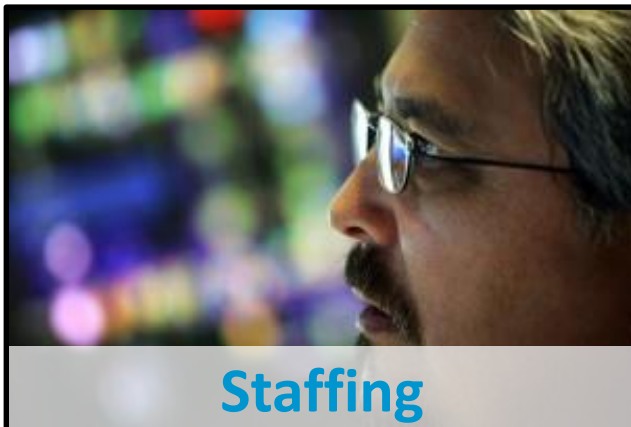
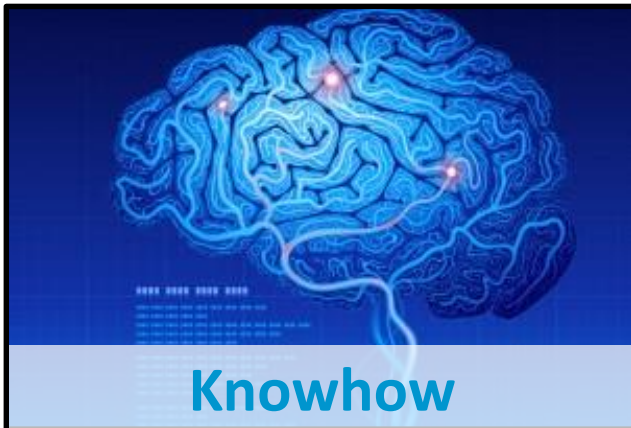


Quantum computers Vs. Modern cryptography

Kristof Verslype
Cryptographer, PhD
Smals Research



SUPPORT FOR E-GOVERNMENT



WWW.SMALS.BE



**Innovation with
new technologies**



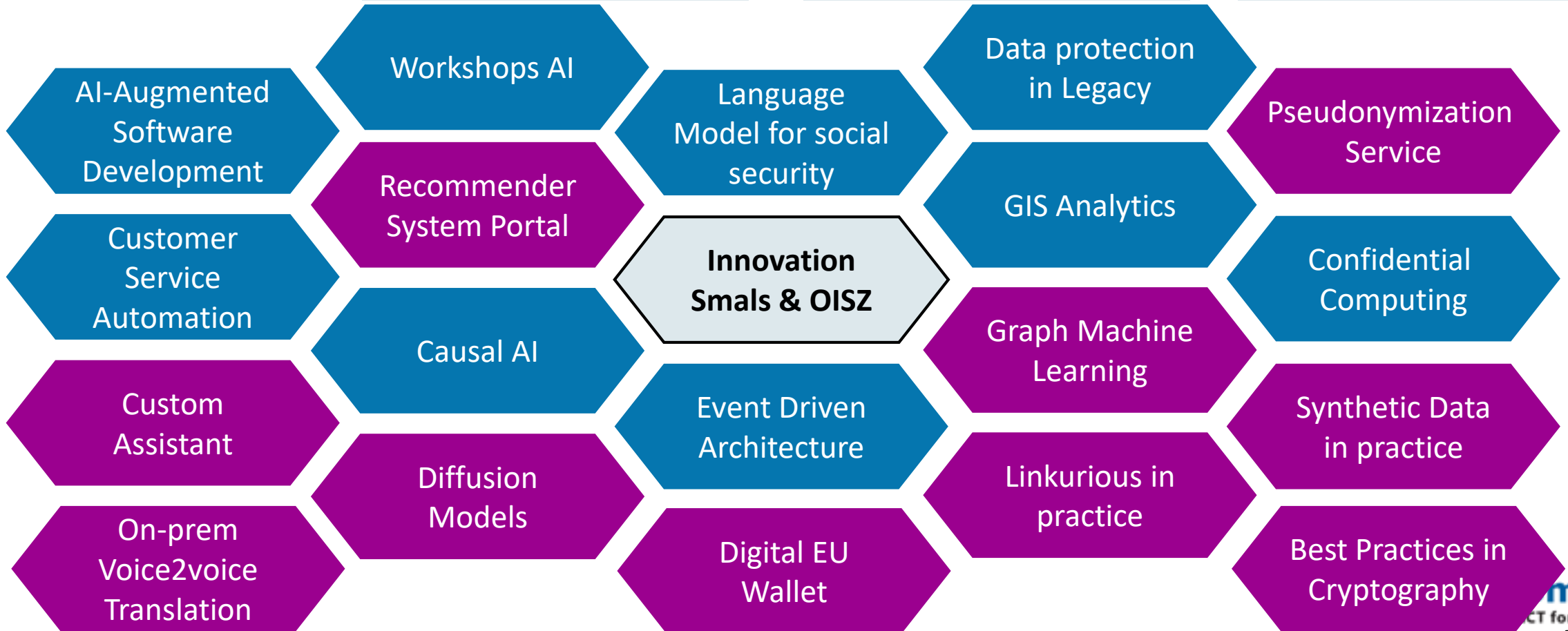
**Consultancy
& expertise**



**Internal & external
knowledge transfer**



**Support for
going live**



Kristof Verslype
Cryptographer, PhD
Smals Research



KU Leuven

PhD. of Engineering
Dept. CS, KU Leuven (2011)
Applied cryptography

Smals

- Cryptography for privacy
- Advice on cryptography
- Blockchain

No background in quantum physics



✉ kristof.verslype@smals.be

☎ +32(0)2 7875376

🌐 www.smals.be
www.smalsresearch.be
www.cryptov.net

🐦 @KristofVerslype

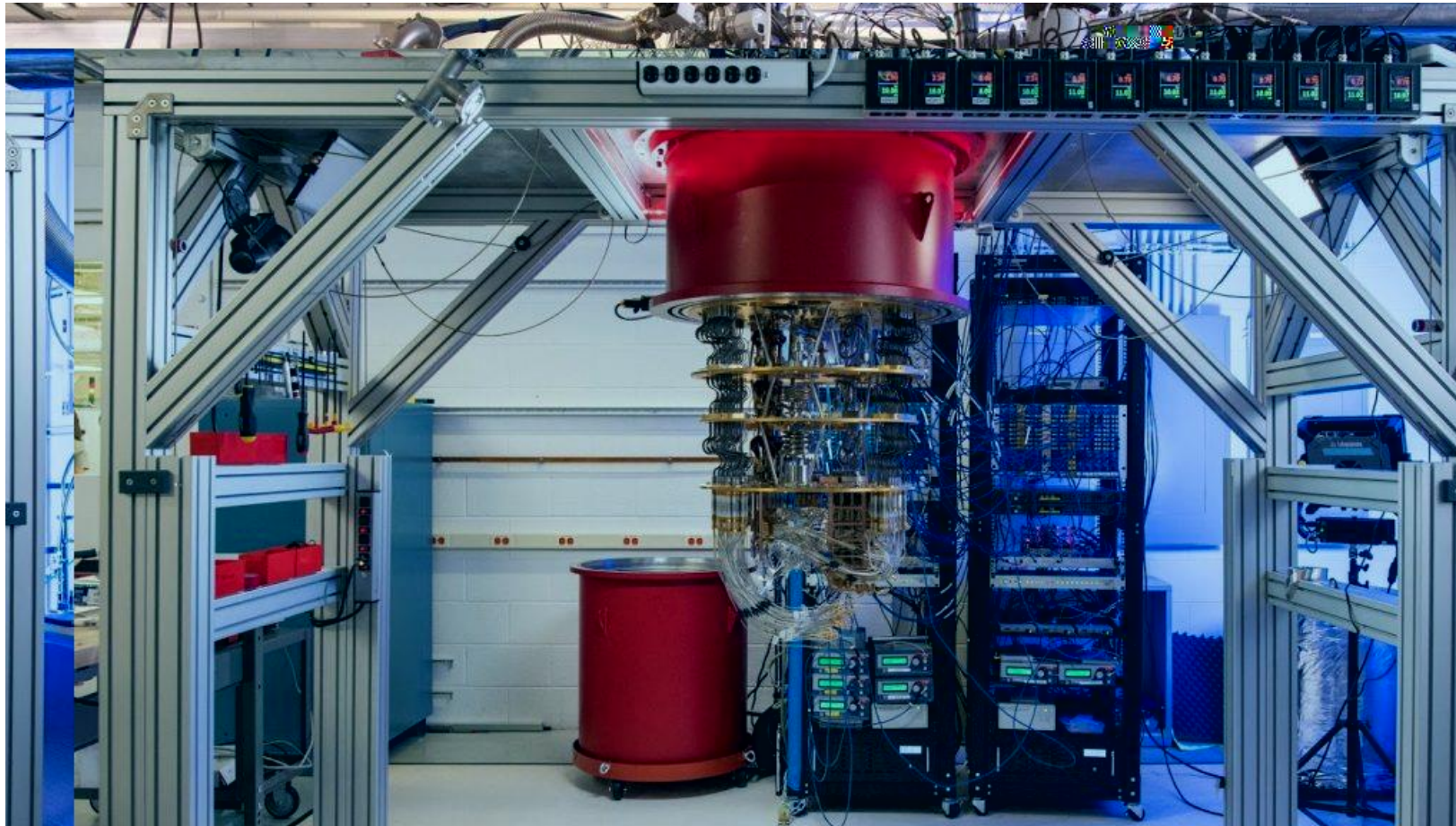
in [linkedin.com/in/verslype](https://www.linkedin.com/in/verslype)

23 oktober 2019



Article

Quantum supremacy using a programmable superconducting processor



27 oktober 2021



Two Chinese teams claim to have reached primacy with quantum computers

by Bob Yirka , Phys.org



Two Chinese teams claim to have reached quantum primacy with their quantum computers.

The teams, one from the University of Science and Technology of China (USTC) and the other from the Chinese Academy of Sciences (CAS), claim to have achieved quantum primacy with their quantum computers. This means that their quantum computers can perform a task that is beyond the capabilities of classical computers. The teams' work is a significant milestone in the development of quantum computing.

27 januari 2022

QUANTUM APOCALYPSE

EXPERTS WARN OF "QUANTUM APOCALYPSE"

"IT'S A THREAT TO OUR WAY OF LIFE."

Experts are warning that quantum computers could eventually overpower conventional **encryption methods**, a potentially dangerous fate for humanity that they're evocatively dubbing the "quantum apocalypse,

— MISHA FRIEDMAN/CONTRIBUTOR

Is the quantum army advancing at a rapid pace?



Agenda

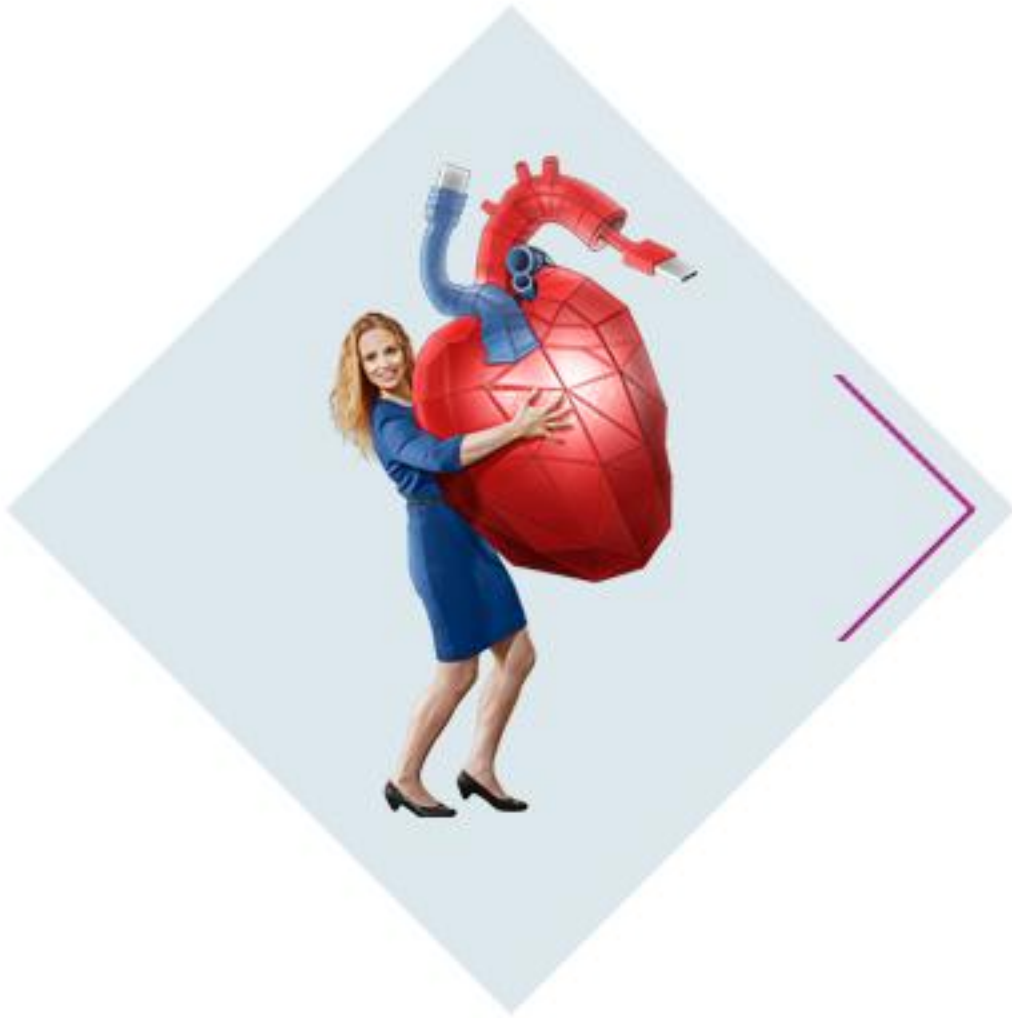
Quantum computer Vs. classical computer

Quantum computers in practice

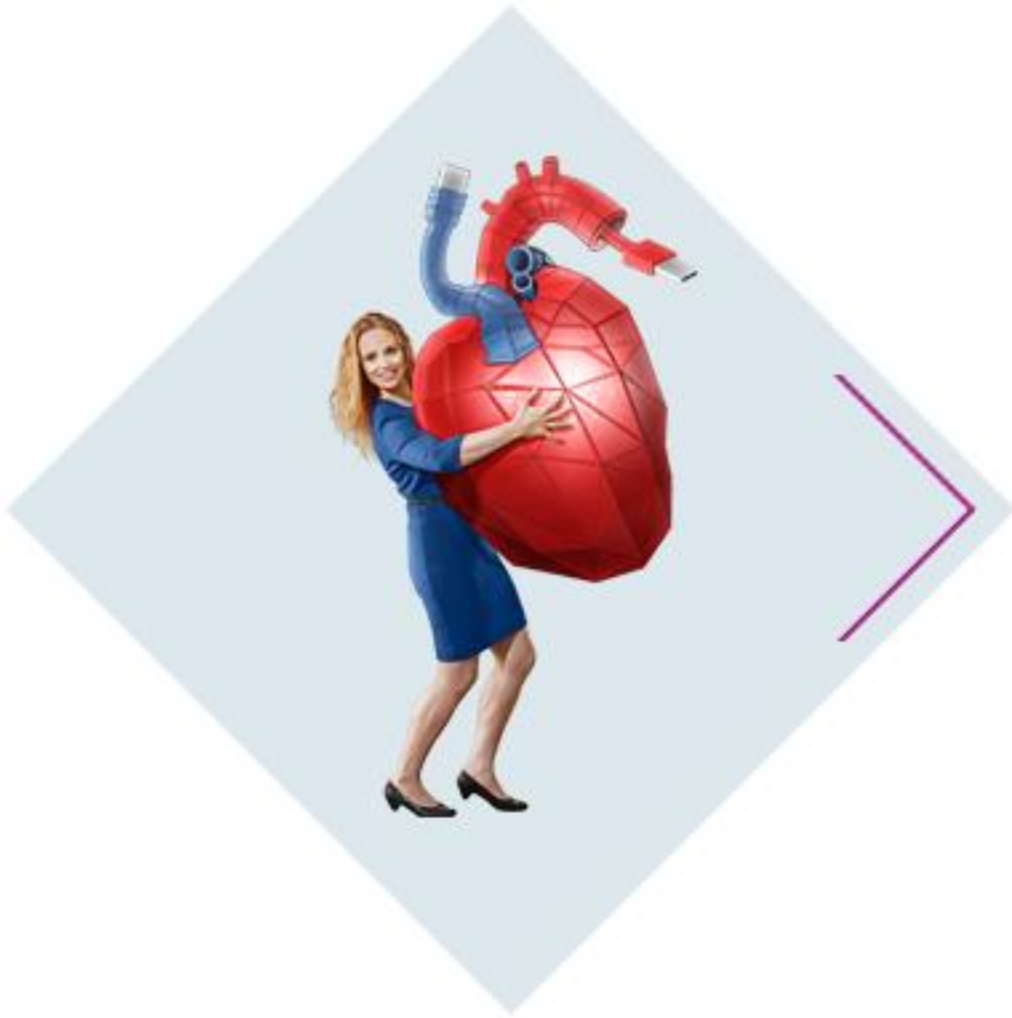
Crypto-apocalypse now?

