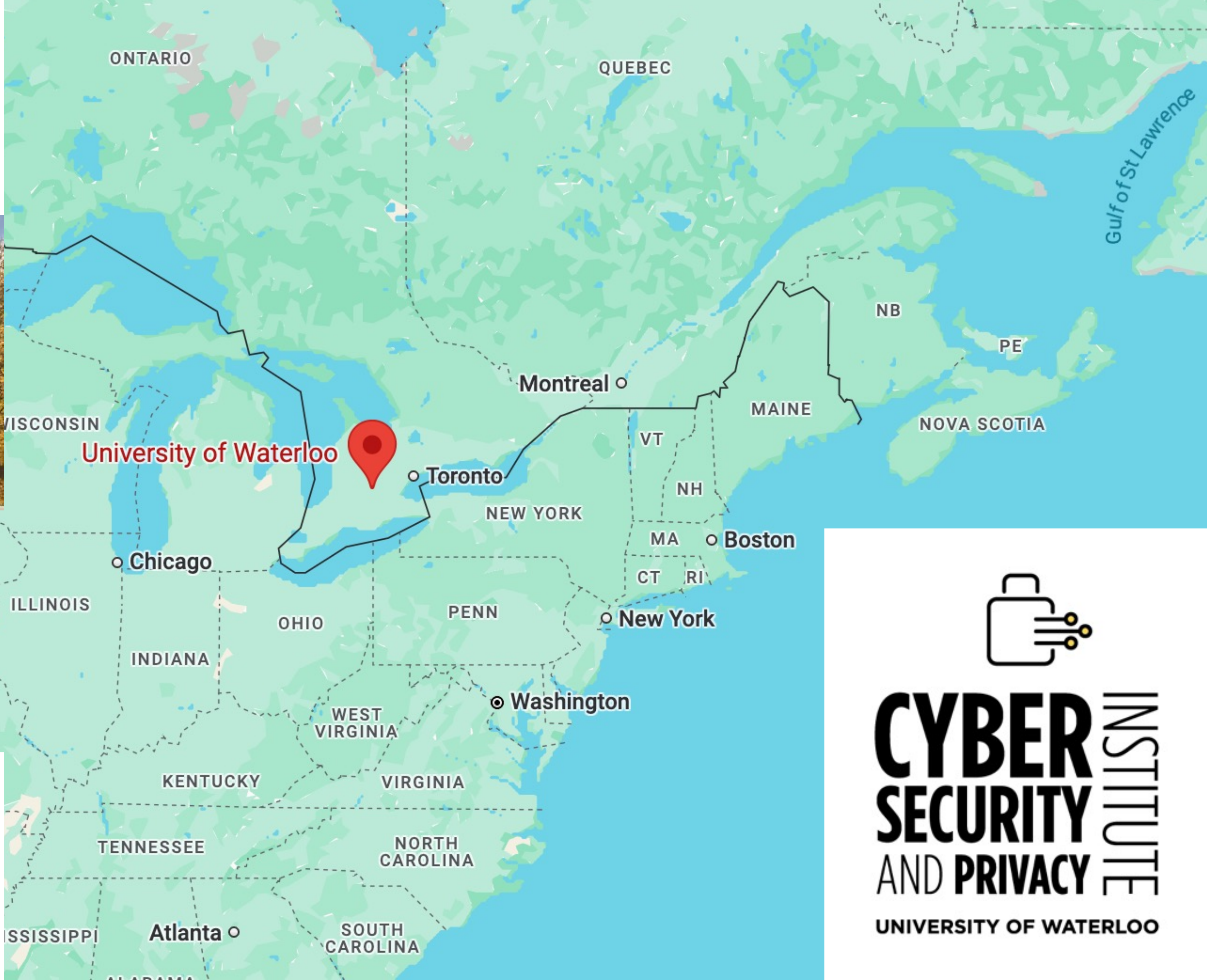
Post-Quantum Cryptography

Douglas Stebila

UNIVERSITY OF WATERLOO

M3AAWG • Toronto • 2024-10-08

UNIVERSITY OF WATERLOO



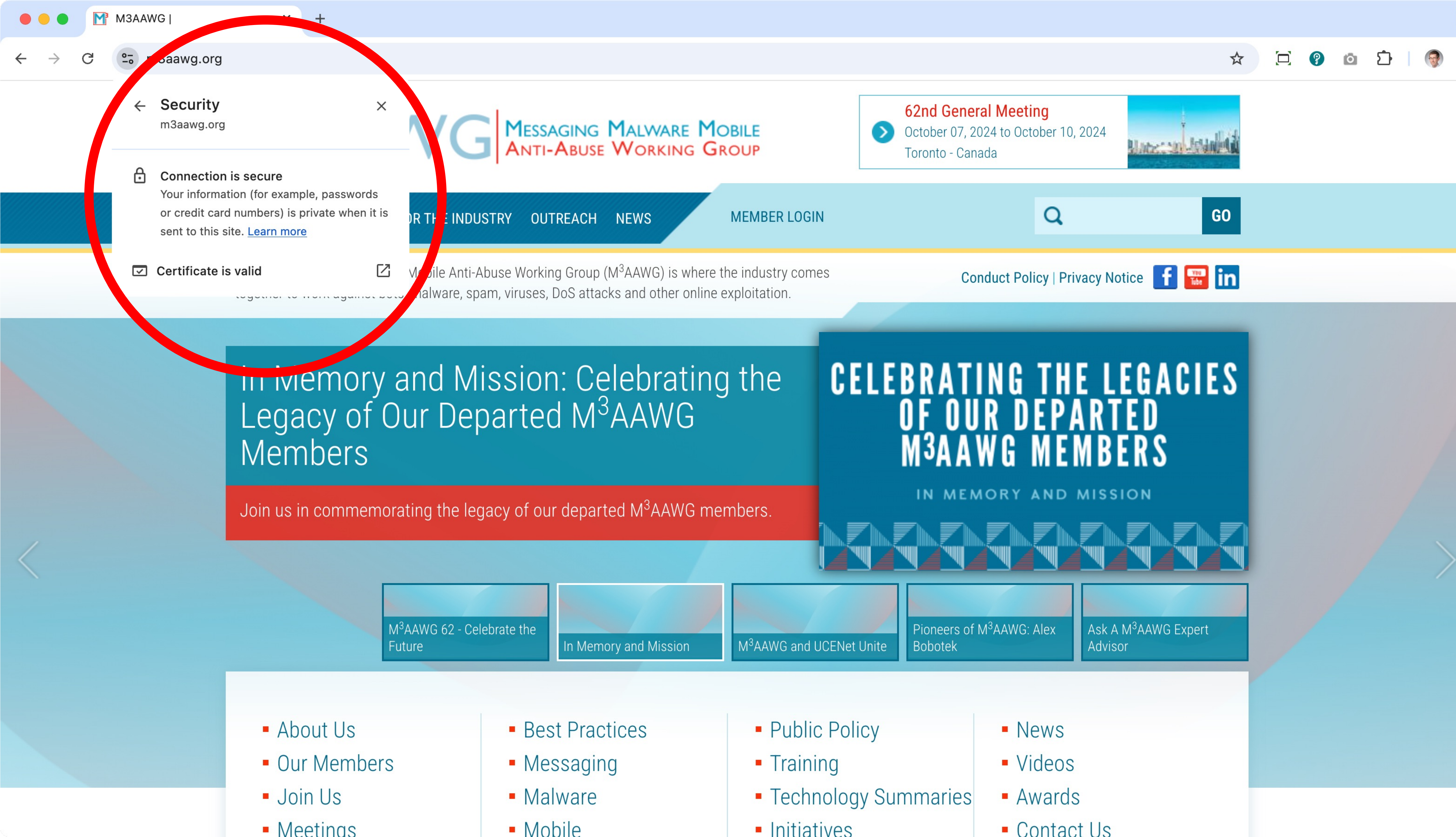
IQC Institute for Quantum Computing

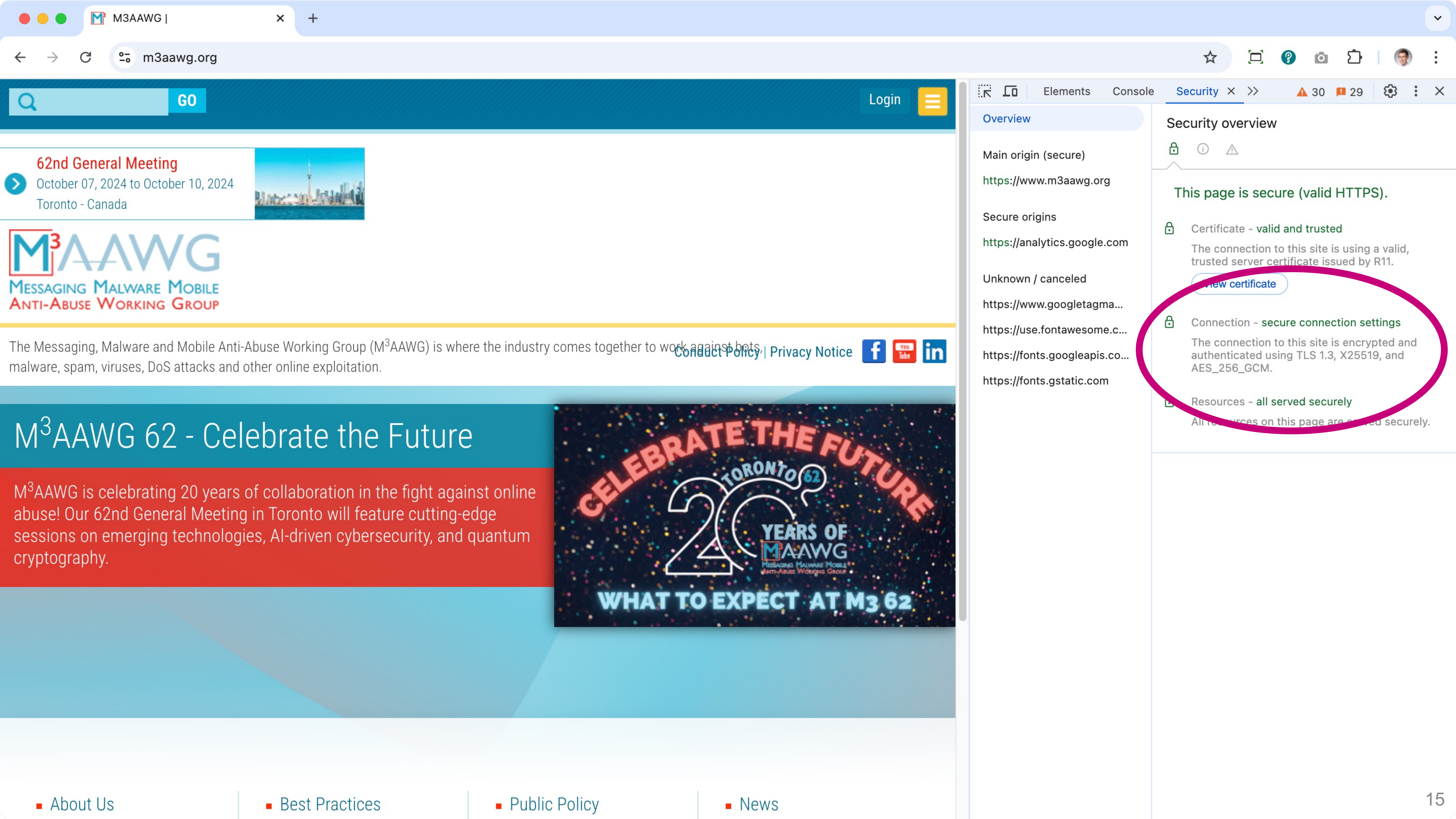
CYBER SECURITY AND PRIVACY INSTITUTE
UNIVERSITY OF WATERLOO

Agenda

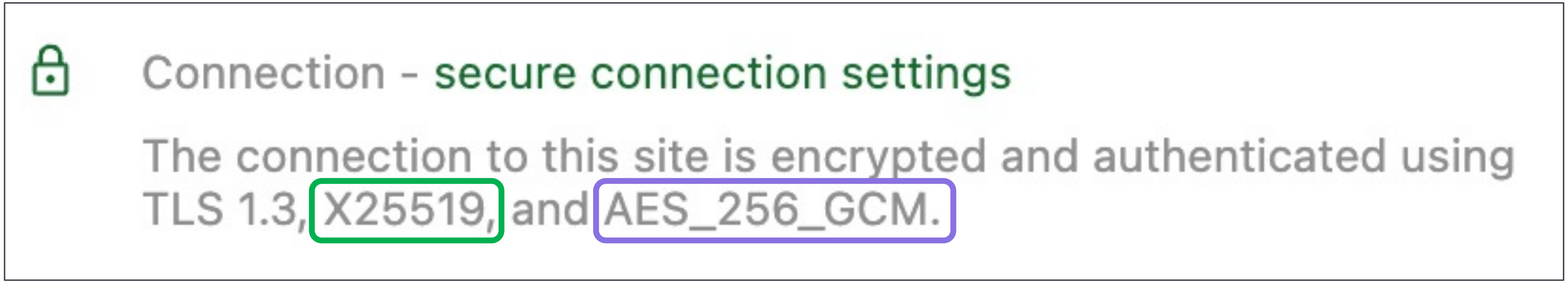
- The role of cryptography in online security
- The quantum threat
- Post-quantum cryptography
- Standardization
- Post-quantum TLS
- Open source software
- Challenges
- Discussion

