The quantum computing threat to cryptography

Course 01410, Crypto I

Christian Majenz

Assistant Professor, Cybersecurity Engineering Section, DTU Compute

After today, you will…

- …be able to put quantum computing as a disruptive technology into perspective,
- …have identified cryptographic infrastructure that is susceptible to quantum computing attacks,
- …have a basic understanding of how quantum computers can be used to attack cryptographic schemes, and
- …have a rough idea when cryptanalytically relevant quantum computers can be expected to become reality.

Intro

Quantum computers

Quantum computers

- Accelerating effort to build a quantum computer

Quantum computers

- Accelerating effort to build a quantum computer
- Major investments:

Google IBM

intel Microsoft

Quantum computers

- Accelerating effort to build a quantum computer
- Major investments:







We need to prepare cryptography for the arrival of quantum computers!

Quantum computers

- Accelerating effort to build a quantum computer
- Major investments:







We need to prepare cryptography for the arrival of quantum computers!

- Security against quantum attackers

Quantum computers

- Accelerating effort to build a quantum computer
- Major investments:



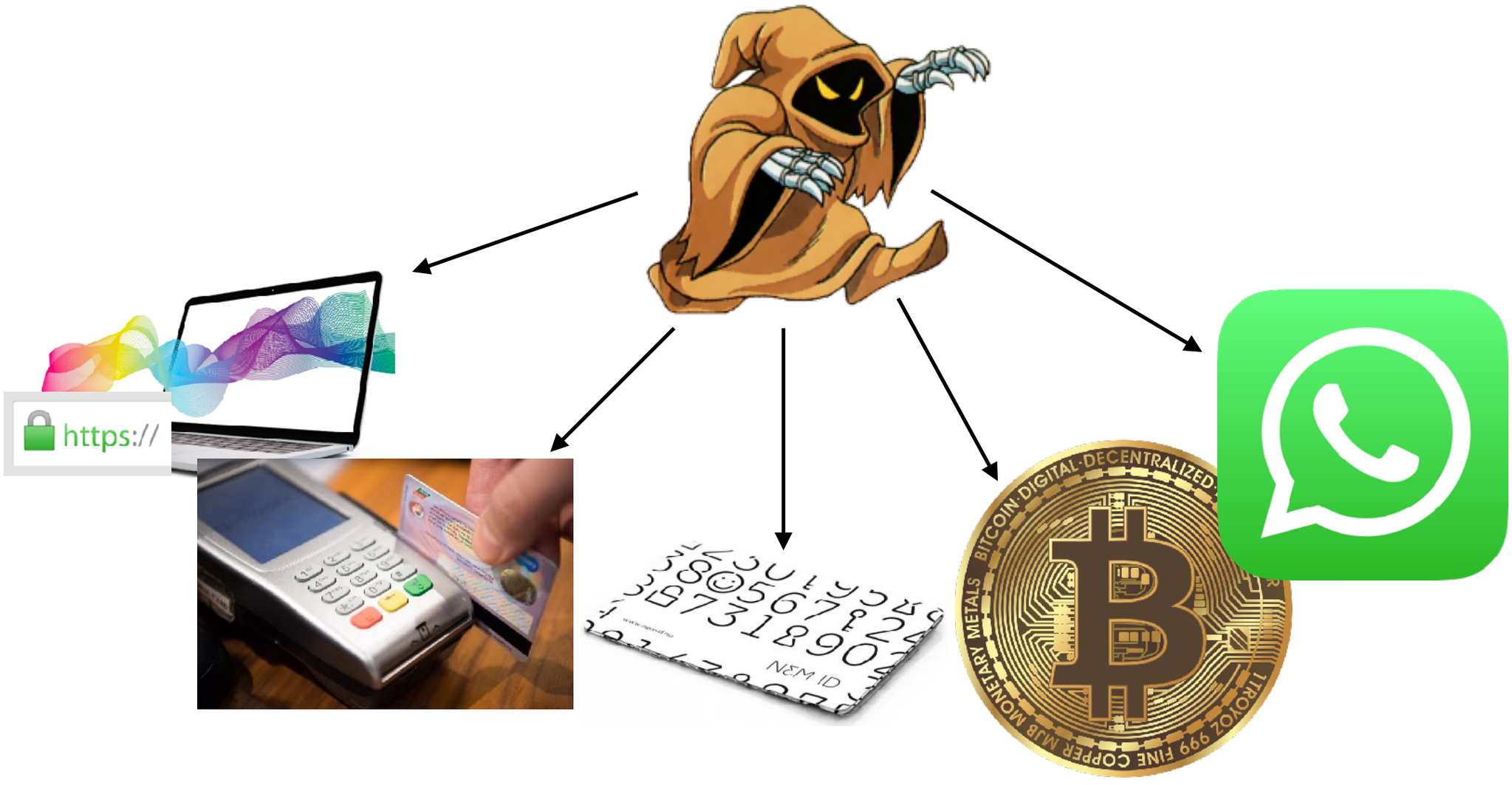




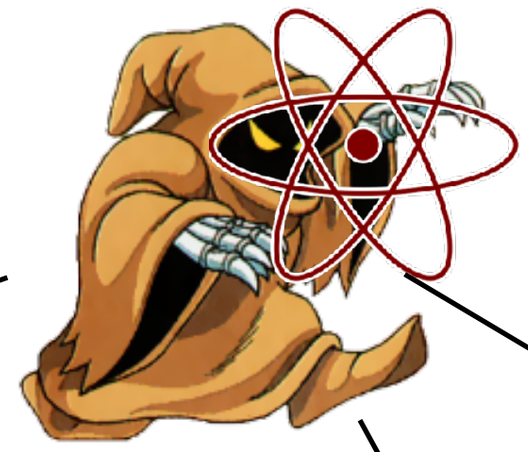
We need to prepare cryptography for the arrival of quantum computers!

- Security against quantum attackers
- Quantum cryptography

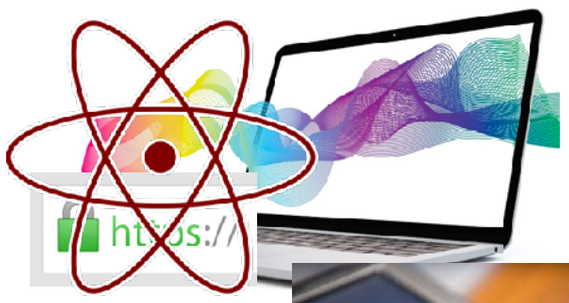
Cryptography is everywhere



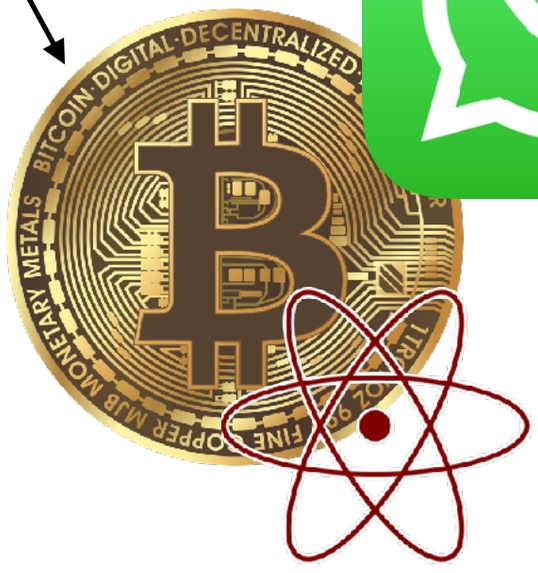
Quantum computing is changing cryptography

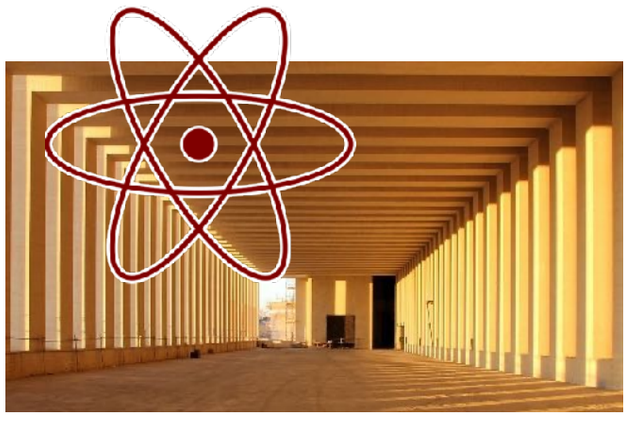


Post-quantum security



Quantum crypto

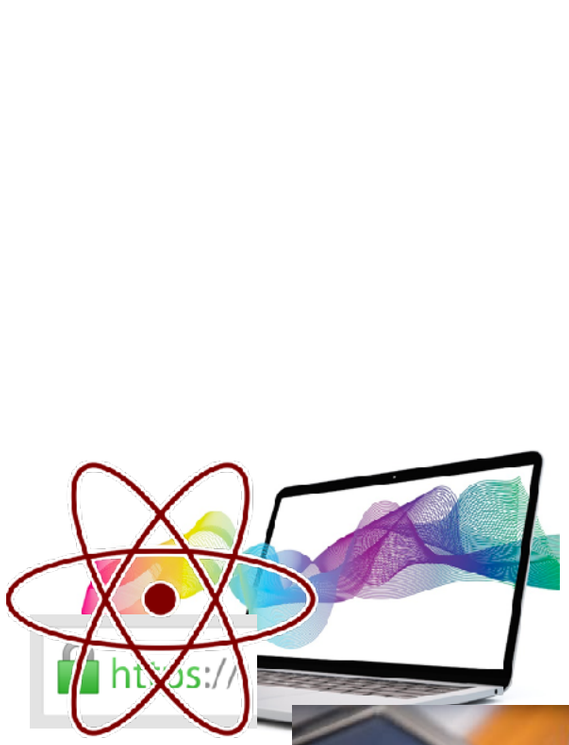




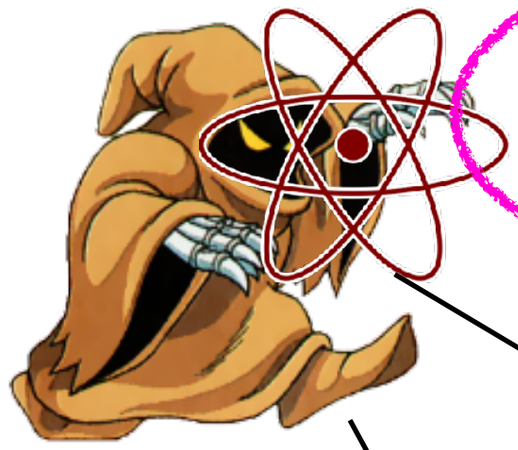
Theoretical Foundation

Quantum-enhanced crypto

Quantum computing is changing cryptography

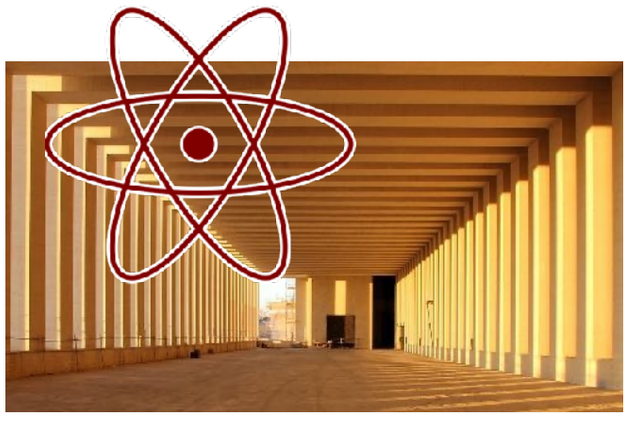


Quantum crypto



Post-quantum security

Quantum-enhanced crypto



Theoretical Foundation

What is a quantum computer?