Quantum-resistant cryptography

Conclusions



Agenda



Quantum computer Vs. classical computer

Quantum computers in practice

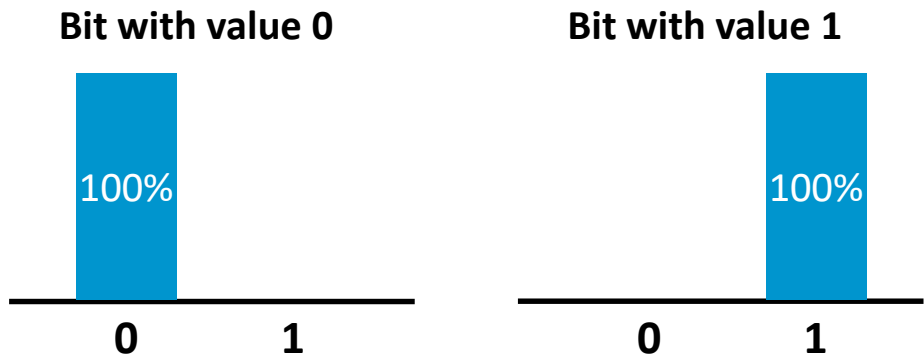
Crypto-apocalypse now?

Quantum-resistant cryptography

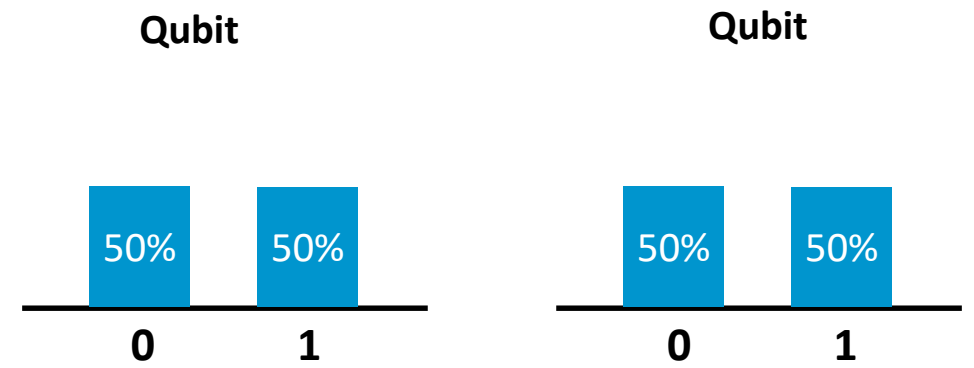
Conclusions

Superposition simplified

Classical computer



Quantum Computer



Electrical charge

The value is already fixed before the measurement

Measurement no impact on state bit

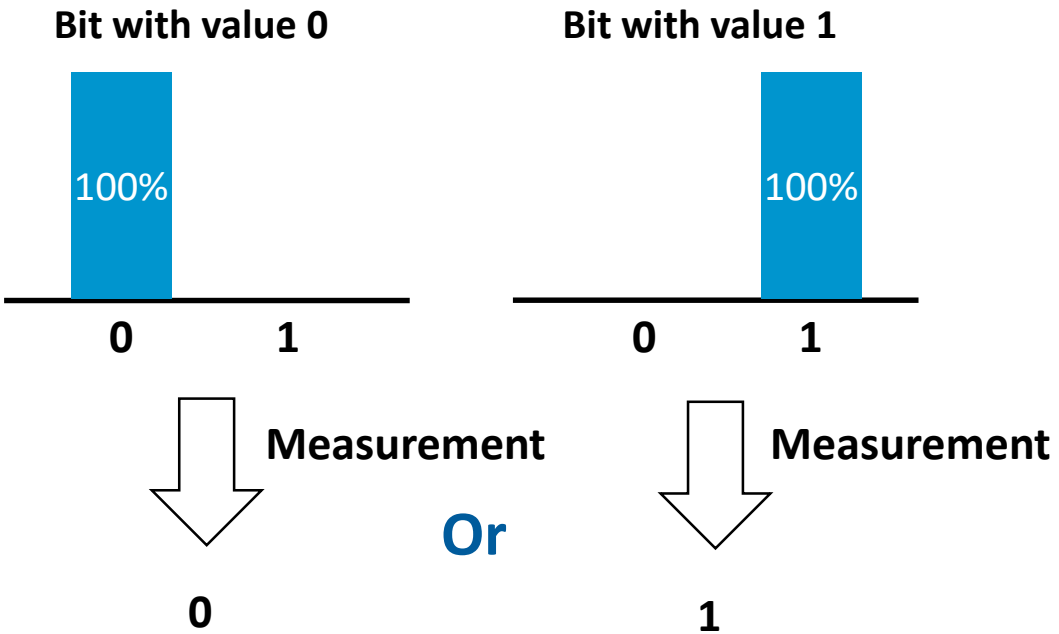
(Sub)atomic 'particle' (e.g.. Polarization photon, spin electron)

Value undetermined (smeared out) until measurement

Measurement destroys quantum state: The possible becomes a concrete value

Superposition simplified

Classical computer

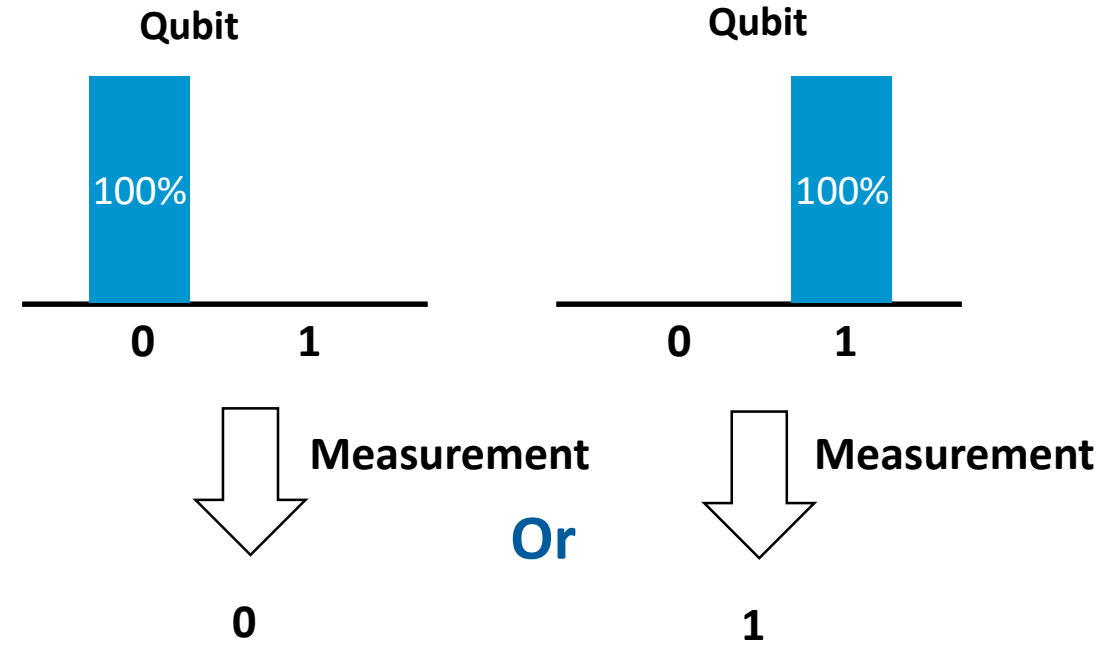


Electrical charge

The value is already fixed before the measurement

Measurement no impact on state bit

Quantum Computer

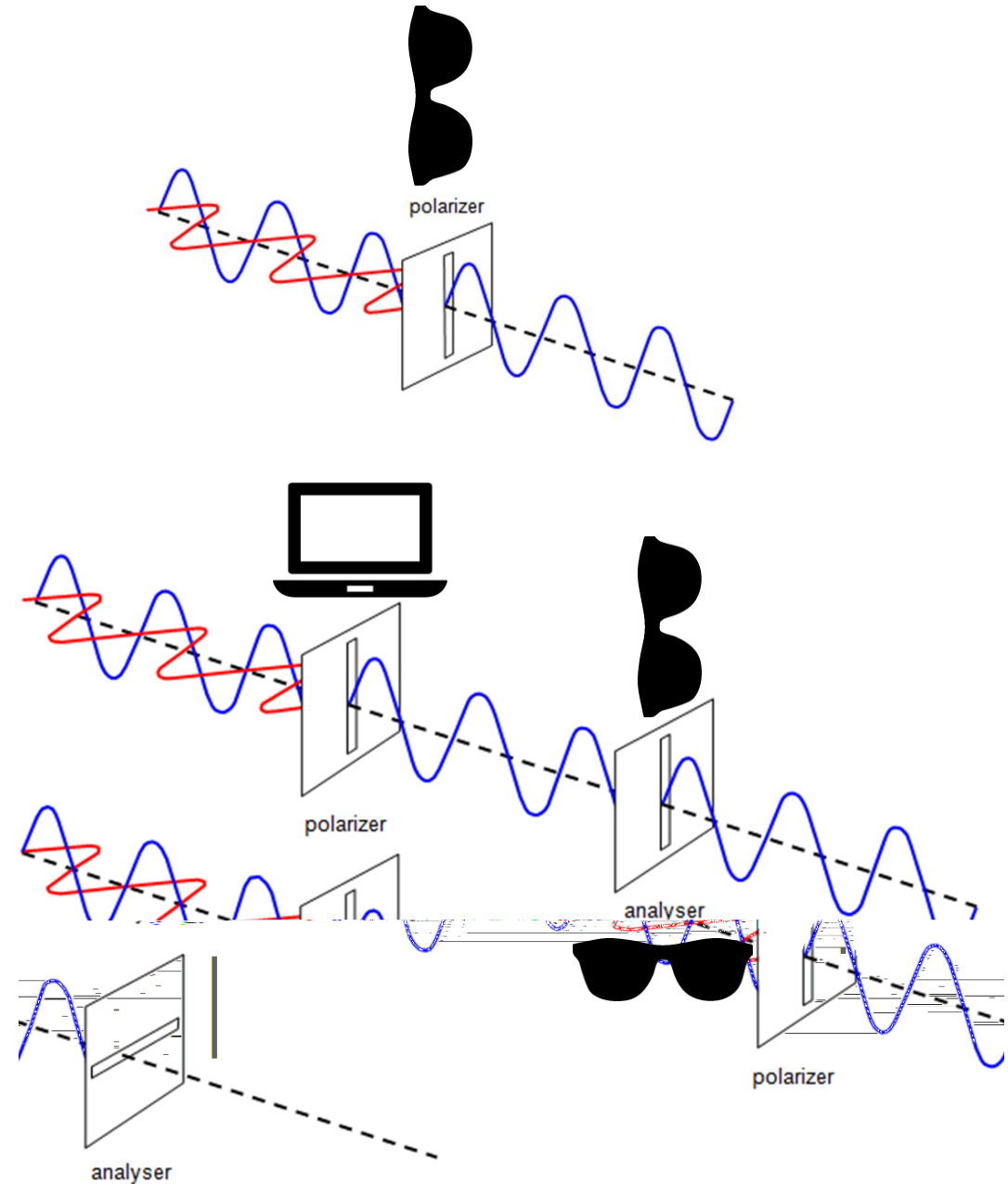
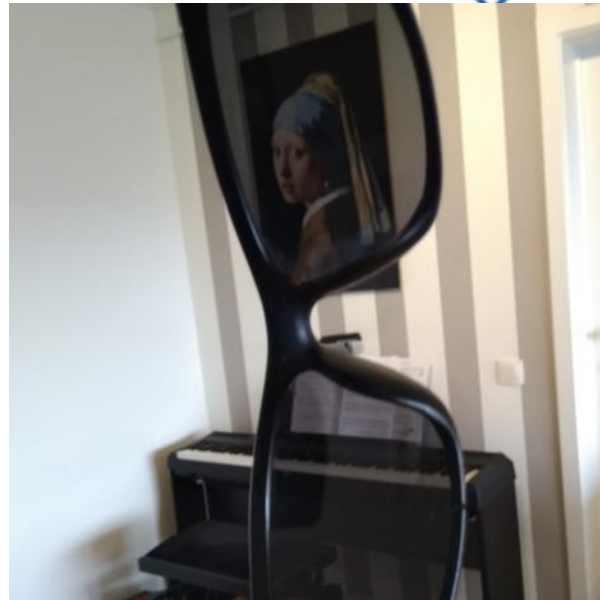


(Sub)atomic 'particle' (e.g.. Polarization photon, spin electron)

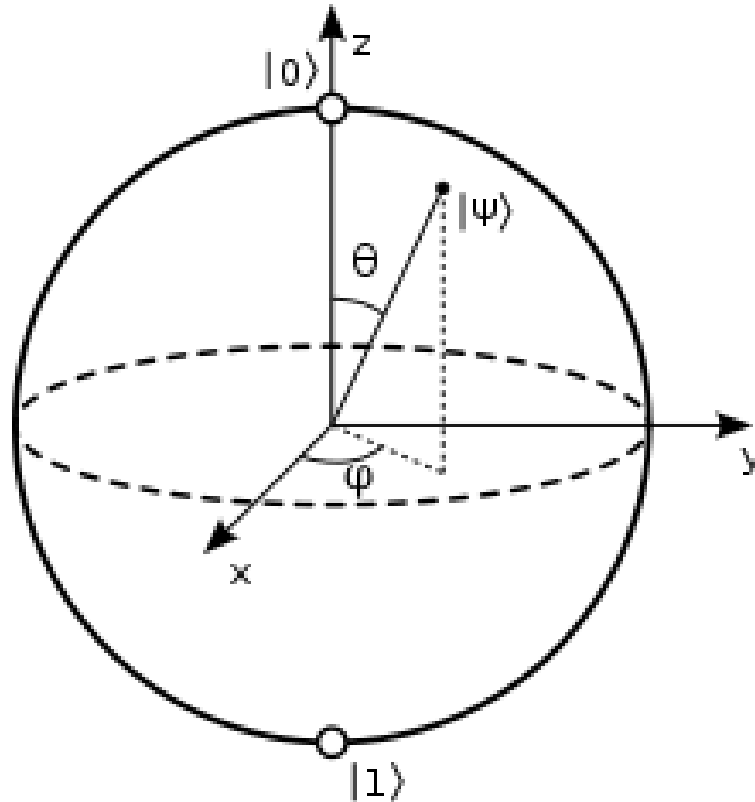
Value undetermined (smeared out) until measurement

