Understanding the impact of quantum computers on information security

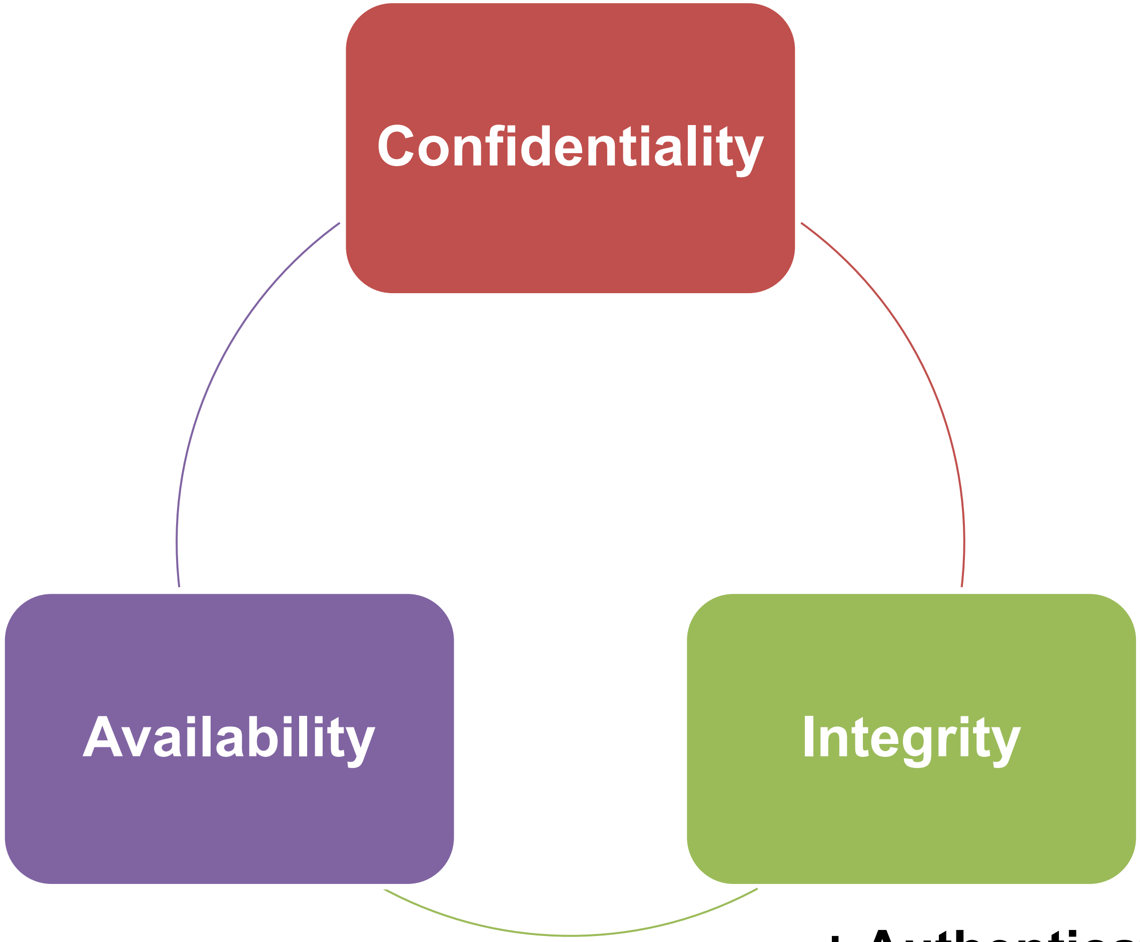
Douglas Stebila McMaster University

Funding acknowledgements:

NSERC CRSNG

Global Risk Institute Summit • Toronto • October 4, 2017

Security goals



+ Authentication

Data at rest

Data in transit

Data while processing

Cryptography in finance

- Inter-bank communications
- Blockchain

- Intra-bank communications
  - Virtual private networks (VPNs)
  - PKI
- Encrypted databases

- Merchant-bank communications

- Customer-bank communications
  - EMV Chip-and-PIN
  - Online banking

Quantum computing

Represent and process information using **quantum mechanics**

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

- 0 and 1

Quantum computers handle information as **qubits:**

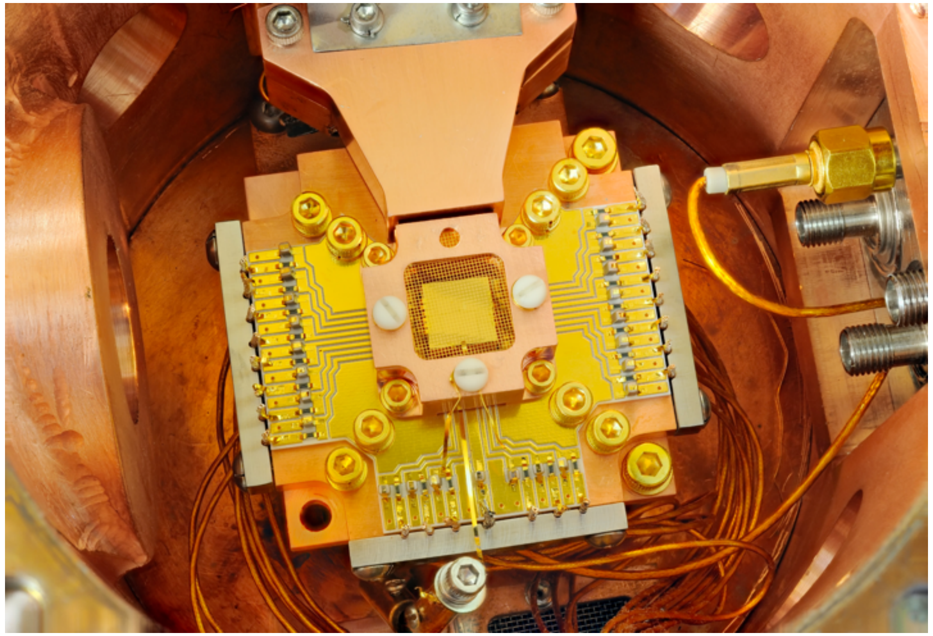
- Any "superposition" of 0 and 1

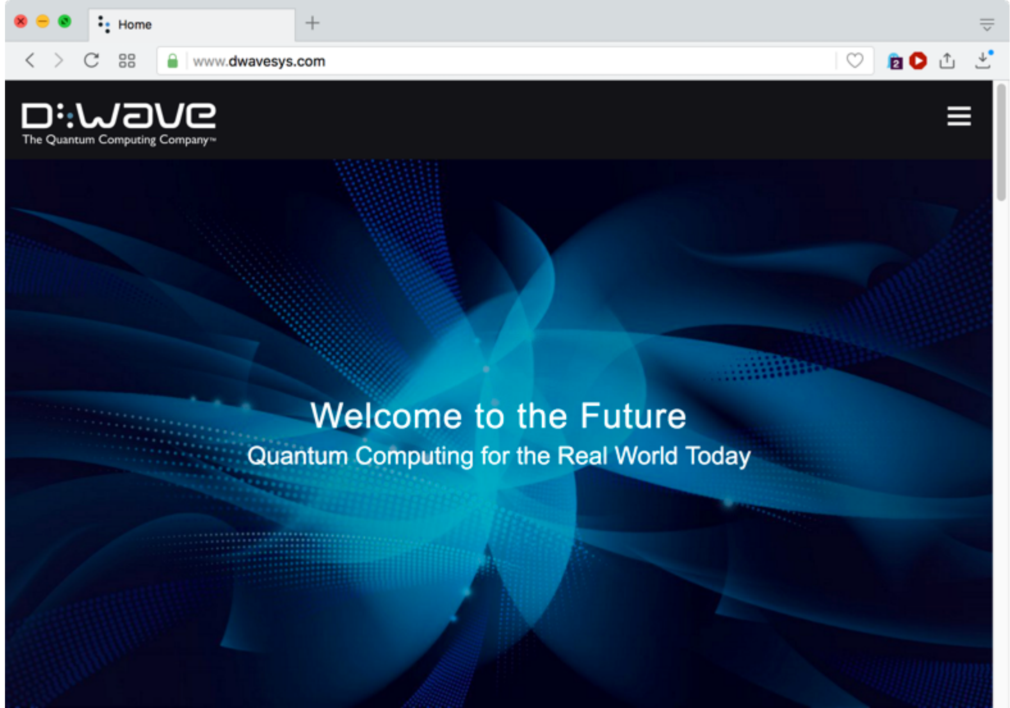
Processing information in superposition can dramatically speed some computations

- Chemical reaction simulations
- Optimization problems
- Arithmetic

But not magic

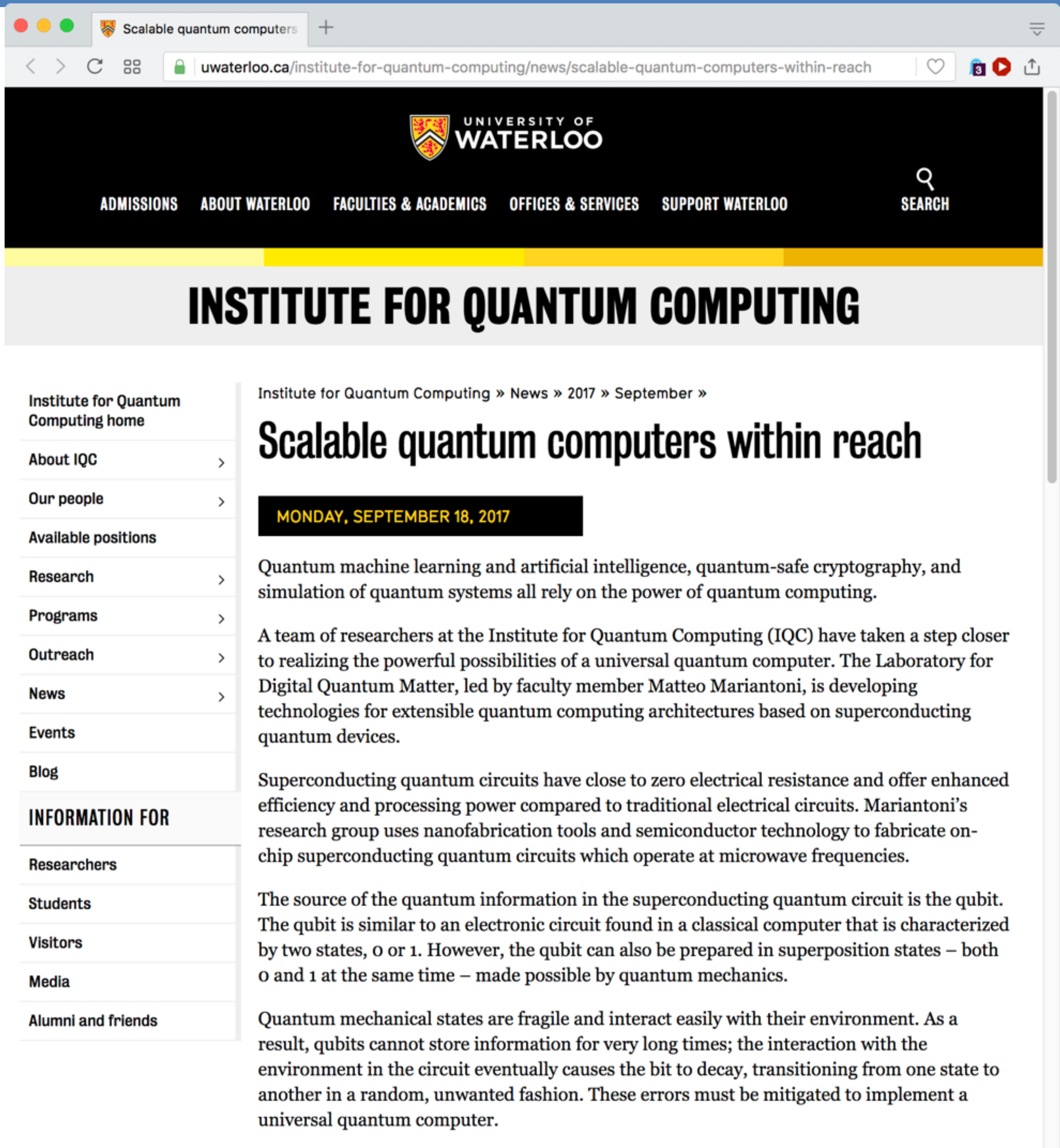
- Doesn't dramatically speed up all computations





