Cryptography and finance: overview, trends, the quantum threat

Douglas Stebila

University of Waterloo

Funding acknowledgements:

NSERC CRSNG

Ontario Securities Commission Academy • September 12, 2018

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

Outline

- Cryptography in finance
- Background on cryptography
- Examples of cryptography in finance
- Recent trends in cryptography
- The threat of quantum computing

Cryptography in finance

Cryptography in finance

- Public data feeds
- Electronic signatures

- Inter-bank communications

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

- Merchant-bank communications

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

- Blockchain

Who mandates the use of information security?

Privacy legislation

- PIPEDA – federally regulated private sector organizations
- Privacy Act – federally regulated public bodies

PIPEDA principle #7

- An organization should use safeguards appropriate to the sensitivity of the information
  - Legislation doesn’t specify which measures to apply

Who mandates the use of information security?

Industry bodies

- Payment Card Industry Data Security Standard (PCI-DSS)
  - Specifies technological measures to be used for systems that process credit card data

Who mandates the use of information security?

Principles

- Legislation
  - PIPEDA, Privacy Act, ...
- Regulators

Policies

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

Tools

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

Mathematics

- Specialist organizations
  - NIST, CFRG

Background on cryptography

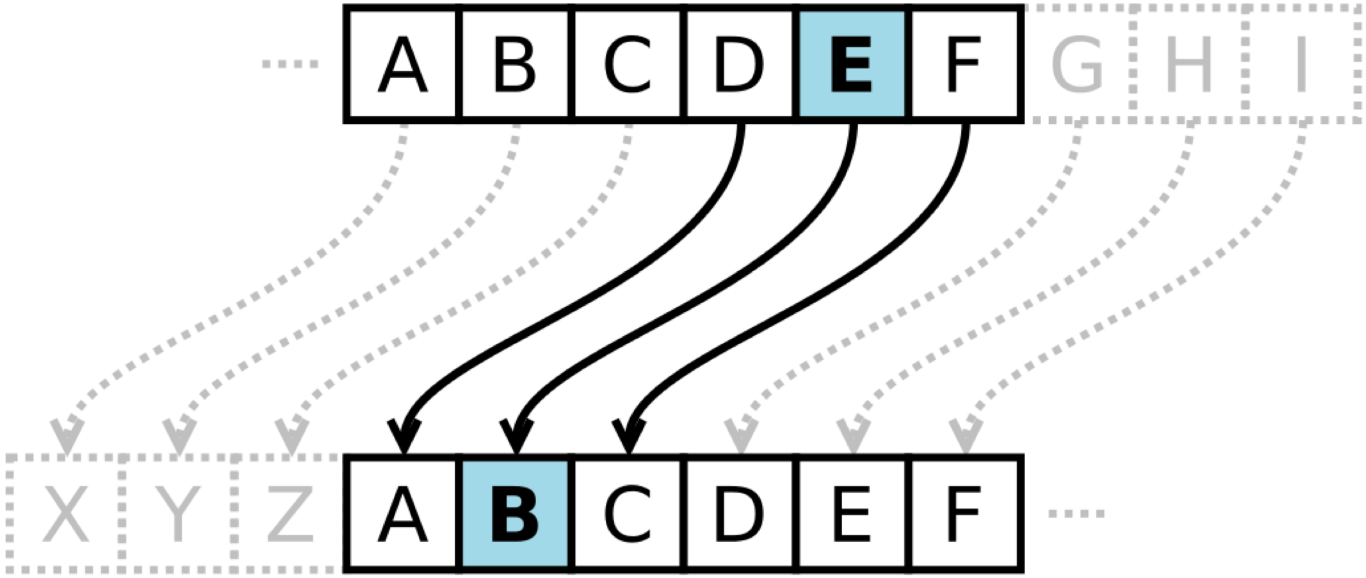
Security goals

- Confidentiality
- Integrity
- Availability

+ Authentication

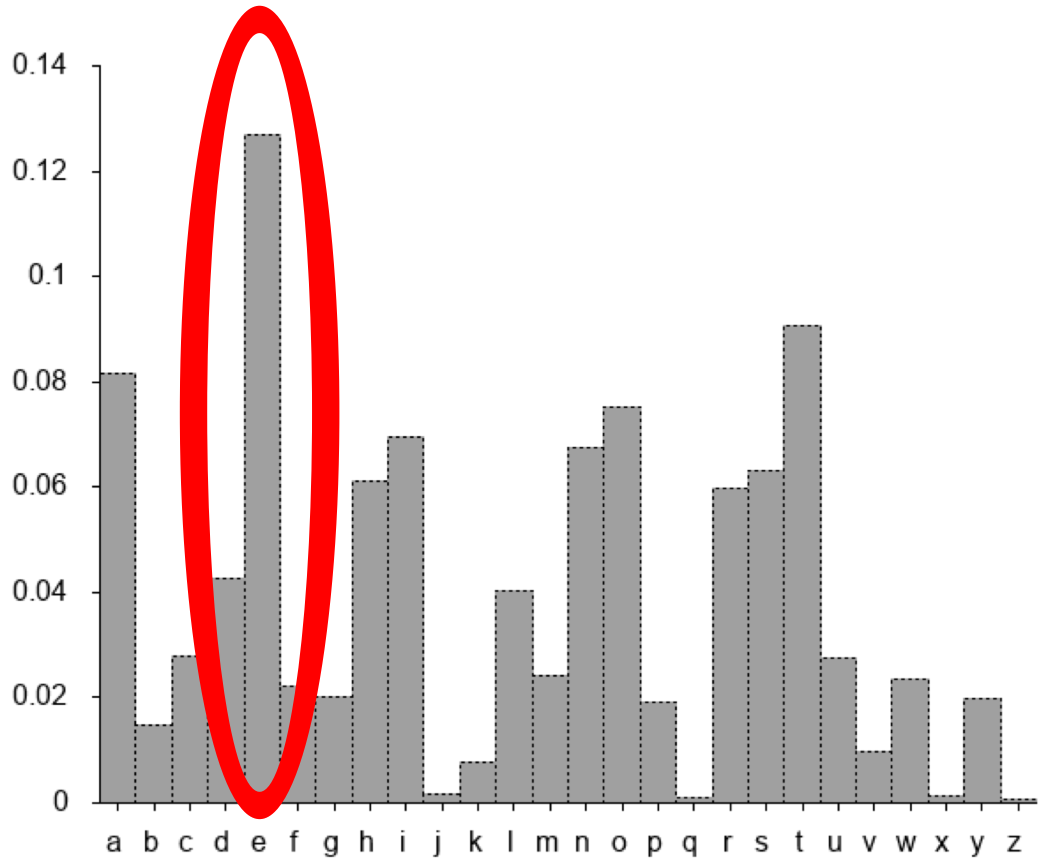
- Data at rest
- Data in transit
- Data while processing

Caesar cipher

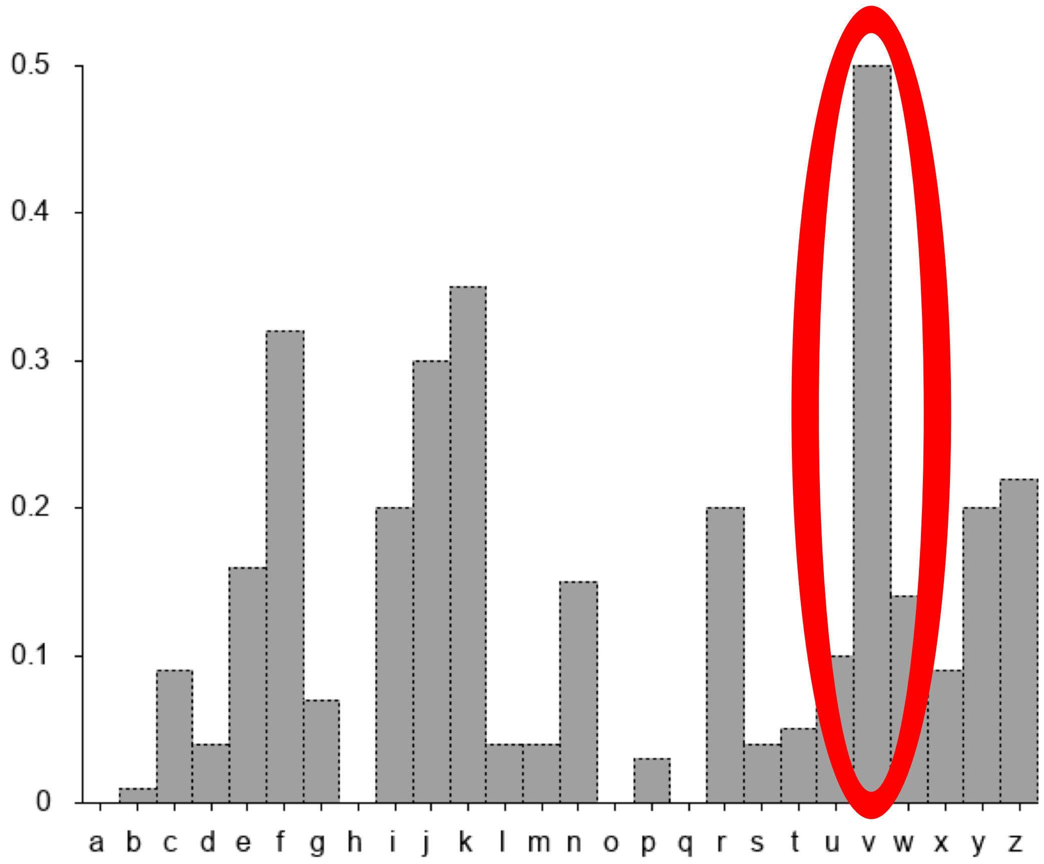


Caesar cipher

Frequency analysis

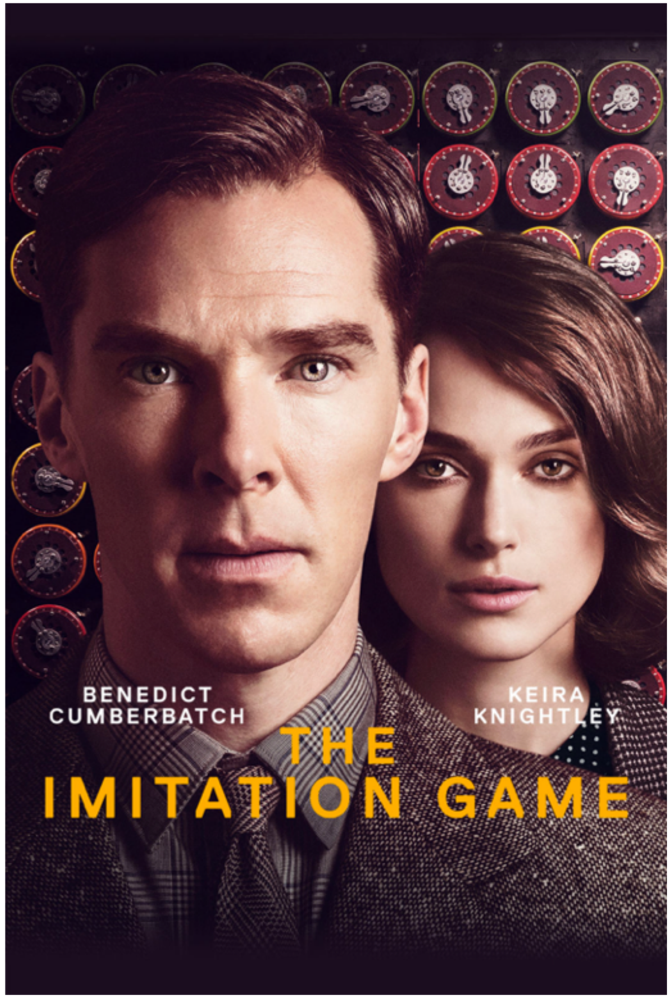


Frequency of letters in English text

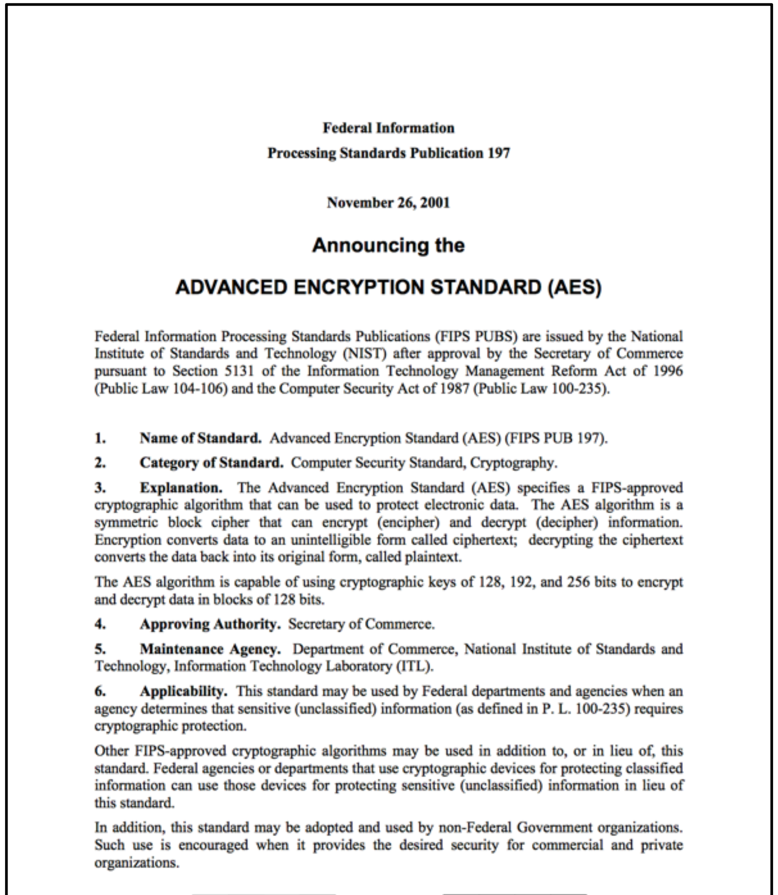


Frequency of letters in encrypted message

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).