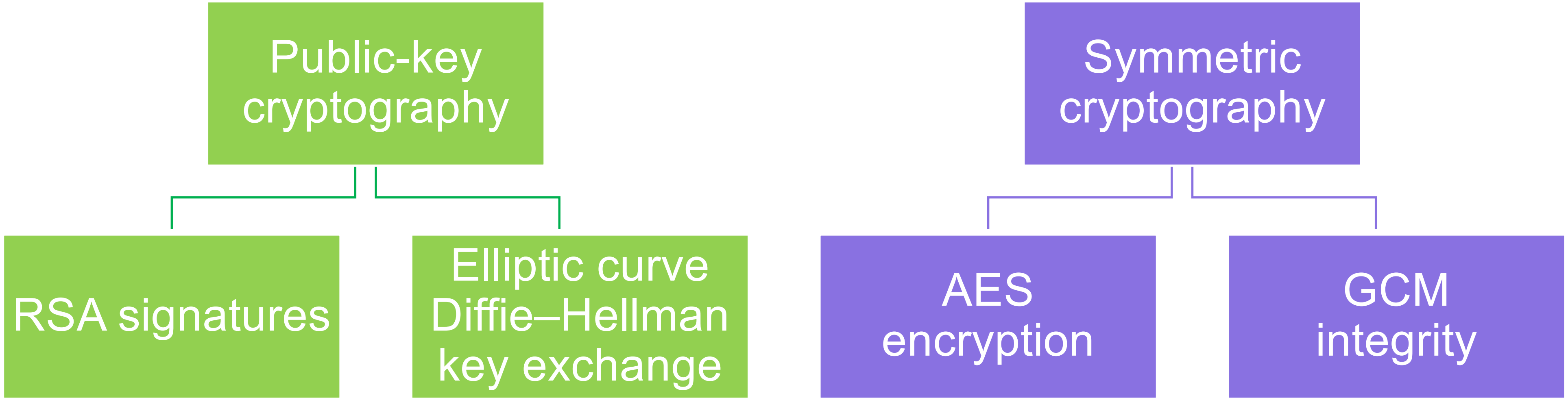

M3AAWG |
m3aawg.org
M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group
62nd General Meeting
October 07, 2024 to October 10, 2024
Toronto - Canada
ABOUT US
MEETINGS
FOR THE INDUSTRY
OUTREACH
NEWS
MEMBER LOGIN
GO
The Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) is where the industry comes together to work against bots, malware, spam, viruses, DoS attacks and other online exploitation.
Conduct Policy | Privacy Notice
M3AAWG 62 - Celebrate the Future
M3AAWG is celebrating 20 years of collaboration in the fight against online abuse! Our 62nd General Meeting in Toronto will feature cutting-edge sessions on emerging technologies, AI-driven cybersecurity, and quantum cryptography.
CELEBRATE THE FUTURE
TORONTO 62
20 YEARS OF M3AAWG
WHAT TO EXPECT AT M3 62
M3AAWG 62 - Celebrate the Future
In Memory and Mission
M3AAWG and UCENet Unite
Pioneers of M3AAWG: Alex Bobotek
Ask A M3AAWG Expert Advisor
About Us
Our Members
Join Us
Best Practices
Messaging
Malware
Mobile
Public Policy
Training
Technology Summaries
Initiatives
News
Videos
Awards
Contact Us
https://www.m3aawg.org/blog/M3AAWG62CelebrateTheFuture


M3AAWG |
m3aawg.org
Security
Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more
Certificate is valid
Messaging Malware Mobile
Anti-Abuse Working Group
62nd General Meeting
October 07, 2024 to October 10, 2024
Toronto - Canada
OUTREACH
NEWS
MEMBER LOGIN
GO
Conduct Policy | Privacy Notice
In Memory and Mission: Celebrating the Legacy of Our Departed M3AAWG Members
Join us in commemorating the legacy of our departed M3AAWG members.
CELEBRATING THE LEGACIES OF OUR DEPARTED M3AAWG MEMBERS
IN MEMORY AND MISSION
M3AAWG 62 - Celebrate the Future
In Memory and Mission
M3AAWG and UCENet Unite
Pioneers of M3AAWG: Alex Bobotek
Ask A M3AAWG Expert Advisor
About Us
Our Members
Join Us
Meetings
Best Practices
Messaging
Malware
Mobile
Public Policy
Training
Technology Summaries
Initiatives
News
Videos
Awards
Contact Us


M3AAWG |
m3aawg.org
GO
Login
62nd General Meeting
October 07, 2024 to October 10, 2024
Toronto - Canada
M3AAWG
Messaging Malware Mobile Anti-Abuse Working Group
The Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) is where the industry comes together to work against bots, malware, spam, viruses, DoS attacks and other online exploitation.
Conduct Policy | Privacy Notice
M3AAWG 62 - Celebrate the Future
M3AAWG is celebrating 20 years of collaboration in the fight against online abuse! Our 62nd General Meeting in Toronto will feature cutting-edge sessions on emerging technologies, AI-driven cybersecurity, and quantum cryptography.
CELEBRATE THE FUTURE
TORONTO 62
20 YEARS OF M3AAWG
WHAT TO EXPECT AT M3 62
About Us
Best Practices
Public Policy
News
Elements
Console
Security
30
29
Overview
Main origin (secure)
https://www.m3aawg.org
Secure origins
https://analytics.google.com
Unknown / canceled
https://www.googletagma...
https://use.fontawesome.c...
https://fonts.googleapis.co...
https://fonts.gstatic.com
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 R11.
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.