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

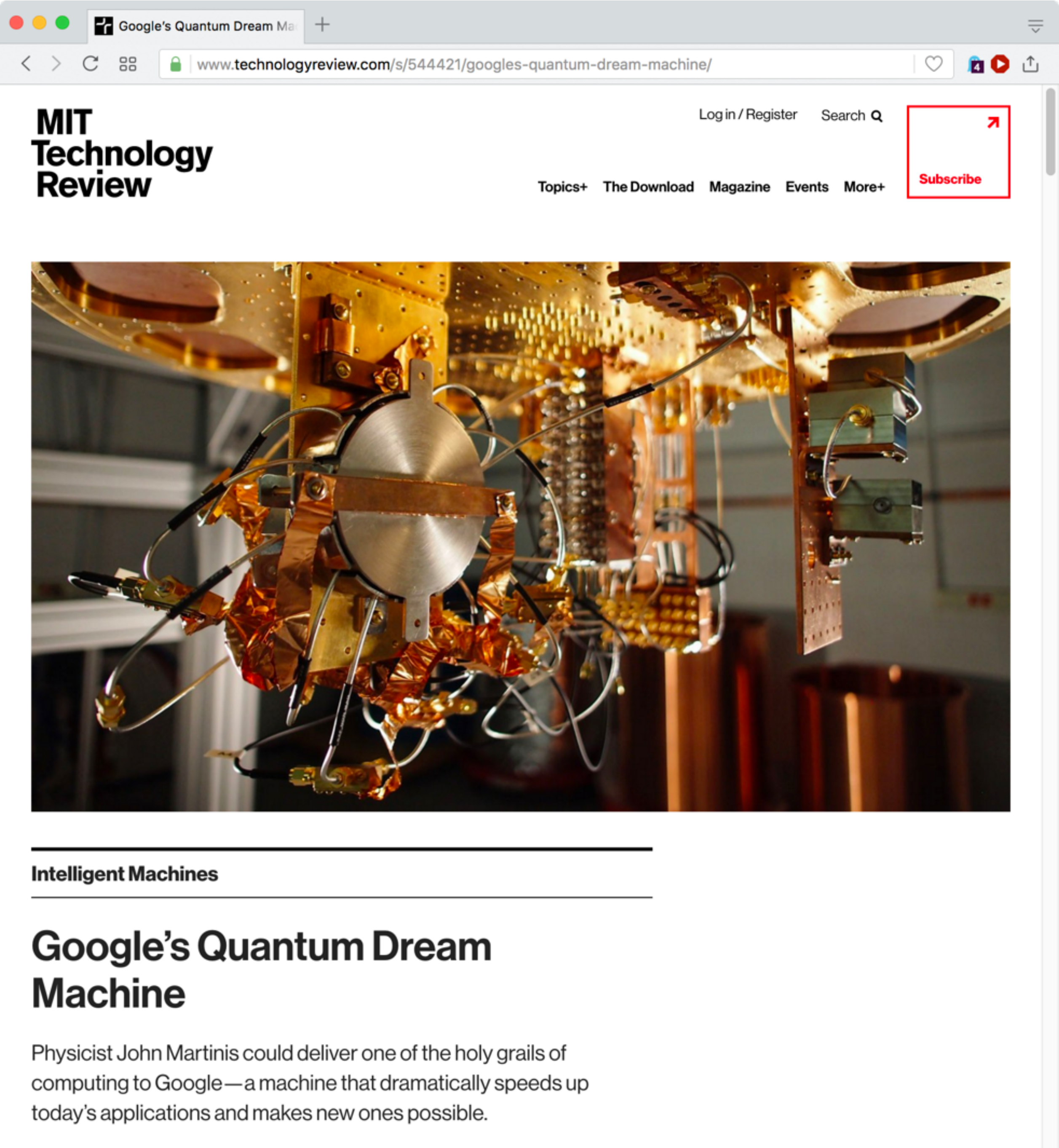
Quantum machine learning and artificial intelligence, quantum-safe cryptography, and simulation of quantum systems all rely on the power of quantum computing.

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.

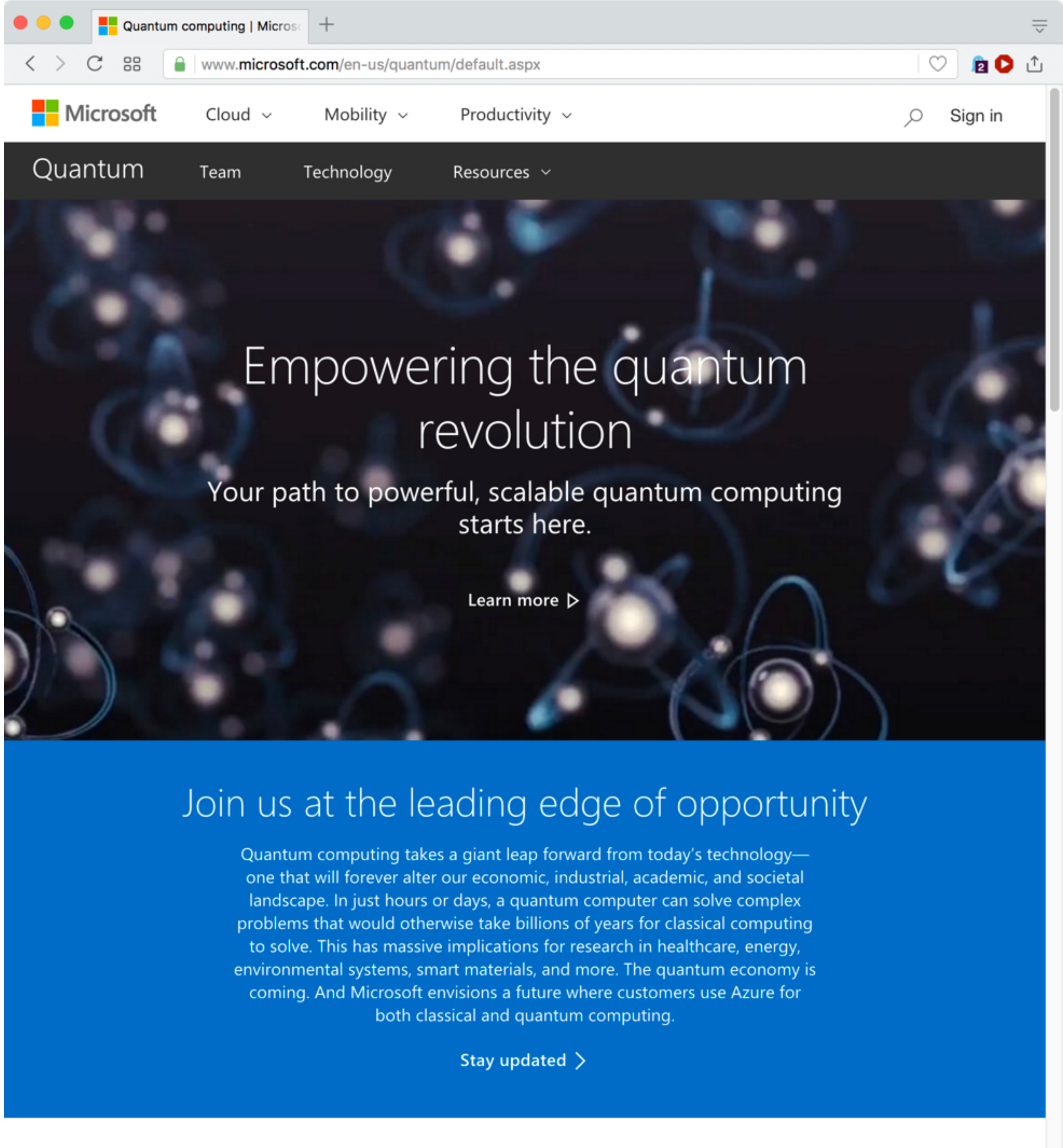
Quantum mechanical states are fragile and interact easily with their environment. As a result, qubits cannot store information for very long times; the interaction with the environment in the circuit eventually causes the bit to decay, transitioning from one state to another in a random, unwanted fashion. These errors must be mitigated to implement a universal quantum computer.



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.



Empowering the quantum revolution

Your path to powerful, scalable quantum computing starts here.

Learn more ▷

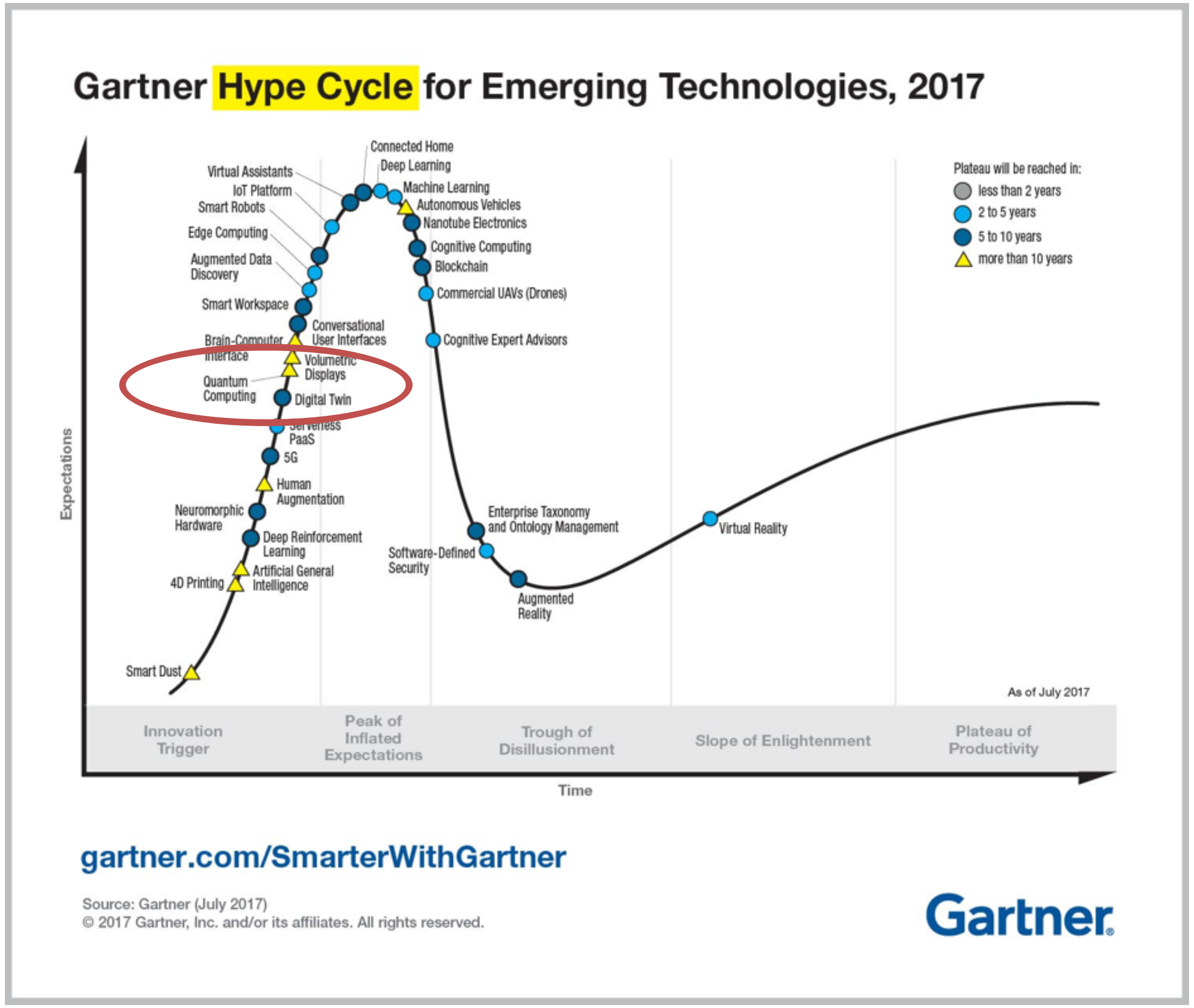
Join us at the leading edge of opportunity

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?
MARCH 11TH–17TH 2017
Quantum leaps
A mind-bending technology goes mainstream

March 2017


Gartner Hype Cycle for Emerging Technologies, 2017

gartner.com/SmarterWithGartner

Source: Gartner (July 2017)
© 2017 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner.