Quantum physics is everywhere

Quantum physics is everywhere

In Information technology:

- Semiconductors

Quantum physics is everywhere

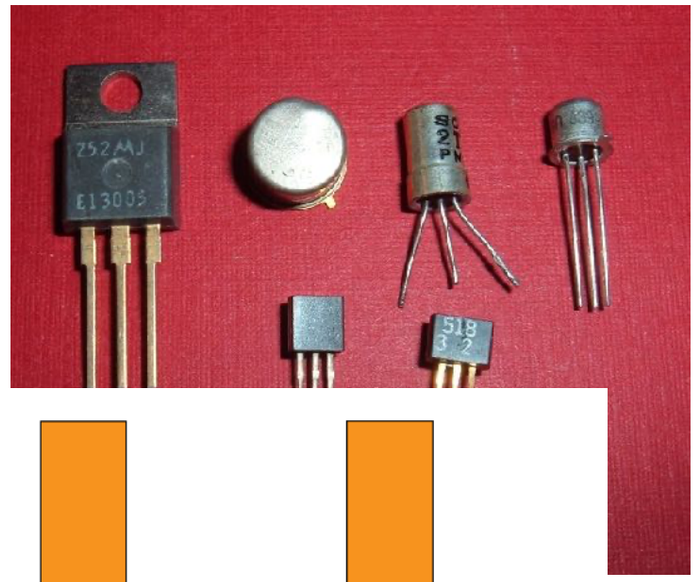
In Information technology:

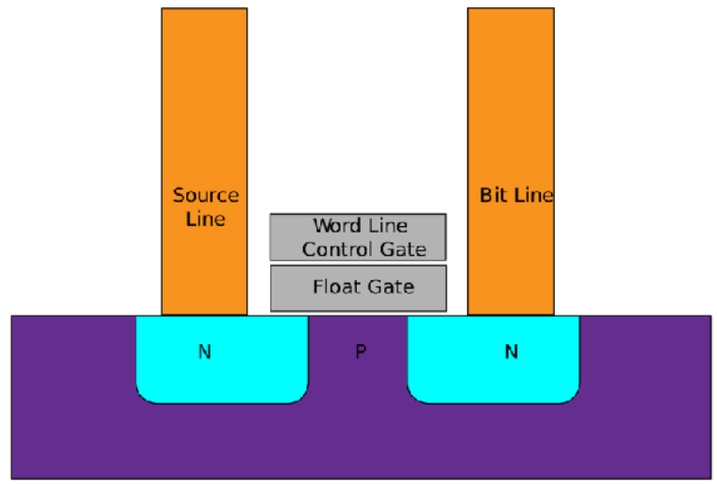
- Semiconductors
  - Transistors

Quantum physics is everywhere

In Information technology:

- Semiconductors
  - Transistors
  - Flash memory

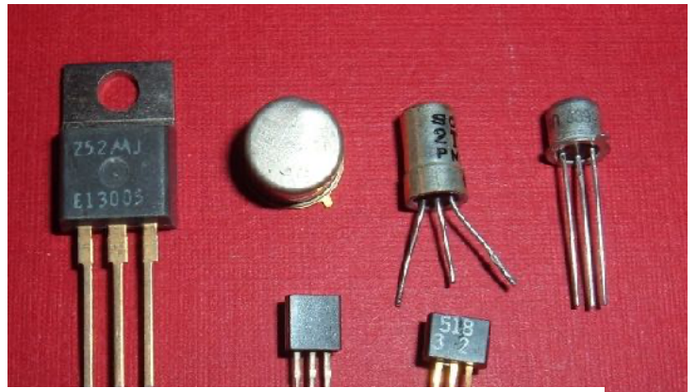




Quantum physics is everywhere

In Information technology:

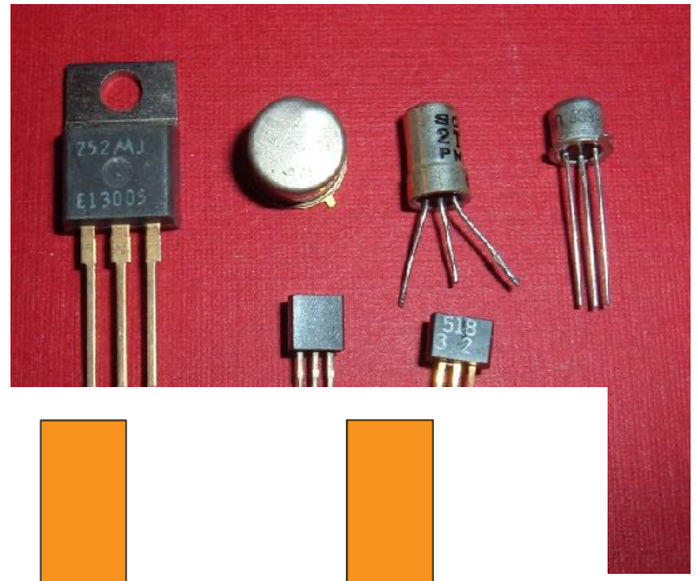
- Semiconductors
  - Transistors
  - Flash memory
  - OLED
  - …



Quantum physics is everywhere

In Information technology:

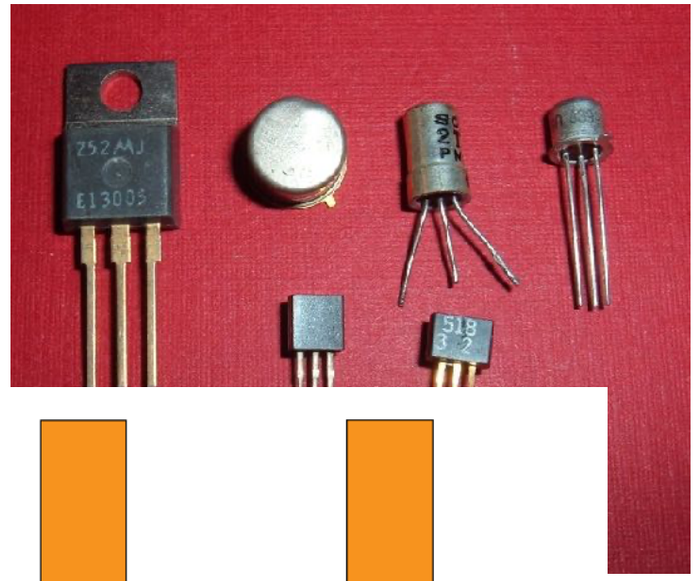
- Semiconductors
  - Transistors
  - Flash memory
  - OLED
  - …
- Optical communication

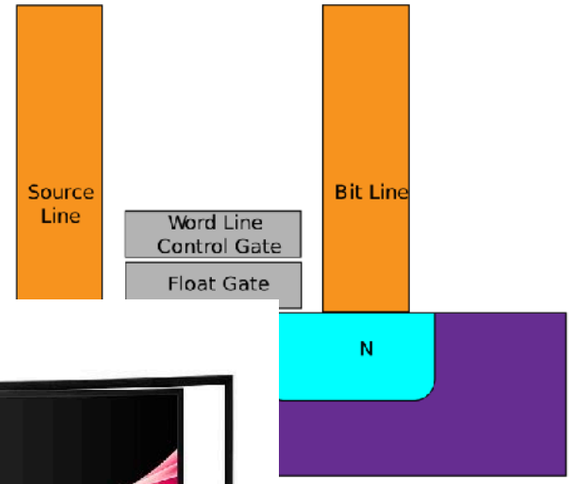


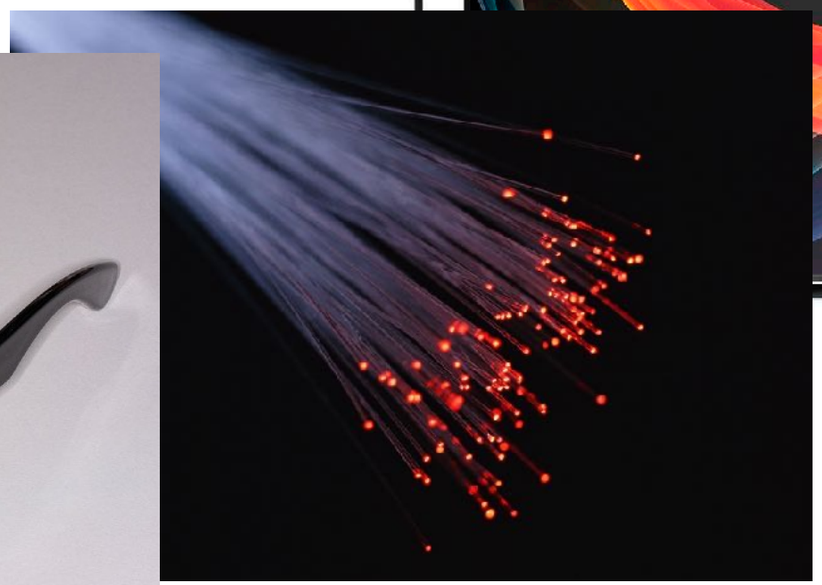
Quantum physics is everywhere

In Information technology:

- Semiconductors
  - Transistors
  - Flash memory
  - OLED
  - …
- Optical communication
- 3D movie theatre
- …







Example: polarization of light

Example: polarization of light

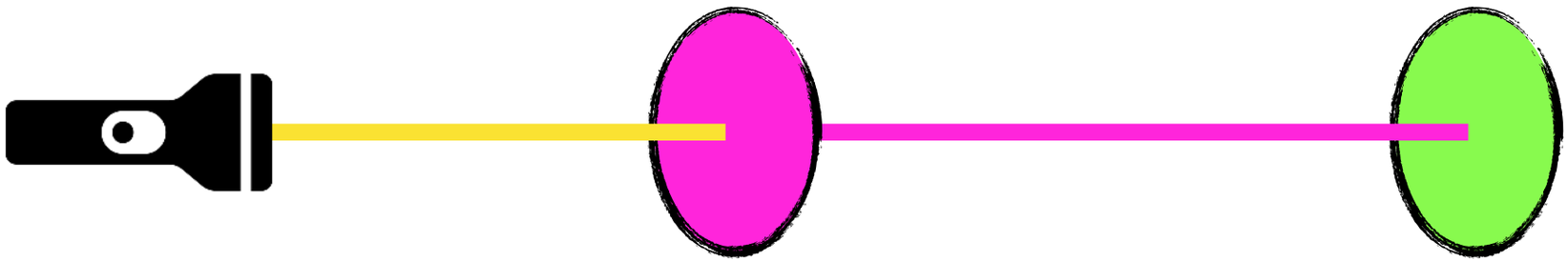
Classical* property of Light: Color

Example: polarization of light

Classical* property of Light: Color

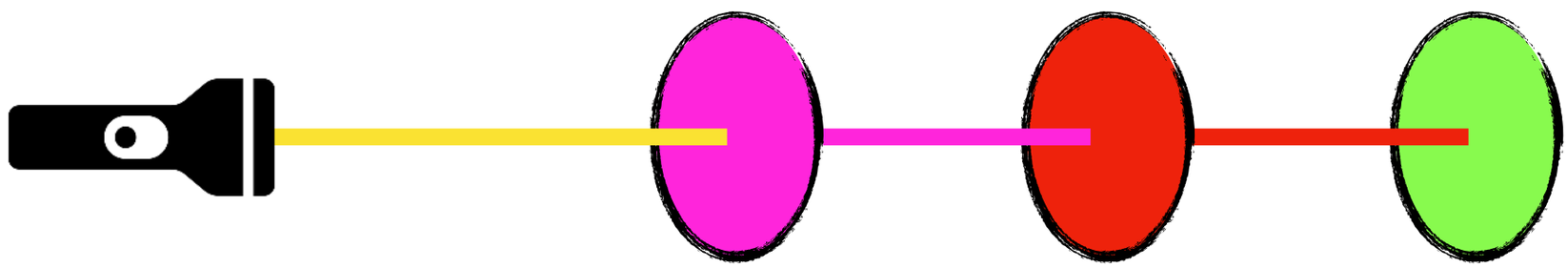
Example: polarization of light

Classical* property of Light: Color



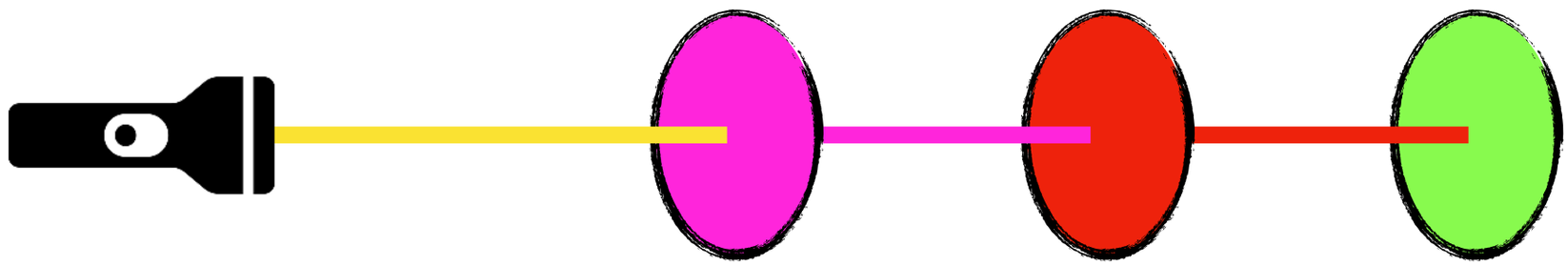
Example: polarization of light

Classical* property of Light: Color



Example: polarization of light

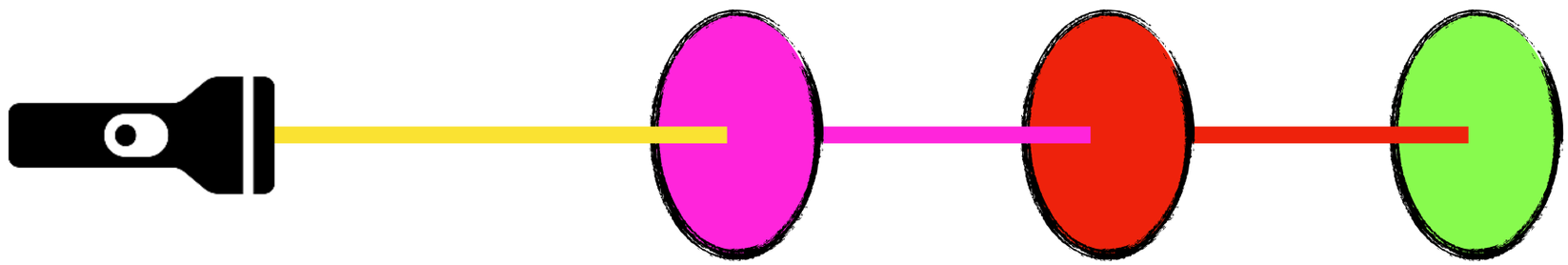
Classical* property of Light: Color



Quantum property of light: Polarization

Example: polarization of light

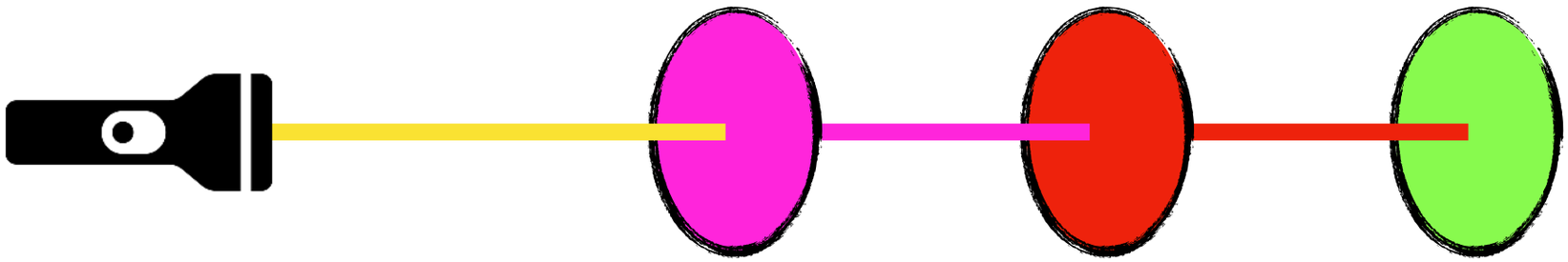
Classical* property of Light: Color



Quantum property of light: Polarization

Example: polarization of light

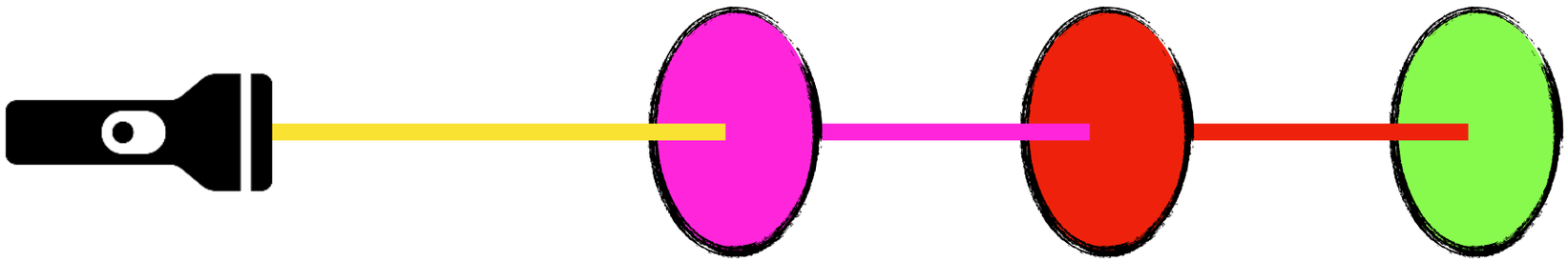
Classical* property of Light: Color



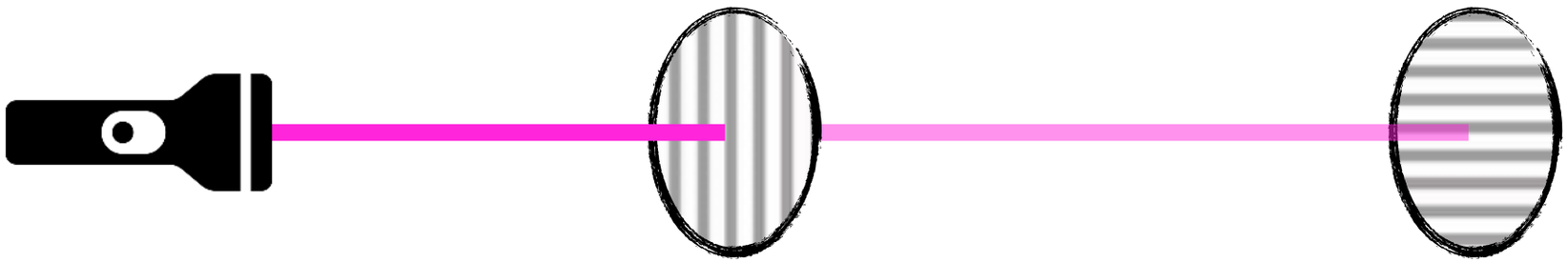
Quantum property of light: Polarization

Example: polarization of light

Classical* property of Light: Color

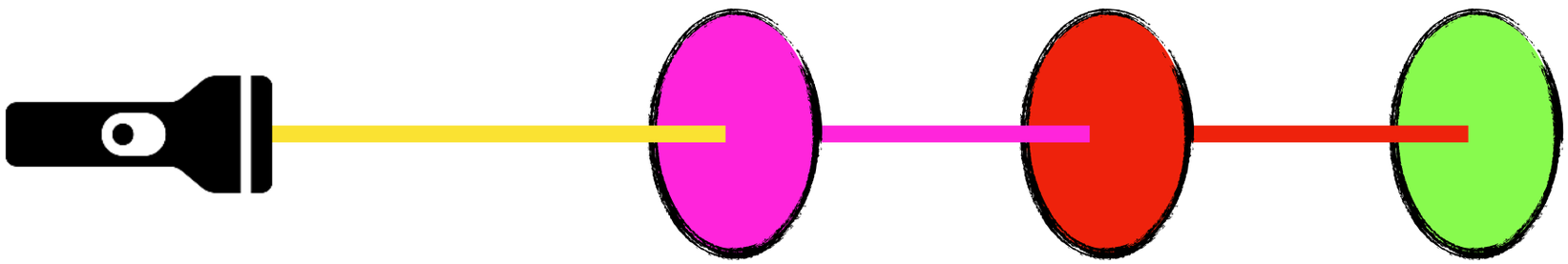


Quantum property of light: Polarization

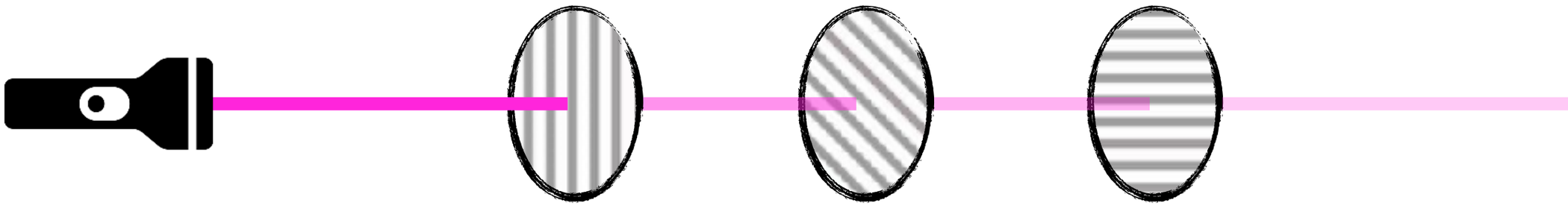


Example: polarization of light

Classical* property of Light: Color



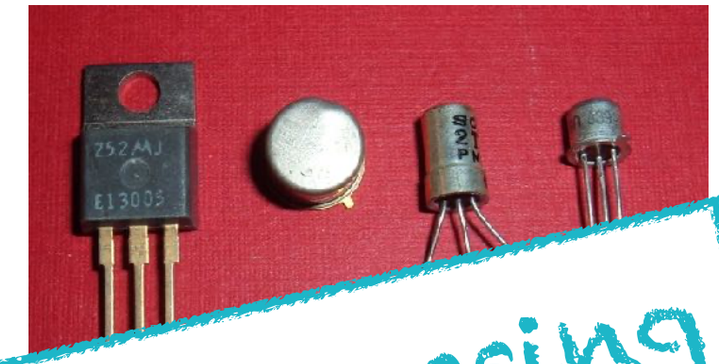
Quantum property of light: Polarization

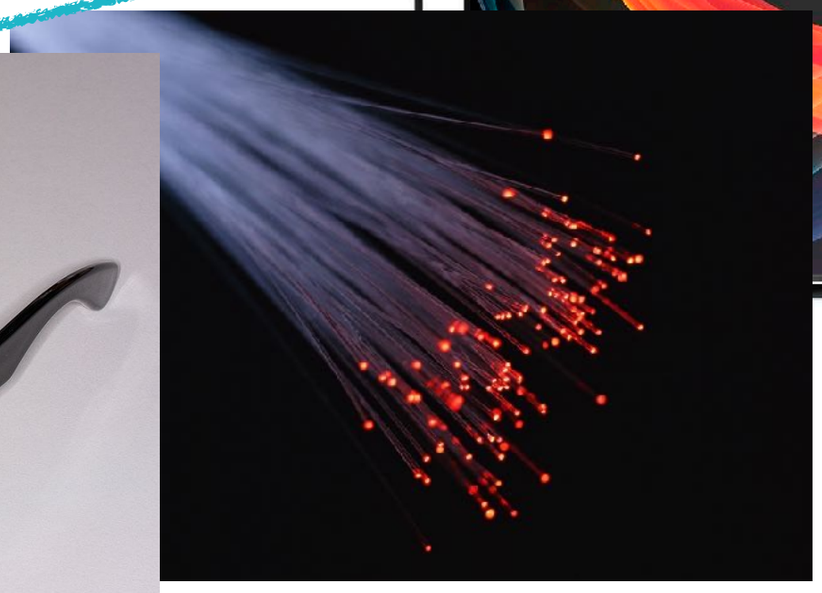


Quantum physics is everywhere

In Information technology:

- Semiconductors
  - Transistors
  - Flash memory
  - OLED
  - …
- Optical co





"Quantum physics is used for processing "non-quantum" Information.

Quantum computing