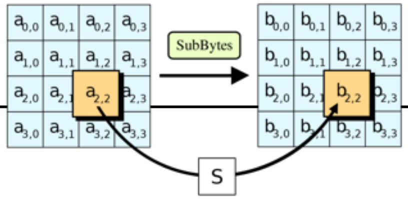
1. **Name of Standard.** Advanced Encryption Standard (AES) (FIPS PUB 197).
2. **Category of Standard.** Computer Security Standard, Cryptography.
3. **Explanation.** The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. 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.

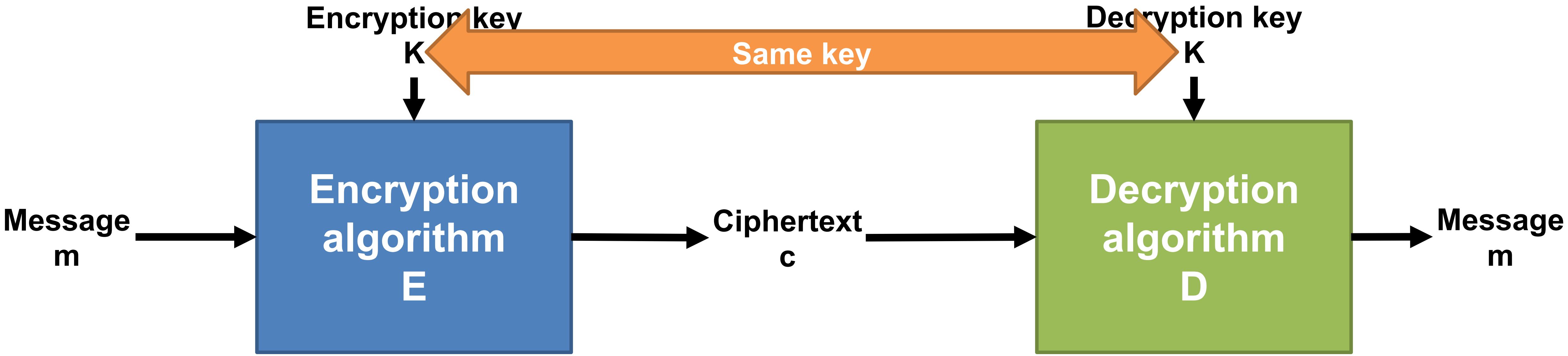
In addition, this standard may be adopted and used by non-Federal Government organizations. Such use is encouraged when it provides the desired security for commercial and private organizations.



<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:

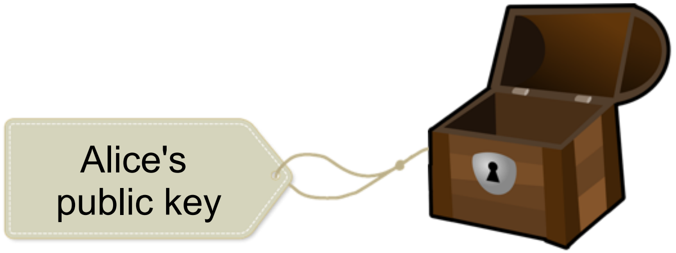
- public key
- private key

Publish the public key

Anyone can use the public key to encrypt

Only the person with the private key can decrypt

public key private key



encrypt a message

Public key cryptography – RSA algorithm

based on multiplying large secret prime numbers

115792089237316195423570985008687907853269984665640564039457584007913129640233

X

231584178474632390847141970017375815706
1516801582625928002

=

268156158598851941991480499964116922549587 ... 675544
712288744352806023382228442498426706061523151570959355071
320222072548089446870314794232112526291

Efficient for a computer to do

Public key cryptography – RSA algorithm

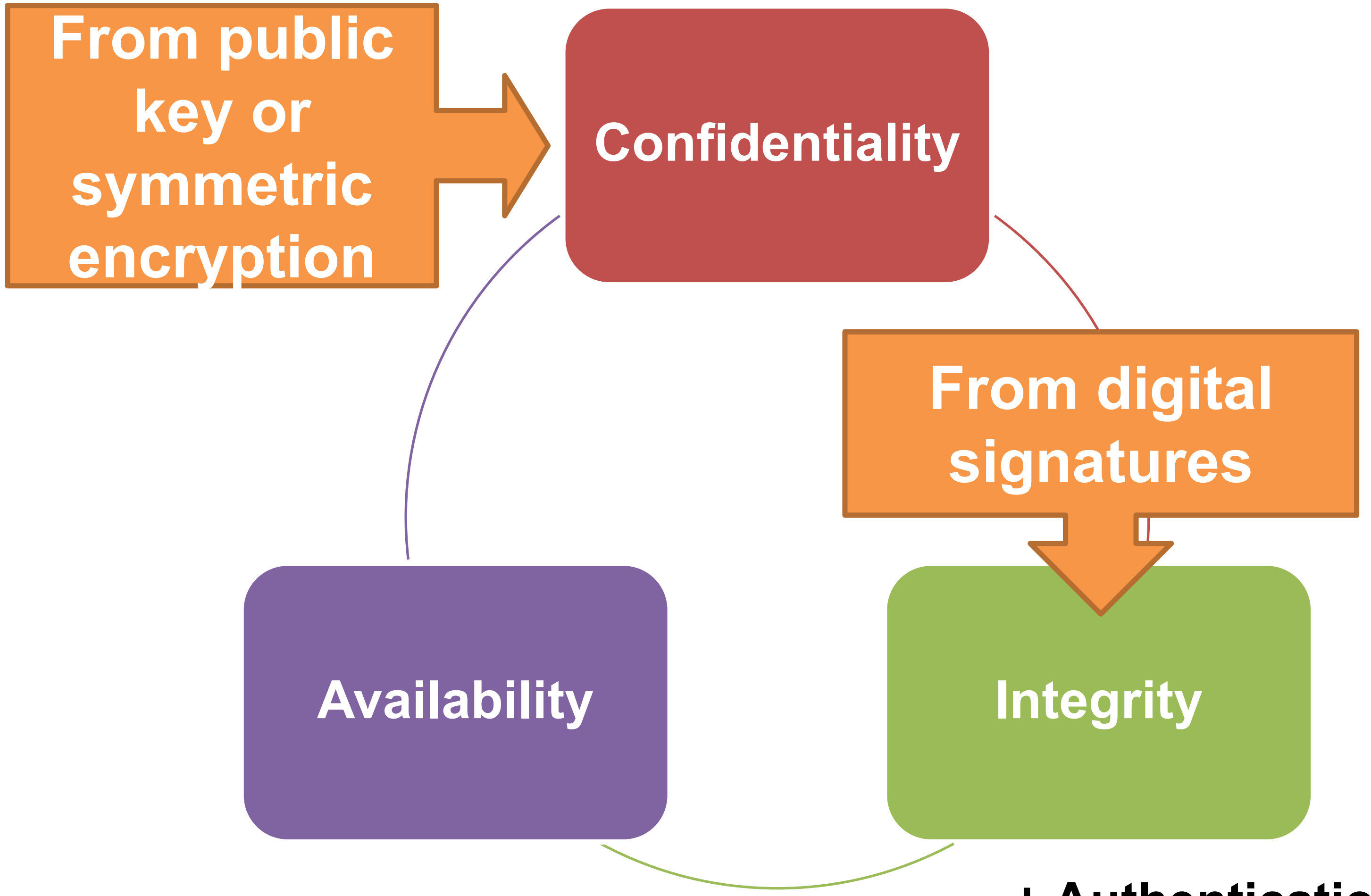
Given the product

268156158598851941991480499964116922549587316411847867554471228874435280602338222284 … 1
523151570959355071320222072548089 …
12526291

Don't know any efficient way to do this

Find one of the original factors

Security goals



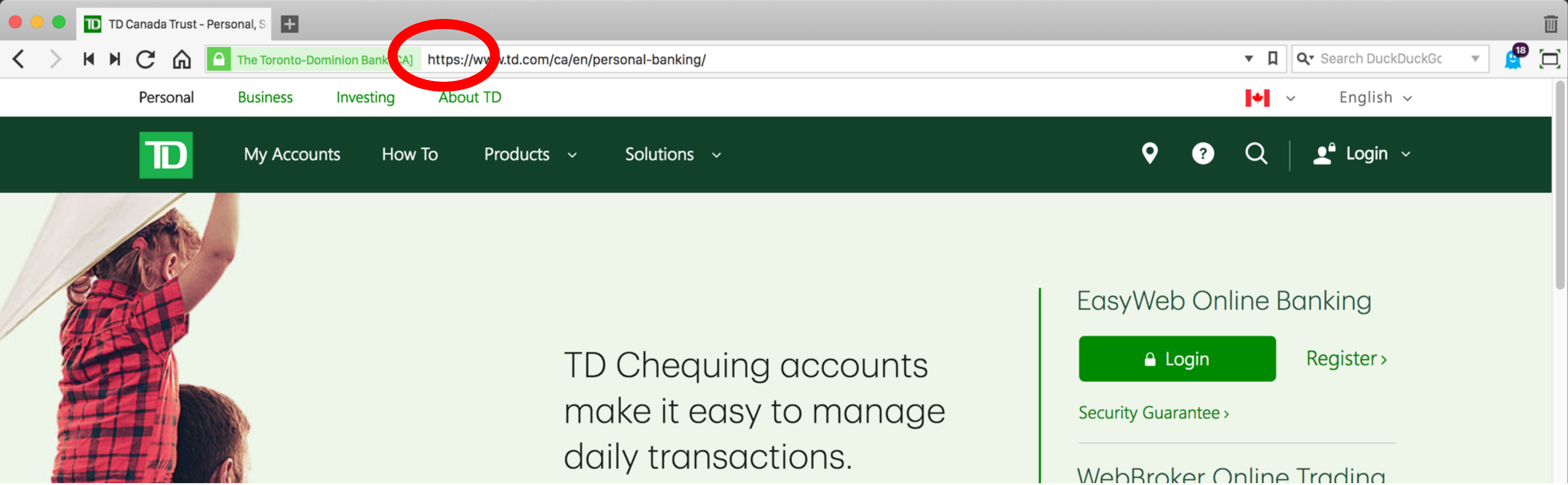
+ Authentication

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

Cryptography in finance

1) Confidentiality & integrity for data in transit

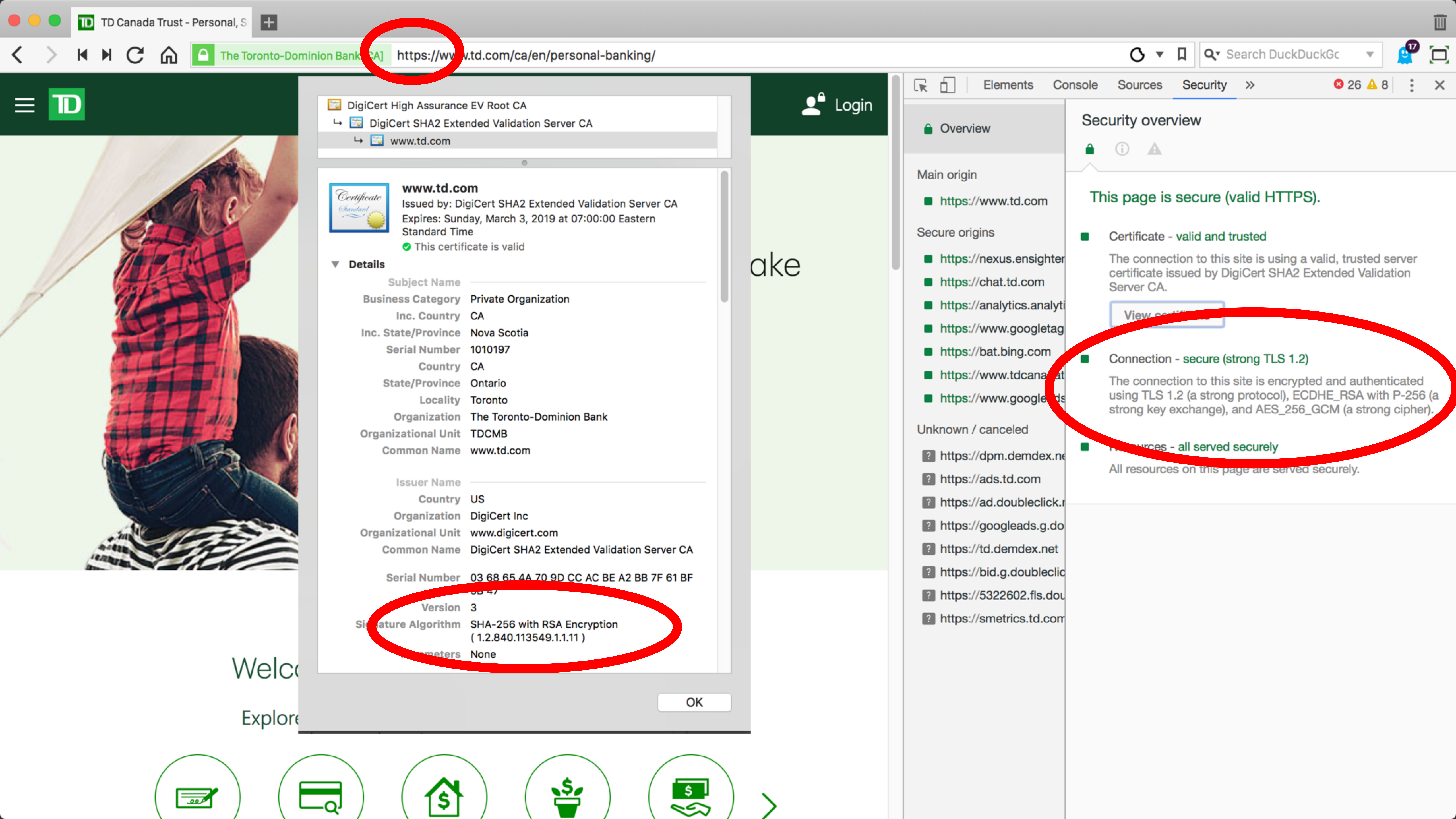
- Inter-bank communications
- Intra-bank communications
  - Virtual private networks (VPNs)
  - PKI
- Merchant-bank communications
- Customer-bank communications
  - EMV Chip-and-PIN
  - Online banking