Measurement destroys quantum state: The possible becomes a concrete value

Polarisation of photons – Sun glasses experiment



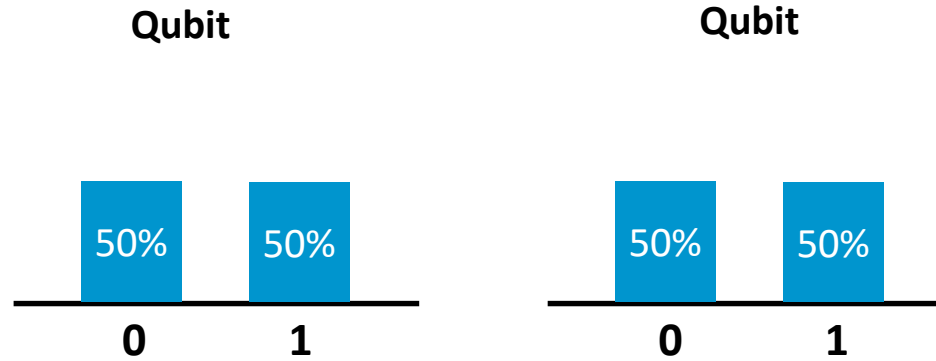
Bloch Sphere



Dirac or Bra-ket notation of qubit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Entanglement



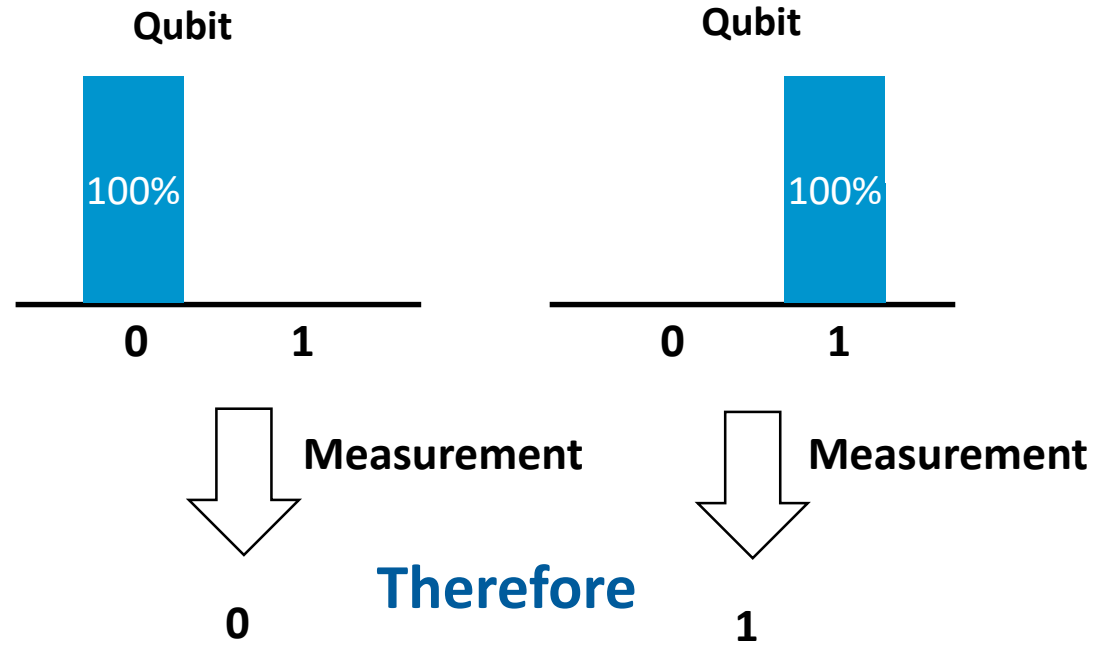
Correlation between measurements of related particles

Measuring one qubit is sufficient to know the result of another

Independent of distance between qubits
(\leftrightarrow Newtonian physics)

Entanglement of more than 2 qubits is also possible

Entanglement



Correlation between measurements of related particles

Measuring one qubit is sufficient to know the result of another

Independent of distance between qubits (\leftrightarrow Newtonian physics)

Entanglement of more than 2 qubits is also possible

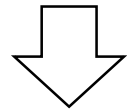
Entanglement

Superposition

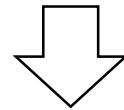
Value is undetermined until the time of measurement

Entanglement

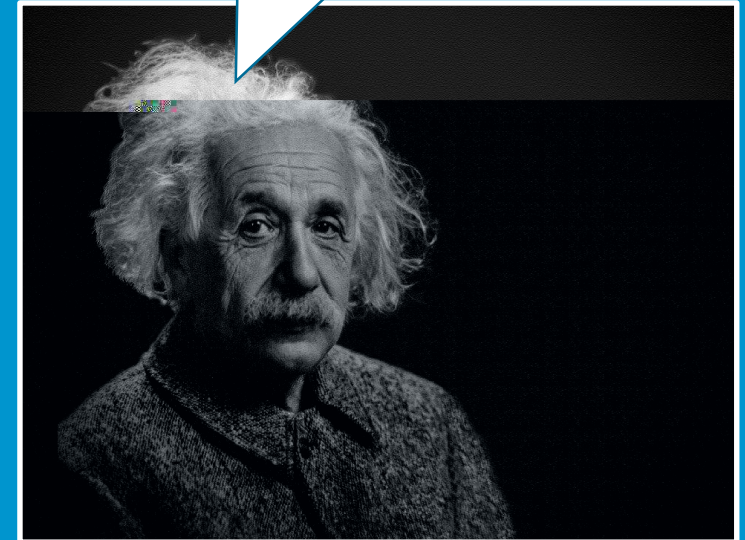
Measurement of one qubit has impact on the outcome of measurement of another qubit



**At the time of measurement of one qubit,
the value of the other qubit is determined**
→ Type of connection, independent of distance



Spukhafte Fernwirkung!
(Spooky action at a distance!)



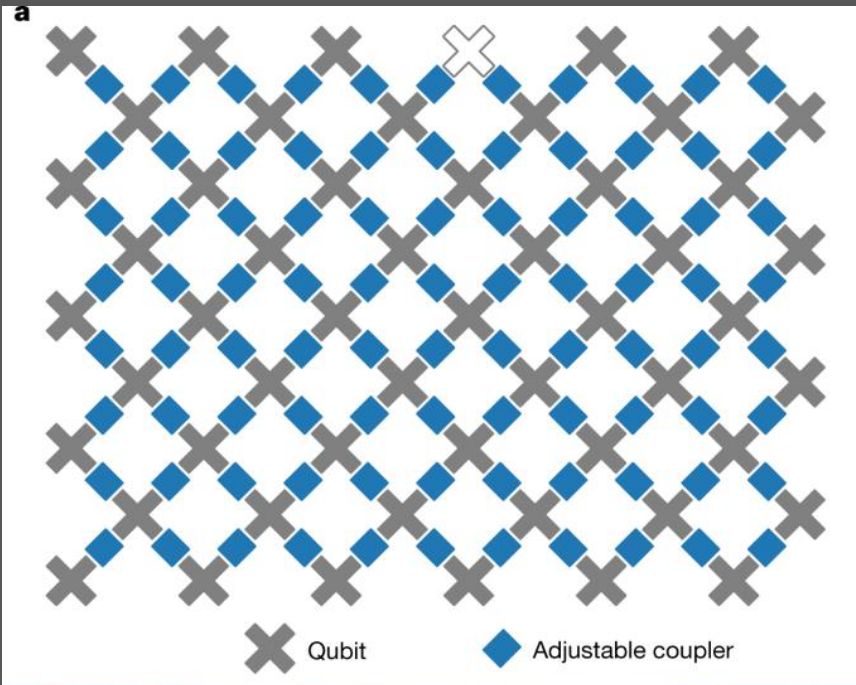
Confirmed with high probability
by experiments
(e.g. Bell test experiments)
No “hidden variables”

Quantum state

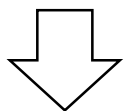
- ❖ **Superposition**
Value qubit undetermined until time of measurement
- ❖ **Entanglement**
Measurement of one qubit has an impact on the outcome of measurement of another qubit

Quantum logic gates
Pauli-X, Hadamard, SWAP, ...

Quantum state

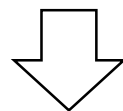


Building bricks for calculations: Logic gates



Classical computer

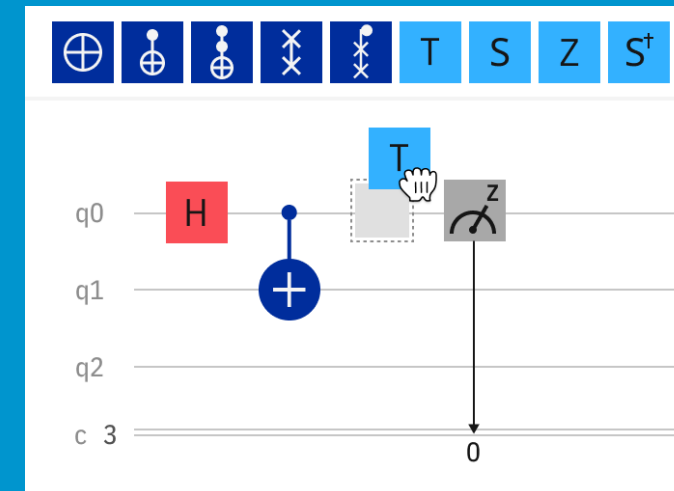
Logic gates:
AND, NOT, OR, XOR, ...



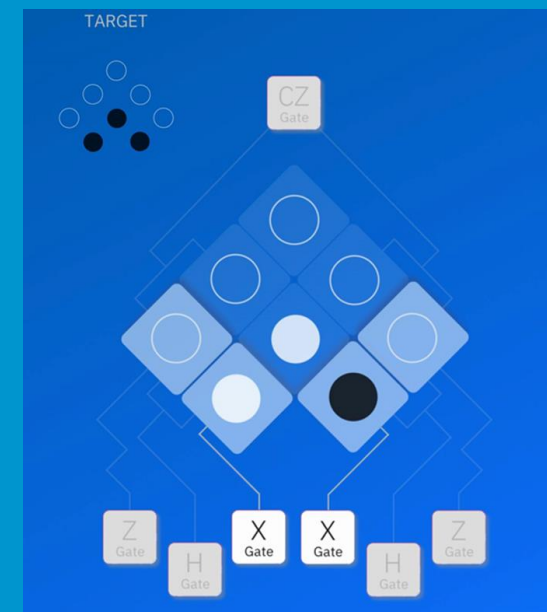
Quantum Computer

Quantum logic gates:
Pauli-X, Hadamard, SWAP, ...

- ❖ **Quantum instruction sets**
Convert algorithms to quantum processor instructions
vb. Quil, OpenQASM
- ❖ **Quantum software development kits**
Tools to create and manipulate
vb. Qiskit, ProjectQ, Forest
Often extensions existing programming languages
- ❖ **Quantum programming languages**
Quantum Computation Language (QCL), Q#, Q language



IBM Quantum Experience



IBM Hello quantum app

Observation

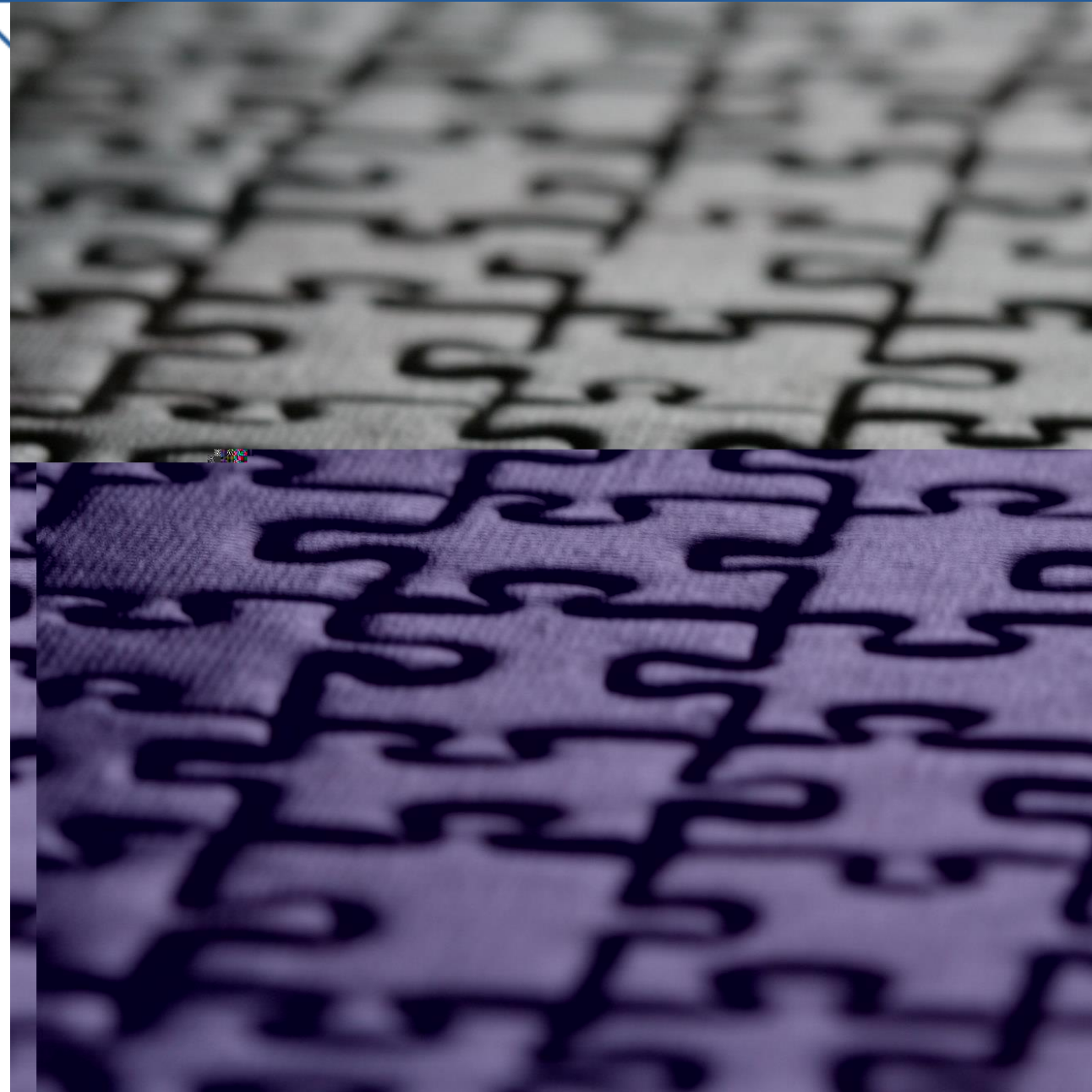
When people don't understand something, they may attribute mythical properties to it

Misconception

“Quantum computers will be able to solve all problems that are difficult (or even impossible) for classical computers.”