"Information is Physical."

Rolf Landauer

Quantum computing

"Information is Physical."

Rolf Landauer

$\Longrightarrow$ If the physics is quantum, information is as well.

What is a quantum computer?

Classical information: “Does the flashlight emit green light?”

Specified by a bit $b \in \{0,1\}$

More generally: bit strings $x \in \{0,1\}^n$

Basic operations: Logical gates

What is a quantum computer?

Classical information: “Does the flashlight emit green light?”

Specified by a bit $b \in \{0,1\}$

More generally: bit strings $x \in \{0,1\}^n$

Basic operations: Logical gates

Quantum information: “What is the polarization of the light emitted from the flashlight?”

Specified by a unit vector $|v\rangle \in \mathbb{R}^2$

What is a quantum computer?

Classical information: “Does the flashlight emit green light?”

Specified by a bit $b \in \{0,1\}$

More generally: bit strings $x \in \{0,1\}^n$

Basic operations: Logical gates

Quantum information: “What is the polarization of the light emitted from the flashlight?”

Specified by a unit vector $|v\rangle \in \mathbb{R}^2$

More generally: unit vectors $|\psi\rangle \in \mathbb{C}^{2^n}$ (bit strings: basis)

What is a quantum computer?

Classical information: “Does the flashlight emit green light?”

Specified by a bit $b \in \{0,1\}$

More generally: bit strings $x \in \{0,1\}^n$

Basic operations: Logical gates

Quantum information: “What is the polarization of the light emitted from the flashlight?”

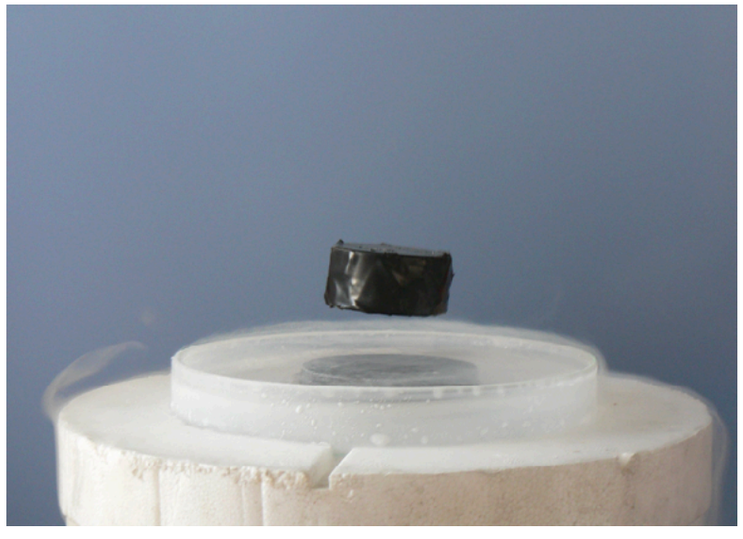
Specified by a unit vector $|v\rangle \in \mathbb{R}^2$

More generally: unit vectors $|\psi\rangle \in \mathbb{C}^{2^n}$ (bit strings: basis)

