Quantum computers
Vs.
Modern cryptography

Kristof Verslype
Smals Research

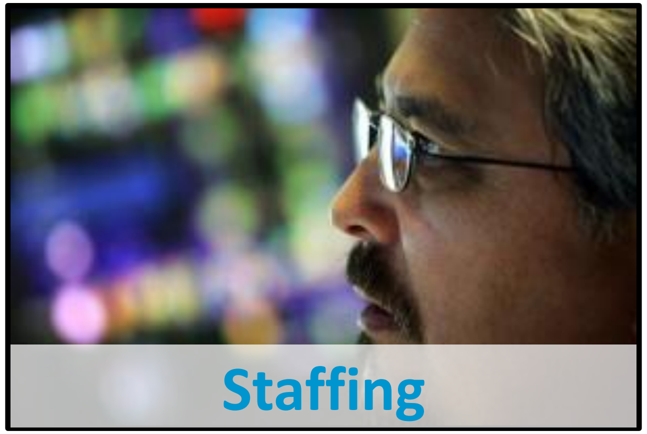
Smals
ICT for society

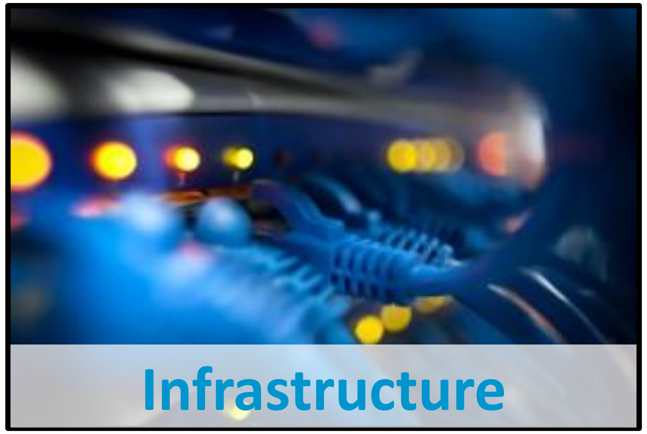
Smals
ICT for society

SUPPORT FOR E-GOVERNMENT


Knowhow


Development


Staffing


Infrastructure

g-cloud

top EMPLOYER
BELGIË
BELGIQUE
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

WWW.SMALS.BE

Many articles, but sometimes hard to interpret correctly

Google claims quantum supremacy

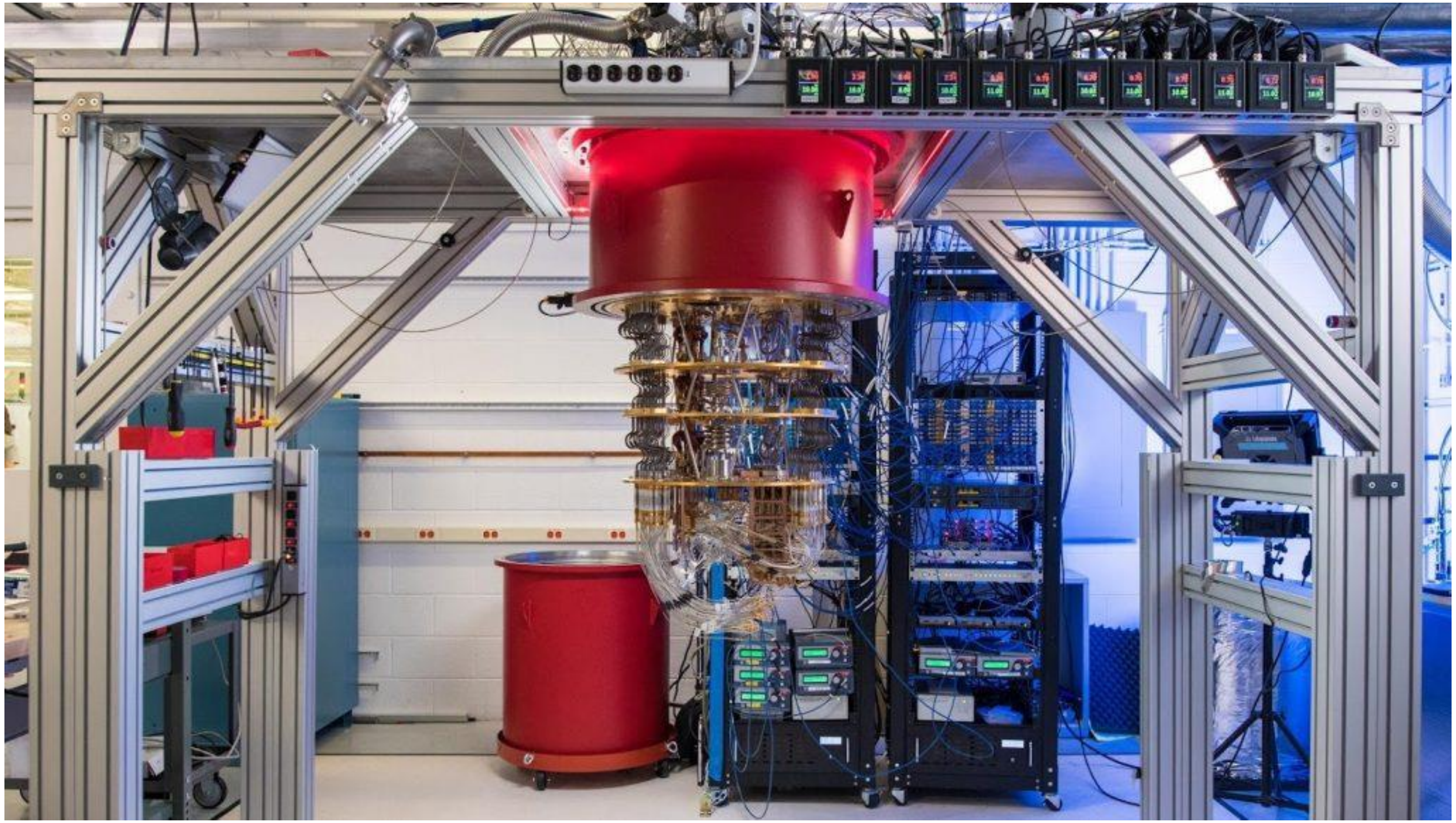
23 October 2019

Google

Article

Quantum supremacy using a programmable superconducting processor

nature
International journal of science



Smals
ICT for society

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

China claims quantum primacy

PHYS.ORG

27 October 2021

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 …

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*.

Smals
ICT for society

In the news

"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".*

WIRED | SIGN IN

DAN GOODIN, ARS TECHNICA | SECURITY | AUG 3, 2022 9:00 AM

A New Attack Easily Knocked Out a Potential Encryption Algorithm

SIKE was a contender for post-quantum-computing encryption. It took researchers an hour and a single PC to break it.

In the news

FINANCIAL TIMES

Quantum technologies + Add to myFT

Chinese researchers claim to find way to break encryption using quantum computers

Experts assess whether method outlined in scientific paper could be a sooner-than-expected turning point in the technology

Richard Waters JANUARY 5 2023

DATA PROTECTION

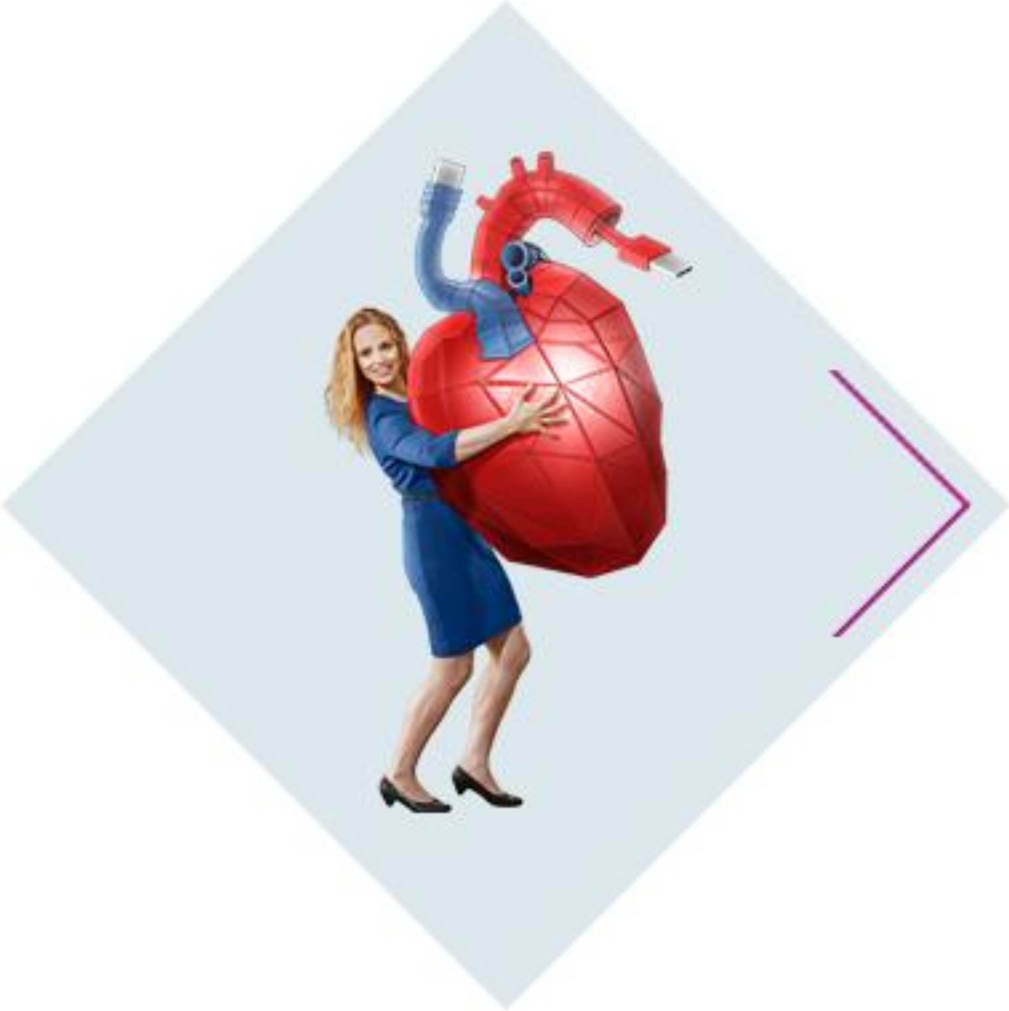
AI Helps Crack NIST-Recommended Post-Quantum Encryption Algorithm

