Transitioning to post-quantum cryptography

Douglas Stebila

UNIVERSITY OF WATERLOO

Funding acknowledgements:

NSERC CRSNG

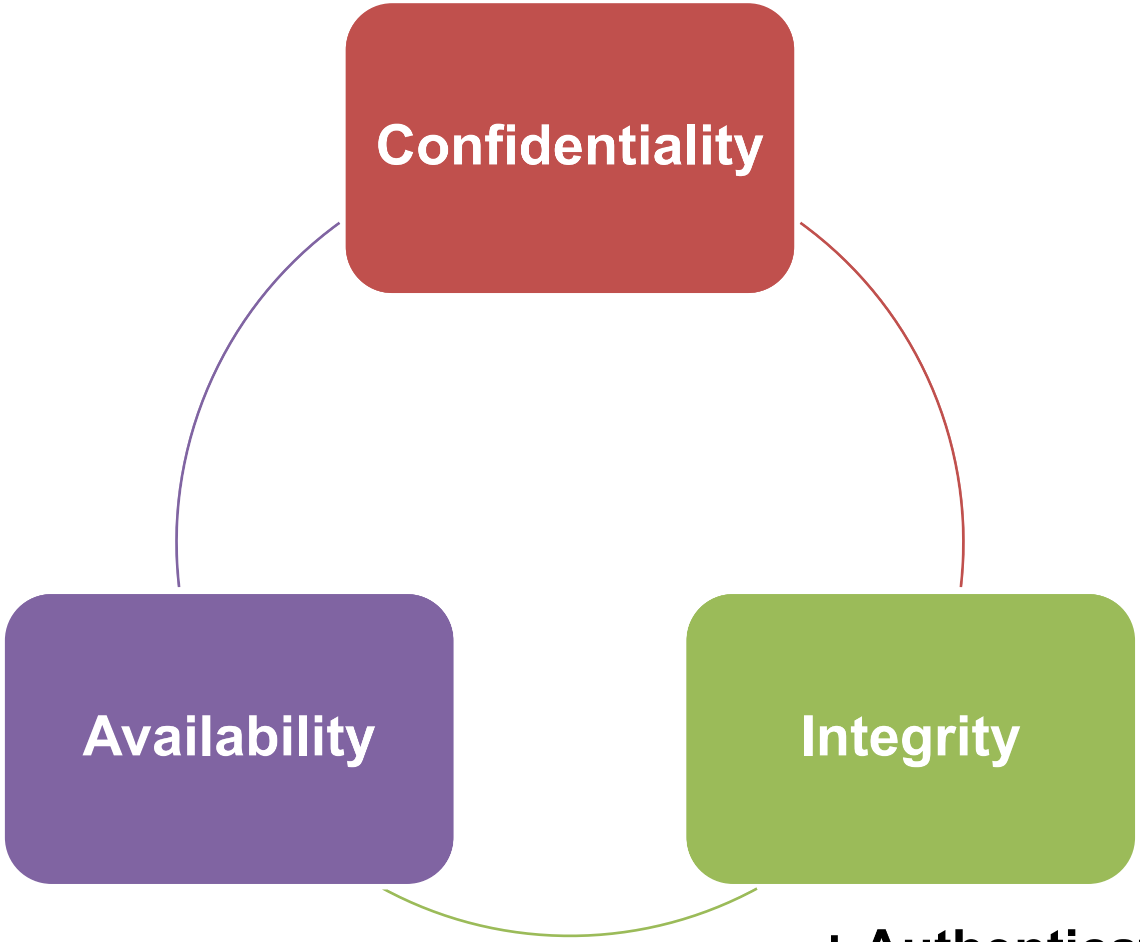
GoSec • August 29, 2018

Outline

- Background on cryptography
- The threat of quantum computing
- Overview of post-quantum cryptography
- Transitioning to post-quantum crypto