TLS (Transport Layer Security) protocol

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

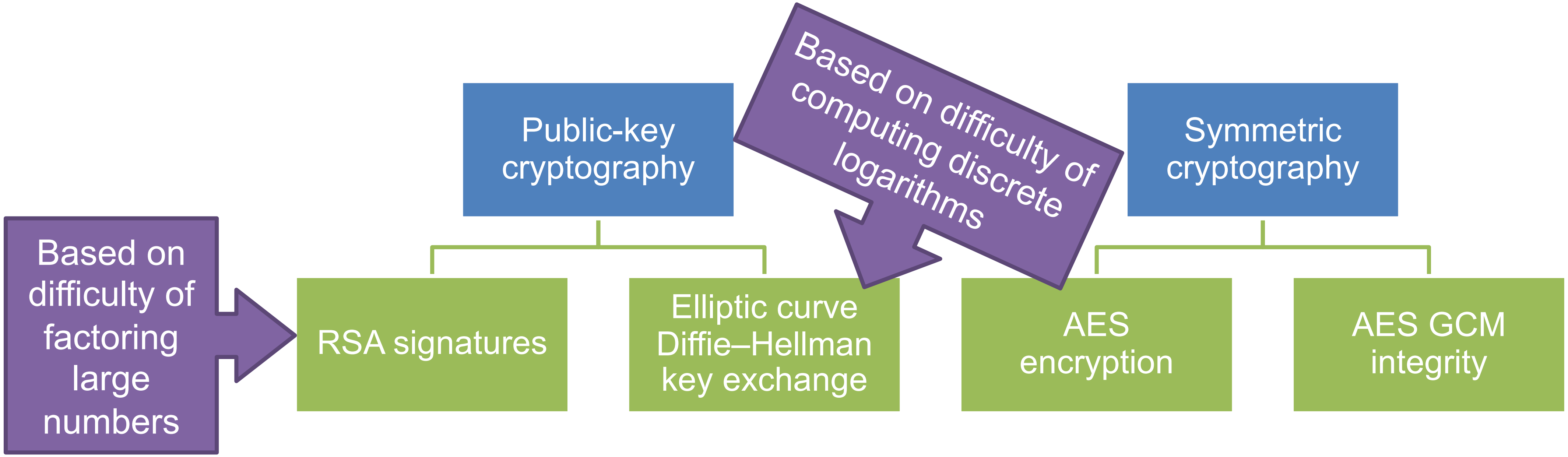
- The “s” in “https”
- The **most important cryptographic protocol on the Internet** — used to secure billions of connections every day.


TD Canada Trust - Personal, S
The Toronto-Dominion Bank [CA]
https://ww .td.com/ca/en/personal-banking/
Search DuckDuckGo
Login
DigiCert High Assurance EV Root CA
DigiCert SHA2 Extended Validation Server CA
www.td.com
www.td.com
Issued by: DigiCert SHA2 Extended Validation Server CA
Expires: Sunday, March 3, 2019 at 07:00:00 Eastern Standard Time
This certificate is valid
Details
Subject Name
Business Category Private Organization
Inc. Country CA
Inc. State/Province Nova Scotia
Serial Number 1010197
Country CA
State/Province Ontario
Locality Toronto
Organization The Toronto-Dominion Bank
Organizational Unit TDCMB
Common Name www.td.com
Issuer Name
Country US
Organization DigiCert Inc
Organizational Unit www.digicert.com
Common Name DigiCert SHA2 Extended Validation Server CA
Serial Number 03 68 65 4A 70 9D CC AC BE A2 BB 7F 61 BF
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters None
OK
Welco
Explore
ake
Elements
Console
Sources
Security
26
8
Overview
Main origin
https://www.td.com
Secure origins
https://nexus.ensighter
https://chat.td.com
https://analytics.analyti
https://www.googletag
https://bat.bing.com
https://www.tdcana
https://www.google
Unknown / canceled
https://dpm.demdex.ne
https://ads.td.com
https://ad.doubleclick.r
https://googleads.g.do
https://td.demdex.net
https://bid.g.doubleclic
https://5322602.fls.dou
https://smetrics.td.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 DigiCert SHA2 Extended Validation Server CA.
View certificate
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_256_GCM (a strong cipher).
Resources - all served securely
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).



2) Confidentiality for data at rest

- Encrypted databases, hard drives

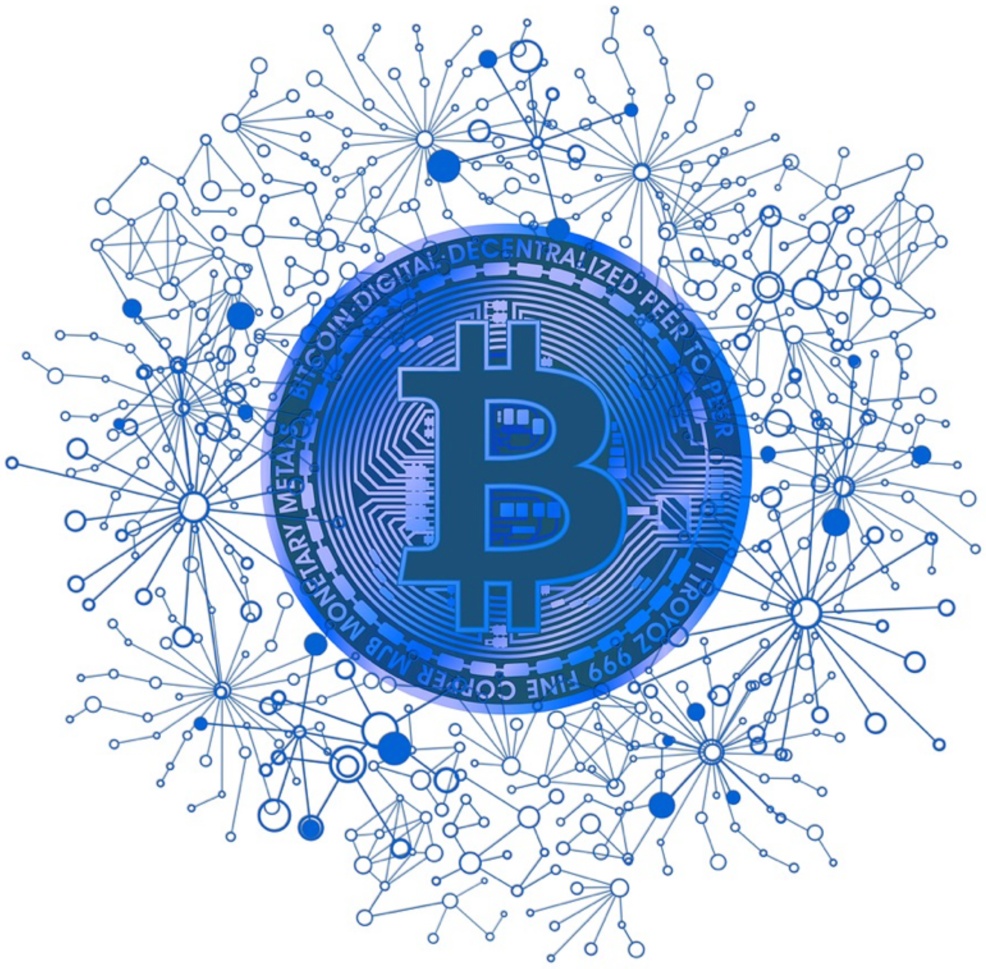
Database encryption

Cloud storage encryption

Hard drive encryption

3) Integrity of (public) data

- Electronic signatures
- Public data feeds
- Blockchain



https://www.maxpixel.net/Money-Bitcoin-Cryptocurrency-Blockchain-Virtual-3349122

Cryptocurrencies / cryptoassets

- Cryptography used to maintain a **distributed ledger** (“blockchain”)
  - Digital signatures used to **authenticate** messages on the ledger
  - Cryptographic “puzzles” used to **incentivize consensus** about ledger maintainers (“miners”)

- **Cryptocurrency**:
  - Messages on the ledger are parties authorizing transfer of tokens from themselves to another party
  - Parties are typically identified by **cryptographic key**, not by any real world identity

Tension between security and privacy

Enacting security requires visibility into potential attacks, ability to investigate leads, aggregate data

Privacy: ability of an entity to control access to information about themselves

- Cryptography **helps** security and privacy by preventing adversaries from unauthorized reading or modification of information

- Cryptography **hinders** security by decreasing visibility into attacks and making investigation harder

Backdoors, lawful access: "going dark"

- Let's design an encryption scheme that only the good guys can break
- Let's use a secure encryption scheme but give the good guys the key to decrypt
- Let's design a secure communication system that can be tapped by law enforcement

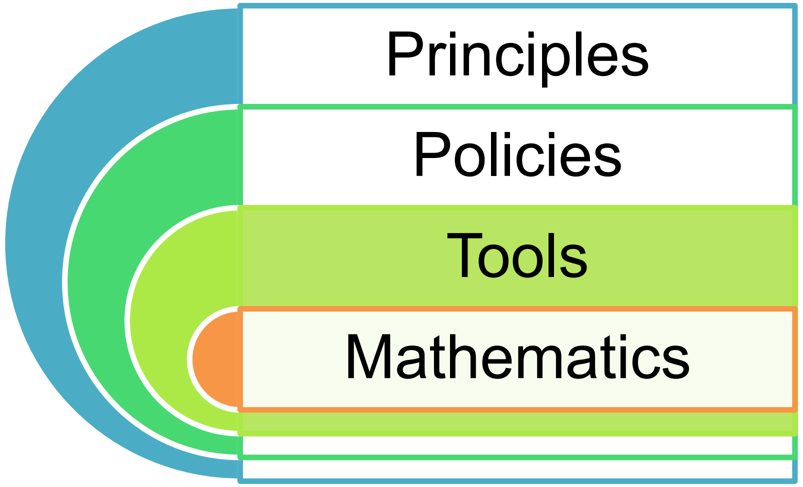
- Backdoors and key escrow introduce their own risks: there's a "**golden ticket**" key that opens everything
- Can we really keep that safe?
  - The cryptographic key
  - The procedures around its use
- Cryptographers and information security researchers almost universally believe it's not possible

Recent trends in cryptography

Recent trend 1: upgrading TLS

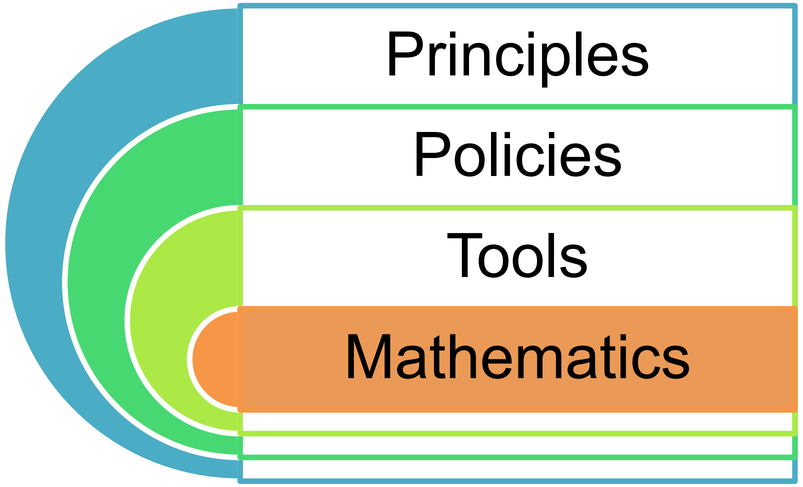
- TLS is the communications protocol used ubiquitously on the web
- Newest version (TLS 1.3) just standardized in August 2018

