

# Quantum computers Vs. Modern cryptography

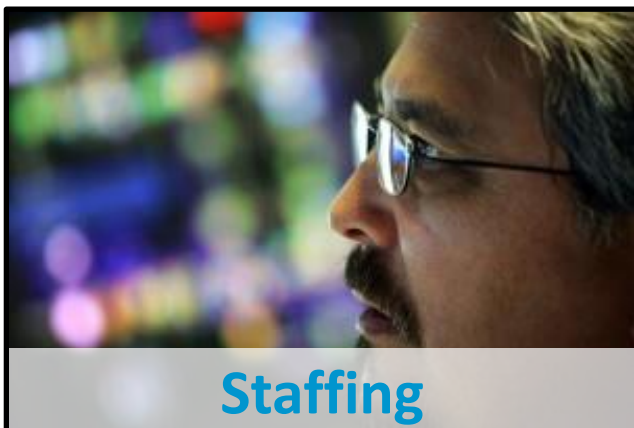
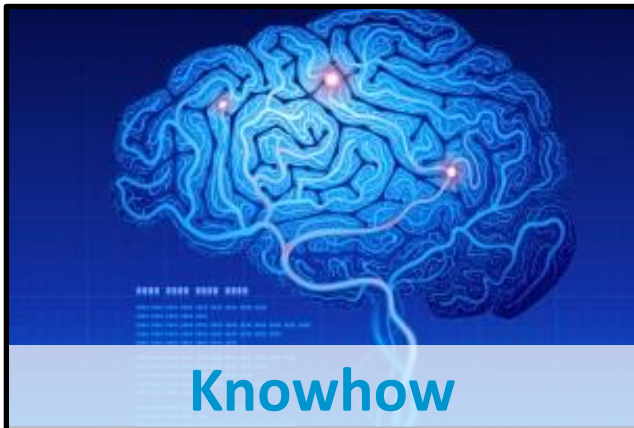
---

Kristof Verslype  
Smals Research





# SUPPORT FOR E-GOVERNMENT



[WWW.SMALS.BE](http://WWW.SMALS.BE)





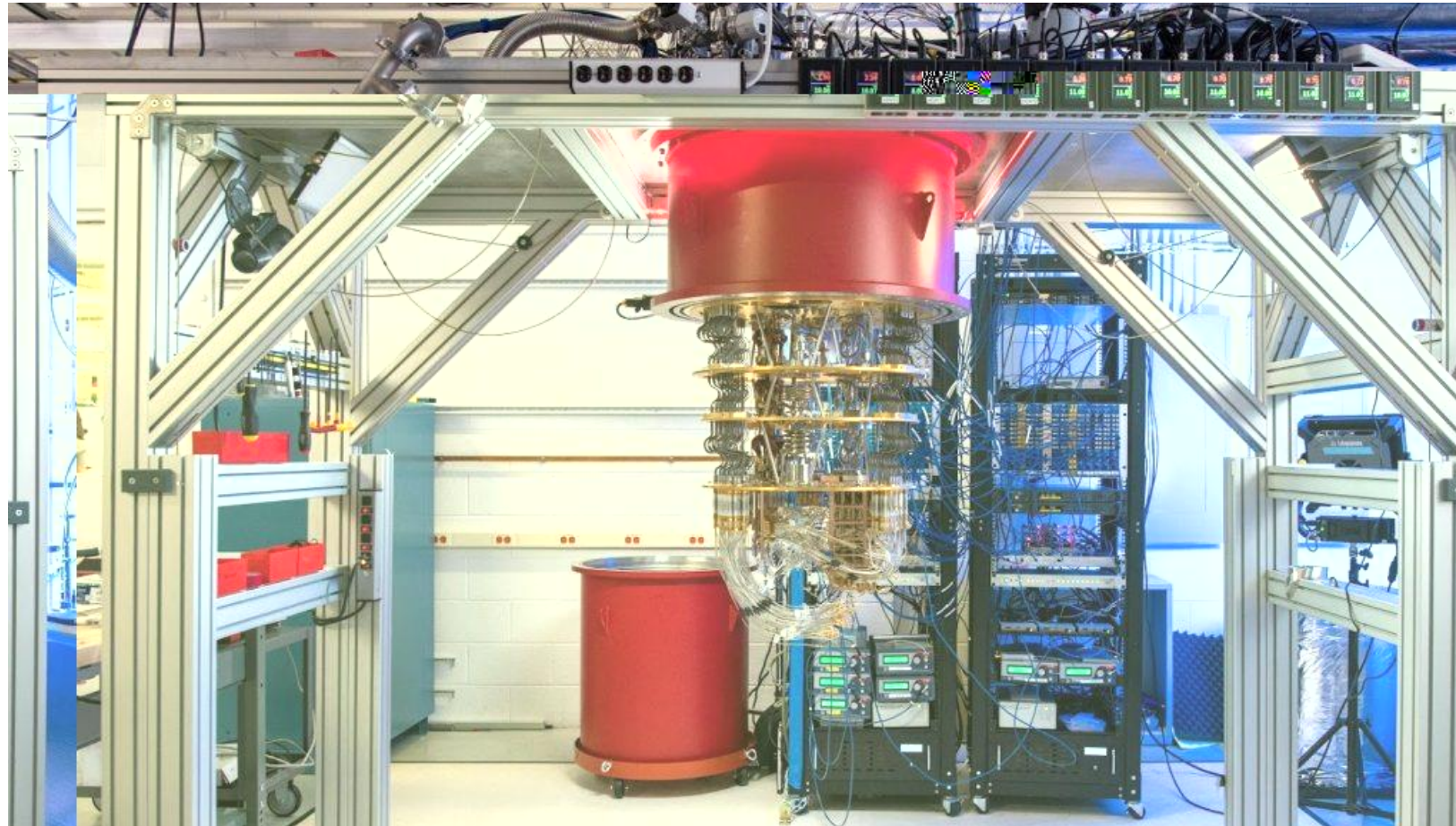
**Many articles, but sometimes hard to interpret correctly**