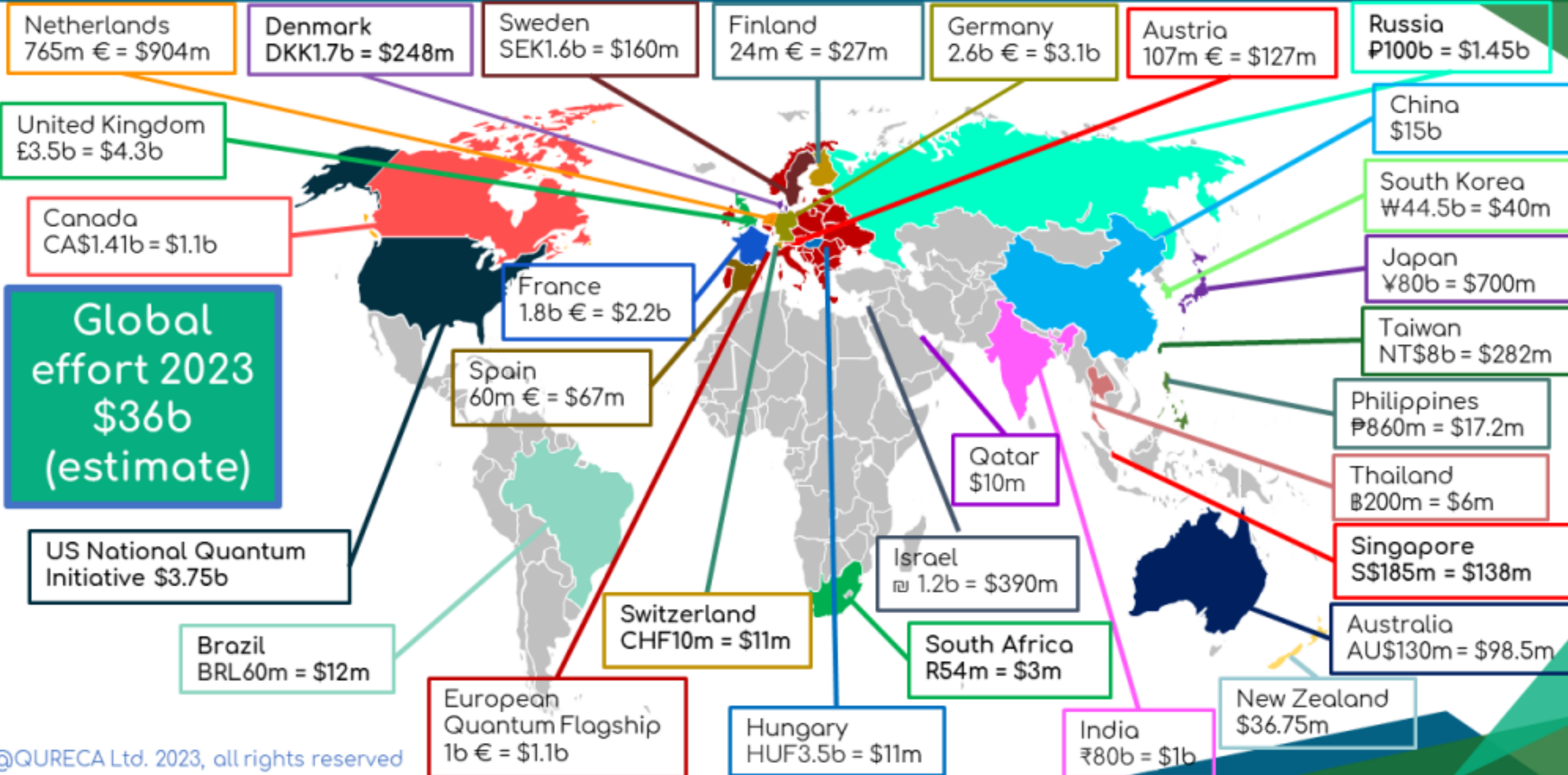
Depends on problem

- ❖ Probably no significant added value
E.g. Combinatorial search problems such as traveling salesman problem (NP-hard)
- ❖ Potentially added value
E.g. *Deep learning*
- ❖ Clear added value
E.g. Simulations natural processes
E.g. **Breaking modern cryptography**



Quantum effort worldwide

Global quantum technology market is projected to reach \$42.4 billion by 2027



Universal quantum computers

- ❖ Relying on unintuitive principles such as entanglement and superposition
- ❖ Have Qubits – (sub)atomic particles / waves – as the smallest storage and calculation unit
- ❖ Calculation is done in a fundamentally different way than with classical computers
- ❖ Are – on paper – powerful for a limited group of problems



" O T

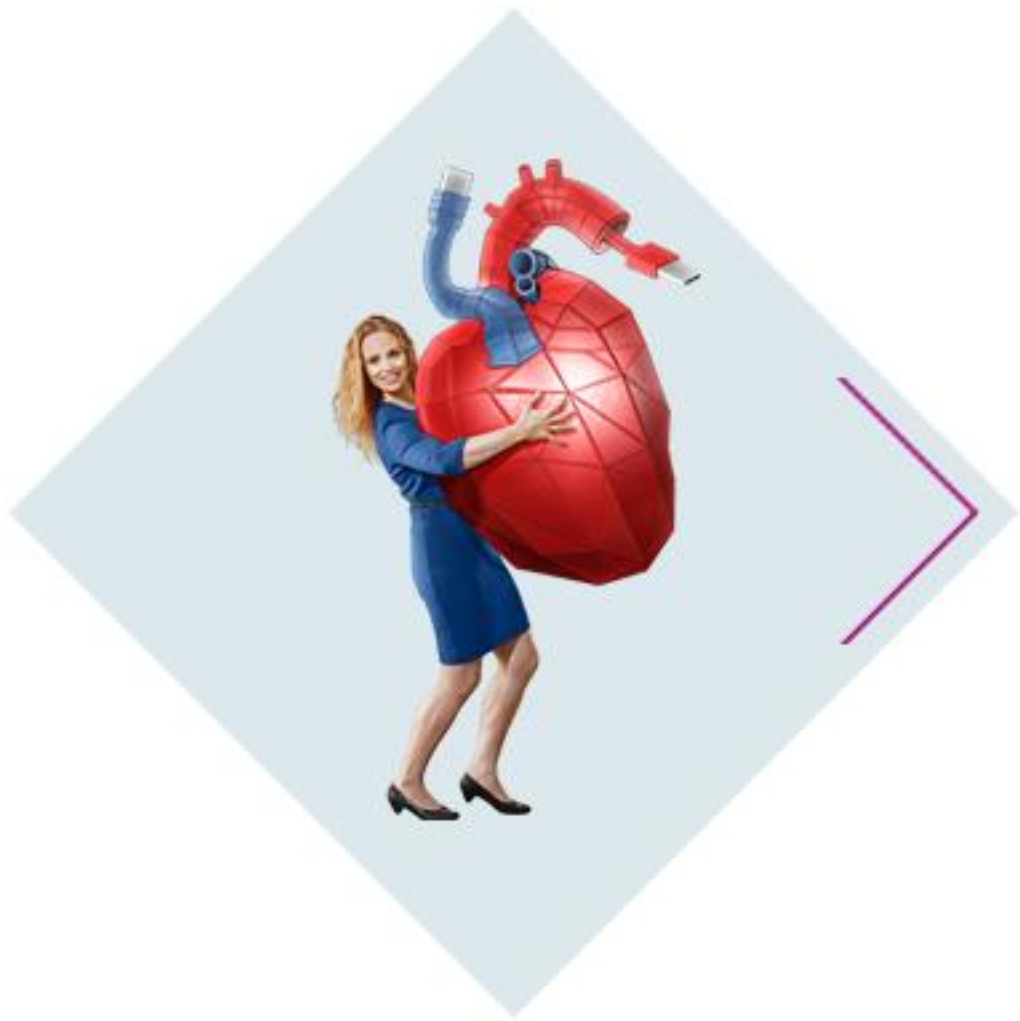
O

"

Koen Bertels

Belgian professor at TU Delft

Head Quantum Computer Architectures Lab TU Delft



Agenda

Quantum computer Vs. classical computer

Quantum computers in practice

Crypto-apocalypse now?

Quantum-resistant cryptography

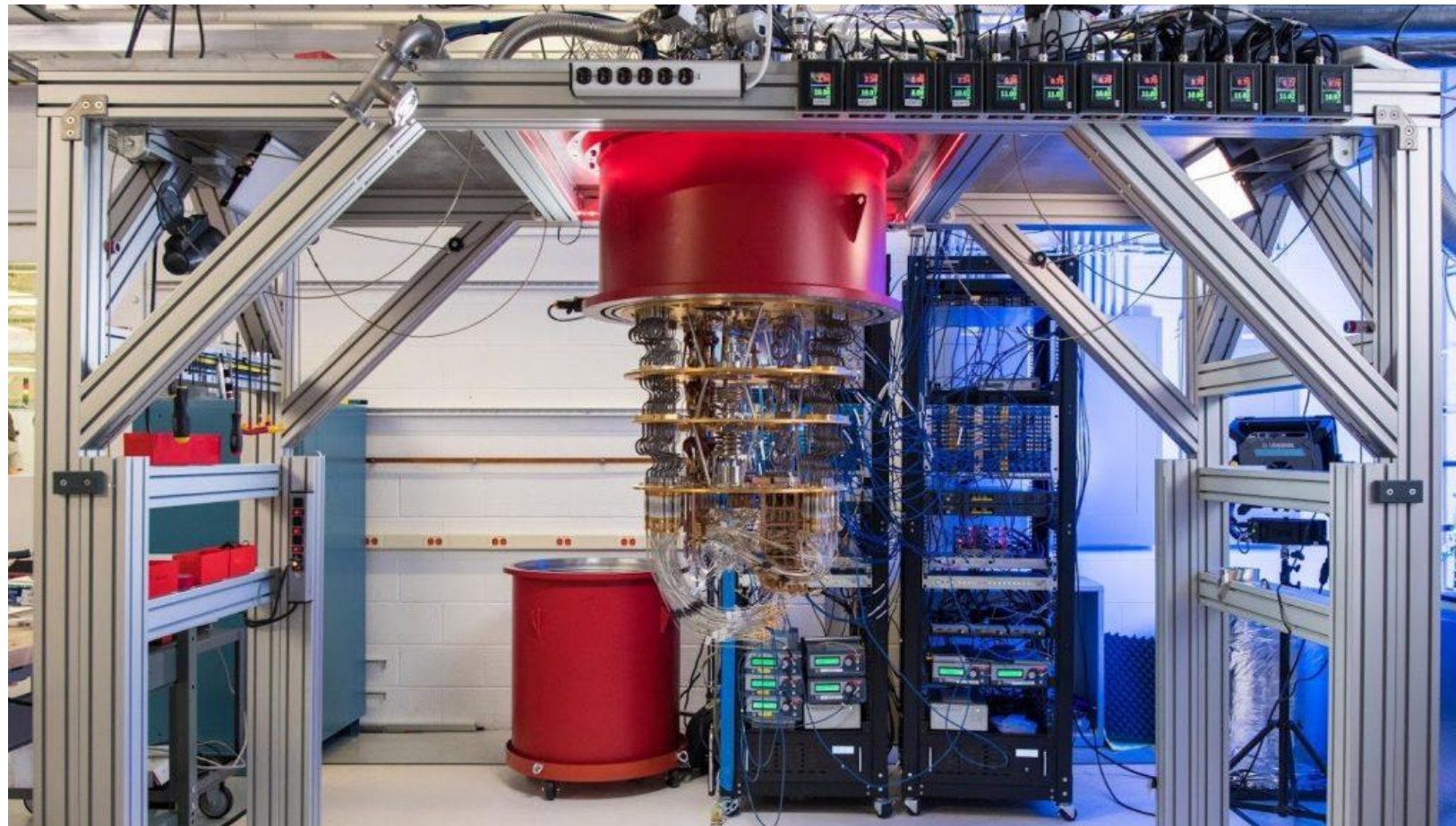
Conclusions

23 October 2019



Article

Quantum supremacy using a programmable superconducting processor



<https://www.nature.com/articles/s41586-019-1666-5>

23 oktober 2019



Article

Quantum supremacy using a programmable superconducting processor



Quantum supremacy / Primacy

Quantum computers can solve a problem that is **practically impossible** for classical computers.

One, practically useless problem, is enough!

John Preskill, Theoretical physicist, 2012

Nevertheless, building a quantum computer with 53 qubits is a very strong achievement

The problem

- Randomly choose numbers according to specific distribution
- Tailored to quantum computers
- Not really useful

The claim

“ ” T

The response

- IBM

“ O O T T T T RT ”

- Koen Bertels

Head Quantum Computer Architectures Lab, TU Delft

“ ”

27 oktober 2021

PHYS.ORG

Two Chinese teams claim to have reached primacy with quantum computers

by Bob Yirka, Phys.org



The Pan team's optical quantum computer uses a 144-mode interferometer to solve a Gaussian boson sampling problem.

Two teams in China are claiming that they have reached primacy with their individual quantum computers. Both have published the details of their work in the journal *Physical Review Letters*.

The problem

- Simulation for calculating probabilities output circuit with photons (quantum effects)
- Tailored to quantum computers
- Not really useful

The claim

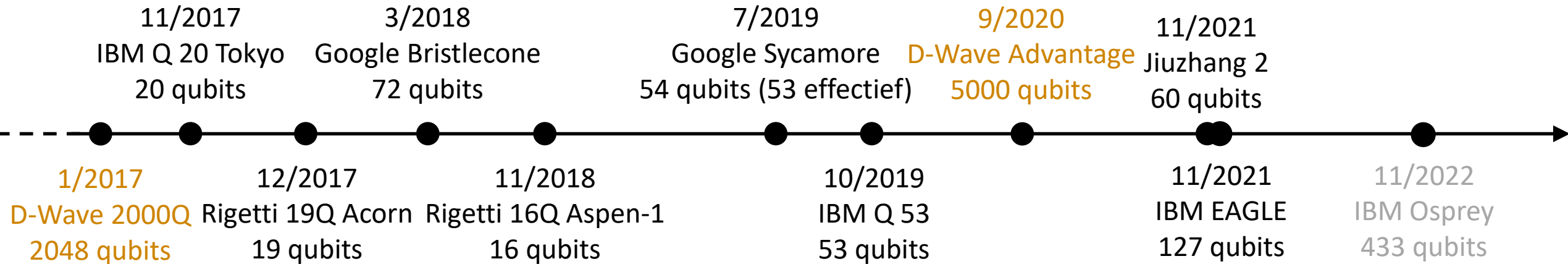
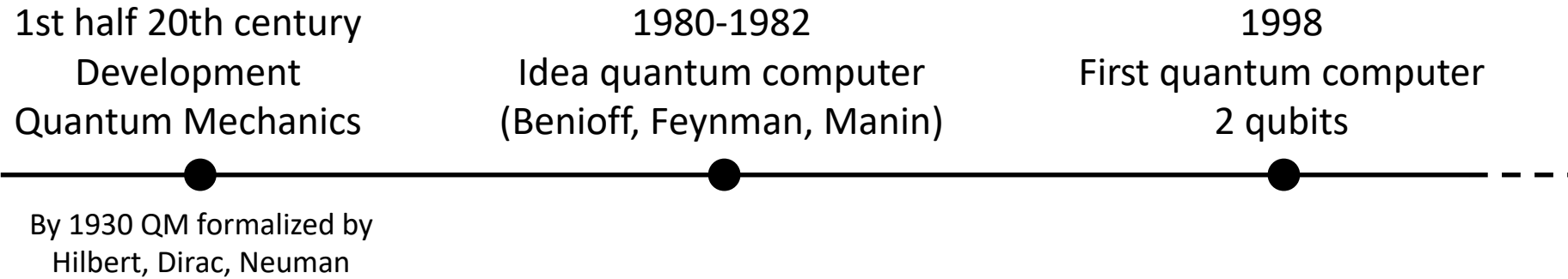
“ T ”

The response

- Not contested
- This time, quantum supremacy / primacy reached

**Another very strong performance!
(I.e. calculations with 56 qubits)**

Timeline quantum computers







Properties

- ❖ Requires less entanglement
- ❖ But more qubits
- ❖ Quantum annealing: combinatorial optimization problems (i.e. search space is discrete, s.a. traveling salesmen problem)
- ❖ Machines being sold (\$10M-\$15M)
- ❖ No quantum advantage yet

Quantum advantage

Quantum computers can solve a problem **FASTER** than classical computers.
One, practically useless problem, is enough!