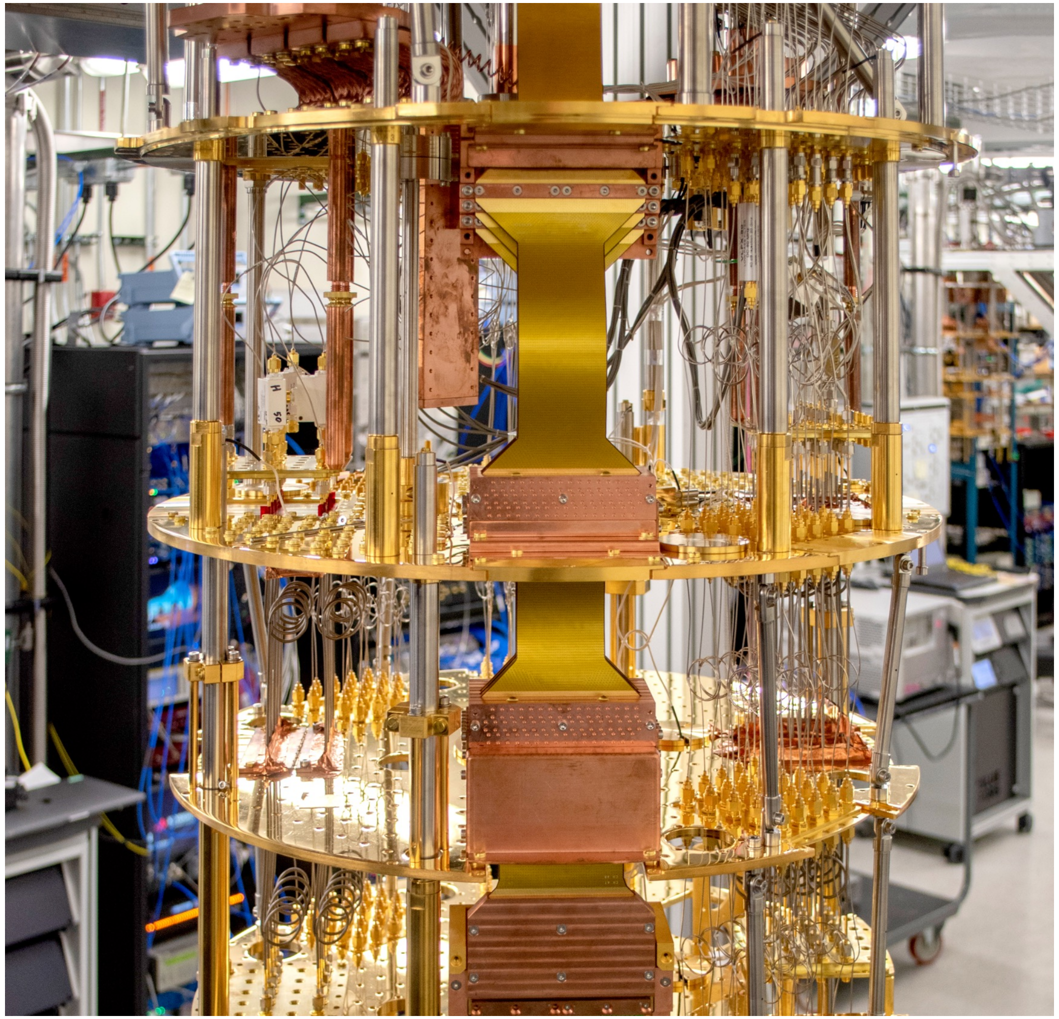
Cryptographic building blocks

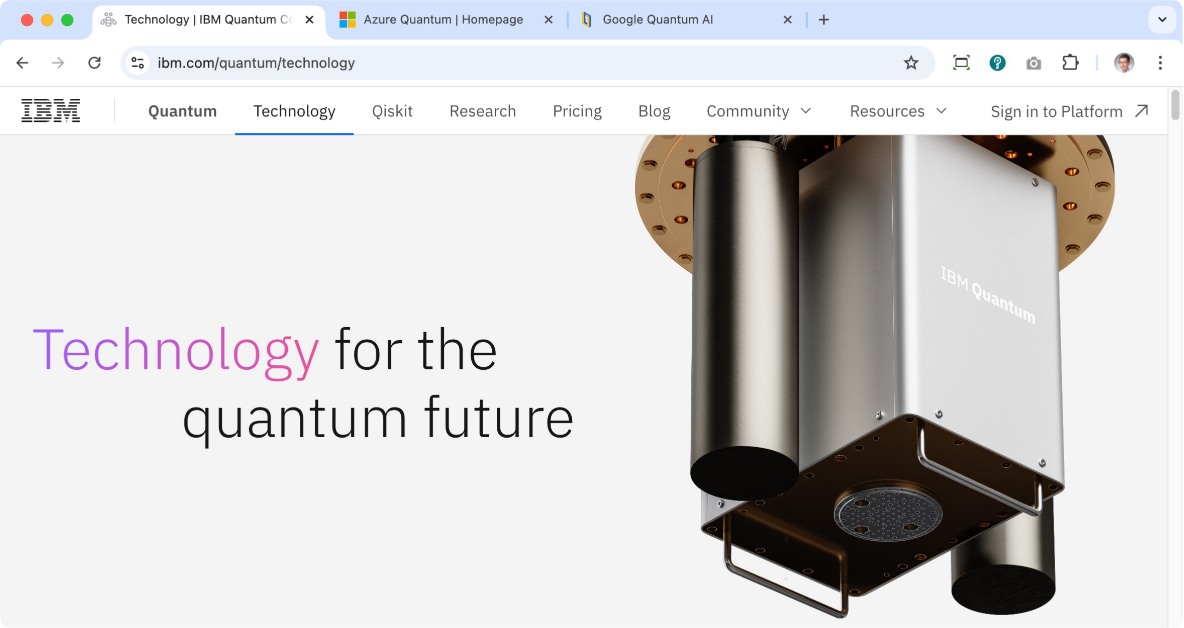


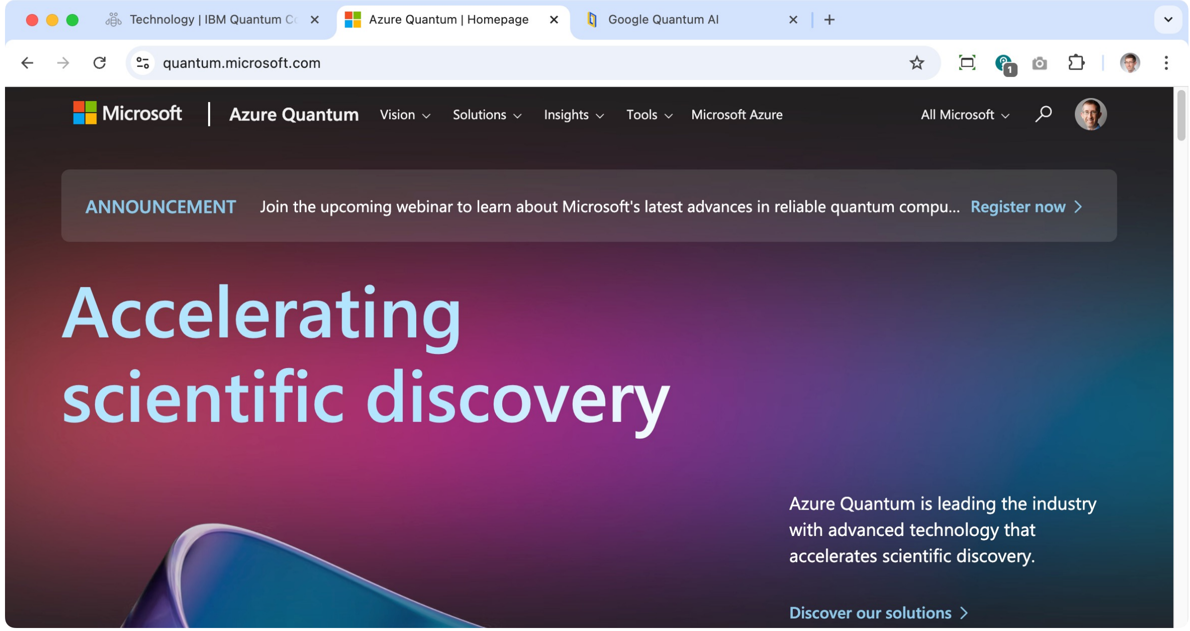


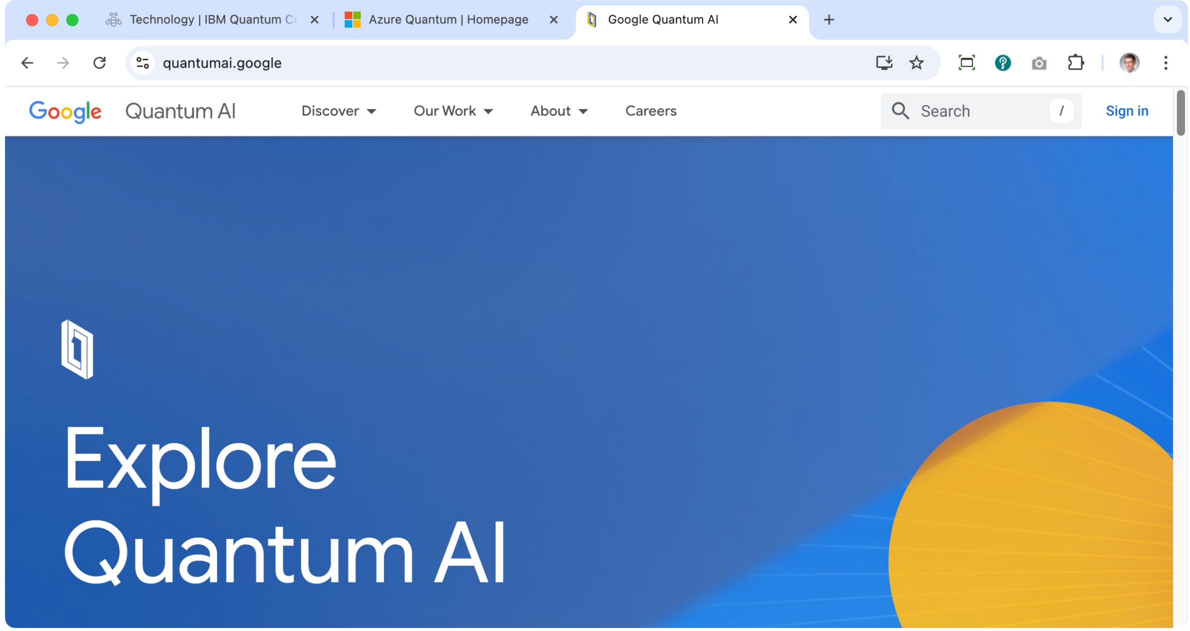
Quantum computing

- Represent and process information using **quantum mechanics**
- Processing information in superposition can dramatically speed some computations
    - But not necessarily all (quantum computers aren't magic)







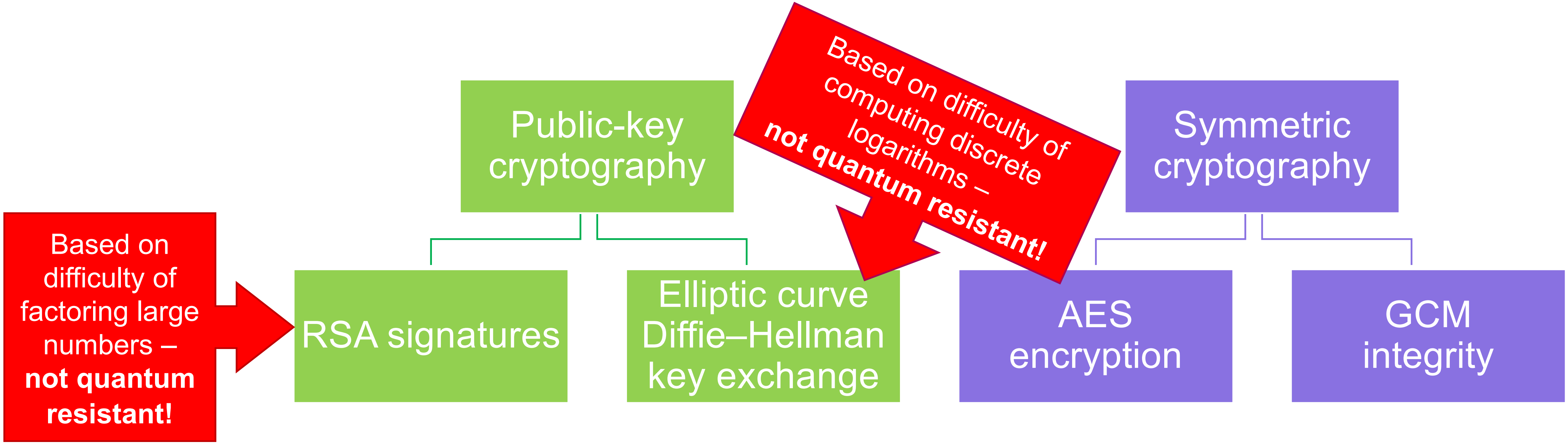


Theorem (Shor, 1984): There exists a polynomial-time quantum algorithm that can factor and compute discrete logarithms.

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.



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

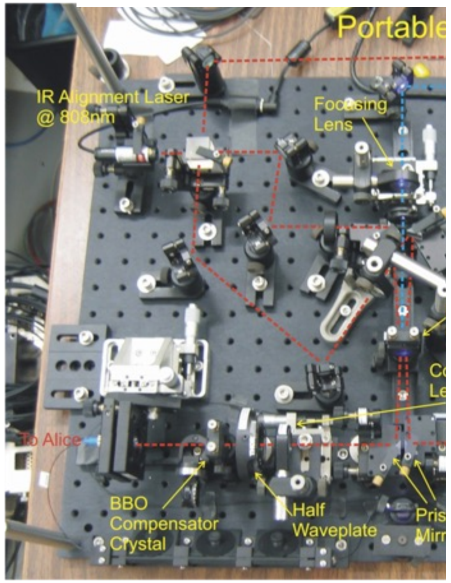
Uses quantum mechanics to protect information

