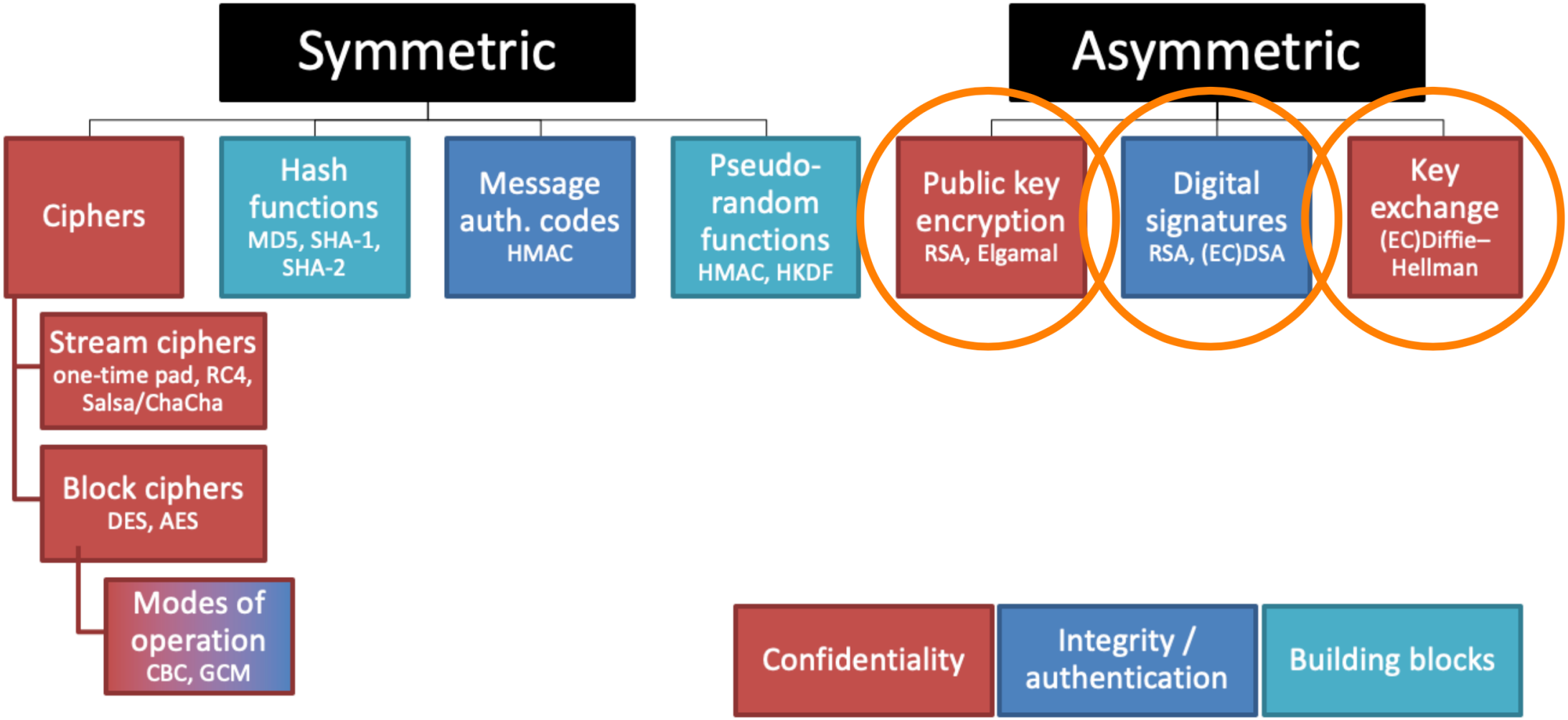
Topic 3.7 - Public-key cryptography
Learning with errors and post-quantum crypto

CO 487/687 • Applied Cryptography

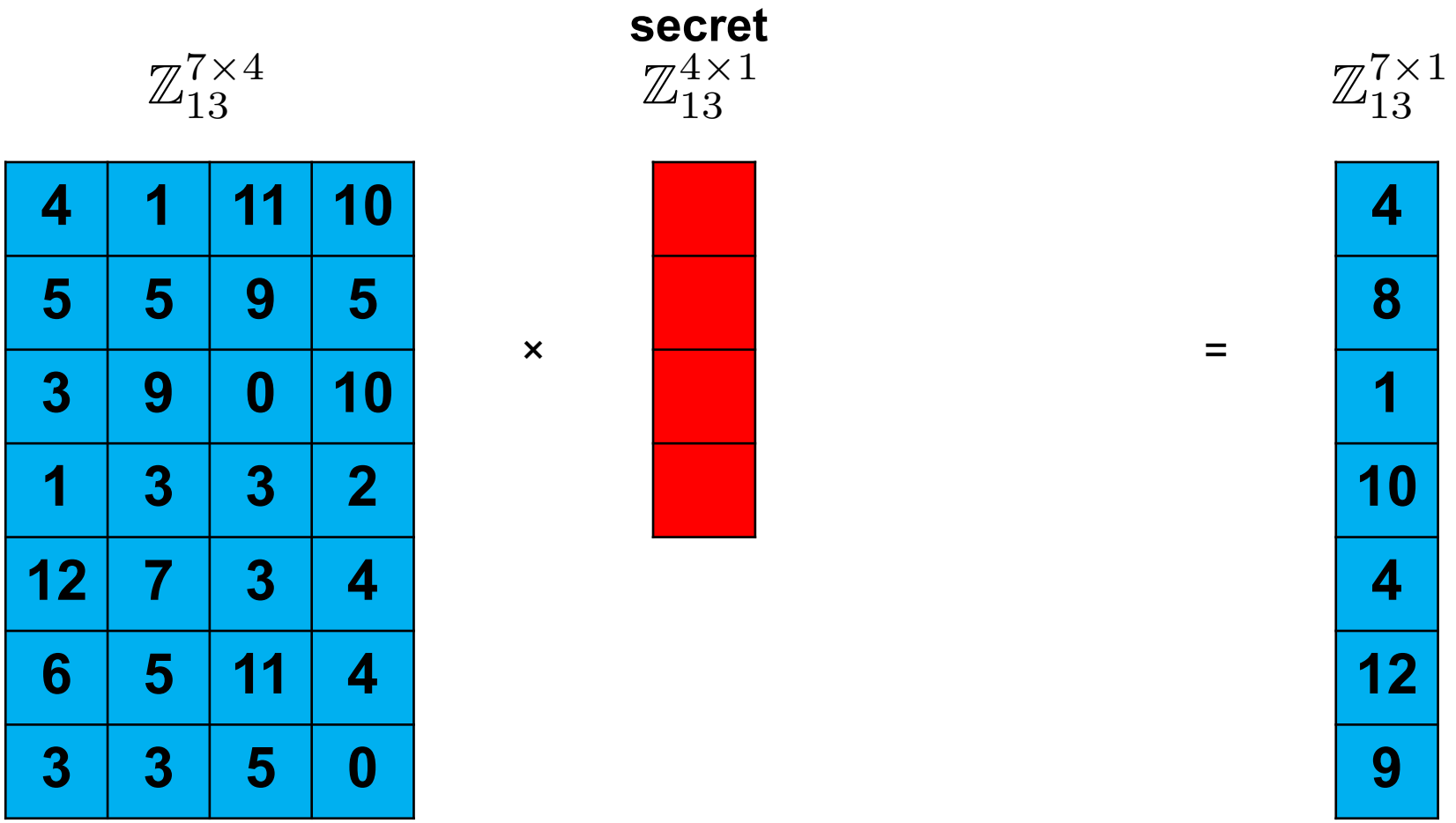
Douglas Stebila

Map of cryptographic primitives



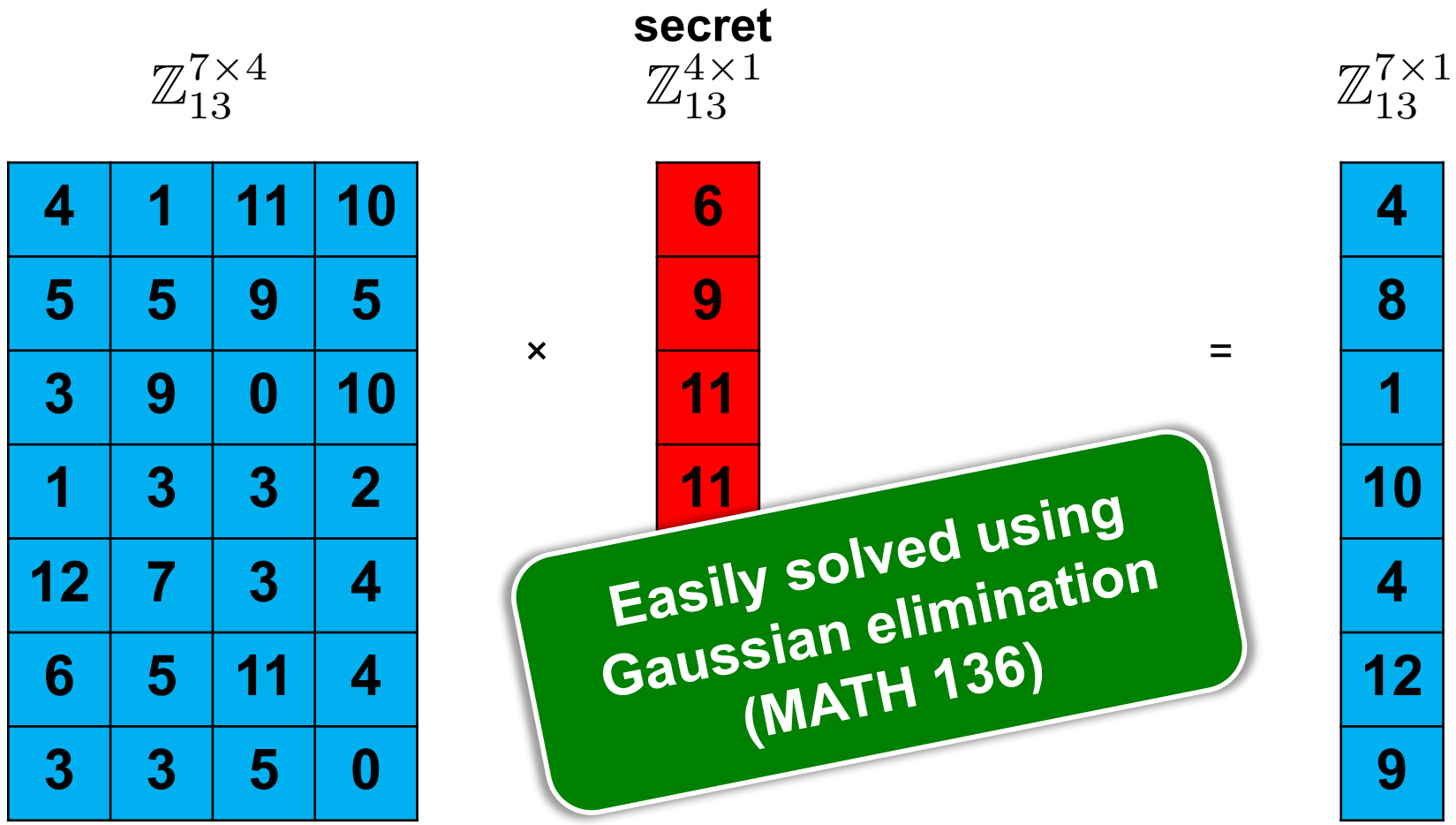
Learning with errors problems

Solving systems of linear equations



Linear system problem: given **blue**, find **red**

Solving systems of linear equations



Linear system problem: given **blue**, find **red**

Learning with errors problem

[Regev 2005]

random $\mathbb{Z}_{13}^{7\times 4}$

4	1	11	10
5	5	9	5
3	9	0	10
1	3	3	2
12	7	3	4
6	5	11	4
3	3	5	0

×

secret $\mathbb{Z}_{13}^{4\times 1}$

6
9
11
11

+

small noise $\mathbb{Z}_{13}^{7\times 1}$

0
-1
1
1
1
0
-1

=

$\mathbb{Z}_{13}^{7\times 1}$

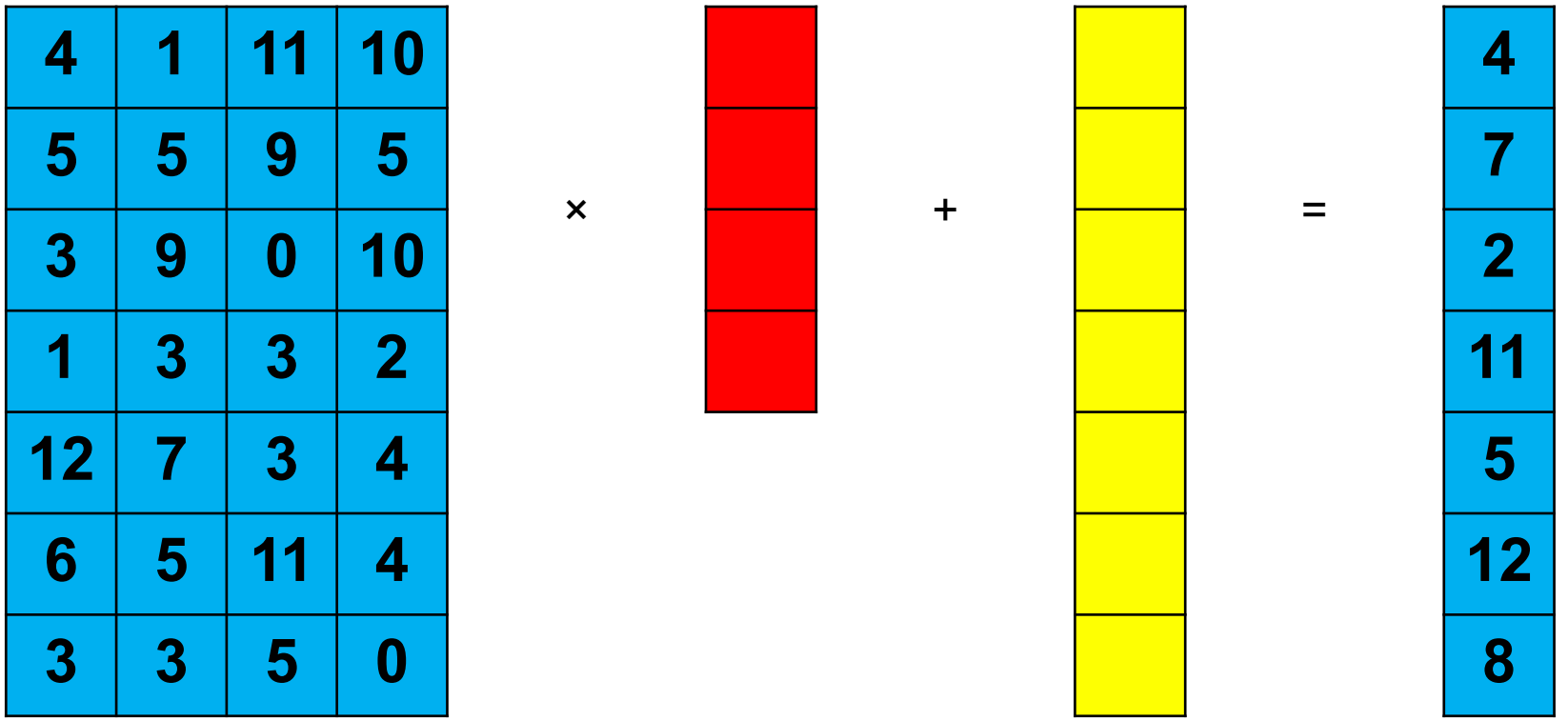
4
7
2
11
5
12
8

Like Discrete Logarithm problem

Learning with errors problem

[Regev 2005]

random $\mathbb{Z}_{13}^{7\times 4}$ | **secret** $\mathbb{Z}_{13}^{4\times 1}$ | **small noise** $\mathbb{Z}_{13}^{7\times 1}$ | $\mathbb{Z}_{13}^{7\times 1}$