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

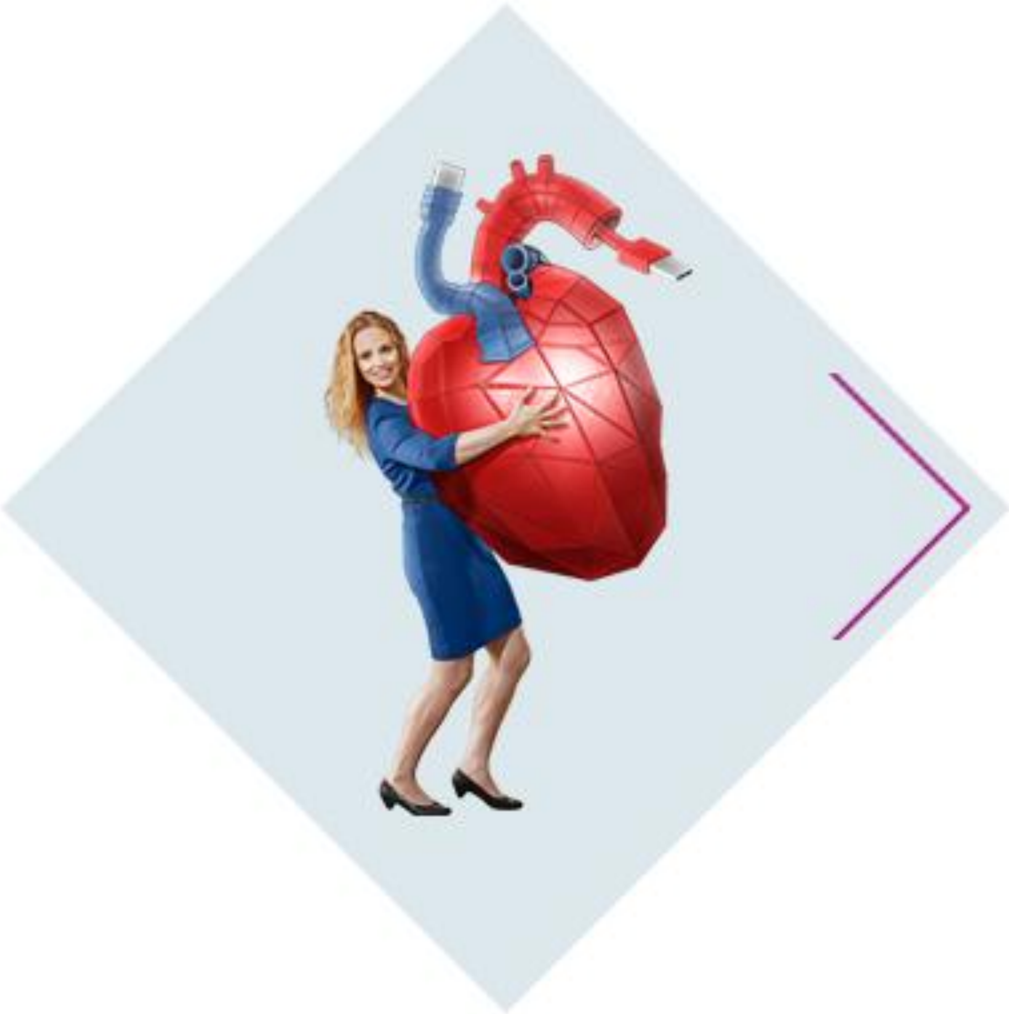
https://www.securityweek.com/ai-helps-crack-a-nist-recommended-post-quantum-encryption-algorithm/

Is the quantum army advancing at a rapid pace?



Agenda

- Quantum computers in theory
- Quantum computers in practice
- Crypto-apocalypse now?
- Quantum-resistant cryptography



Agenda

- **Quantum computers in theory**
- Quantum computers in practice
- Crypto-apocalypse now?
- Quantum-resistant cryptography

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

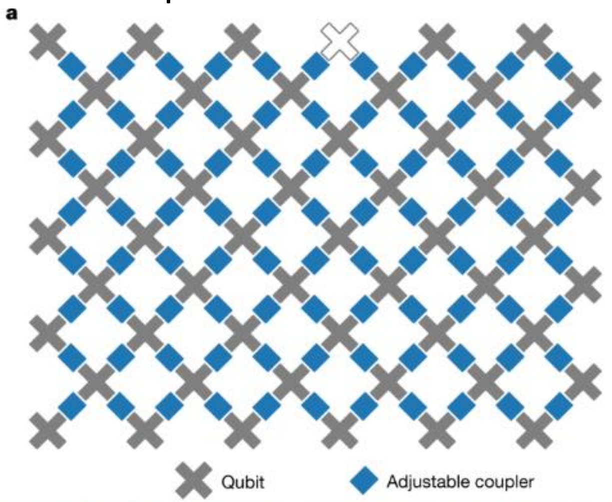
Quantum state

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

Quantum state

- **Superposition**
  Value qubit undetermined until moment of measurement (Quantum state collapses)
- **Entanglement**
  Measurement of one qubit has impact on outcome measurement other qubit

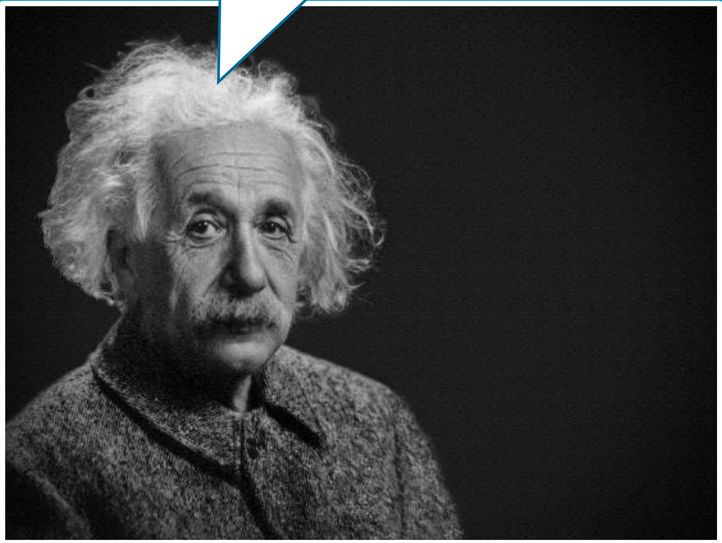
When one qubit measured,
value of the other qubit determined
→ **Type of connection, independent of distance**



State → **Gate** → **State** → **Gate** → **State**

longest path in algorithm

Spukhafte Fernwirkung!
(Spooky action at a distance!)



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

Theoretical power of quantum computers

Observation
When technology is not well understood, we may have a tendency to attribute mythical properties to it

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

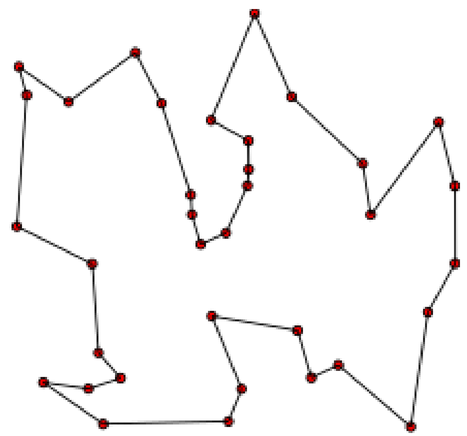
Theoretical power depends on problem

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

Halting problem

No program can be written that can predict whether or not any other program halts after a finite number of steps.

Traveling Salesman problem



Given a list of cities and the distances between each pair of cities, what is the shortest possible route that visits each city exactly once and returns to the origin city?

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 compared to classical computers
- Are – on paper – powerful for a limited group of problems