23 October 2019



Article

# Quantum supremacy using a programmable superconducting processor



## 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*.

27 January 2022

# **THE    BYTE.**

QUANTUM APOCALYPSE

## **EXPERTS WARN OF "QUANTUM APOCALYPSE"**

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

*encryption methods*



The image shows a screenshot of a news article from the website Wired. At the top left, there is a menu icon (three horizontal lines) followed by the 'WIRED' logo in a bold, black, sans-serif font. To the right of the logo, the text 'SIGN IN' is visible, followed by a vertical line and a magnifying glass icon representing a search function. Below the header, the author's name 'DAN GOODIN, ARS TECHNICA' is displayed in white text on a black rectangular background. To the right of the author's name, the category 'SECURITY' and the date and time 'AUG 3, 2022 9:00 AM' are shown in a smaller, black, sans-serif font. The main title of the article is 'A New Attack Easily Knocked Out a Potential Encryption Algorithm', written in a large, bold, black, sans-serif font. Below the title, a short paragraph of text reads: 'SIKE was a contender for post-quantum-computing encryption. It took researchers an hour and a single PC to break it.'

## 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



Correct

**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



**Is the quantum army advancing at a rapid pace?**



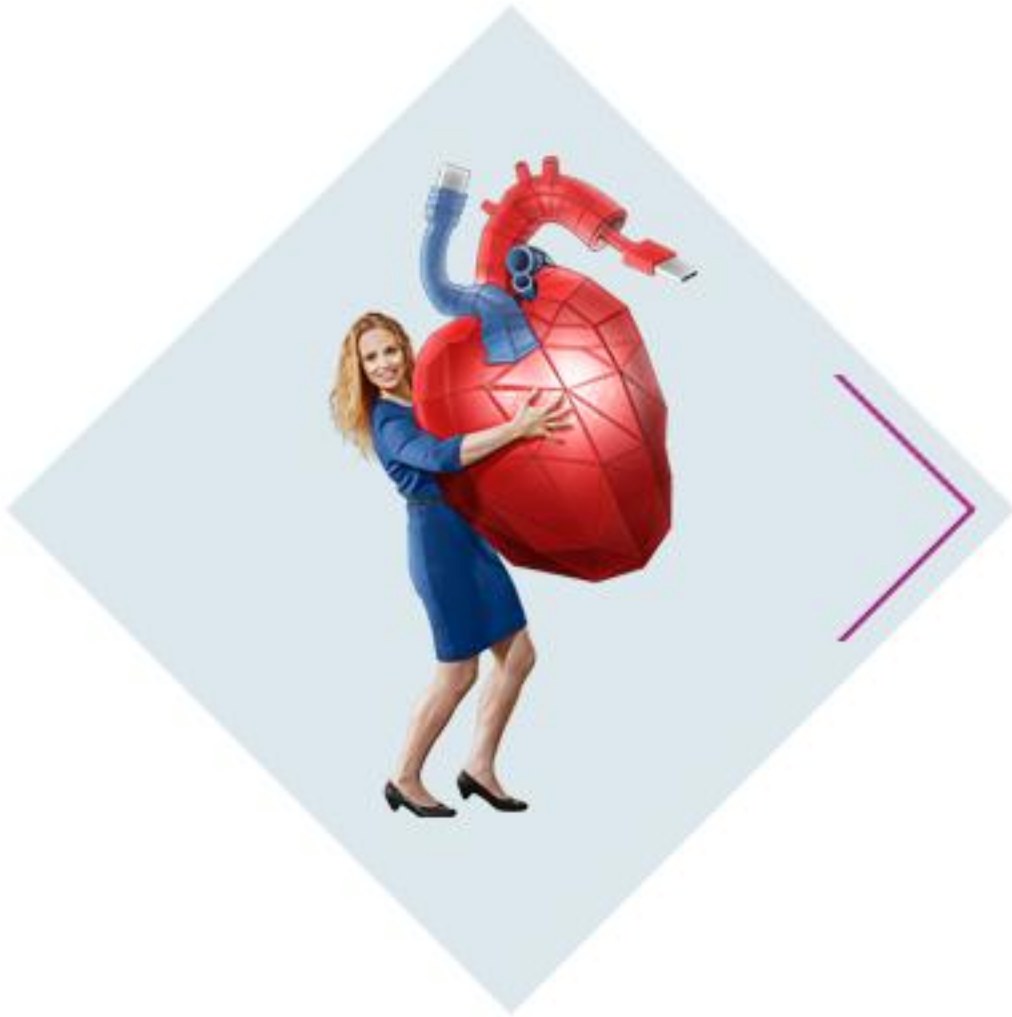
# Agenda

Quantum computers in theory

Quantum computers in practice

Crypto-apocalypse now?