Background on cryptography

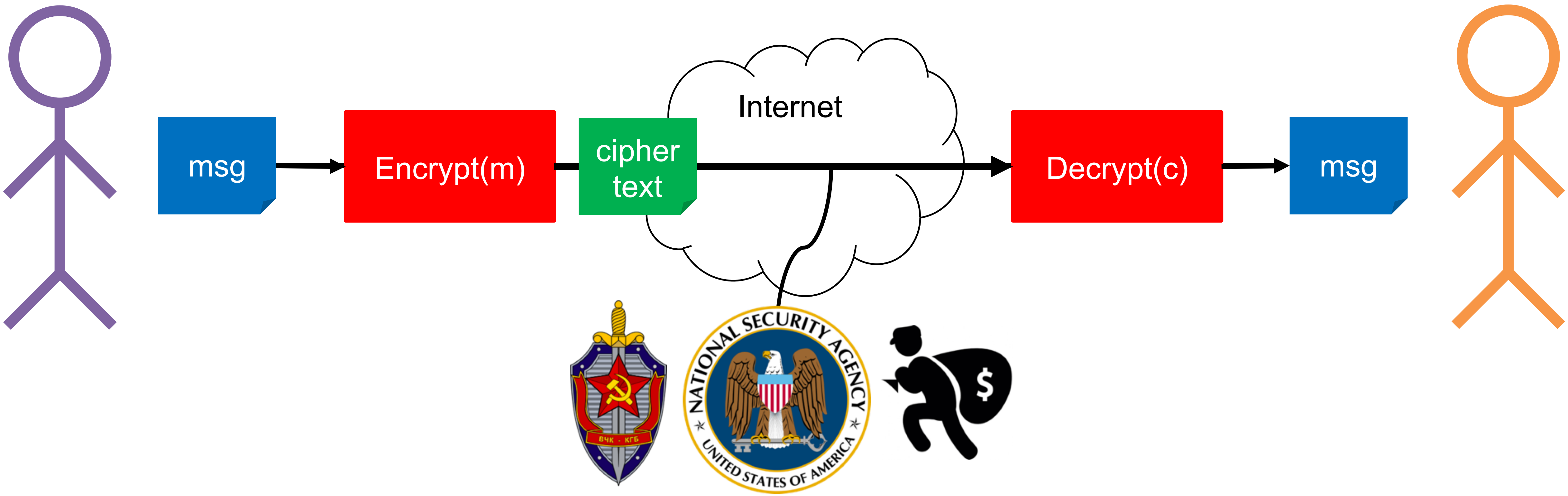
Security goals



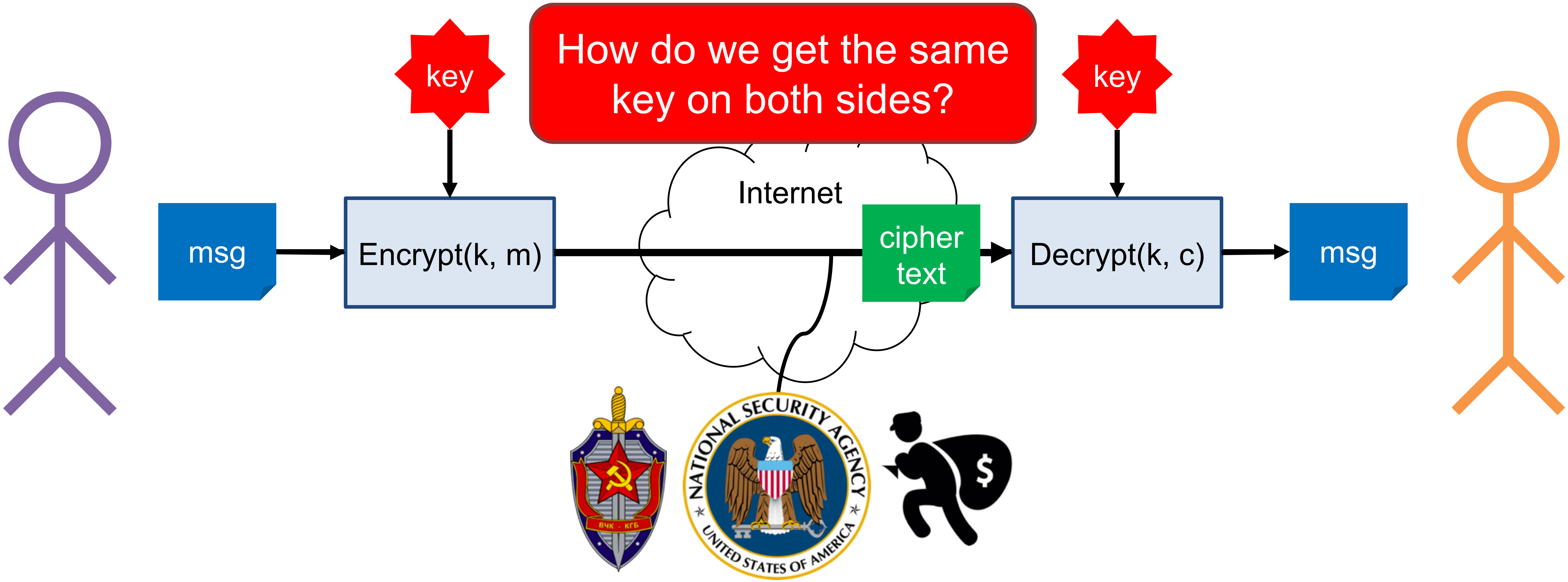
+ Authentication

- Data at rest
- Data in transit
- Data while processing

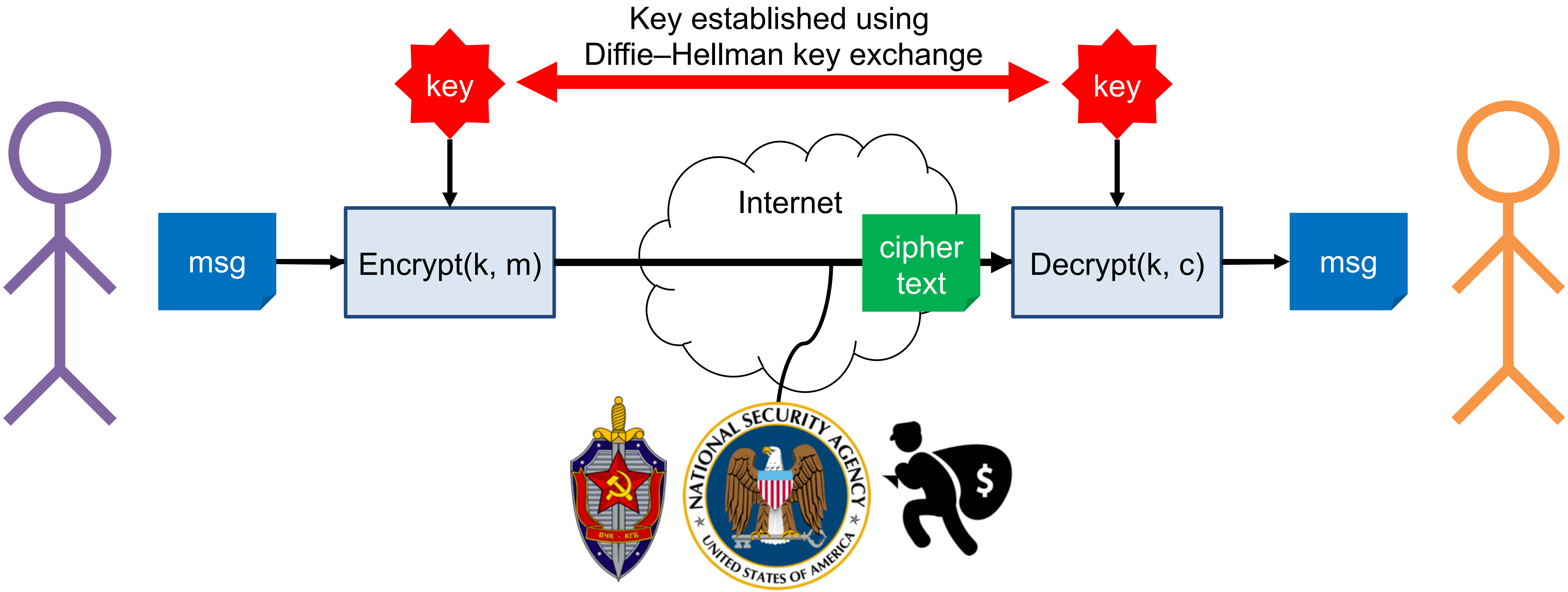
Encryption



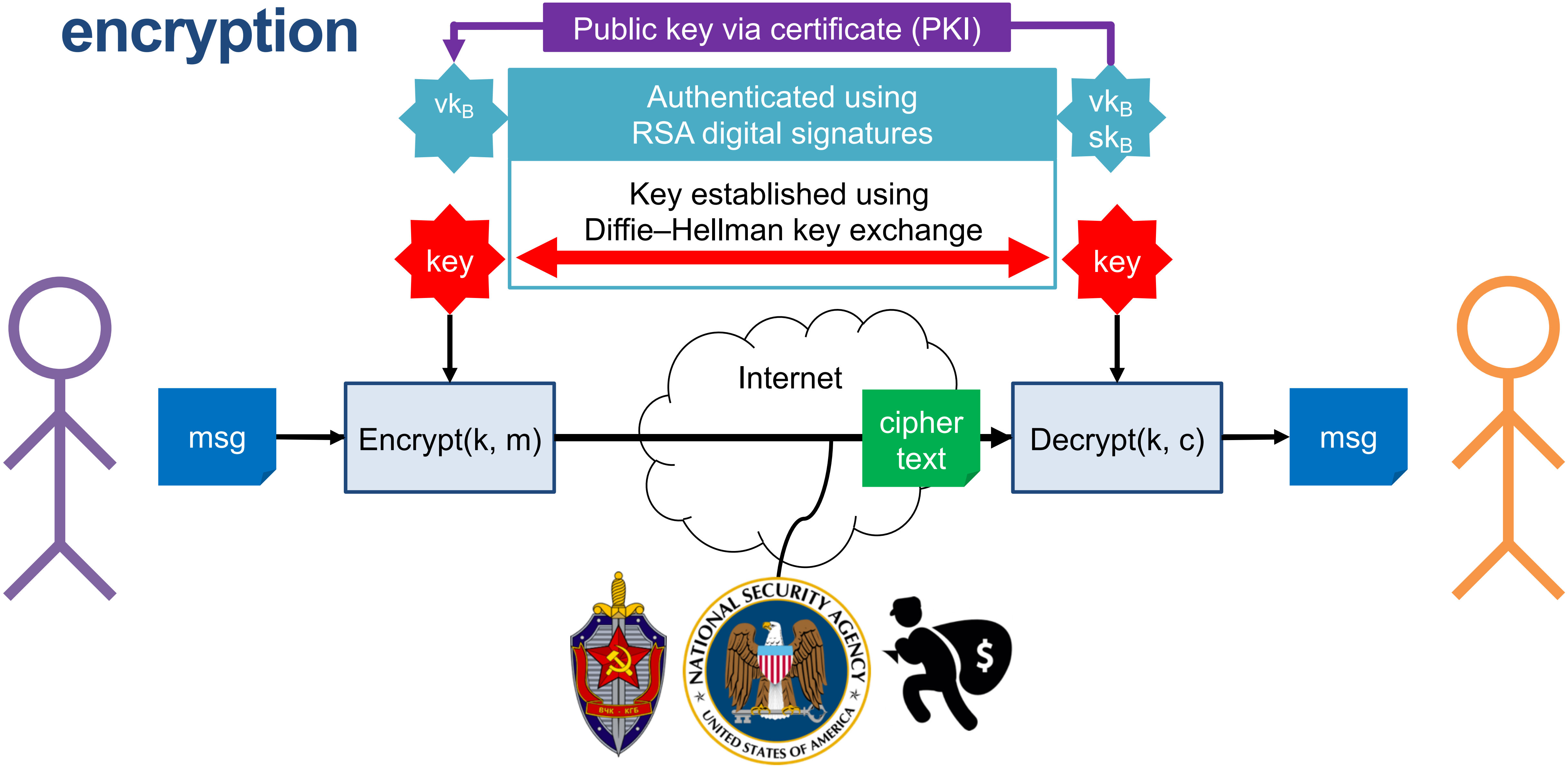
Symmetric encryption

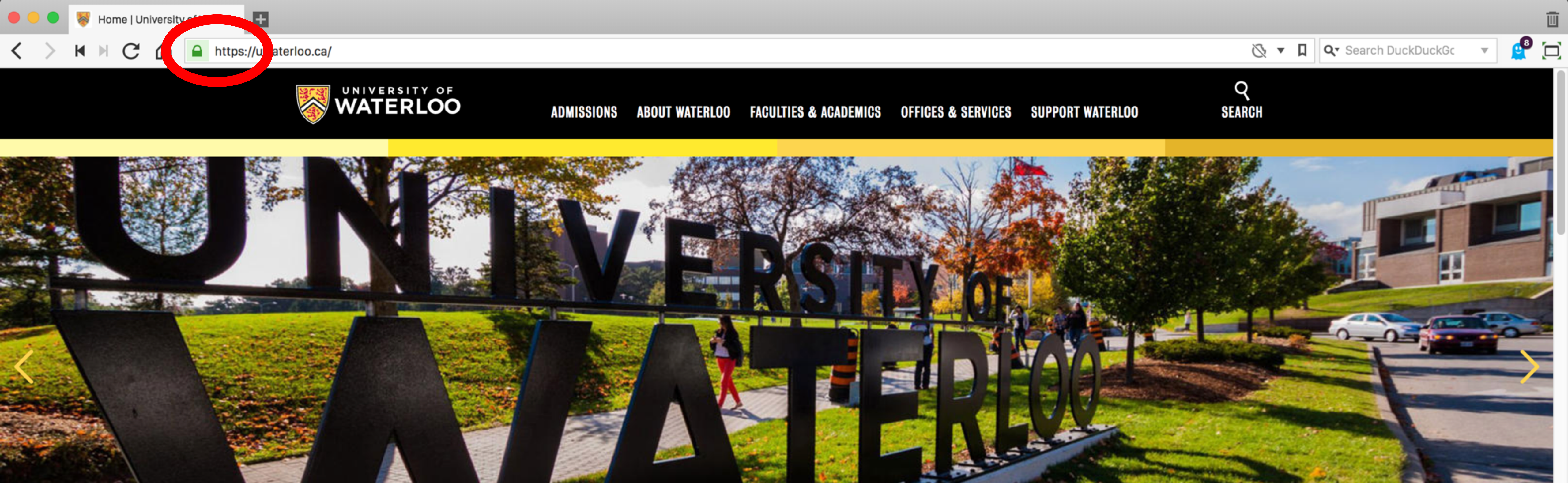


Key exchange + symmetric encryption



Authenticated key exchange + symmetric encryption

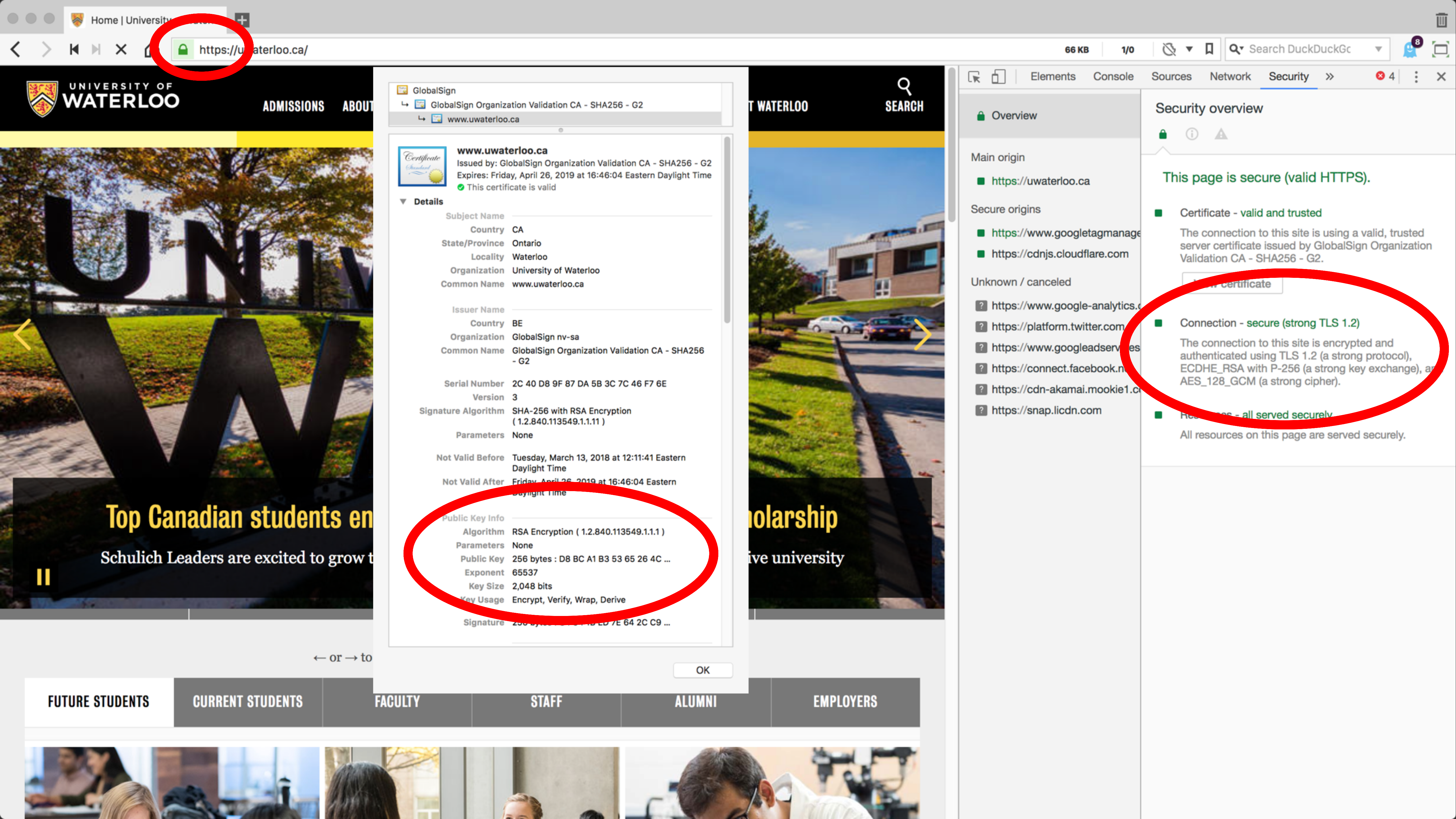




TLS (Transport Layer Security) protocol

a.k.a. SSL (Secure Sockets Layer)

- The “s” in “https”
- The **most important cryptographic protocol on the Internet** — used to secure billions of connections every day.

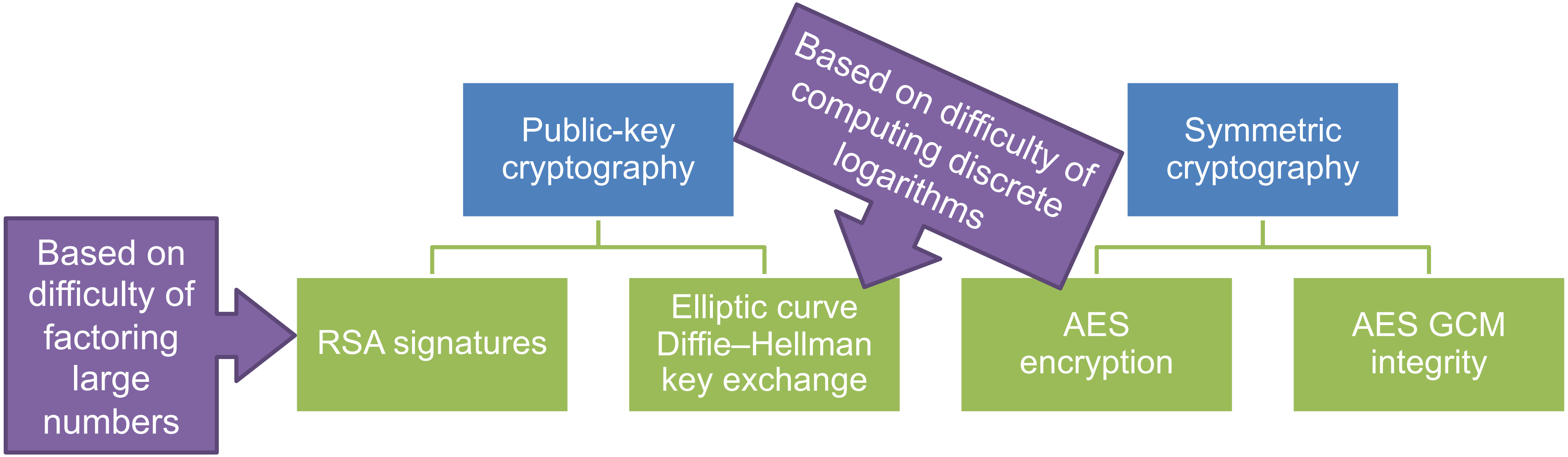


Home | University
https://uwaterloo.ca/
UNIVERSITY OF WATERLOO
ADMISSIONS
SEARCH
GlobalSign
GlobalSign Organization Validation CA - SHA256 - G2
www.uwaterloo.ca
www.uwaterloo.ca
Issued by: GlobalSign Organization Validation CA - SHA256 - G2
Expires: Friday, April 26, 2019 at 16:46:04 Eastern Daylight Time
This certificate is valid
Details
Subject Name
Country CA
State/Province Ontario
Locality Waterloo
Organization University of Waterloo
Common Name www.uwaterloo.ca
Issuer Name
Country BE
Organization GlobalSign nv-sa
Common Name GlobalSign Organization Validation CA - SHA256 - G2
Serial Number 2C 40 D8 9F 87 DA 5B 3C 7C 46 F7 6E
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters None
Not Valid Before Tuesday, March 13, 2018 at 12:11:41 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
Key Size 2,048 bits
Encrypt, Verify, Wrap, Derive
OK
Top Canadian students en
Schulich Leaders are excited to grow t
FUTURE STUDENTS
CURRENT STUDENTS
FACULTY
STAFF
ALUMNI
EMPLOYERS
Elements
Console
Sources
Network
Security
Overview
Main origin
https://uwaterloo.ca
Secure origins
https://cdnjs.cloudflare.com
Unknown / canceled
https://platform.twitter.com
https://snap.licdn.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 GlobalSign Organization Validation CA - SHA256 - G2.
Connection - secure (strong TLS 1.2)
The connection to this site is encrypted and authenticated using TLS 1.2 (a strong protocol), ECDHE_RSA with P-256 (a strong key exchange), AES_128_GCM (a strong cipher).
All resources on this page are served securely.

Cryptographic building blocks

Connection - secure (strong TLS 1.2)

The connection to this site is encrypted and authenticated using TLS 1.2 (a strong protocol), ECDHE_RSA with P-256 (a strong key exchange), and AES_128_GCM (a strong cipher).



What can go wrong

- Mathematical advances break cryptographic assumptions
- Good cryptography is used improperly in applications and protocols
- Bugs in how good cryptography is implemented in software & hardware

Quantum computing

Quantum computing

Represent and process information using **quantum mechanics**

"Classical" computers handle information as **bits:**

- 0 and 1

Quantum computers handle information as **qubits:**

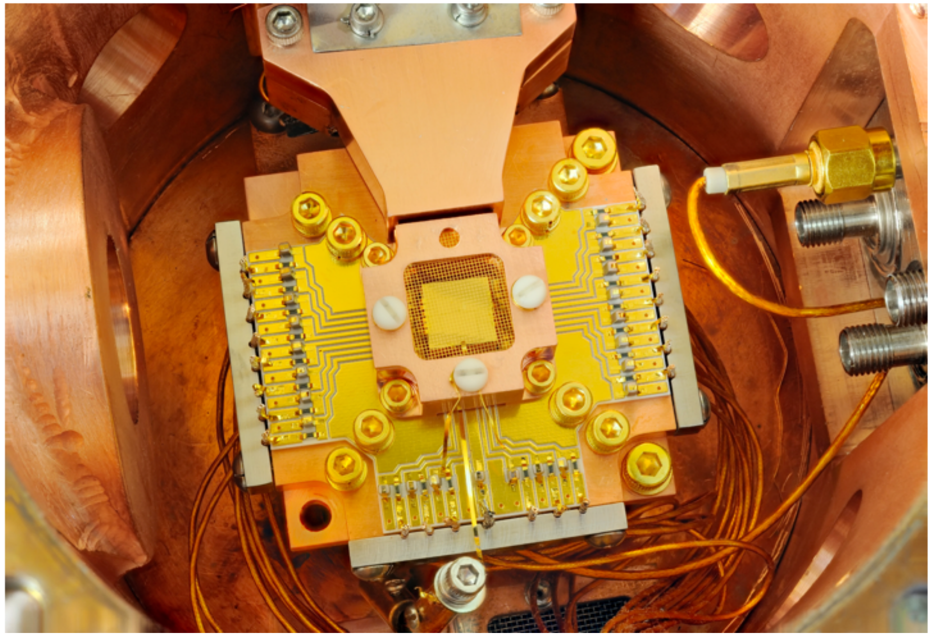
- Any "superposition" of 0 and 1

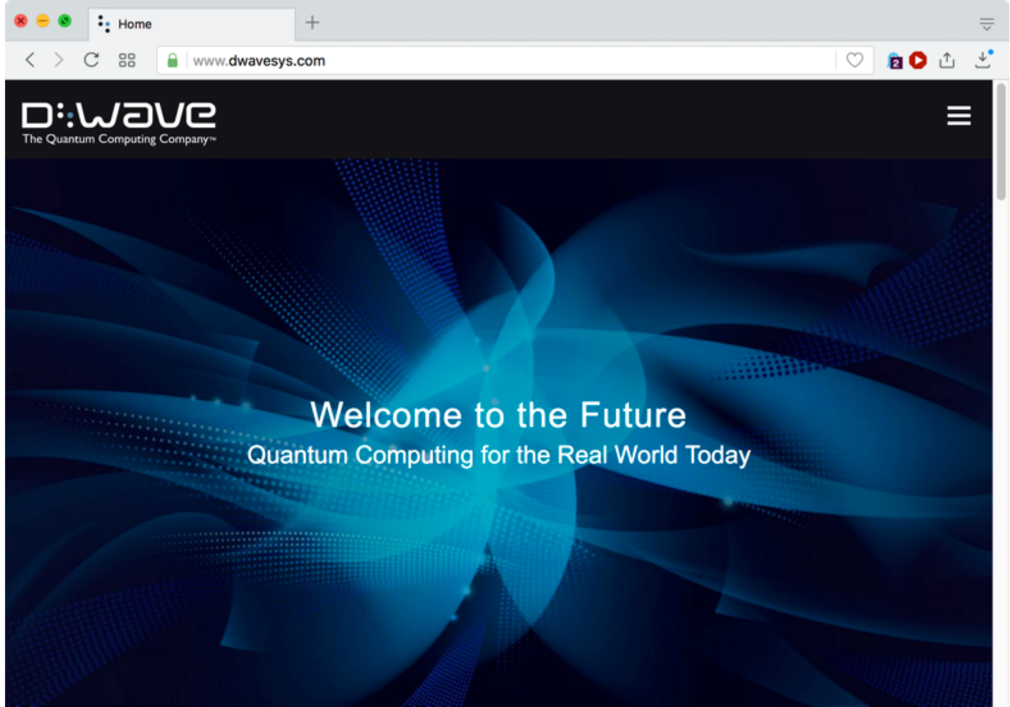
Processing information in superposition can dramatically speed some computations