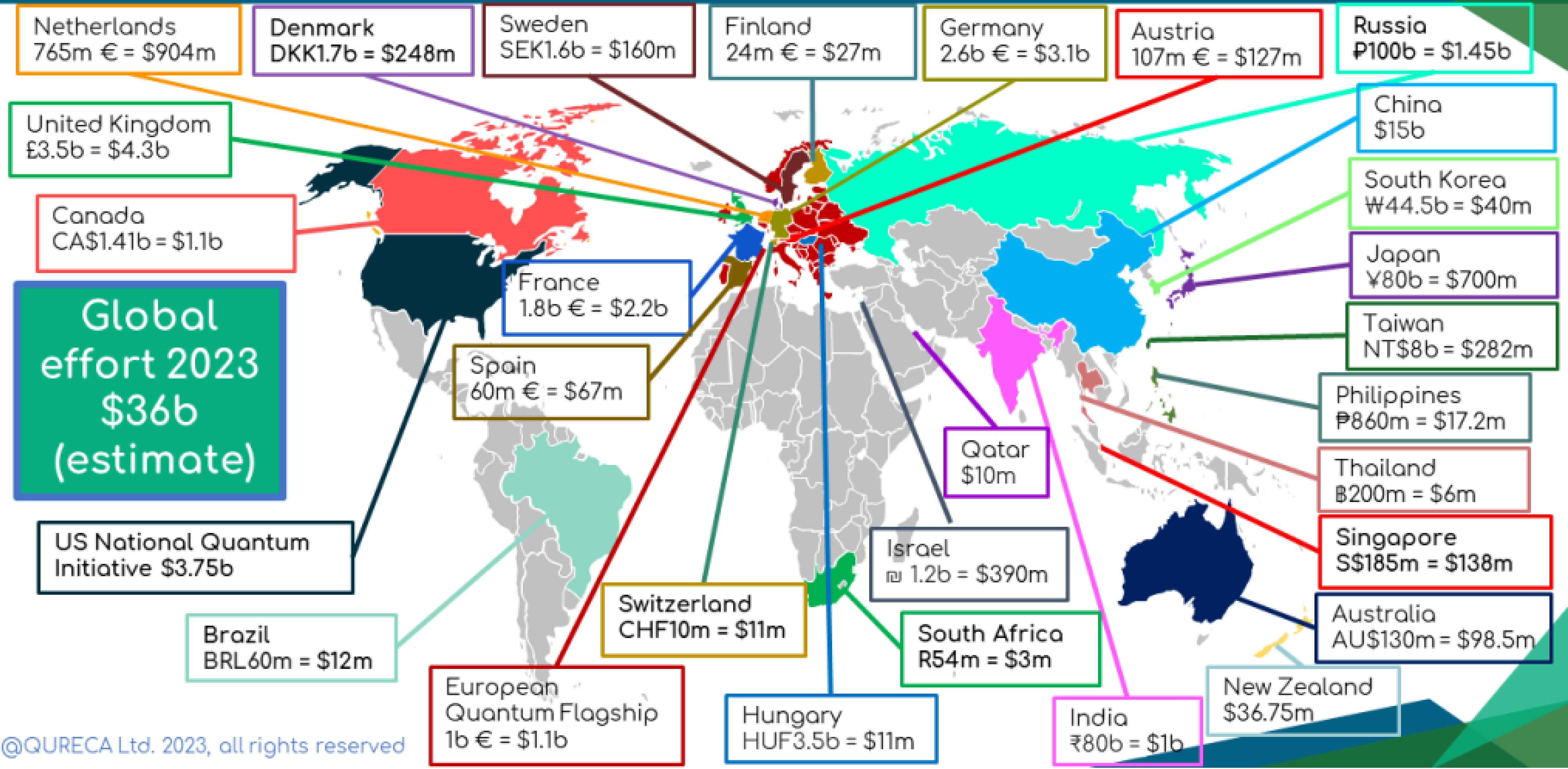
"However, how many times faster [quantum computers will be] remains to be seen. Maybe 10 times, maybe 100 times. Some even talk about 100 million times faster. "

Koen Bertels
Belgian professor at TU Delft
Head Quantum Computer Architectures Lab TU Delft

Source: https://www.vrt.be/vrtnws/nl/2019/12/24/vlaamse-topwetenschappers-blikken-vooruit-naar-2030-kwantumcomp/

Quantum effort worldwide

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



Belgium

Quantum communication = quantum key exchange
≠ quantum computing
→ One way to protect against quantum computing threats on communication level

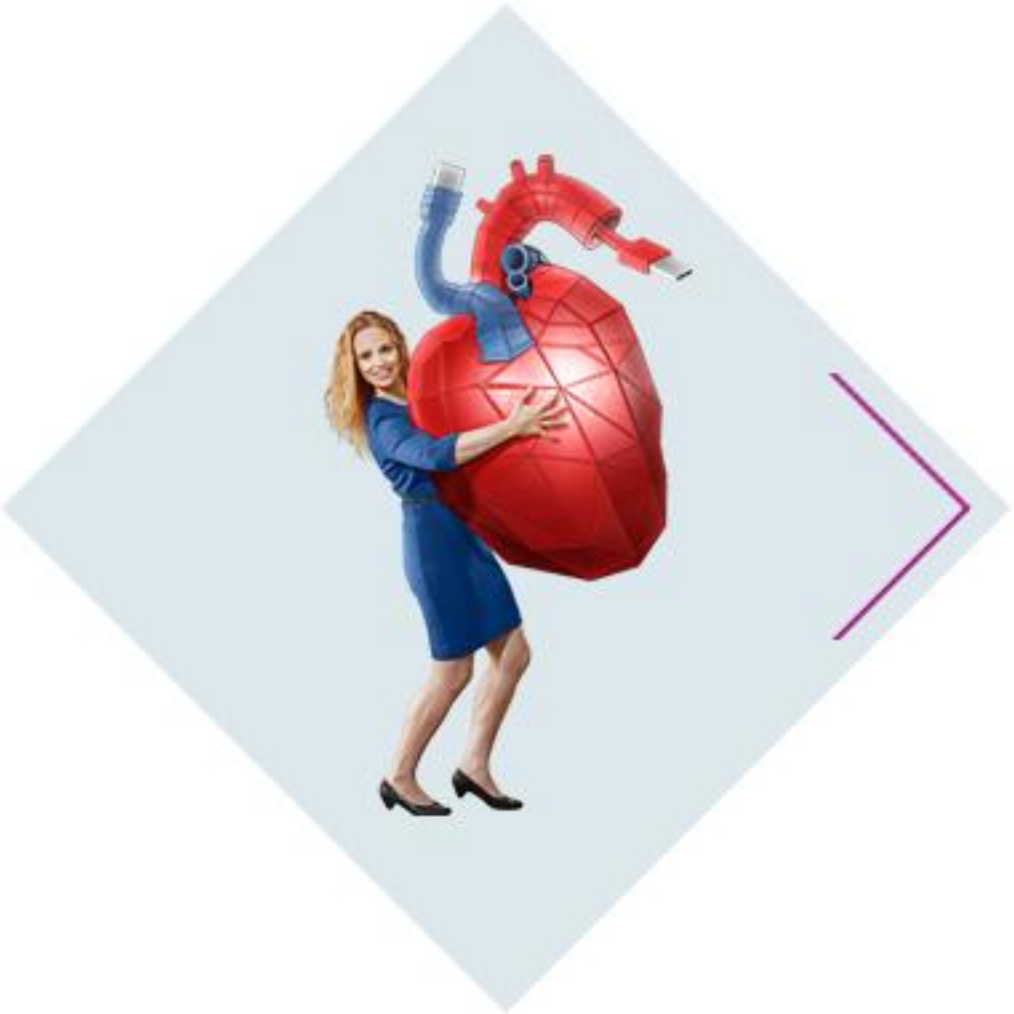
https://beqci.eu/

The goal of BeQCI is to introduce, evaluate and develop quantum communication infrastructure (QCI) in Belgium. Our consortium unites theoretical, experimental and engineering expertise on quantum technology, bringing together different university research groups, research centers, governmental agencies and private companies. BeQCI is part of the European EuroQCI initiative and is co-funded by the EU through the Digital Europe program and the Belgian Federal Science Policy Office (Belspo) through the Federal restart and transition plan.

Funded by the EU and the Belgian Science Policy Office

belspo

Smals
ICT for society



Agenda

- Quantum computers in theory
- **Quantum computers in practice**
- Crypto-apocalypse now?
- Quantum-resistant cryptography

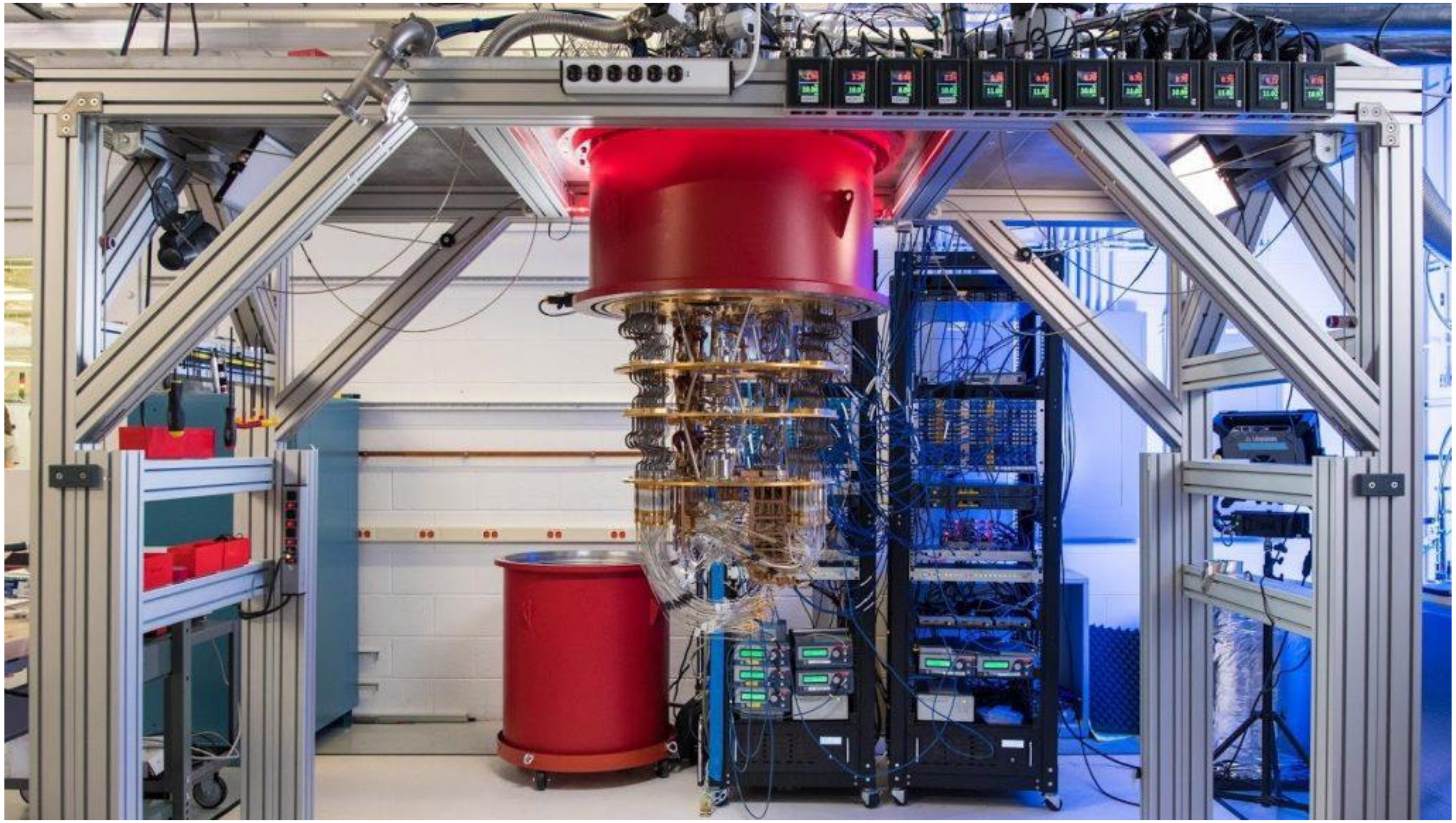
23 October 2019

Google

Article

Quantum supremacy using a programmable superconducting processor

nature International journal of science



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

Google claims quantum supremacy

23 oktober 2019

Google

Article

Quantum supremacy using a programmable superconducting processor

nature
International journal of science

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 strong achievement

The problem

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

The claim

“Our Sycamore quantum computer does in 200 seconds what a classical computer would take 10 000 years to do.”