Quantum-resistant cryptography



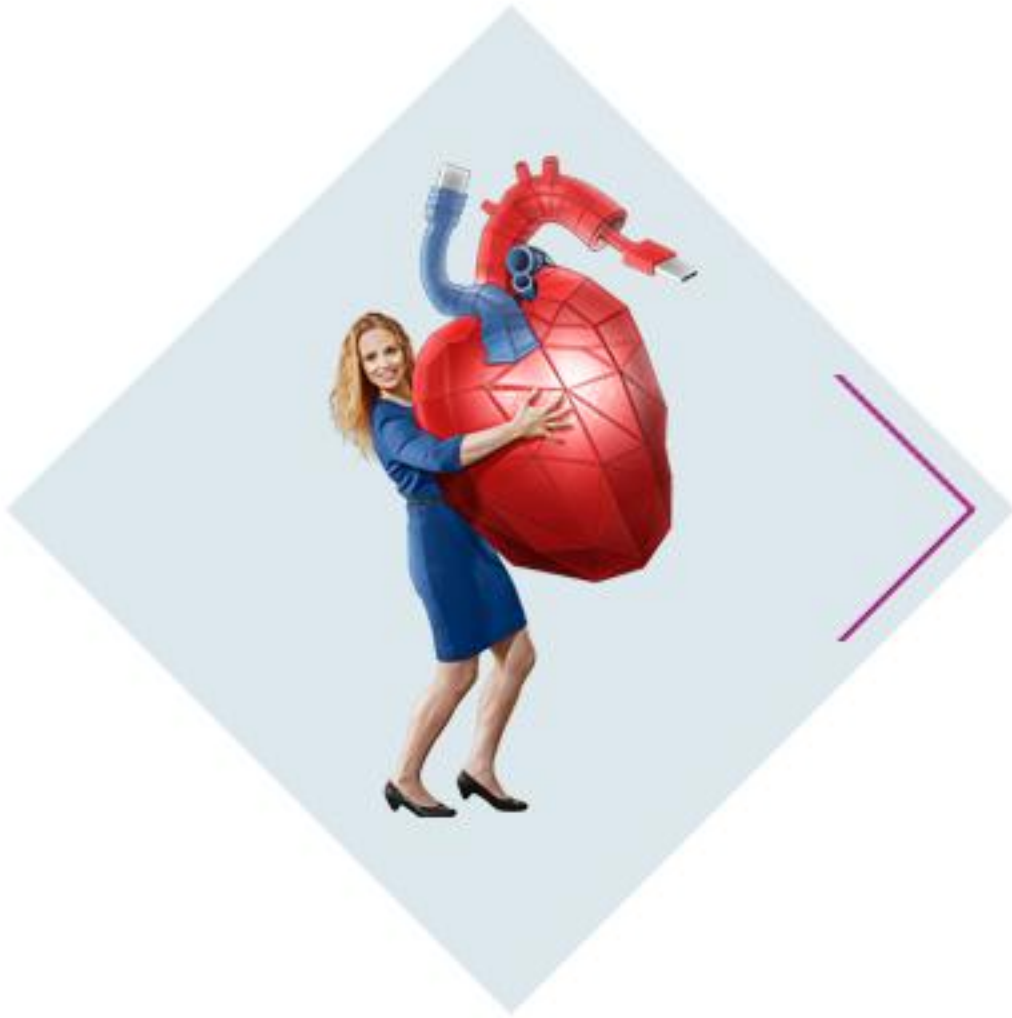
# Agenda

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

### ❖ Superposition

Value qubit undetermined until moment of measurement (Quantum state collapses)

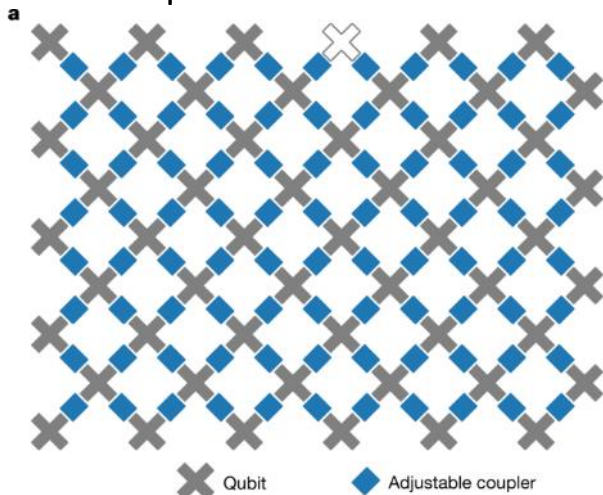
### ❖ Entanglement

Measurement of one qubit has impact on outcome measurement other qubit

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

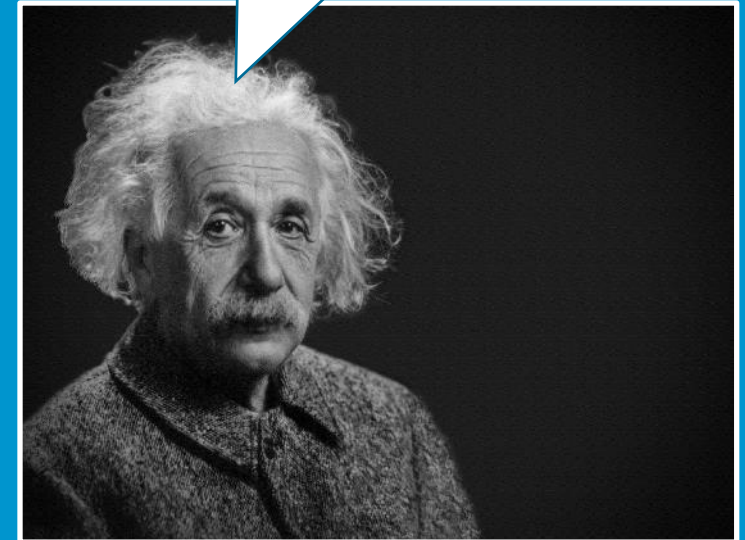
## Quantum state

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



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"

## 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.”*

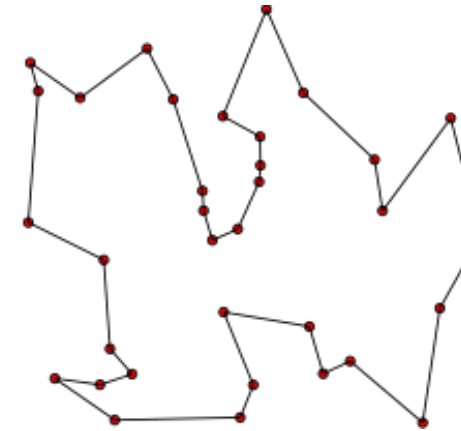
## Theoretical power depends on problem

- ❖ 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



”