Search LWE problem: given **blue**, find **red**

Like Decision Diffie–Hellman problem

Decision learning with errors problem

random $\mathbb{Z}_{13}^{7\times 4}$					secret $\mathbb{Z}_{13}^{4\times 1}$		small noise $\mathbb{Z}_{13}^{7\times 1}$		looks random $\mathbb{Z}_{13}^{7\times 1}$
4	1	11	10						4
5	5	9	5						7
3	9	0	10	×		+		=	2
1	3	3	2						11
12	7	3	4						5
6	5	11	4						12
3	3	5	0						8

Decision LWE problem: given **blue**, distinguish **green** from random

Choice of noise distribution

- Usually a discrete Gaussian distribution of width $s = \alpha q$ for error rate $\alpha < 1$

- Define the Gaussian function

$$\rho_s(\mathbf{x}) = \exp(-\pi \|\mathbf{x}\|^2 / s^2)$$

- The continuous Gaussian distribution has probability density function

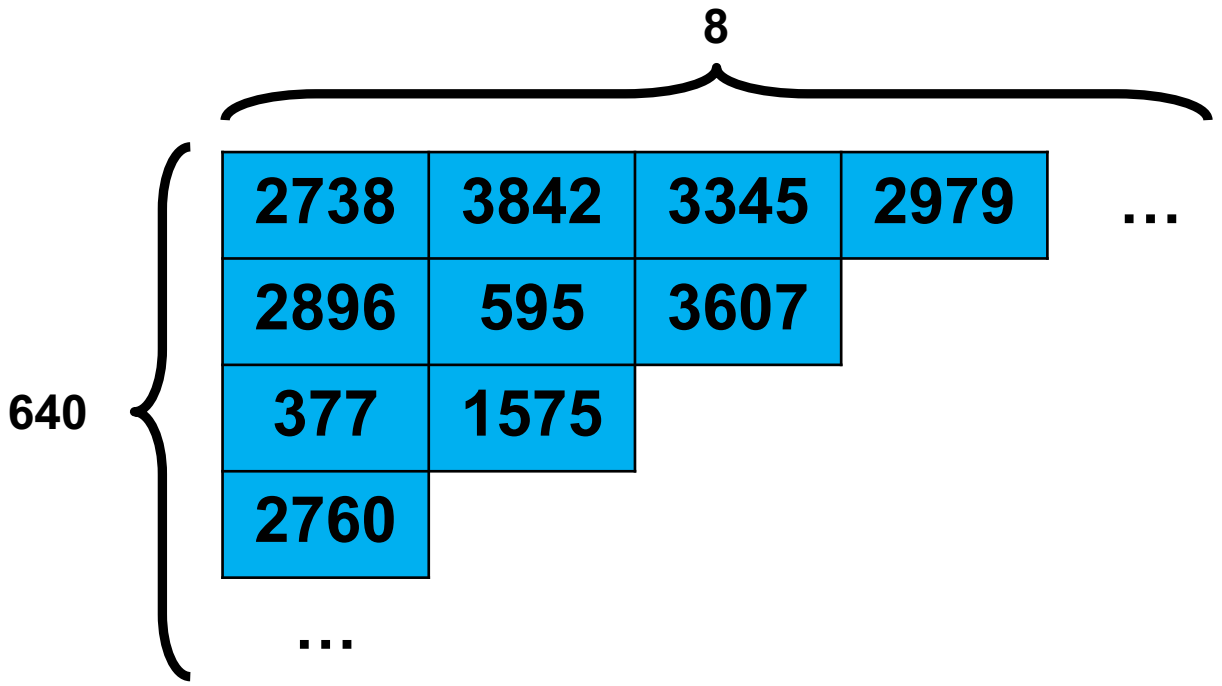
$$f(\mathbf{x}) = \rho_s(\mathbf{x}) / \int_{\mathbb{R}^n} \rho_s(\mathbf{z}) d\mathbf{z} = \rho_s(\mathbf{x}) / s^n$$

Toy example versus real-world example

$\mathbb{Z}_{13}^{7\times 4}$

4	1	11	10
5	5	9	5
3	9	0	10
1	3	3	2
12	7	3	4
6	5	11	4
3	3	5	0

$\mathbb{Z}_{2^{15}}^{640\times 8}$



640 × 8 × 15 bits = **9.4 KiB**

Ring learning with errors problem

[Lyubashevsky, Peikert, Regev 2010]

random

$$\mathbb{Z}_{13}^{7\times 4}$$

4	1	11	10
10	4	1	11
11	10	4	1
1	11	10	4
4	1	11	10
10	4	1	11
11	10	4	1

Each row is the cyclic shift of the row above

Ring learning with errors problem

[Lyubashevsky, Peikert, Regev 2010]

random

$$\mathbb{Z}_{13}^{7\times 4}$$

4	1	11	10
3	4	1	11
2	3	4	1
12	2	3	4
9	12	2	3
10	9	12	2
11	10	9	12

Each row is the cyclic shift of the row above

…

with a special wrapping rule:

x wraps to –*x* mod 13.

Ring learning with errors problem

[Lyubashevsky, Peikert, Regev 2010]

random

$$\mathbb{Z}_{13}^{7\times 4}$$

4	**1**	**11**	**10**

Each row is the cyclic shift of the row above

…

with a special wrapping rule:

x wraps to –*x* mod 13.

So I only need to tell you the first row.

Ring learning with errors problem

[Lyubashevsky, Peikert, Regev 2010]

Coefficients reduced mod 13, polynomials reduced with $x^4 = -1$

$$\mathbb{Z}_{13}[x]/\langle x^4 + 1\rangle$$

	$4 + 1x + 11x^2 + 10x^3$	**random**
×	$6 + 9x + 11x^2 + 11x^3$	**secret**
+	$0 - 1x + 1x^2 + 1x^3$	**small noise**
=	$10 + 5x + 10x^2 + 7x^3$	

Ring learning with errors problem

[Lyubashevsky, Peikert, Regev 2010]

$\mathbb{Z}_{13}[x]/\langle x^4 + 1\rangle$

$4 + 1x + 11x^2 + 10x^3$ **random**

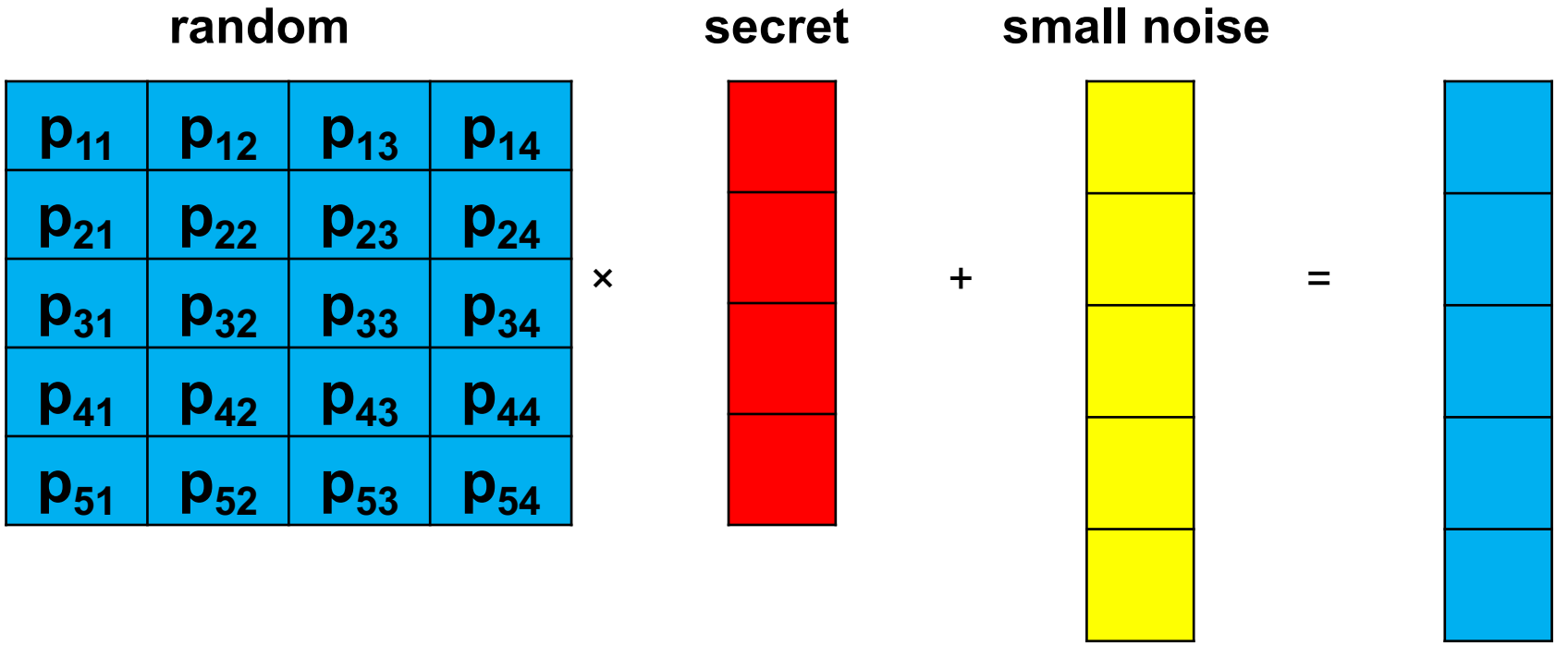
$\times$ **secret**

$+$ **small noise**

$= 10 + 5x + 10x^2 + 7x^3$

Search ring-LWE problem: given **blue**, find **red**

Module learning with errors problem



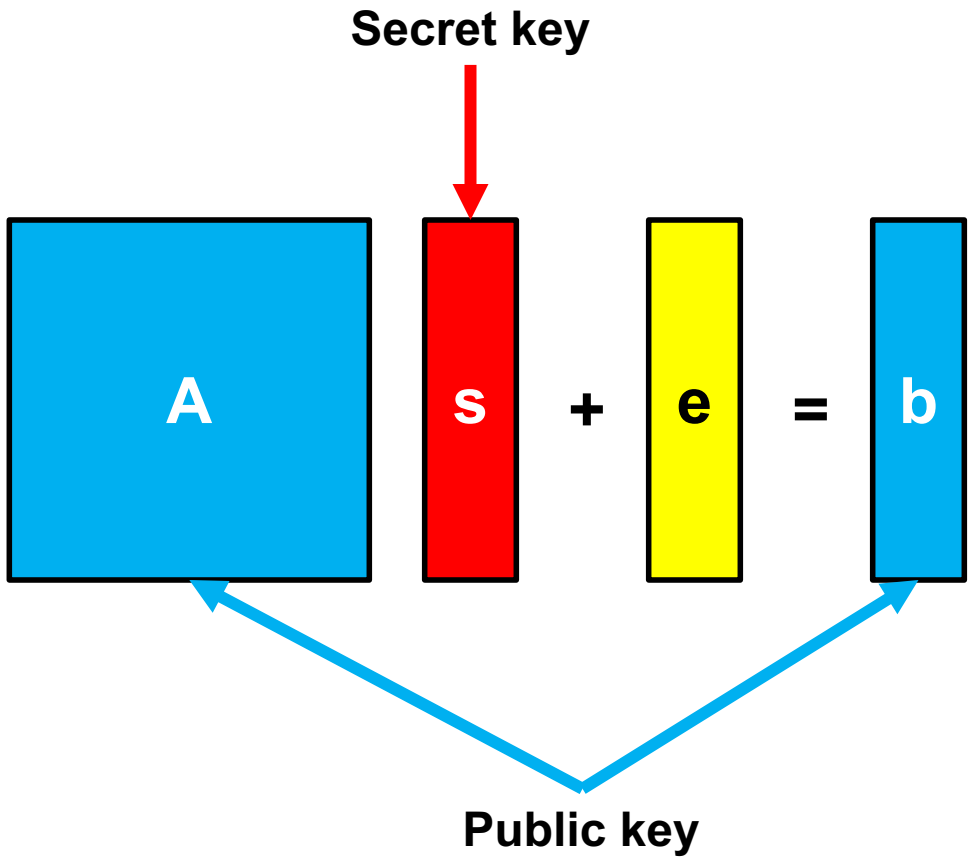
every matrix entry is a polynomial in $\mathbb{Z}_q[x]/(x^n+1)$

Search Module-LWE problem: given **blue**, find **red**

[Langlois & Stehlé, https://eprint.iacr.org/2012/090, DCC 2015]

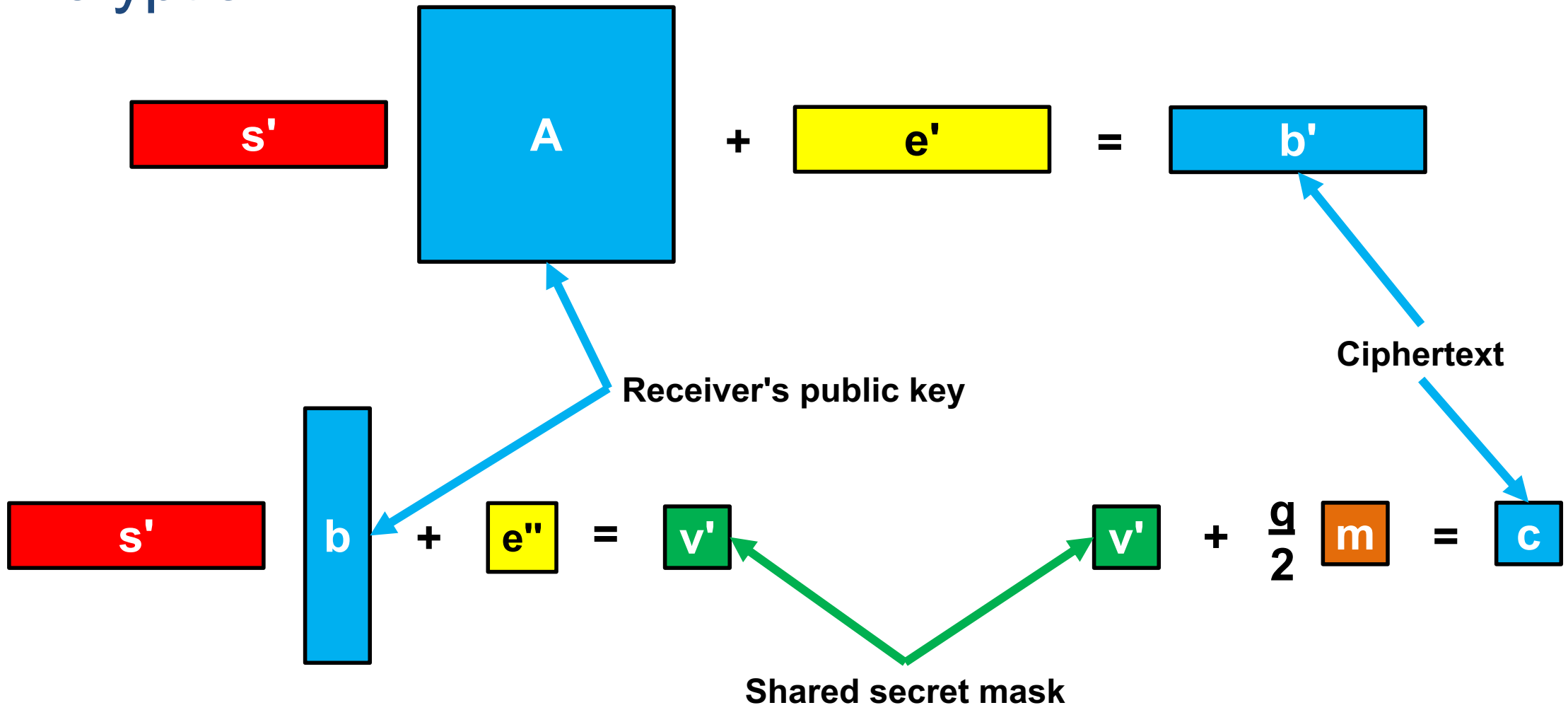
Public key encryption from LWE

Public key encryption from LWE: Key generation



[Lindner, Peikert. CT-RSA 2011]