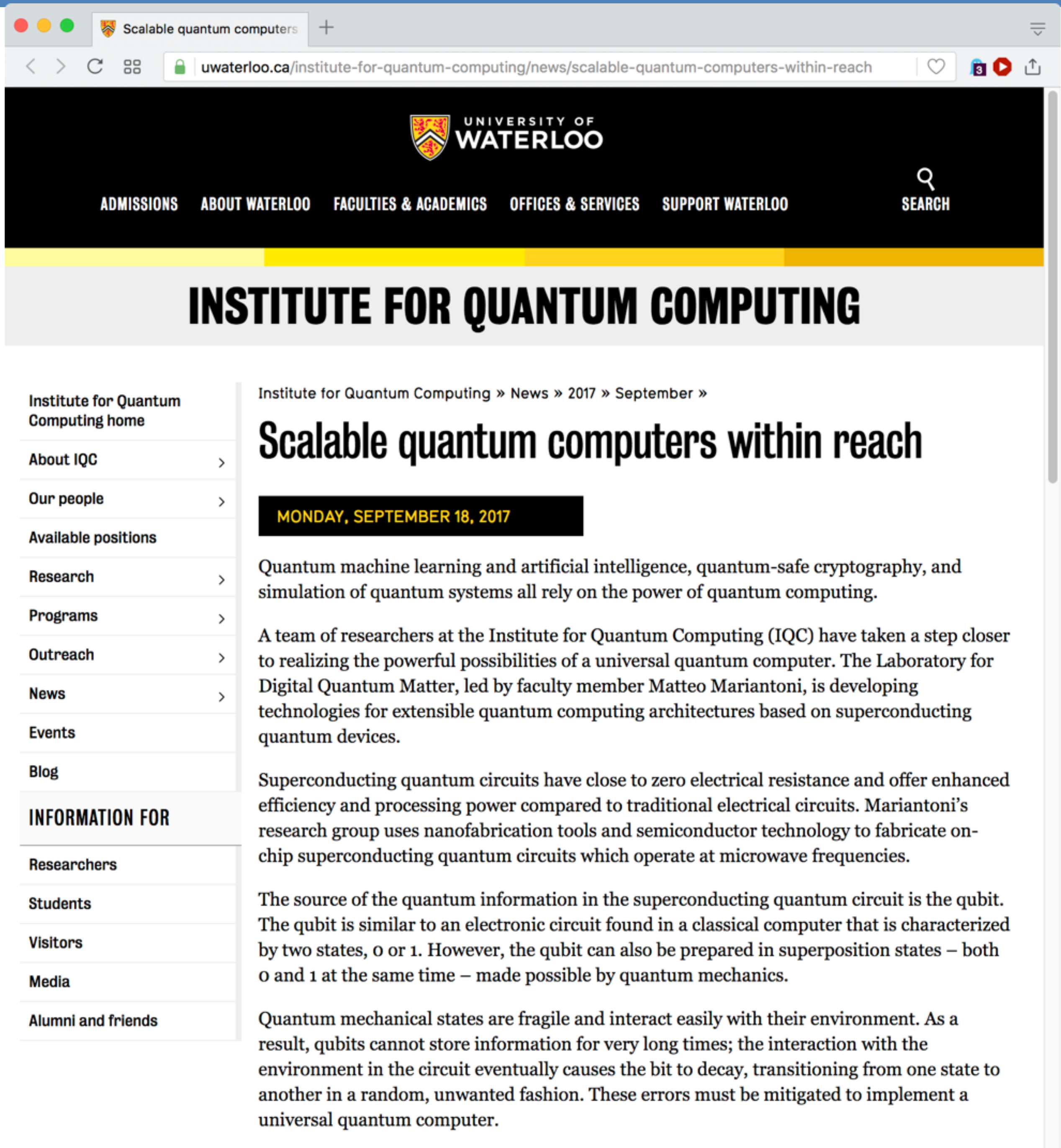
- Chemical reaction simulations
- Optimization problems
- Arithmetic

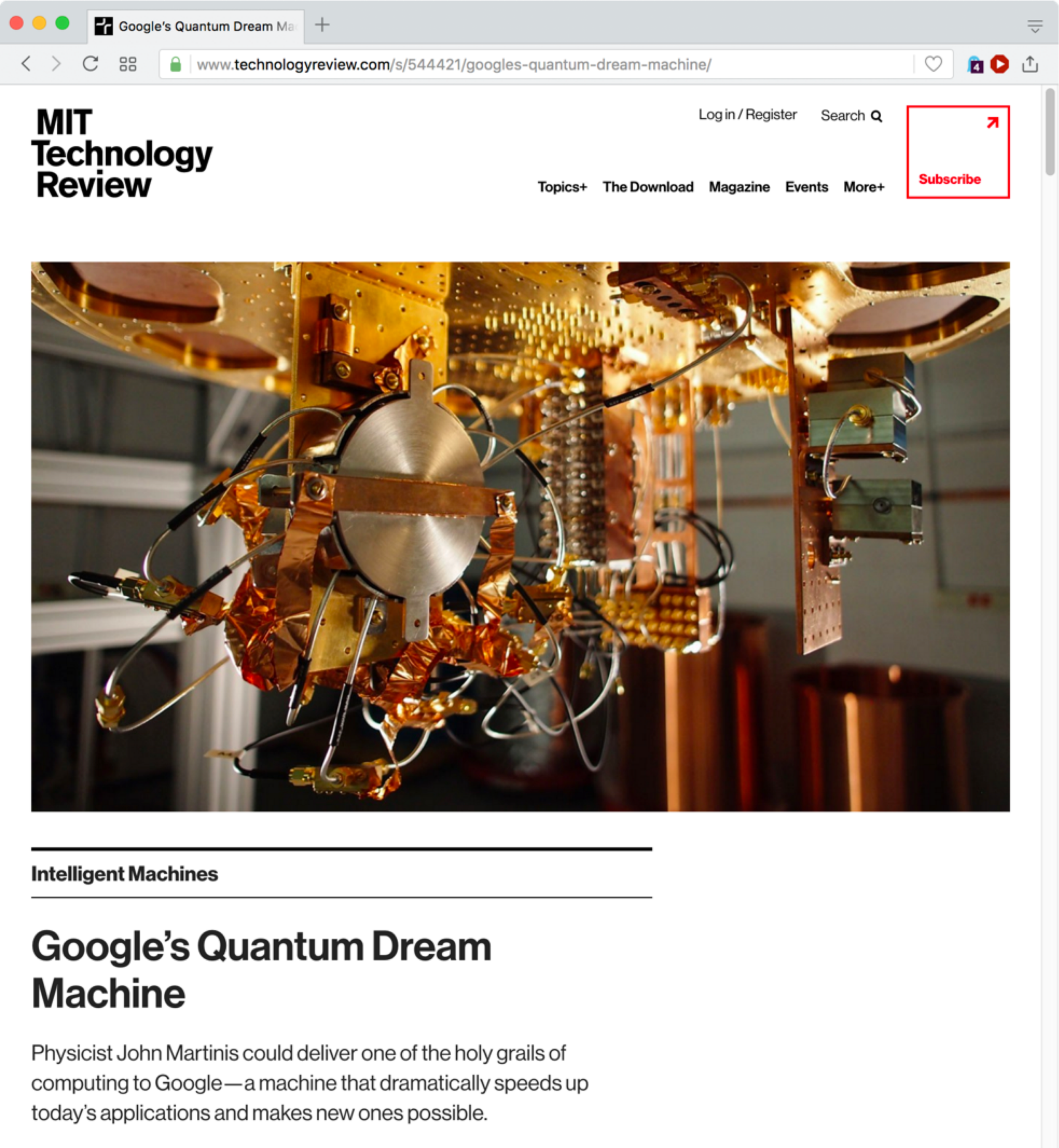
But not magic

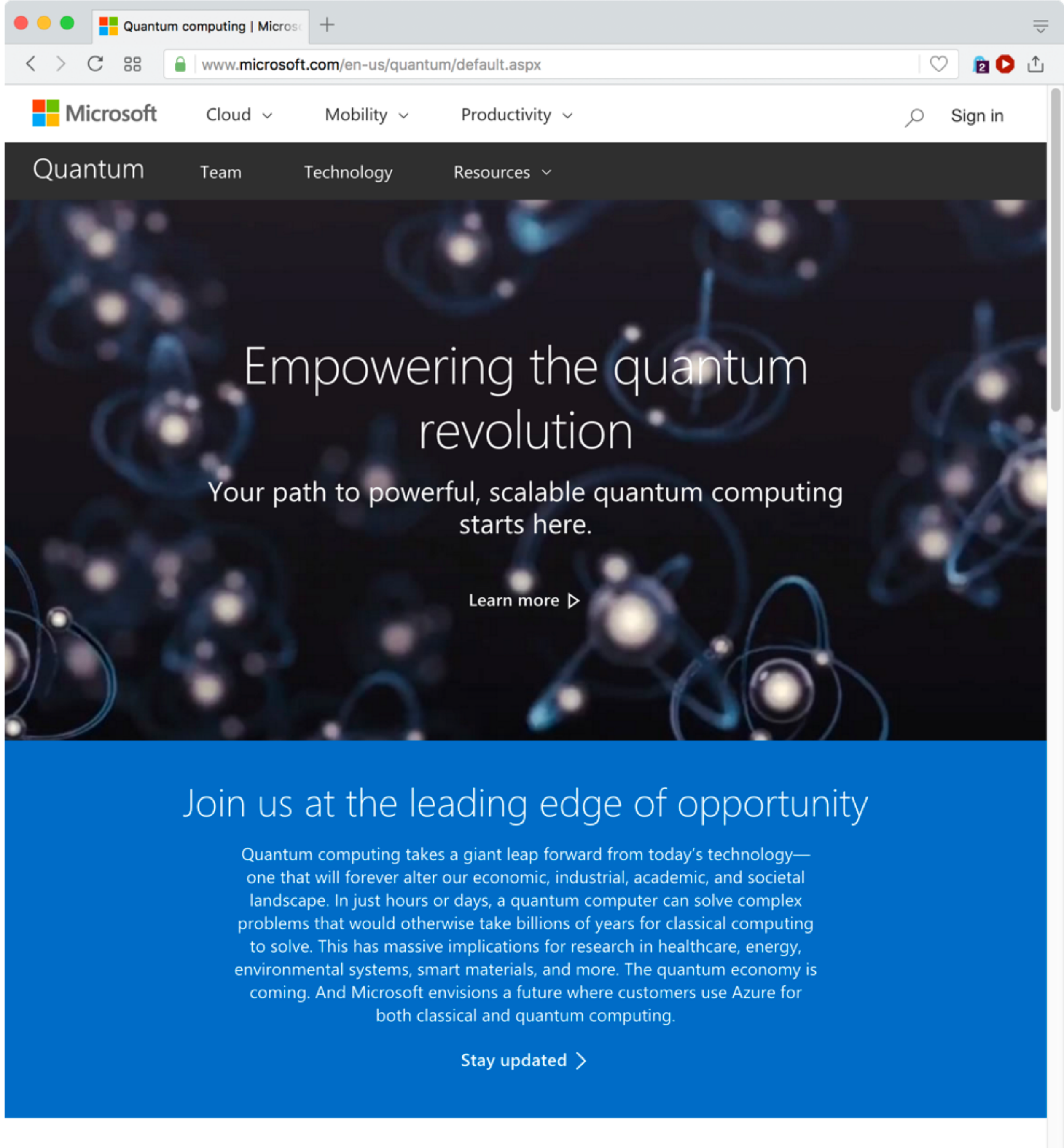
- Doesn't dramatically speed up all computations




Home
www.dwavesys.com
D:Wave
The Quantum Computing Company™
Welcome to the Future
Quantum Computing for the Real World Today

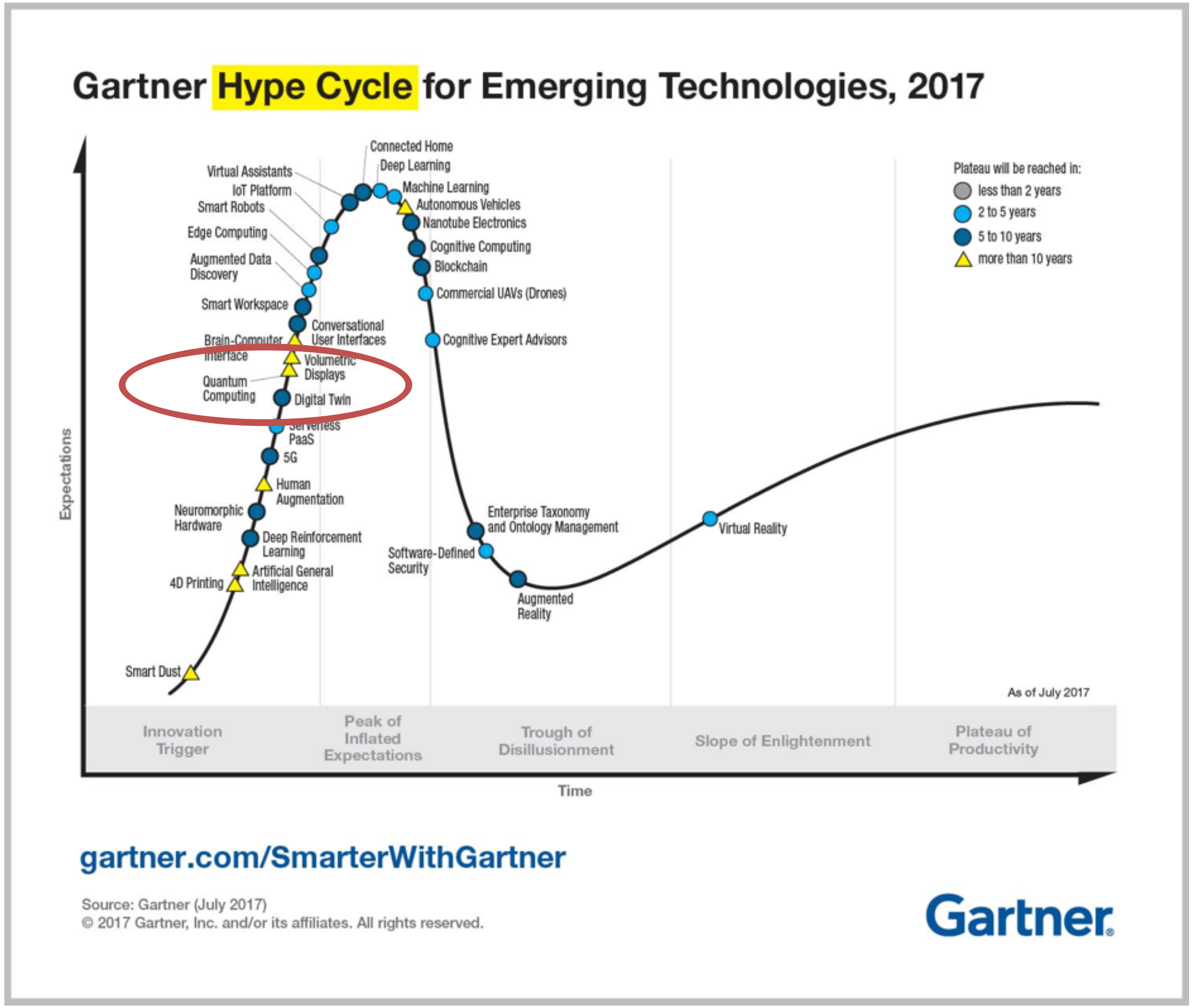

Scalable quantum computers
uwaterloo.ca/institute-for-quantum-computing/news/scalable-quantum-computers-within-reach
UNIVERSITY OF WATERLOO
ADMISSIONS
ABOUT WATERLOO
FACULTIES & ACADEMICS
OFFICES & SERVICES
SUPPORT WATERLOO
SEARCH
INSTITUTE FOR QUANTUM COMPUTING
Institute for Quantum Computing home
About IQC
Our people
Available positions
Research
Programs
Outreach
News
Events
Blog
INFORMATION FOR
Researchers
Students
Visitors
Media
Alumni and friends
Institute for Quantum Computing » News » 2017 » September »
Scalable quantum computers within reach
MONDAY, SEPTEMBER 18, 2017
Quantum machine learning and artificial intelligence, quantum-safe cryptography, and simulation of quantum systems all rely on the power of quantum computing.
A team of researchers at the Institute for Quantum Computing (IQC) have taken a step closer to realizing the powerful possibilities of a universal quantum computer. The Laboratory for Digital Quantum Matter, led by faculty member Matteo Mariantoni, is developing technologies for extensible quantum computing architectures based on superconducting quantum devices.
Superconducting quantum circuits have close to zero electrical resistance and offer enhanced efficiency and processing power compared to traditional electrical circuits. Mariantoni's research group uses nanofabrication tools and semiconductor technology to fabricate on-chip superconducting quantum circuits which operate at microwave frequencies.
The source of the quantum information in the superconducting quantum circuit is the qubit. The qubit is similar to an electronic circuit found in a classical computer that is characterized by two states, 0 or 1. However, the qubit can also be prepared in superposition states – both 0 and 1 at the same time – made possible by quantum mechanics.
Quantum mechanical states are fragile and interact easily with their environment. As a result, qubits cannot store information for very long times; the interaction with the environment in the circuit eventually causes the bit to decay, transitioning from one state to another in a random, unwanted fashion. These errors must be mitigated to implement a universal quantum computer.