“

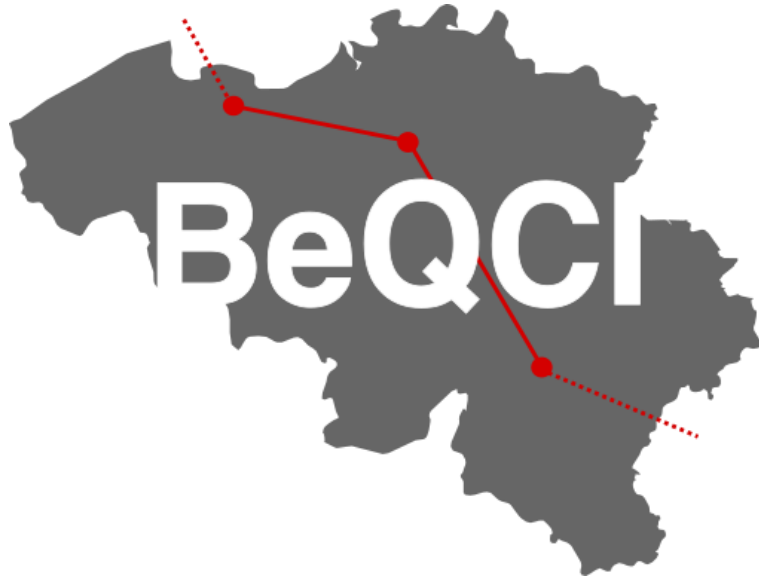
**Koen Bertels**  
Belgian professor at TU Delft  
Head Quantum Computer Architectures Lab TU Delft

# Quantum effort worldwide

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



**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



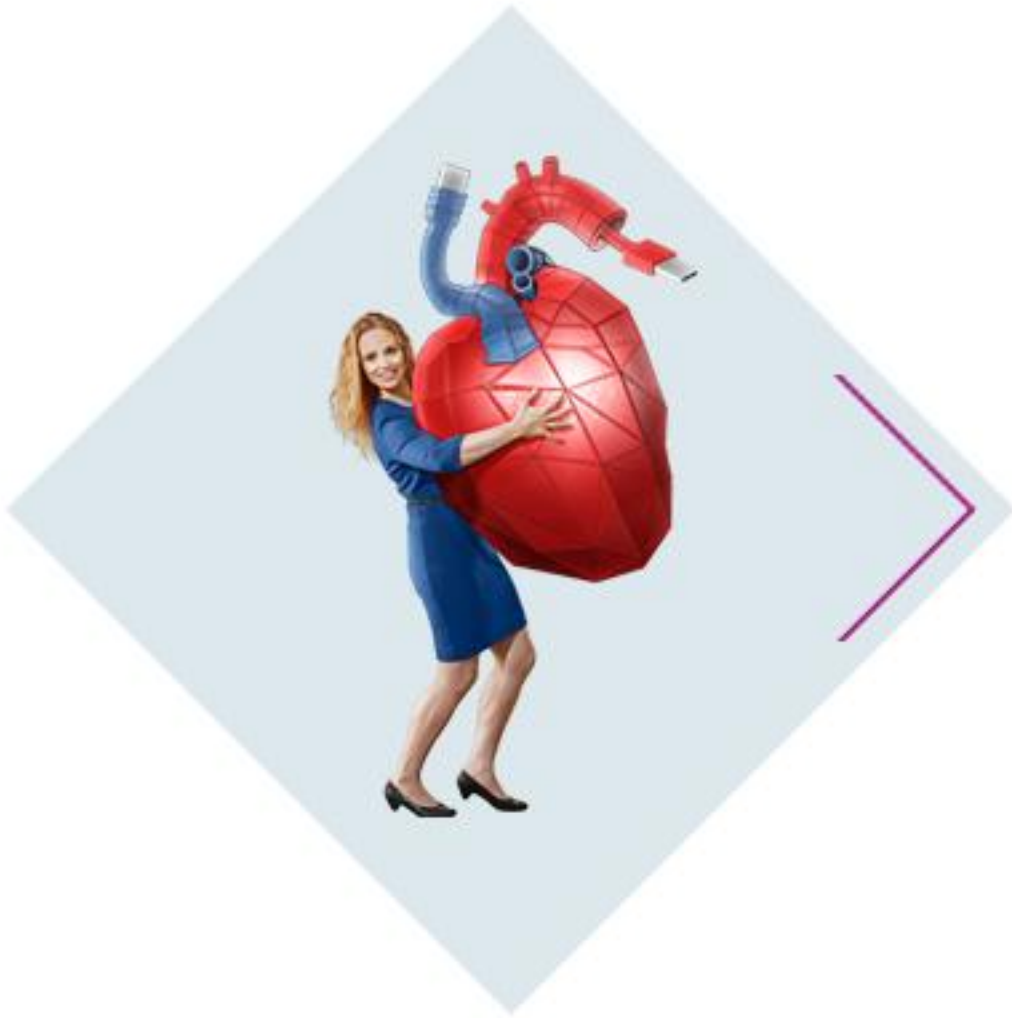
# Agenda

Quantum computers in theory

Quantum computers in practice

Crypto-apocalypse now?