Basic operations: “Quantum gates”⇔Unitary matrices

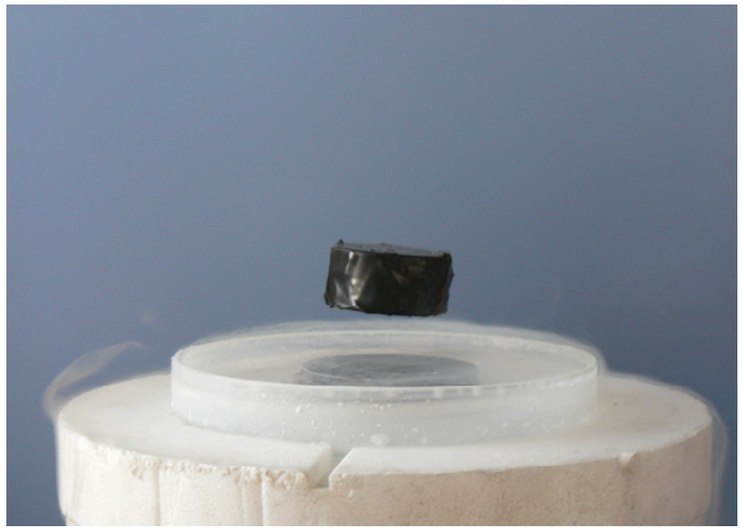
Physical realization

Physical realization

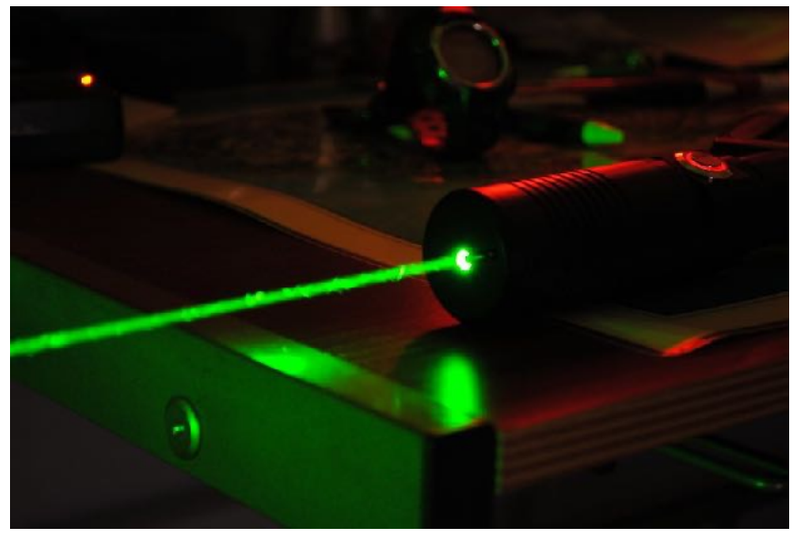


- Superconducting

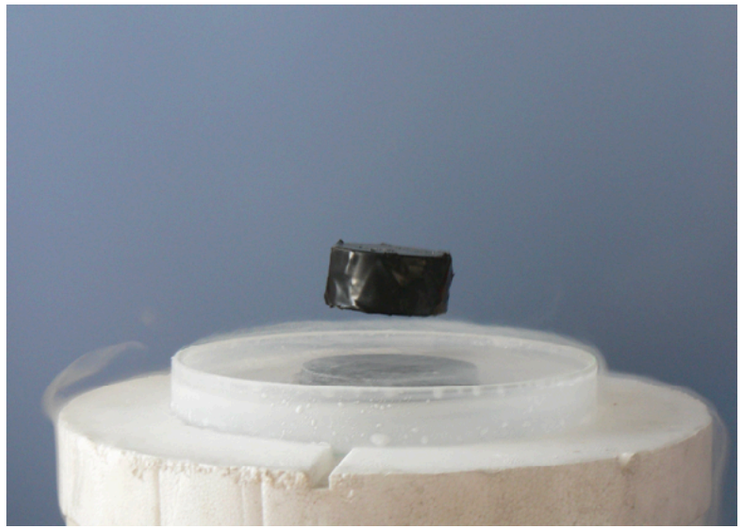
Physical realization



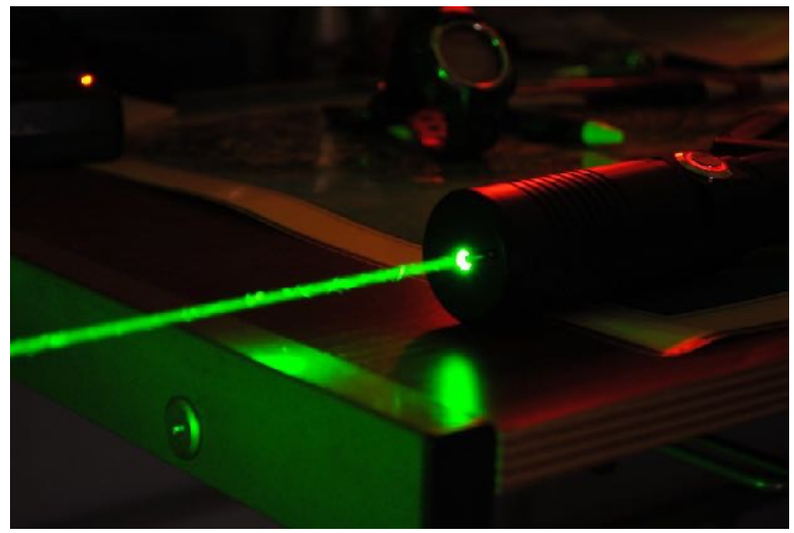
- Superconducting
- Photonic

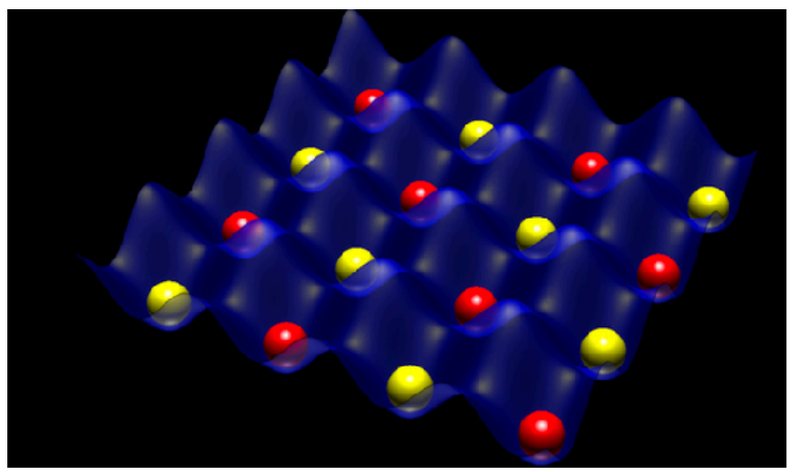


Physical realization

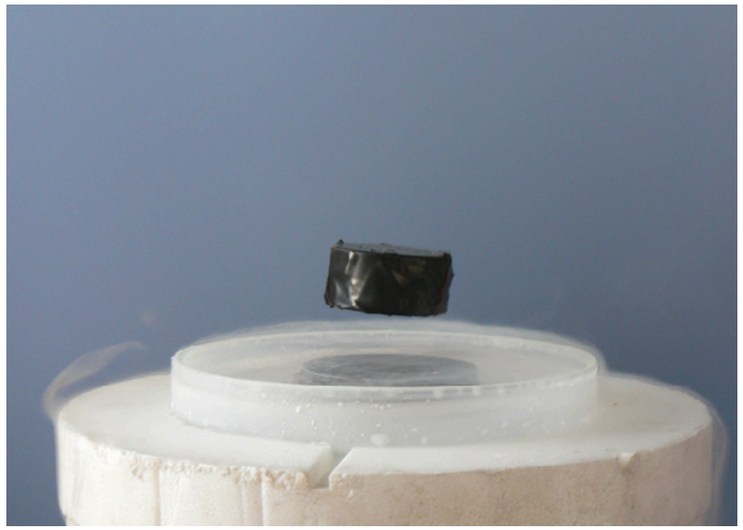


- Superconducting
- Photonic
- Cold atoms

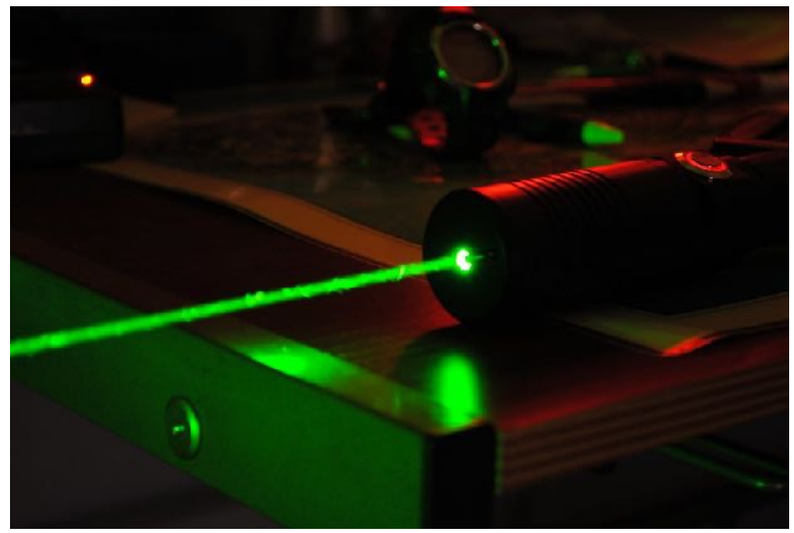


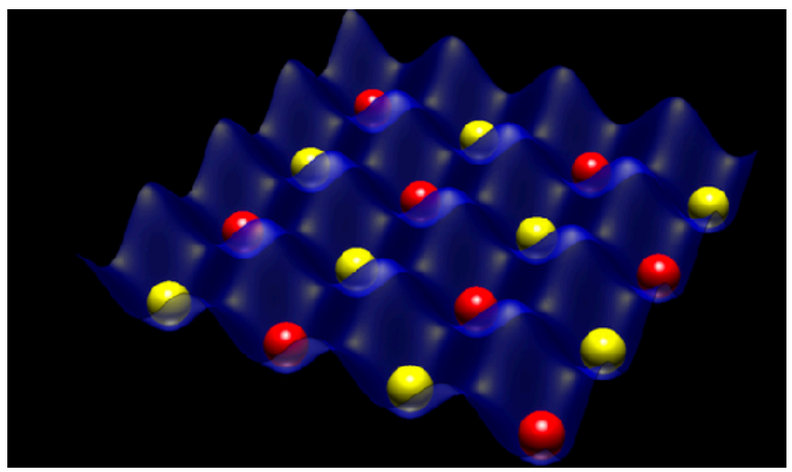


Physical realization



- Superconducting
- Photonic
- Cold atoms
- Trapped ions





But what is it good for...

Potential applications of quantum computing

Potential applications of quantum computing

- Quantum chemistry simulation (For material science, pharmacology, battery tech…)

Potential applications of quantum computing

- Quantum chemistry simulation (For material science, pharmacology, battery tech…)
- Breaking cryptographic schemes

Potential applications of quantum computing

- Quantum chemistry simulation (For material science, pharmacology, battery tech…)
- Breaking cryptographic schemes
- Optimization?

Potential applications of quantum computing

- Quantum chemistry simulation (For material science, pharmacology, battery tech…)
- **Breaking cryptographic schemes!**
- Optimization?

Which cryptographic schemes are quantum-vulnerable?

Which schemes are quantum-vulnerable?

Which schemes are quantum-vulnerable?

- RSA

Which schemes are quantum-vulnerable?

- RSA
- Diffie-Hellman (ordinary and elliptic curve)

Which schemes are quantum-vulnerable?