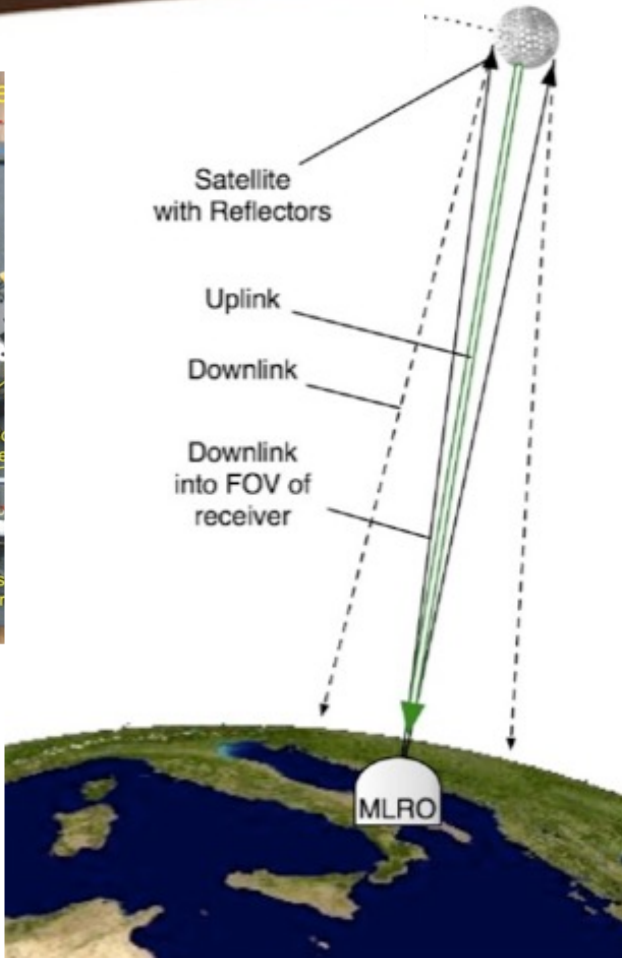
Doesn't require a full quantum computer

But does require new communication infrastructure

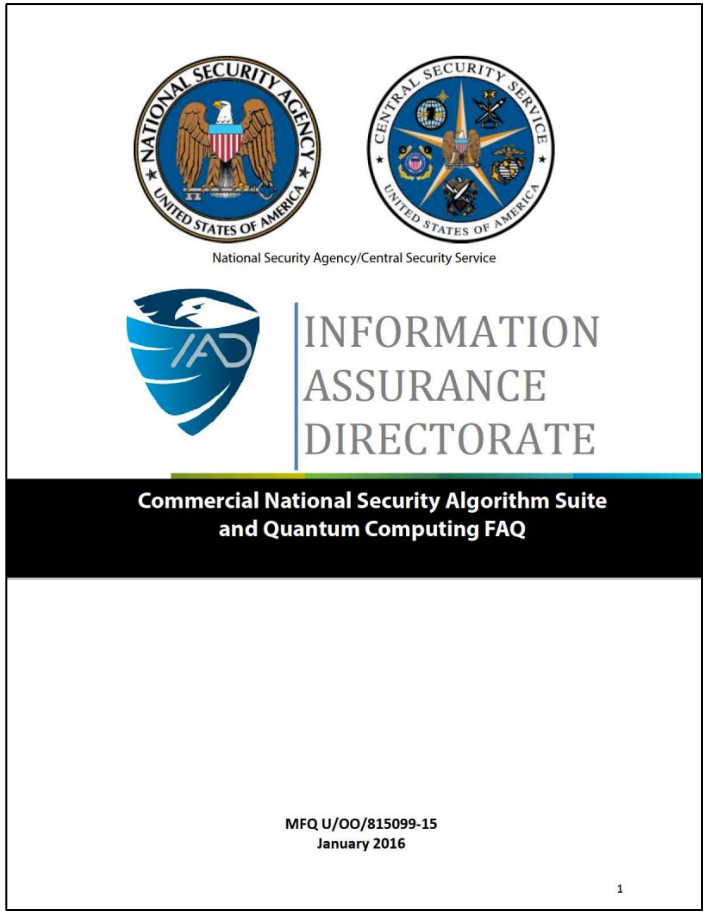
- Lasers, telescopes, fiber optics, …

=> Not the subject of this talk





Start of US government activity on PQC


National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

Commercial National Security Algorithm Suite and Quantum Computing FAQ

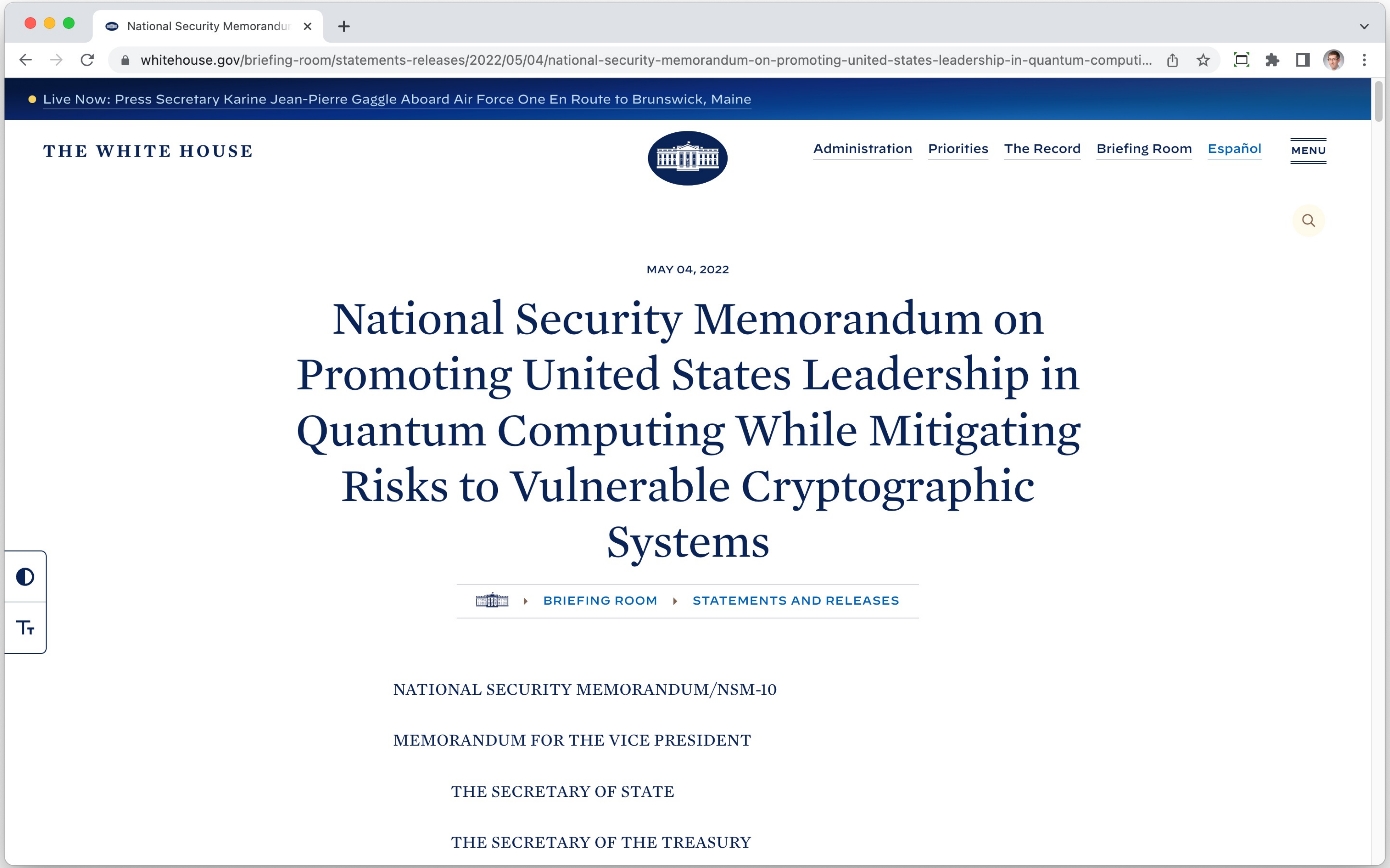
MFQ U/OO/815099-15
January 2016

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



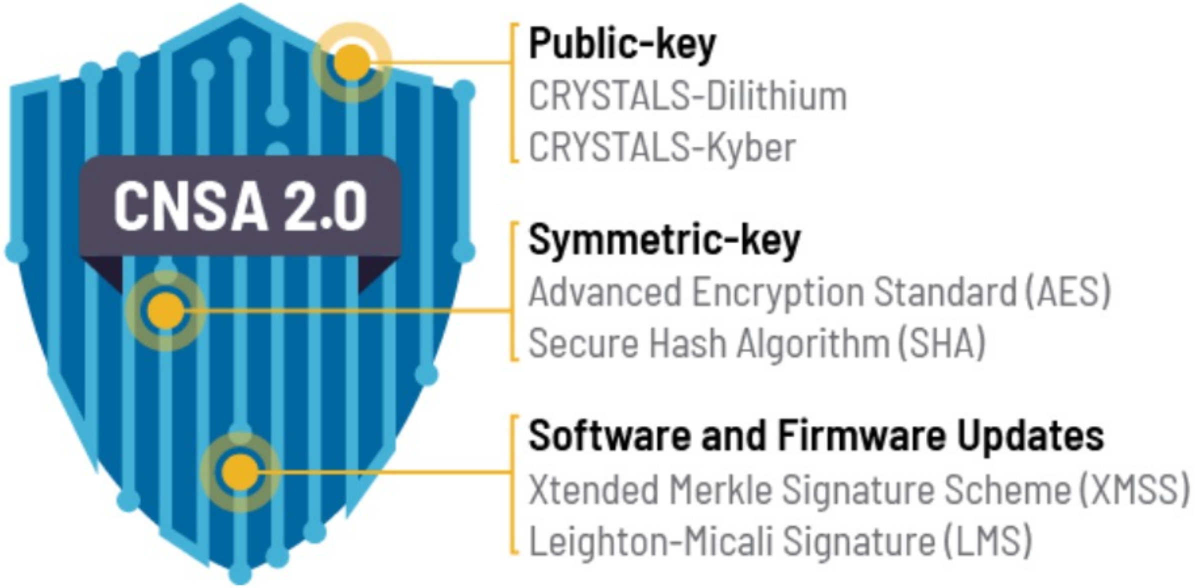
https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

National Security Agency | Cybersecurity Advisory

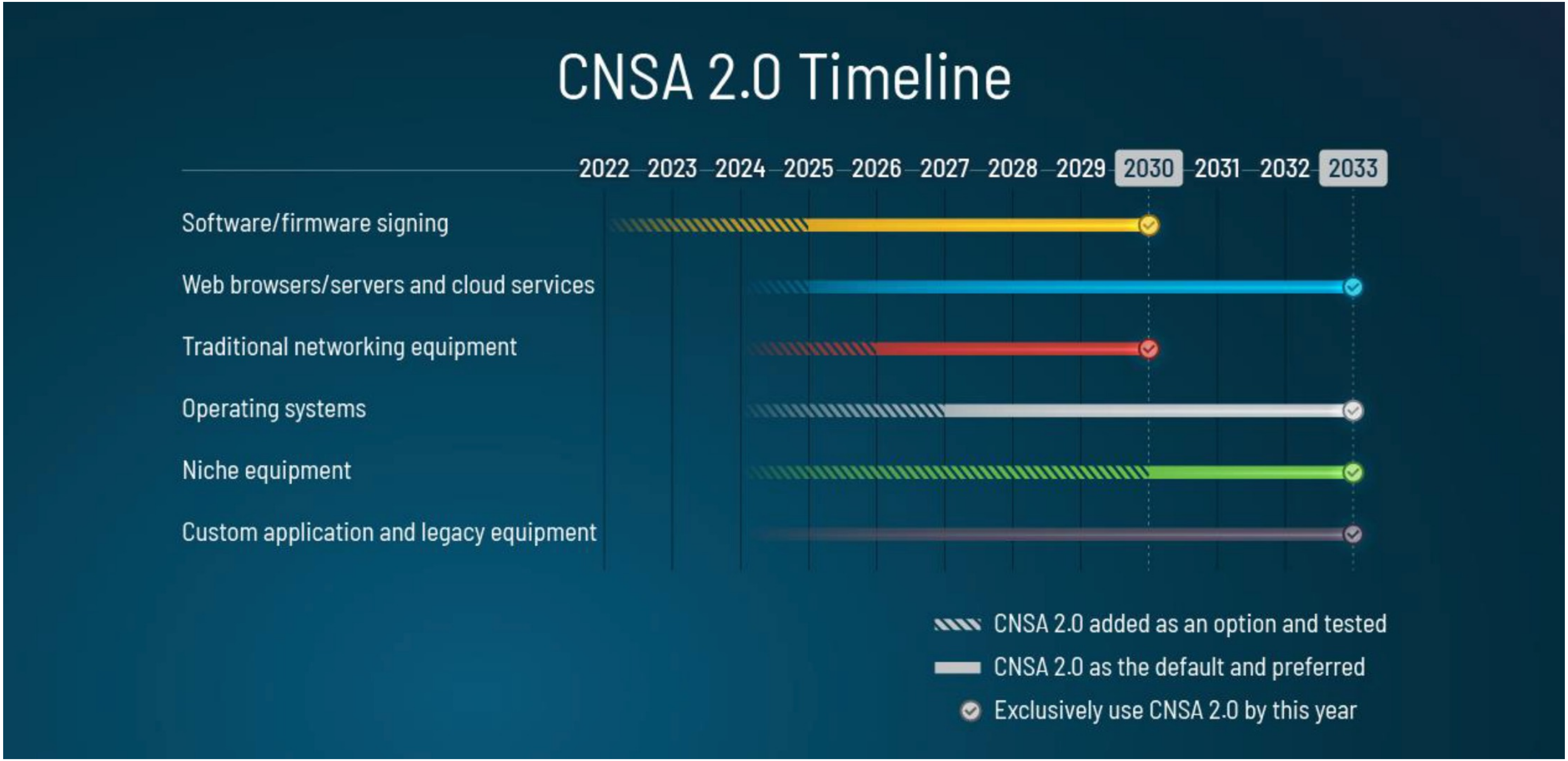
Announcing the Commercial National Security Algorithm Suite 2.0

Executive summary

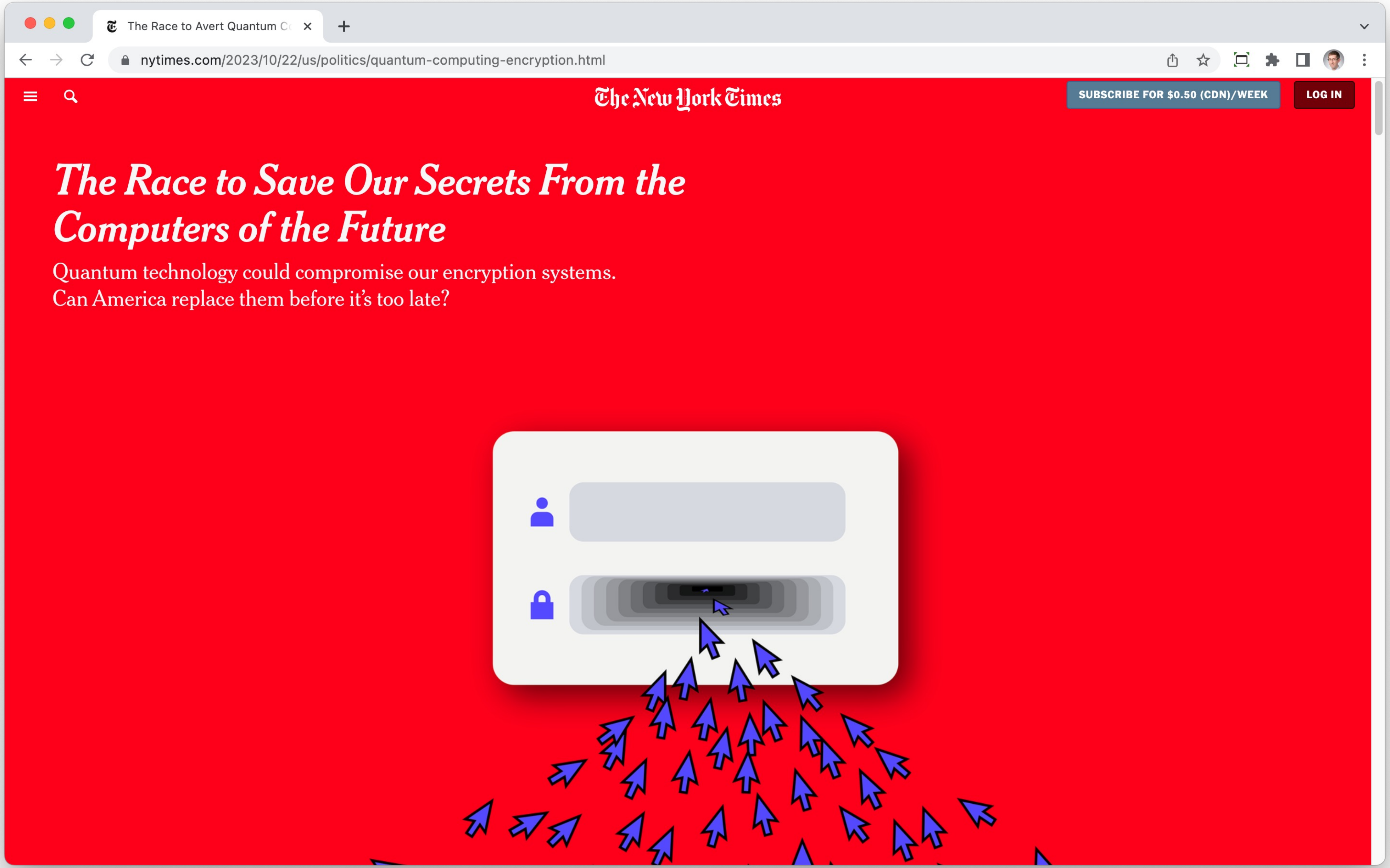
The need for protection against a future deployment of a cryptanalytically relevant quantum computer (CRQC) is well documented. That story begins in the mid-1990s when Peter Shor discovered a CRQC would break