Quantum-resistant cryptography

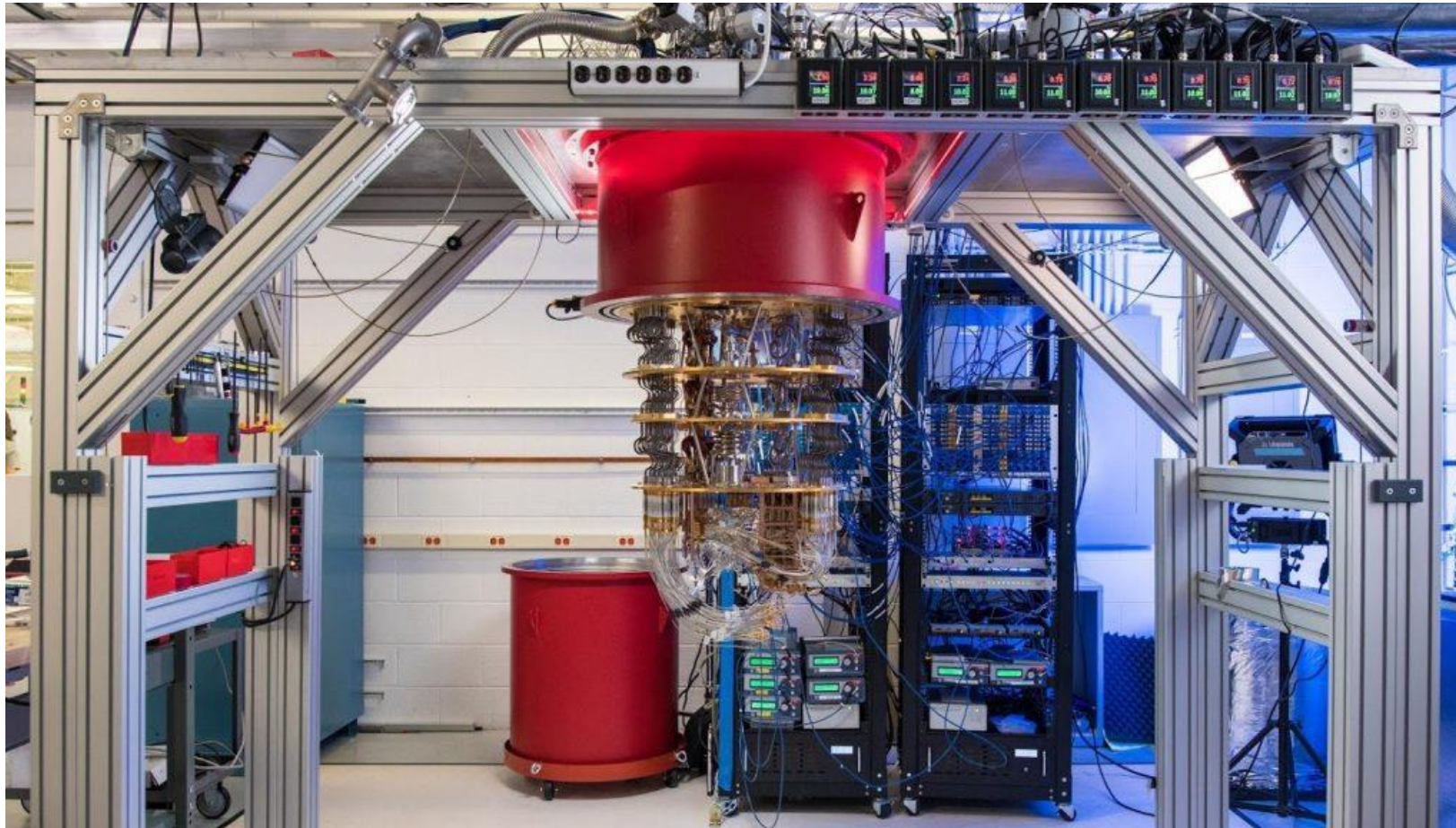


23 October 2019



Article

## Quantum supremacy using a programmable superconducting processor



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 strong achievement**

### The problem

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

### The claim

“

”

### The response

- IBM

“

”


- “

”, August 2022, Science

**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

“ ”