- RSA
- Diffie-Hellman (ordinary and elliptic curve)

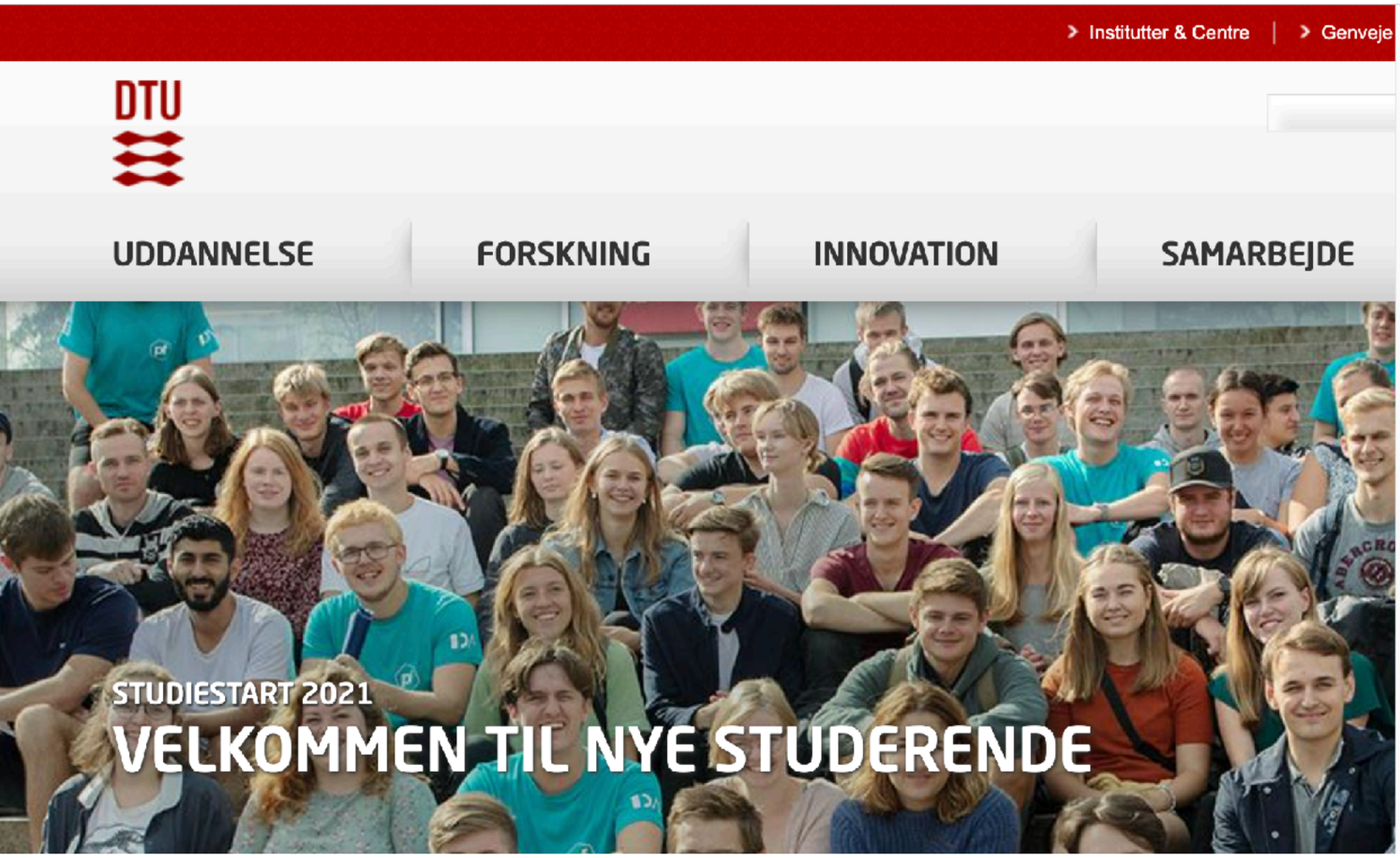
=>All* currently used public-key crypto!

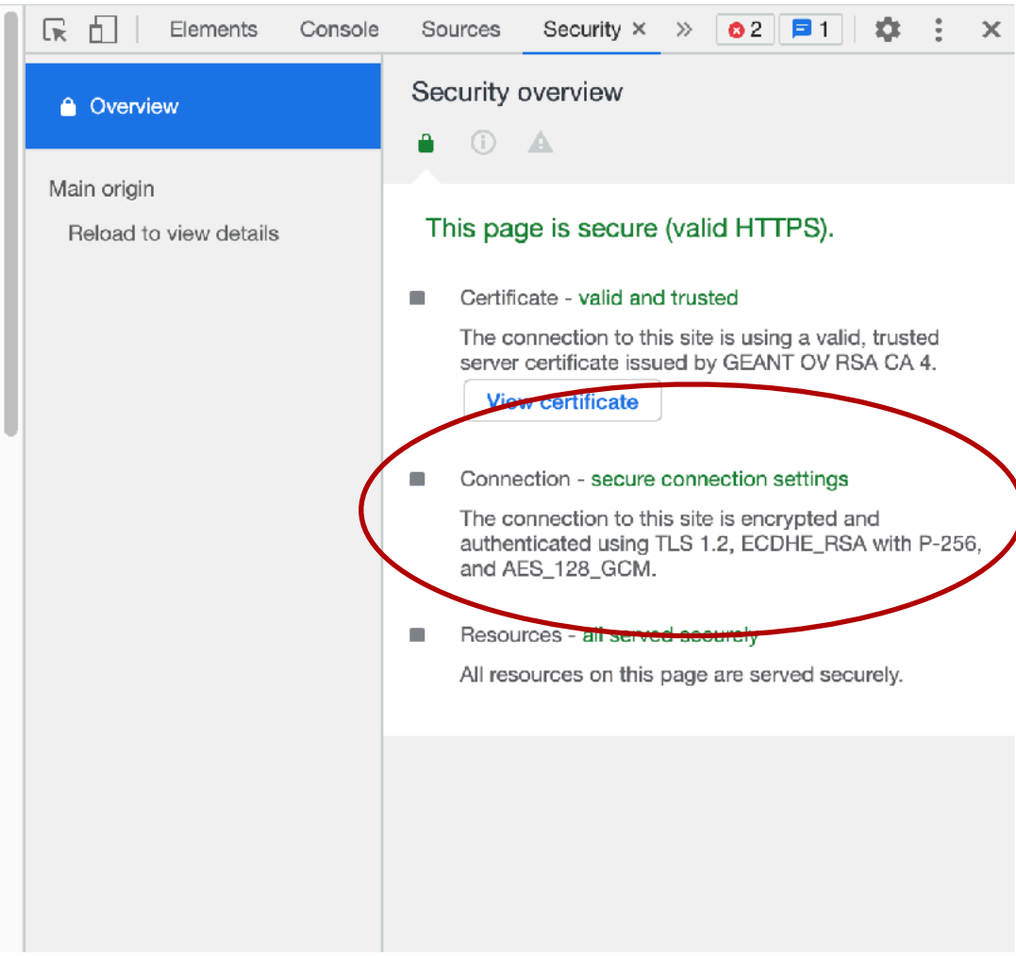
Where are the broken schemes?

Discuss in pairs and collect examples: what technology you have used today that depends on quantum-broken crypto?

Where is the broken stuff?

Example: TLS





Quantum vulnerabilities in TLS

Breakdown of TLS used by dtu.dk and Brave 1.28.106

TLS (TLS 1.2, ECDHE_RSA
with P-256, and AES_128_GCM)

Quantum vulnerabilities in TLS

Breakdown of TLS used by dtu.dk and Brave 1.28.106

TLS (TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM)

Handshake: Authenticated key exchange, ECDHE_RSA with P-256

Quantum vulnerabilities in TLS

Breakdown of TLS used by dtu.dk and Brave 1.28.106

TLS (TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM)

Handshake: Authenticated key exchange, ECDHE_RSA with P-256

Session: Authenticated encryption with associated data, Galois Counter Mode (AES_128_GCM)

Quantum vulnerabilities in TLS

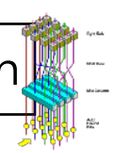
Breakdown of TLS used by dtu.dk and Brave 1.28.106

TLS (TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM)

Handshake: Authenticated key exchange, ECDHE_RSA with P-256

Session: Authenticated encryption with associated data, Galois Counter Mode (AES_128_GCM)

Block cipher: AES 128



AES round function

Quantum vulnerabilities in TLS

Breakdown of TLS used by dtu.dk and Brave 1.28.106

TLS (TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM)

Handshake: Authenticated key exchange, ECDHE_RSA with P-256

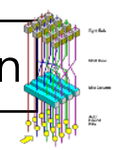
Session: Authenticated encryption with associated data, Galois Counter Mode (AES_128_GCM)

Key Exchange ECDHE (Elliptic curve Diffie Hellman) with curve P-256

Digital signature scheme: RSA hash-then-sign PKCS#1 v1.5

Block cipher: AES 128

AES round function



Quantum vulnerabilities in TLS

Breakdown of TLS used by dtu.dk and Brave 1.28.106

TLS (TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM)

Handshake: Authenticated key exchange, ECDHE_RSA with P-256

Session: Authenticated encryption with associated data, Galois Counter Mode (AES_128_GCM)

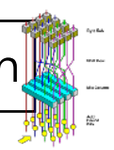
Key Exchange ECDHE (Elliptic curve Diffie Hellman) with curve P-256

Digital signature scheme: RSA hash-then-sign PKCS#1 v1.5

Block cipher: AES 128

DH problem

AES round function



Quantum vulnerabilities in TLS

Breakdown of TLS used by dtu.dk and Brave 1.28.106

TLS (TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM)

Handshake: Authenticated key exchange, ECDHE_RSA with P-256

Session: Authenticated encryption with associated data, Galois Counter Mode (AES_128_GCM)

Key Exchange ECDHE (Elliptic curve Diffie Hellman) with curve P-256

Digital signature scheme: RSA hash-then-sign PKCS#1 v1.5

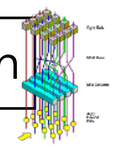
Block cipher: AES 128

DH problem

Plain RSA signature scheme

Hash function SHA-384, Merkle-Damgård

AES round function



Quantum vulnerabilities in TLS

Breakdown of TLS used by dtu.dk and Brave 1.28.106

TLS (TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM)

Handshake: Authenticated key exchange, ECDHE_RSA with P-256

Session: Authenticated encryption with associated data, Galois Counter Mode (AES_128_GCM)

Key Exchange ECDHE (Elliptic curve Diffie Hellman) with curve P-256

Digital signature scheme: RSA hash-then-sign PKCS#1 v1.5

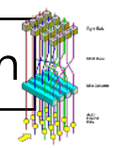
Block cipher: AES 128

DH problem

Plain RSA signature scheme

Hash function SHA-384, Merkle-Damgård

AES round function



RSA problem

Quantum vulnerabilities in TLS

Breakdown of TLS used by dtu.dk and Brave 1.28.106

TLS (TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM)