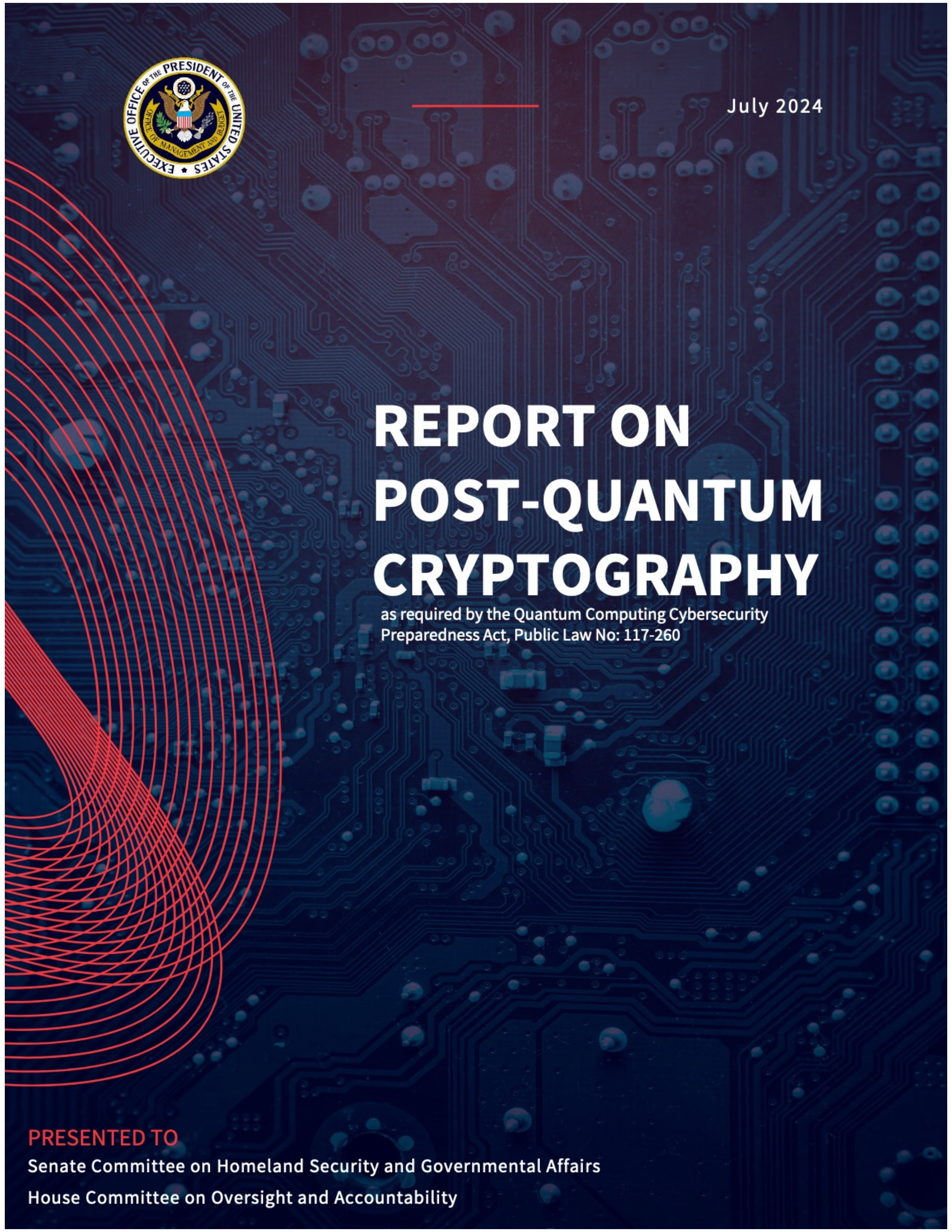
https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF



https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF



https://www.nytimes.com/2023/10/22/us/politics/quantum-computing-encryption.html

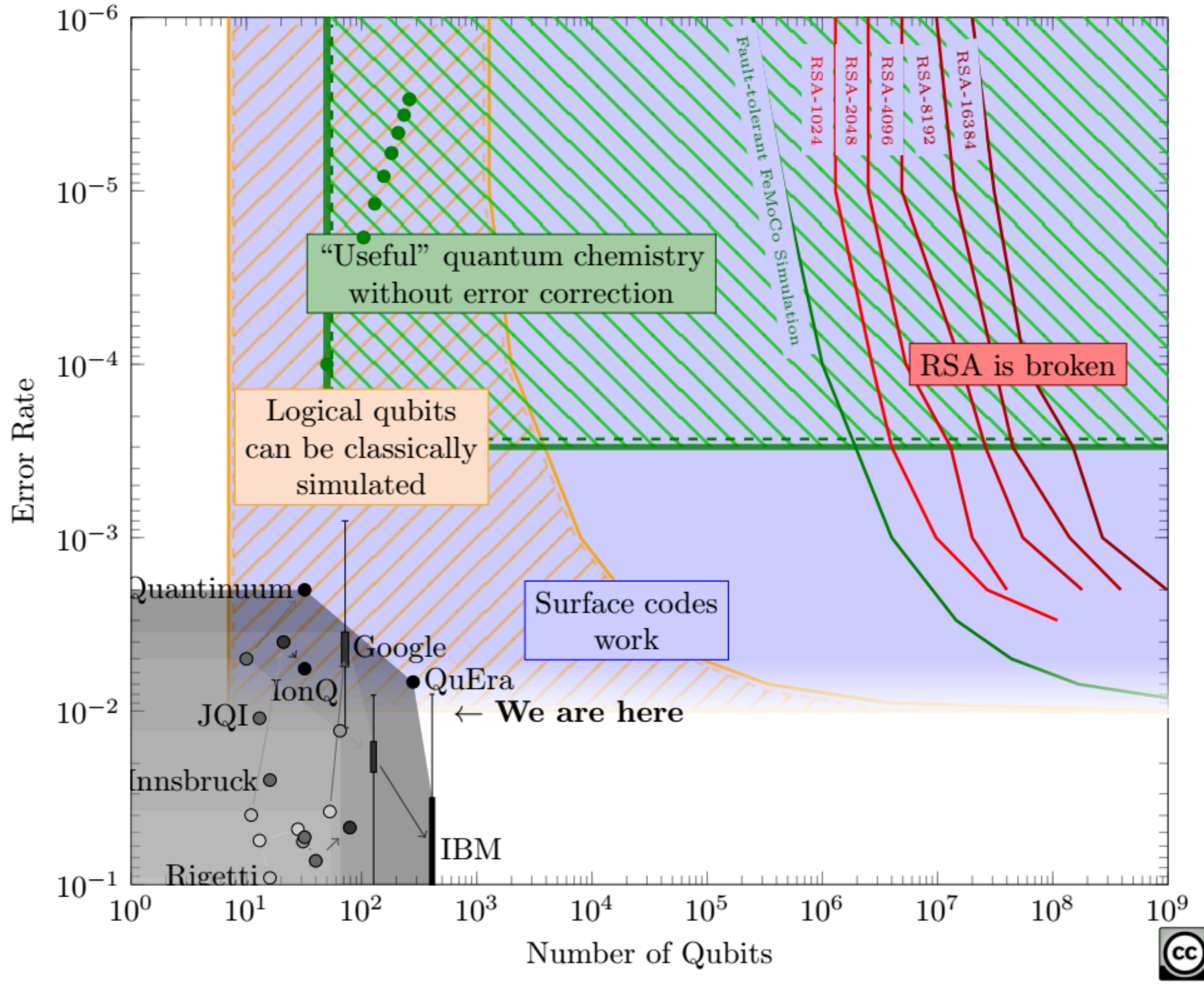


Estimated cost to migrate US government to PQC between 2025–2035:

$7.1 billion

https://www.whitehouse.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf • cost in 2024 dollars