The response

- **IBM**
  “Conservatively estimated, this can be done in 2,5 days with a conventional computer, and with a much higher accuracy”
- *“Ordinary computers can beat Google’s quantum computer after all”*, August 2022, Science

Smals
ICT for society

China claims quantum primacy

PHYS.ORG — 27 oktober 2021

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 ...

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

"10^{23} x faster than a classical supercomputer"
"600 million years on traditional computers"

The response

- Not contested → quantum supremacy / primacy reached
- Several months on classical computer (jan 22)

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

Catch-up by classical algorithms

Sources
https://phys.org/news/2021-10-chinese-teams-primacy-quantum.html
https://www.science.org/doi/10.1126/sciadv.abl9236

Expectation

Quantum computers are catching up and it is likely that sooner or later they will perform certain *useful* tasks better than conventional computers

Smals
ICT for society

Timeline quantum computers

1st half 20th century
Development
Quantum Mechanics

By 1930 QM formalized by
Hilbert, Dirac, Neuman

1980-1982
Idea quantum computer
(Benioff, Feynman, Manin)

1998
First quantum computer
2 qubits

1/2017
D-Wave 2000Q
2048 qubits

R

11/2017
IBM Q 20 Tokyo
20 qubits

3/2018
Google Bristlecone
72 qubits

7/2019
Google Sycamore
54 qubits (53 working)

9/2020
D-Wave Advantage
5000 qubits

11/2021
Jiuzhang 2
60 qubits

/2021
EAGLE
qubits

11/2022
IBM Osprey
433 qubits

D-Wave

- Easier to build
- Requires less entanglement, more qubits
- Initially for optimization questions
- Out of scope

Disclaimer: not an exhaustive list. More complete timeline https://en.wikipedia.org/wiki/List_of_quantum_processors

Development Roadmap | Executed by IBM ✓ On target

IBM **Quantum**

	2019 ✓	2020 ✓	2021 ✓	2022	2023	2024	2025	Beyond 2026
	Run quantum circuits on the IBM cloud	Demonstrate and prototype quantum algorithms and applications	Run quantum programs 100x faster with Qiskit Runtime	Bring dynamic circuits to Qiskit Runtime to unlock more computations	Enhancing applications with elastic computing and parallelization of Qiskit Runtime	Improve accuracy of Qiskit Runtime with scalable error mitigation	Scale quantum applications with circuit knitting toolbox controlling Qiskit Runtime	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 (on target)	Threaded primitives	Error suppression and mitigation		Error correction
System Modularity	Falcon ✓ 27 qubits	Hummingbird ✓ 65 qubits	Eagle ✓ 127 qubits	Osprey (on target) 433 qubits	Condor 1,121 qubits	Flamingo 1,386+ qubits	Kookaburra 4,158+ qubits	Scaling to 10K-100K qubits with classical and quantum communication
					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 ***Quantum Volume***
→ 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° C)
- Schielded from vibrations, light & magnetic radiation

Coherence time

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

Manipulation

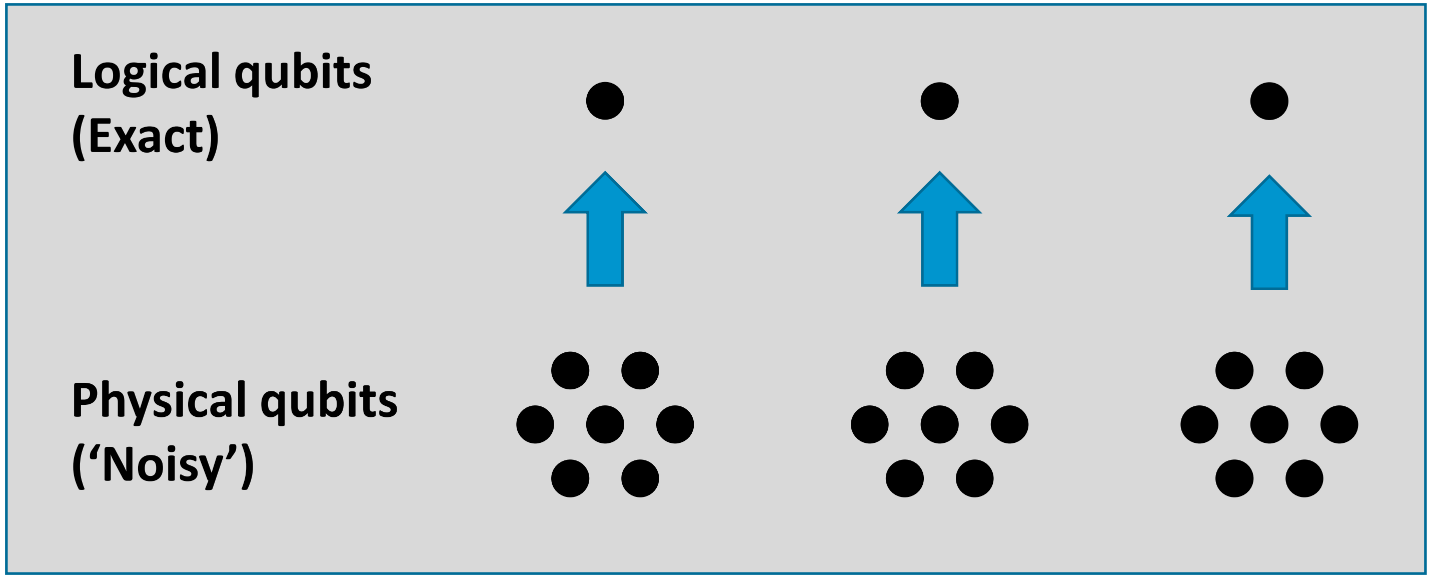
- Quantum logic gates sensitive to errors
- Reading (Measuring qubits)

Evolution

- Significant progress in recent years
- Errors most likely unavoidable

Challenge 2: Error correction

Errors may be unavoidable → error correction necessary
Multiple physical qubits together form 1 logical qubit

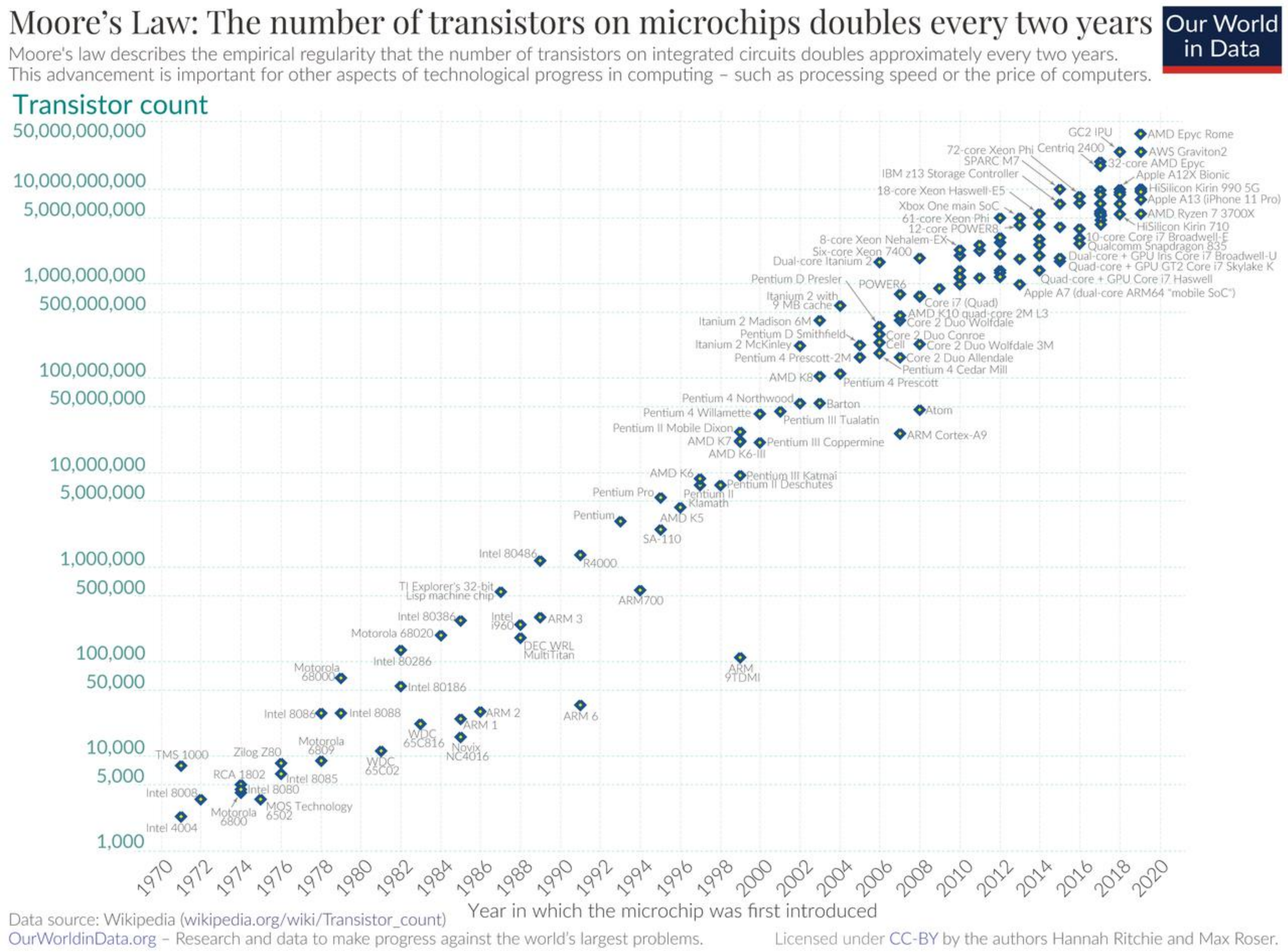


Evolution

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

Requirments

- ❖ Sufficiently long coherence time
- ❖ Estimates: 1000 to 100 000 physical qubits for a logical qubit
  - Noise physical qubits
  - Circuit depth