- Browser and server vendors already deploying
- Likely to become required for PCI-DSS, HIPAA, … in the next 5 years



Recent trend 2: encrypted cloud processing

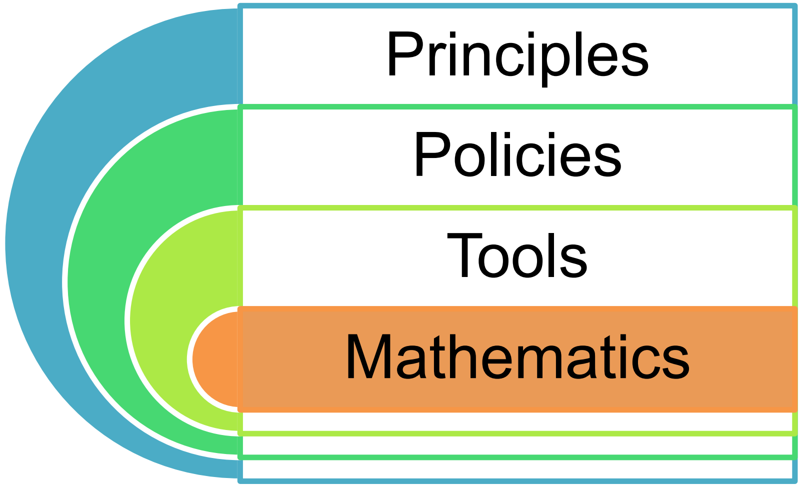
- Lots of companies store data encrypted on cloud servers
- But it has to be decrypted in order to be processed – so the cloud server can see the data
- “Fully homomorphic encryption” would allow cloud server to do computations on the encrypted data without seeing the original values
- Theoretically possible, but practically inefficient right now – 5+ years before viable



Recent trend 3: quantum computing

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

Need to migrate encryption to quantum-resistant algorithms



The threat of quantum computing to cryptography

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

Represent and process information using **quantum mechanics**

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

- 0 and 1

Quantum computers handle information as **qubits:**

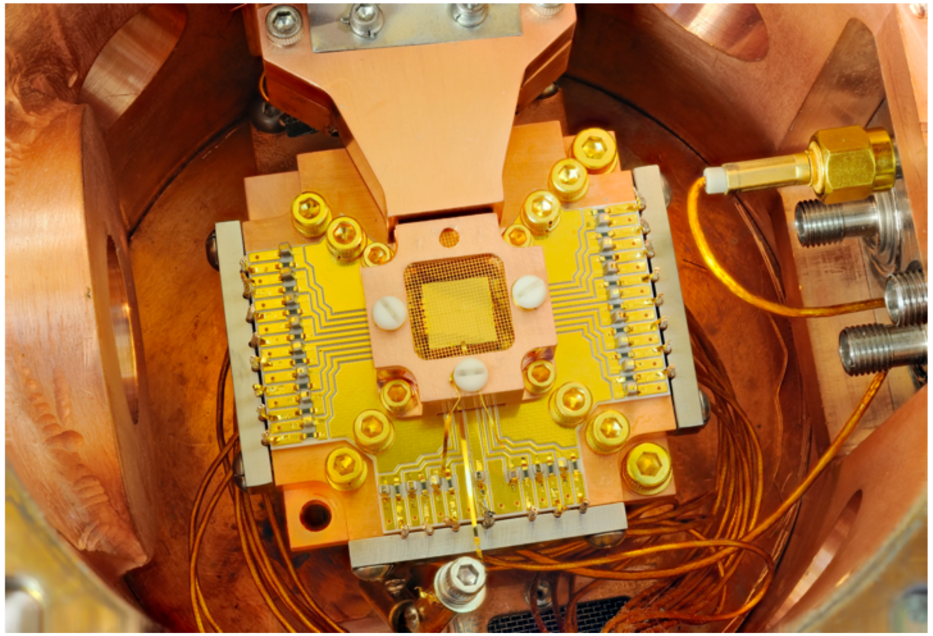
- Any "superposition" of 0 and 1

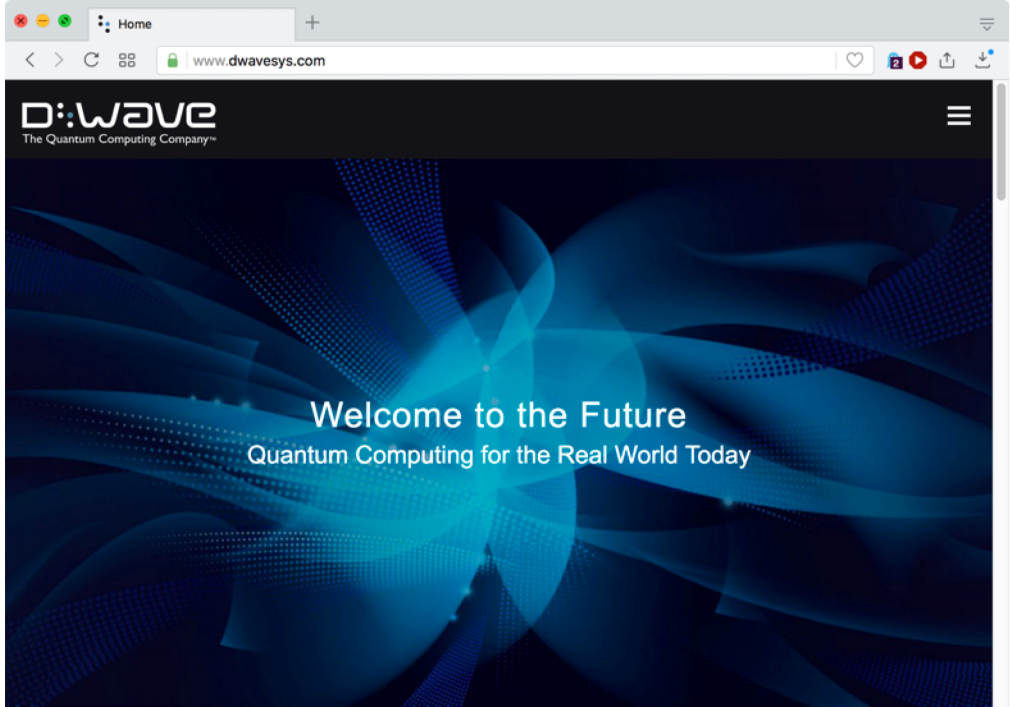
Processing information in superposition can dramatically speed some computations

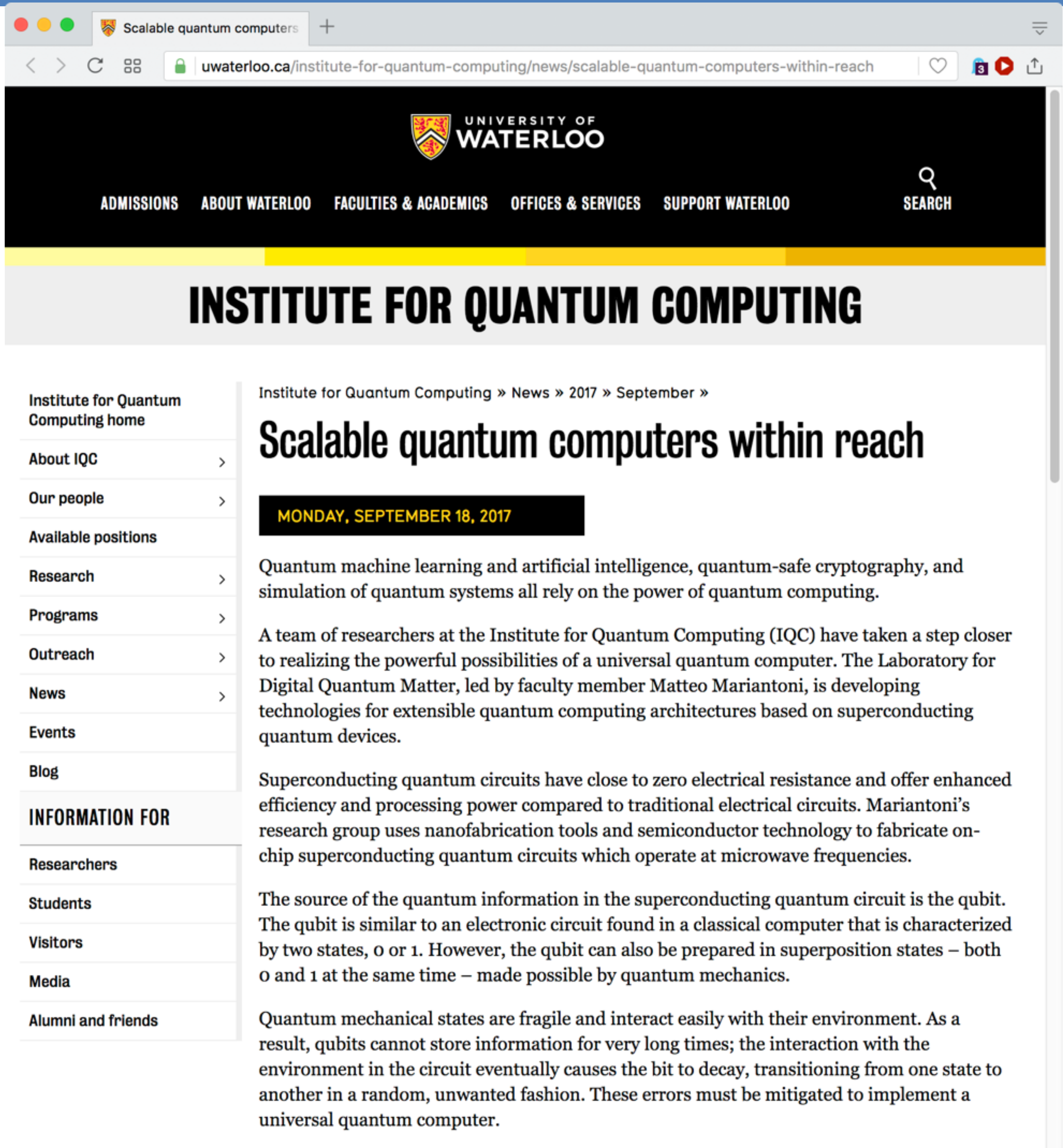
- Chemical reaction simulations
- Optimization problems
- Arithmetic