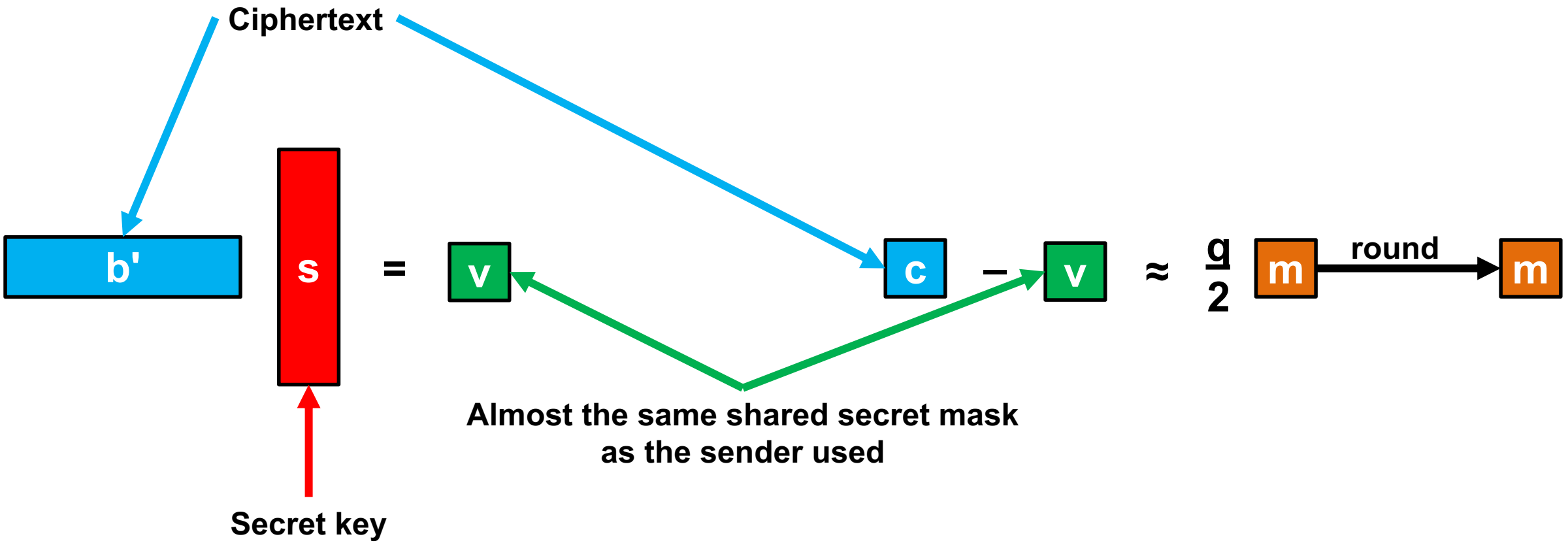
Public key encryption from LWE: Encryption



[Lindner, Peikert. CT-RSA 2011]

Public key encryption from LWE: Decryption

$$v' + \frac{q}{2} m = c$$



[Lindner, Peikert. CT-RSA 2011]

Approximately equal shared secret

The sender uses

$v' = s' (A s + e) + e''$

$= s' A s + (s' e + e'')$

$\approx s' A s$

The receiver uses

$v = (s' A + e') s$

$= s' A s + (e' s)$

$\approx s' A s$

=> Can decrypt as long as noise terms are small with high probability

Lindner–Peikert public key encryption

Let n, q be integers, and χ be a distribution. All arithmetic modulo q.

- KeyGen(): Select $\mathbf{s} \in_R \chi(\mathbb{Z}^n)$, $\mathbf{A} \in_R \mathbb{Z}_q^{n \times n}$, $\mathbf{e} \in_R \chi(\mathbb{Z}^n)$. Compute $\mathbf{b} \leftarrow \mathbf{A}\mathbf{s} + \mathbf{e}$. Return $pk \leftarrow (\mathbf{A}, \mathbf{b})$ and $sk \leftarrow \mathbf{s}$.

- Enc$(pk, x \in \{0,1\})$: Select $\mathbf{s}' \in_R \chi(\mathbb{Z}^n)$, $\mathbf{e}' \in_R \chi(\mathbb{Z}^n)$, $e'' \in_R \chi(\mathbb{Z})$. Compute $\mathbf{b}' \leftarrow \mathbf{s}'\mathbf{A} + \mathbf{e}'$, $v' \leftarrow \langle \mathbf{s}', \mathbf{b} \rangle + e''$, and $c \leftarrow \frac{q}{2}x + v'$. Return $ctxt \leftarrow (\mathbf{b}', c)$.

- Dec$(sk, (\mathbf{b}', c))$: Compute $v \leftarrow \langle \mathbf{b}', \mathbf{s} \rangle$.

$$\text{Return} \begin{cases} 0, & \text{if } c - v \in \{0, \ldots, \frac{q}{4} - 1\} \cup \{\frac{3q}{4}, \ldots, q-1\} \\ 1, & \text{if } c - v \in \{\frac{q}{4}, \ldots, \frac{3q}{4} - 1\} \end{cases}$$

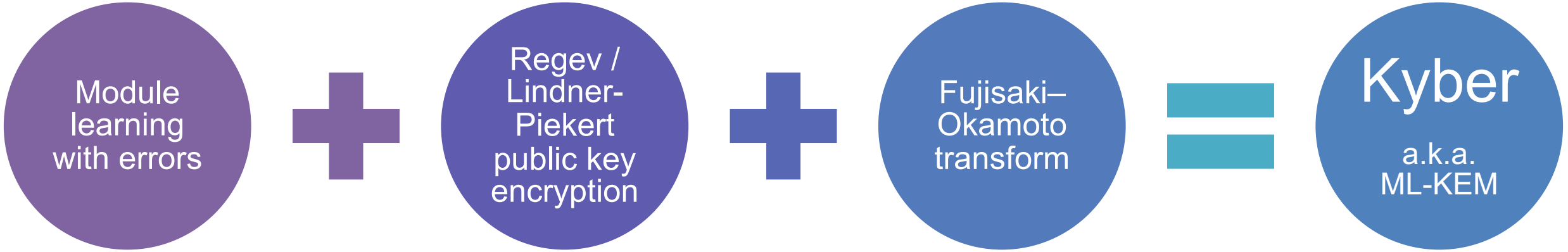
[Lindner, Peikert; CT-RSA 2011]

Security of Lindner–Peikert

- **Theorem:** If the decision learning with errors problem is hard, then Lindner–Peikert encryption is semantically secure against chosen plaintext attacks.

- Is the decision learning with errors problem hard?

[Lindner, Peikert; CT-RSA 2011]

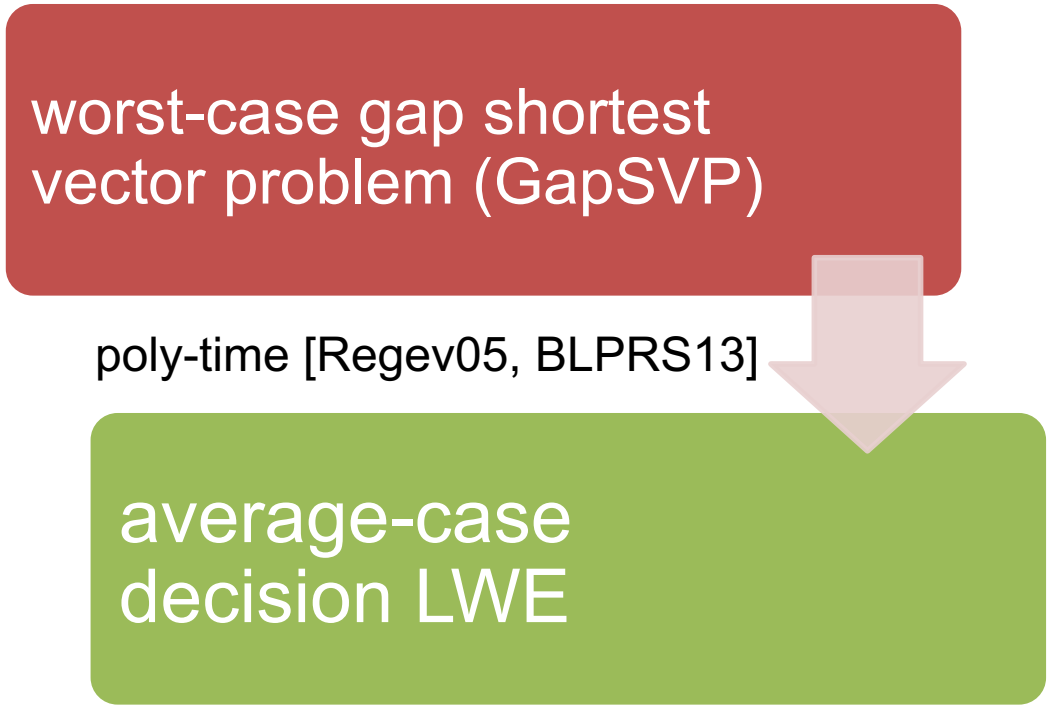


FO converts
IND-CPA PKE
into
IND-CCA KEM

Security of LWE-based cryptography

"Lattice-based"

Hardness of decision LWE – "lattice-based"



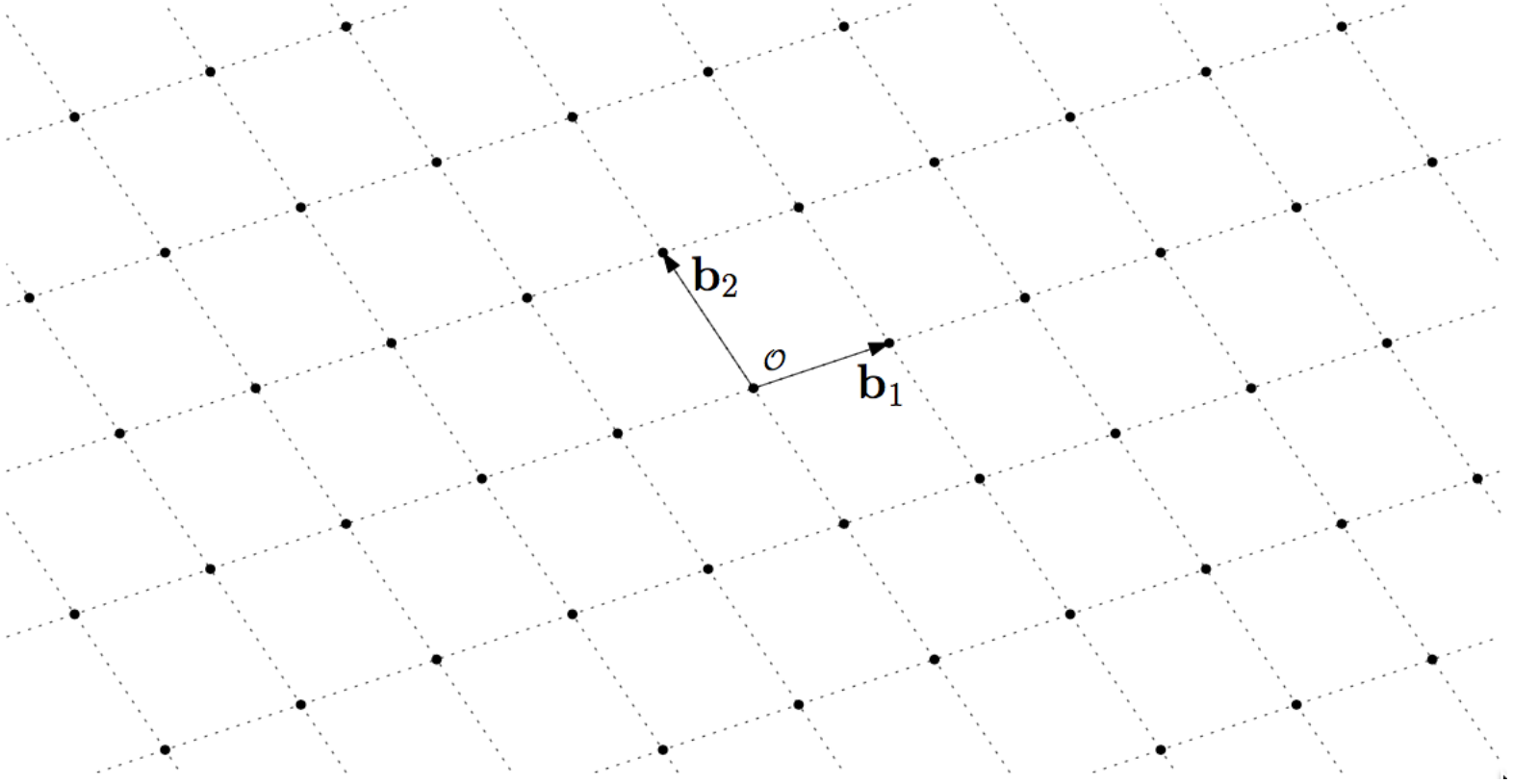
Lattices

Let $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subseteq \mathbb{Z}_q^{n \times n}$ be a set of linearly independent basis vectors for $\mathbb{Z}_q^n$. Define the corresponding **lattice**

$$\mathcal{L} = \mathcal{L}(\mathbf{B}) = \left\{ \sum_{i=1}^{n} z_i \mathbf{b}_i : z_i \in \mathbb{Z} \right\} .$$

(In other words, a lattice is a set of *integer* linear combinations.)