Google's Quantum Dream Ma
www.technologyreview.com/s/544421/googles-quantum-dream-machine/
MIT Technology Review
Log in / Register
Search
Subscribe
Topics+ The Download Magazine Events More+
Intelligent Machines
Google's Quantum Dream Machine
Physicist John Martinis could deliver one of the holy grails of computing to Google—a machine that dramatically speeds up today's applications and makes new ones possible.


Quantum computing | Micros
www.microsoft.com/en-us/quantum/default.aspx
Microsoft
Cloud
Mobility
Productivity
Sign in
Quantum
Team
Technology
Resources
Empowering the quantum revolution
Your path to powerful, scalable quantum computing starts here.
Learn more
Join us at the leading edge of opportunity
Quantum computing takes a giant leap forward from today's technology—one that will forever alter our economic, industrial, academic, and societal landscape. In just hours or days, a quantum computer can solve complex problems that would otherwise take billions of years for classical computing to solve. This has massive implications for research in healthcare, energy, environmental systems, smart materials, and more. The quantum economy is coming. And Microsoft envisions a future where customers use Azure for both classical and quantum computing.
Stay updated


The Economist
Ryancare attacked from left and right
IS up against the wall in Mosul
Taiwan and the one-China fiction
Is there a bubble in the markets?
Quantum leaps
A mind-bending technology goes mainstream

March 2017


Gartner Hype Cycle for Emerging Technologies, 2017
Connected Home
Deep Learning
Machine Learning
Autonomous Vehicles
Nanotube Electronics
Cognitive Computing
Blockchain
Commercial UAVs (Drones)
Cognitive Expert Advisors
Virtual Assistants
IoT Platform
Smart Robots
Edge Computing
Augmented Data Discovery
Smart Workspace
Conversational User Interfaces
Brain-Computer Interface
Volumetric Displays
Quantum Computing
Digital Twin
PaaS
5G
Human Augmentation
Neuromorphic Hardware
Deep Reinforcement Learning
Artificial General Intelligence
4D Printing
Smart Dust
Software-Defined Security
Enterprise Taxonomy and Ontology Management
Augmented Reality
Virtual Reality
Plateau will be reached in:
less than 2 years
2 to 5 years
5 to 10 years
more than 10 years
As of July 2017
Expectations
Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
Time
gartner.com/SmarterWithGartner
Source: Gartner (July 2017)
© 2017 Gartner, Inc. and/or its affiliates. All rights reserved.
Gartner

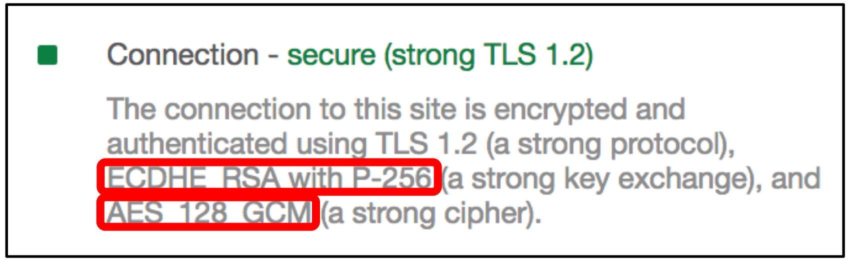
Quantum algorithms

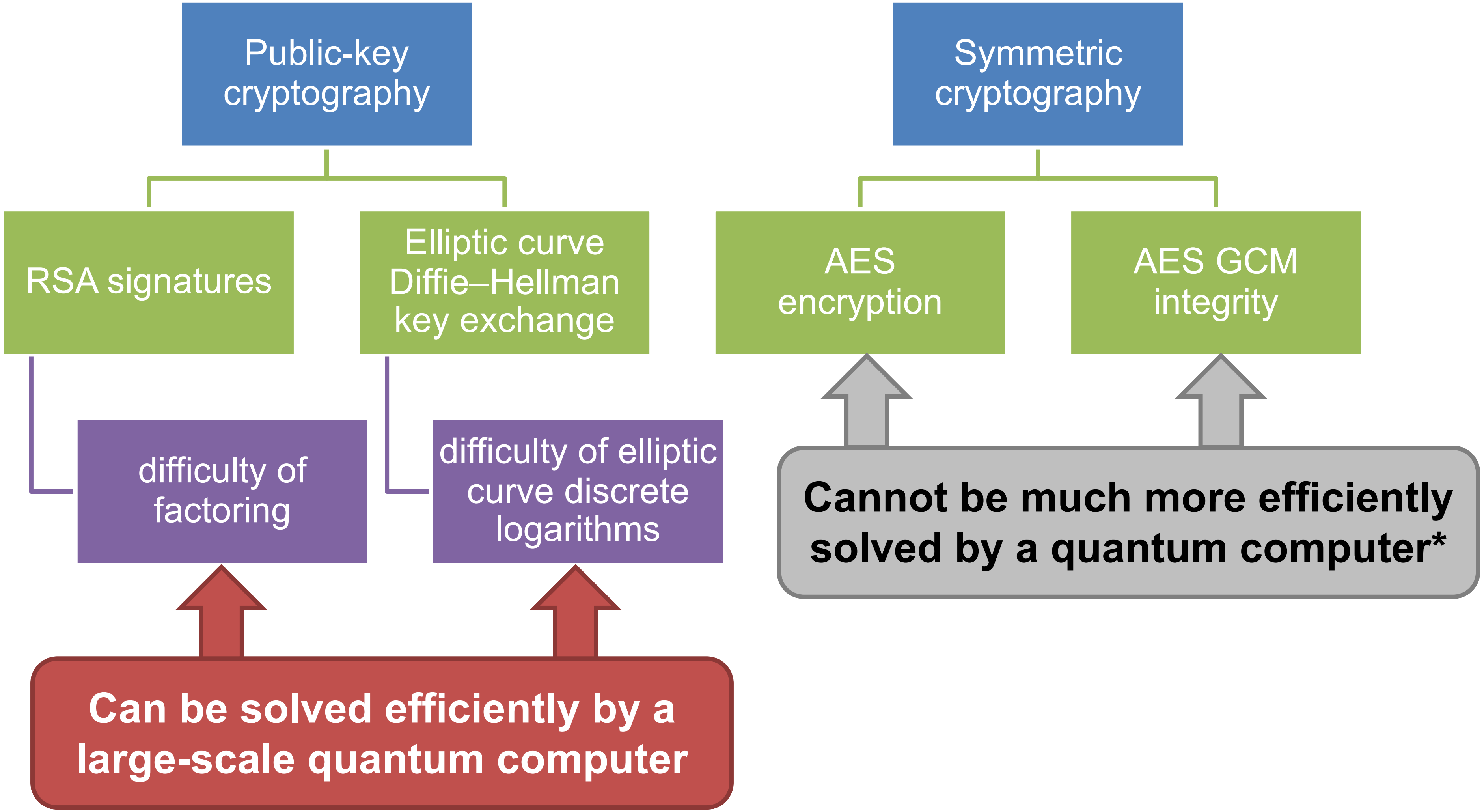
- Quantum simulation
  - Feynmann's original idea: simulate many-particle quantum systems
    - E.g. chemical reactions, topological quantum field theories
- Quantum annealing
  - Find ground state of a system
- Grover's search algorithm
  - Partial speedup of search of unstructured database

Quantum algorithms

- Quantum Fourier transform (QFT):
  - Apply Fourier transform within superposition in exponentially fewer gates than classical discrete Fourier transform
- Quantum phase estimation:
  - Use QFT to estimate eigenvalues of a unitary operator
- Shor's algorithm:
  - Use QFT to solve factor large numbers and compute discrete logarithms

Cryptographic building blocks





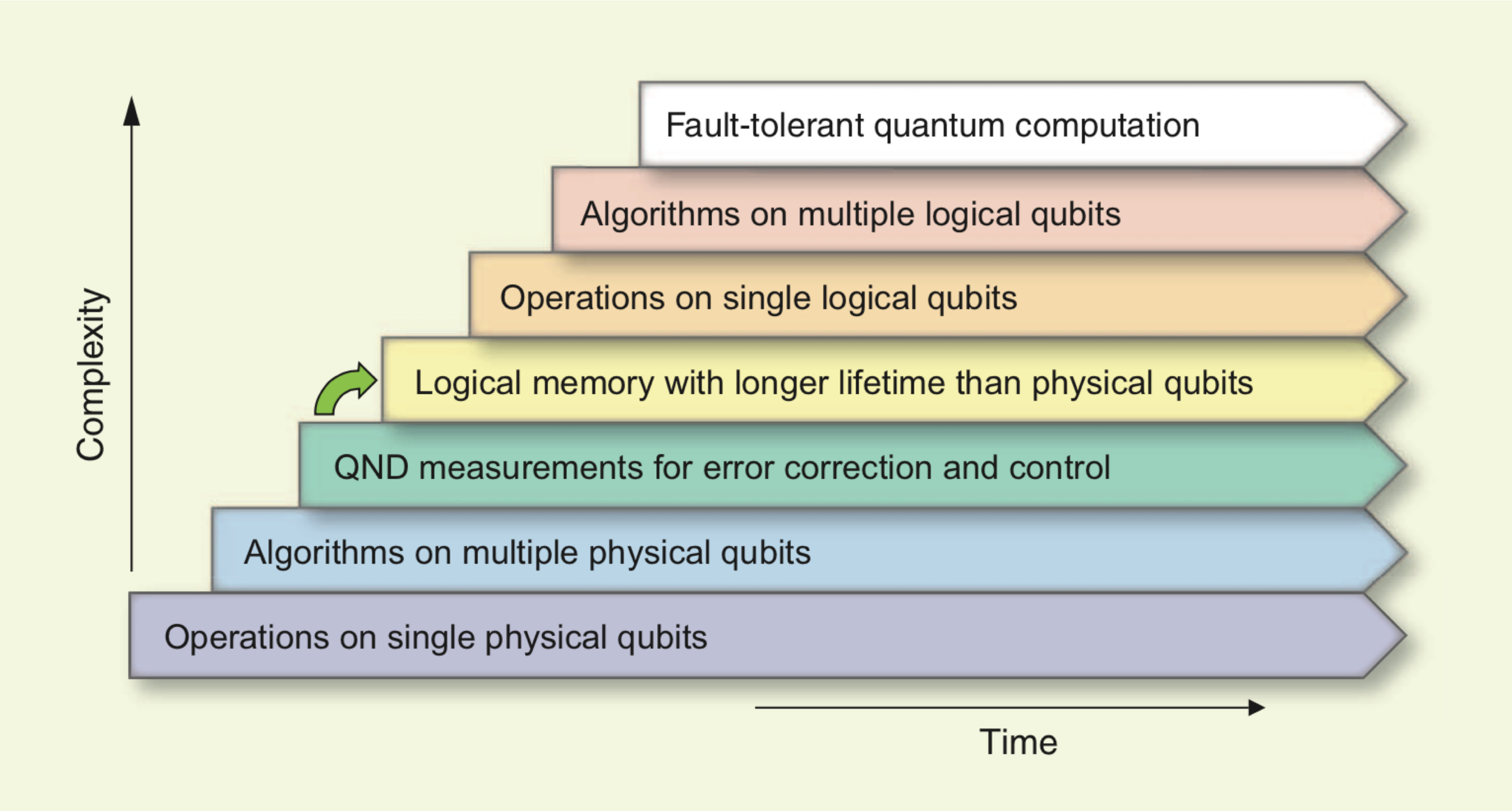
Quantum threat to information security

Large-scale general-purpose quantum computers could break some encryption schemes

Need to migrate encryption to quantum-resistant algorithms

When should you start the process?

When will a large-scale quantum computer be built?

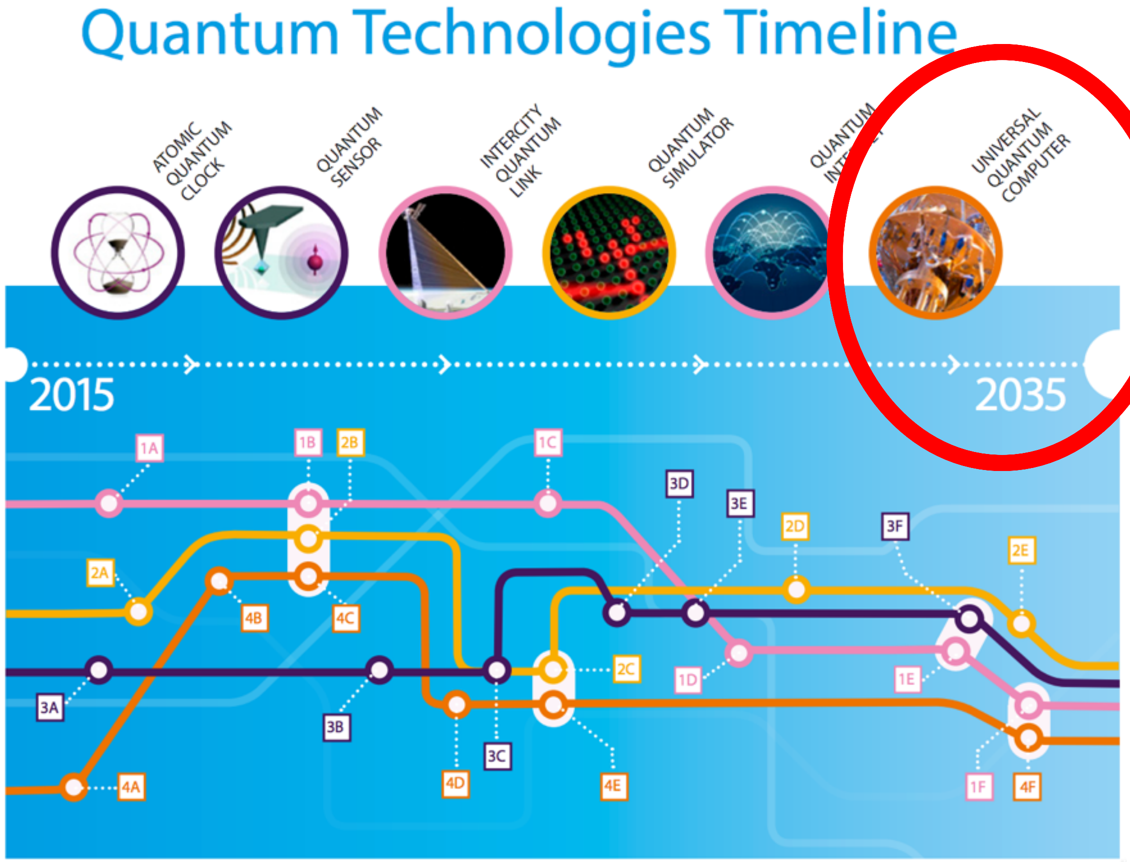


Devoret, Schoelkopf. *Science* 339:1169–1174, March 2013.

