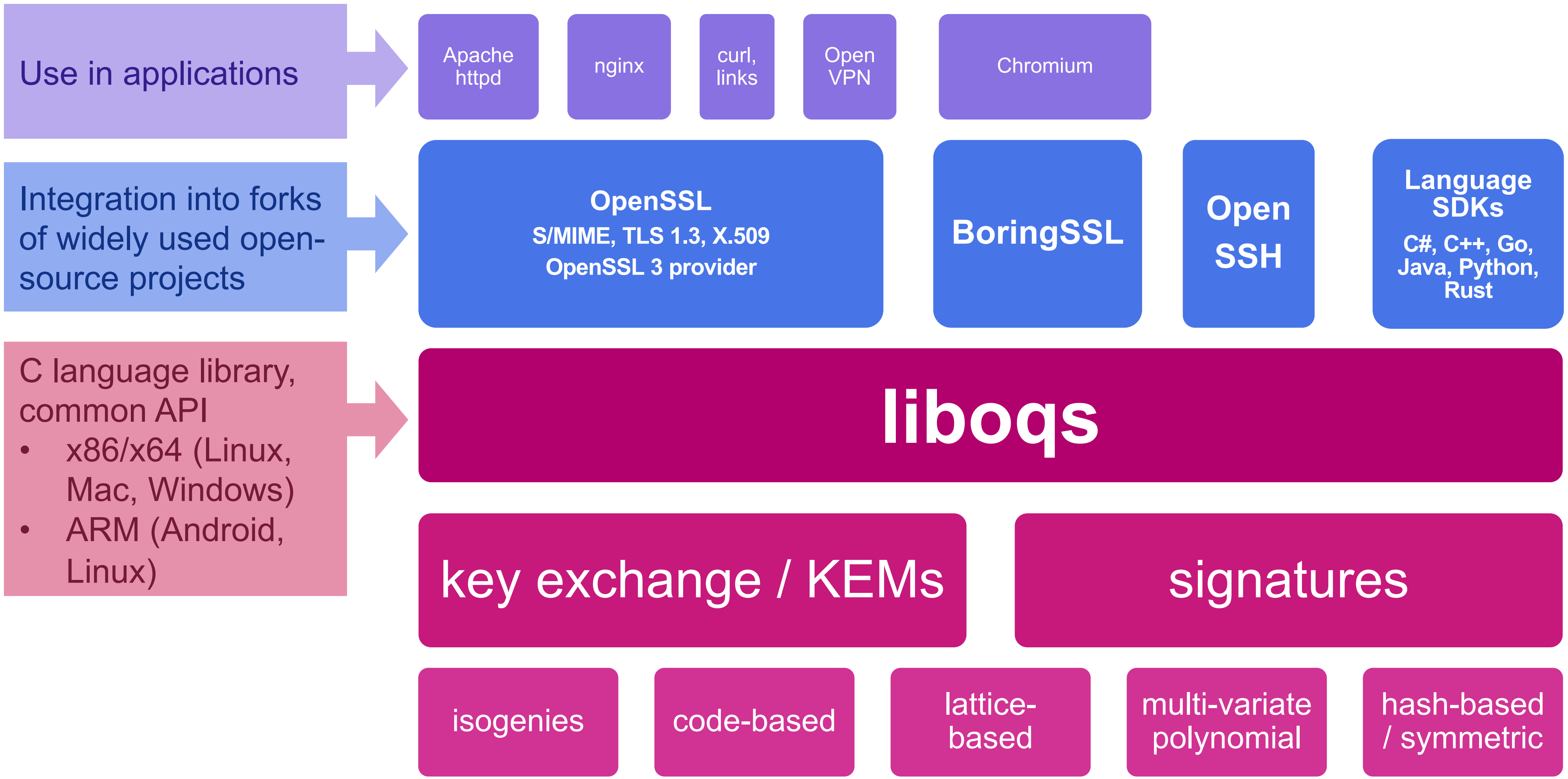
https://openquantumsafe.org/ • https://blog.cloudflare.com/experiment-with-pq/

Progress on other Internet protocols

- **Secure Shell (SSH)**
  - Internet-Draft on hybrid key exchange
  - Hybrid key exchange by default in OpenSSH since April 2022
  - Open Quantum Safe experiments
- **X.509 certificates**
  - Internet-Drafts for composite keys and signatures in X.509 certificates
  - Open Quantum Safe experiments
- **PGP** (Pretty Good Privacy email encryption/authentication)
  - Internet-Draft
- **IPsec** (virtual private network)
  - Internet-Draft on hybrid key exchange
- **Wireguard** (virtual private network)
  - Research paper

https://datatracker.ietf.org/doc/draft-kampanakis-curdle-ssh-pq-ke/ • https://datatracker.ietf.org/doc/html/draft-ounsworth-pq-composite-keys-03
https://datatracker.ietf.org/doc/html/draft-ounsworth-pq-composite-sigs-07 • https://datatracker.ietf.org/doc/draft-wussler-openpgp-pqc/
https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-ikev2-multiple-ke • https://eprint.iacr.org/2020/379

Open Quantum Safe Project



Led by University of Waterloo

Industry partners:

- Amazon Web Services
- Cisco
- evolutionQ
- IBM Research
- Microsoft Research

Additional contributors:

- Senetas
- PQClean project
- Individuals

Financial support:

- AWS
- Canadian Centre for Cyber Security
- Cisco
- NLNet
- NSERC
- Unitary Fund
- Verisign

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

Post-Quantum Cryptography

Douglas Stebila

UNIVERSITY OF WATERLOO

Public key cryptography designed to resist attacks by quantum computers

- Five families of mathematical assumptions
- Standardization of core algorithms under way by US National Institute of Standards and Technology
- Starting the process of standardizing post-quantum cryptography in Internet protocols

Up next:

- Atefeh Mashatan:
  - Strategic and operational implications for enterprises transitioning to post-quantum cryptography
  - Quantum readiness roadmaps and timelines
- David Jao:
  - Post-quantum hard problems and cryptographic schemes
  - Technical challenges with post-quantum cryptography

https://www.douglas.stebila.ca/research • https://openquantumsafe.org/