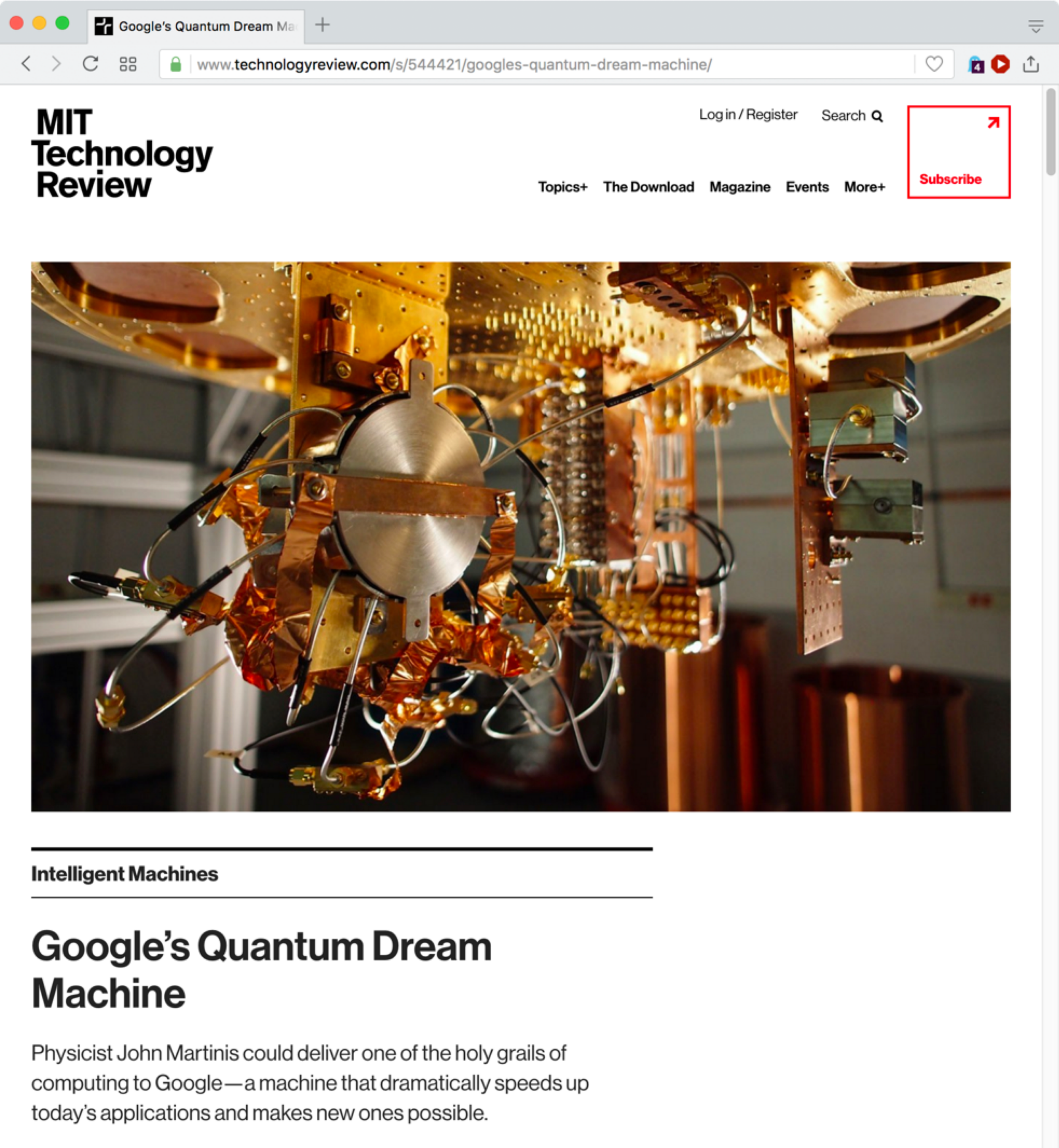
But not magic

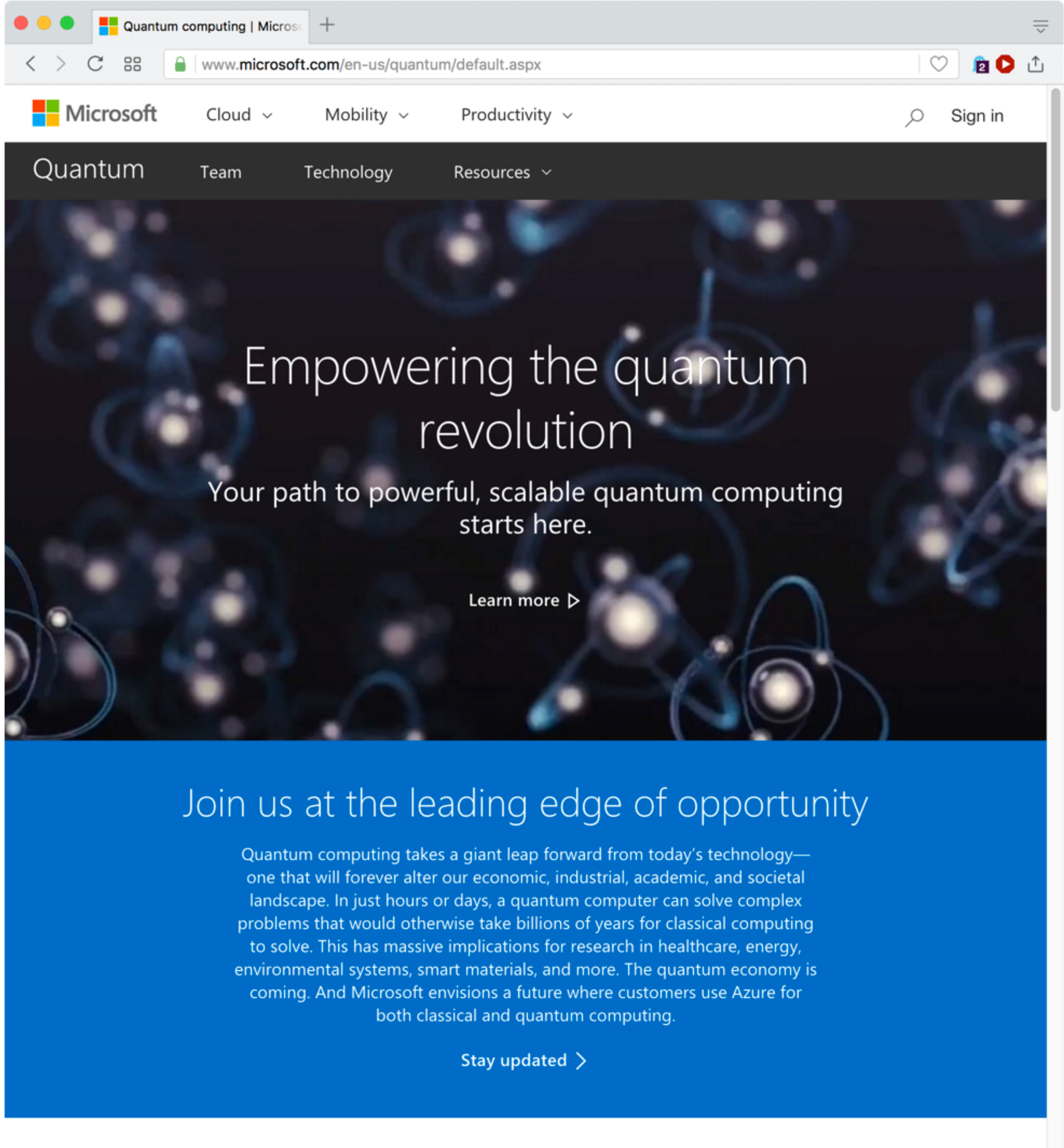
- Doesn't dramatically speed up all computations




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

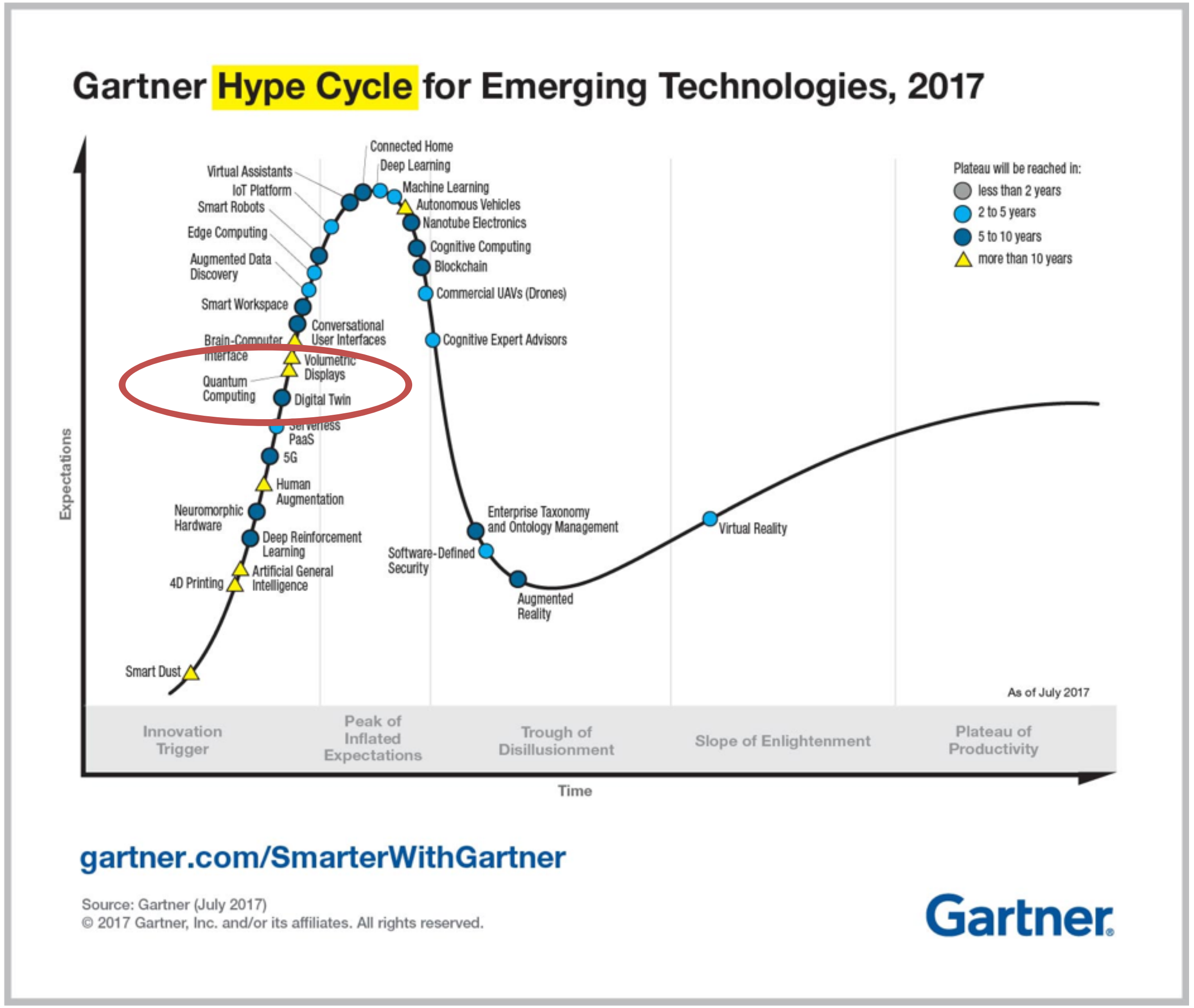

Scalable quantum computers
uwaterloo.ca/institute-for-quantum-computing/news/scalable-quantum-computers-within-reach
UNIVERSITY OF WATERLOO
ADMISSIONS
ABOUT WATERLOO
FACULTIES & ACADEMICS
OFFICES & SERVICES
SUPPORT WATERLOO
SEARCH
INSTITUTE FOR QUANTUM COMPUTING
Institute for Quantum Computing home
About 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
Expectations
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
Enterprise Taxonomy and Ontology Management
Software-Defined Security
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
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 threat to information security

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

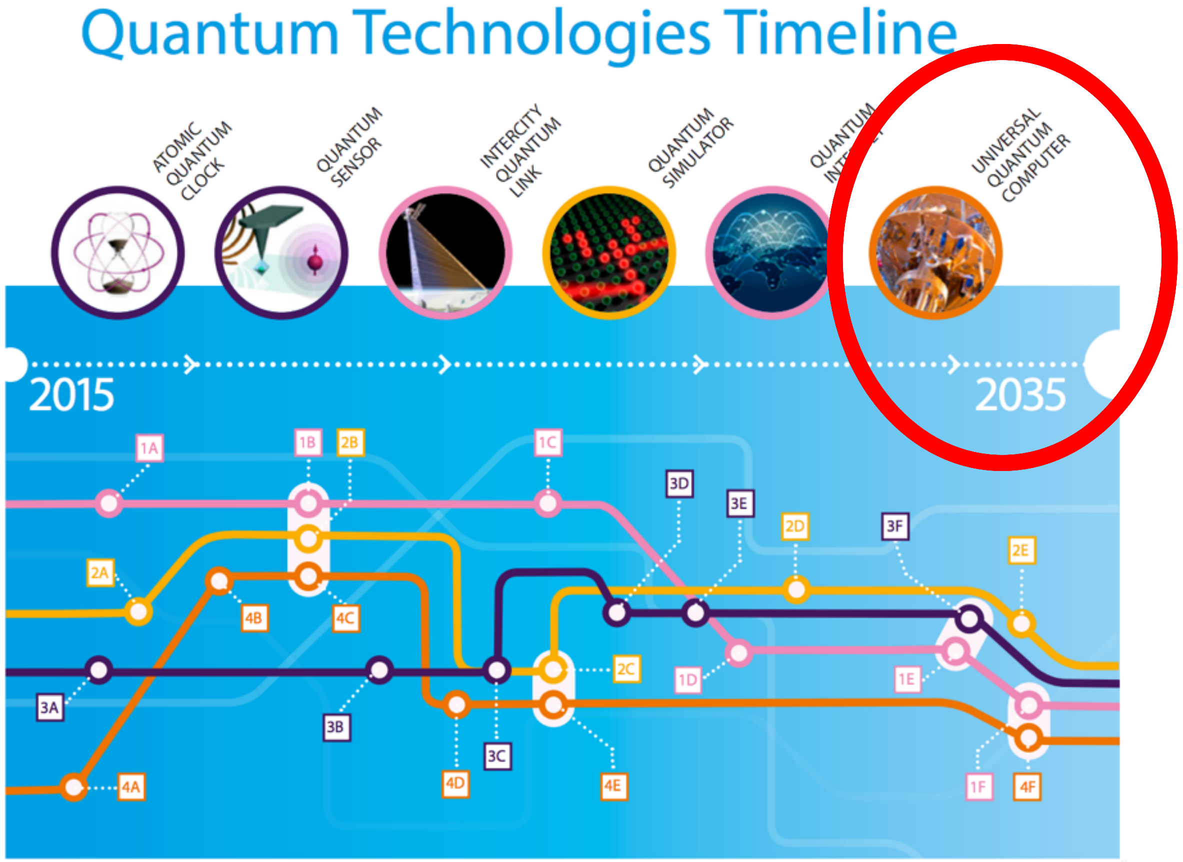
Need to migrate encryption to quantum-resistant algorithms

When should you start the process?