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

Post-quantum crypto

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

Code-based

Multivariate quadratic

Lattice-based

Elliptic curve isogenies

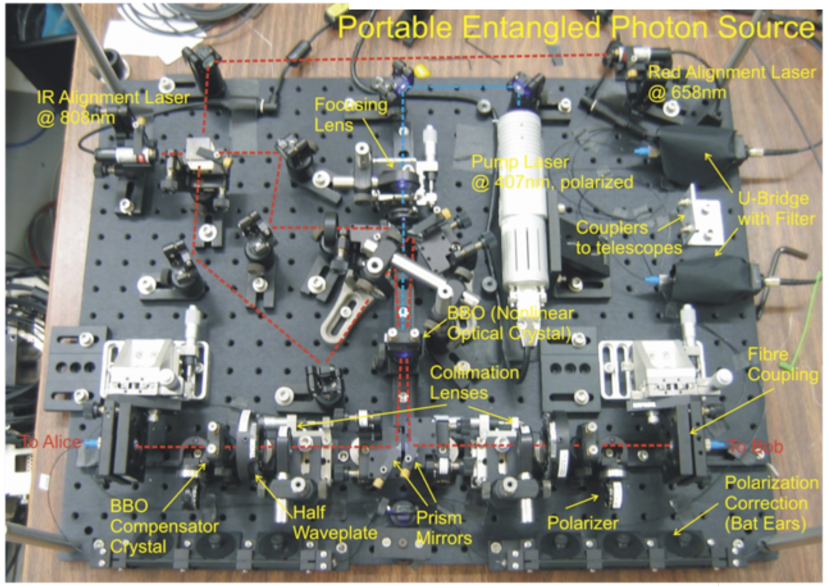
Quantum key distribution

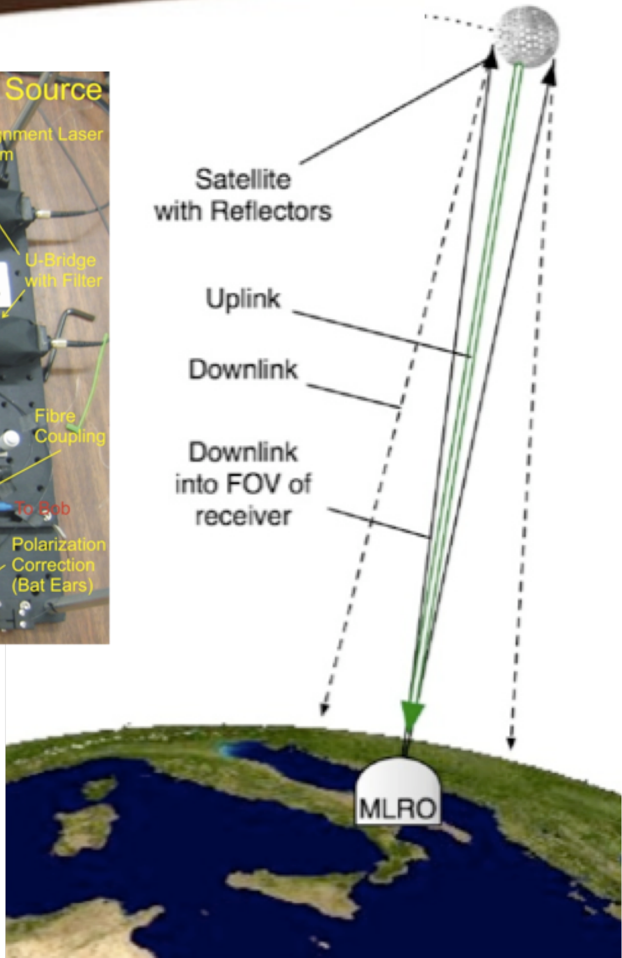
Uses quantum mechanics to protect information

Doesn't require a full quantum computer

But does require new communications infrastructure and hardware

=> Not the subject of this talk

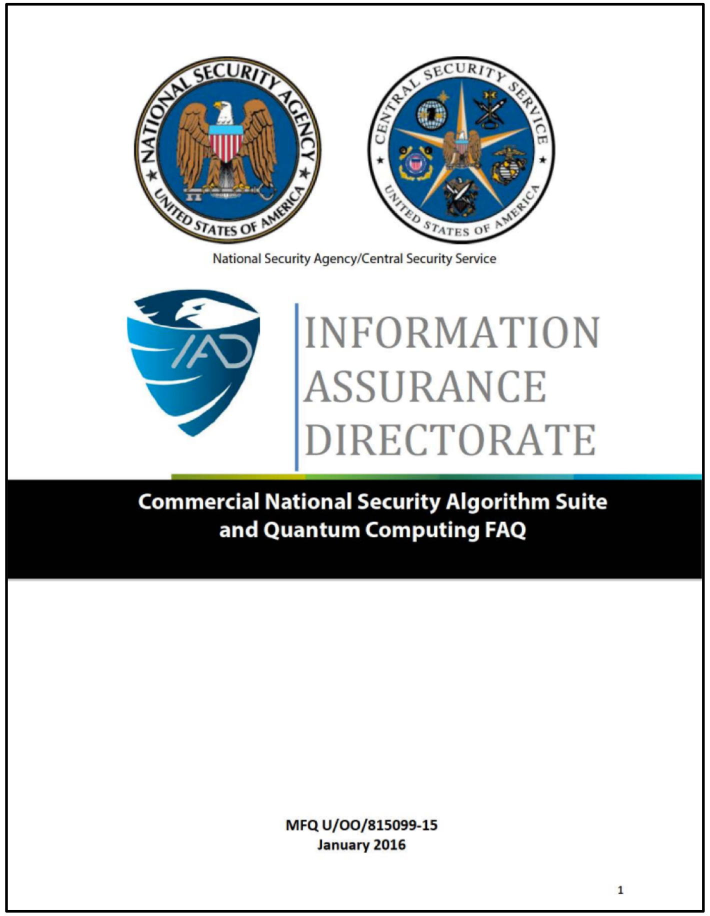




Lots of questions about post-quantum crypto

- Design better post-quantum key exchange and signature schemes
- Improve classical and quantum attacks
- Pick parameter sizes
- Develop fast, secure implementations
- Integrate them into the existing infrastructure

Standardizing post-quantum cryptography



Aug. 2015 (Jan. 2016)

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

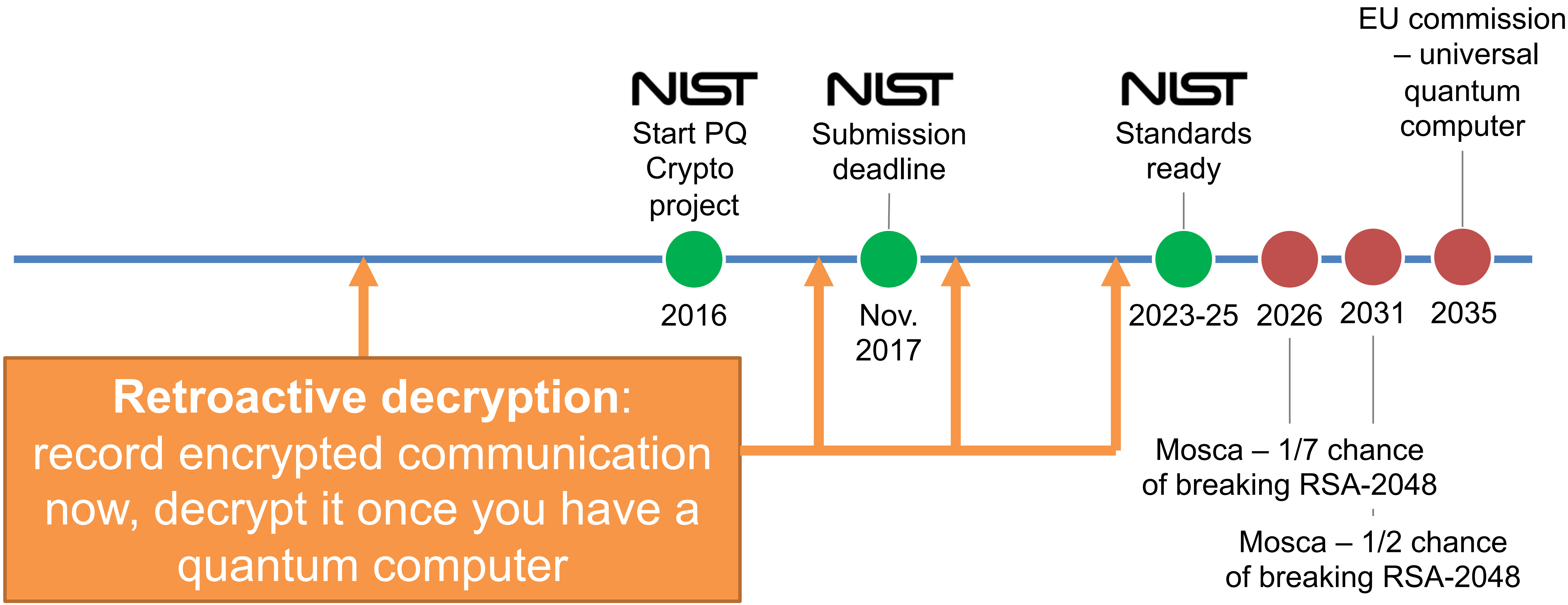
– NSA Information Assurance Directorate, Aug. 2015

NIST Post-quantum Crypto Project timeline

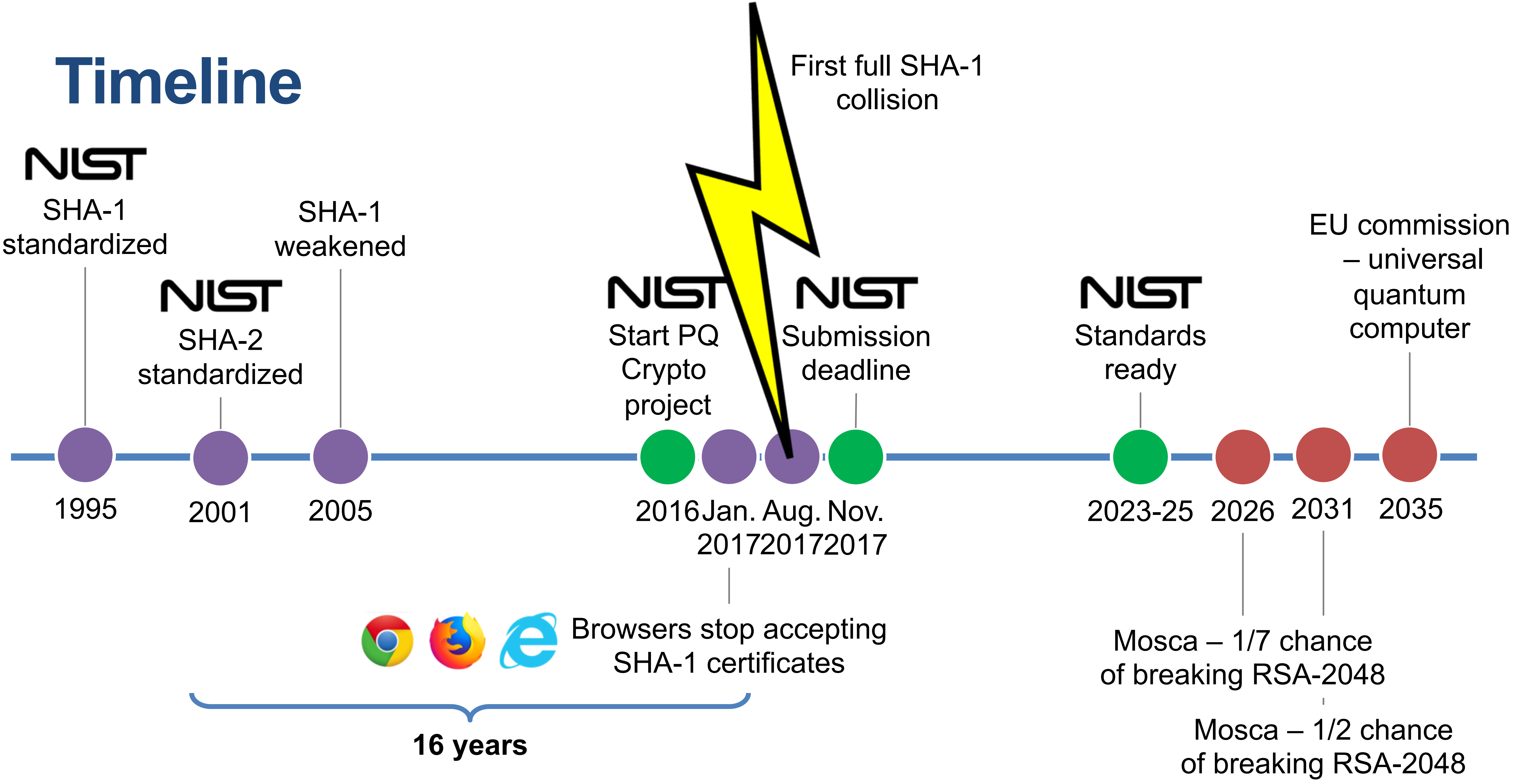
http://www.nist.gov/pqcrypto

December 2016	Formal call for proposals
November 2017	Deadline for submissions 69 submissions 1/3 signatures, 2/3 KEM/PKE
3–5 years	**Analysis phase**
2 years later (2023–2025)	Draft standards ready

Timeline


NIST
Start PQ Crypto project
2016
NIST
Submission deadline
Nov. 2017
NIST
Standards ready
2023-25
2026
Mosca – 1/7 chance of breaking RSA-2048
2031
Mosca – 1/2 chance of breaking RSA-2048
EU commission – universal quantum computer
2035
Retroactive decryption:
record encrypted communication now, decrypt it once you have a quantum computer