## 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>



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

# Timeline quantum computers

1st half 20th century  
Development  
Quantum Mechanics

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

1998  
First quantum computer  
2 qubits

By 1930 QM formalized by  
Hilbert, Dirac, Neuman

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

1/2017

D-Wave 2000Q R  
2048 qubits



## D-Wave

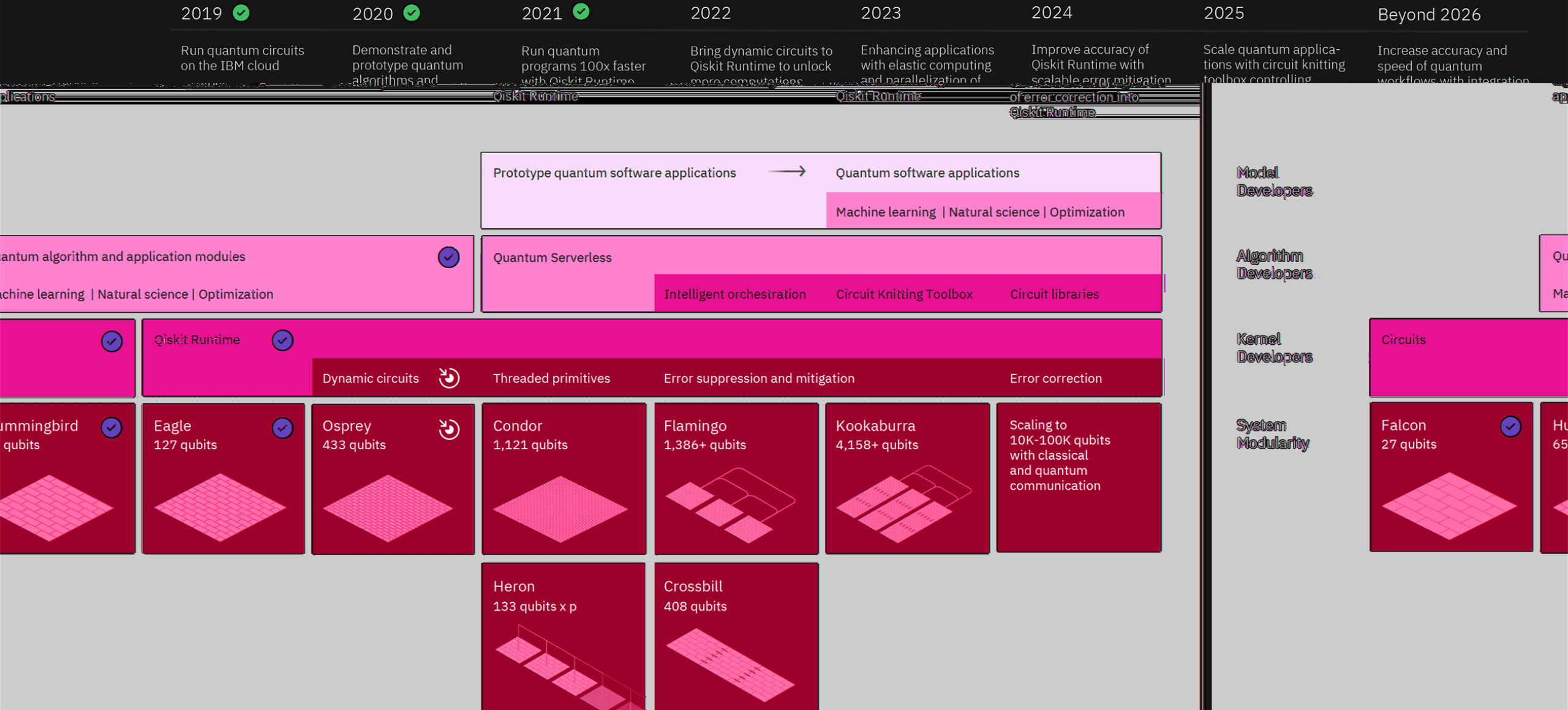
- ❖ Easier to build
- ❖ Requires less entanglement, more qubits
- ❖ Initially for optimization questions
- ❖ Out of scope

'2021  
EAGLE  
qubits

11/2022  
IBM Osprey  
433 qubits

# Development Roadmap

Executed by IBM ✔  
On target ↻



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



## 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

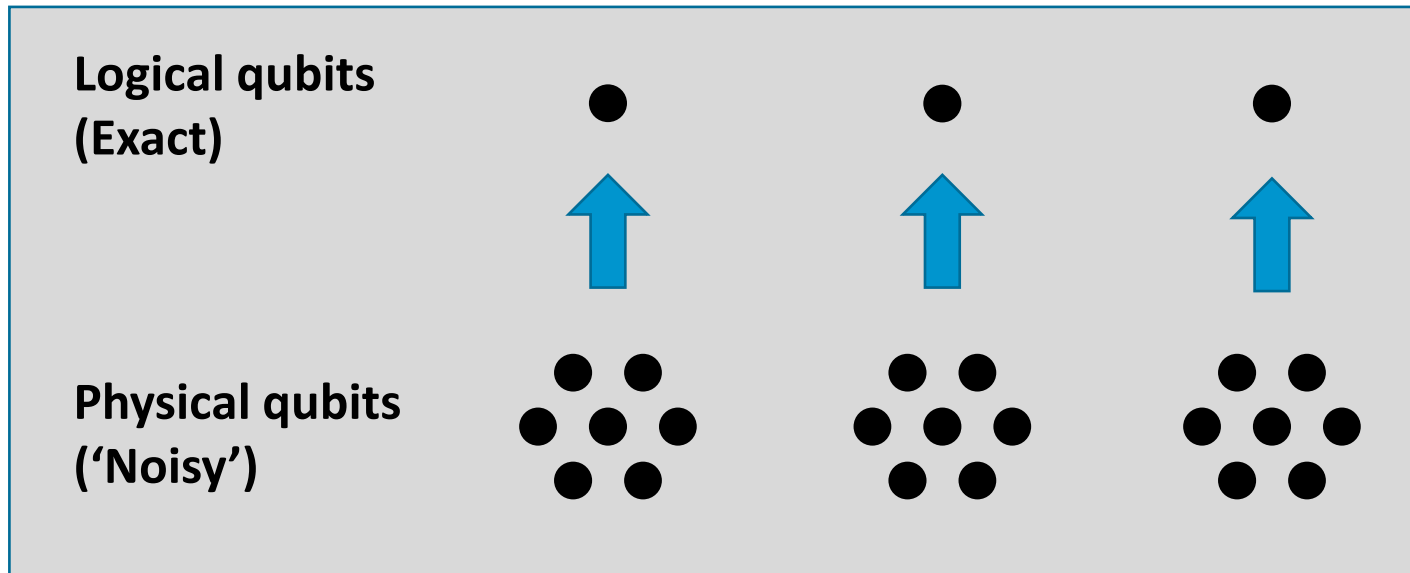
- ❖ Quantum logic gates sensitive to errors
- ❖ Reading (Measuring qubits)