Classical computer

- Number of transistors on a chip doubles every x (12, 18, 24, 30) months

Quantum computer

- $O(100) \longrightarrow O(10^7)$
- Requires exponential growth
- That can be maintained long enough
- Also higher accuracy required

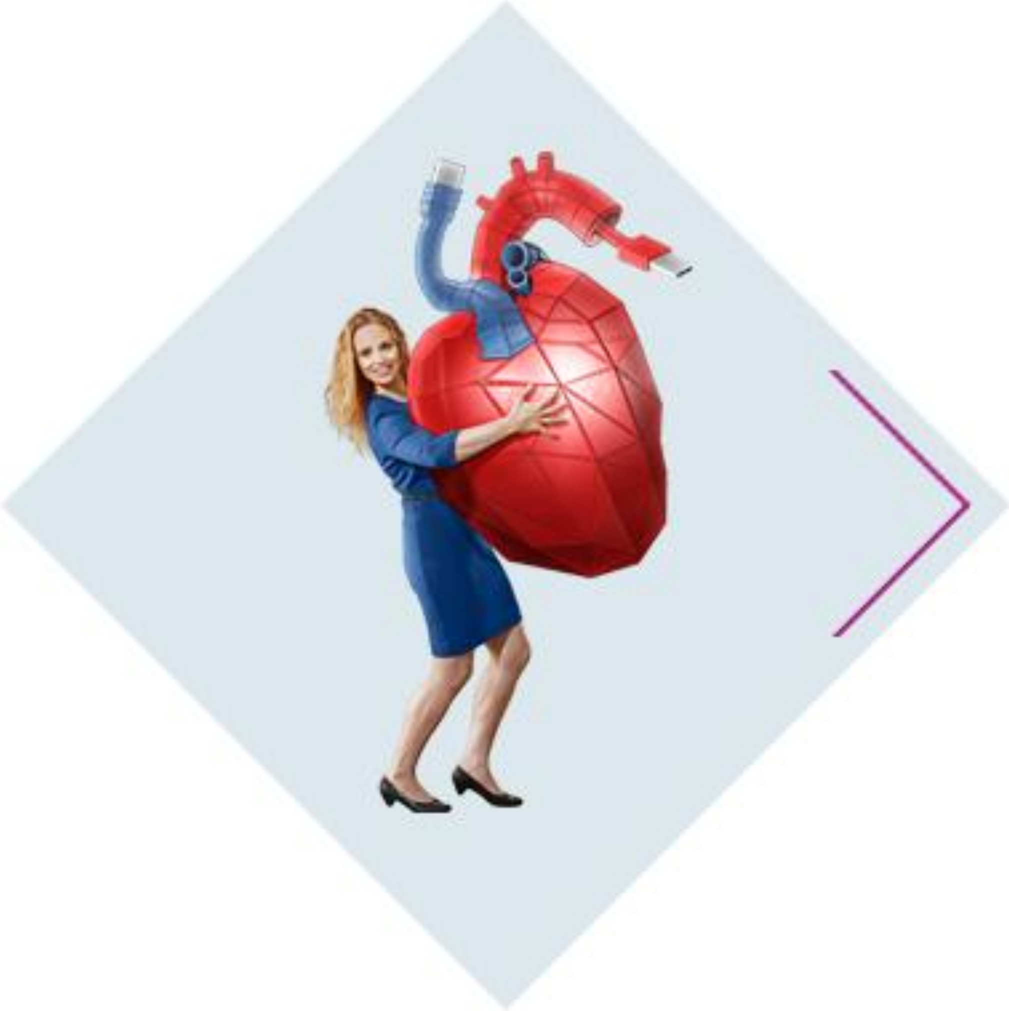
Why is building a quantum computer so complex?

Isolation

Error correction

Scalability

Challenges are astronomical



Agenda

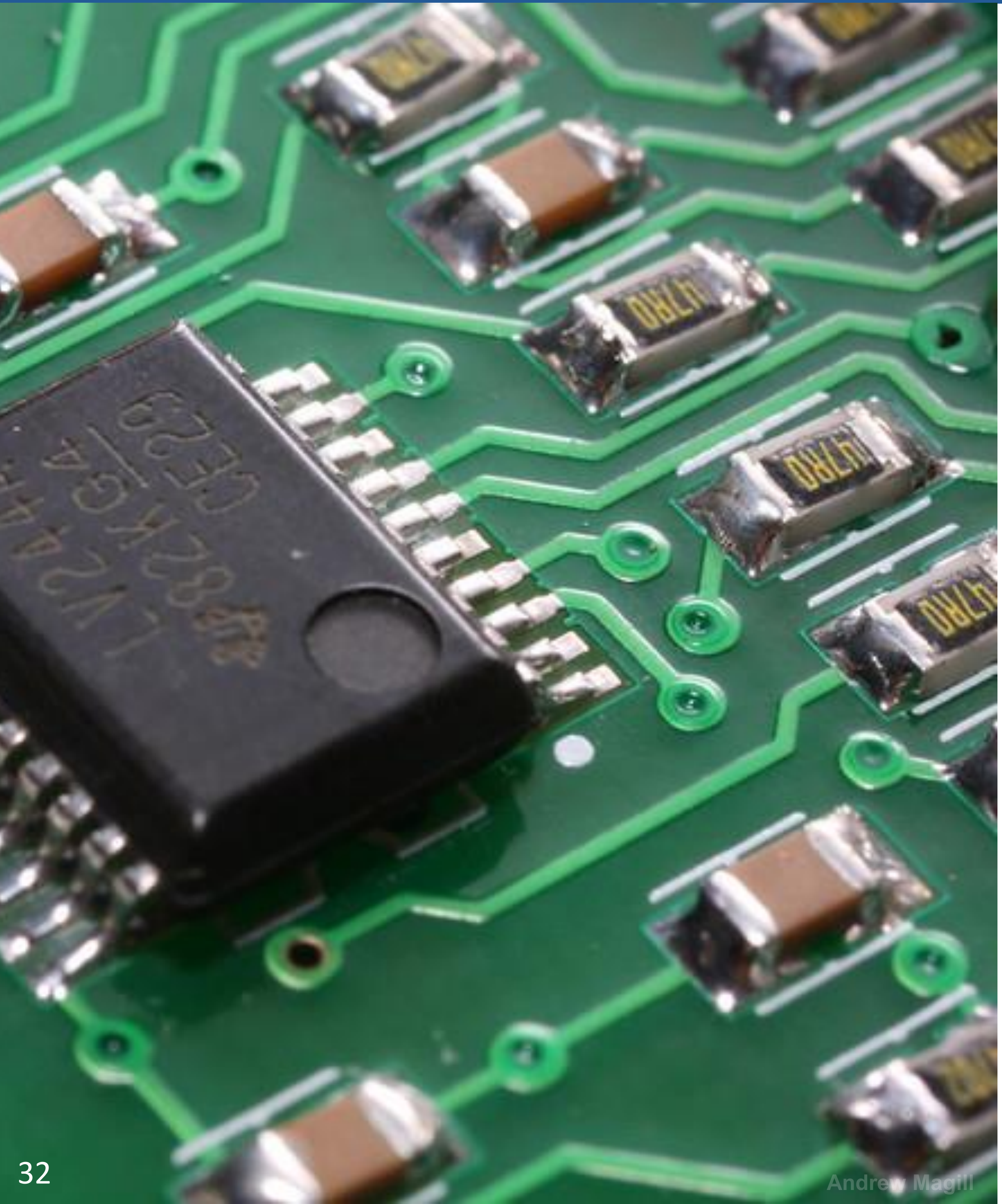
Quantum computers in theory

Quantum computers in practice

Crypto-apocalypse now?

Quantum-resistant cryptography

Modern cryptography



In summary

- ► Cryptography since advent classical computers (1970s)
- ► More than protecting confidentiality of data in transit

Cryptographic mechanisms

Public-key cryptography

Public-key encryption
RSA, ElGamal, …

Authentication
SSH, CHAP, …

Digitals signatures
RSA, DSA, ECDSA, …

Key Exchange
Diffie Hellman, …

Symmetric cryptography

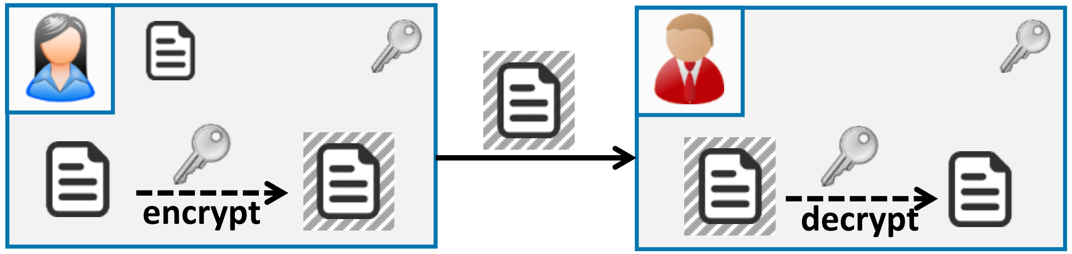
Symmetric encryption
AES, …

Secure hashing
SHA-2, SHA-3, …

Symmetric cryptography

Symmetric encryption & decryption

- Encryption and decryption with same secret key
- Confidentiality
- AES



Marcus Griep

Breaking encryption = 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

Smals
ICT for society

Grover's Algorithm on a quantum computer

Number of LOGICAL qubits required

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

> 10 million PHYSICAL qubits

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

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 $\approx \pi 2^{\frac{n-4}{2}}/\sqrt{k}$ time units, where one unit of time corresponds to the time needed to execute the block cipher on a single quantum computer