Lattices

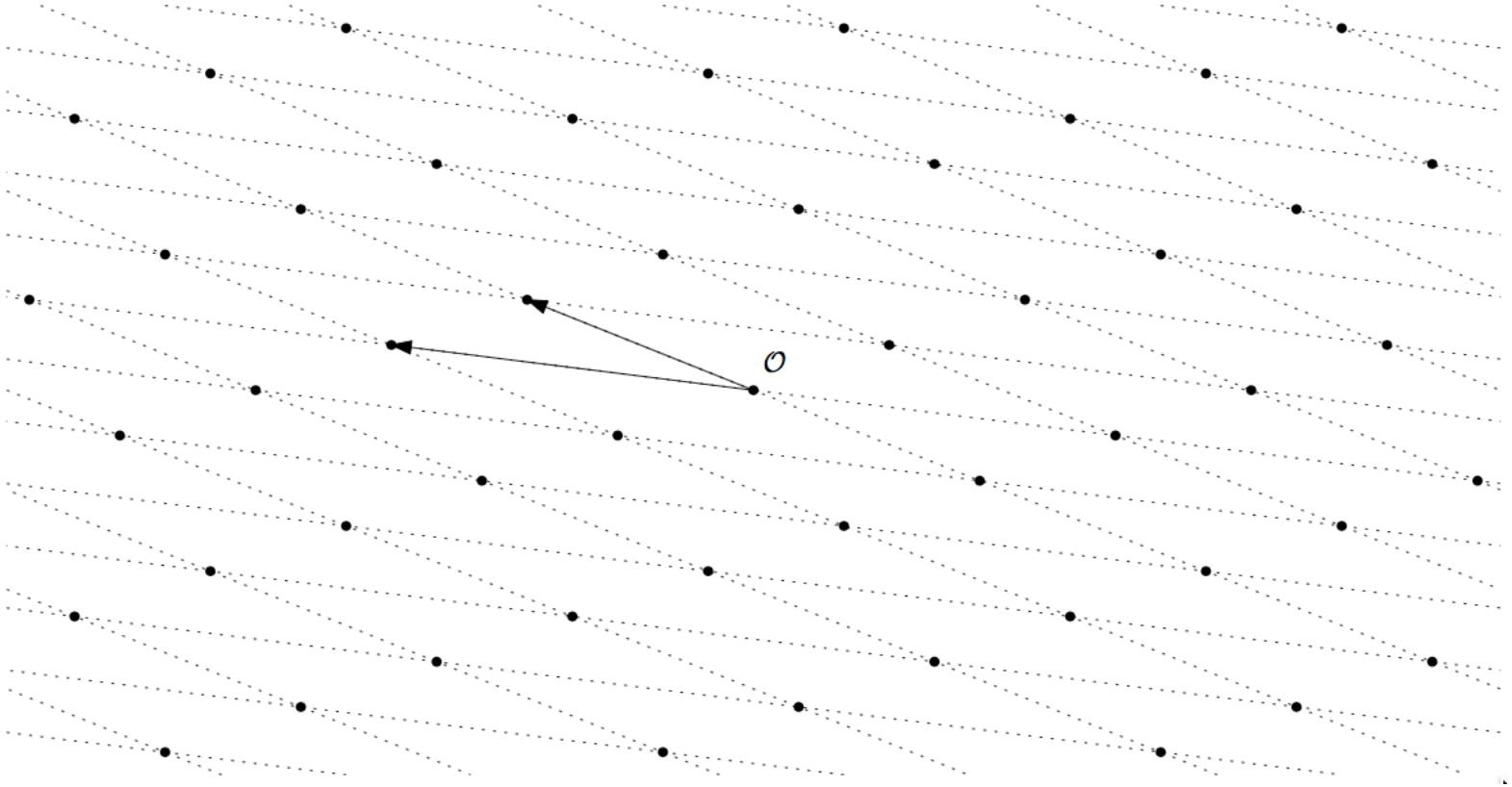


Discrete additive subgroup of $\mathbb{Z}^n$

Equivalently, integer linear combinations of a basis

Diagram from http://www.cs.bris.ac.uk/pgrad/csjhvdp/files/bkz.pdf

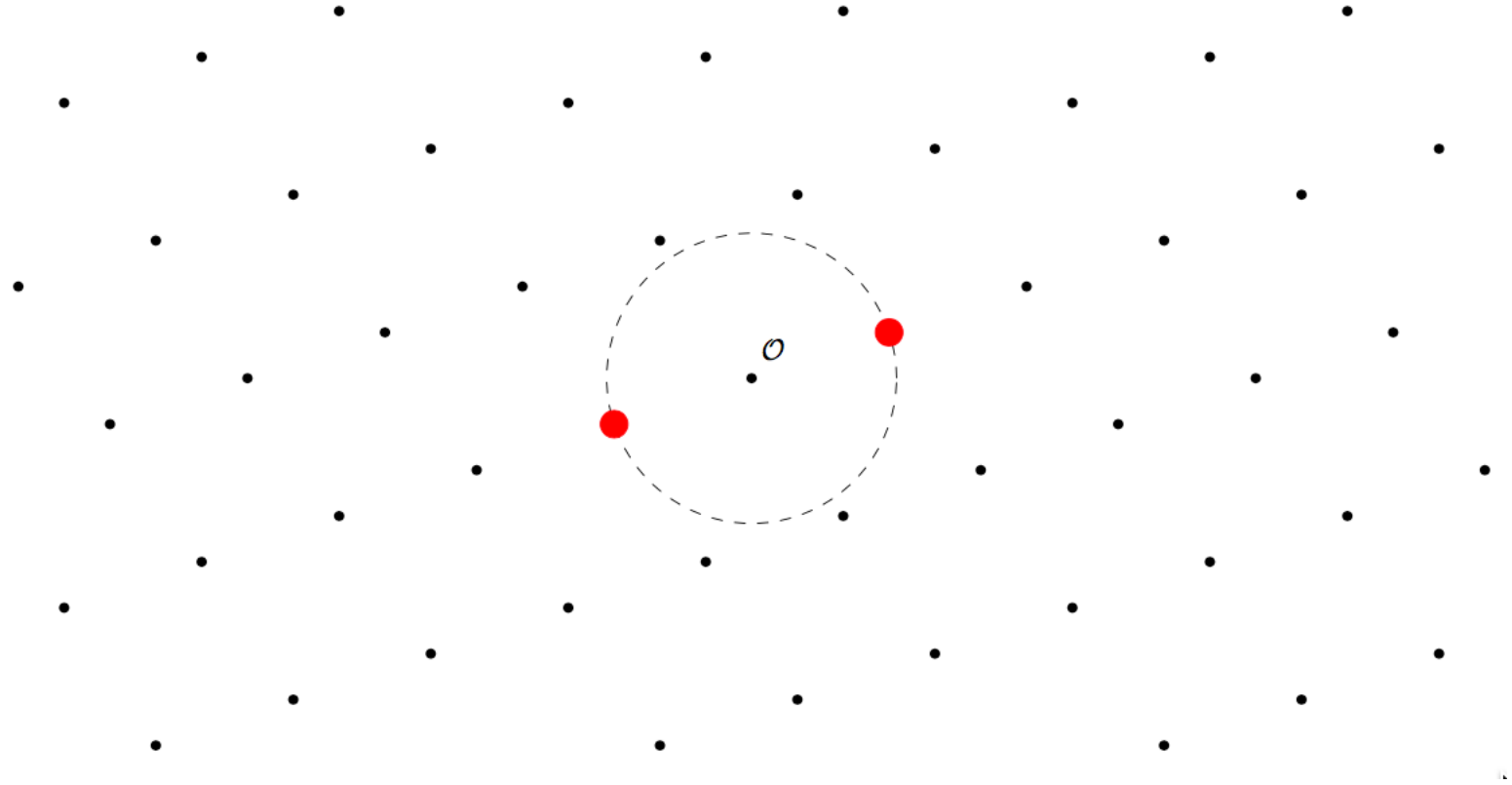
Lattices



There are many bases for the same lattice – some short and orthogonalish, some long and acute.

Diagram from http://www.cs.bris.ac.uk/pgrad/csjhvdp/files/bkz.pdf

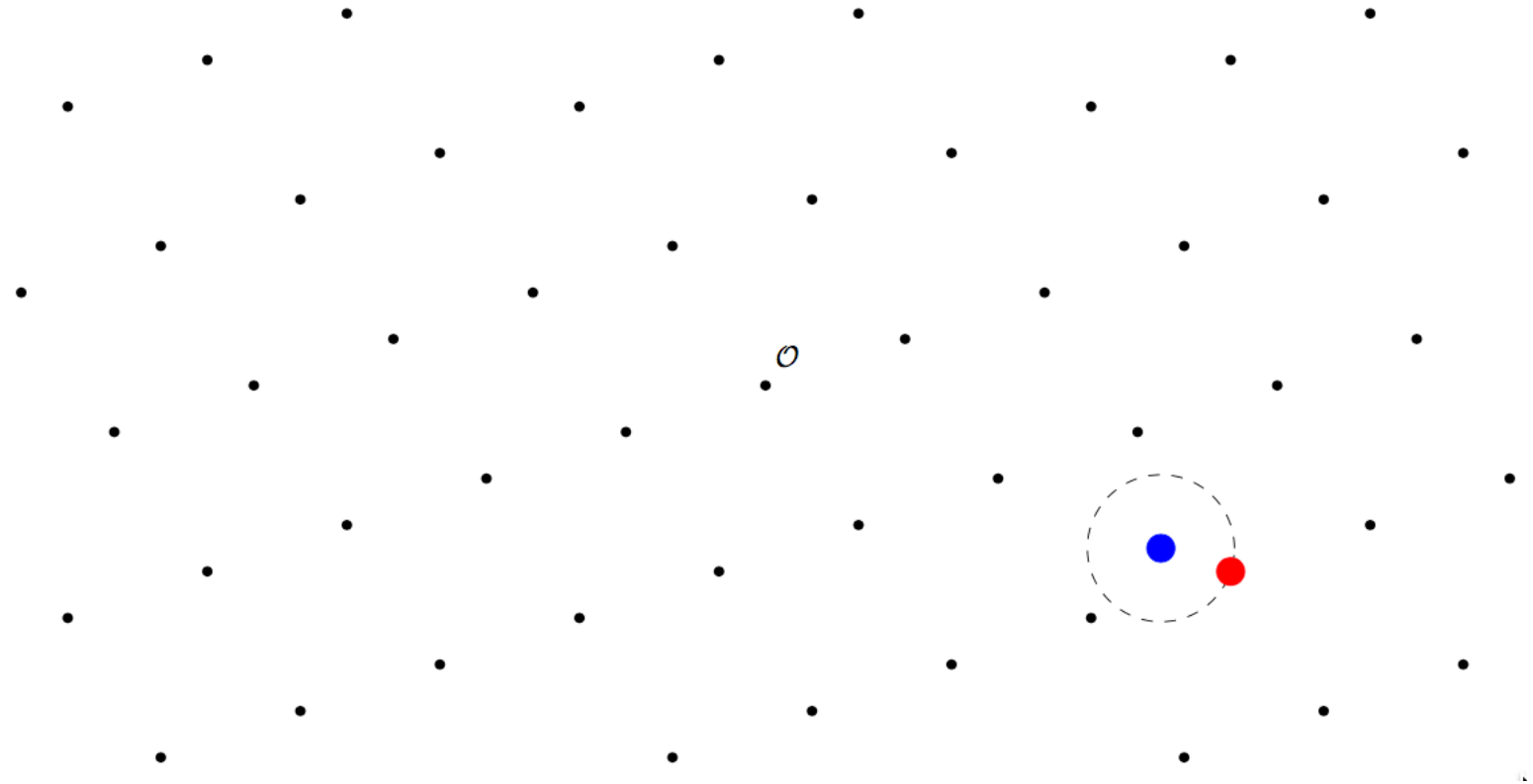
Shortest vector problem



Given some basis for the lattice, find the shortest non-zero lattice point.

Diagram from http://www.cs.bris.ac.uk/pgrad/csjhvdp/files/bkz.pdf

Closest vector problem



Given some basis for the lattice and a target point in the space, find the closest lattice point.

Diagram from http://www.cs.bris.ac.uk/pgrad/csjhvdp/files/bkz.pdf

Connecting LWE and shortest vector problem

- **Theorem [Regev 2005].** For appropriate modulus q and error distribution, solving the decision LWE problem is at least as hard as solving a variant of the shortest vector problem on an n-dimensional lattice.

- (Several technical details omitted.)

[Regev; STOC 2005]

Is solving shortest vector problem hard?

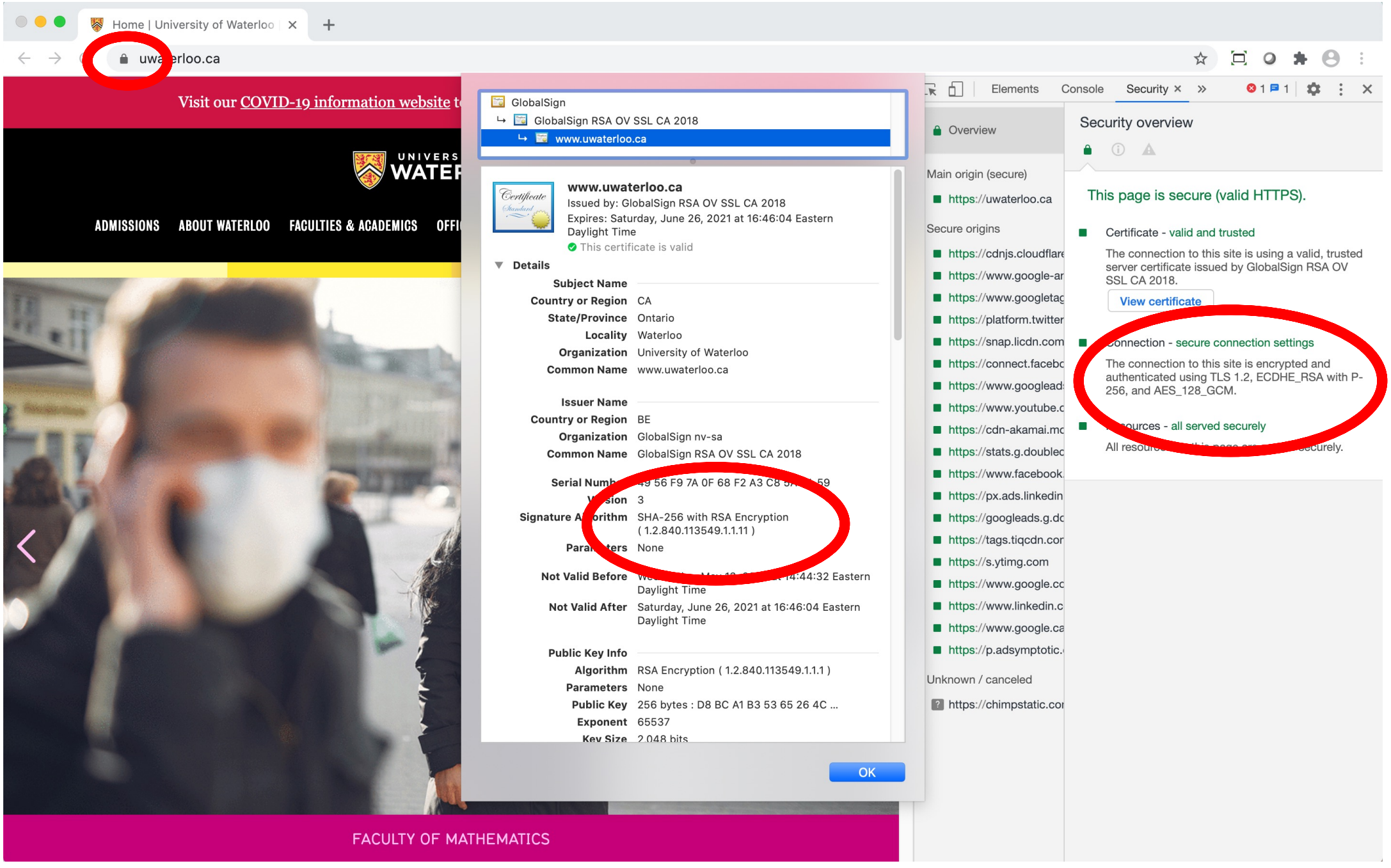
- For some parameters, we can prove it is NP-hard.
  (But these are not the parameters we use in cryptography.)

- Best algorithms to date for parameters used in cryptography are sub-exponential.

- Notably, quantum computers do not seem to give a substantial improvement on solving shortest vector problem or LWE.

- => Promising candidate for quantum-resistant cryptography.