Quantum threat to information security

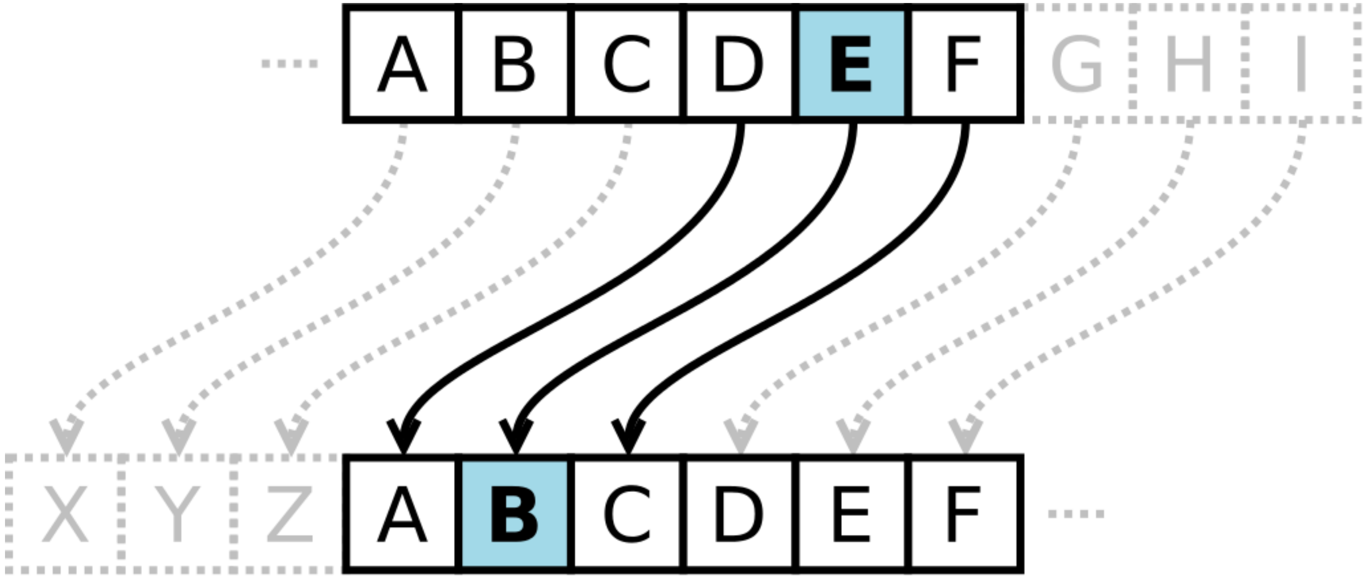
Large-scale general-purpose quantum computers could break some encryption schemes

Need to migrate encryption to quantum-resistant algorithms

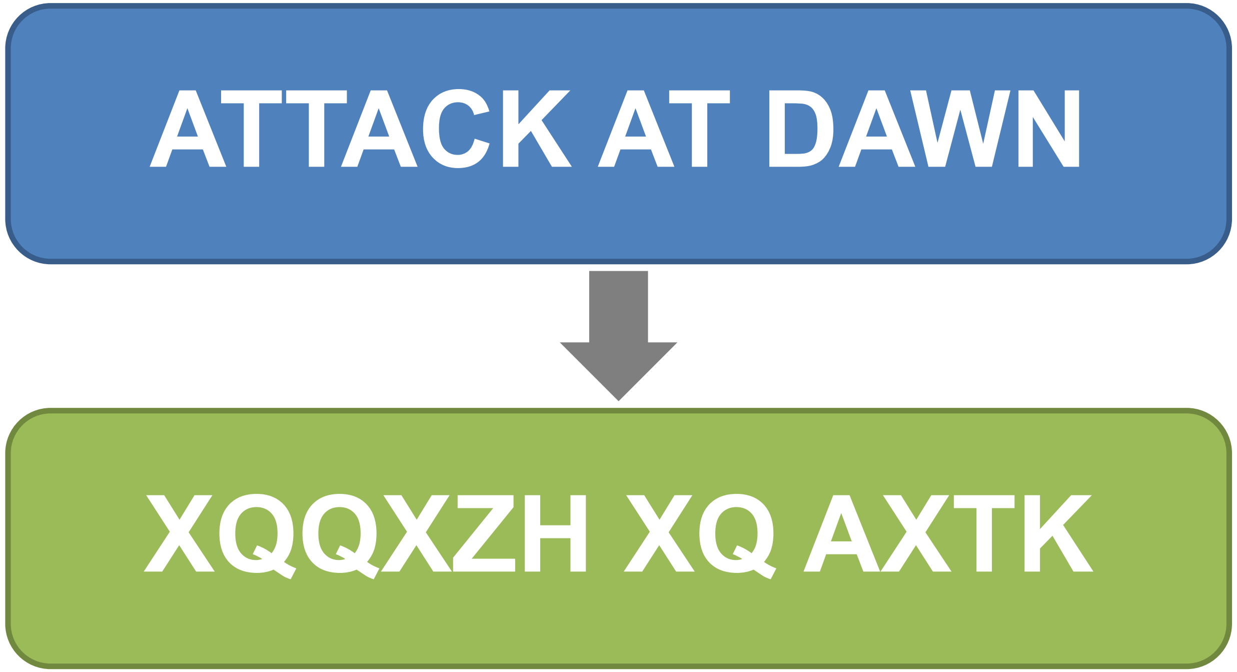
When should you start the process?