Development Roadmap

Executed by IBM 
On target 

IBM Quantum

2019 

Run quantum circuits on the IBM cloud

2020 

Demonstrate and prototype quantum algorithms and applications

2021 

Run quantum programs 100x faster with Qiskit Runtime

2022

Bring dynamic circuits to Qiskit Runtime to unlock more computations

2023

Enhancing applications with elastic computing and parallelization of Qiskit Runtime

2024

Improve accuracy of Qiskit Runtime with scalable error mitigation

2025

Scale quantum applications with circuit knitting toolbox controlling Qiskit Runtime

Beyond 2026

Increase accuracy and speed of quantum workflows with integration of error correction into Qiskit Runtime

Model Developers

Prototype quantum software applications

Quantum software applications

Machine learning | Natural science | Optimization

Algorithm Developers

Quantum algorithm and application modules 

Machine learning | Natural science | Optimization

Quantum Serverless

Intelligent orchestration

Circuit Knitting Toolbox

Circuit libraries

Kernel Developers

Circuits 

Qiskit Runtime 


Dynamic circuits 


Threaded primitives

Error suppression and mitigation

Error correction

Hummingbird qubits 

Eagle 127 qubits 

Osprey 433 qubits 


Condor 1,121 qubits

Flamingo 1,386+ qubits

Kookaburra 4,158+ qubits

Scaling to 10K-100K qubits with classical and quantum communication

System Modularity

Falcon 27 qubits 

Hu 65

Heron 133 qubits x p

Crossbill 408 qubits

More qubits ≠ more computation power

Type quantum computer

- Universal (Rigetti, Google, IBM)
- Adiabatic (D-Wave)

Noise / Accuracy

...

→ IBM prefers the term

→ Not easy to compare. Companies are not always transparent about inner workings & specs



Why is building a quantum computer so complex?

Isolation

Error correction

Scalability

Challenge 1: Isolation



Interference

- ❖ Quantum state extremely sensitive for external interference
- ❖ Temperatures close to absolute zero ($-273,15^{\circ}\text{C}$)
- ❖ Shielded from vibrations, light & magnetic radiation

Coherence time

- ❖ Challenge: keeping quantum state sufficiently long coherent
- ❖ Googles Sycamore: tenths or hundredths of a microsecond

Manipulation

- ❖ Quantum logic gates sensitive to errors
- ❖ Reading (Measuring qubits)

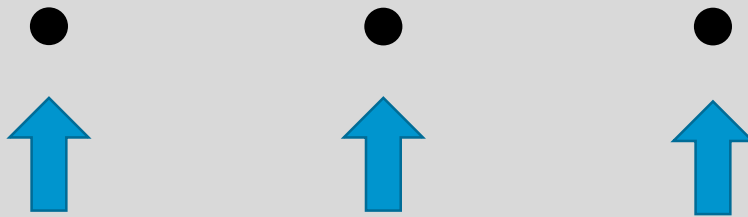
Evolution

- ❖ Significant progress in recent years
- ❖ Errors most likely unavoidable

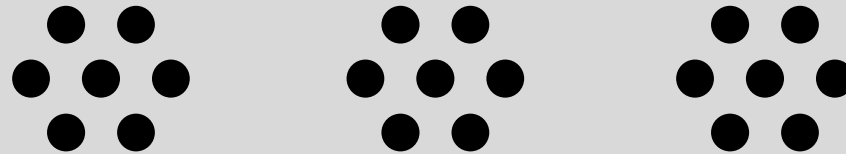
Errors may be unavoidable → error correction necessary

Multiple physical qubits together form 1 logical qubit

Logical qubits
(Exact)



Physical qubits
(‘Noisy’)



Evolution

- ❖ Years '80 and '90: “*impossible!*”
- ❖ First experiments

Requirements

- ❖ Sufficiently long coherence time
- ❖ Estimates: 1000 to 100 000 physical qubits for a logical qubit
 - Noise physical qubits
 - Length of the circuit



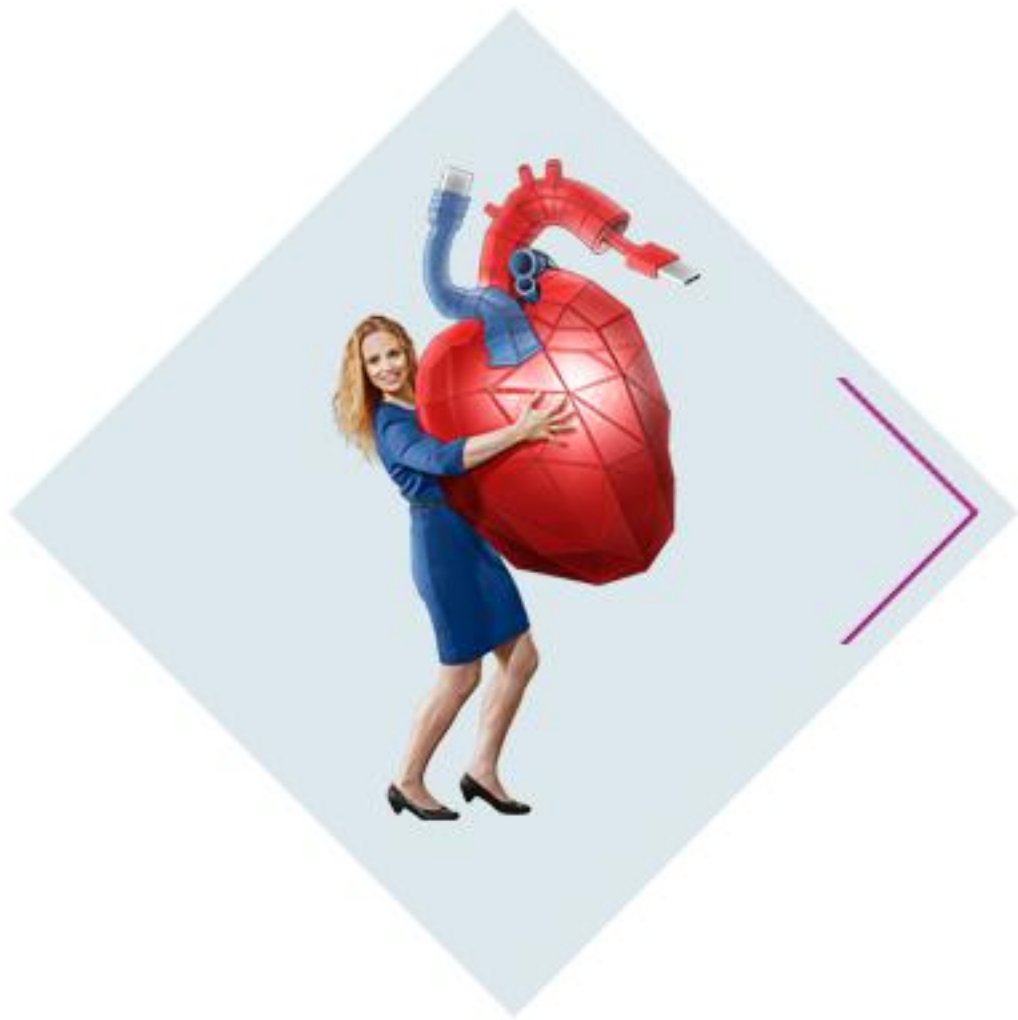
Why is building a quantum computer so complex?

Isolation

Error correction

Scalability

Challenges are astronomical



Agenda

Quantum computer Vs. classical computer

Quantum computers in practice

Crypto-apocalypse now?

Quantum-resistant cryptography

Conclusions



- ▶ Since the advent of classical computers (1970s)
- ▶ Public algorithms, secret keys
- ▶ Security based on assumptions
(from which security of algorithm is proven)
- ▶ Much more than confidential communications

CRYPTO WORKHORSES

Encryption

DES, AES, ElGamal, RSA, ...

Digital signatures

RSA, DSA, Schnorr, ...

Authentication

SSH, CHAP, ...

Hashing

MD5, RipeMD, SHA-1, SHA-2, SHA-3

Key exchange

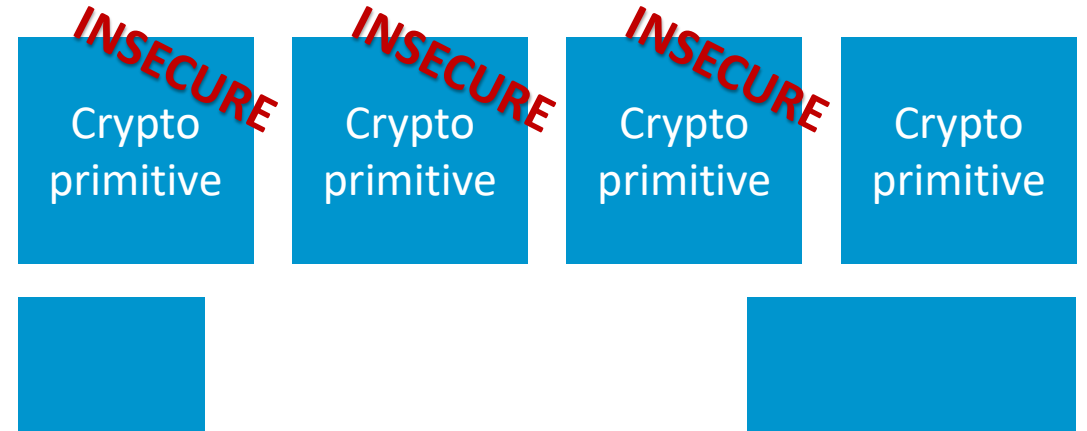
Diffie–Hellman, ...

Message authentication code

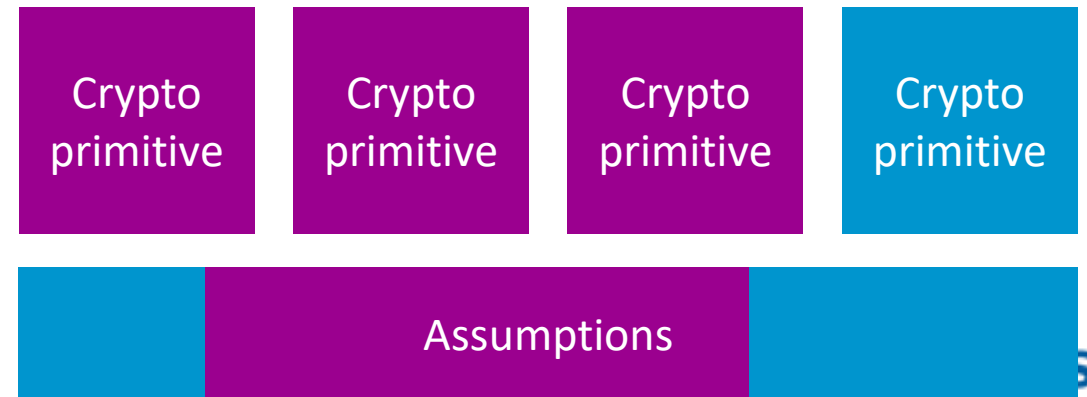
HMAC, ...



MODERN CRYPTOGRAPHY



QUANTUM RESISTANT CRYPTOGRAPHY

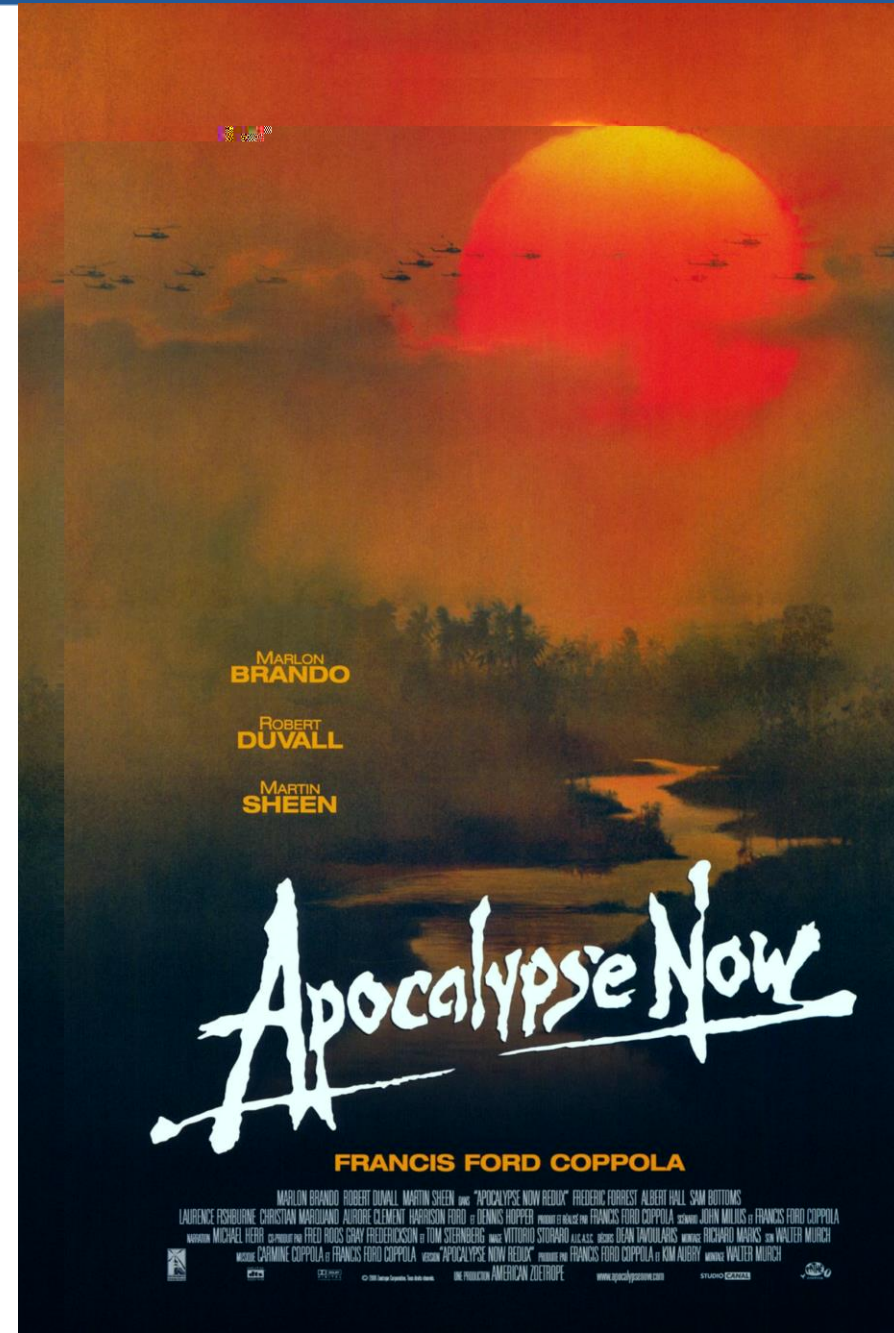


Impact quantum computers on modern cryptography?