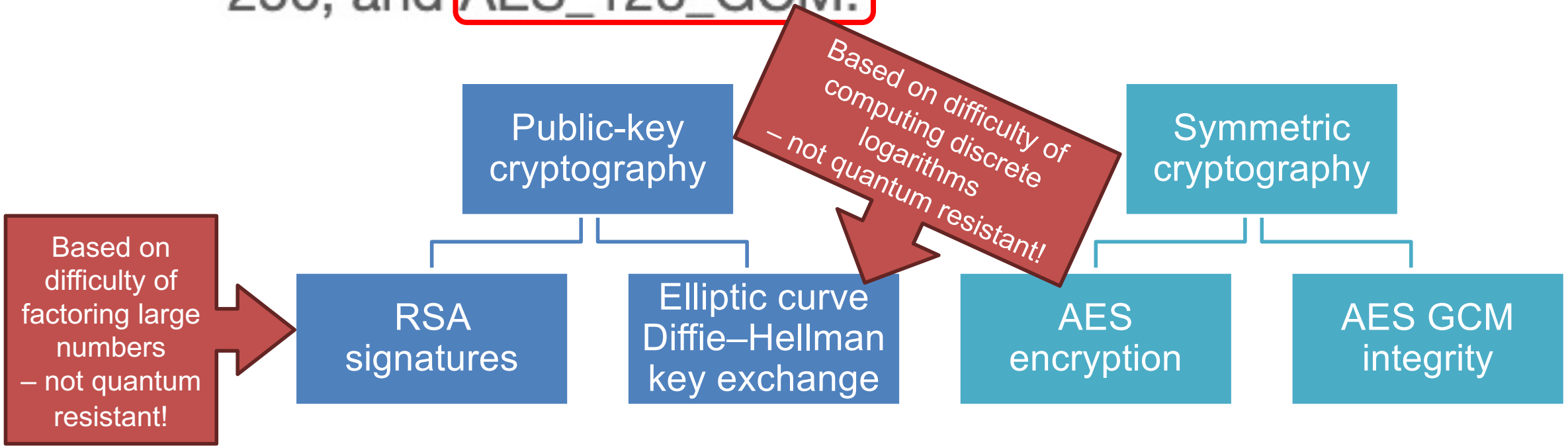
Post-quantum cryptography


Home | University of Waterloo
uwaterloo.ca
Visit our COVID-19 information website
ADMISSIONS
ABOUT WATERLOO
FACULTIES & ACADEMICS
FACULTY OF MATHEMATICS
GlobalSign
GlobalSign RSA OV SSL CA 2018
www.uwaterloo.ca
www.uwaterloo.ca
Issued by: GlobalSign RSA OV SSL CA 2018
Expires: Saturday, June 26, 2021 at 16:46:04 Eastern Daylight Time
This certificate is valid
Details
Subject Name
Country or Region CA
State/Province Ontario
Locality Waterloo
Organization University of Waterloo
Common Name www.uwaterloo.ca
Issuer Name
Country or Region BE
Organization GlobalSign nv-sa
Common Name GlobalSign RSA OV SSL CA 2018
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters None
Not Valid Before Daylight Time
Not Valid After Saturday, June 26, 2021 at 16:46:04 Eastern Daylight Time
Public Key Info
Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters None
Public Key 256 bytes : D8 BC A1 B3 53 65 26 4C ...
Exponent 65537
OK
Elements
Console
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 GlobalSign RSA OV SSL CA 2018.
View certificate
Connection - secure connection settings
The connection to this site is encrypted and authenticated using TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM.

Cryptographic building blocks

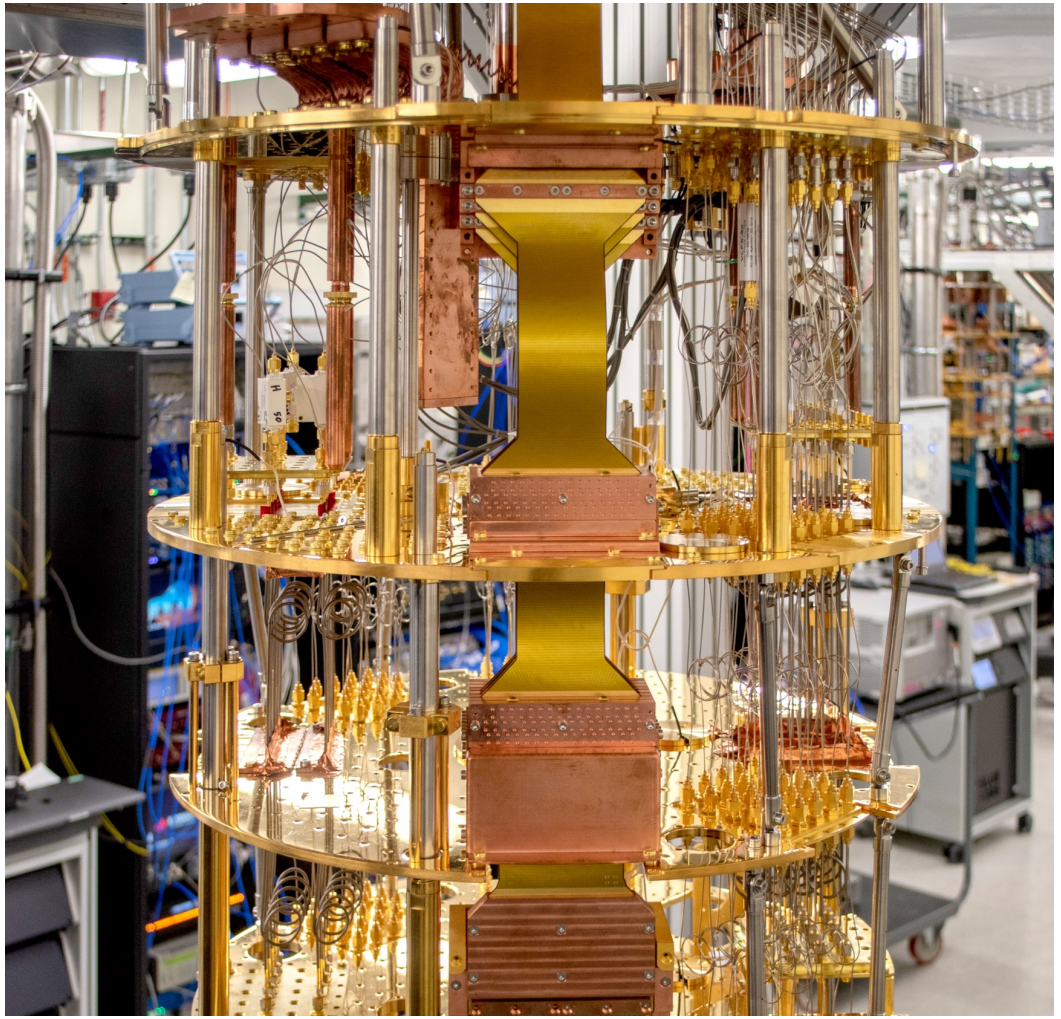
Connection - secure connection settings

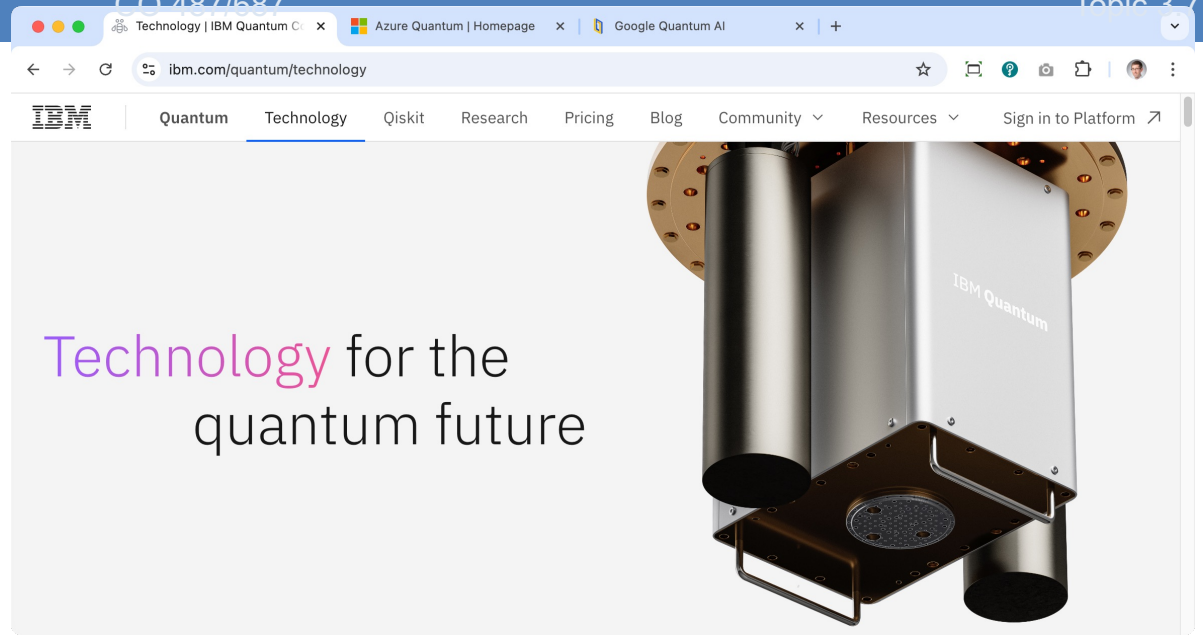
The connection to this site is encrypted and authenticated using TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM.

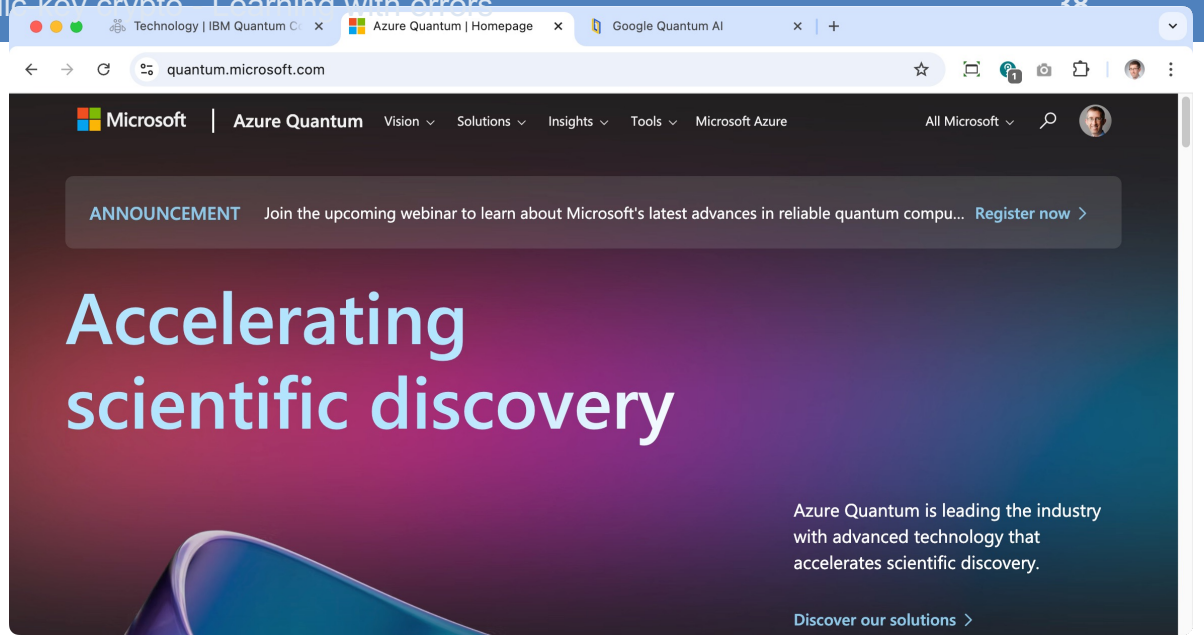


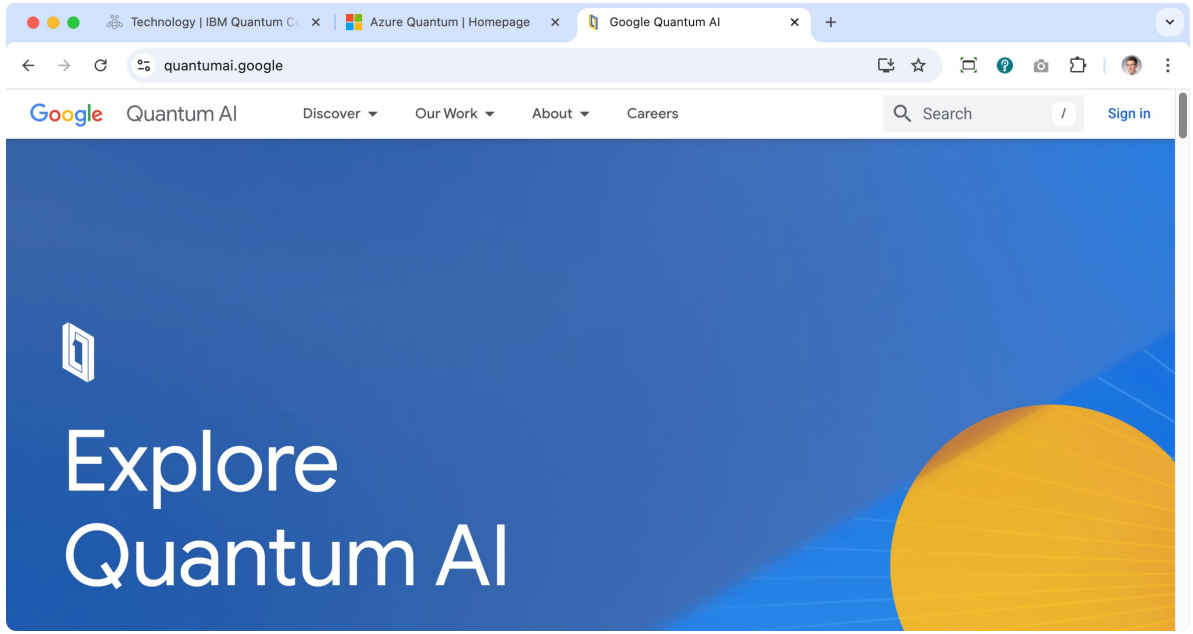
Quantum computing

- 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.