Encryption

Caesar cipher



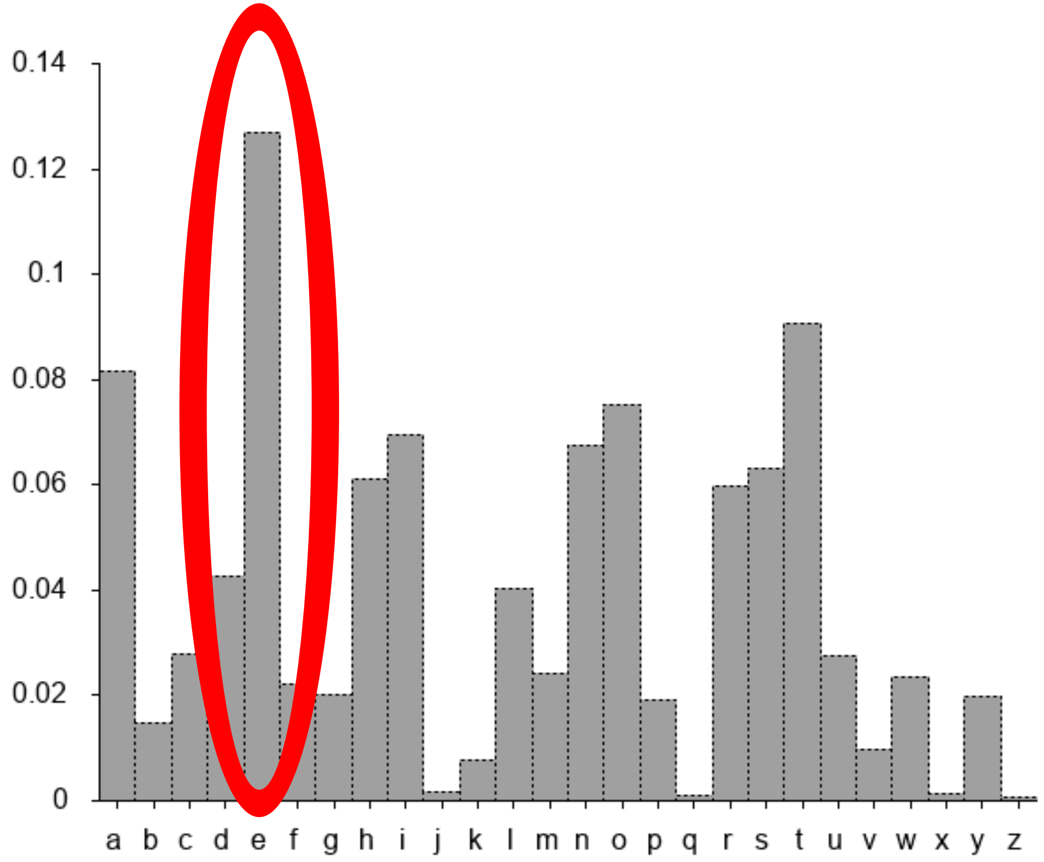
Caesar cipher



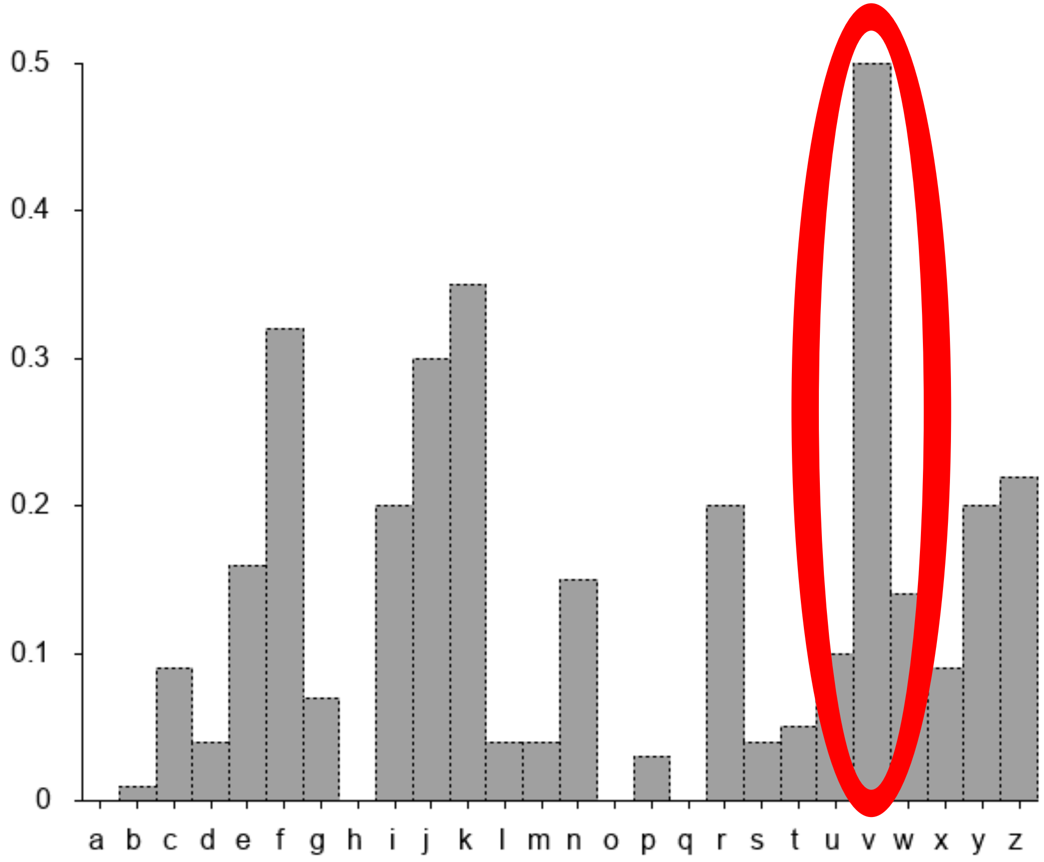
ATTACK AT DAWN

XQQXZH XQ AXTK

Frequency analysis

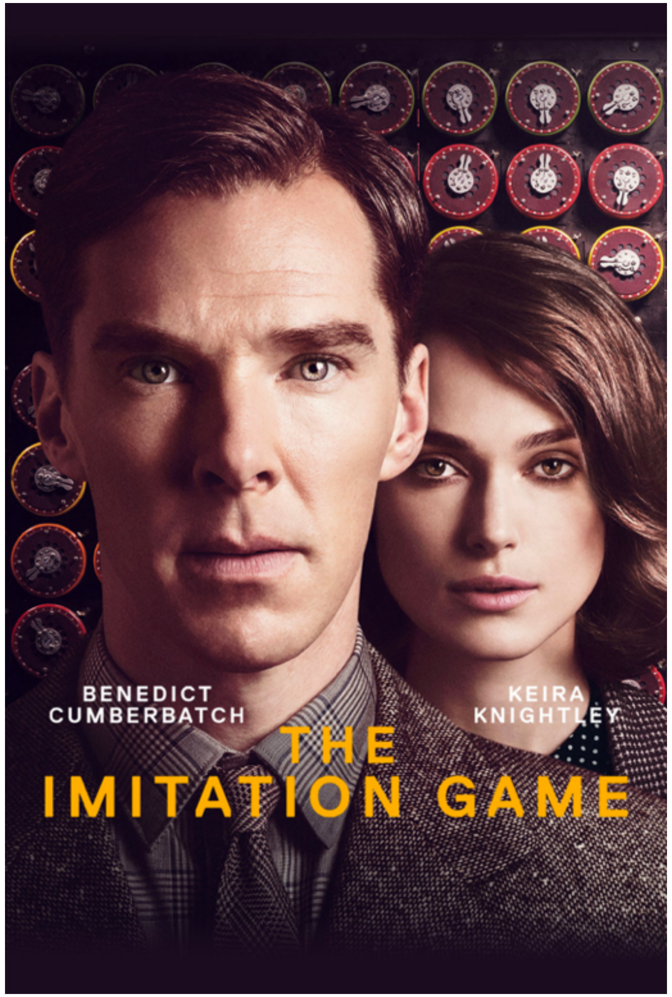


Frequency of letters in English text

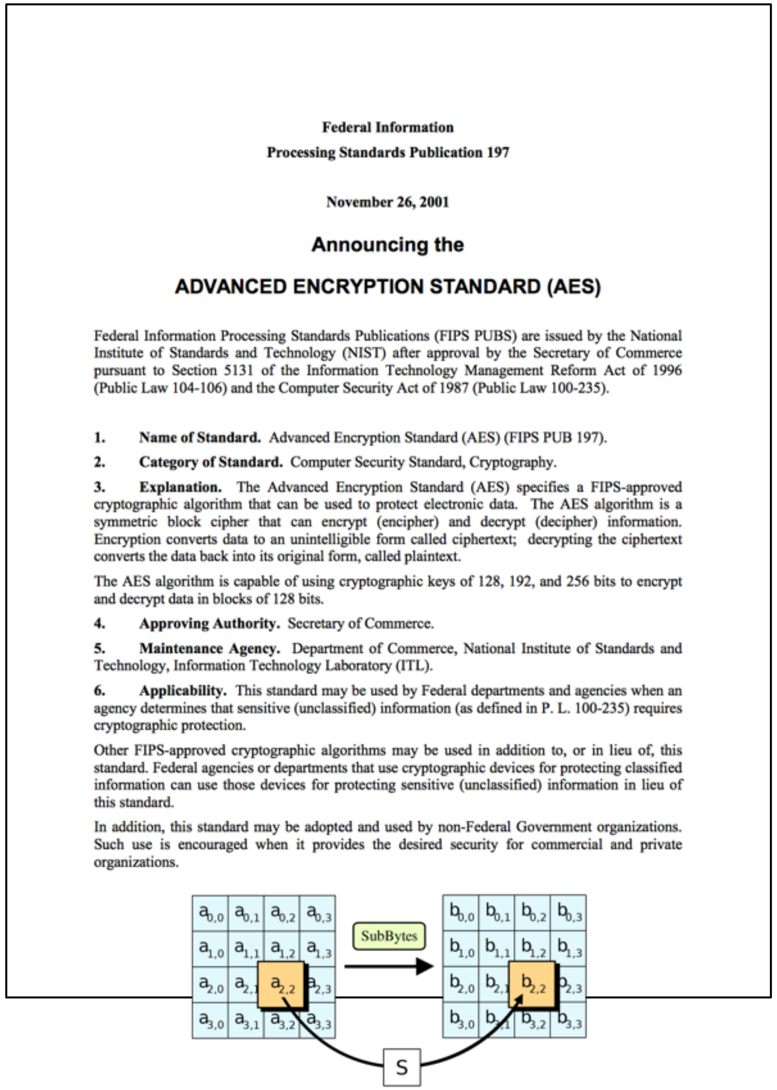


Frequency of letters in encrypted message

World War II – The Enigma machine



Modern ciphers



Federal Information
Processing Standards Publication 197

November 26, 2001

Announcing the

ADVANCED ENCRYPTION STANDARD (AES)

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).

1. **Name of Standard.** Advanced Encryption Standard (AES) (FIPS PUB 197).

2. **Category of Standard.** Computer Security Standard, Cryptography.

3. **Explanation.** The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext.

The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

4. **Approving Authority.** Secretary of Commerce.

5. **Maintenance Agency.** Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL).

6. **Applicability.** This standard may be used by Federal departments and agencies when an agency determines that sensitive (unclassified) information (as defined in P. L. 100-235) requires cryptographic protection.

Other FIPS-approved cryptographic algorithms may be used in addition to, or in lieu of, this standard. Federal agencies or departments that use cryptographic devices for protecting classified information can use those devices for protecting sensitive (unclassified) information in lieu of this standard.

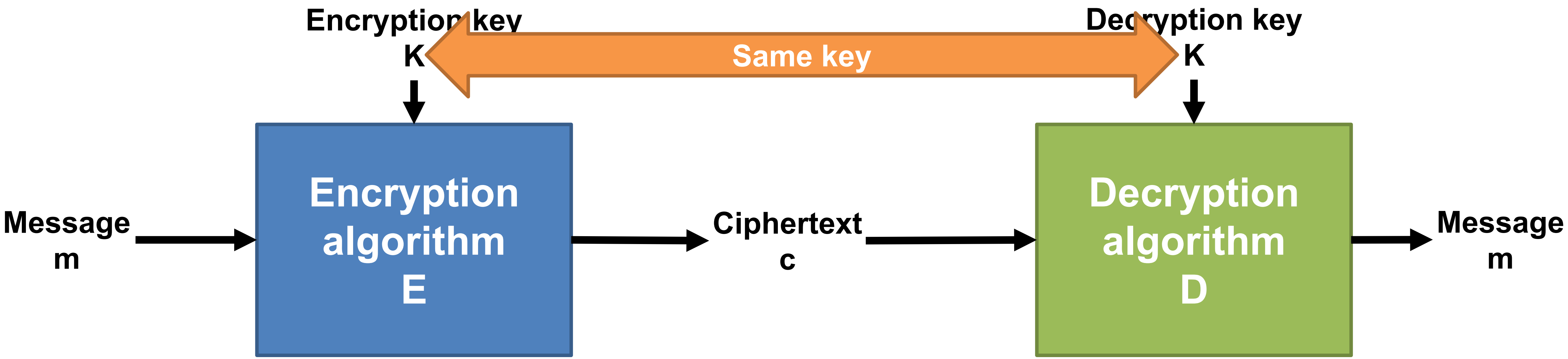
In addition, this standard may be adopted and used by non-Federal Government organizations. Such use is encouraged when it provides the desired security for commercial and private organizations.

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
S

<u>Kerckhoff's principle:</u>

- Security should not depend on keeping the design of the system secret.
- Only a (small) key should have to be kept secret.

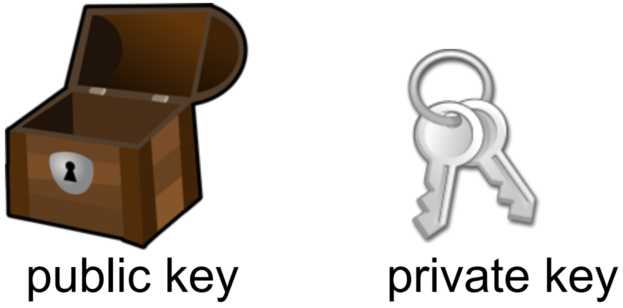
Symmetric encryption



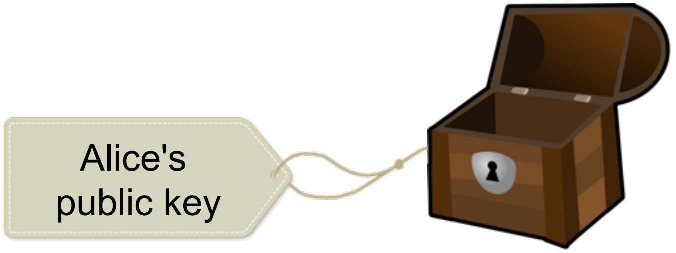
Public key cryptography

A pair of related keys:

- public key
- private key



Publish the public key



Anyone can use the public key to encrypt

Only the person with the private key can decrypt

encrypt a message

Public key cryptography – RSA algorithm

based on multiplying large secret prime numbers

11579208923731619542357098500868790785326998466564056403945758400791312964023 3

X

231584178474632390847141970017375815706
151680158262592800

=

26815615859885194199148049996411692254958 675544
71228874435280602338222844249842670606152315157095935507 1
3202220725480894468703147942321125 26291

Efficient for a computer to do

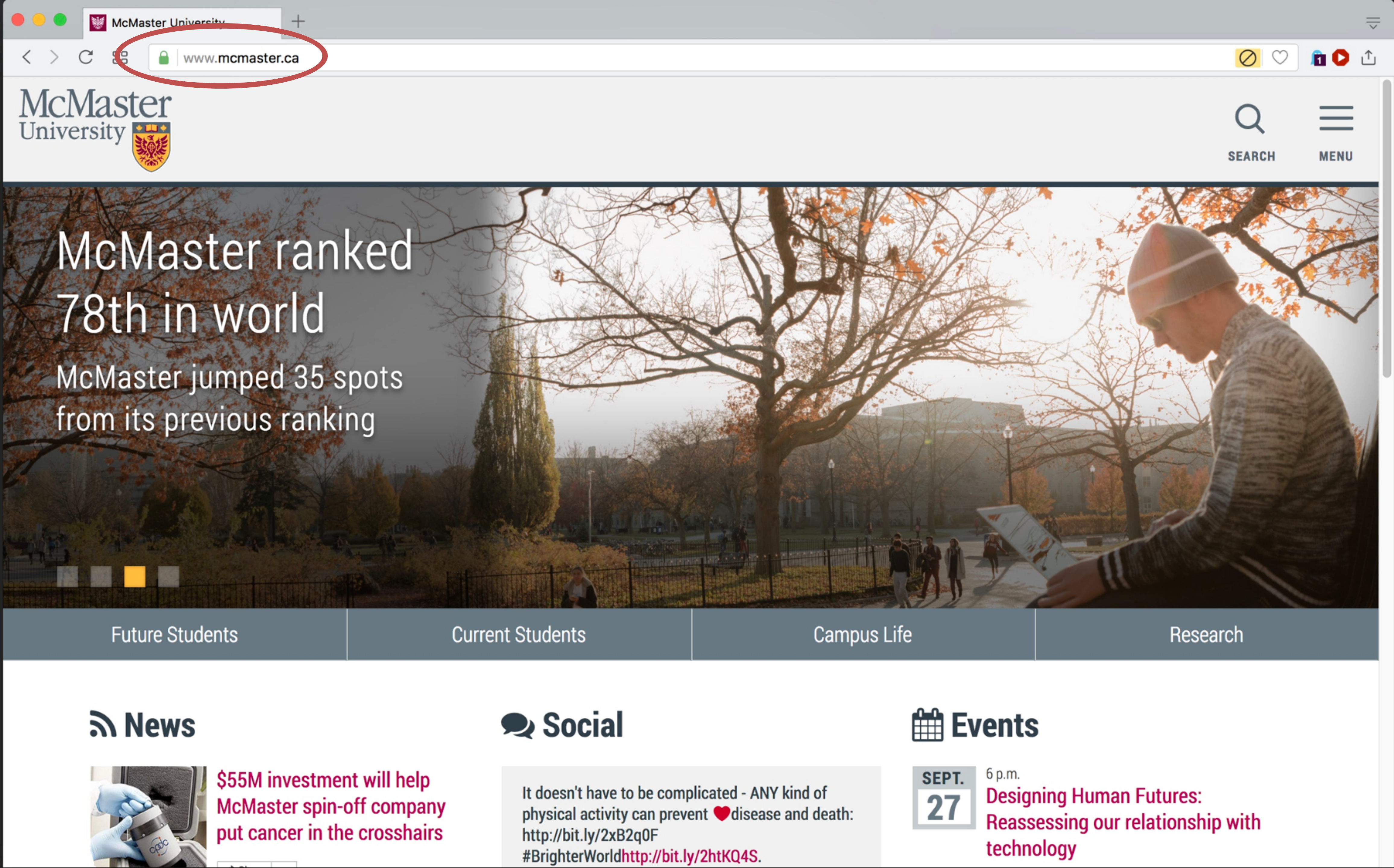
Public key cryptography – RSA algorithm

Given the product

268156158598851941991480499964116922549587316411847867554471228874435280602338222284[illegible]1
523151570959355071320222072548089[illegible]
12526291