Handshake: Authenticated key exchange, ECDHE_RSA with P-256

Session: Authenticated encryption with associated data, Galois Counter Mode (AES_128_GCM)

Key Exchange ECDHE (Elliptic curve Diffie Hellman) with curve P-256

Digital signature scheme: RSA hash-then-sign PKCS#1 v1.5

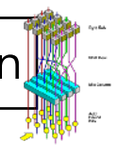
Block cipher: AES 128

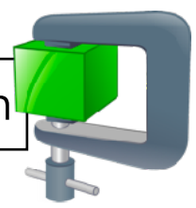
DH problem

Plain RSA signature scheme

Hash function SHA-384, Merkle-Damgård

AES round function





Compression function

RSA problem

Quantum vulnerabilities in TLS

Breakdown of TLS used by dtu.dk and Brave 1.28.106

TLS (TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM)

Handshake: Authenticated key exchange, ECDHE_RSA with P-256

Session: Authenticated encryption with associated data, Galois Counter Mode (AES_128_GCM)

Key Exchange ECDHE (Elliptic curve Diffie Hellman) with curve P-256

Digital signature scheme: RSA hash-then-sign PKCS#1 v1.5

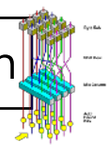
Block cipher: AES 128

DH problem

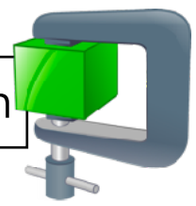
Plain RSA signature scheme

Hash function SHA-384, Merkle-Damgård

AES round function



Compression function



RSA problem

Quantum vulnerabilities in TLS

Breakdown of TLS used by dtu.dk and Brave 1.28.106

TLS (TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM)

Handshake: Authenticated key exchange, ECDHE_RSA with P-256

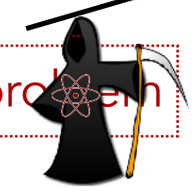
Session: Authenticated encryption with associated data, Galois Counter Mode (AES_128_GCM)

Key Exchange ECDHE (Elliptic curve Diffie Hellman) with curve P-256

Digital signature scheme: RSA hash-then-sign PKCS#1 v1.5

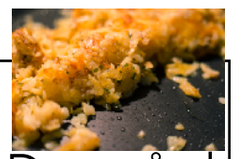
Block cipher: AES 128

DH problem

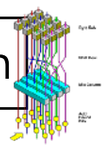


Plain RSA signature scheme

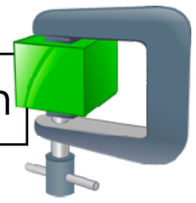
Hash function SHA-384, Merkle-Damgård



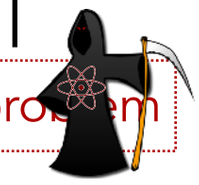
AES round function



Compression function



RSA problem



Quantum vulnerabilities in TLS

Breakdown of TLS used by dtu.dk and Brave 1.28.106

TLS (TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM)

Handshake: Authenticated key exchange, ECDHE_RSA with P-256

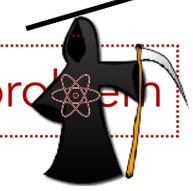
Session: Authenticated encryption with associated data, Galois Counter Mode (AES_128_GCM)

Key Exchange ECDHE (Elliptic curve Diffie Hellman) with curve P-256

Digital signature scheme: RSA hash-then-sign PKCS#1 v1.5

Block cipher: AES 128

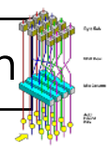
DH problem



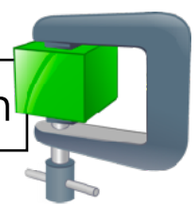
Plain RSA signature scheme

Hash function SHA-384, Merkle-Damgård

AES round function



Compression function



Quantum vulnerabilities in TLS

Breakdown of TLS used by dtu.dk and Brave 1.28.106

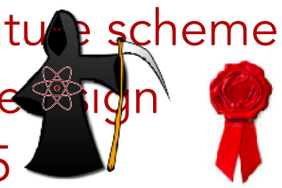
TLS (TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM)

Handshake: Authenticated key exchange, ECDHE_RSA with P-256

Session: Authenticated encryption with associated data, Galois Counter Mode (AES_128_GCM)

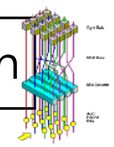
Key Exchange ECDH (Elliptic curve Diffie Hellman) with curve P-256

Digital signature scheme: RSA hash-then-sign PKCS#1 v1.5

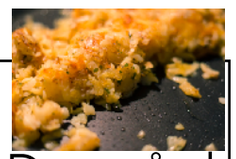


Block cipher: AES 128

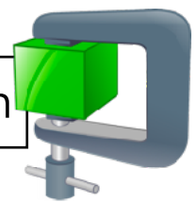
AES round function



Hash function SHA-384, Merkle-Damgård



Compression function



Quantum vulnerabilities in TLS

Breakdown of TLS used by dtu.dk and Brave 1.28.106

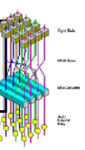
TLS (TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM)

Handshake: Authenticated key exchange

??????????????????????????????

Session: Authenticated encryption with associated data, Galois Counter Mode (AES_128_GCM)

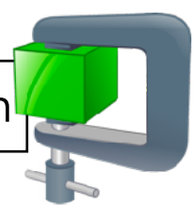
Block cipher: AES 128



AES round function

Hash function
SHA-384, Merkle-Damgård

Compression function



How does a quantum computer break crypto?

Example: RSA

- Public-key cryptosystem: encryption and digital signature
- Based on number theory
- Used e.g. in HTTPS, Certificates…
- Can be broken via *factoring*

Factoring

Factoring

- Multiplying is easy.

Factoring

- Multiplying is easy.

$$7 \cdot 11$$

Factoring

- Multiplying is easy.

$$7 \cdot 11$$

$$47 \cdot 53$$

Factoring

- Multiplying is easy.

$$7 \cdot 11$$

$$47 \cdot 53$$

$$5201819300953669437777897868400987444737 \cdot 27505893044478565097389357278392740789$$

Factoring

- Multiplying is easy.
- Factoring is hard!

$$7 \cdot 11$$

$$47 \cdot 53$$

$$5201819300953669437777897868400987444737 \cdot 27505893044478565097389357278392740789$$

Factoring

- Multiplying is easy.
- Factoring is hard!

$$7 \cdot 11$$

$$47 \cdot 53$$

$$5201819300953669437777897868400987444737 \cdot 27505893044478565097389357278392740789$$

$$55 = ? \cdot ?$$

Factoring

- Multiplying is easy.
- Factoring is hard!

$$7 \cdot 11$$

$$47 \cdot 53$$

$$5201819300953669437777897868400987444737 \cdot 27505893044478565097389357278392740789$$

$$55 = ? \cdot ?$$

$$143 = ? \cdot ?$$

Factoring

- Multiplying is easy.
- Factoring is hard!

$$7 \cdot 11$$

$$47 \cdot 53$$

$$5201819300953669437777897868400987444737 \cdot 27505893044478565097389357278392740789$$

$$55 = ? \cdot ?$$

$$143 = ? \cdot ?$$

$$1430806853287358879152132030080994132696671597708550332440811957233111032774 93 = ? \cdot ?$$

Factoring

- Multiplying is easy.
- Factoring is hard?

$$7 \cdot 11$$

$$47 \cdot 53$$

$$5201819300953669437777897868400987444737 \cdot 27505893044478565097389357278392740789$$

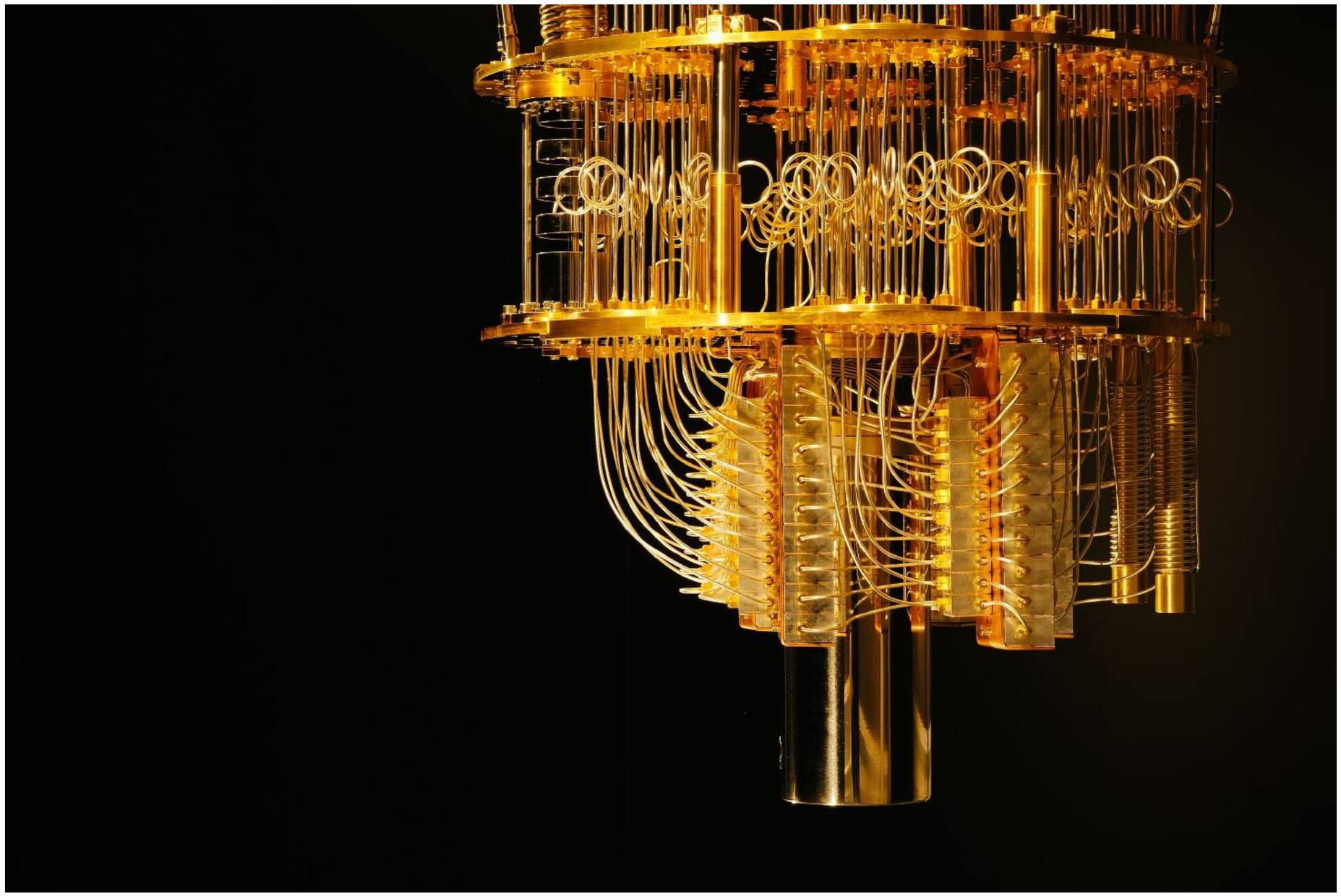
$$55 = ? \cdot ?$$

$$143 = ? \cdot ?$$

$$1430806853287358879152132030080994132696671597708550332440811957233111032774 93 = ? \cdot ?$$

Turns out that…

…it is not hard for quantum computers.