Timeline

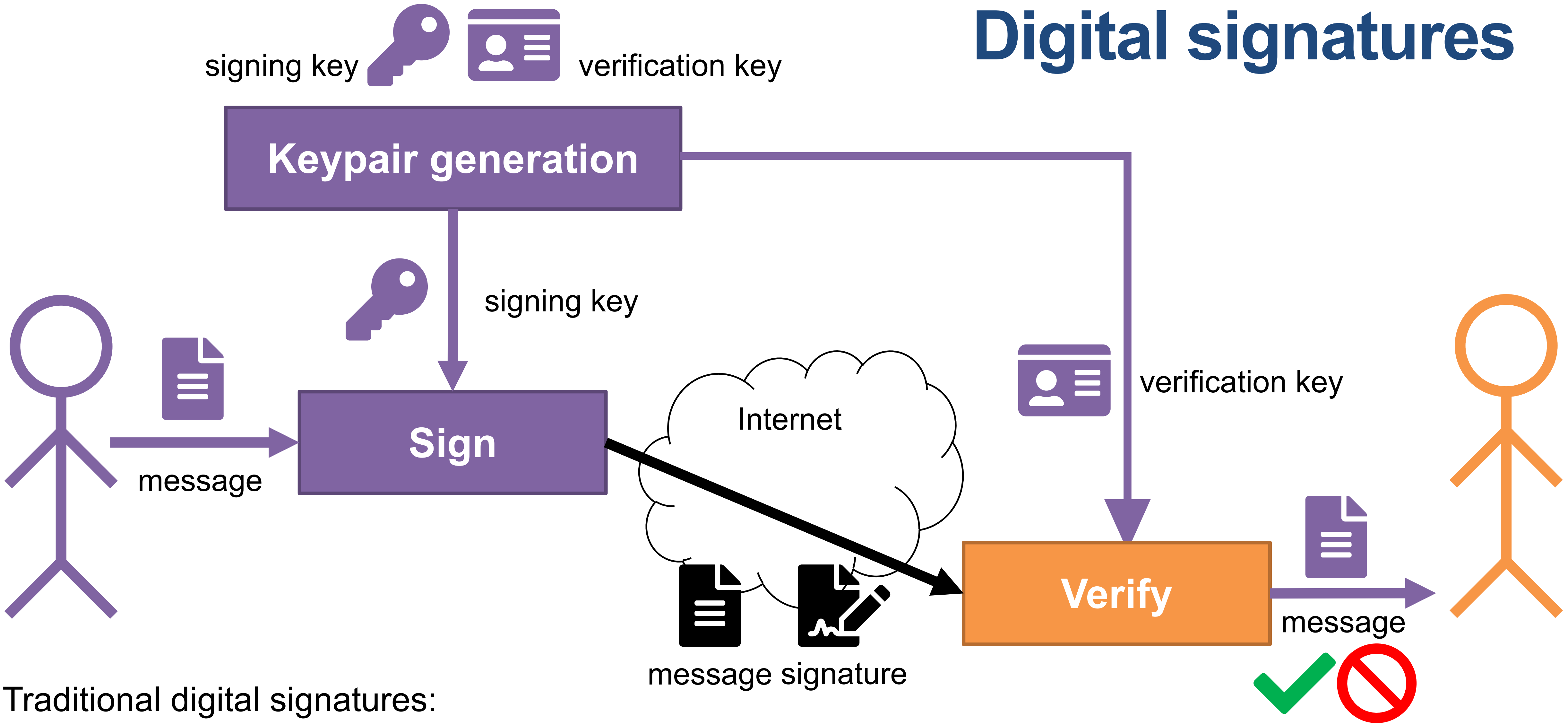

SHA-1 standardized
1995
SHA-2 standardized
2001
SHA-1 weakened
2005
Start PQ Crypto project
2016
Jan. 2017
Browsers stop accepting SHA-1 certificates
First full SHA-1 collision
Aug. 2017
Submission deadline
Nov. 2017
16 years
Standards ready
2023-25
2026
Mosca – 1/7 chance of breaking RSA-2048
2031
Mosca – 1/2 chance of breaking RSA-2048
EU commission – universal quantum computer
2035

Types of post-quantum cryptography

Types of post-quantum cryptography

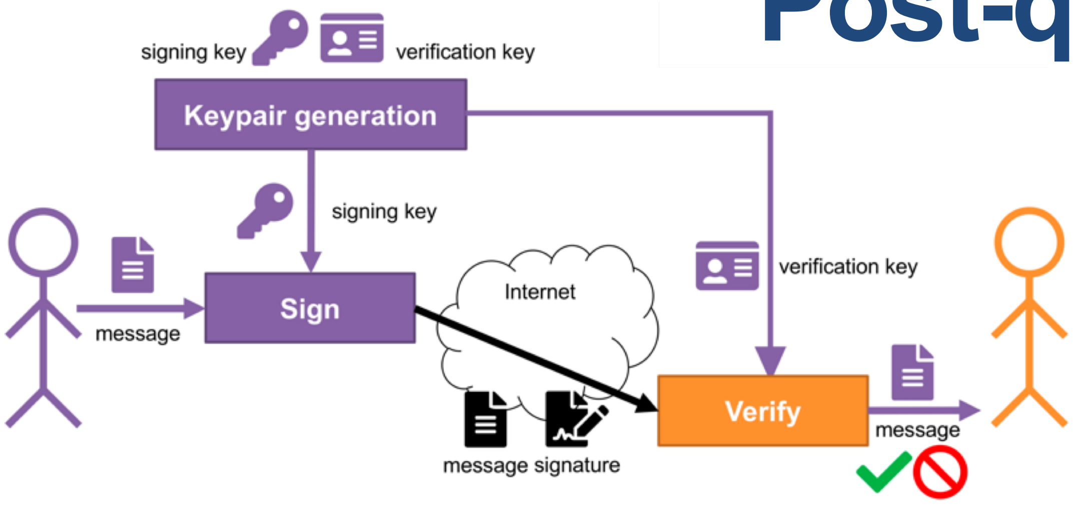
- Hash-based
- Code-based
- Multivariate quadratic
- Lattice-based
- Elliptic curve isogenies

Digital signatures



Traditional digital signatures:
RSA or DSA (256 byte keys & signatures)
Elliptic curve DSA (ECDSA) (32-byte verification keys, 64-byte signatures)

Post-quantum digital signatures



Hash-based

- Known and understood since 1980s
- Very high confidence in security
- Very small public keys (32 bytes)
- Large-ish signatures (8-29 KB)
  - SPHINCS+, Gravity-SPHINCS
  - Related: Picnic
- Variant: stateful hash-based signatures
  - XMSS, LMS, …

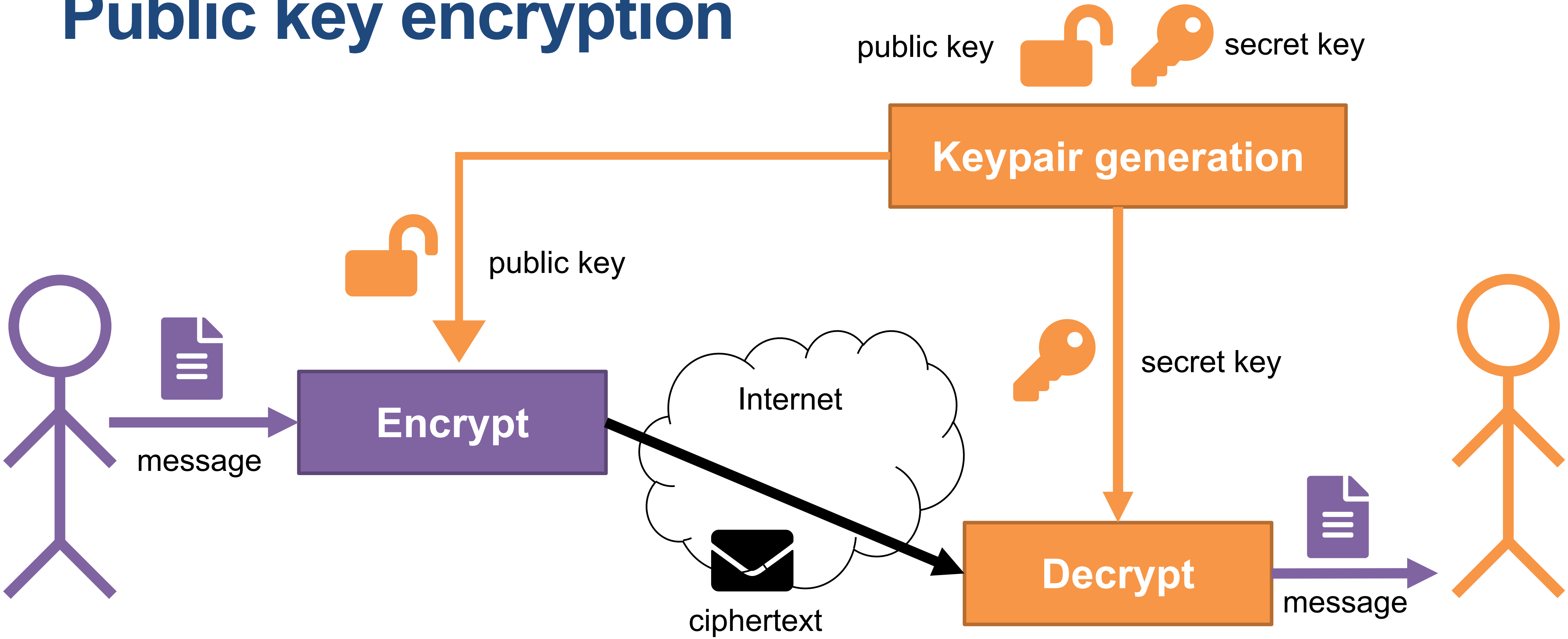
Lattice-based

- Dating from early 2010s
- Popular mathematics but hardness still being studied
- Medium public keys (1-6 KB)
- Medium signatures (2-6 KB)
  - CRYSTALS-Dilithium, qTESLA

Multivariate quadratic

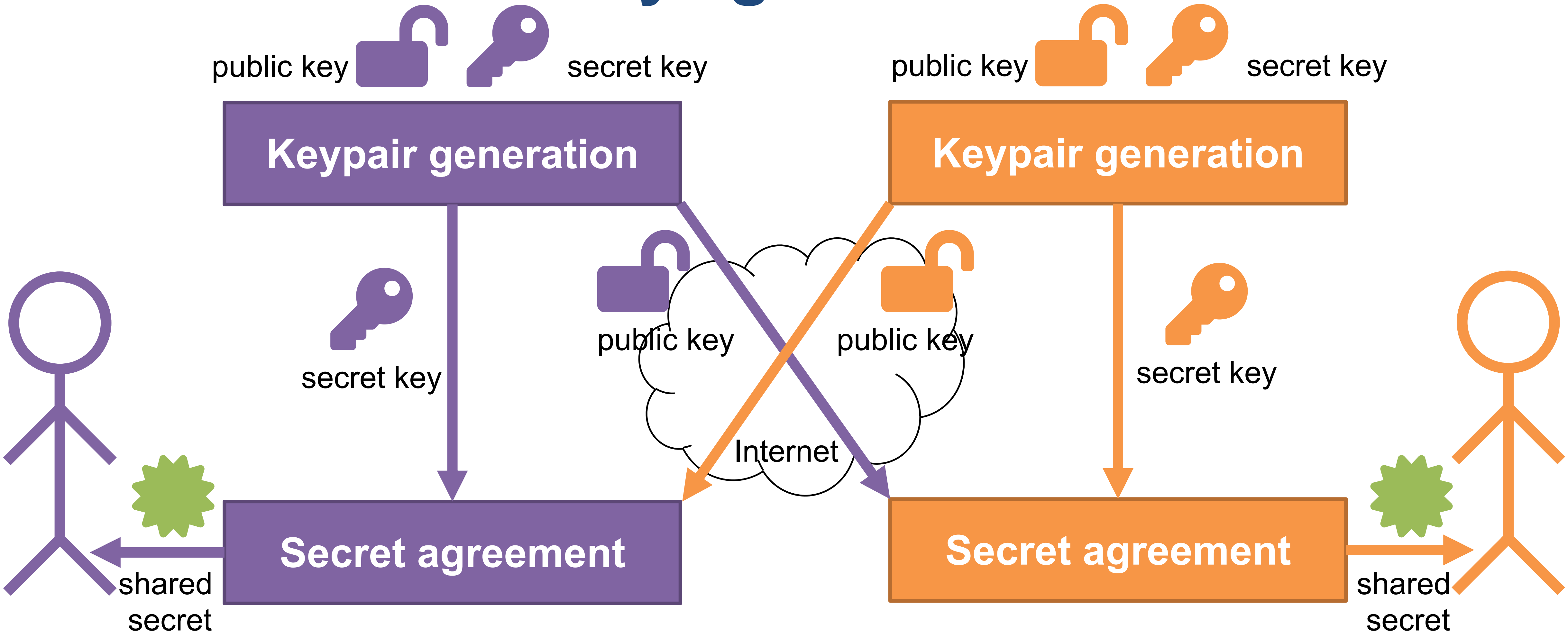
- Ideas date from 1980s but have significantly varied over time
- Large public keys (15-3000 KB)
- Very small signatures (70-500 bytes)
  - DualModeMS, GeMSS, HiMQ-3, LUOV, …

Public key encryption



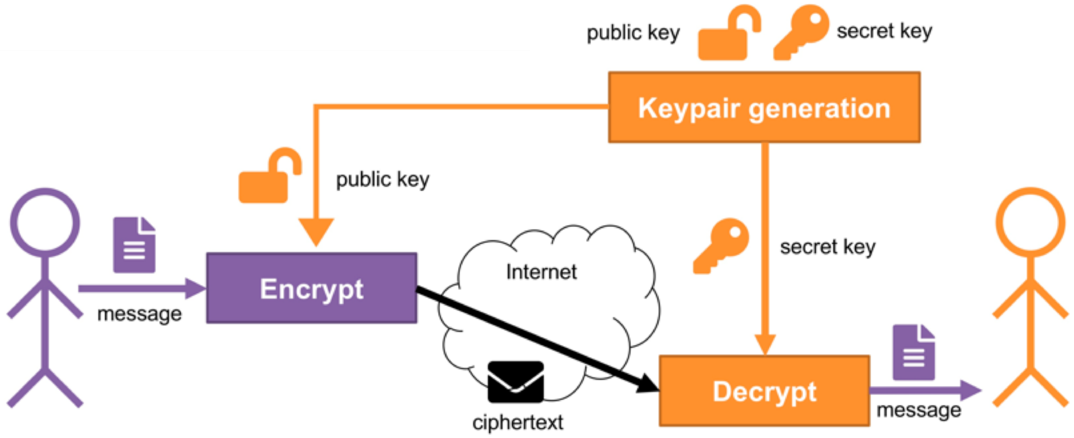
Traditional public key encryption:
RSA public key encryption (256-byte keys)

Key agreement



Traditional key agreement:
Diffie–Hellman (256 byte public keys)
Elliptic curve Diffie–Hellman (32 byte public keys)

Post-quantum key agreement / public key encryption

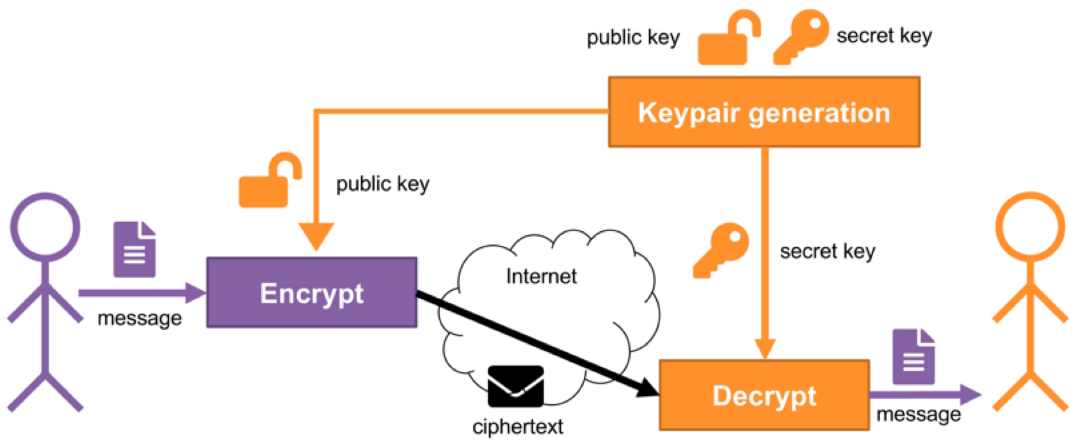


Lattice-based

- Dating from late 1990s/mid 2000s
- Popular mathematics but hardness still being studied
- Various categories based on amount of "structure"
  - "generic" versus "structured"
  - Less structure => bigger keys/ciphertexts but potentially harder to break

- Structured lattices
  - Small-medium public keys/ciphertexts (1-25 KB)
    - Kyber, NewHope, NTRU, …
- Generic lattices
  - Medium public keys/ciphertexts (10-20 KB)
    - FrodoKEM, …

Post-quantum key agreement / public key encryption



Code-based

- McEliece cryptosystem dates from late 1970s
- Basic system well-studied
- Small ciphertexts: ~256 bytes
- Large public keys: 25-1300 KB
  - BIG-QUAKE, Classic McEliece, …

Elliptic curve isogenies

- Dates from early 2010s
- New and specialized mathematical problem
- Small ciphertexts/public keys: ~500 bytes
- Slower computation
  - SIKE

Post-quantum cryptography

Hash-based

- Can only be used to make signatures, not public key encryption
- But very high confidence in high-based signatures
- Large-ish signatures

Code-based

- Long-studied public key encryption with moderately high confidence
- Large public keys

Multivariate quadratic

- Variety digital signature schemes with various levels of confidence and trade-offs
- Large public keys

Lattice-based

- High level of academic interest
- Flexible constructions – both encryption and signatures
- Reasonable sizes

Elliptic curve isogenies

- Specialized but promising technique
- Small communication, slow computation

Preparing to transition to post-quantum crypto

"Quantum risk assessment"

Identify your organization's reliance on cryptography

- Where is used? What type is used? How long does the information need to be secure for?