Don't know any efficient way to do this

Find one of the original factors



McMaster ranked 78th in world

McMaster jumped 35 spots from its previous ranking

News

$55M investment will help McMaster spin-off company put cancer in the crosshairs

Social

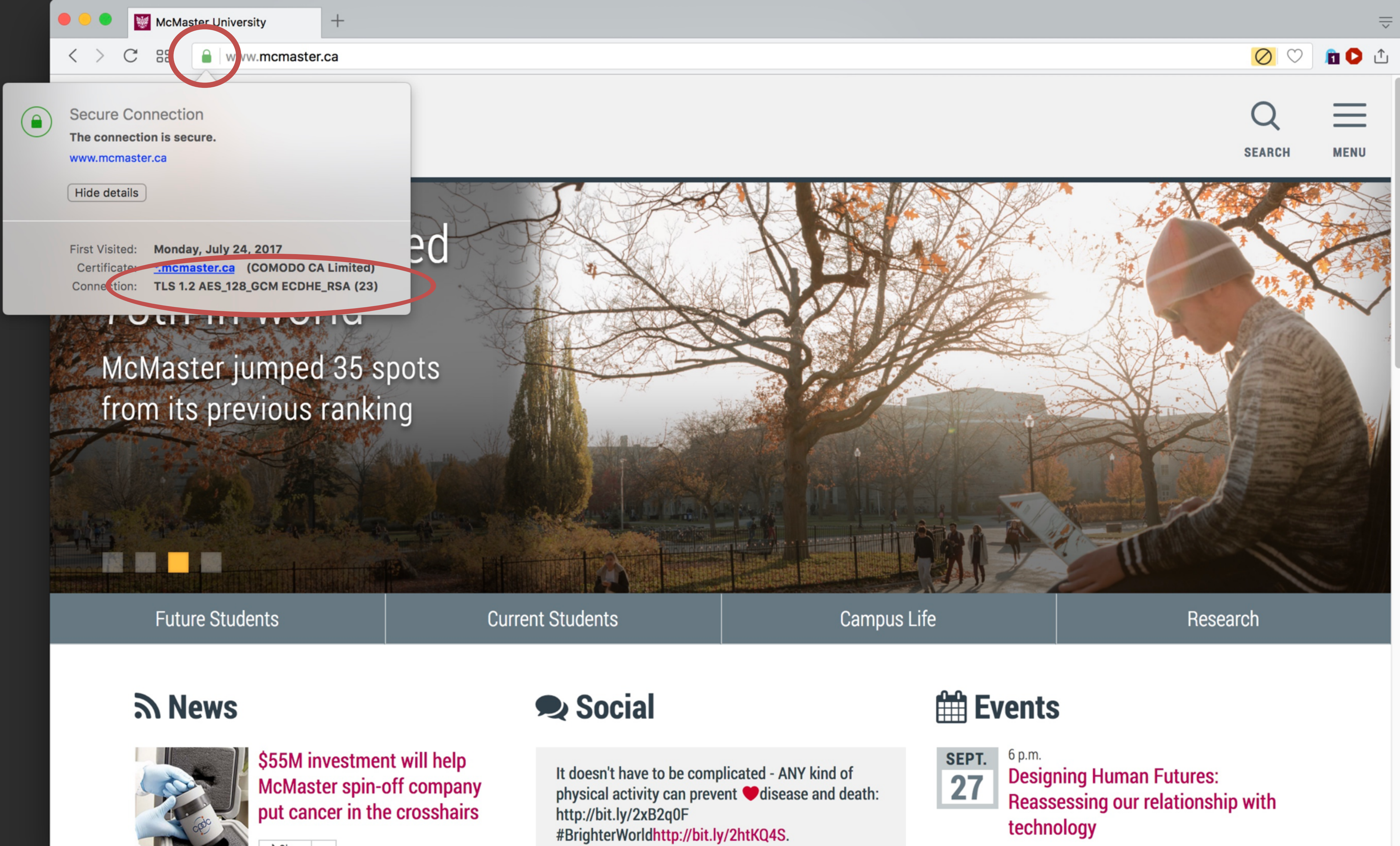
It doesn't have to be complicated - ANY kind of physical activity can prevent ❤disease and death: http://bit.ly/2xB2q0F #BrighterWorldhttp://bit.ly/2htKQ4S.

Events

SEPT. 27

6 p.m.

Designing Human Futures: Reassessing our relationship with technology



Secure Connection

The connection is secure.

www.mcmaster.ca

First Visited: Monday, July 24, 2017

Certificate: *.mcmaster.ca (COMODO CA Limited)

Connection: TLS 1.2 AES_128_GCM ECDHE_RSA (23)

McMaster jumped 35 spots from its previous ranking

News

$55M investment will help McMaster spin-off company put cancer in the crosshairs

Social

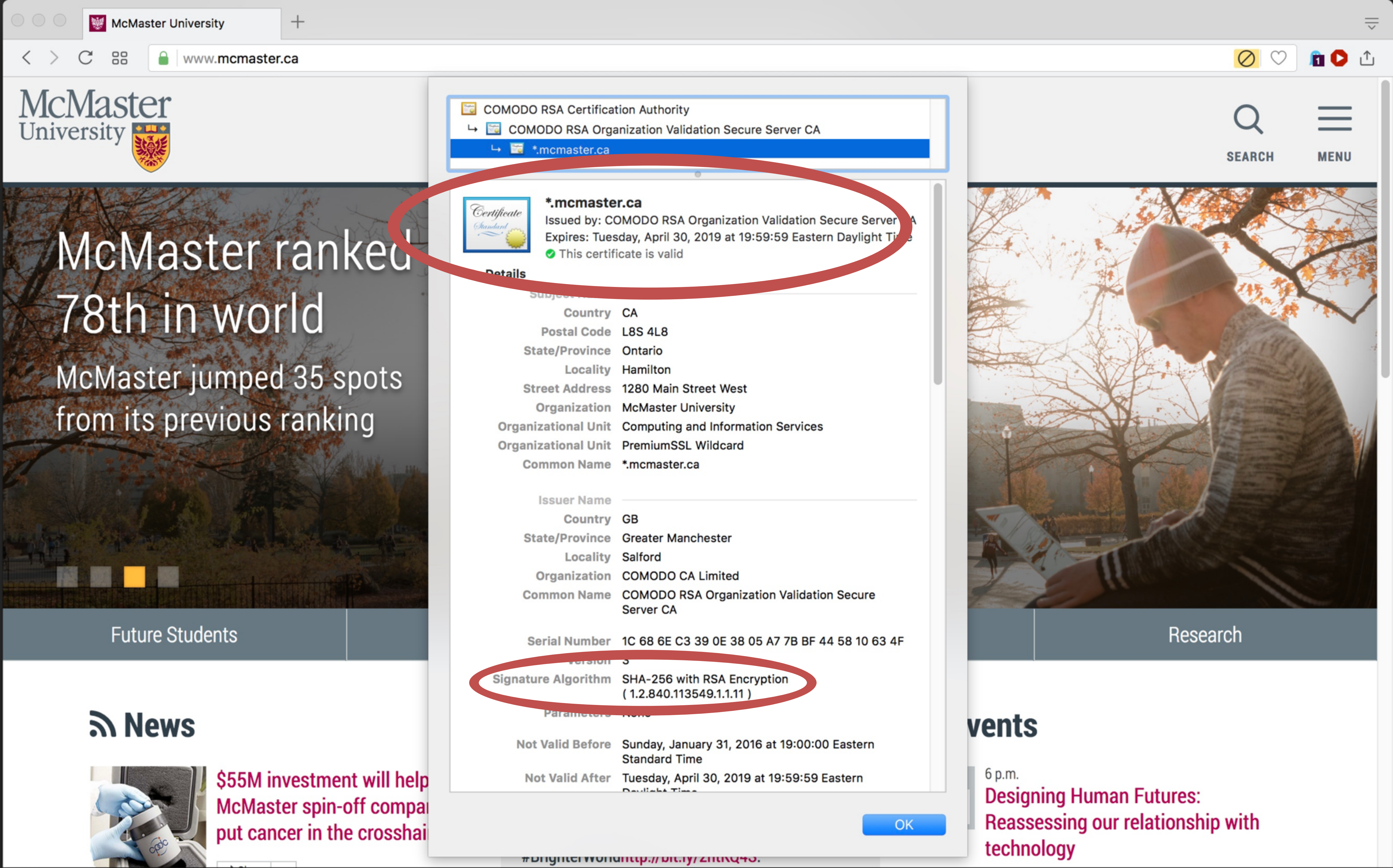
It doesn't have to be complicated - ANY kind of physical activity can prevent ❤disease and death: http://bit.ly/2xB2q0F #BrighterWorldhttp://bit.ly/2htKQ4S.

Events

SEPT. 27

6 p.m.

Designing Human Futures: Reassessing our relationship with technology


McMaster University
www.mcmaster.ca
McMaster University
SEARCH
MENU
McMaster ranked 78th in world
McMaster jumped 35 spots from its previous ranking
Future Students
Research
News
$55M investment will help McMaster spin-off compa put cancer in the crosshai
vents
6 p.m.
Designing Human Futures: Reassessing our relationship with technology
OK

COMODO RSA Certification Authority
↳ COMODO RSA Organization Validation Secure Server CA
↳ *.mcmaster.ca

***.mcmaster.ca**
Issued by: COMODO RSA Organization Validation Secure Server CA
Expires: Tuesday, April 30, 2019 at 19:59:59 Eastern Daylight Time
✓ This certificate is valid

Details

Subject Name

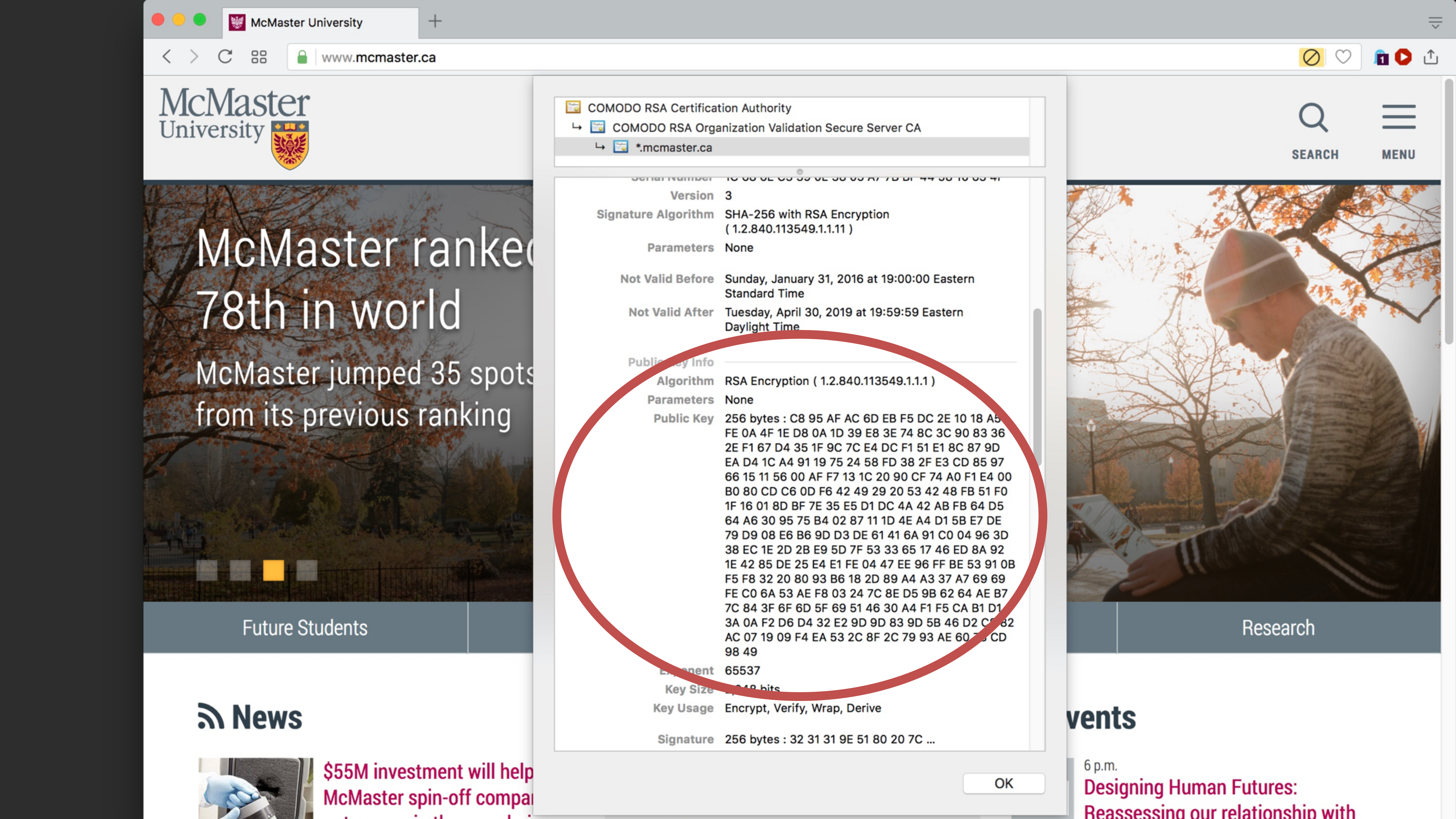
Country	CA
Postal Code	L8S 4L8
State/Province	Ontario
Locality	Hamilton
Street Address	1280 Main Street West
Organization	McMaster University
Organizational Unit	Computing and Information Services
Organizational Unit	PremiumSSL Wildcard
Common Name	*.mcmaster.ca

Issuer Name

Country	GB
State/Province	Greater Manchester
Locality	Salford
Organization	COMODO CA Limited
Common Name	COMODO RSA Organization Validation Secure Server CA

Serial Number	1C 68 6E C3 39 0E 38 05 A7 7B BF 44 58 10 63 4F
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	None

Not Valid Before	Sunday, January 31, 2016 at 19:00:00 Eastern Standard Time
Not Valid After	Tuesday, April 30, 2019 at 19:59:59 Eastern Daylight Time



COMODO RSA Certification Authority
↳ COMODO RSA Organization Validation Secure Server CA
↳ *.mcmaster.ca