## 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



### 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
  - Circuit depth



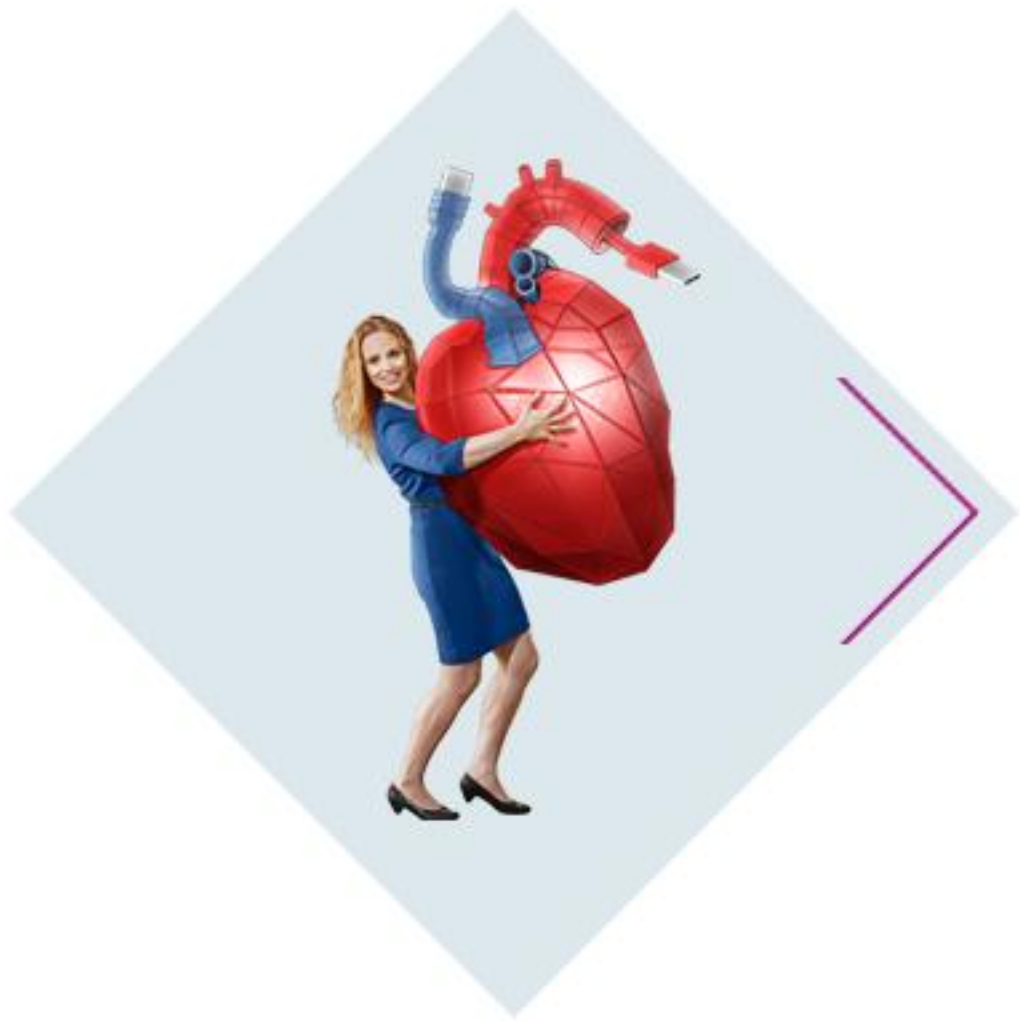
Why is building a quantum computer so complex?