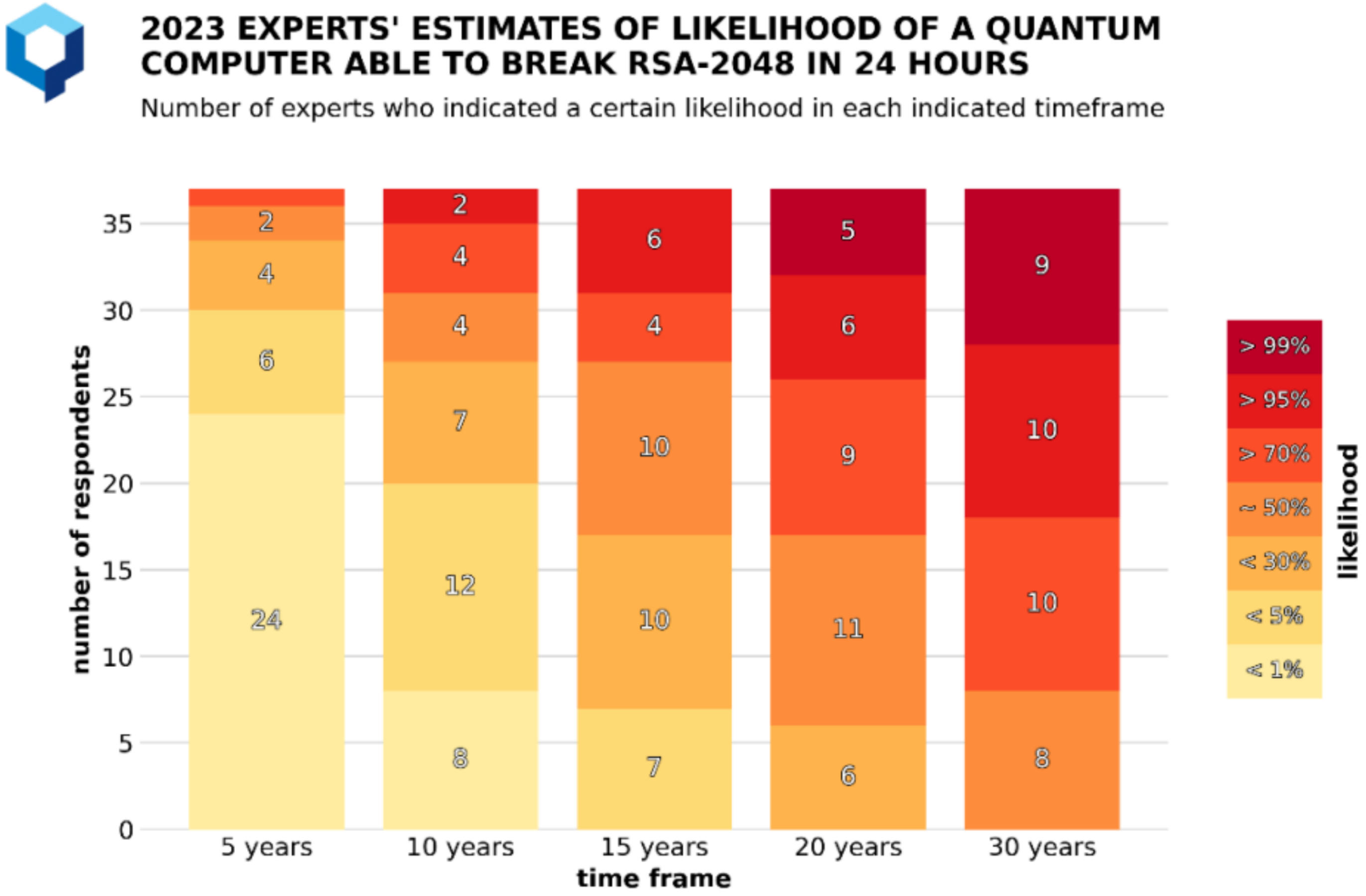
Landscape of quantum computing



https://sam-jaques.appspot.com/quantum_landscape_2023

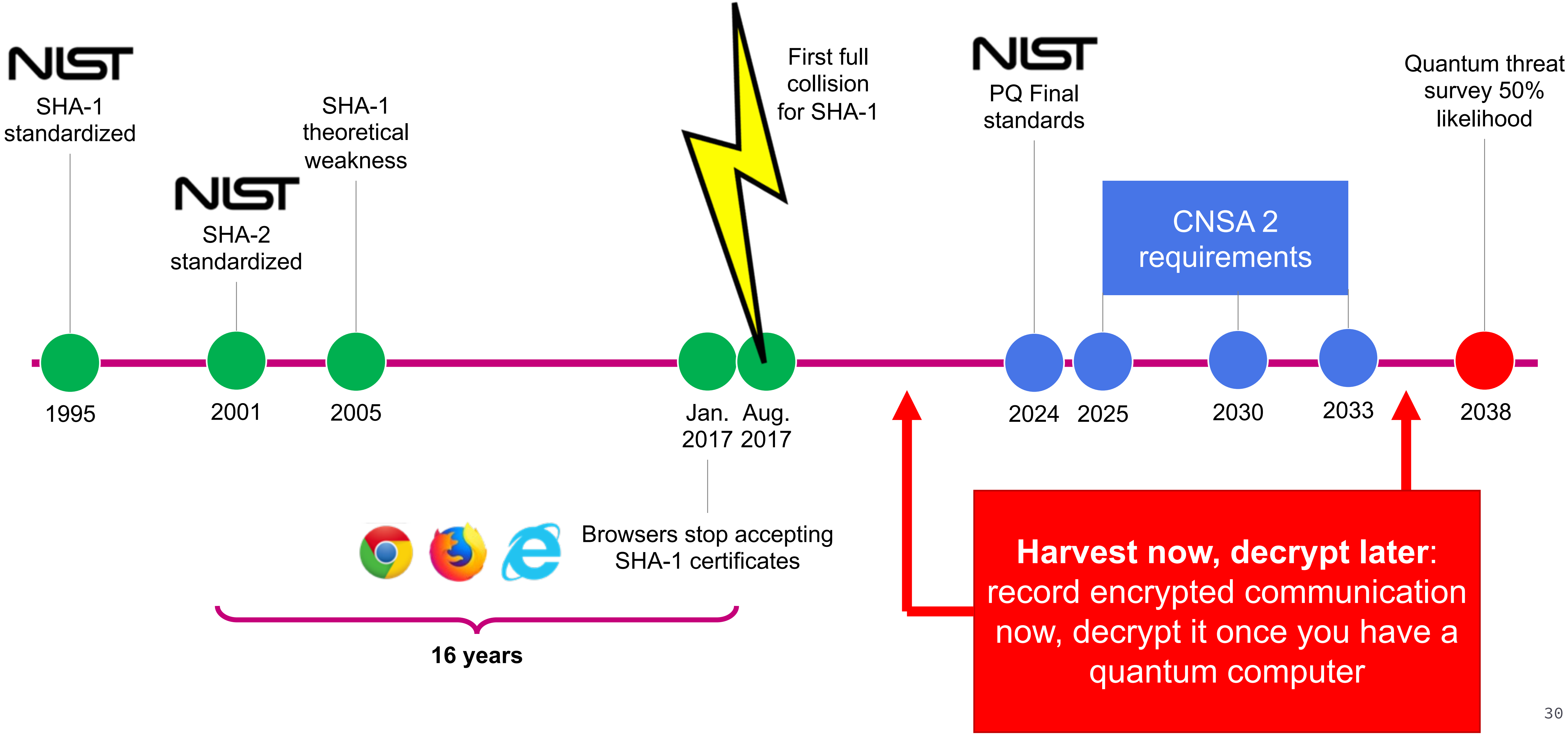
When will a cryptographically relevant quantum computer be built?

≥ 50% of experts surveyed think there's ≥ 50% chance of a cryptographically relevant quantum computer by 2038



https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/

Timeline to replace cryptographic algorithms



Standardization of PQ cryptography

The path to standardization

Principles

- Legislation
- Regulators

Policies

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

Protocols

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

Mathematics

- Specialist organizations
  - NIST, CFRG

Primary goals for post-quantum crypto

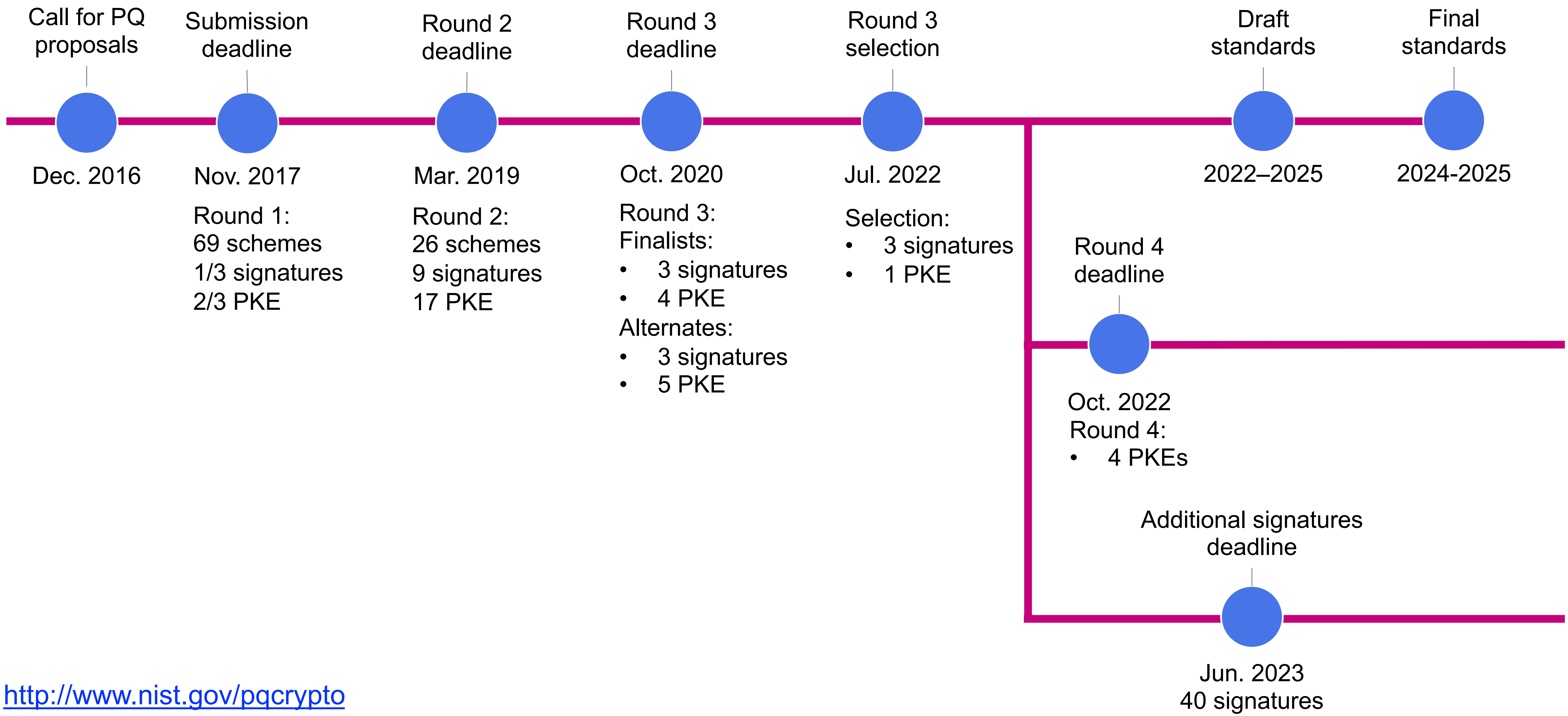
Confidentiality
in the public key setting

- **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**

NIST Post-quantum Crypto Project timeline



http://www.nist.gov/pqcrypto

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

NIST PQC standards

Key encapsulation mechanisms

- ML-KEM (FIPS 203)
  - a.k.a. Kyber
  - Lattice-based

Digital signatures

- ML-DSA (FIPS 204)
  - a.k.a. Dilithium
  - Lattice-based
- SLH-DSA (FIPS 205)
  - a.k.a. SPHINCS+
  - Stateless hash-based
- FN-DSA (draft pending)
  - a.k.a. Falcon
  - Lattice-based