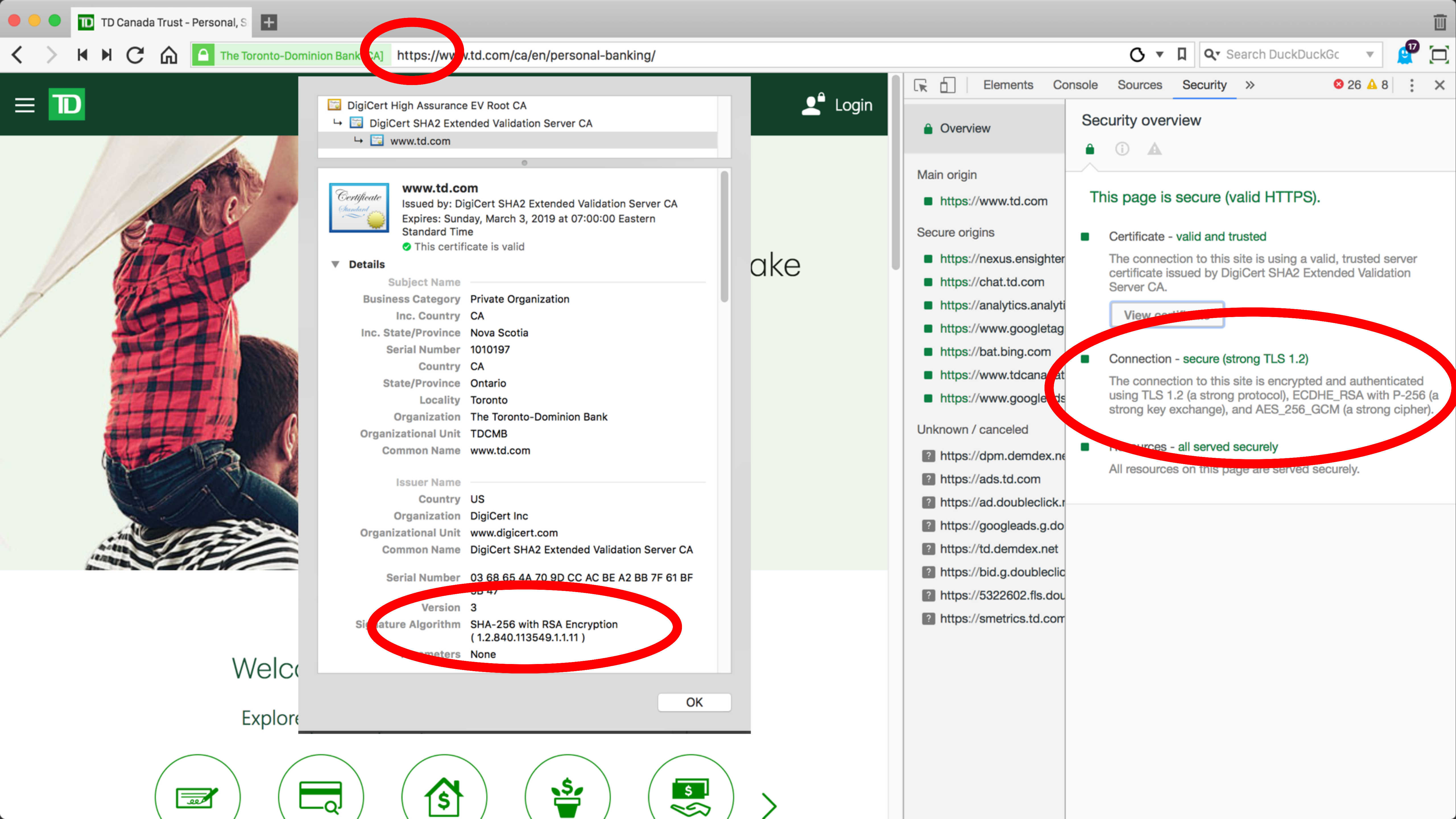
When will a large-scale quantum computer be built?

"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



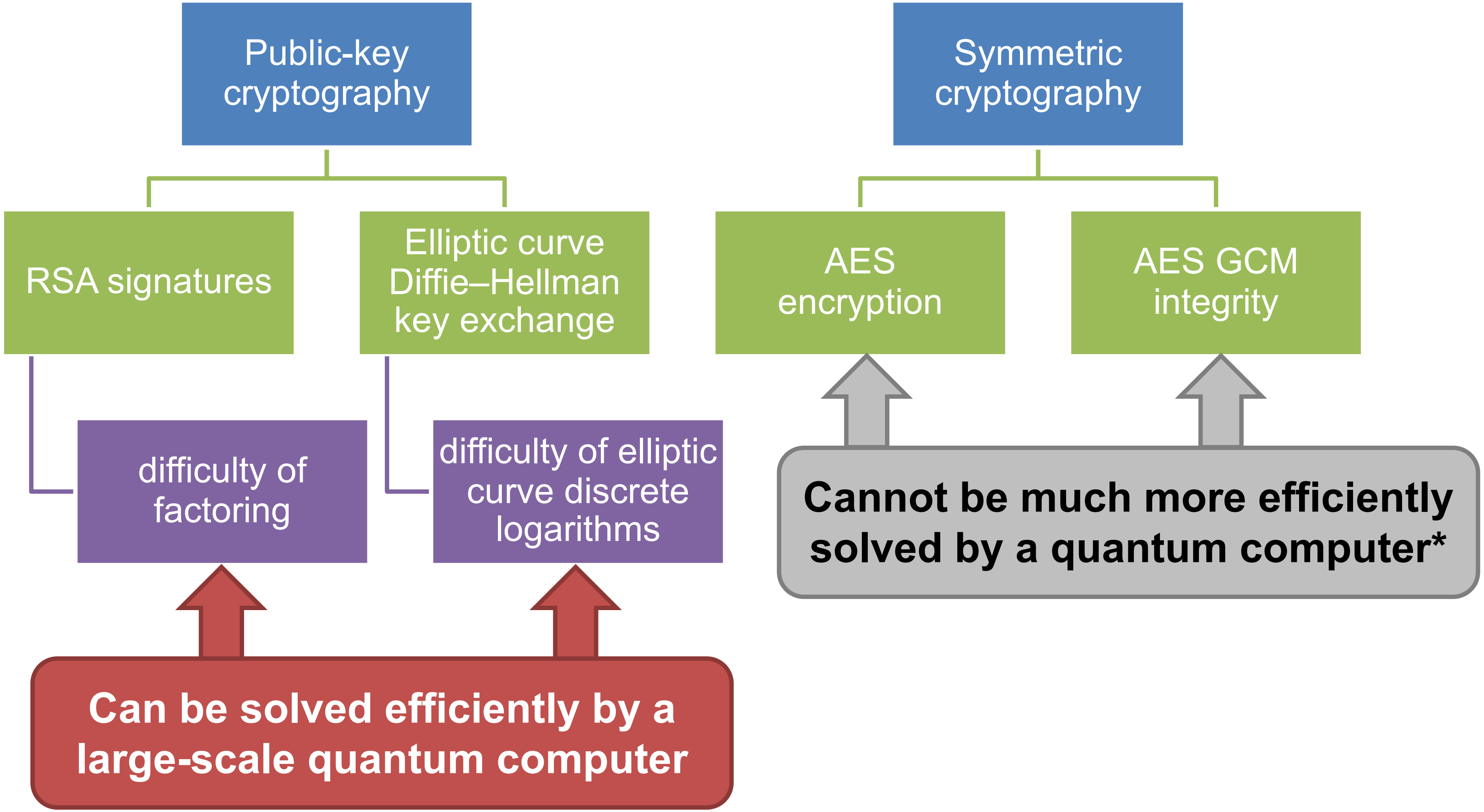
http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf


TD Canada Trust - Personal, S
The Toronto-Dominion Bank [CA]
https://www.td.com/ca/en/personal-banking/
Search DuckDuckGo
Login
DigiCert High Assurance EV Root CA
DigiCert SHA2 Extended Validation Server CA
www.td.com
www.td.com
Issued by: DigiCert SHA2 Extended Validation Server CA
Expires: Sunday, March 3, 2019 at 07:00:00 Eastern Standard Time
This certificate is valid
Details
Subject Name
Business Category Private Organization
Inc. Country CA
Inc. State/Province Nova Scotia
Serial Number 1010197
Country CA
State/Province Ontario
Locality Toronto
Organization The Toronto-Dominion Bank
Organizational Unit TDCMB
Common Name www.td.com
Issuer Name
Country US
Organization DigiCert Inc
Organizational Unit www.digicert.com
Common Name DigiCert SHA2 Extended Validation Server CA
Serial Number 03 68 65 4A 70 9D CC AC BE A2 BB 7F 61 BF
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters None
OK
Elements
Console
Sources
Security
26
8
Overview
Main origin
https://www.td.com
Secure origins
https://nexus.ensighter
https://chat.td.com
https://analytics.analyti
https://www.googletag
https://bat.bing.com
https://www.tdcanadat
https://www.googleads
Unknown / canceled
https://dpm.demdex.ne
https://ads.td.com
https://ad.doubleclick.n
https://googleads.g.do
https://td.demdex.net
https://bid.g.doublecli
https://5322602.fls.dou
https://smetrics.td.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 DigiCert SHA2 Extended Validation Server CA.
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_256_GCM (a strong cipher).
Resources - all served securely
All resources on this page are served securely.
Welco
Explore

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).



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

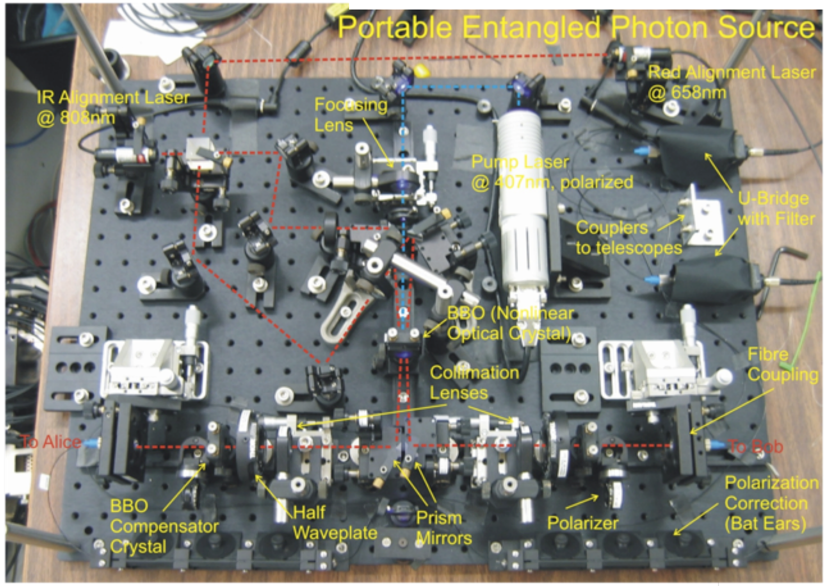
Multivariate quadratic

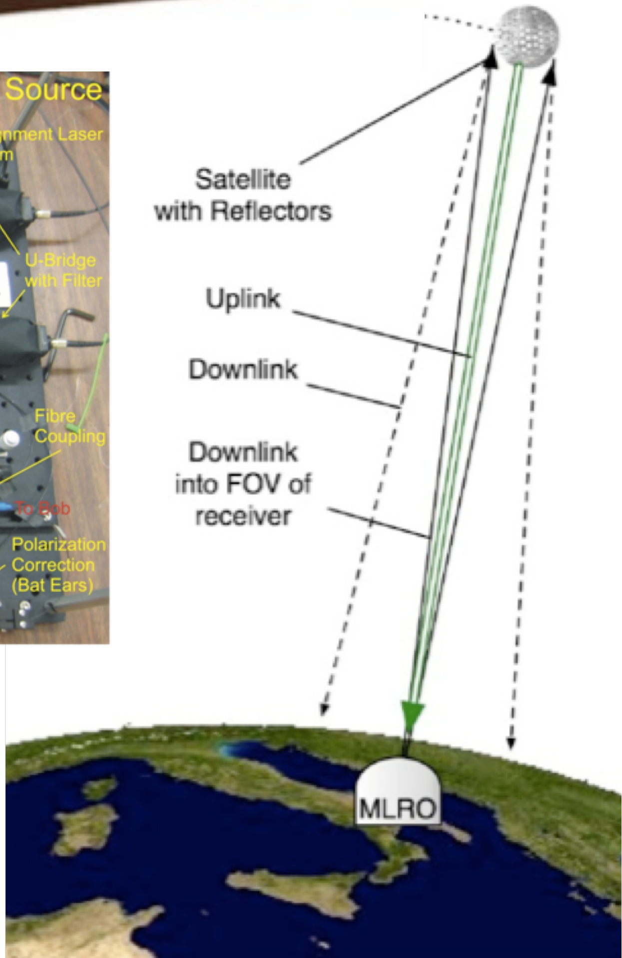
Lattice-based

Elliptic curve isogenies

Quantum key distribution

Uses quantum mechanics to protect information



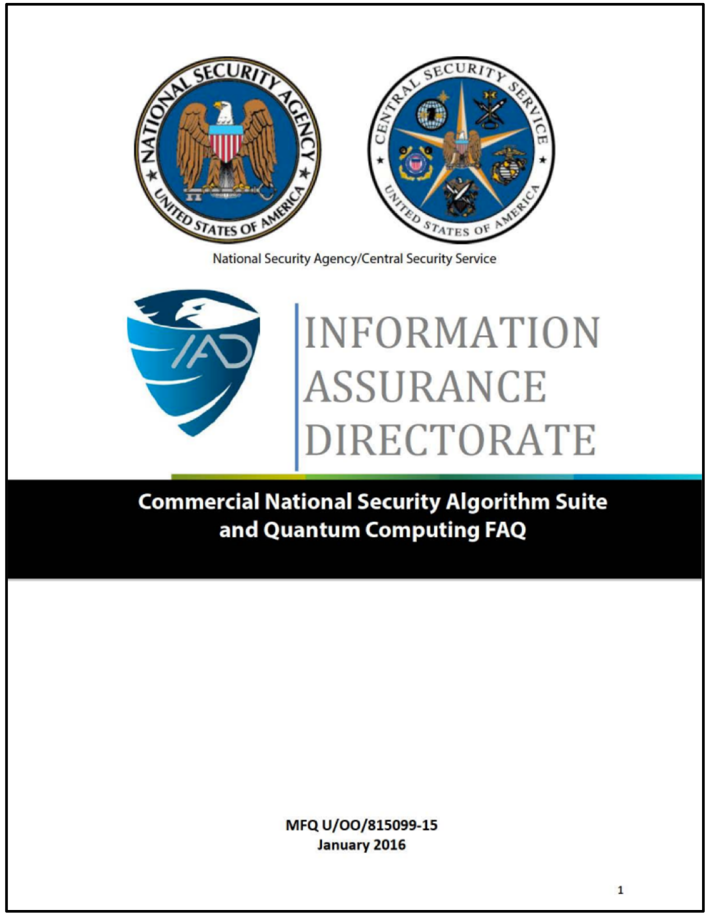


Doesn't require a full quantum computer

But does require new communications infrastructure and hardware

=> Not the subject of this talk

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)