Symmetric
cryptography

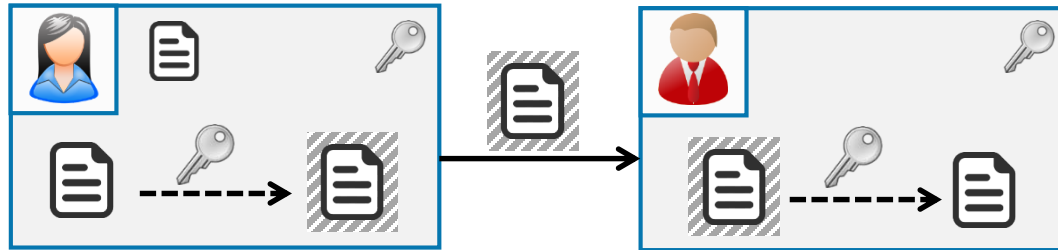
Cryptographic
hash function

Public-key
cryptography



Symmetric cipher

- ▶ Encryption and decryption with same secret key
- ▶ AES (KU Leuven)



Breaking = finding secret key

Toy classical computer

- ▶ Key length = ~~6 bits~~ **128 bits**
- ▶ $8^2 = 2^6 = 64$ potential keys (= search space)
- ▶ Security = 6 bit
- ▶ Best attack is ± exhaustively testing each possible key
- ▶ On average, key found after 32 attempts

Toy quantum computer

- ▶ Promises quadratic speedup
Size search space decreases from 64 to $\sqrt{64} = 8$
- ▶ Security decreased to 3 bit (because $8 = 2^3$)
- ▶ On average, key found after 4 attempts

Toy measure 128 → 256 bits

- ▶ Double key length: ~~6~~ **→ 12 bits**
- ▶ Size of search space classical computer: $2^{12} = 64^2 = 4096$
- ▶ Size search space quantum computer: $\sqrt{4096} = 64$

Search space

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

Grover's Algorithm on a quantum computer

Number of LOGICAL qubits required

- ▶ AES-128: 2953
- ▶ AES-192: 4449
- ▶ AES-256: 6681
- ▶ Entangled

Personal thought

First, a “quantum oracle” must be built. This step MAY negate the performance gain of Grover's algorithm

Zoekruimte

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63



Bundesamt
für Sicherheit in der
Informationstechnik

“At the present time, there is no evidence that symmetric cryptographic mechanisms are threatened in any significant way by quantum computers.

Generally, an adversary which has access to k universal quantum computers can perform a key recovery attack against a block cipher with a key length of n bits by executing the Grover algorithm in parallel on all available quantum computers within $\approx \pi 2^{\frac{n-4}{2}} / \sqrt{k} / k$ time units, where one unit of time corresponds to the time needed to execute the block cipher on a single quantum computer”

**TR-02102-1: Cryptographic Mechanisms:
Recommendations and Key Lengths
January 2023**

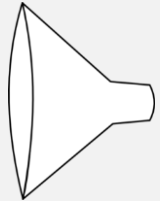


Powerful quantum computers pose no threat to symmetric cryptography

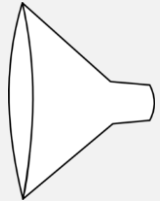
(As a precaution, take sufficiently long keys)

Cryptographic hash function

- ▶ Integrity
- ▶ Very commonly used (e.g. electronic signatures, files, blockchain)
- ▶ Examples: SHA1, SHA2, SHA3

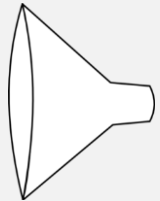


5e 50 6e 82 7f d5 50 ec 4e 08 8e e7 75 8f 34 b3
a6 8e 34 93 d5 89 98 52 97 48 f0 c6 c1 70 f3 3c



5f 3b fa 41 9c 63 be 2a 3a 09 ad bd 06 30 c5 1f
64 5e b0 3a ba fc d5 f2 ad 39 63 7a 30 6b 41 77

“Hello world!”



c0 53 5e 4b e2 b7 9f fd 93 29 13 05 43 6b f8 89
31 4e 4a 3f ae c0 5e cf fc bb 7d f3 1a d9 e5 1a

Fixed-length output

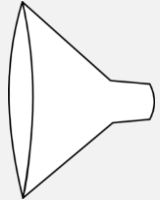
Collision resistance

Pre-image resistance

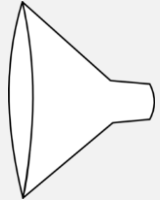
Second pre-image resistance

Cryptographic hash function

- ▶ Integrity
- ▶ Very commonly used (e.g. electronic signatures, files, blockchain)
- ▶ Examples: SHA1, SHA2, SHA3

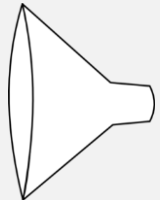


5e 50 6e 82 7f d5 50 ec 4e 08 8e e7 75 8f 34 b3
a6 8e 34 93 d5 89 98 52 97 48 f0 c6 c1 70 f3 3c



5f 3b fa 41 9c 63 be 2a 3a 09 ad bd 06 30 c5 1f
64 5e b0 3a ba fc d5 f2 ad 39 63 7a 30 6b 41 77

“Hello world!”



c3 5e 79 4b cf 52 34 c4 5a fc 19 c0 04 79 3d e7
d3 d2 4b 20 12 d0 3b f6 13 8b 23 c9 97 41 8a 50

Fixed-length output

Collision resistance

Pre-image resistance

Second pre-image resistance

Collision attack

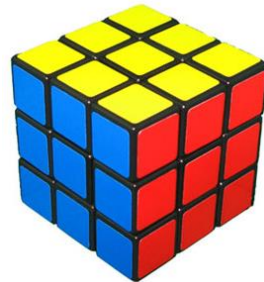
- ▶ Finding two inputs that result in the same output
- ▶ Successful attack against SHA1 in 2017

Classical computer

- ▶ 256 bits outputs results in 128 bits security
P[collision] \approx 50% after $\sqrt{2^{256}} = 2^{128}$ attempts
- ▶ Cfr. Birthday paradox

Quantum computer

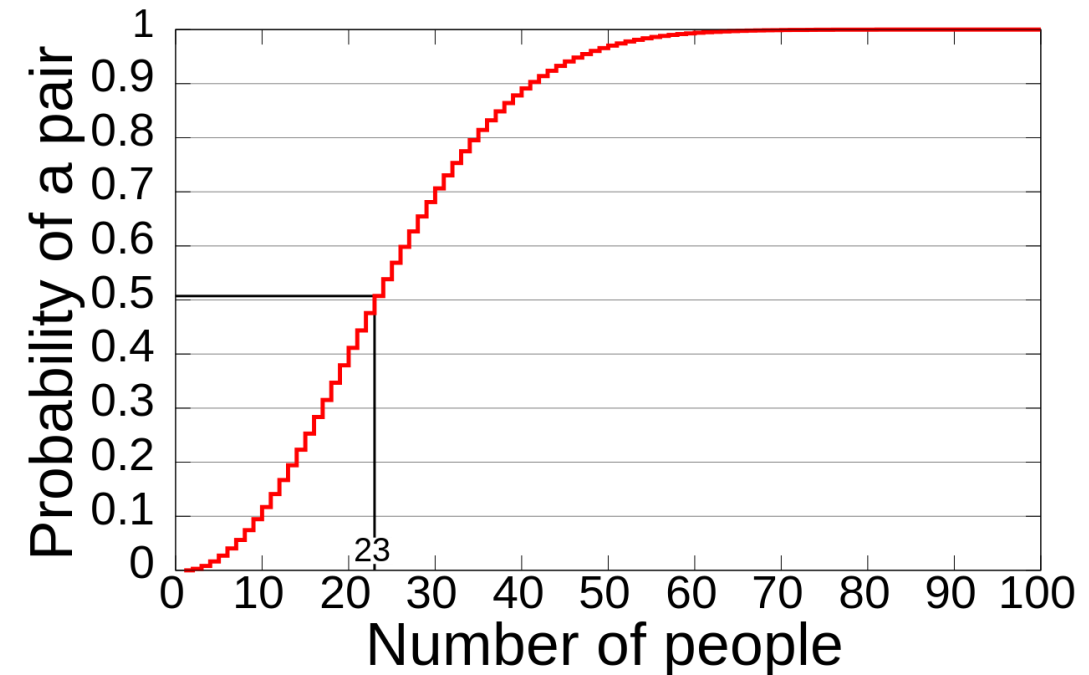
- ▶ Grover's algorithm
- ▶ Security decreases
from $\sqrt{2^{256}} = 2^{128}$
to $\sqrt[3]{2^{256}} = 2^{85} \approx 10^{26}$ (insecure)



Measure

- ▶ Output length x 1,5: 256 \rightarrow 384 bits ($\sqrt[3]{2^{384}} = 2^{128}$)
- ▶ Manageable!

Birthday paradox



By Rajkiran, CC BY-SA 3.0,
<https://commons.wikimedia.org/w/index.php?curid=10784025>

<https://arxiv.org/pdf/1804.00200.pdf>

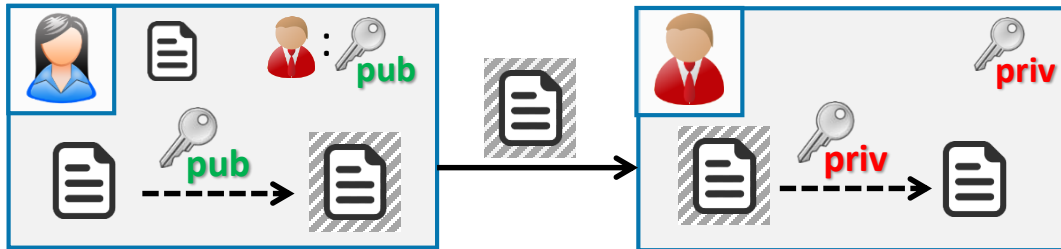


Powerful quantum computers pose no threat to cryptographic hash functions

(Make sure the output is long enough)

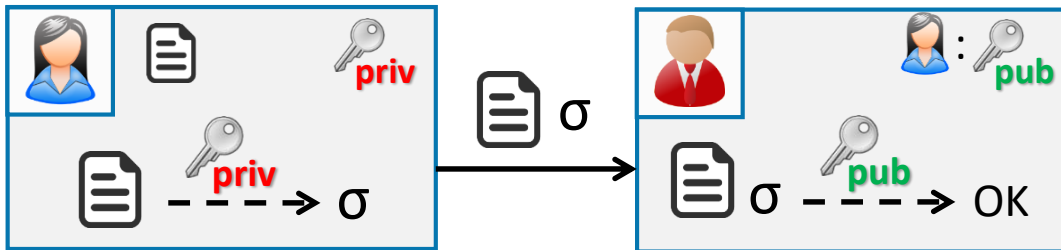
Public-key encryption

- ▶ Confidentiality
- ▶ Encryption with public key, decryption with private key



Digital signatures

- ▶ Integrity, data authenticity
- ▶ Vb. Belgian eID card



Look authentication & establishing secure channels (TLS)

Most common systems based on
RSA or elliptic curves



Prime number

Natural number only divisible by 1 and itself

E.g. 2, 3, 5, 7, 11, 13, 17, 19, 23, ...

Factoring a number in prime factors

Unique for each number

Example: $12 = 2^2 * 3$

RSA assumption

There is no efficient algorithm for factoring a number that is the product of two large prime numbers. In practice infeasible when sufficiently large primes are chosen.

**Powerful quantum computer
could do this efficiently
with the help of Shor's algorithm**

Example

RSA-250 (829 bits) published in 1991

```
214032465024074496126442307283933356300861
471514475501779775492088141802344714013664
334551909580467961099285187247091458768739
626192155736304745477052080511905649310668
769159001975940569345745223058932597669747
1681738069364894699871578494975937497937
```

=

```
641352894770715802787901901705773890848250
147429434472081168596320245323446302386235
98752668347708737661925585694639798853367
```

×

```
333720275949781565562260106053551142279407
603447675546667845209870238417292100370802
57448673296881877565718986258036932062711
```

**Was factored by classical computers
in February 2020**

Biggest RSA number factored by classical computer

RSA-250 (829 bits)

214032465024074496126442307283933356
300861471514475501779775492088141802
344714013664334551909580467961099285
187247091458768739626192155736304745
477052080511905649310668769159001975
940569345745223058932597669747168173
8069364894699871578494975937497937

(in 2020, 2700 core-years)

Biggest RSA number factored With Shor's algorithm by quantum computer...

21

(in 2012)

RSA-2048 (2048 bits)

251959084756578934940271832400483985
714292821262040320277771378360436620
207075955562640185258807844069182906
412495150821892985591491761845028084
891200728449926873928072877767359714
183472702618963750149718246911650776
133798590957000973304597488084284017
974291006424586918171951187461215151
726546322822168699875491824224336372
590851418654620435767984233871847744
479207399342365848238242811981638150
106748104516603773060562016196762561
338441436038339044149526344321901146
575444541784240209246165157233507787
077498171257724679629263863563732899
121548314381678998850404453640235273
819513786365643912120103971228221207
20357

Disclaimer

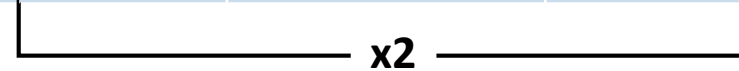
- Quantum computers already factored larger, very specifically chosen numbers without Shor's algorithm.