Track development of quantum technology

Manage technology lifecycle to adopt quantum-resistant technologies

Be wary of "snake oil cryptography"

"proprietary algorithm"

"secret technique"

"virtual one-time pad"

"chaos encryption"

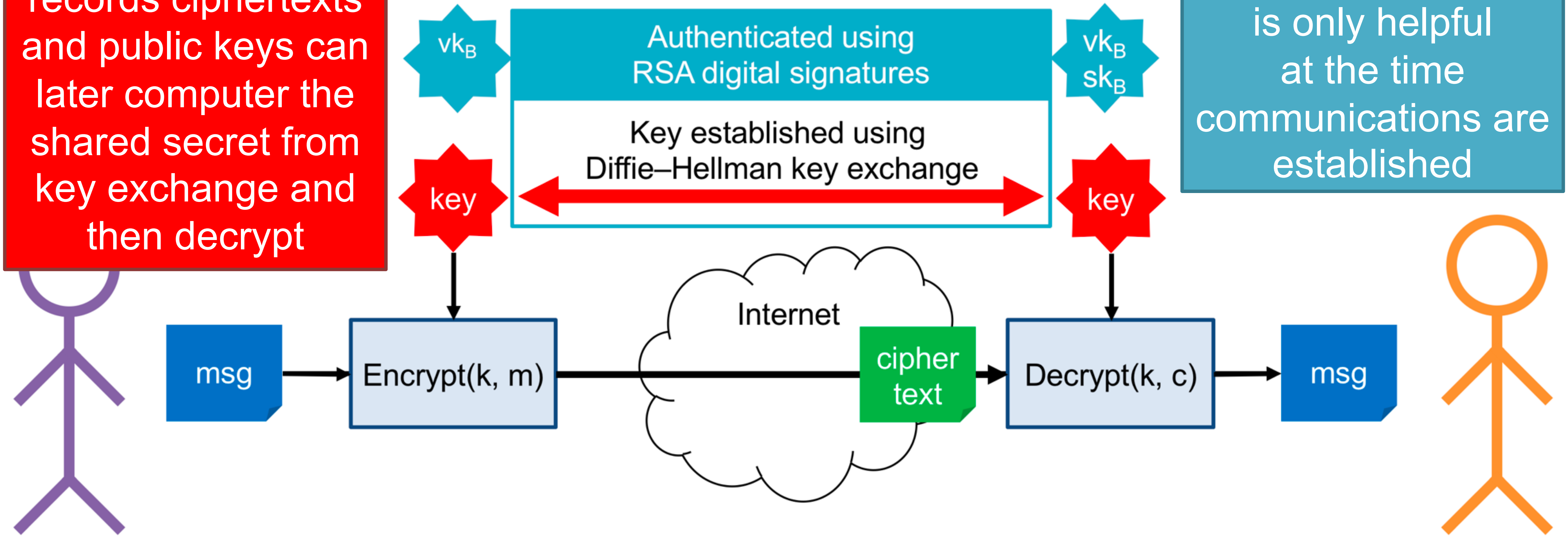
"unbreakable"

Focus instead on algorithms progressing through the NIST PQ crypto project

Prioritizing post-quantum public key encryption and key exchange

Any attacker who records ciphertexts and public keys can later computer the shared secret from key exchange and then decrypt

Breaking authentication keys is only helpful at the time communications are established



Hybrid cryptography

- Use pre-quantum and post-quantum algorithms together
- Secure if either one remains unbroken

Need to consider backward compatibility for non-hybrid-aware systems

Why hybrid?

- Potential post-quantum security for early adopters
- Maintain compliance with older standards (e.g. FIPS)
- Reduce risk from uncertainty on PQ assumptions/parameters

Hybrid ciphersuites

	Key exchange	Authentication
1	Hybrid traditional + PQ	Single traditional
2	Hybrid traditional + PQ	Hybrid traditional + PQ
3	Single PQ	Single traditional
4	Single PQ	Single PQ

Likely focus
for next 10 years

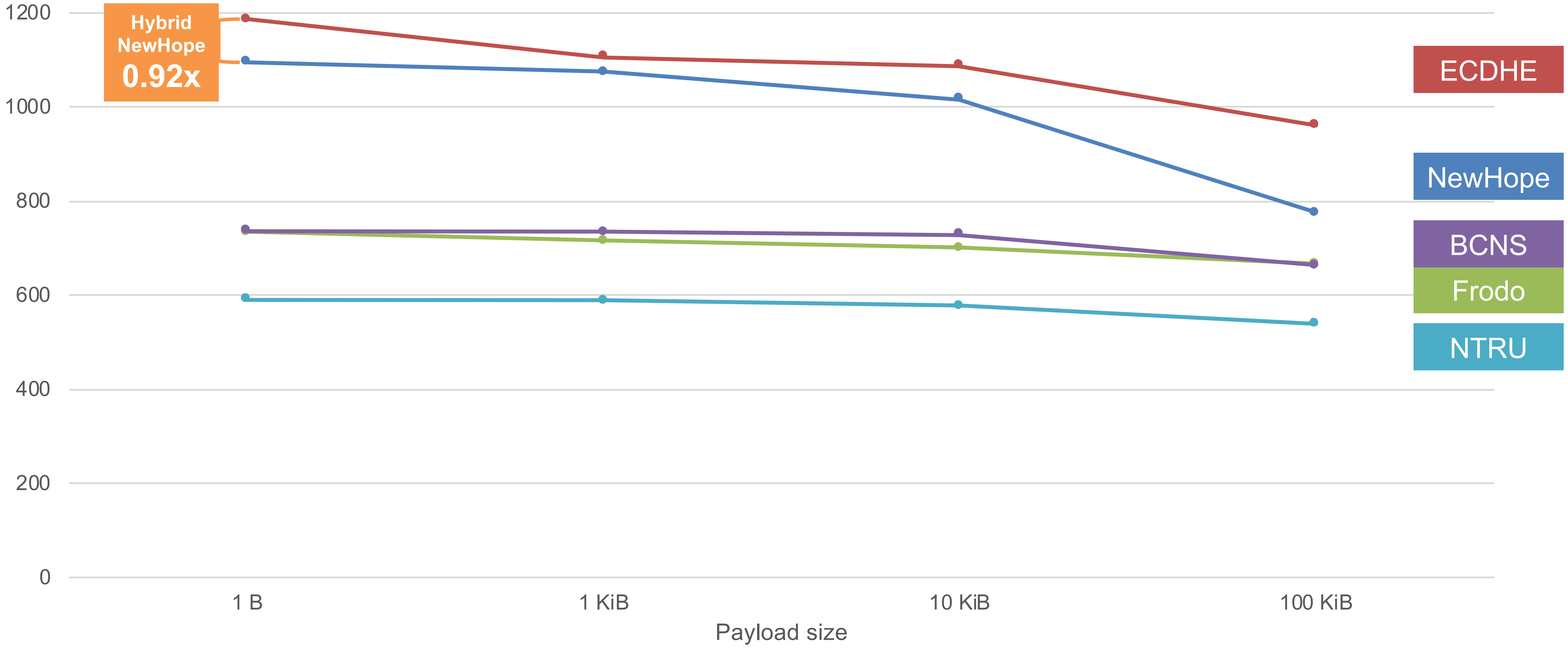
Post-quantum key exchange in TLS

- Various prototypes and experiments:
  - [BCNS] S&P 2015
  - [BCDMNNRS] ACM CCS 2016
  - Google/CloudFlare experiments (2016, 2018)
  - liboqs OpenSSL fork
  - TLS 1.3 drafts
    - Schanck and Stebila
    - Whyte et al.
- Demonstrated for both TLS 1.2 and TLS 1.3
- Unlikely to be standardized until completion of NIST competition
- Optional extension for PQ key exchange doesn't break backwards compatibility
- Most PQ algorithms don't substantially impact server load
  - Even with hybrid key exchange
- Public key/ciphertext sizes up to ~20KB don't break backwards compatibility
  - But sizes above 5KB have significant impact on latency on a non-trivial fraction of connections

TLS connection throughput – hybrid w/ECDHE

ECDSA signatures

bigger (top) is better



[BCDMNNRS] ACM CCS 2016
x86_64, 2.6 GHz Intel Xeon E5 (Sandy Bridge) – server Google `n1-standard-4`, client `-32`

Note somewhat incomparable security levels

Post-quantum key exchange in SSH

- Prototype implementation:
  - liboqs OpenSSH fork

- Initial experiments demonstrate feasibility
- No testing on backwards compatibility, latency, server load

Post-quantum/hybrid X.509 public key certificates

- How to convey multiple public keys & signatures in a single certificate?
- Various proposals:
  - second certificate/public key in X.509 extension
    - [BHMS] PQCrypto 2017
    - ISARA http://www.test-pqpki.com/

- Basic X.509 libraries can handle large certificates
- But relying applications (TLS, S/MIME) may struggle

	Extension size in KiB				
	1.5	3.5	9.0	43.0	1333.0
Libraries (library's command-line client talking to library's command-line server					
GnuTLS 3.5.11	✓	✓	✓	✓	×
Java SE 1.8.0_131	✓	✓	✓	✓	✓
mbedTLS 2.4.2	✓	✓	✓	×	×
NSS 3.29.1	✓	✓	✓	✓	×
OpenSSL 1.0.2k	✓	✓	✓	✓	×
Web browsers (talking to OpenSSL's command-line server)					
Apple Safari 10.1 (12603.1.30.0.34)	✓	✓	✓	✓	✓
Google Chrome 58.0.3029.81	✓	✓	✓	✓	×
Microsoft Edge 38.14393.1066.0	✓	✓	✓	×	×
Microsoft IE 11.1066.14393.0	✓	✓	✓	×	×
Mozilla Firefox 53.0	✓	✓	✓	✓	×
Opera 44.0.2510.1218	✓	✓	✓	✓	×

https://openquantumsafe.org/

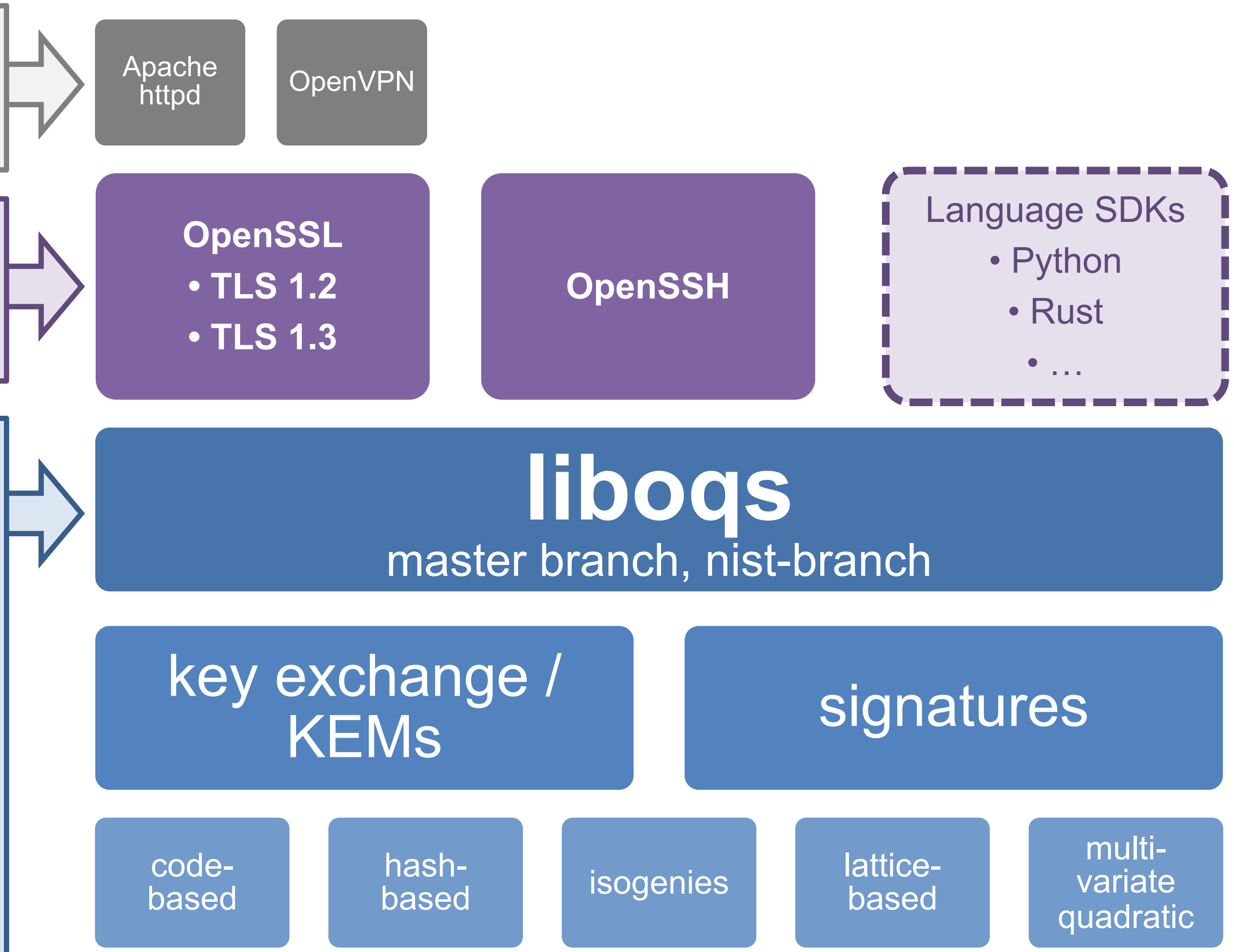
Open Quantum Safe Project

Potential and reported uses (outside the OQS project)