Under the very optimistic assumption that one unit of time **in the case of AES-128** in a concrete quantum computer implementation corresponds to one nanosecond and that the adversary has to search a key space of size 2^{120} (due to non-ideal random number generation, for example), **an attack with a single quantum computer takes ≈ 30 years”**

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

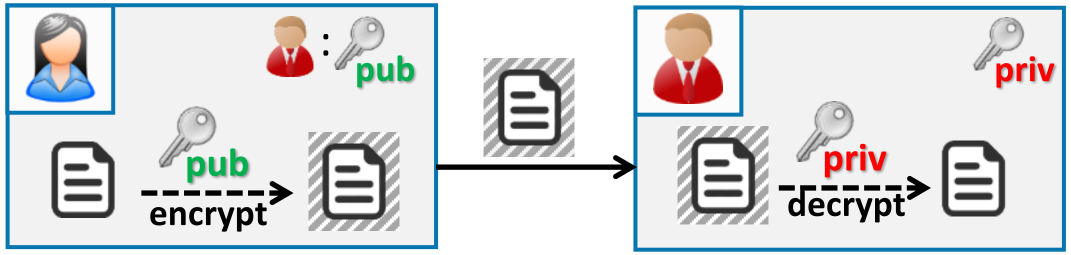
As a precaution, you can take longer keys

Smals ICT for society

 Source: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html

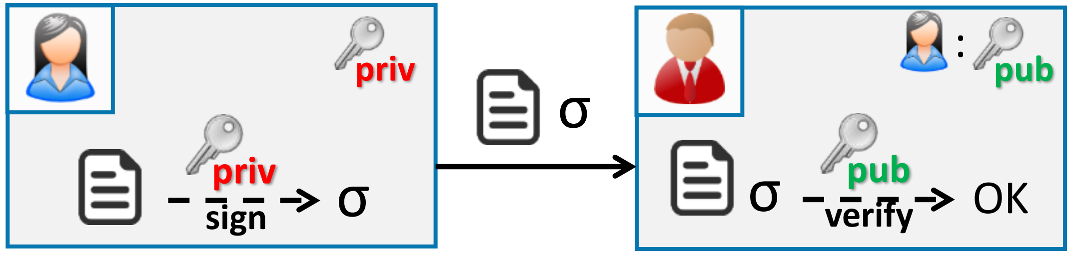
Public-key encryption

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



Digital signatures

- ▶ Data authenticity
- ▶ E.g. Belgian eID card



Also 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 natural 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

2140324650240744961264423072839333563008614715144755017797754920881418023447140136643345519095804679610992851872470914587687396261921557363047454770520805119056493106687691590019759405693457452230589325976697471681738069364894699871578494975937497937

=

6413528947707158027879019017057738908482501474294344720811685963202453234463023862359875266834770873766192558569463979885336 7

×

3337202759497815655622601060535511422794076034476755466678452098702384172921003708025744867329688187756571898625803693206271 1

Was factored by classical computers in February 2020

Public key cryptography – Factorisation

Biggest RSA number factored by classical computer
RSA-250 (829 bits)

2140324650240744961264423072839333563008614715144755017797754920881418023447140136643345519095804679610992851872470914587687396261921557363047454770520805119056493106687691590019759405693457452230589325976697471681738069364894699871578494975937497937

(in 2020, 2700 core-years)

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

21

(in 2012)

Disclaimer

- Quantum computers already factored larger, very specifically chosen numbers without Shor's algorithm.
- Quantum factoring criticized for relying heavily on classical computers

Example of RSA-2048 (2048 bits)

25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357

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

Algoritme	# bits security	# logical qubits	# physical qubits
*RSA-**1024***	80	± 2048	
*RSA-**2048***	112	± 4096	**20 million** (8 hours, 2019)
*RSA-**3072***	128	± 6144	
*RSA-**7680***	192	± 15360	
*RSA-**15360***	256	± 30720	

x2

Elliptic curves

Algoritme	# bits security	# logical qubits	# physical qubits
*P-**256** = secp256r1*	128	± 1536	**13 million** (24 hours, 2022)
*P-**384** = secp384r1*	192	± 2304	
*P-**521** = secp521r1*	256	± 3126	

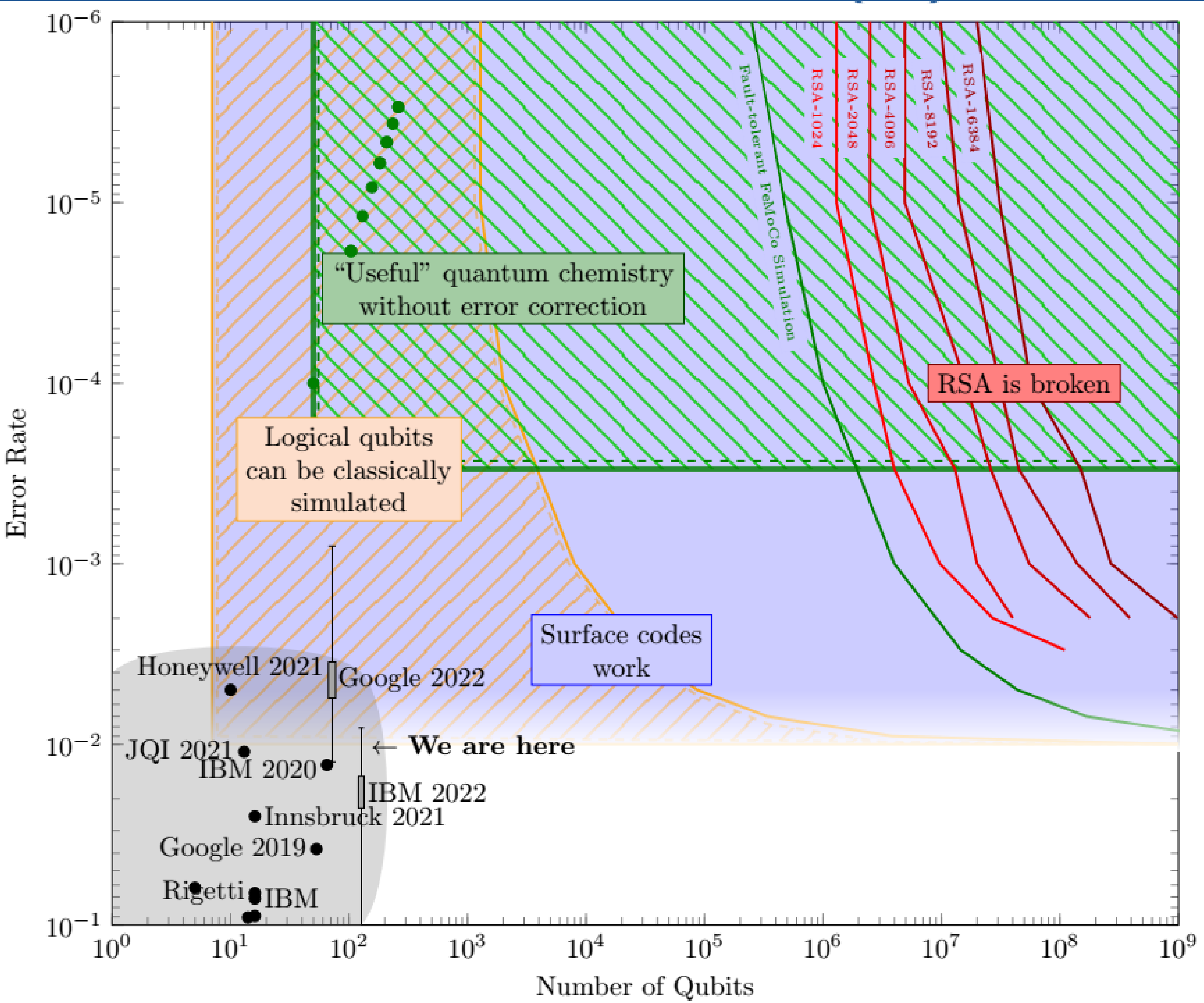
x6

Sources
https://arxiv.org/abs/1905.09749
https://avs.scitation.org/doi/10.1116/5.0073075

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

In the news

INCORRECT CLAIMS!