Shor's Algorithm (1994)

- Quantum algorithm to find the prime factors of an integer (RSA)
- Also applicable on cryptography based on elliptic curves (EC)

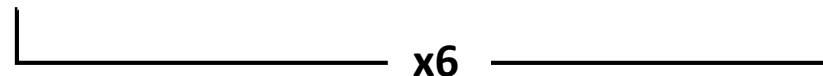
RSA

Algorithme	# bits security	# logical qubits	# physical qubits
	80	± 2048	
	112	± 4096	20 million (8 hours, 2019)
	128	± 6144	
	192	± 15360	
	256	± 30720	



Elliptic curves

Algorithme	# bits security	# logical qubits	# physical qubits
	128	± 1536	13 million (24 hours, 2022)
	192	± 2304	
	256	± 3126	

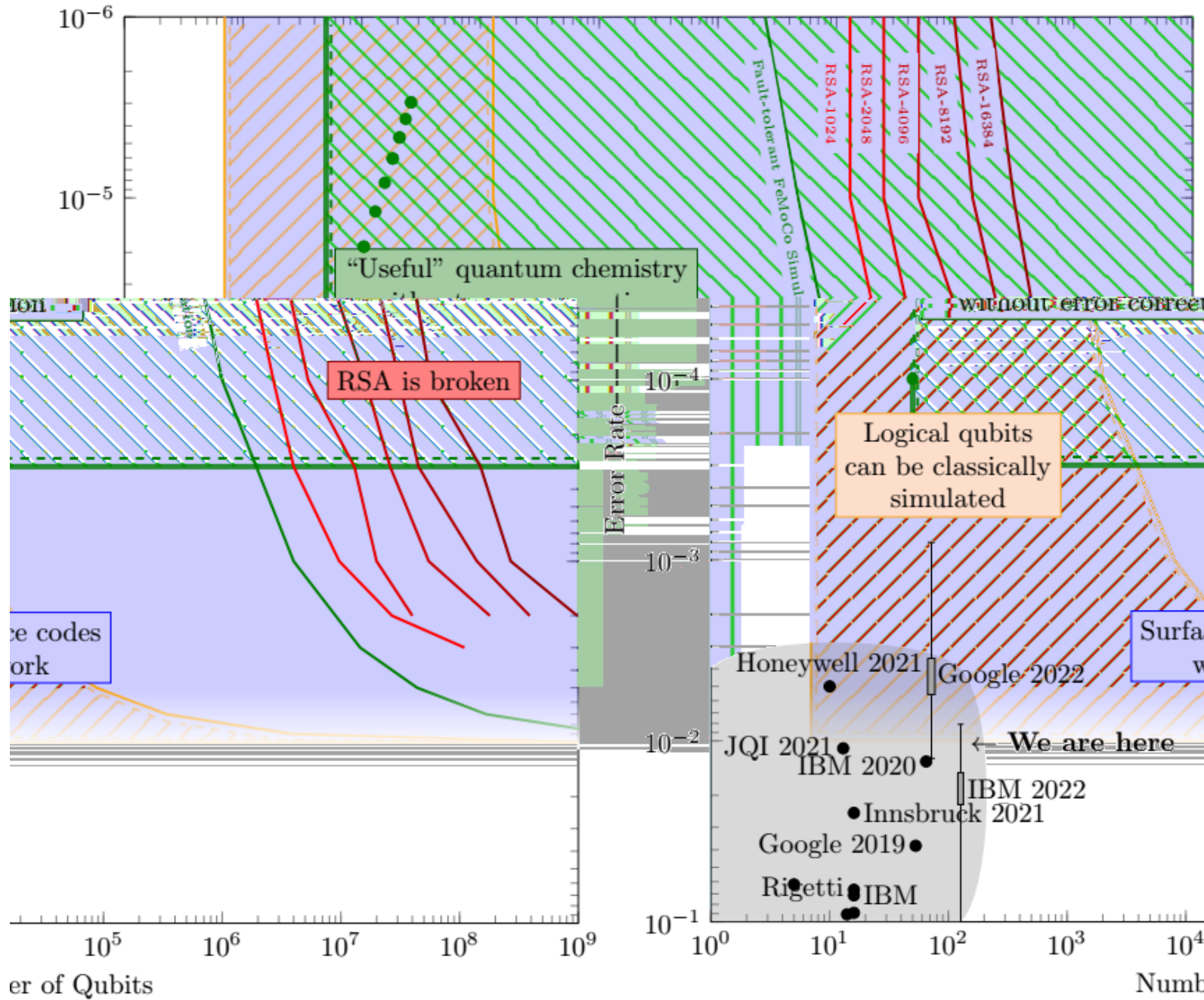




Powerful quantum computers with tens of millions of physical qubits threaten public key cryptography

(But we're not there yet)

Overview



Surface codes = error correction

“Longer algorithm’s like Shor’s algorithm (to break RSA) likely require more than 1000 physical qubits per logical qubit.”

“We need Moore’s-law type scaling for quantum computers to ever be useful”

By Samuel Jaques,
University of Oxford, 2022

https://sam-jaques.appspot.com/quantum_landscape_2022

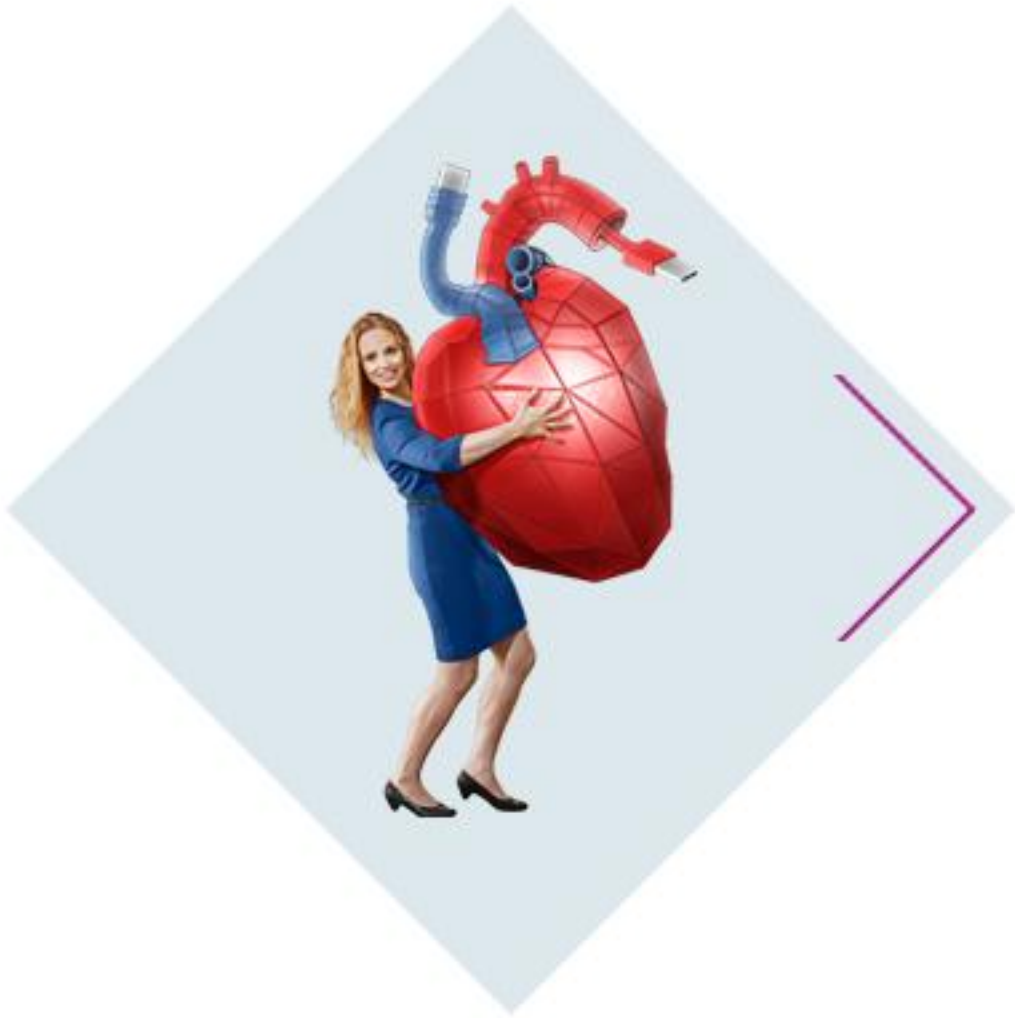
Impact of quantum computers on modern cryptography

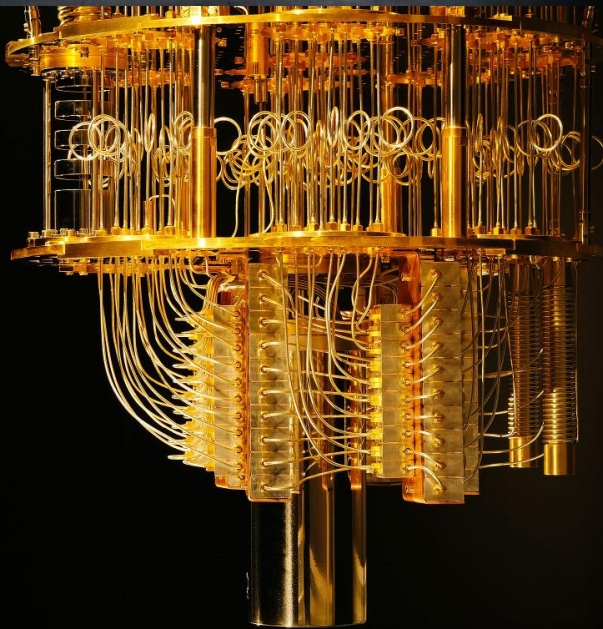
	Symmetric cryptography	Cryptographic hash function	Public-key cryptography
Quantum Threat	Grover's algorithm	Grover's algorithm	Shor's algorithm
Number of qubits	Several thousand logical = several million physical qubits		
What if?	Key length x 2	Output length x 1,5	Quantum resistant alternatives
Impact efficiency	Requires 25% more time(*)	Nihil (*)	Mixed (see later)

(*) Indicative. Result testing performed on Thinkpad laptop with core i5 processor

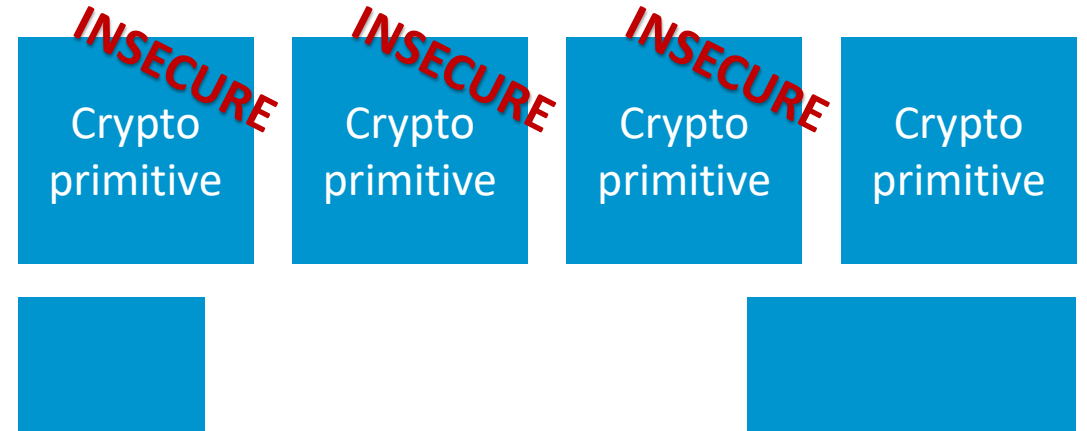
Agenda

Quantum computer Vs. classical computer

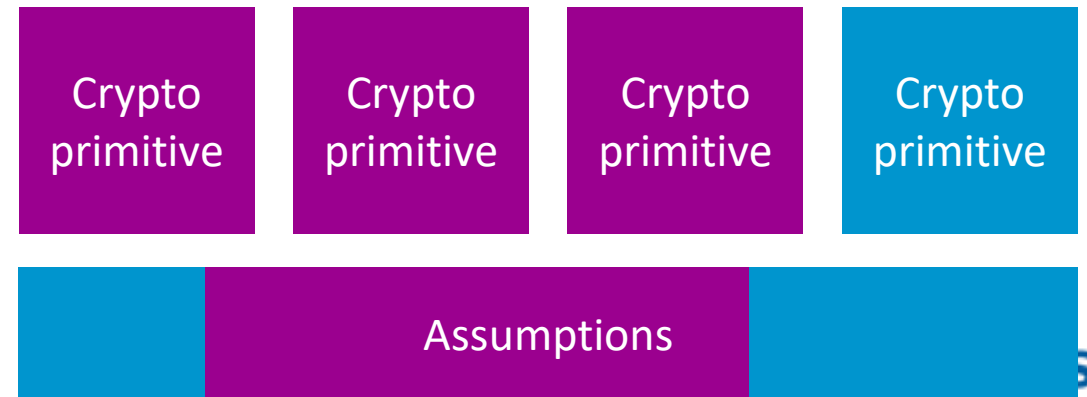




MODERN CRYPTOGRAPHY



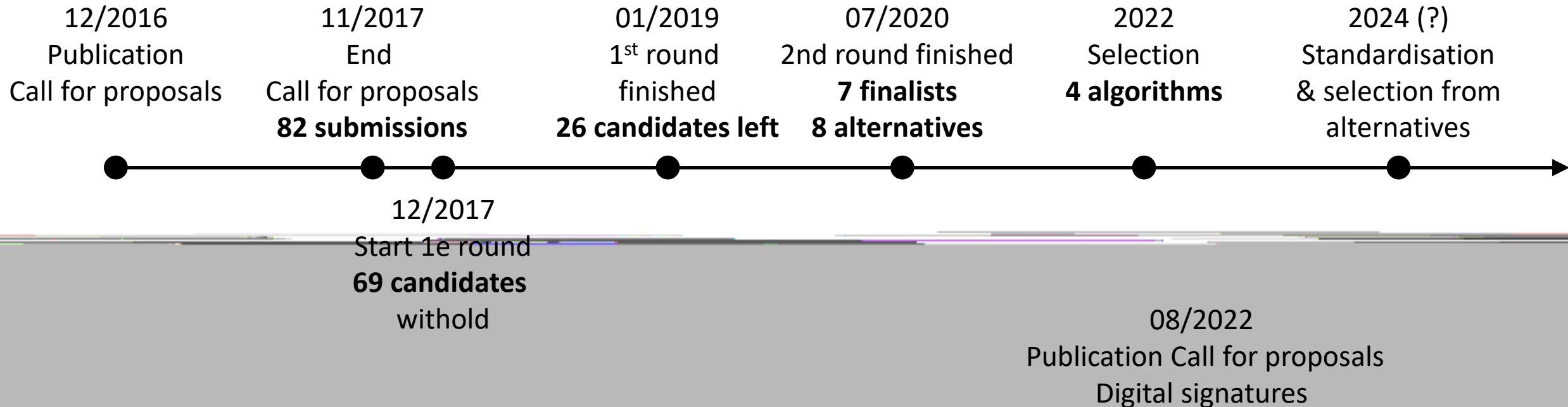
QUANTUM RESISTANT CRYPTOGRAPHY



Quantum resistant cryptography – NIST standardisation procedure

Two parts

- Public-key Encryption and Key-establishment Algorithms
- Digital Signature Algorithms



Algorithms are ASSUMED to be secure against both Classical and quantum computers

KU Leuven submission (SABER and LUOV) didn't make it



Chosen algorithm: Kyber

- Kyber-512 \approx 128 bit security
- Kyber-768 \approx 192 bit security
- Kyber-1024 \approx 256 bit security



	Quantum Resistant	Size public key (in bytes)	Data transmission (in bytes)	Client-side computation (higher is better)	Server-side computation (higher is better)
	Nee	256	512	29 ops / sec	150 000 ops / sec
<i>o</i>	Nee	32	64	15 000 ops / sec	15 000 ops / sec
	Ja	800	1568	57 000 ops / sec	80 000 ops / sec

Alternative candidates

- BIKE, Classic McEliece and HQC
- Goal: select at least a 2nd KEM standard by 2028
- Alternative in case weaknesses against Kyber found
- Fourth alternative candidate, SIKE, has been broken (summer 2022)

<https://pq-crystals.org/kyber/>

<https://blog.cloudflare.com/nist-post-quantum-surprise/>

<https://www.wired.com/story/new-attack-sike-post-quantum-computing-encryption-algorithm/>



DATA PROTECTION

AI Helps Crack NIST-Recommended Post-Quantum Encryption Algorithm

The CRYSTALS-Kyber public-key encryption and key encapsulation mechanism recommended by NIST for post-quantum cryptography has been broken using AI combined with side channel attacks.



By **Kevin Townsend**
February 21, 2023



Correction

Not the algorithm was cracked, but an implementation of it

	Quantum Resistant	Size public key (in bytes)	Size signature (in bytes)	CPU time Signing (lower is better)	CPU time Verification (lower is better)
	Nee	32	64	1 (baseline)	1 (baseline)
	Nee	256	256	70	0,3
	Ja	1 312	2 420	4,8	0,5
	Ja	897	666	8	0,5
	Ja	32	7 856	8 000	2,8
	Ja	32	17 088	550	7

[1] Falcon Has a high implementation complexity => Higher risk of vulnerabilities
In particular floating point operations in constant time

Lack of an efficient and generically usable quantum-resistant signature scheme prompted NIST to initiate a new standardization procedure.