PQ algorithms being standardized

Kyber NIST ISO IRTF
NTRU IRTF
FrodoKEM ISO
Classic McEliece ISO

Lattice-based KEMs

Lattice-based signatures

Dilithium NIST
Falcon NIST

+ national efforts in China, South Korea, …

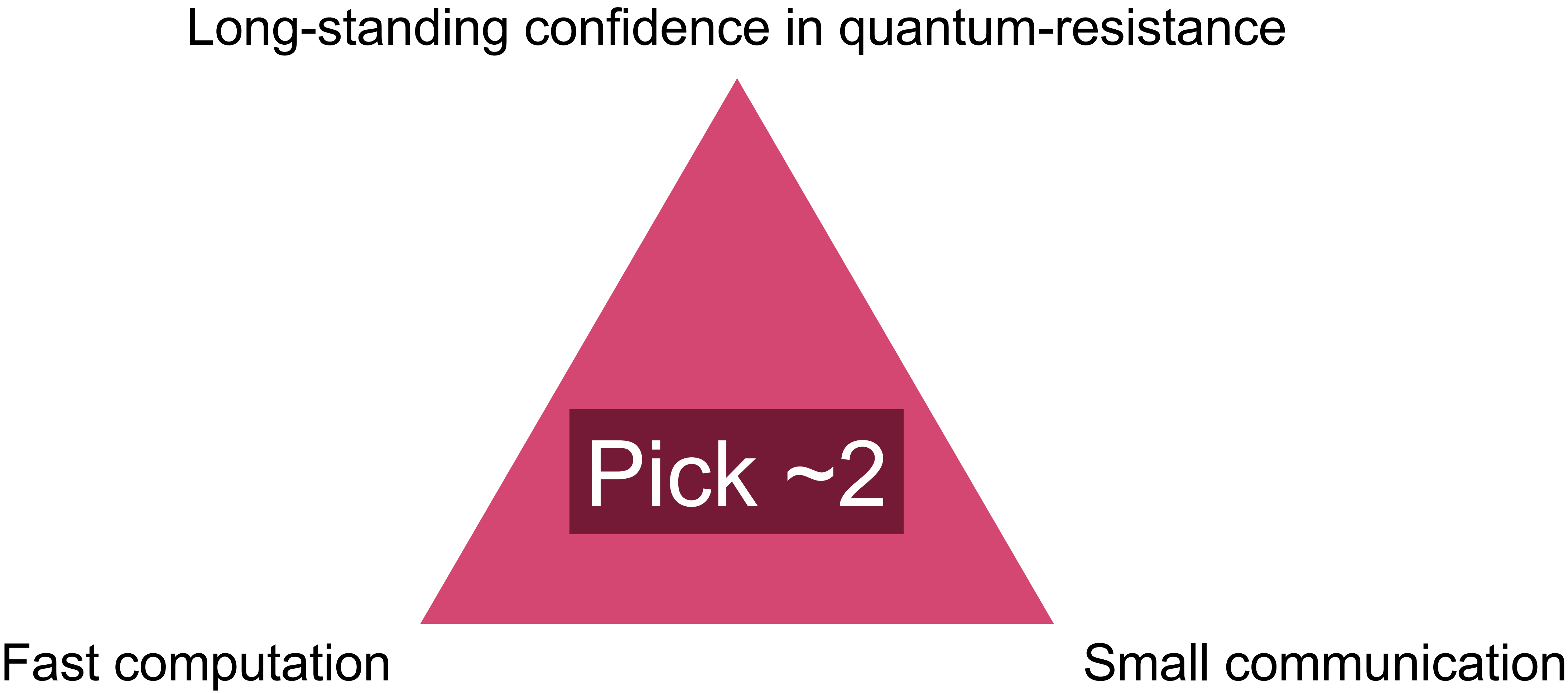
Stateful hash-based signatures

XMSS
HSS/LMS
{ IRTF, NIST }

Stateless hash-based signatures

SPHINCS+ NIST

Trade-offs with post-quantum crypto

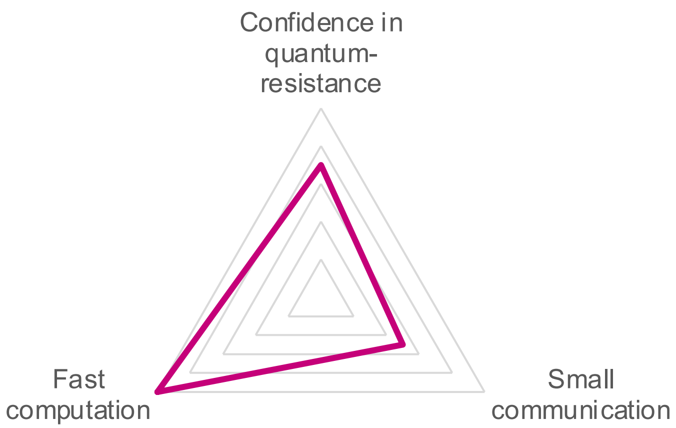


Trade-offs with post-quantum crypto

RSA and elliptic curves

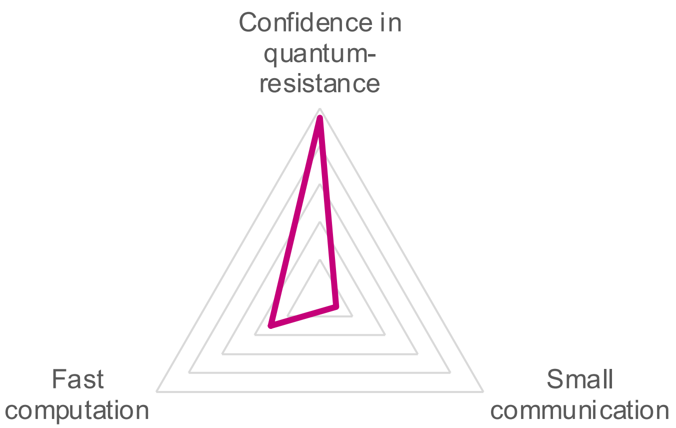
TLS handshake:
1.3 KB

Lattice-based cryptography



TLS handshake:
11.2 KB

Hash-based signatures



TLS handshake:
24.6 KB

Addressing the challenges of using PQ crypto

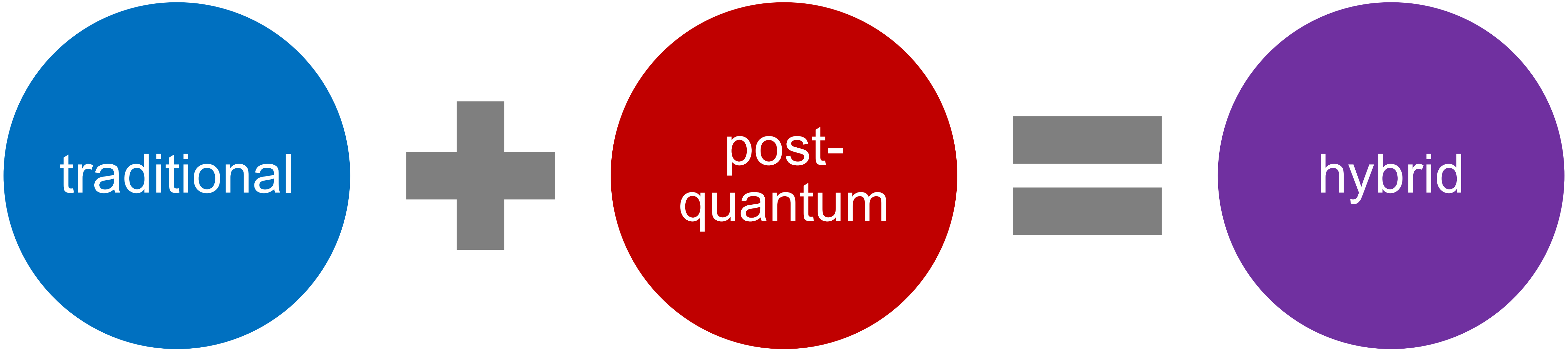
- Lack of confidence in security
- Slow computation
- Large communication

"Just" make better PQ crypto!

Addressing the challenges of using PQ crypto

Lack of confidence in security	"Hybrid": Use multiple algorithms
Slow computation	Actually not too bad; research on algorithmic optimizations; general CPU improvements
Large communication	Hardest to avoid; may need to change how network protocols use PQ crypto

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



Hybrid: 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

Why to <u>not</u> use hybrid

- Increases number of design choices
- Increases implementation complexity
- Increases code size

- Regulatory fracturing:
  - Hybrids required: BSI (Germany), ANSSI (France)
  - Hybrids allowed: ENISA (EU), ETSI
  - Hybrids discouraged: NSA (US)

  No decision on hybrids: NCSC (UK), CSE (Canada)

Bottom half of slide from Mike Ounsworth presentation https://pkic.org/events/2023/post-quantum-cryptography-conference/pkic-pqcc-pqc-at-ietf-mike-ounsworth-entrust.pdf ; updated 2023-03-27 with corrected information from https://pkic.org/events/2023/post-quantum-cryptography-conference/pkic-pqcc-how-gc-preparing-for-pqc-melanie-anderson-jonathan-hammell-canadian-government.pdf

Challenge: larger communication sizes

Higher bandwidth usage

- Impact on high-traffic providers
- Higher power usage in battery-operated devices

Higher latency

- Larger data in early flows of TCP leads to more round trips if exceeding the TCP congestion window
- More packets on poor-quality links leads to more retransmission

Impossible to fit in some protocols

- e.g. DNSSEC over UDP has problems with packets larger than 1232 bytes [1]

[1] Müller et al, ACM SIGCOMM Computer Communication Review 50(4):49–57, 2020.

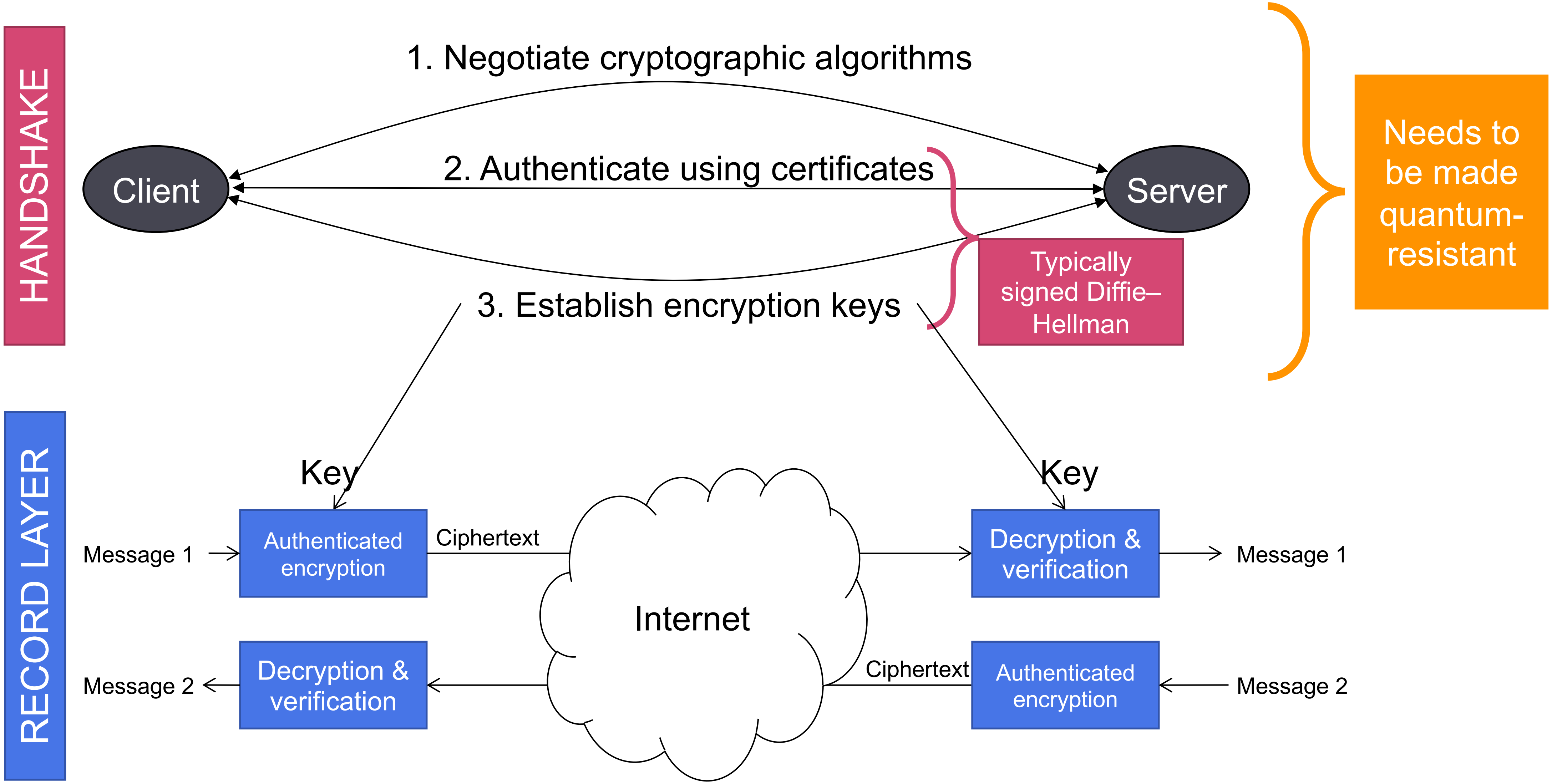
PQ algorithm sizes

Public key encryption scheme	Public key size (bytes)	Ciphertext overhead (bytes)
RSA-2048	256	256
ECDH (NISTp256, X25519)	32	32
ML-KEM-512	800	768
ML-KEM-768	1184	1088

Signature scheme	Public key size (bytes)	Signature size (bytes)
RSA-2048	256	256
ECDSA (NISTp256, Ed25519)	32	64
ML-DSA-44	1312	2420
SLH-DSA-SHA2-128s	32	7856
Falcon-512	897	752
XMSS / LMS	48–128	1600–25000+

Making TLS post-quantum

SSL/TLS Protocol



Three dimensions of “post-quantum TLS”

What is “post-quantum TLS”?

Pre-shared key (PSK) mode

- Already implemented
- Still has key distribution problem
- No forward secrecy
- New mode: external PSK

What is “post-quantum TLS”?

<table>
<tr><th rowspan="2">Pre-shared key (PSK) mode</th><th colspan="2">Key exchange</th></tr>
<tr><th>PQ-only</th><th>Hybrid</th></tr>
<tr><td rowspan="2">• Already implemented
• Still has key distribution problem
• No forward secrecy
• New mode: external PSK</td><td colspan="2">• Fairly easy to implement
• Needed soonest: harvest now, decrypt later</td></tr>
<tr><td></td><td>• Robust to 1 algorithm break
• "Safe choice"
• In demand during pre-certification</td></tr>
</table>

What is "post-quantum TLS"?

<table>
<tr><th rowspan="2">Pre-shared key (PSK) mode</th><th colspan="2">Key exchange</th><th colspan="2">Authentication</th></tr>
<tr><th>PQ-only</th><th>Hybrid</th><th>PQ-only</th><th>Hybrid / Composite</th></tr>
<tr><td rowspan="2">• Already implemented
• Still has key distribution problem
• No forward secrecy
• New mode: external PSK</td><td colspan="2">• Fairly easy to implement
• Needed soonest: harvest now, decrypt later</td><td colspan="2">• Requires coordination with certificate authorities
• Less urgently needed: can't retroactively break authentication
• Size ☹</td></tr>
<tr><td></td><td>• Robust to 1 algorithm break
• "Safe choice"
• In demand during pre-certification</td><td></td><td>• May not make sense in the context of a negotiated protocol like TLS</td></tr>
</table>

What is “post-quantum TLS”?

Pre-shared key (PSK) mode	Key exchange		Authentication		Alternative protocol designs
	PQ-only	Hybrid	PQ-only	Hybrid / Composite	
• Already implemented • Still has key distribution problem • No forward secrecy • New mode: external PSK	• Fairly easy to implement • Needed soonest: harvest now, decrypt later		• Requires coordination with certificate authorities • Less urgently needed: can't retroactively break authentication • Size ☹		• e.g. AuthKEM / KEMTLS • Harder to implement; may require state machine changes • Lots of interesting research!
		• Robust to 1 algorithm break • "Safe choice" • In demand during pre-certification		• May not make sense in the context of a negotiated protocol like TLS	

Area of initial focus

Hybrid key exchange in TLS 1.3

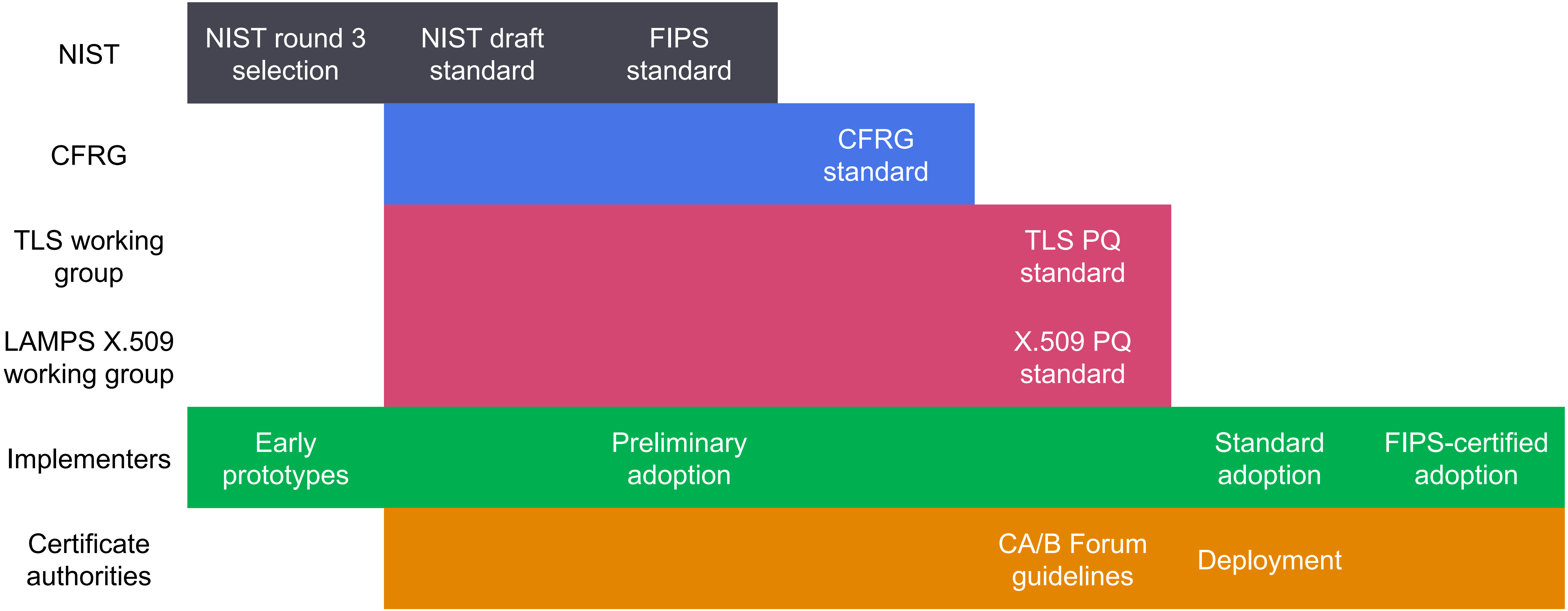
```
Network Working Group                                    D. Stebila
Internet-Draft                                University of Waterloo
Intended status: Informational                           S. Fluhrer
Expires: 10 March 2024                                Cisco Systems
                                                           S. Gueron
                                                            U. Haifa
                                                    7 September 2023


                  Hybrid key exchange in TLS 1.3
                 draft-ietf-tls-hybrid-design-09

Abstract

   Hybrid key exchange refers to using multiple key exchange algorithms
   simultaneously and combining the result with the goal of providing
   security even if all but one of the component algorithms is broken.
   It is motivated by transition to post-quantum cryptography.  This
   document provides a construction for hybrid key exchange in the
   Transport Layer Security (TLS) protocol version 1.3.
```