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

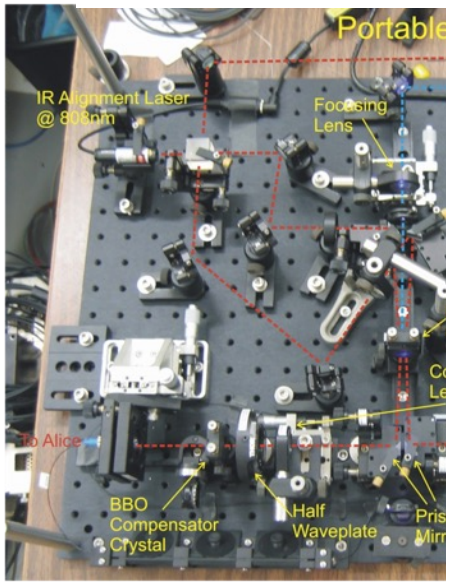
Uses quantum mechanics to protect information

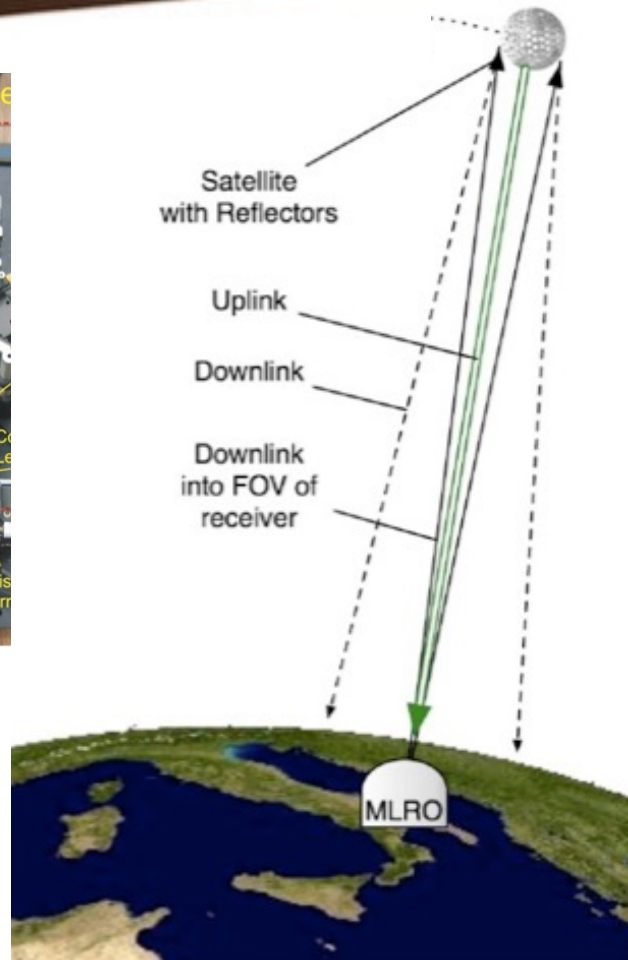
Doesn't require a full quantum computer

But does require new communication infrastructure

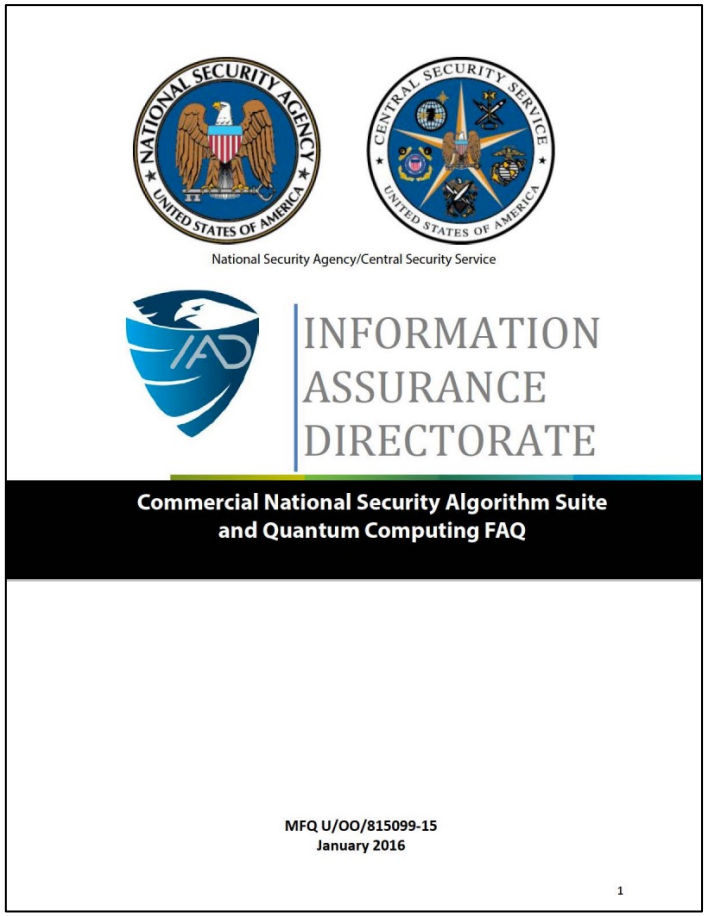
- Lasers, telescopes, fiber optics, …

=> 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

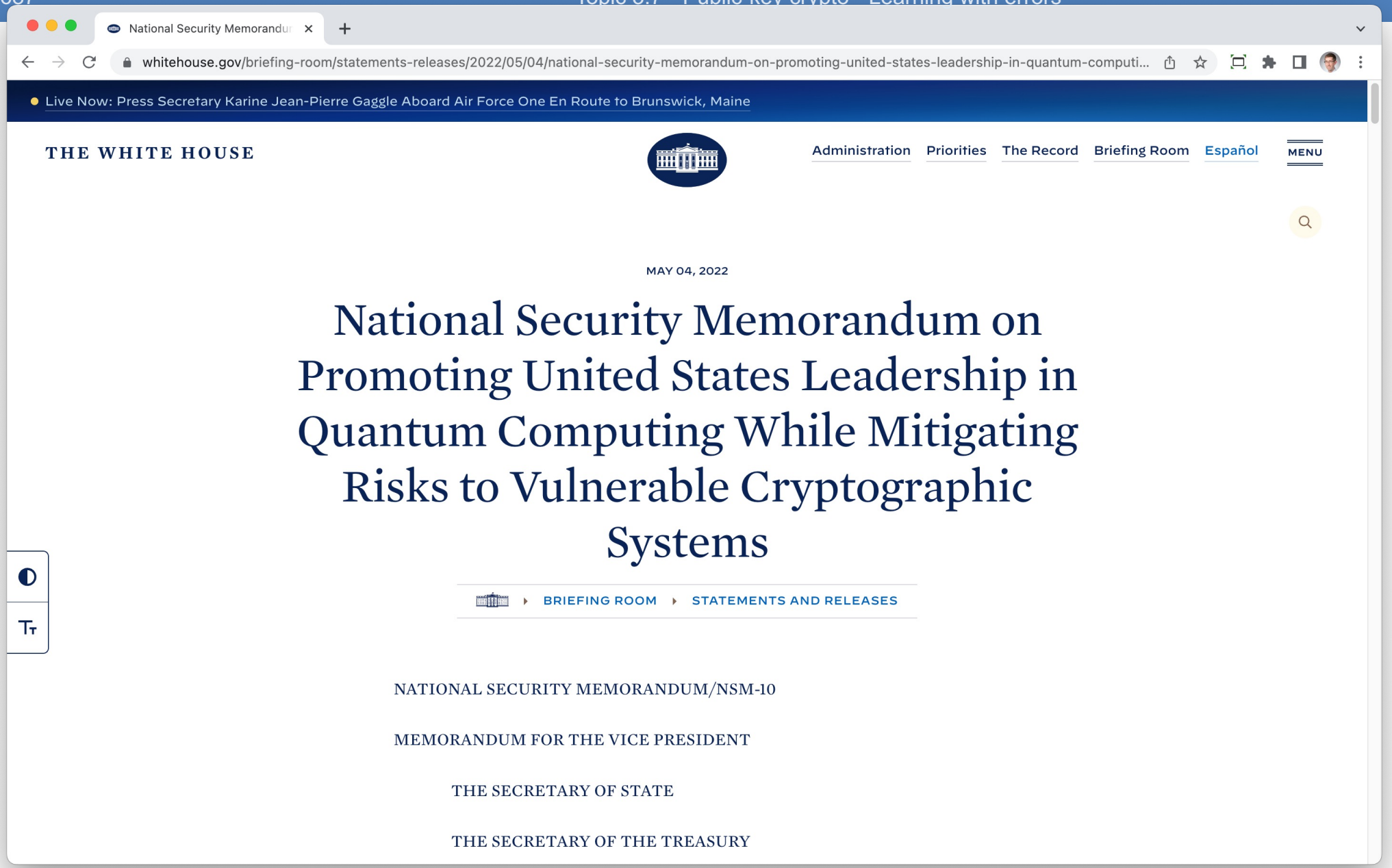
MFQ U/OO/815099-15
January 2016

1

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

– NSA Information Assurance Directorate, Aug. 2015

Aug. 2015 (Jan. 2016)



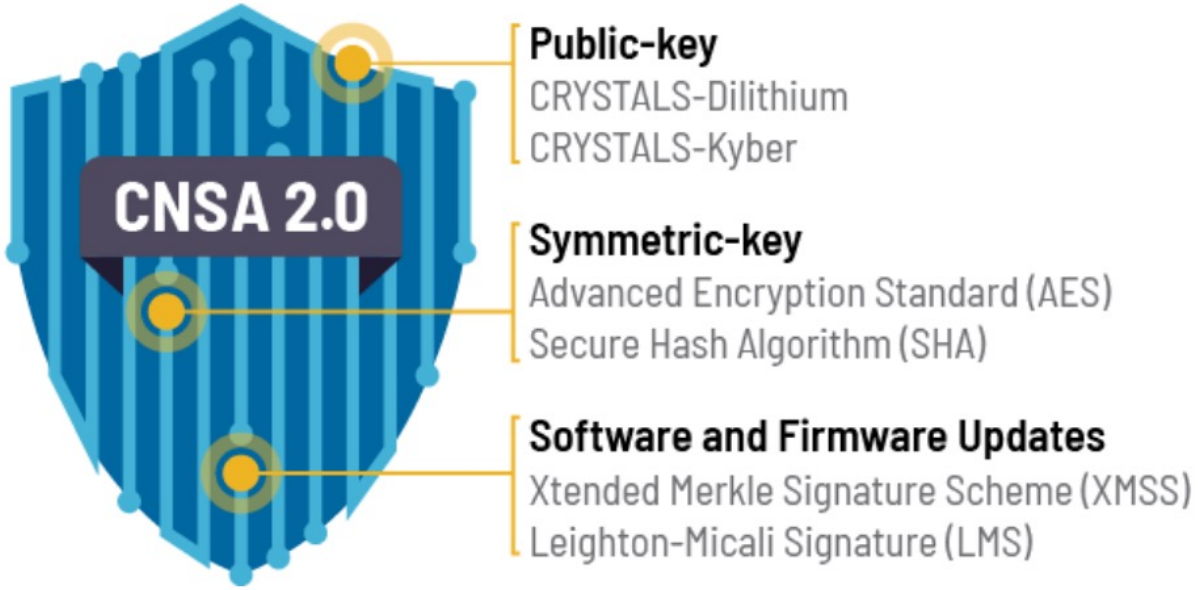
https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

National Security Agency | Cybersecurity Advisory

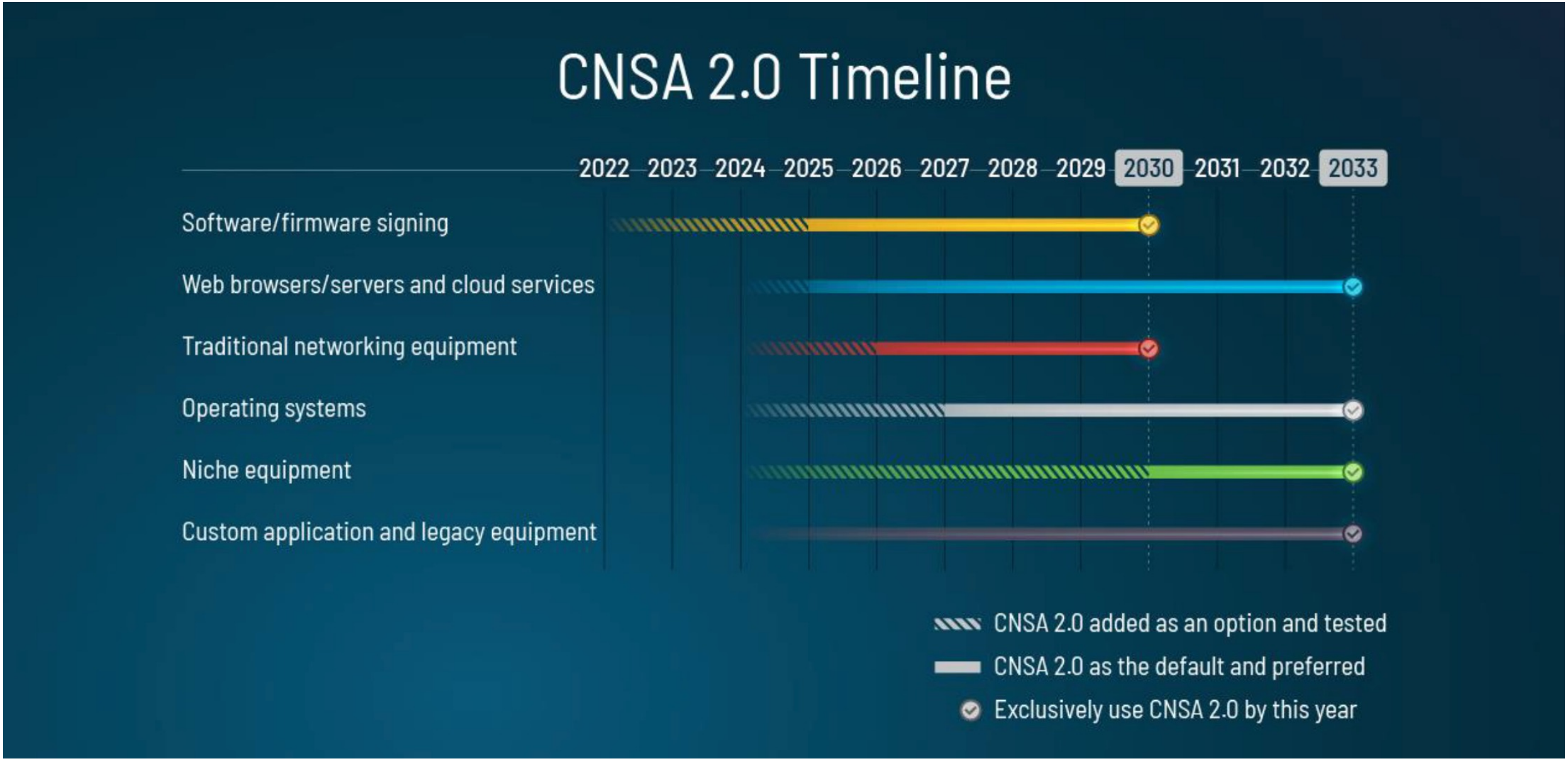
Announcing the Commercial National Security Algorithm Suite 2.0