Also: Stateful hash-based signatures (XMSS, LMS)

2021

- ❖ “Cryptographically Relevant Quantum Computer” (CRQC)
- ❖ **NSA does not know when or even if a [CRQC] will exist**
- ❖ The cryptographic systems that NSA produces, certifies, and supports often have very long lifecycles. NSA has to produce requirements today for systems that will be used for many decades in the future
- ❖ **New cryptography can take 20 years or more to be fully deployed to all National Security Systems**

2022

- ❖ Given foreign pursuits in quantum computing, **now is the time to plan, prepare and budget for a transition** to QR algorithms to assure sustained protection of [classified and critical information] in the event a CRQC becomes an achievable reality.
- ❖ We want people to take note of these requirements to plan and budget for the expected transition, but **we don’t want to get ahead of the standards process**



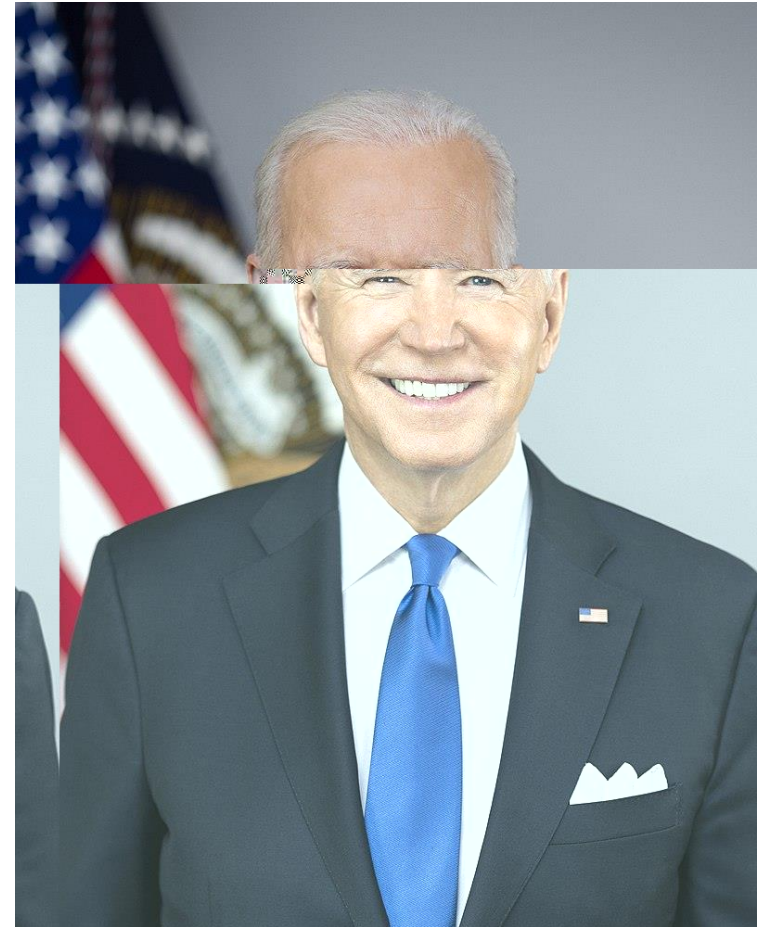
“Unfortunately, the growth of elliptic curve use has bumped up against the fact of continued progress in the research on quantum computing, which has made it clear that elliptic curve cryptography is not the long term solution many once hoped it would be.”

IAD, defensive tak NSA, 2015

Law signed by Biden on 21 December 2022

Quantum Computing Cybersecurity Preparedness Act

- Cryptography essential for national security and the functioning of the economy
- Potential risks posed by “**harvest now, decrypt later**” attacks
- Prioritize the post-quantum cryptography migration within a year after the NIST issues post-quantum cryptography standards
- Within six months, federal agencies must develop a strategy for migrating to post-quantum cryptography



Migration

- ❖ NIST standardisation procedure ongoing
- ❖ Then consider migration (or wait a bit?)
- ❖ Urgency depends on risk assessment

Prepare with crypto agility

- ❖ Overview: Which cryptography and keys where and why?
- ❖ Build systems sufficiently flexible to minimize friction when replacing crypto keys & algorithms
- ❖ Foresee migration procedures

Agenda

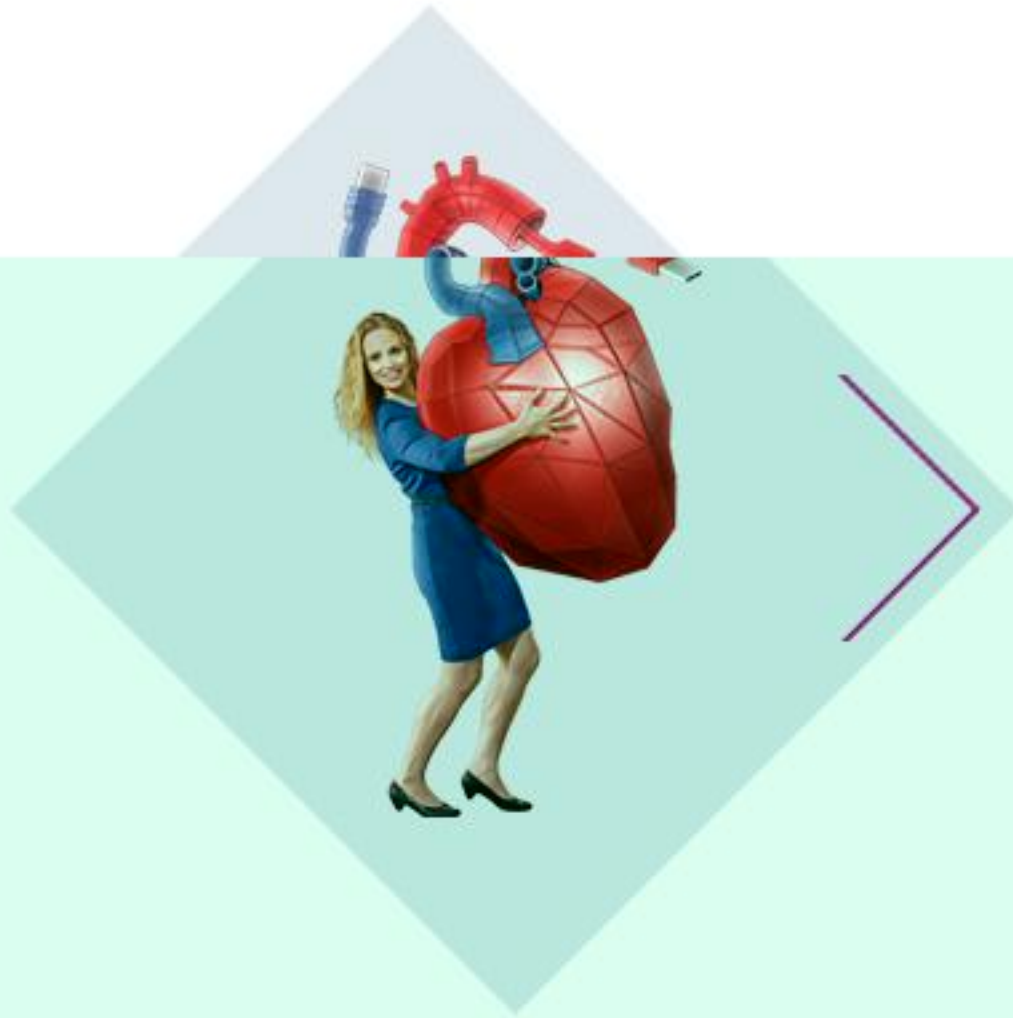
Quantum computer Vs. classical computer

Quantum computers in practice

Crypto-apocalypse now?

Quantum-resistant cryptography

Conclusions



Conclusion

Quantum computers are based on principles from quantum physics (entanglement & superposition)

Building quantum computers extremely complex
(Isolation, error correction, scalability)

Longer symmetric keys and hash output
Several million physical qubits required to crack public key cryptography → Alternatives needed

The NIST standardization process is ongoing

Agenda

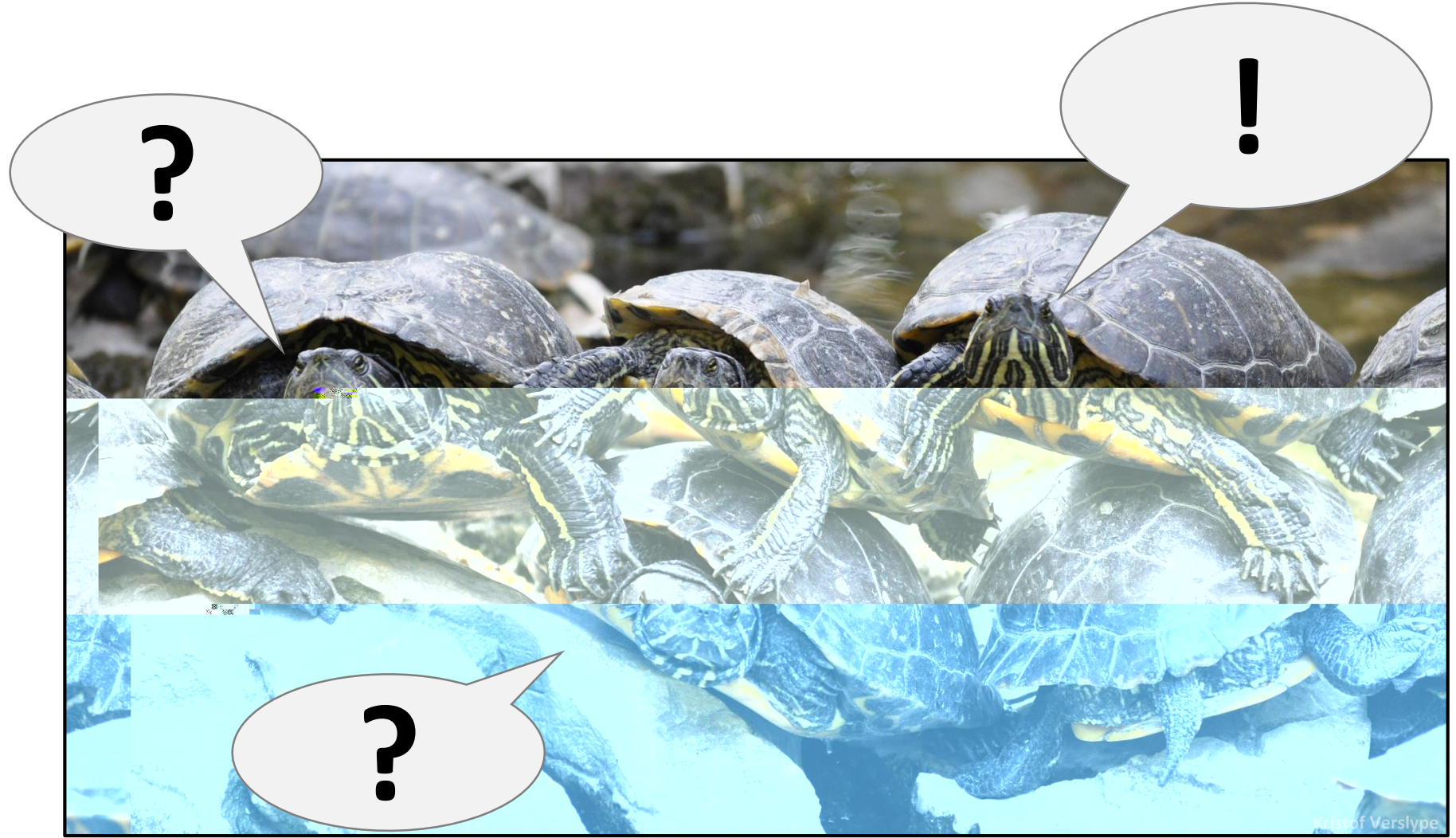
Quantum computer Vs. classical computer

Quantum computers in practice

Crypto-apocalypse now?

Quantum-resistant cryptography

Kristof Verslype
Cryptographer, PhD
Smals Research



✉ kristof.verslype@smals.be

☎ +32(0)2 7875376

🌐 www.smals.be
www.smalsresearch.be
www.cryptov.net

🐦 @KristofVerslype

in [linkedin.com/in/verslype](https://www.linkedin.com/in/verslype)

Referenties

- F. ARUTE, K. ARYA, [...] J. MARTINIS. R R R . Nature, 23 October 2019
<https://www.nature.com/articles/s41586-019-1666-5>
- R T V O O . NIST.
<https://csrc.nist.gov/projects/post-quantum-cryptography>
- R T . NSA.
<https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm>
- R T . NSA.
<https://www.nsa.gov/what-we-do/cybersecurity/post-quantum-cybersecurity-resources/>
- S. DAS SARMA. R T T T R O . 22 Maart 2022
<https://www.technologyreview.com/2022/03/28/1048355/quantum-computing-has-a-hype-problem/>
- M. GRASS, B. LANGENBERG, M. ROETTELER, R. STEINWANDT. R O R T . Post-Quantum Cryptography, Springer, Cham, 2016.
<https://arxiv.org/pdf/1512.04965.pdf>
- C. GIDNEY, M. EKERA. R T R . arXiv preprint arXiv:1905.09749, 2019.
<https://arxiv.org/abs/1905.09749>
- M. DYAKONOV. T R R . IEEE Spectrum 56.3, 15 November 2018.
<https://spectrum.ieee.org/computing/hardware/the-case-against-quantum-computing>
- H. HELSMOORTEL, W. DE MAESENEER. T O P
VRT Nieuws, 15 January 2020,
<https://www.vrt.be/vrtnws/nl/2019/12/24/vlaamse-topwetenschappers-blikken-vooruit-naar-2030-kwantumcomp/>
- D. MASLOV, J. GAMBETTA. On “Quantum Supremacy”. IBM Research Blog, 21 October 2019.
<https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/>
- V. MAVROEIDIS, K. VISHI, M. Zych, A Jøsang. T R R T . arXiv preprint arXiv:1804.00200, 2018 Mar 31.
<https://arxiv.org/pdf/1804.00200.pdf>
- J. Preskill. *Quantum computing in the NISQ era and beyond*. Quantum. 2018 Aug 6;2:79.
<https://arxiv.org/abs/1801.00862>

- IBM. Q System One quantum.
<https://www.ibm.com/quantum-computing/systems/>
- Andrew Magill. JTAG board 1
<https://flickr.com/photos/amagill/2877921712/>
- Max Roser – Transistor count.
<https://ourworldindata.org/uploads/2019/05/Transistor-Count-over-time-to-2018.png>
- Alex Does Physics. Polarization
<http://alexdoesphysics.blogspot.com/2018/11/mathematical-description-of-polarization.html>
- Orren Jack Turner. Einstein in 1947
https://en.wikipedia.org/wiki/Albert_Einstein#/media/File:Albert_Einstein_Head.jpg
- INTVGene. Puzzle.
<https://www.flickr.com/photos/intvgene/370973576/>
- Nature. Layout Sycamore processor.
<https://www.nature.com/articles/s41586-019-1666-5>
- D-Wave Systems. D-Wave 2000Q Quantum Computer.
<https://www.dwavesys.com/press-releases/d-wave%20announces%20d-wave-2000q-quantum-computer-and-first-system-order>
- Quantum computing
<https://www.roche.com/quantum-computing.htm>
- Pixabay. Jug Thermos Hot Cold Drink Coffee
<https://pixabay.com/photos/jug-thermos-hot-cold-drink-coffee-3638398>
- Marcus Gripe, Garv... (writing)
<https://flickr.com/photos/neoeinstein/4503776883>
- Willian Clifford. This is as close as you get. (fingerprint)
<https://www.flickr.com/photos/williac/2503890509/>
- Birthday paradox
<https://commons.wikimedia.org/w/index.php?curid=10784025>
- Natascha. Keys.
<https://www.flickr.com/photos/tasj/5207744064>
- Kristof Verslype. Threatening clouds above Lake Titicaca, Peru.
<https://www.flickr.com/photos/verslype/23928588621>