Factoring

How a quantum computer factors integers:

Problem: given N not prime, find $q \notin \{1, N\}$ such that $q \mid N$

Algorithm:

- Pick a random a with $1 < a < N$
- Compute $\gcd(a, N)$. If it's $\neq 1$ we found a factor (Yay!)
- Otherwise, let $f(x) = a^x \mod N$, find $r < N$ with $f(x + r) = f(x)$
- hope that r is even and $-1 \neq a^{r/2} \mod N$
- Output $\gcd(a^{r/2} - 1, N)$

Factoring

How a quantum computer fa

Problem: given N not prime,

Algorithm:

- Pick a random a with $1 < a < N$
- Compute $\gcd(a, N)$. If it's $\neq 1$ we found a factor (Yay!)
- Otherwise, let $f(x) = a^x \mod N$, find $r < N$ with $f(x + r) = f(x)$???
- hope that r is even and $-1 \neq a^{r/2} \mod N$
- Output $\gcd(a^{r/2} - 1, N)$

The period-finding problem

Period-finding via Fourier transform

- Otherwise, let $f(x) = a^x \mod N$ and find r with $f(x + r) = f(x)$????

Quantum Fourier transform

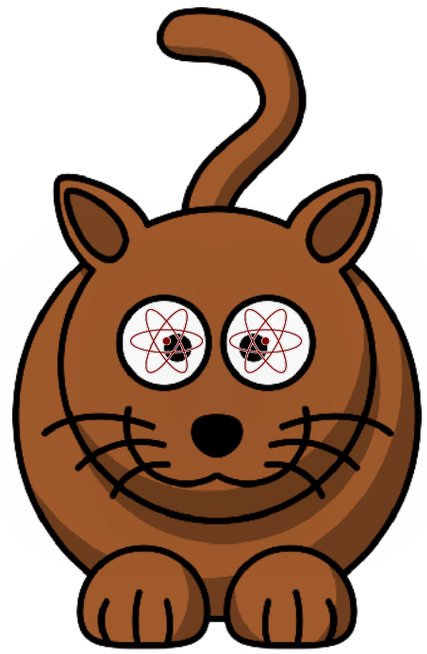
Cartoon slide (sorry!)

Quantum Fourier transform

Cartoon slide (sorry!)

Classical Computer

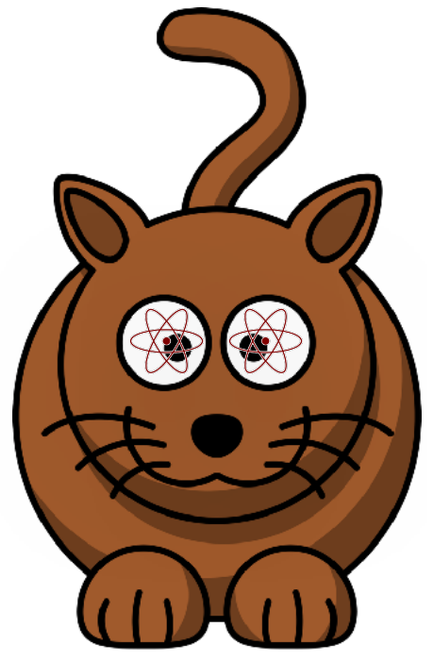
Quantum Computer



Quantum Fourier transform

Cartoon slide (sorry!)

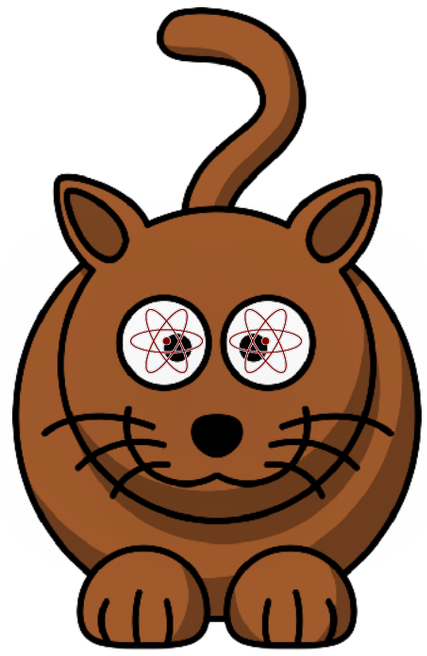
Classical Computer	Quantum Computer
Bits!	Qubits!
$x \in \{0,1\}^n$	$\lvert\psi\rangle \in \mathbb{C}^{2^n}$



Quantum Fourier transform

Cartoon slide (sorry!)

Classical Computer	Quantum Computer
Bits!	Qubits!
$x \in \{0,1\}^n$	$\lvert\psi\rangle \in \mathbb{C}^{2^n}$
Fourier sampling in $\mathcal{O}(\ell)$.	Fourier sampling in $\mathcal{O}(\log \ell)$.



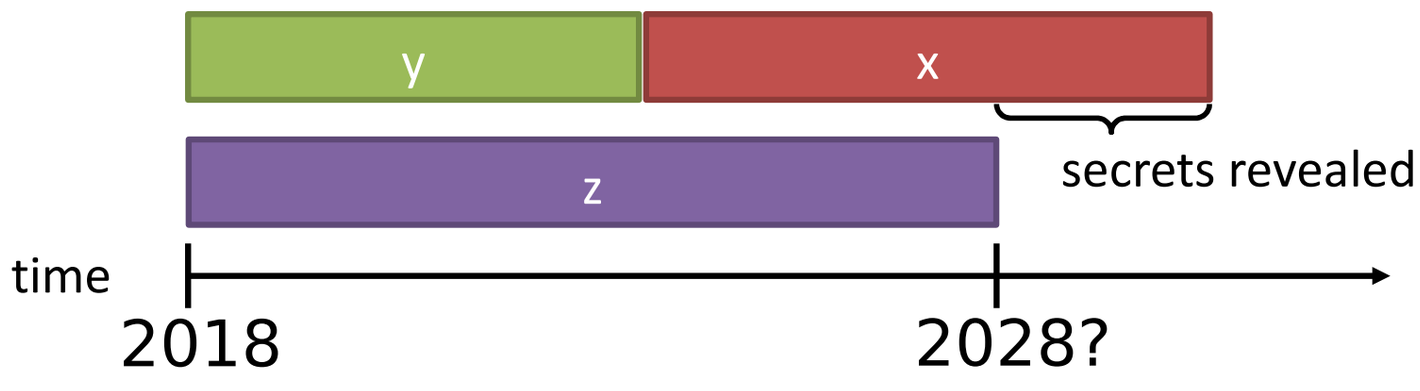
Assessing quantum attack risk

By when do we need to fix quantum-vulnerabilities?

Depends on:

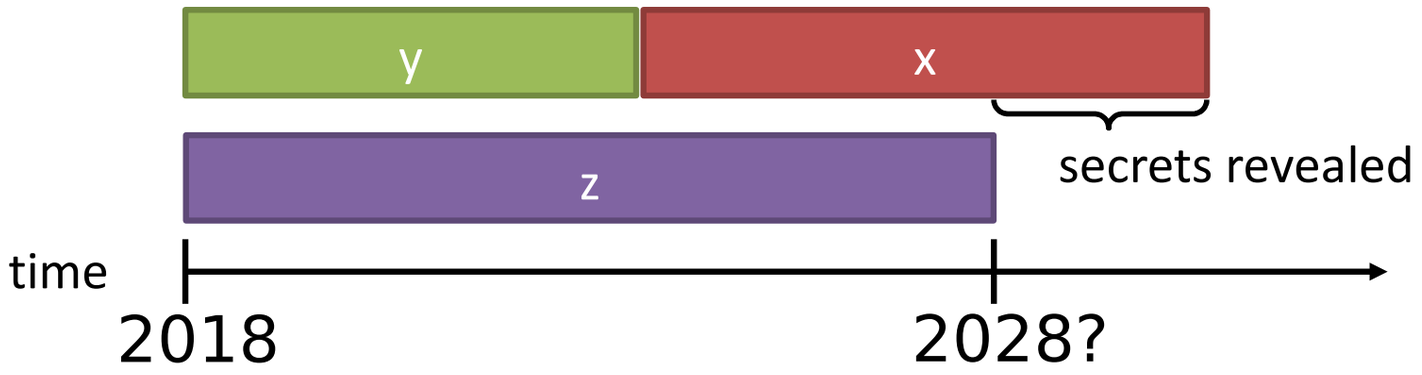
- How long do you need to keep your secrets secure? (x years)
- How much time will it take to re-tool the existing infrastructure? (y years)
- How long will it take for a large-scale quantum computer to be built? (z years)

Theorem (Mosca): If x + y > z, then worry.



Slide by Michele Mosca

By when do we need to fix quantum-vulnerabilities?



- How big is y?
- How big is x?
- How big is z? Hard to say… ⇒Exercise sheet!

Summary: quantum computing threat

- Quantum computers are fundamentally different from regular computers
- Quantum computers are currently not available
- They have *a* computing power *incomparable* to regular computers
- They are good at discovering *structure* in big mathematical objects
- Once they are built, they can be used to launch attacks against RSA and Diffie-Hellman