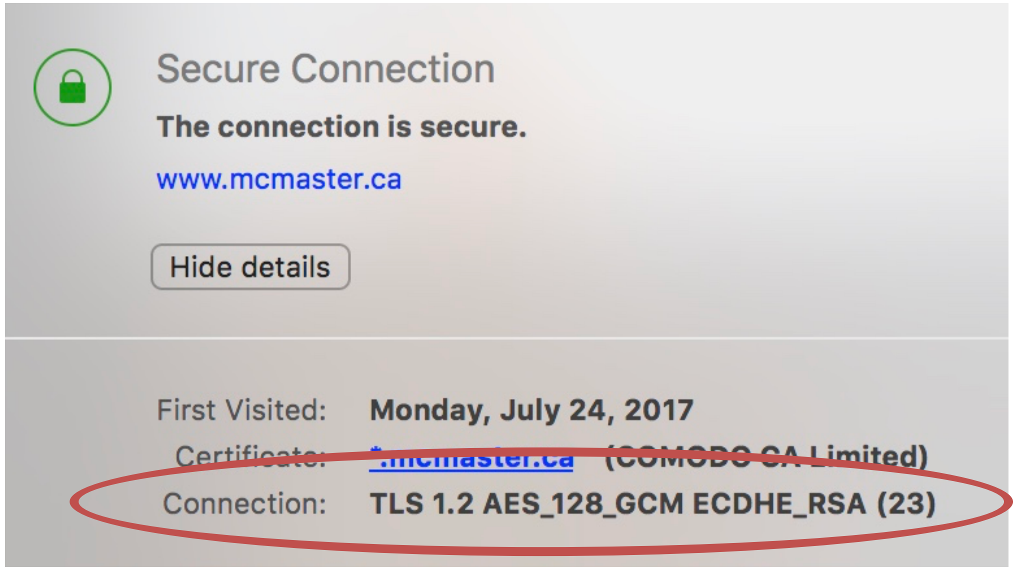
```
Version              3
Signature Algorithm  SHA-256 with RSA Encryption
                     ( 1.2.840.113549.1.1.11 )
Parameters           None

Not Valid Before     Sunday, January 31, 2016 at 19:00:00 Eastern
                     Standard Time
Not Valid After      Tuesday, April 30, 2019 at 19:59:59 Eastern
                     Daylight Time

Public Key Info
Algorithm            RSA Encryption ( 1.2.840.113549.1.1.1 )
Parameters           None
Public Key           256 bytes : C8 95 AF AC 6D EB F5 DC 2E 10 18 A5
                     FE 0A 4F 1E D8 0A 1D 39 E8 3E 74 8C 3C 90 83 36
                     2E F1 67 D4 35 1F 9C 7C E4 DC F1 51 E1 8C 87 9D
                     EA D4 1C A4 91 19 75 24 58 FD 38 2F E3 CD 85 97
                     66 15 11 56 00 AF F7 13 1C 20 90 CF 74 A0 F1 E4 00
                     B0 80 CD C6 0D F6 42 49 29 20 53 42 48 FB 51 F0
                     1F 16 01 8D BF 7E 35 E5 D1 DC 4A 42 AB FB 64 D5
                     64 A6 30 95 75 B4 02 87 11 1D 4E A4 D1 5B E7 DE
                     79 D9 08 E6 B6 9D D3 DE 61 41 6A 91 C0 04 96 3D
                     38 EC 1E 2D 2B E9 5D 7F 53 33 65 17 46 ED 8A 92
                     1E 42 85 DE 25 E4 E1 FE 04 47 EE 96 FF BE 53 91 0B
                     F5 F8 32 20 80 93 B6 18 2D 89 A4 A3 37 A7 69 69
                     FE C0 6A 53 AE F8 03 24 7C 8E D5 9B 62 64 AE B7
                     7C 84 3F 6F 6D 5F 69 51 46 30 A4 F1 F5 CA B1 D1
                     3A 0A F2 D6 D4 32 E2 9D 9D 83 9D 5B 46 D2 [illegible] 82
                     AC 07 19 09 F4 EA 53 2C 8F 2C 79 93 AE 60 [illegible] CD
                     98 49
Exponent             65537
Key Size             2,048 bits
Key Usage            Encrypt, Verify, Wrap, Derive

Signature            256 bytes : 32 31 31 9E 51 80 20 7C ...
```

Cryptographic building blocks



Secure Connection

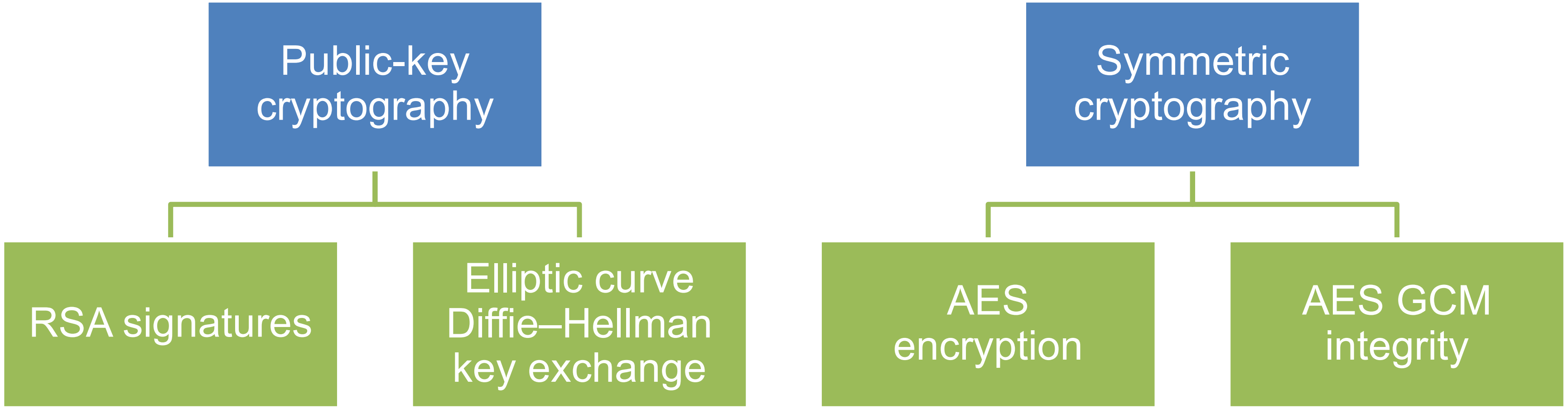
The connection is secure.

www.mcmaster.ca

First Visited: **Monday, July 24, 2017**

Certificate: *.mcmaster.ca (COMODO CA Limited)

Connection: **TLS 1.2 AES_128_GCM ECDHE_RSA (23)**



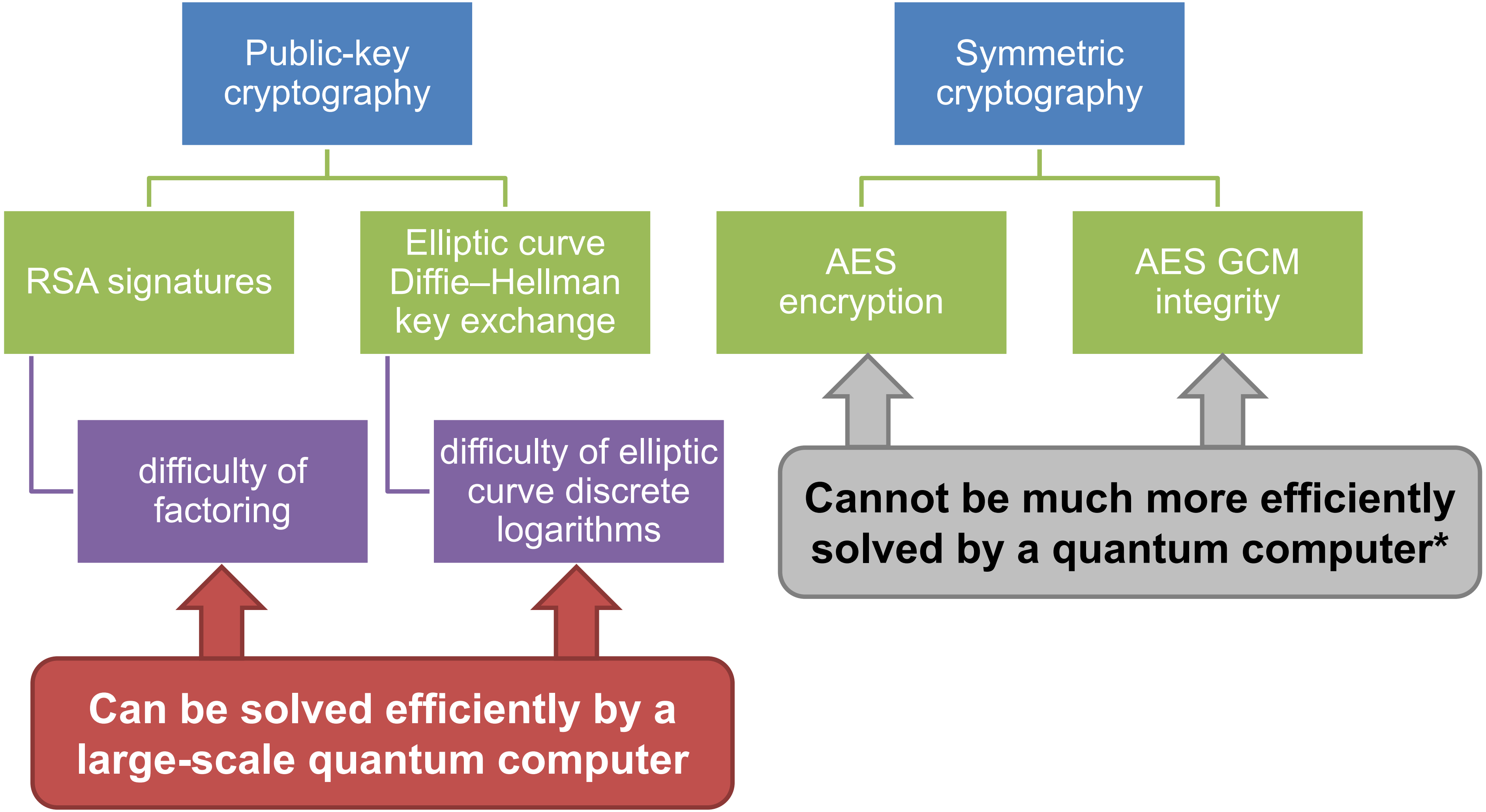
Public-key cryptography

- RSA signatures
- Elliptic curve Diffie–Hellman key exchange

Symmetric cryptography

- AES encryption
- AES GCM integrity

Cryptographic building blocks



Public-key cryptography

RSA signatures

Elliptic curve Diffie–Hellman key exchange

difficulty of factoring

difficulty of elliptic curve discrete logarithms

Can be solved efficiently by a large-scale quantum computer

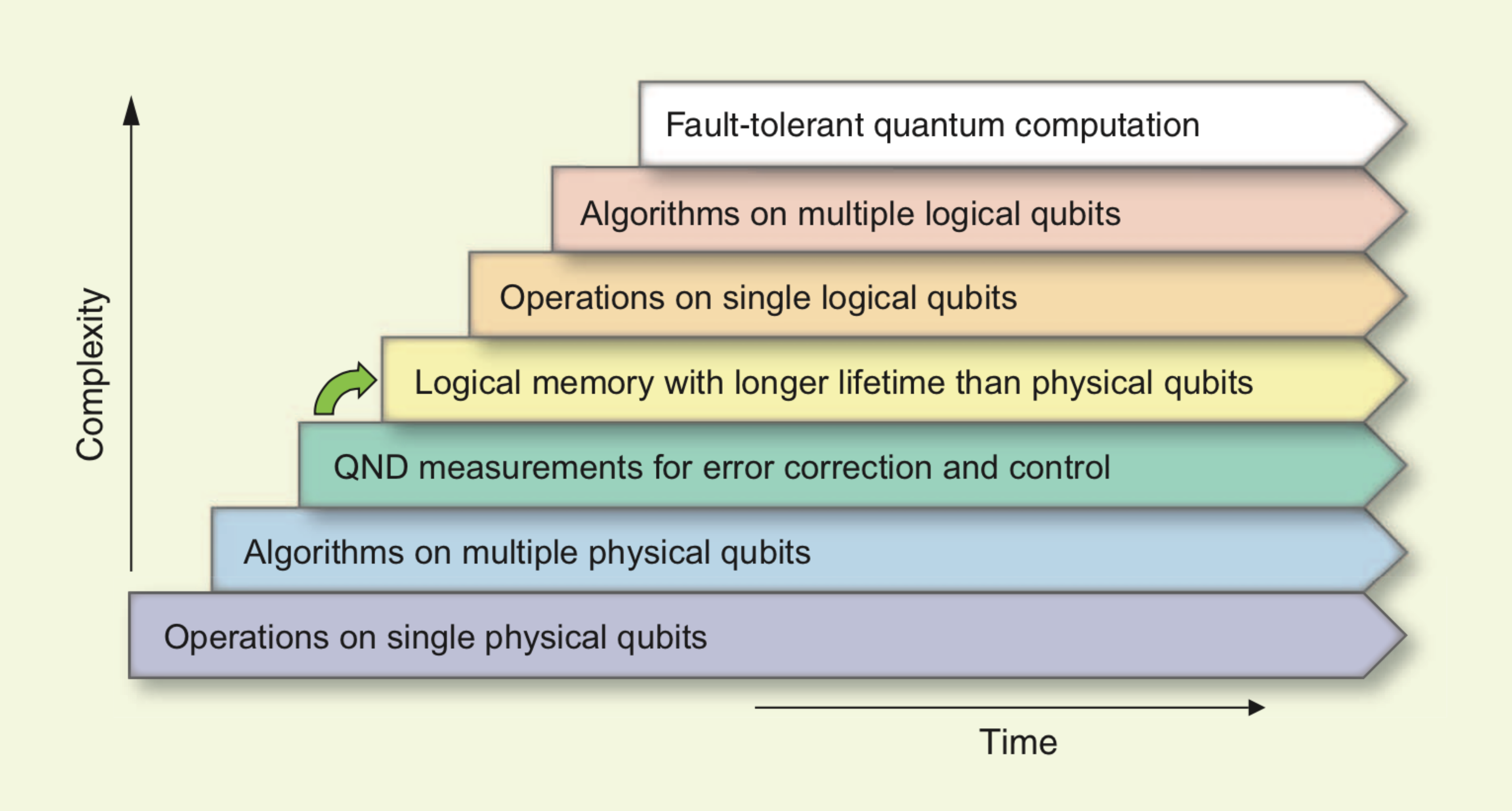
Symmetric cryptography

AES encryption

AES GCM integrity

Cannot be much more efficiently solved by a quantum computer*

When will a large-scale quantum computer be built?