Integration into forks of widely used open-source projects

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

Two versions:
- master branch: high quality audited code; MIT licensed
- nist-branch: as many NIST submissions as possible



OQS team

- Project leads
  - Douglas Stebila (Waterloo)
  - Michele Mosca (Waterloo)
- Industry collaborators
  - Amazon Web Services
  - evolutionQ
  - Microsoft Research
- Individual contributors

- Financial support
  - Government of Canada
    - NSERC
    - Tutte Institute
- In-kind contributions of developer time from industry collaborators

Transitioning to post-quantum cryptography

Douglas Stebila
UNIVERSITY OF WATERLOO

Widely deployed public key cryptography would be broken by quantum computers

Post-quantum cryptography is about designing potentially quantum-resistant algorithms using different mathematical primitives

Need to start preparing for the quantum transition

- **Identify reliance on cryptography**
- **Follow NIST post-quantum crypto standardization process**

Survey paper

- https://eprint.iacr.org/2016/1017

Open Quantum Safe project

- https://openquantumsafe.org/

Presentations

- https://www.douglas.stebila.ca/research/presentations/

Appendices

Lattice-based crypto

From the "learning with errors" problem

Solving systems of linear equations

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

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

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

=

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

4
8
1
10
4
12
9

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

Solving systems of linear equations

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

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

=

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

4
8
1
10
4
12
9

Easily solved using Gaussian elimination (Linear Algebra 101)

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

Learning with errors problem

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

$$
\begin{pmatrix} 4 & 1 & 11 & 10 \\ 5 & 5 & 9 & 5 \\ 3 & 9 & 0 & 10 \\ 1 & 3 & 3 & 2 \\ 12 & 7 & 3 & 4 \\ 6 & 5 & 11 & 4 \\ 3 & 3 & 5 & 0 \end{pmatrix} \times \begin{pmatrix} 6 \\ 9 \\ 11 \\ 11 \end{pmatrix} + \begin{pmatrix} 0 \\ -1 \\ 1 \\ 1 \\ 1 \\ 0 \\ -1 \end{pmatrix} = \begin{pmatrix} 4 \\ 7 \\ 2 \\ 11 \\ 5 \\ 12 \\ 8 \end{pmatrix}
$$

Learning with errors problem

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

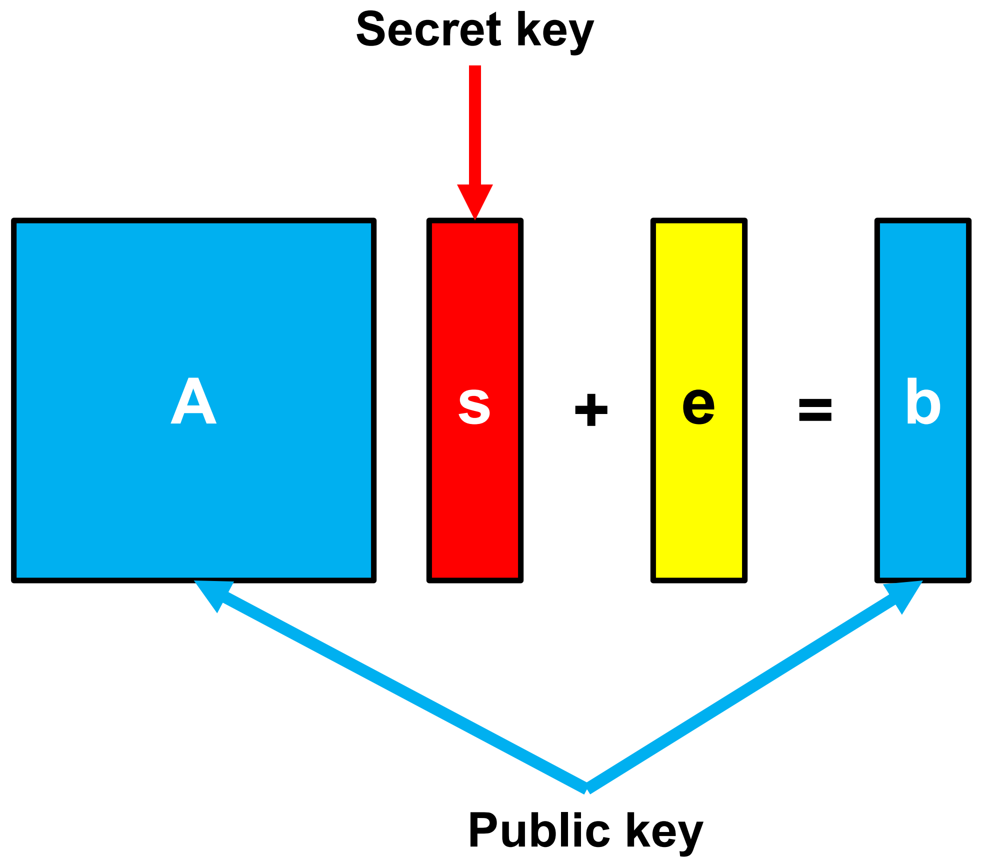
$$\begin{pmatrix} 4 & 1 & 11 & 10 \\ 5 & 5 & 9 & 5 \\ 3 & 9 & 0 & 10 \\ 1 & 3 & 3 & 2 \\ 12 & 7 & 3 & 4 \\ 6 & 5 & 11 & 4 \\ 3 & 3 & 5 & 0 \end{pmatrix} \times \begin{pmatrix} \ \\ \ \\ \ \\ \ \end{pmatrix} + \begin{pmatrix} \ \\ \ \\ \ \\ \ \\ \ \\ \ \\ \ \end{pmatrix} = \begin{pmatrix} 4 \\ 7 \\ 2 \\ 11 \\ 5 \\ 12 \\ 8 \end{pmatrix}$$

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

Building cryptography from learning with errors

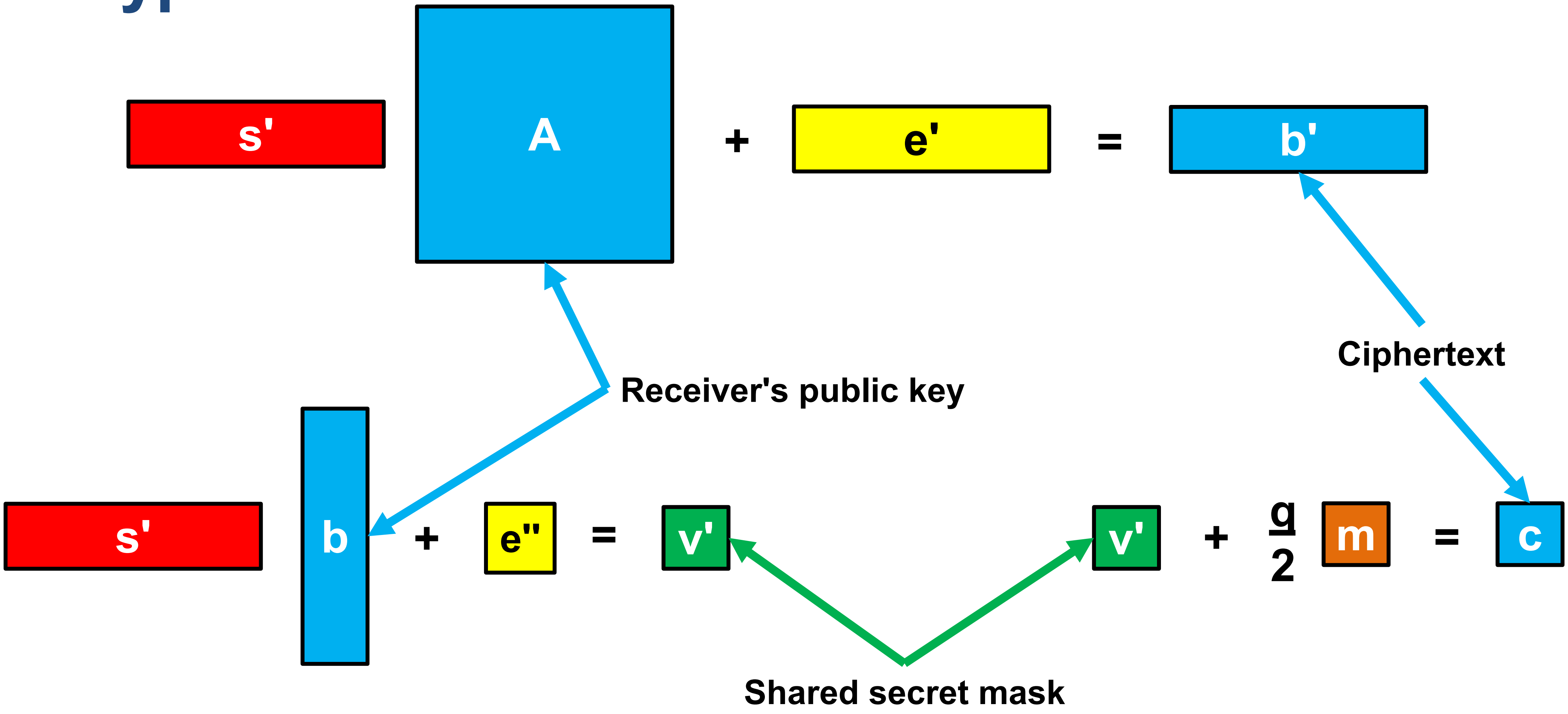
- Can build a key exchange replacement algorithm using learning with errors-like problems
- Difficulty of breaking learning with errors is related to the difficulty of finding short vectors in certain types of lattices
  - "lattice-based"
- Quantum computers don't seem to be able to break these efficiently

Public key encryption from LWE
Key generation



[Lindner, Peikert. CT-RSA 2011]

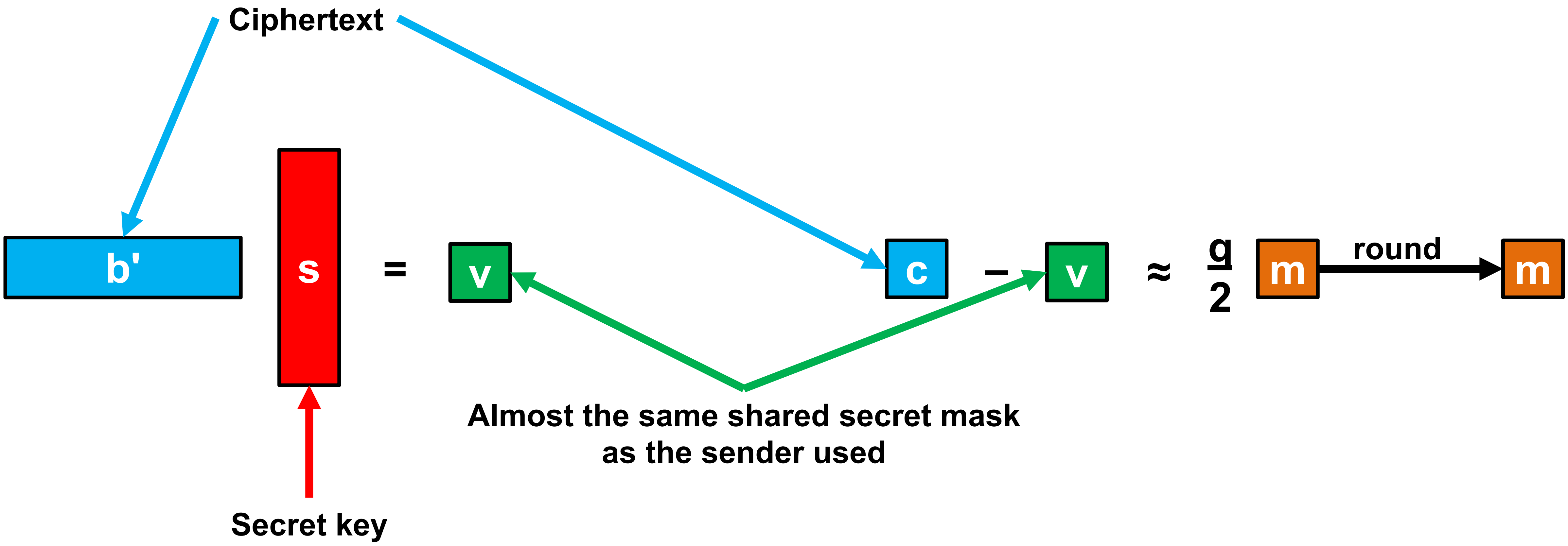
Public key encryption from LWE
Encryption



[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

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

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

$$\approx s' A s$$

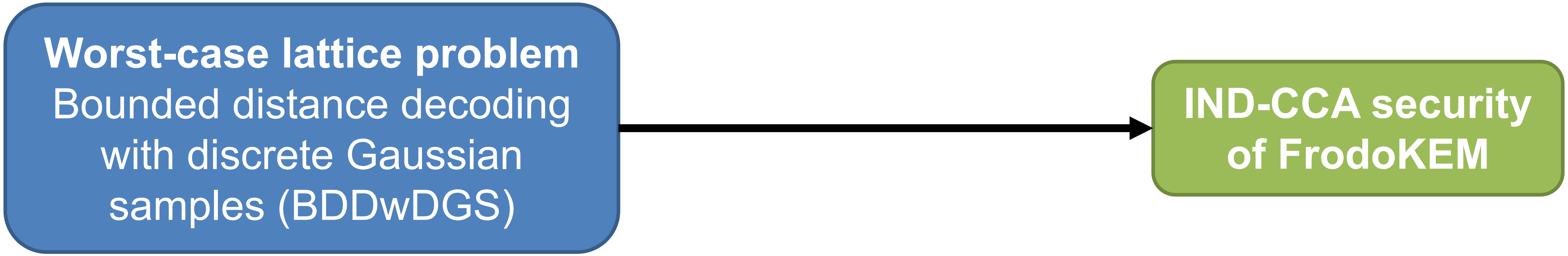
FrodoKEM

- KEM: Key encapsulation mechanism (simplified key exchange protocol)
- Builds on basic (IND-CPA) LWE public key encryption
- Achieves IND-CCA security against adaptive adversaries
  - By applying a variant of the Fujisaki–Okamoto transform
- Negligible error rate

- Simple design:
  - Free modular arithmetic ($q = 2^{16}$)
  - Simple Gaussian sampling
  - Parallelizable matrix-vector operations
  - No reconciliation
  - Simple to code

[Bos, Costello, Ducas, Mironov, Naehrig, Nikolaenko, Raghunathan, Stebila. ACM CCS 2016]
[Alkim, Bos, Ducas, Easterbrook, LaMacchia, Longa, Mironov, Naehrig, Nikolaenko, Peikert, Raghunathan, Stebila. FrodoKEM NIST Submission, 2017]

Reductionist security of FrodoKEM



Theorem. If you can break FrodoKEM in time T with probability ϵ, you can break BDDwDGS in time f(T) with probability $\approx\epsilon$.

Limitation:

f is a pretty big polynomial.

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

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

8 (columns) × 640 (rows)

2738	3842	3345	2979	…
2896	595	3607		
377	1575			
2760				
…				

640 × 8 × 15 bits = **9.4 KiB**

Ring learning with errors problem

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

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

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

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

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

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

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

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

Problems

Learning with errors		
Module-LWE	Search	With uniform secrets
Ring-LWE		
Learning with rounding	Decision	With short secrets
NTRU problem		