Executive summary

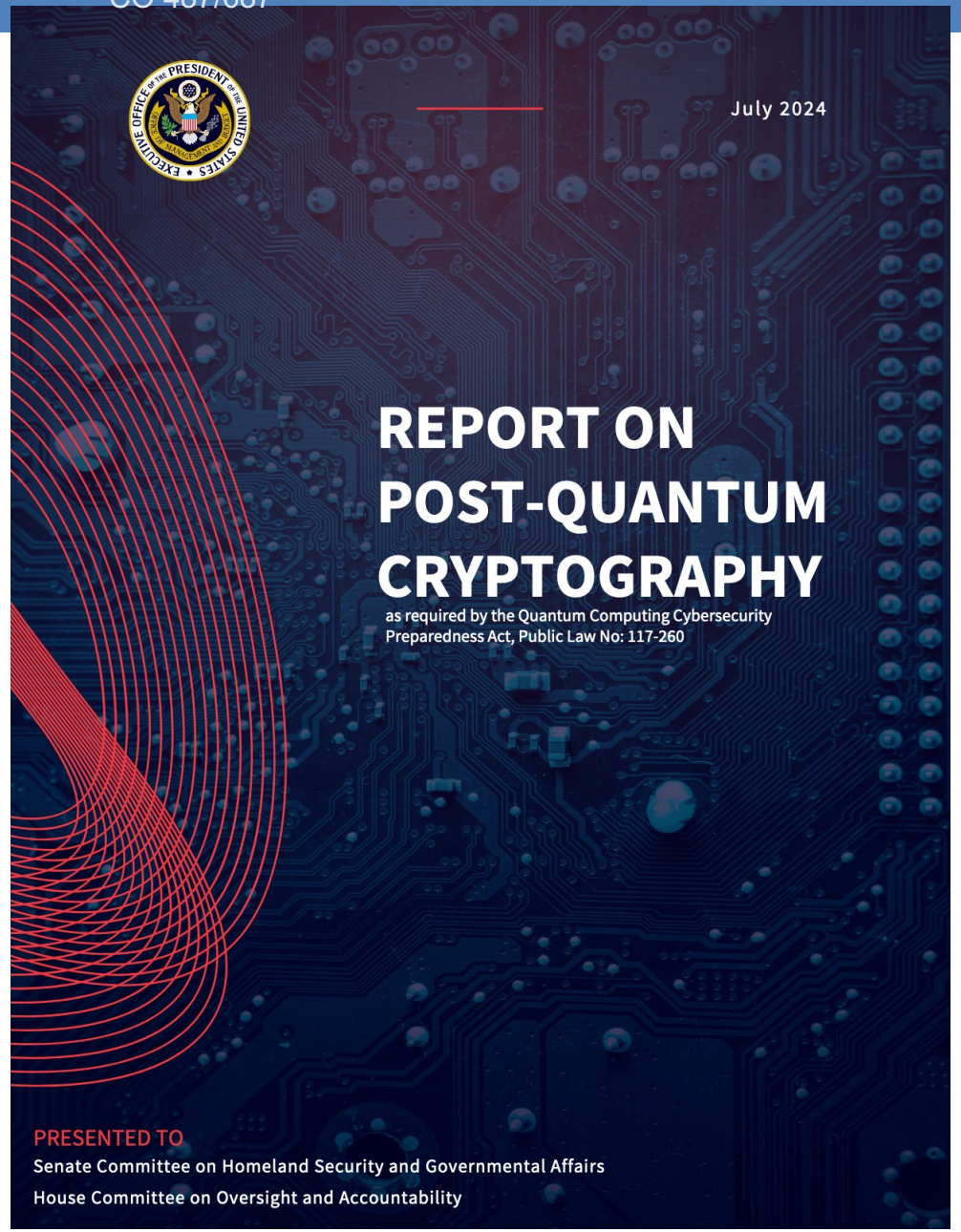
The need for protection against a future deployment of a cryptanalytically relevant quantum computer (CRQC) is well documented. That story begins in the mid-1990s when Peter Shor discovered a CRQC would break



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

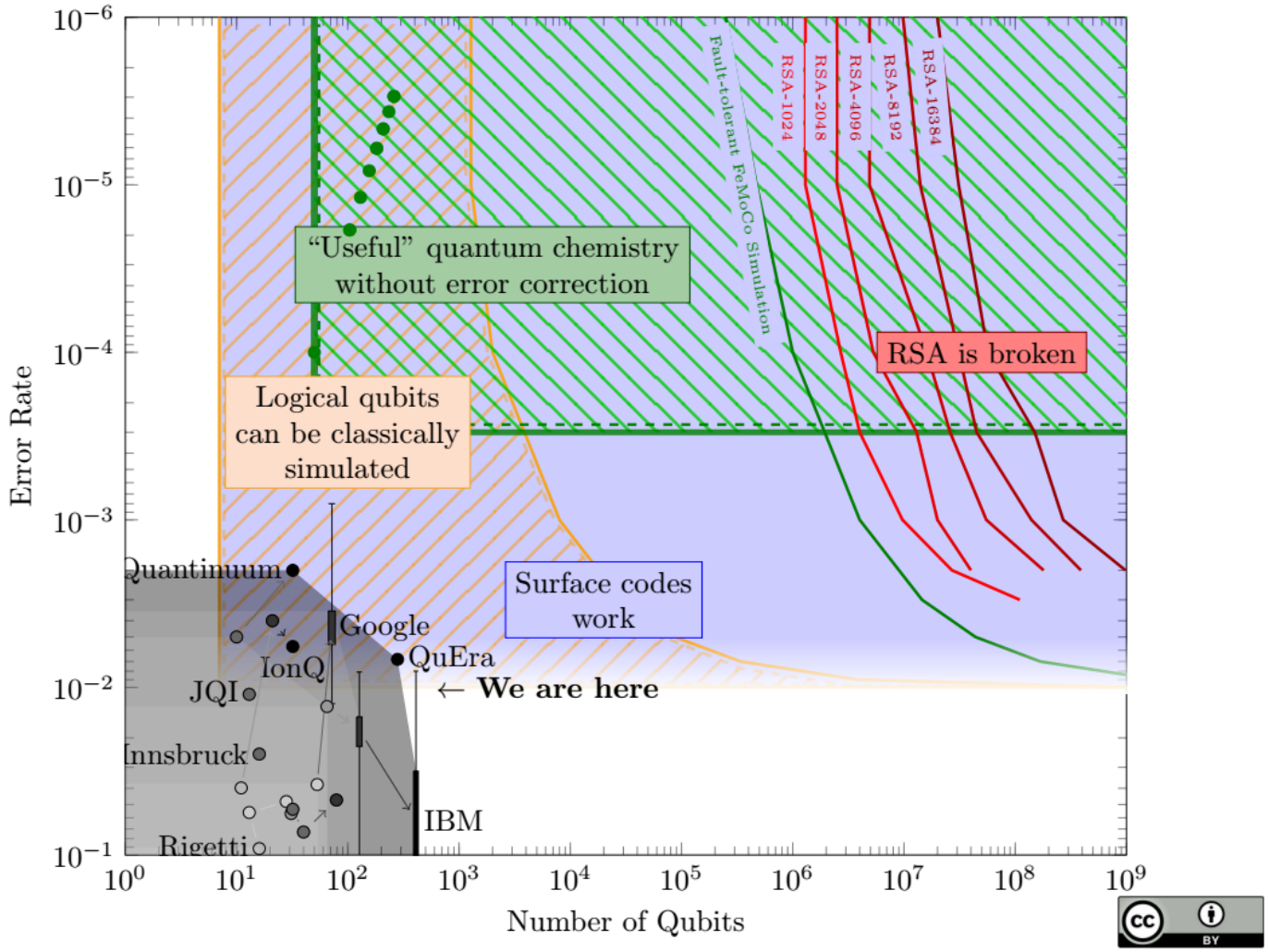


Estimated cost to migrate US government to PQC between 2025–2035:

$7.1 billion

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

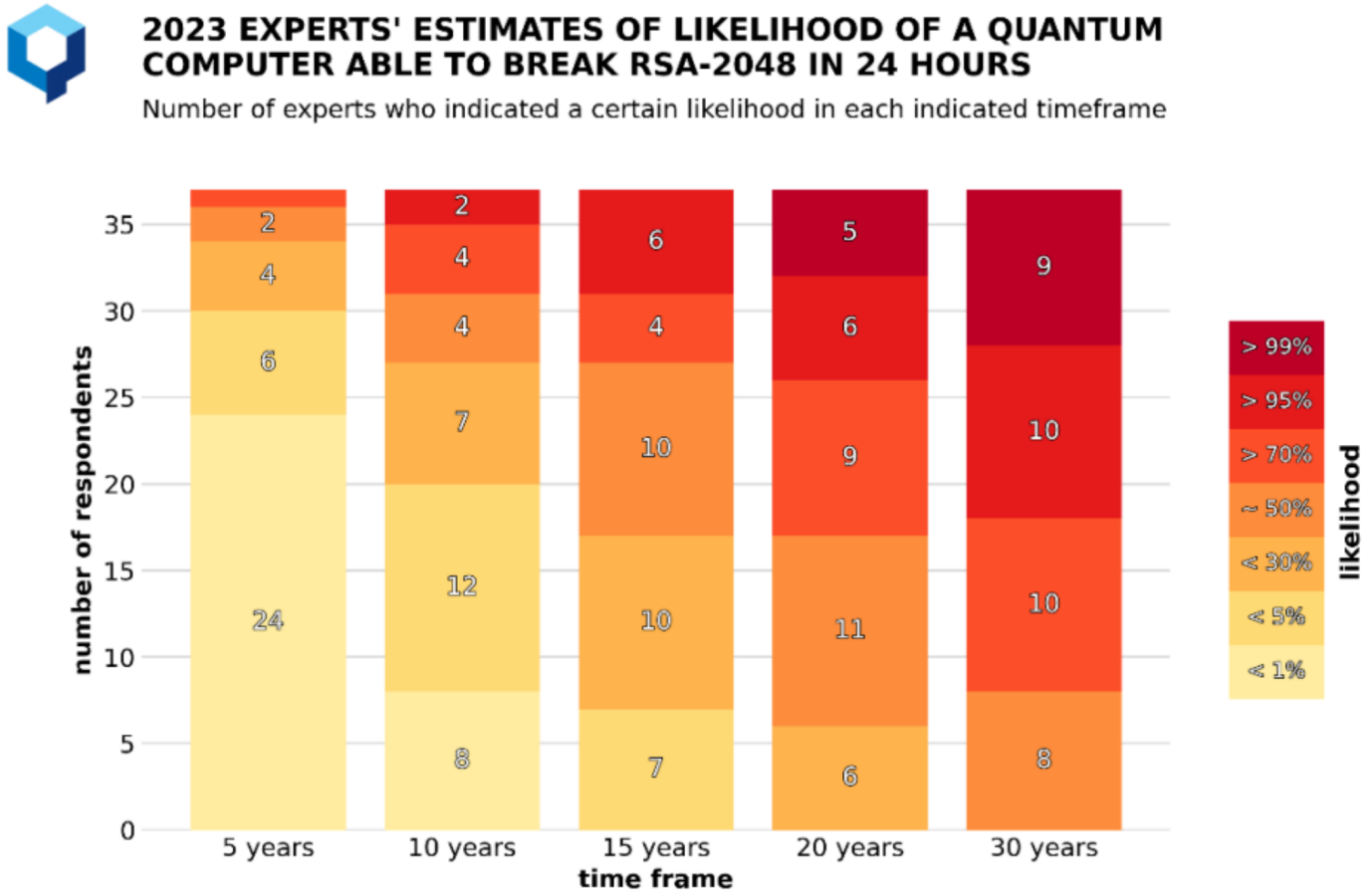
Landscape of quantum computing



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

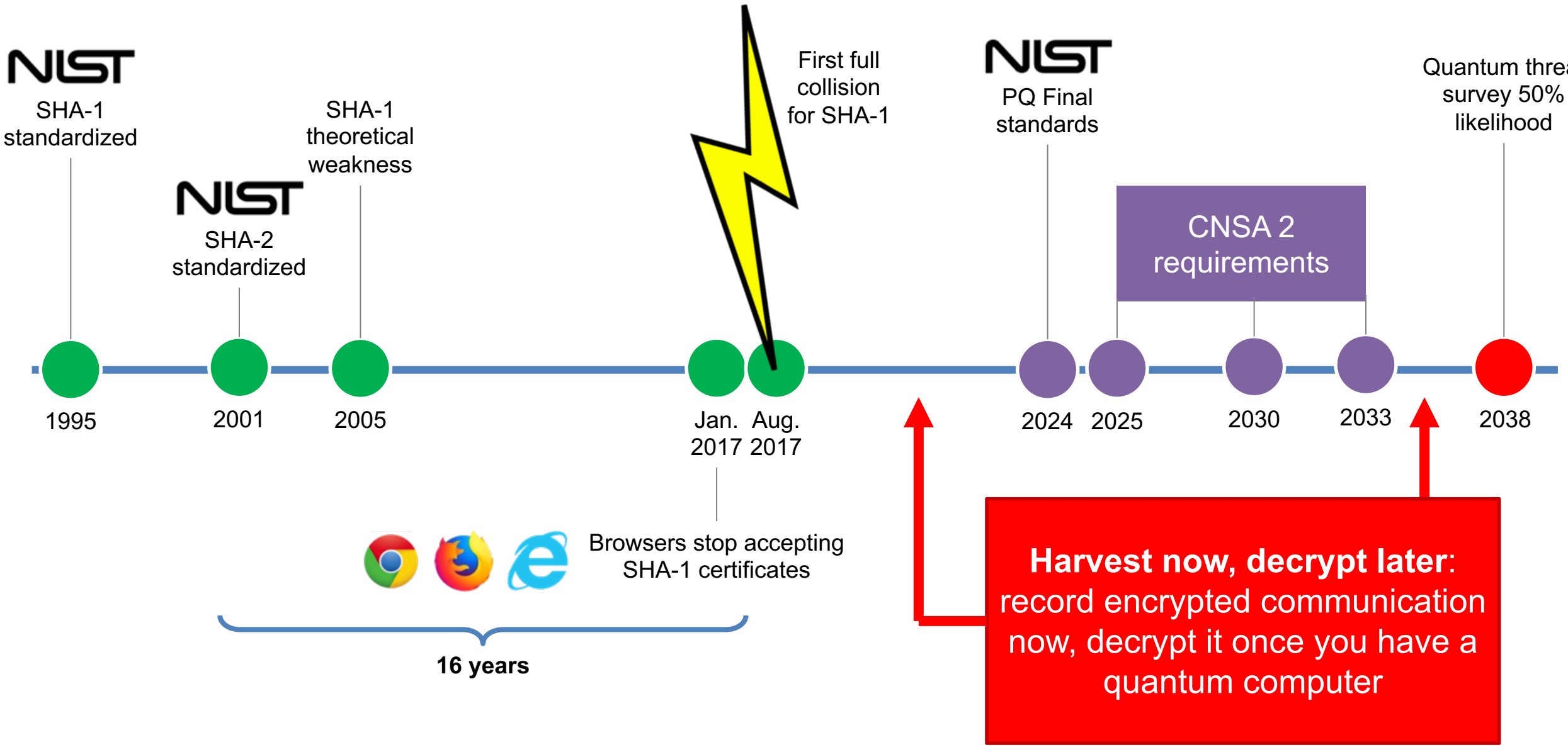
When will a cryptographically relevant quantum computer be built?