"[NSA] will initiate a transition to quantum resistant algorithms in the not too distant future." – Aug. 2015

"NIST has initiated a process to […] standardize one or more quantum-resistant public-key cryptographic algorithms." – 2016


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

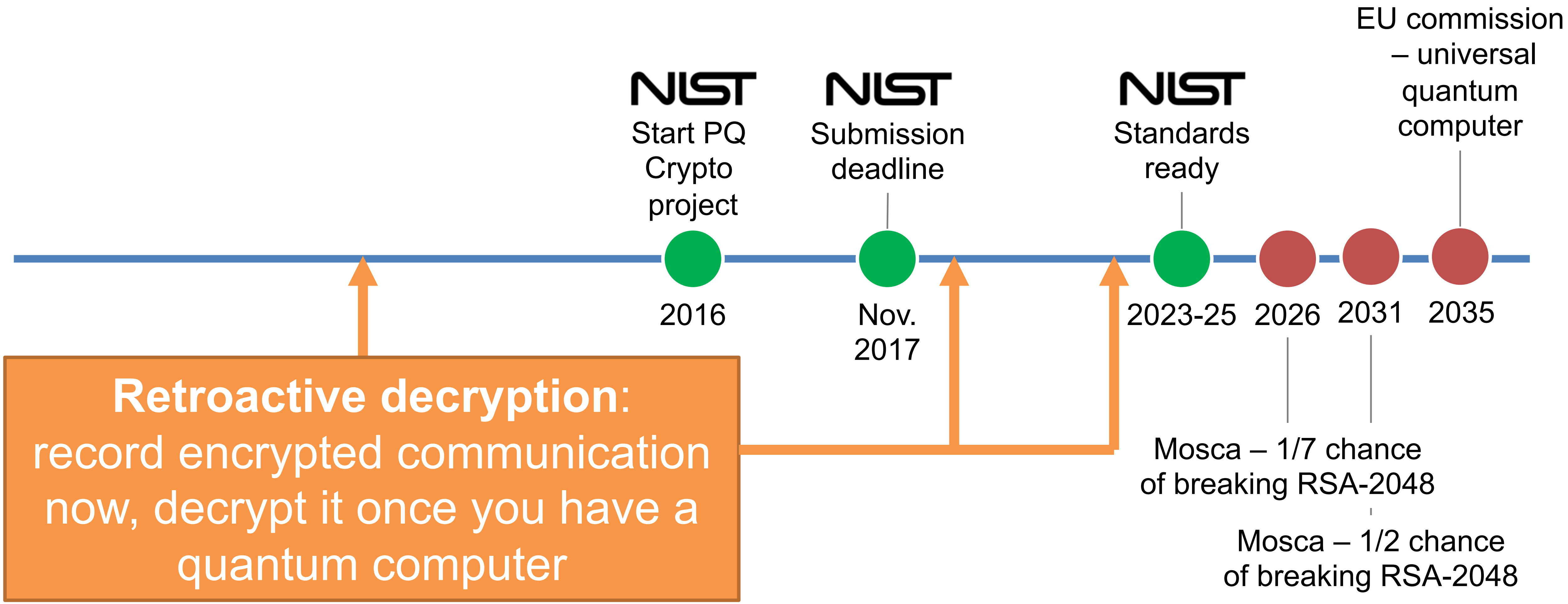
Post-Quantum Cryptography Standardization

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

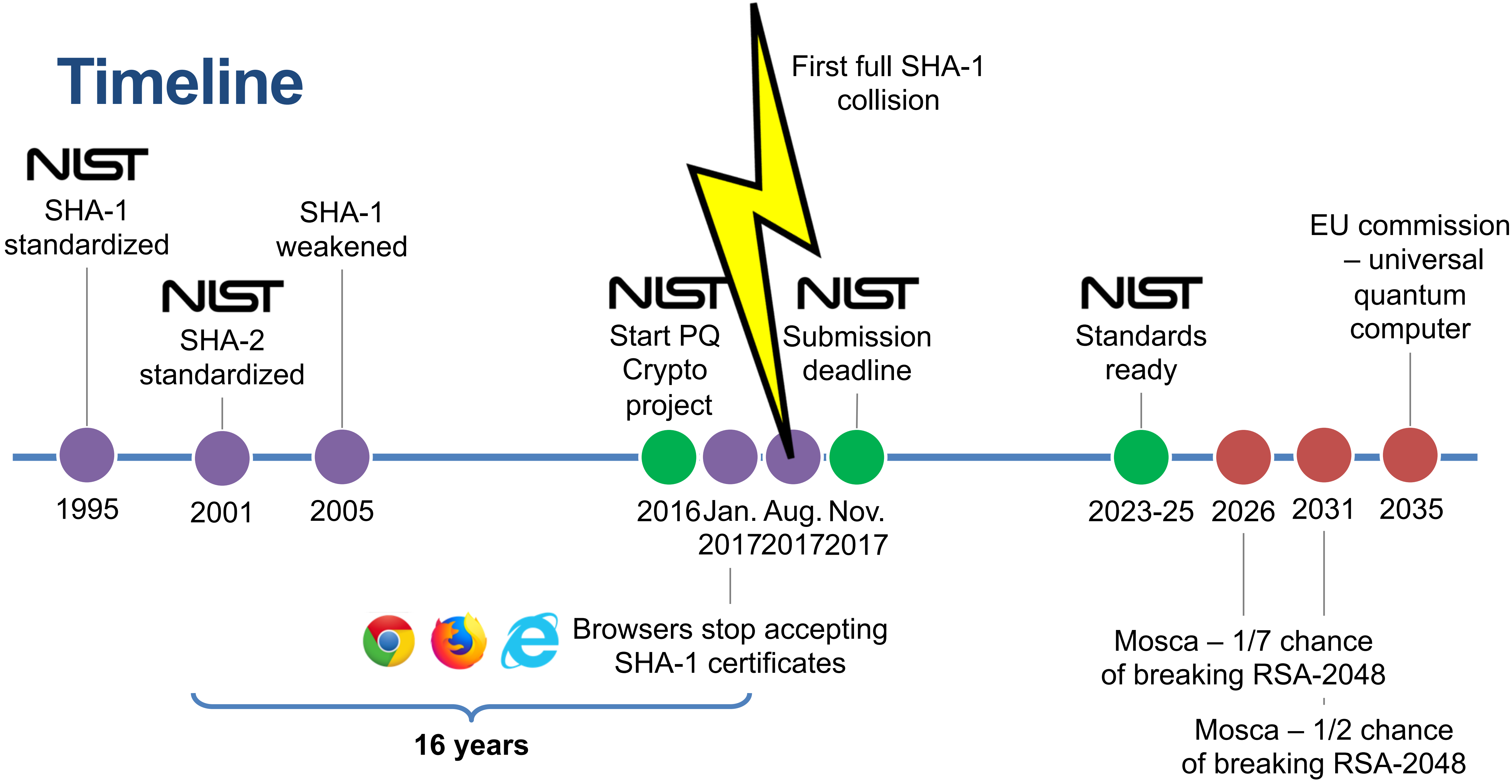
Call for Proposals Announcement

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
Mosca – 1/7 chance of breaking RSA-2048
2031
Mosca – 1/2 chance of breaking RSA-2048
2035
EU commission – universal quantum computer
Retroactive decryption:
record encrypted communication now, decrypt it once you have a quantum computer

Timeline


First full SHA-1 collision
NIST
SHA-1 standardized
1995
NIST
SHA-2 standardized
2001
SHA-1 weakened
2005
NIST
Start PQ Crypto project
2016
Jan. 2017
Aug. 2017
NIST
Submission deadline
Nov. 2017
Browsers stop accepting SHA-1 certificates
16 years
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

"Quantum risk assessment"

Identify the organization's reliance on cryptography

- Where is cryptography used?
- What type is used? Public key versus symmetric
- How long does the information need to be secure for?

Track development of quantum technology

Manage technology lifecycle to adopt quantum-resistant technologies – “cryptographic agility”

Be wary of "snake oil cryptography"

"proprietary algorithm"

"secret technique"

"virtual one-time pad"

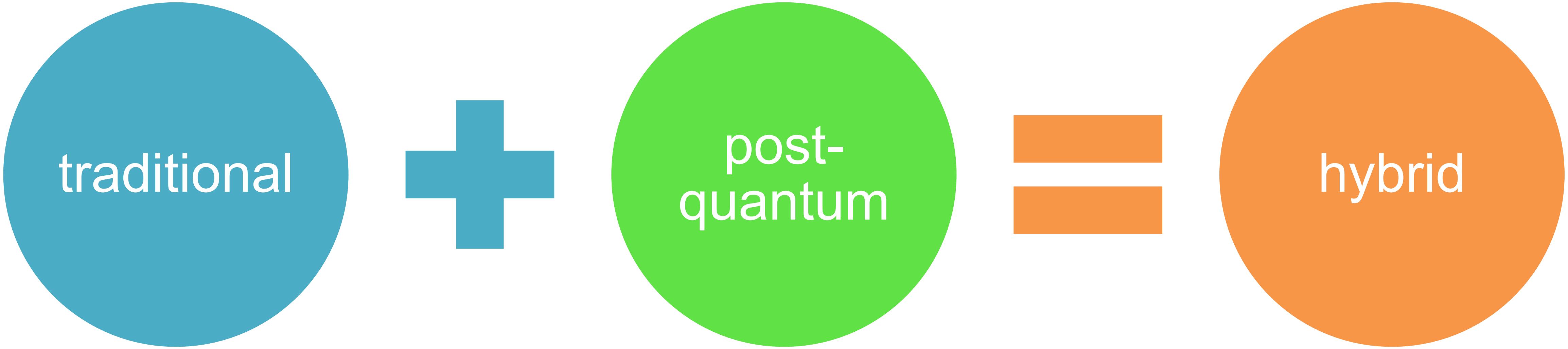
"chaos encryption"

"unbreakable"

Focus instead on algorithms progressing through the NIST PQ crypto project

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
  - University of Waterloo (lead)
  - Calgary, Montreal, McGill, Toronto
- 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

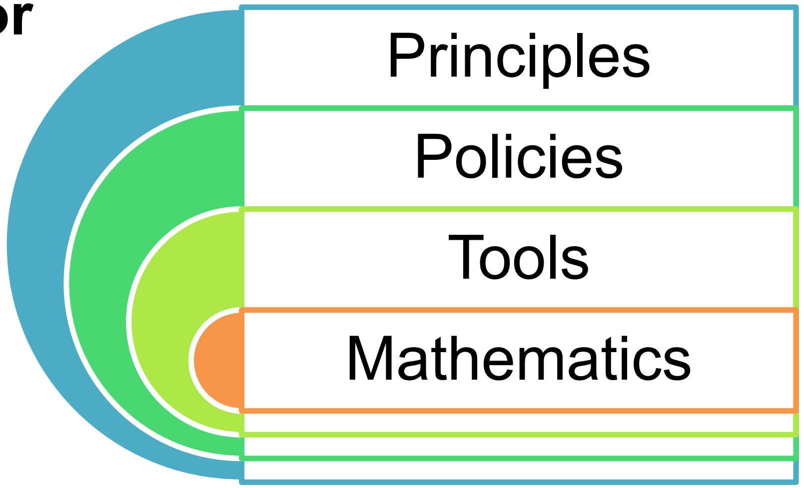
https://openquantumsafe.org

Cryptography and finance: overview, trends, the quantum threat

Douglas Stebila
UNIVERSITY OF WATERLOO

Cryptography used throughout financial infrastructure for protecting information:

- **Confidentiality and integrity of data in transit**
- **Confidentiality of data at rest**
- **Integrity of (public) data**