Fault-tolerant quantum computation
Algorithms on multiple logical qubits
Operations on single logical qubits
Logical memory with longer lifetime than physical qubits
QND measurements for error correction and control
Algorithms on multiple physical qubits
Operations on single physical qubits
Complexity
Time

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

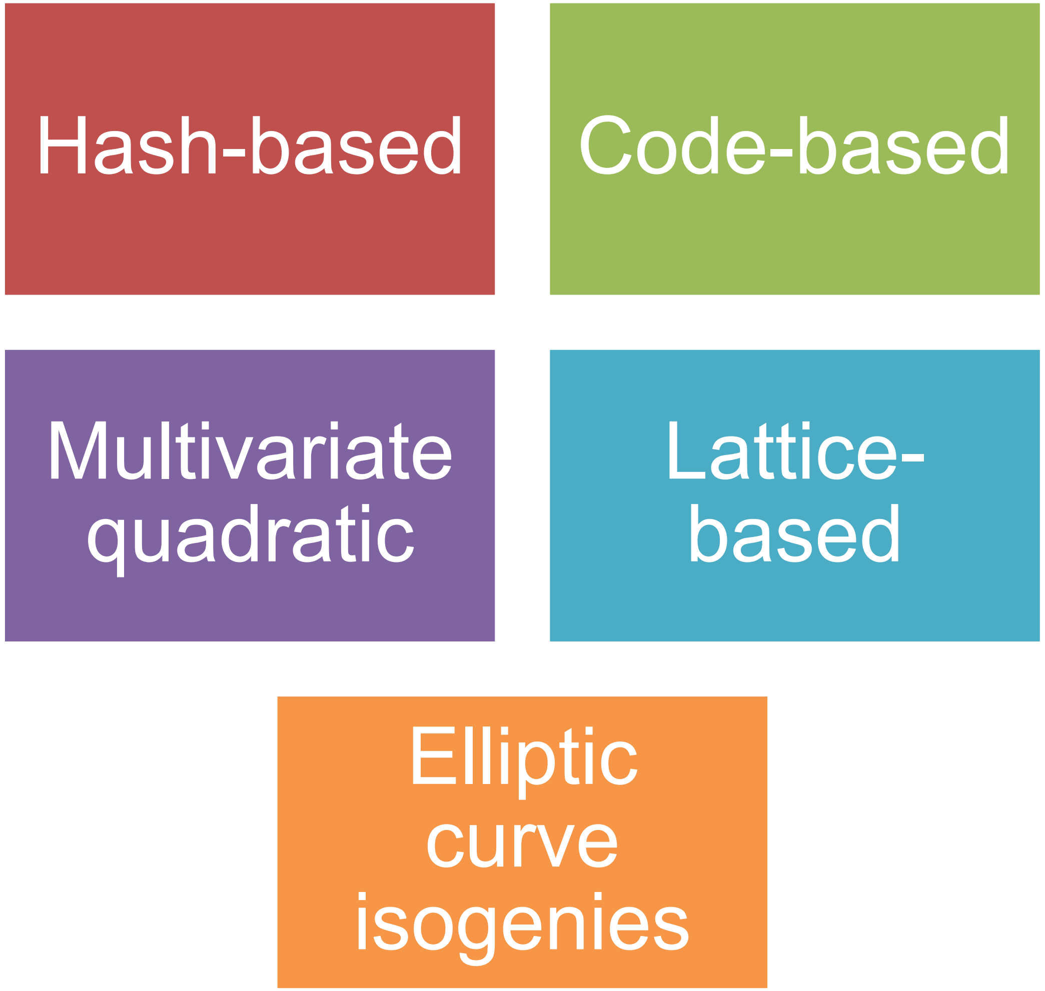
Post-quantum cryptography

a.k.a. quantum-resistant algorithms

Cryptography believed to be resistant to attacks by quantum computers

But not as well-studied as current encryption

- Less confident in its security
- More implementation tradeoffs



Hash-based

Code-based

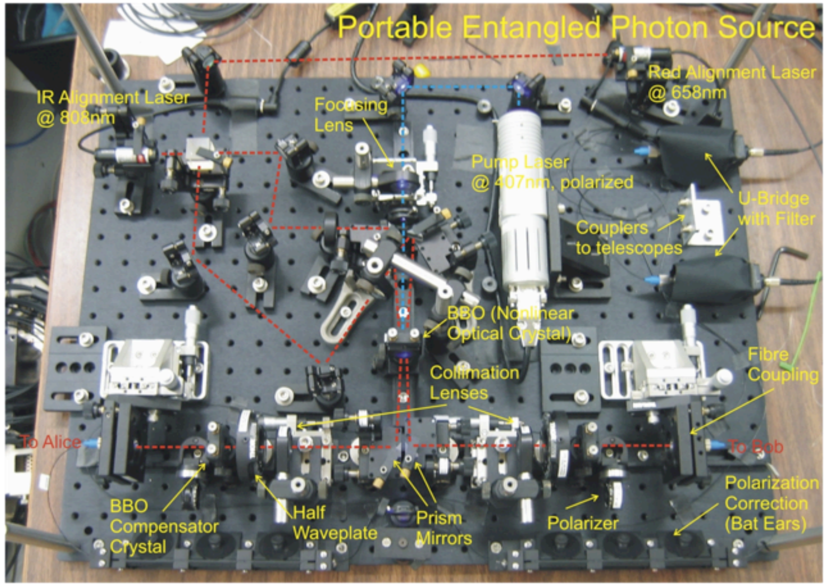
Multivariate quadratic

Lattice-based

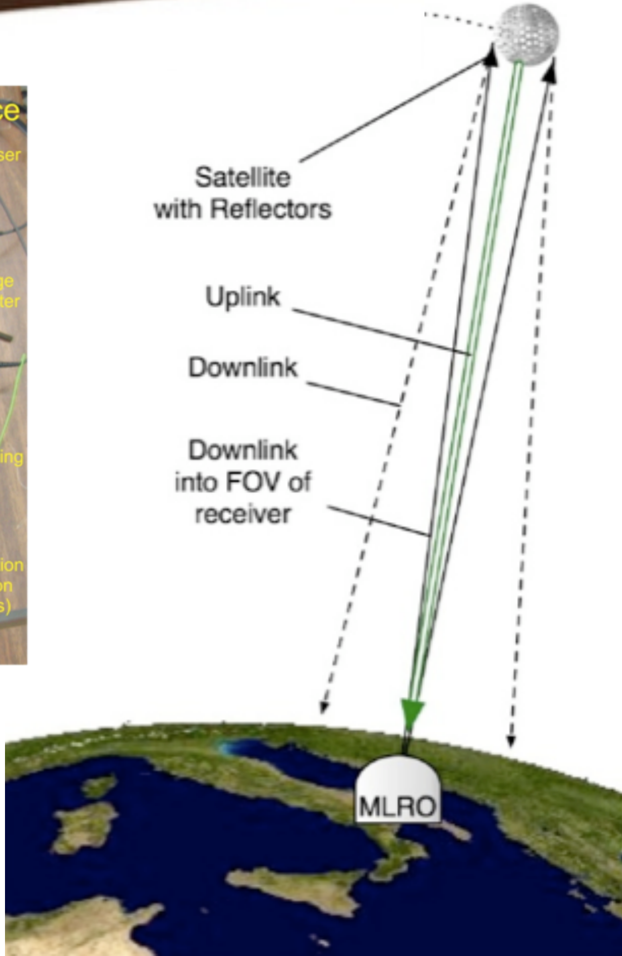
Elliptic curve isogenies

Quantum key distribution

Uses quantum mechanics to protect information

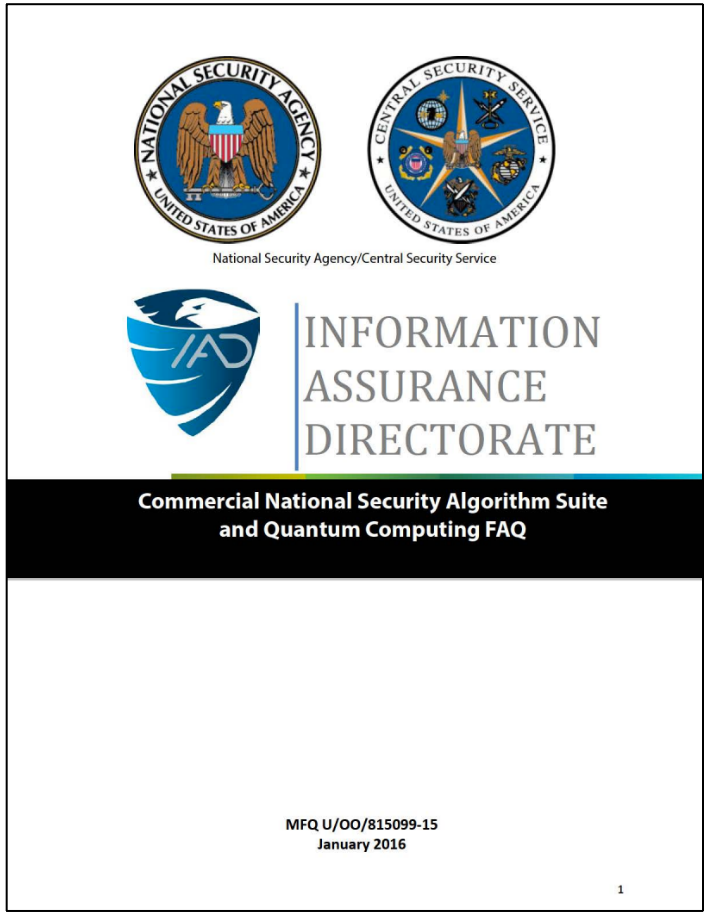

Portable Entangled Photon Source
IR Alignment Laser @ 808nm
Focusing Lens
Red Alignment Laser @ 658nm
Pump Laser @ 407nm, polarized
U-Bridge with Filter
Couplers to telescopes
BBO (Nonlinear Optical Crystal)
Collimation Lenses
Fibre Coupling
To Alice
To Bob
Polarization Correction (Bat Ears)
BBO Compensator Crystal
Half Waveplate
Prism Mirrors
Polarizer