≥ 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



Primary goals for post-quantum crypto

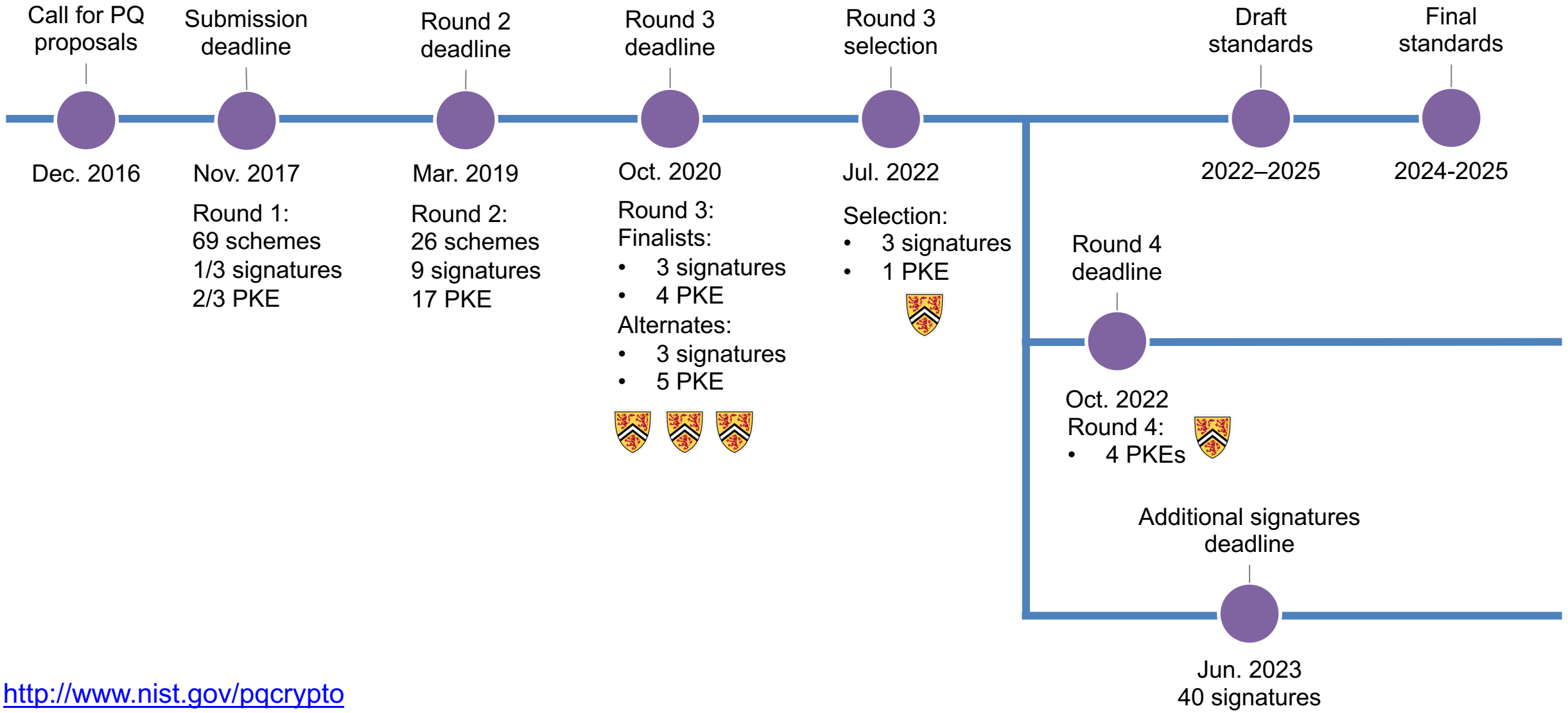
Confidentiality
in the public key setting

- **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

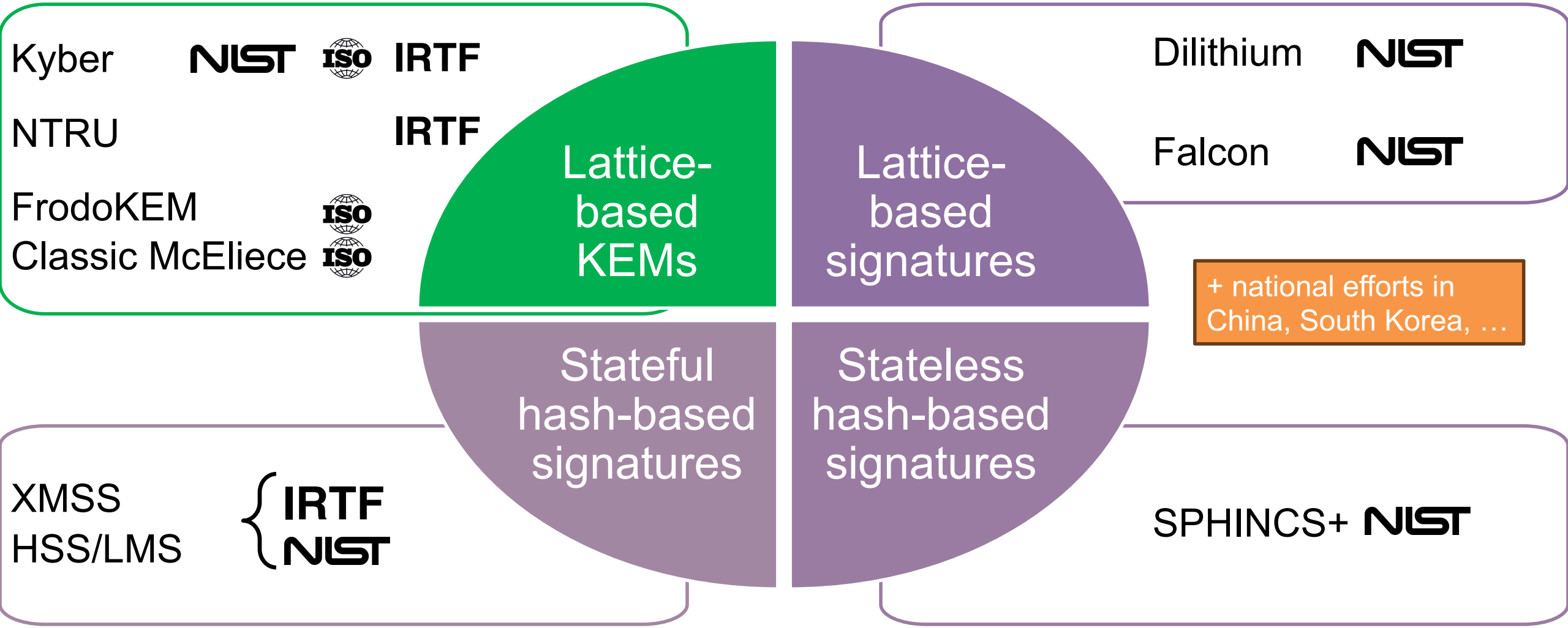
Key encapsulation mechanisms

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

Digital signatures

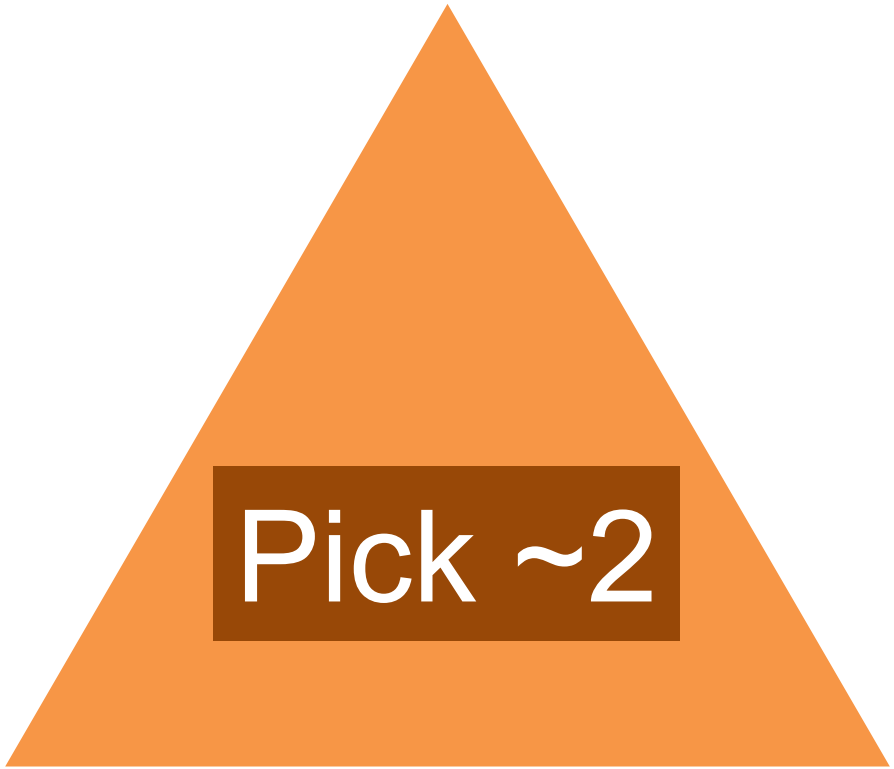
- ML-DSA (FIPS 204)
  - a.k.a. Dilithium
  - Lattice-based
- SLH-DSA (FIPS 205)
  - a.k.a. SPHINCS+
  - Stateless hash-based
- FN-DSA (draft pending)
  - a.k.a. Falcon
  - Lattice-based

PQ algorithms being standardized



Trade-offs with post-quantum crypto

Long-standing confidence in quantum-resistance



Fast computation

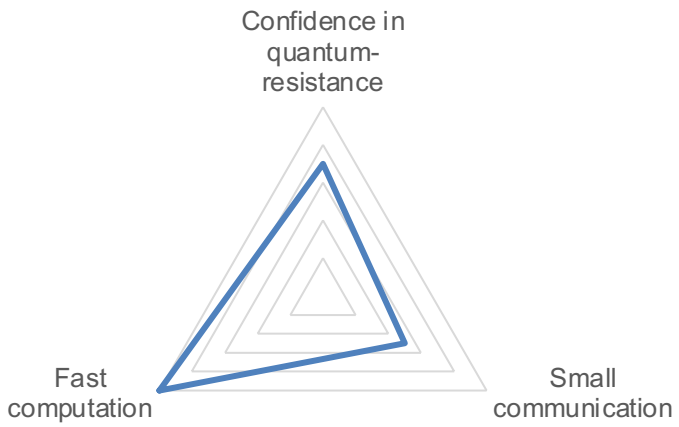
Small communication

Trade-offs with post-quantum crypto

RSA and elliptic curves

TLS handshake:
1.3 KB

Lattice-based cryptography

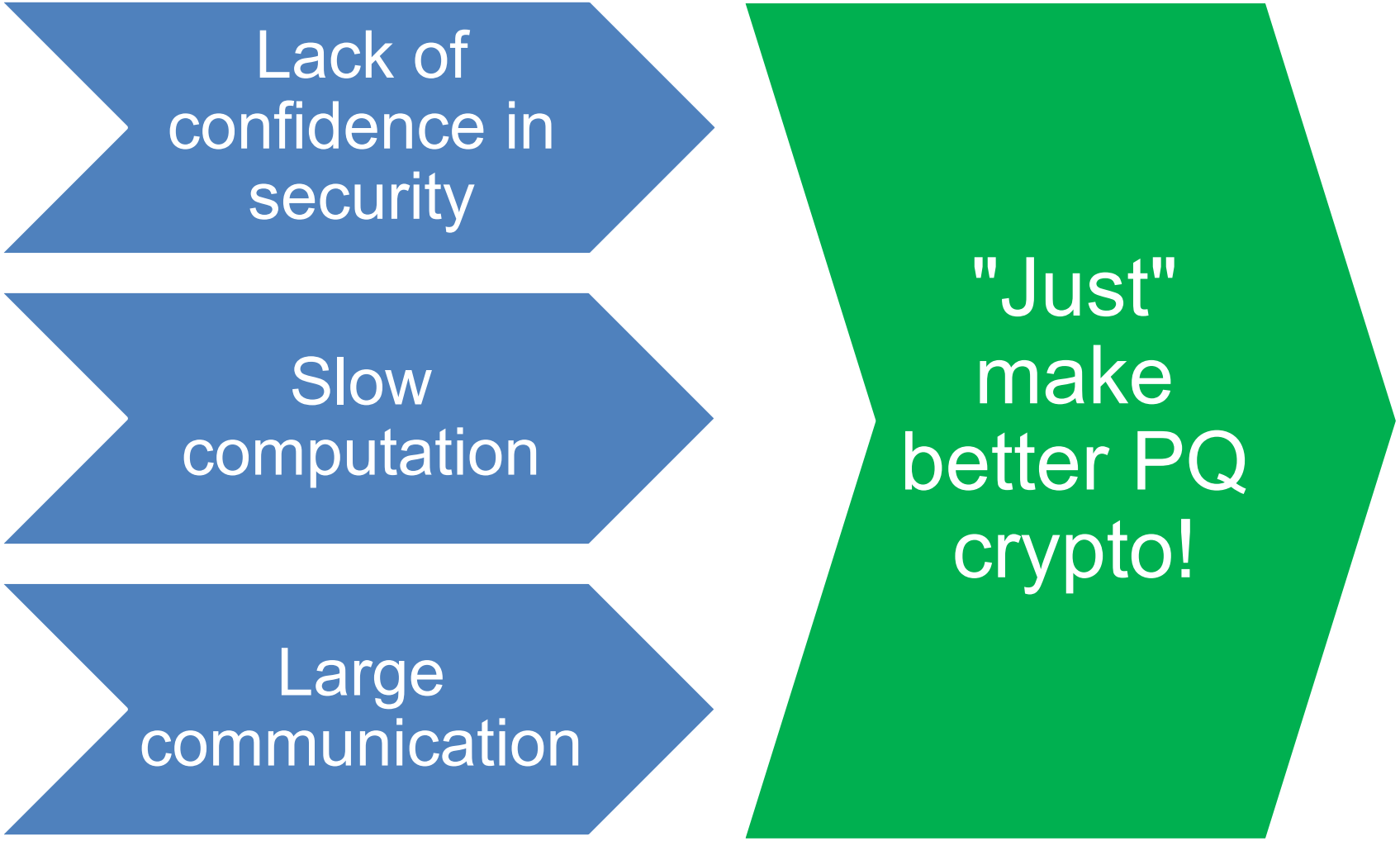


TLS handshake:
11.2 KB

Hash-based signatures

TLS handshake:
24.6 KB

Addressing the challenges of using PQ crypto

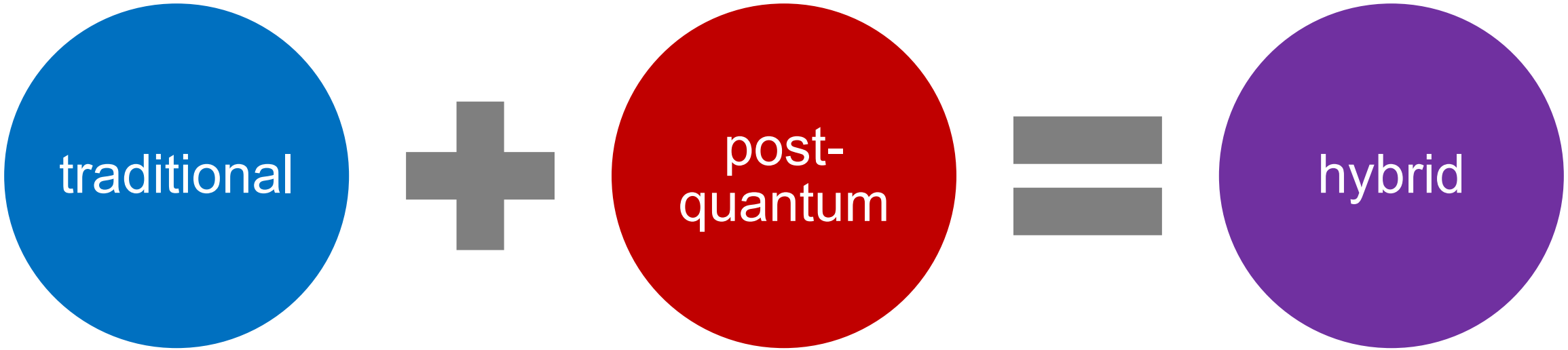


Addressing the challenges of using PQ crypto

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 not 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+

Post-quantum crypto at University of Waterloo

- UW involved in NIST standardized KEM (**Kyber** (J Schanck))
  - and a Round 4 selection **SIKE** (D Jao, A Hutchinson, G Pereira))
  - and two Round 3 candidates (**FrodoKEM** (D Stebila), **NTRU** (J Schanck))
- Isogeny-based crypto: David Jao
- Quantum cryptanalysis: Michele Mosca, Sam Jaques
- Post-quantum protocols and implementations (Open Quantum Safe project): Douglas Stebila
- + quantum key distribution, quantum computing, privacy and security, …

OPEN QUANTUM SAFE

software for the transition to quantum-resistant cryptography

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

4+8+7 things to remember from CO 487

Things to remember

- **Shor's algorithm** on a quantum computer would break all the public key encryption / digital signature / DH key exchange schemes based on factoring (RSA) or discrete logarithms (including elliptic curves).
- **New standards from NIST** under development for quantum-resistant "post-quantum" cryptography based on other mathematical assumptions, like learning with errors / lattices.
- Secure options as of 2024:
  - For key exchange / public key encryption: ML-KEM (Kyber)
  - For digital signatures: ML-DSA (Dilithium), Falcon, and SLH-DSA (SPHINCS+)