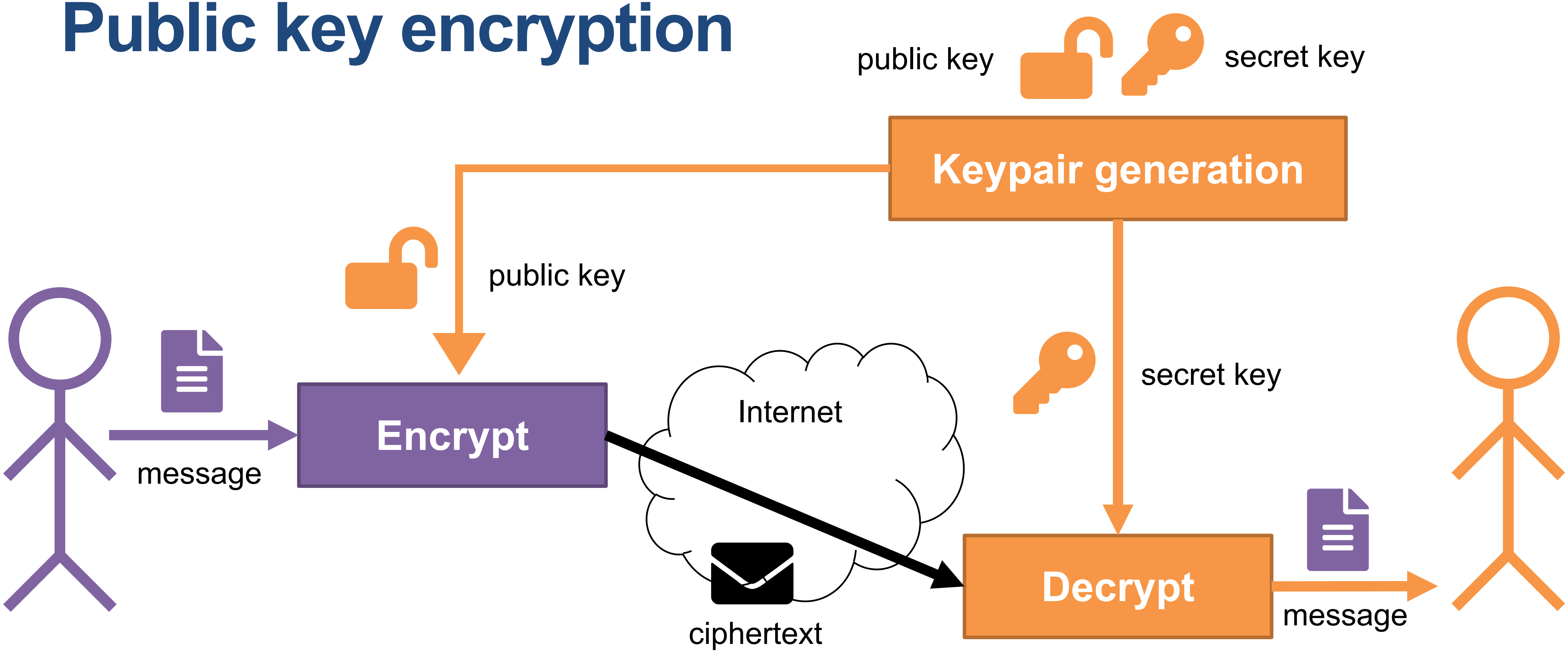
Trends in cryptography:

- **Upgrading communication protocols: in the next 5 years**
- **Encrypted cloud processing: not yet**
- **Quantum-resistant cryptography: starting preparing, but wait for standardized solutions**

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

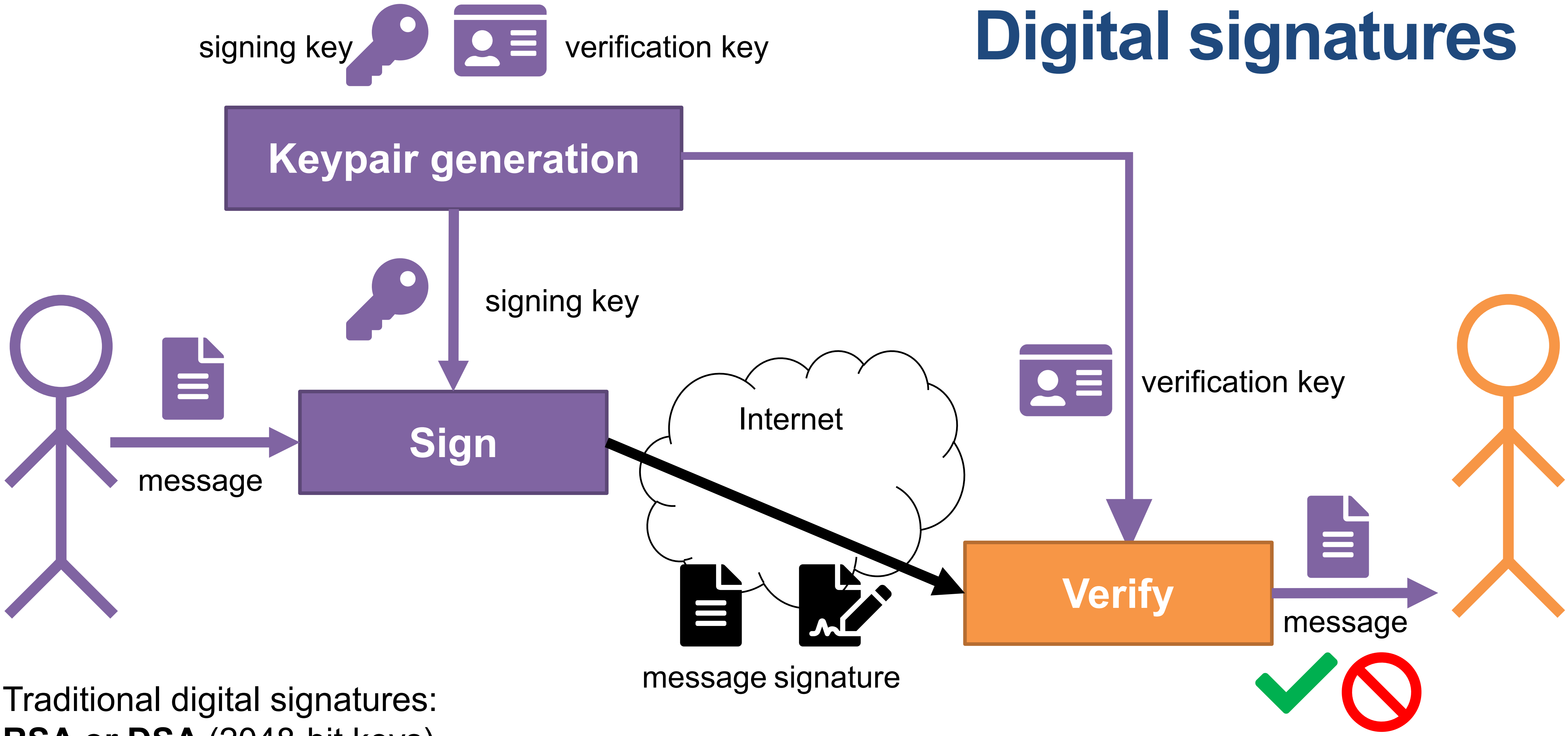
Appendix – Cryptography

Public key encryption



Traditional public key encryption:
RSA public key encryption (2048-bit keys)

Digital signatures



Traditional digital signatures:
RSA or DSA (2048-bit keys)
Elliptic curve DSA (ECDSA) (256-bit keys)

Appendix – Blockchain

Basic idea

1. There's a public ledger that everyone can read with everyone's balance.
2. Alice wants to pay Bob 3 units.
3. Alice requests to put a transaction in the ledger saying "Alice pays Bob 3 units."
4. The maintainer of the ledger checks
   (a) that Alice has big enough balance and
   (b) that Alice really made the request,
   then records the transaction in the ledger.
5. Bob now has a higher balance.

Problems with the basic idea

No anonymity

- Use public keys rather than names.
- Use transaction references rather than accounts.

How to verify someone has authorization to spend from Alice's account?

- Use digital signatures to demonstrate ownership of currency from previous transaction.

Who maintains the ledger?

- Distributed ledger: incentivize community to maintain.

Transaction

"Alice pays Bob 3 units."

"Alice transfers control of 3 units to Bob."

Input:

- Previous transaction ID.
- Public key used in previous transaction.
- Digital signature using based on previous transaction's public key.

Output:

- Bob's address
- # of units
  - Bitcoin address = hash of public key
- Should include own address to "make change"

Transaction

Input: transaction 24d89c02e7ba1

public key 3048c9d000a11789ed	signature 9b8d910afa0b0476c

Output:

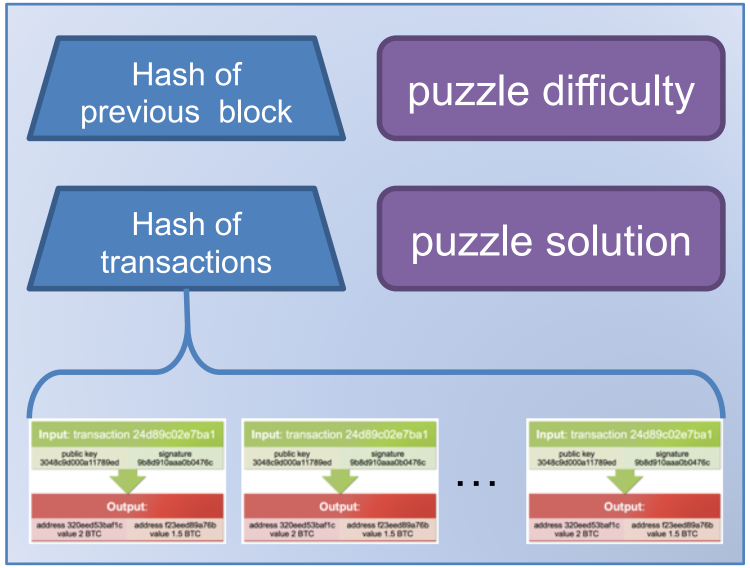
address 320e1d53baf1c value 2 BTC	address f23ea089a76b value 1.5 BTC

Block

Header

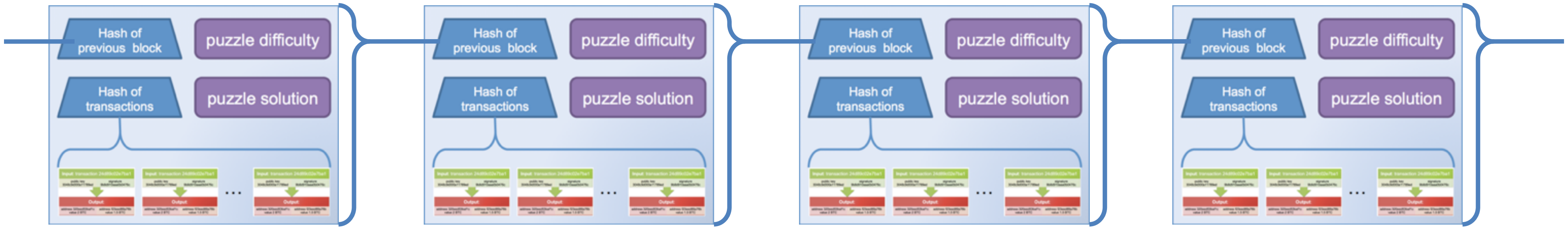
+

a list of transactions



Blockchain

A sequence of blocks = ledger of transactions



Which blockchain?

Blocks form a tree.

- Could have forks in the tree.
- Only the longest chain is considered to be valid by the community.

Adding blocks to the chain

A block can only be added to the blockchain if the hash of the block is small.

- Users try to generate a block with a small hash.
  - ("cryptographic puzzle")

- Updating the blockchain requires work but maintains the public ledger.

- Motivation: whoever constructs the block includes one transaction paying themselves 25 BTC ("**mining**")

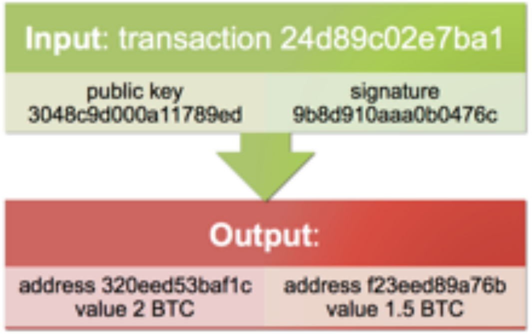
Why people agree on a single ledger

Bitcoin designed so everyone is motivated to agree on a single public ledger

- If I am trying to add a block to the chain and I do so, I'm motivated to grow that chain because that chain has my reward.
- If I am trying to add a block to the chain but someone else beats me, the probability I'll find the next block is the same regardless of whether I use the new block or not.

Cryptographic parts of Bitcoin ledger

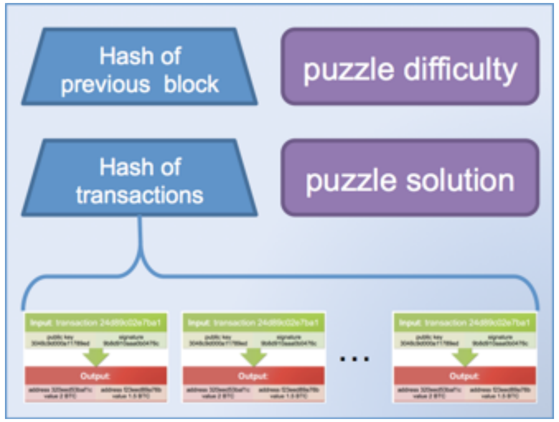
Transactions



Digital signatures for transaction approval

(Hashed) public keys for addresses

Blocks



Hash used to collect transactions together

Cryptographic hash puzzle required to make block valid (Hashcash SHA-256)

Blockchain

Hash used to chain transactions together

Only blocks in longest chain considered valid