FINANCIAL TIMES

Quantum technologies + Add to myFT

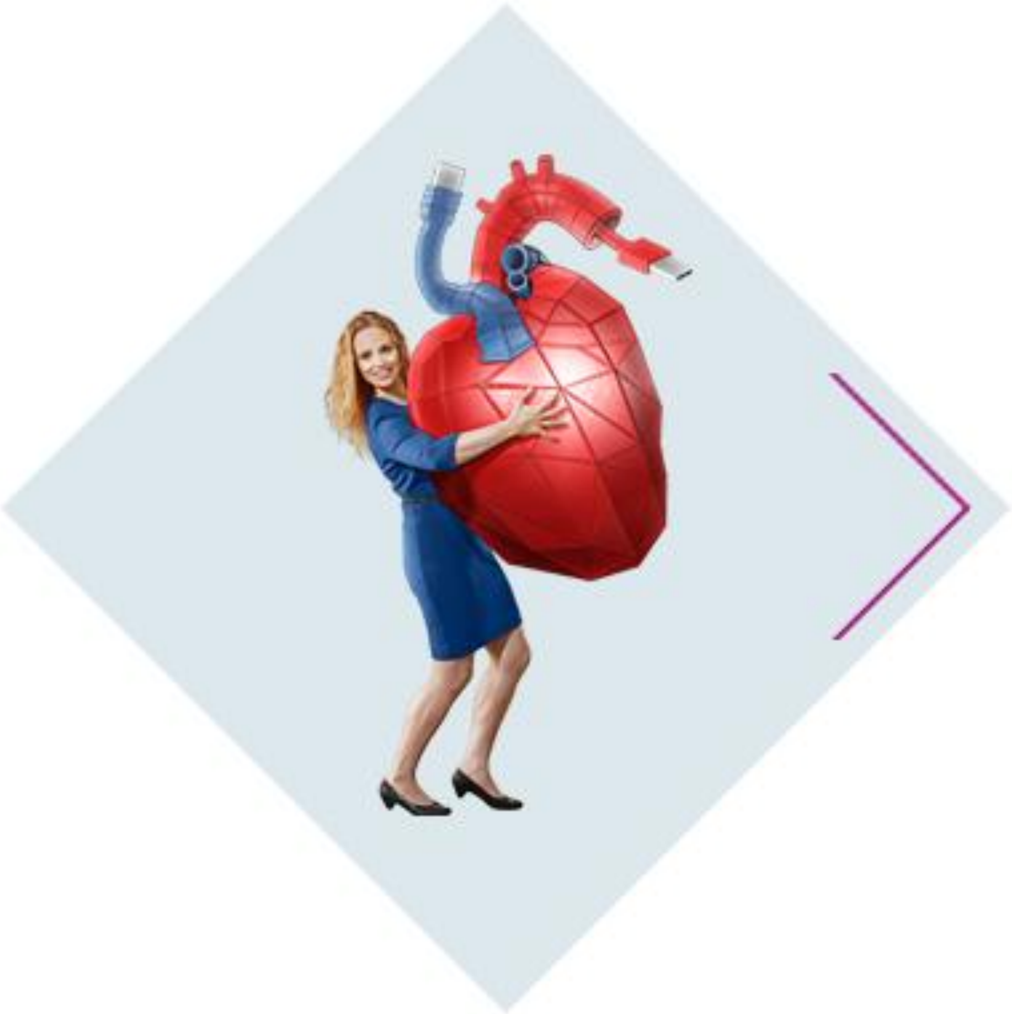
Chinese researchers claim to find way to break encryption using quantum computers

Experts assess whether method outlined in scientific paper could be a sooner-than-expected turning point in the technology

Richard Waters JANUARY 5 2023

Sources
https://www.schneier.com/blog/archives/2023/01/breaking-rsa-with-a-quantum-computer.html
https://arxiv.org/pdf/2307.09651.pdf
https://scottaaronson.blog/?p=6957
https://www.moodysanalytics.com/articles/2023/rsa-and-diffie-hellman-cryptosystems-under-threat-sooner-than-previously-thought

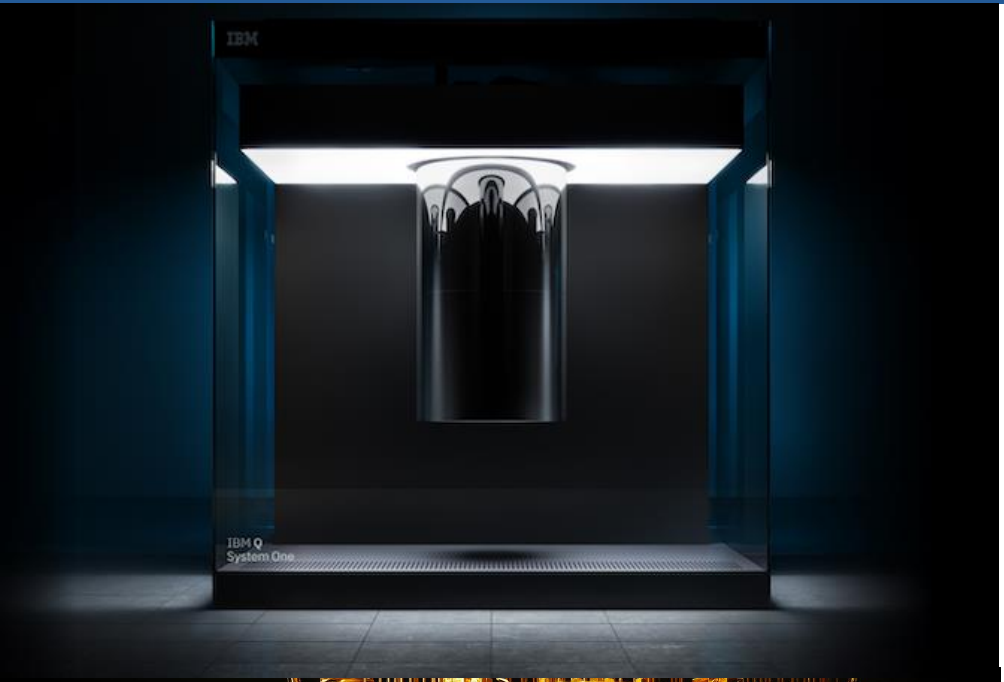
Smals ICT for society

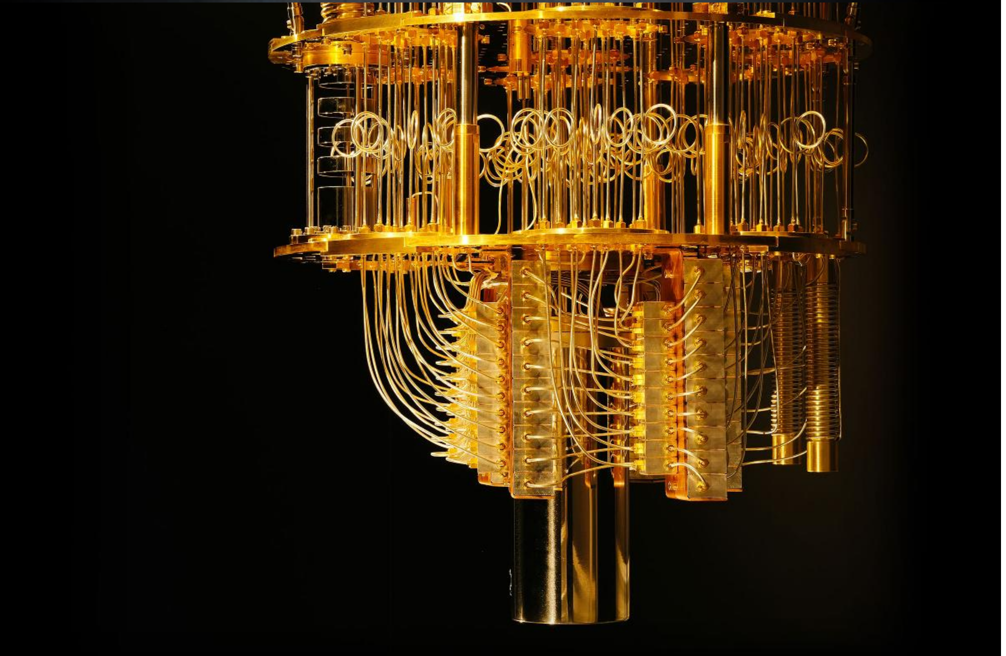


Agenda

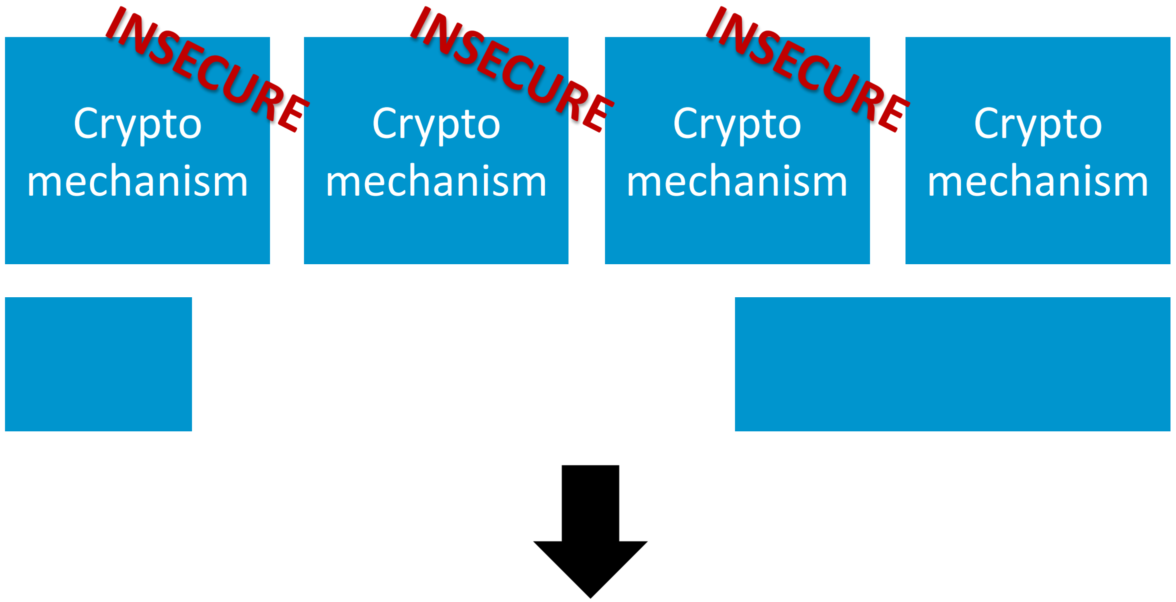
- Quantum computers in theory
- Quantum computers in practice
- Crypto-apocalypse now?
- **Quantum-resistant cryptography**