- Fairly mature
- Early deployments showing reasonable performance:
  - Chrome
  - Cloudflare
  - Open Quantum Safe
  - WolfSSL
  - …

WARNING: IETF considers TLS 1.2 to be frozen. "Post-quantum cryptography for TLS 1.2 WILL NOT be supported."

https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/ • https://datatracker.ietf.org/doc/draft-ietf-tls-tls12-frozen/

Critical path to adoption on the web



Algorithm standardization status

	Kyber/ML-KEM	Dilithium/ML-DSA	Falcon
Primary standardizer:	NIST	NIST	NIST
Status at NIST:	FIPS 203	FIPS 304	Draft pending
Status at IETF/IRTF:	CFRG draft available	—	—

	SPHINCS+	XMSS	LMS
Primary standardizer:	NIST	IRTF	IRTF
Status at NIST:	FIPS 205	Approved in SP 800-208 (2020)	Approved in SP 800-208 (2020)
Status at IETF/IRTF:	—	RFC 8391 (2018)	RFC 8554 (2019) Draft for new parameter sets

Protocol	Key exchange / PKE	Authentication	Alternatives
TLS 1.3 (secure channel)	Drafts: • Hybrid Kyber & ML-KEM • External PSK	Prototypes	• AuthKEM / KEMTLS • TurboTLS • Merkle Tree certs.
X.509 (certificates)	Drafts: • Composite ML-KEM	Drafts: • Composite ML-DSA • IETF PQC PKI hackathon	
Secure Shell (SSH) (secure channel)	Drafts: Hybrid Kyber OpenSSH: Hybrid NTRU Prime	Prototypes	
IPsec (secure channel)	RFCs: PSK Drafts: hybrid, large messages	Drafts: • Hybrid non-composite • Negotiation	
CMS (secure email, …)	Drafts: • Using KEMs in CMS • Composite ML-KEM	RFCs: LMS Drafts: • Composite ML-DSA • SPHINCS+	
DNSSEC (Domain Name Security)	Drafts: Stateful HBS		• Merkle Tree ladder • Request-based frag.
OpenPGP (secure email)	Drafts: • Composite Kyber	Drafts: • Composite Dilithium • PQ-only SPHINCS+	

https://github.com/ietf-wg-pquip/state-of-protocols-and-pqc

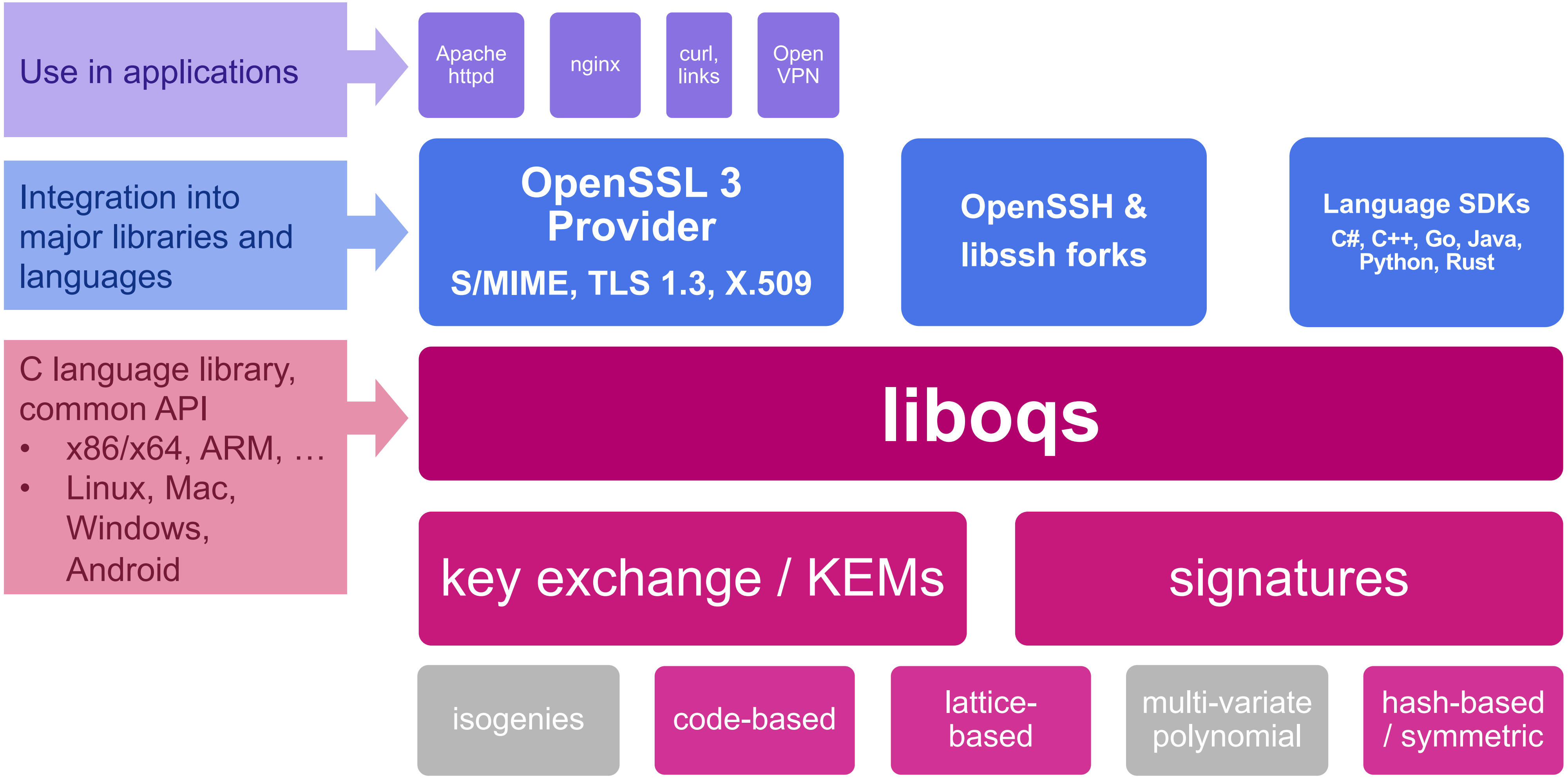
Open source software

OPEN QUANTUM SAFE

software for the transition
to quantum-resistant cryptography

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

Open Quantum Safe Project



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

THE LINUX FOUNDATION

Post-Quantum Cryptography Alliance

To advance the adoption of post-quantum cryptography, by producing high-assurance software implementations of standardized algorithms, and supporting the continued development and standardization of new post-quantum algorithms with software for evaluation and prototyping.

https://pqca.org • https://github.com/PQCA

Post-Quantum Cryptography Alliance

Getting involved

- Current projects: Open Quantum Safe, PQ Code Package
- All development done under open source licenses (MIT, Apache 2)
- Participation open to all
- Organizations can join as members to influence budget and direction

Wrapping up

Call to action

- Inventory where and how your product/code uses cryptography
- Implement crypto agility to minimize code changes
- Begin to pilot the use of post-quantum algorithms
- Prepare to use different algorithms for encryption, key exchange, and signatures
- Test your code for impact of large key sizes, ciphers, and signatures
- Participate in standardization efforts and foster awareness

Post-Quantum Cryptography

Douglas Stebila

UNIVERSITY OF WATERLOO

Public key cryptography designed to resist attacks by quantum computers

- Core algorithms now standardized by US National Institute of Standards and Technology
- In progress: standardization of PQC in Internet protocols
- New technology with different trade-offs

Questions?

- Join the Data & Identity Protection Working Session later today at 4:30pm

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

Appendix

Why use two (or more) algorithms?

1. Reduce risk from break of one algorithm

- Enable early adopters to get post-quantum security without abandoning security of existing algorithms
- Retain security as long as at least one algorithm is not broken
- Uncertainty re: long-term security of existing cryptographic assumptions
- Uncertainty re: newer cryptographic assumptions

2. Ease transition with improved backwards compatibility

3. Standards compliance during transition

Why use two (or more) algorithms?

1. Reduce risk from break of one algorithm

2. Ease transition with improved backwards compatibility

- Design backwards-compatible data structures with old algorithms that can be recognized by systems that haven't been upgraded, but new implementations will use new algorithms
- May not be necessary for negotiated protocols like TLS

3. Standards compliance during transition

Why use two (or more) algorithms?

1. Reduce risk from break of one algorithm

2. Ease transition with improved backwards compatibility and agility

3. Standards compliance during transition

- Early adopters may want to use post-quantum before standards-compliant (FIPS-)certified implementations are available
- Possible to combine (in a certified way) keying material from certified (non-PQ) implementation with non-certified keying material

PQ in other protocols

Composite ML-DSA in X.509

- Data structures for composite public keys and signatures in X.509 (and CMS)
- New OID for each ML-DSA hybrid with RSA, ECDSA, Ed25519, Ed448
- Uses pre-hashing then signs the OID || hash using each algorithm
  - Including composite OID in message adds non-separability
- See IETF PQC Certificates hackathon:
  - https://github.com/IETF-Hackathon/pqc-certificates

https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-sigs/

Secure Shell (SSH)

Key exchange

- Hybrid KEX Internet-Draft available
  - Multiple implementations (Amazon, OQS, wolfSSH, …)
  - OpenSSH using Streamlined NTRU Prime + x25519 **by default** since OpenSSH v9 (April 2022)

Authentication

- No Internet-Drafts for authentication
- Experiments:
  - OQS PQ & hybrid auth
  - OpenSSH using XMSS-based authentication since OpenSSH v7.7 (April 2018)
    - (Not compiled in by default)

IPsec / IKEv2

Key exchange

- RFC for pre-shared keys
- Internet-Drafts for
  - Multiple key exchanges
  - Mechanisms for handling large messages

Authentication

- Internet-Drafts for
  - Hybrid non-composite authentication
  - Negotiation of authentication methods

CMS

Cryptographic Message Syntax; used in S/MIME

Key exchange / PKE

- Internet-Draft for:
  - KEMs generically in CMS
  - Composite KEMs generically, with ML-KEM hybrids

Authentication

- RFC for:
  - LMS in CMS
- Internet-Draft for:
  - SPHINCS+ in CMS

DNSSEC

Authentication

- Internet-Drafts for:
  - Stateful hash-based signatures (expired)

Research ideas

- Merkle Tree ladder [1]
- Request-based fragmentation [2]

[1] https://eprint.iacr.org/2022/1730 [2] https://arxiv.org/abs/2211.14196

OpenPGP

Public key encryption

- Internet-Draft for:
  - Composite PQ/T Kyber + elliptic curves

Digital signatures

- Internet-Draft for:
  - Composite PQ/T Dilithium + elliptic curves
  - SPHINCS+ (standalone – non-hybrid)

Alternative protocol designs

Strategy #1:

Change cryptographic protocols to use PQ algorithms more cleverly/efficiently

- AuthKEM / KEMTLS [1]
- Merkle Tree certificates [2]

Strategy #2:

Change network protocols to be more communication efficient

- Technically about reducing latency due to communication size, not reducing communication size itself
- DNSSEC ARRF [3]
- TurboTLS [4]

[1] https://kemtls.org/ [2] https://datatracker.ietf.org/doc/draft-davidben-tls-merkle-tree-certs/
[3] https://arxiv.org/abs/2211.14196 [4] https://arxiv.org/abs/2302.05311