Doesn't require a full quantum computer



But does require new communications infrastructure and hardware

Standardizing post-quantum cryptography



National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

Commercial National Security Algorithm Suite and Quantum Computing FAQ

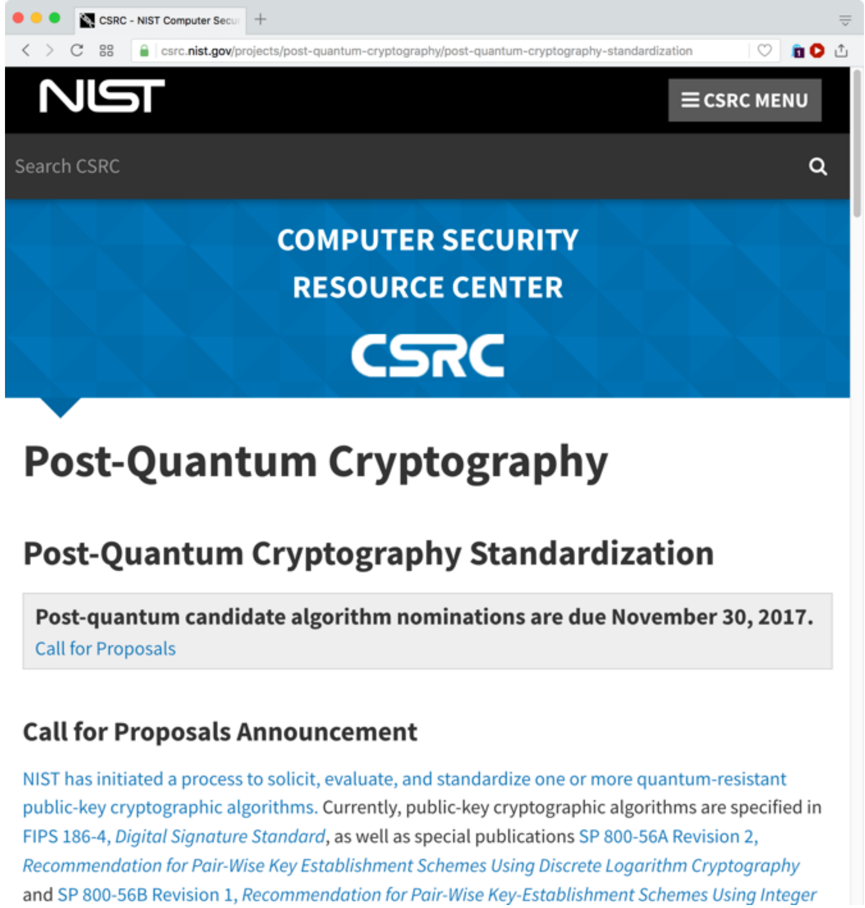
MFQ U/OO/815099-15
January 2016

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


CSRC - NIST Computer Secu
csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
NIST
☰ CSRC MENU
Search CSRC
COMPUTER SECURITY RESOURCE CENTER
CSRC

Post-Quantum Cryptography

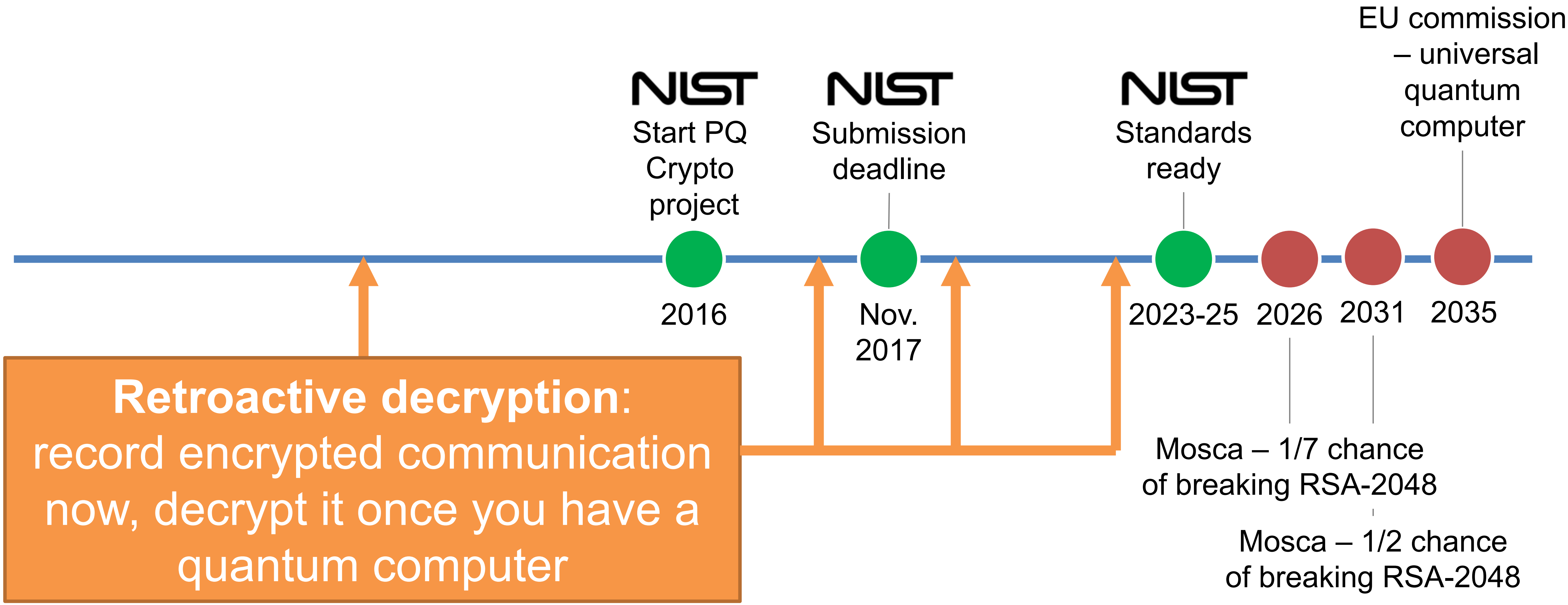
Post-Quantum Cryptography Standardization

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

Call for Proposals Announcement

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

Timeline



NIST Start PQ Crypto project

2016

NIST Submission deadline

Nov. 2017

NIST Standards ready

2023-25

2026

2031

2035

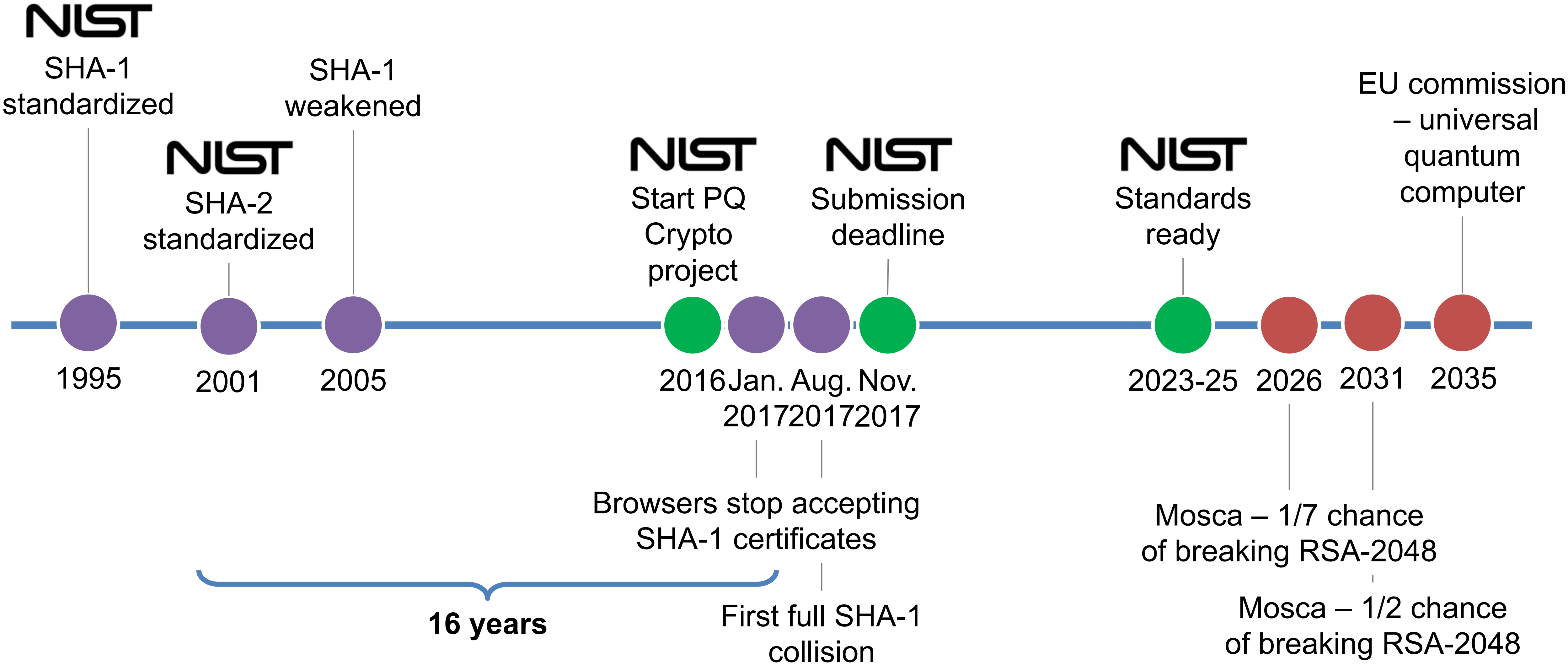
EU commission – universal quantum computer

Mosca – 1/7 chance of breaking RSA-2048

Mosca – 1/2 chance of breaking RSA-2048

Retroactive decryption: record encrypted communication now, decrypt it once you have a quantum computer

Timeline



NIST SHA-1 standardized — 1995

NIST SHA-2 standardized — 2001

SHA-1 weakened — 2005

NIST Start PQ Crypto project — 2016

Jan. 2017 — Browsers stop accepting SHA-1 certificates

Aug. 2017 — First full SHA-1 collision

Nov. 2017 — NIST Submission deadline

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

16 years

What should you do?

"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"

SNAKE OIL LINIMENT

THE STRONGEST AND BEST LINIMENT KNOWN FOR PAIN AND LAMENESS.

USED EXTERNAL ONLY

FOR RHEUMATISM NEURALGIA SCIATICA LAME BACK LUMBAGO CONTRACTED CORDS TOOTHACHE SPRAINS SWELLINGS ETC.

CLARK STANLEY'S SNAKE OIL LINIMENT

TRADE MARK REGISTERED

FOR FROST BITES CHILL BLAINS BRUISES SORE THROAT BITES OF ANIMALS INSECTS AND REPTILES.

GOOD FOR MAN AND BEAST

IT GIVES IMMEDIATE RELIEF.

IS GOOD FOR EVERYTHING A LINIMENT OUGHT TO BE GOOD FOR

Manufactured by CLARK STANLEY Snake Oil Liniment Company Providence, R. I.

Clark Stanley's Snake Oil Liniment

Is for sale by all druggists. If your druggist fails to have it tell him he can get it for you from any wholesale druggists or it will be sent to you to any part of the United States or Canada upon the receipt of fifty cents in stamps by addressing the

Clark Stanley Snake Oil Liniment Co.

PROVIDENCE, R. I.

"proprietary algorithm"

"secret technique"

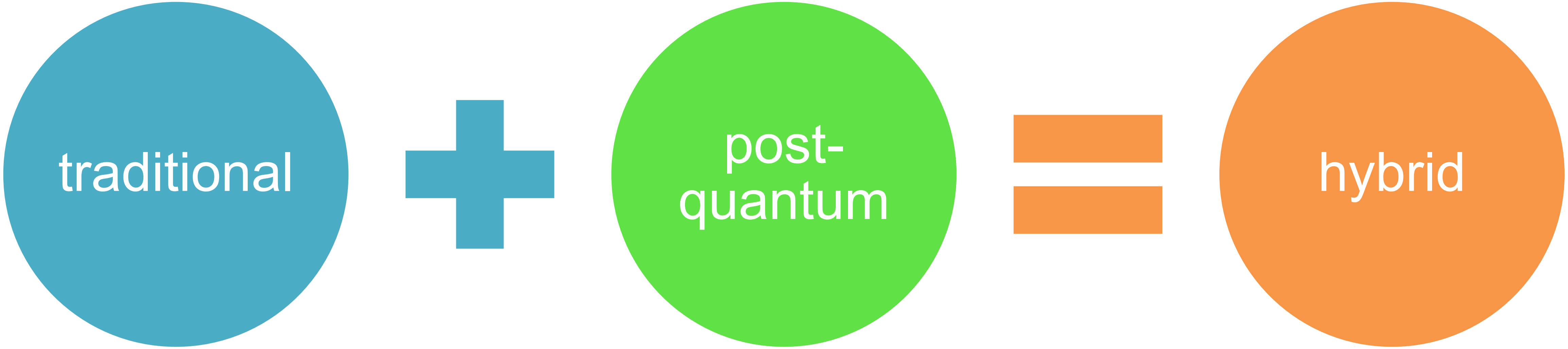
"virtual one-time pad"

"chaos encryption"

"unbreakable"

Cautious "hybrid" approach

- Some proposed post-quantum solutions could be broken
- **Hybrid approach**: use traditional and post-quantum simultaneously to reduce risk during transition
- Focus on algorithms that advance through NIST process



Quantum-safe crypto in Canada

Academia

- Quantum-Safe Canada initiative
  - McMaster University
  - University of Waterloo (lead)
  - others
- Several NIST submissions

Industry

- Post-quantum crypto startups
- QKD startups
- Quantum risk assessment consulting firms

Open Quantum Safe project

Open-source software project for prototyping and testing post-quantum cryptography

https://openquantumsafe.org

Understanding the impact of quantum computers on information security

Douglas Stebila

McMaster University

Encryption used throughout financial infrastructure

Some types of encryption would be broken by quantum computers

Need to start preparing for the quantum transition

- **NIST post-quantum crypto standardization**
- **Quantum risk assessment**
- **Cautious adoption of standardized, hybrid solutions**

Survey paper

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

Open Quantum Safe project

- https://openquantumsafe.org/

This presentation:

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