Crypto assumptions & Quantum computers

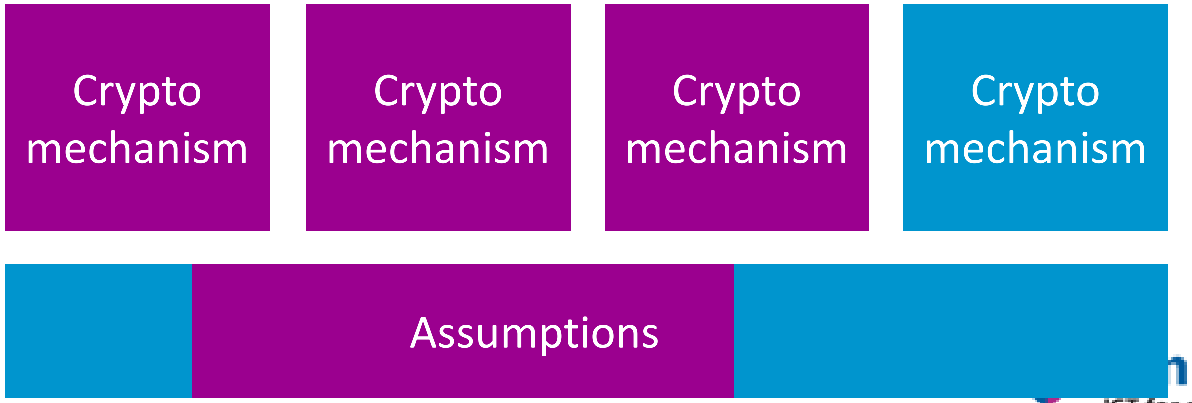




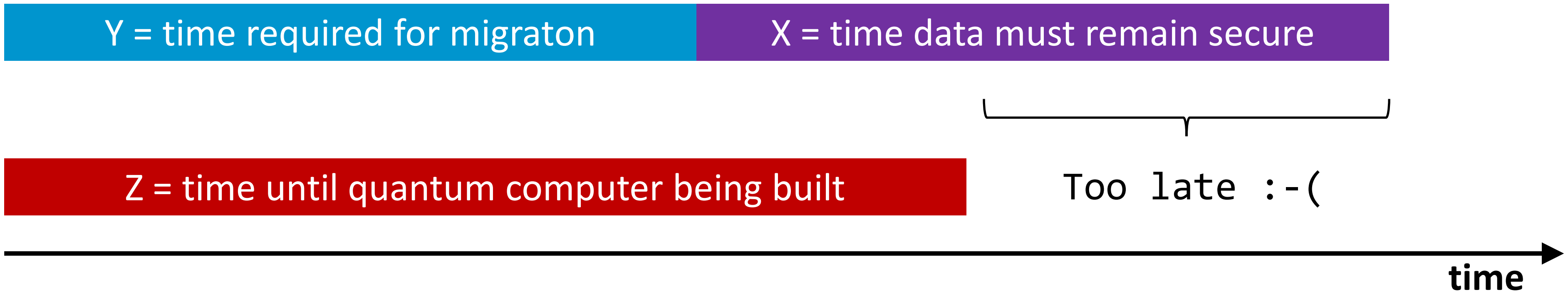
MODERN PUBLIC-KEY CRYPTOGRAPHY



QUANTUM RESISTANT CRYPTOGRAPHY



Mosca's Theorem




```
if      Z > X + Y
then    too late :-(
```

Attack scenario "*Harvest now, decrypt later*" should be taken into account
→ Forced to think a long time in advance!
→ Primarily key-agreement schemes (data in transit)

Smals
ICT for society

Source: Quantum-safe cryptography – fundamentals, current developments and recommendations

Quantum resistant cryptography – NIST standardisation procedure

Two parts

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

National Institute of Standards and Technology
U.S. Department of Commerce

12/2016
Publication
Call for proposals

11/2017
End
Call for proposals
82 submissions

12/2017
Start 1e round
69 candidates
withold

01/2019
1st round
finished
26 candidates left

07/2020
2nd round finished
7 finalists
8 alternatives

2022
Selection
4 algorithms

2024 (?)
Standardization
& selection from
alternatives

08/2022
Publication Call for proposals
Digital signatures

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

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

Smals
ICT for society

WIRED SIGN IN

DAN GOODIN, ARS TECHNICA SECURITY AUG 3, 2022 9:00 AM

A New Attack Easily Knocked Out a Potential Encryption Algorithm

SIKE was a contender for post-quantum-computing encryption. It took researchers an hour and a single PC to break it.

In the news

SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

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 contained vulnerabilities

Smals
ICT for society

https://www.securityweek.com/ai-helps-crack-a-nist-recommended-post-quantum-encryption-algorithm/

National Security Agency (NSA)

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**

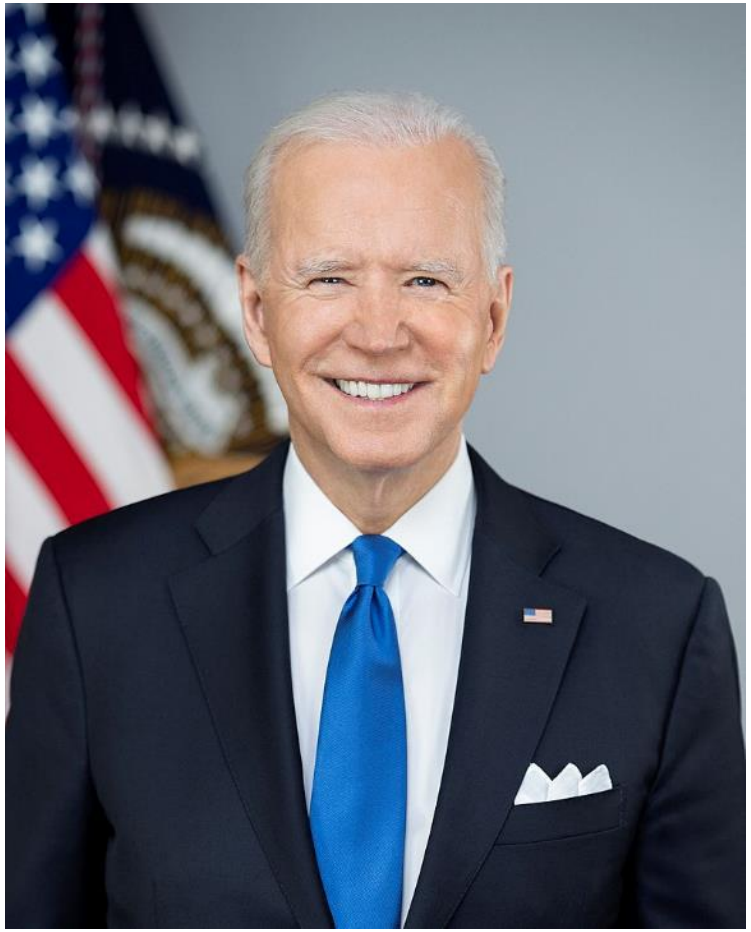
“Unfortunately, the growth of elliptic curve use has bumped up against the fact of continued progress in the research on quantum computing, which has made it clear that ***elliptic curve cryptography is not the long term solution many once hoped it would be****.”*

IAD, defensive branch 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**



Smals ICT for society

Source: https://www.congress.gov/bill/117th-congress/house-bill/7535

Quantum-Readiness: Migration To Post-quantum Cryptography

August 21, 2023

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

- **Establish a quantum-readiness roadmap**
  Establish project management team to plan and scope the organization's migration to PQC
  Initiate cryptographic discovery activities
- **Prepare a cryptographic inventory**
  Offers visibility into how the organization leverages cryptography.
  Cryptographic discovery tools recommended

INVENTORY

- Where in which applications
- Cryptographic mechanisms and parameters
- Security requirements
- Assets & their value (risk)
- Crypto library (dependencies)
- Quantum vulnerable?
- Migration difficulty

Useful even without quantum threat

 Source: https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

Recommendations BSI

Bundesamt für Sicherheit in der Informationstechnik

Hybrid encryption

The quantum-safe algorithms that are currently being standardized are not yet as well researched as the "classical" methods *(for example RSA and ECC). This applies in particular to weaknesses that largely only become apparent in applications, such as typical implementation errors, possible side-channel attacks, etc.* ***BSI therefore recommends that post-quantum cryptography should not be used in isolation if possible, but only in hybrid mode, i.e. in combination with classical algorithms****. […] Hash-based signatures can in principle also be used on its own (i.e., not in hybrid mode).*

Cryptographic agility

Particular attention should be paid to ***making cryptographic mechanisms as flexible as possible in order to be able to react to developments, implement upcoming recommendations and standards****, and possibly replace algorithms in the future that no longer guarantee the desired level of security ("cryptographic agility"). This is particularly important due to the threat posed by quantum computers, though not exclusively: classical attacks can also evolve and make encryption schemes or key lengths once considered secure obsolete.*

Quantum-safe cryptography – fundamentals, current developments and recommendations. October 2022

 Source: Quantum-safe cryptography – fundamentals, current developments and recommendations. 22/05/2022

Crypto agility

- **Crypto policies**
  - ✓ On the level of the organization
    ↔ ad-hoc decisions by individual teams
  - ✓ Compliant with standards, regulations & recommendations

- **Integration in project**
  - ✓ Foresee scenario's for key rotation and migration of crypto mechanisms
  - ✓ Evaluate regularly whether change is required
  - ✓ Evaluate impact on performance, stability, …

- **Programming**
  - ✓ Modular programming
  - ✓ Explicit crypto names and parameters
    (key length, hash length, encryption mode, …)
    ↔ hard-coded, defaults …

- …

Smals
ICT for society

Advice from the BSI

If I could give companies and organisations three pieces of advice as they prepare for quantum safety, they would be:

- **Include the threat in your risk management system**
- **Create a crypto inventory**
- **Implement and use crypto-agility**

Dr. Gerhard Schabhüser
Vice President, BSI

Smals
ICT for society

Source: KPMG, BSI. *Market Survey on Cryptography and Quantum Computing*. 22/08/2023.

Thanks for your attention

If you have any questions, do not hesitate to contact me!
See you at our booth!

kristof.verslype@smals.be
+32(0)2 7875376
linkedin.com/in/verslype

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

DEVOXX™

Smals
ICT for society

Sources pictures

- 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
- 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%C2%A0announces%C2%A0d-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
- Natascha. Keys. https://www.flickr.com/photos/tasj/5207744064
- Kristof Verslype. Threatening clouds above Lake Titicaca, Peru. https://www.flickr.com/photos/verslype/23928588621
- Hari K Patibanda. A Peregrine Falcon in the hunt https://flickr.com/photos/krishnacolor/51822106250/