Isolation

Error correction

Scalability

**Challenges are astronomical**



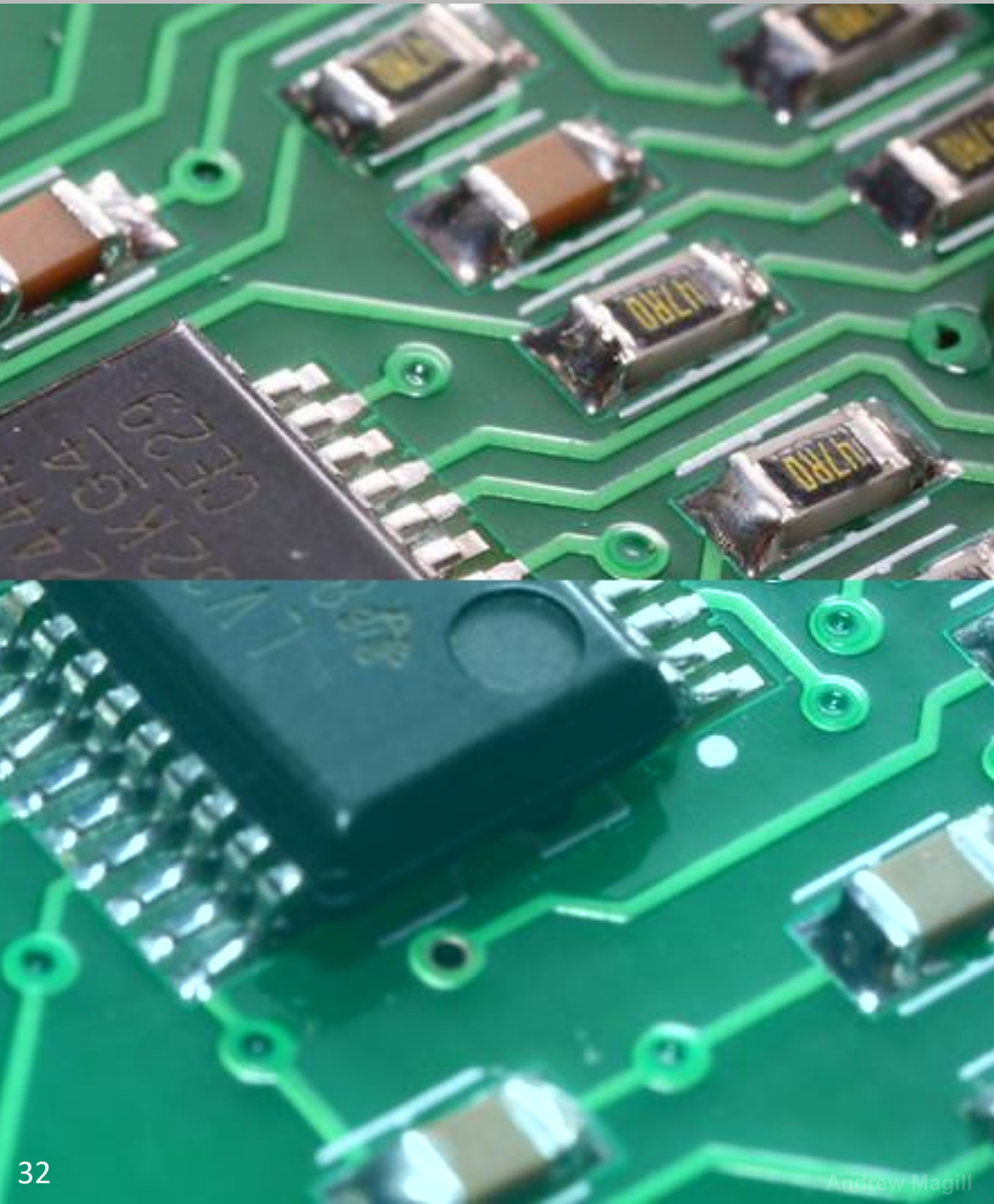
# Agenda

Quantum computers in theory

Quantum computers in practice

**Crypto-apocalypse now?**

Quantum-resistant cryptography



## 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, ...

#### Digital signatures

RSA, DSA, ECDSA, ...

#### Key Exchange

Diffie Hellman, ...

### Symmetric CRYPTOGRAPHY

#### Symmetric encryption

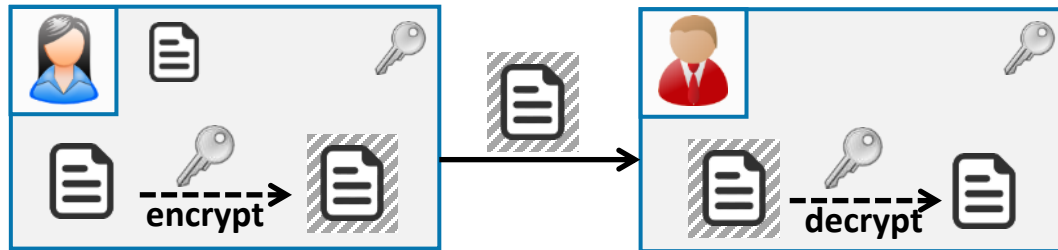
AES, ...

#### Secure hashing

SHA-2, SHA-3, ...

## Symmetric encryption & decryption

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



## 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

- ▶ Double key length: ~~6~~ → 12 bits 128 → 256 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

> 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



**“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

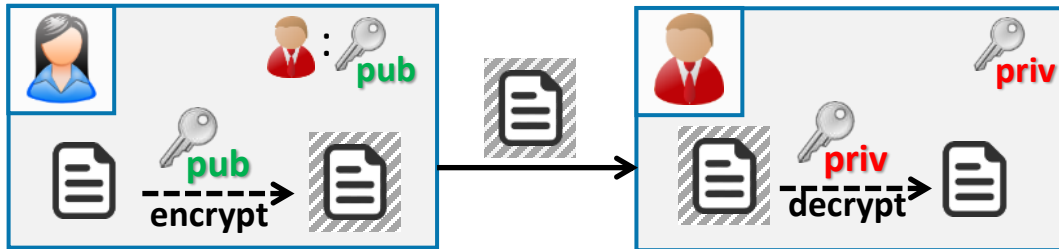
Under the very optimistic assumption that one unit of time **in the case of AES-128** in a concrete quantum computer implementation corresponds to one nanosecond and that the adversary has to search a key space of size  $2^{120}$  (due to non-ideal random number generation, for example), **an attack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

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

**As a precaution, you can take longer keys**

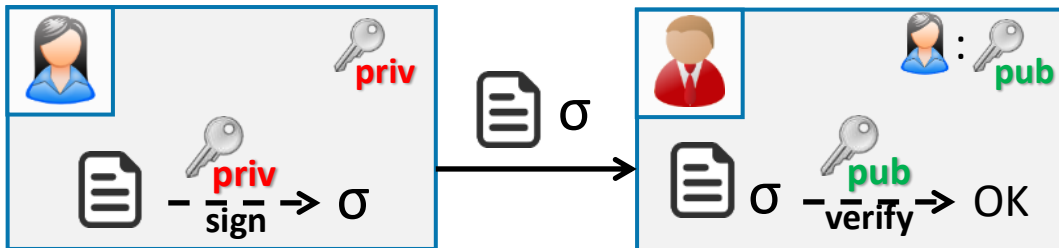
## Public-key encryption

- ▶ 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**

```
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)

## Example of RSA-2048 (2048 bits)

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

### Disclaimer

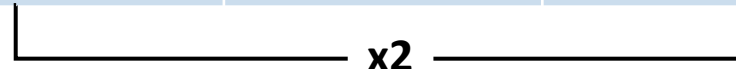
- Quantum computers already factored larger, very specifically chosen numbers without Shor's algorithm.

## Shor's Algorithm (1994)

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

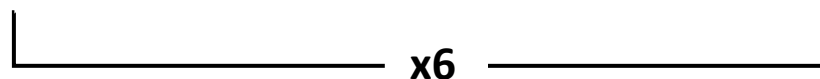
## RSA

Algorithme	# bits security	# logical qubits	# physical qubits
<b>1024</b>	80	± 2048	
<b>2048</b>	112	± 4096	<b>20 million</b> (8 hours, 2019)
<b>3072</b>	128	± 6144	
<b>7680</b>	192	± 15360	
<b>15360</b>	256	± 30720	



## Elliptic curves

Algorithme	# bits security	# logical qubits	# physical qubits
<b>256</b>	128	± 1536	<b>13 million</b> (24 hours, 2022)
<b>384</b>	192	± 2304	
<b>521</b>	256	± 3126	



### Sources

<https://arxiv.org/abs/1905.09749>

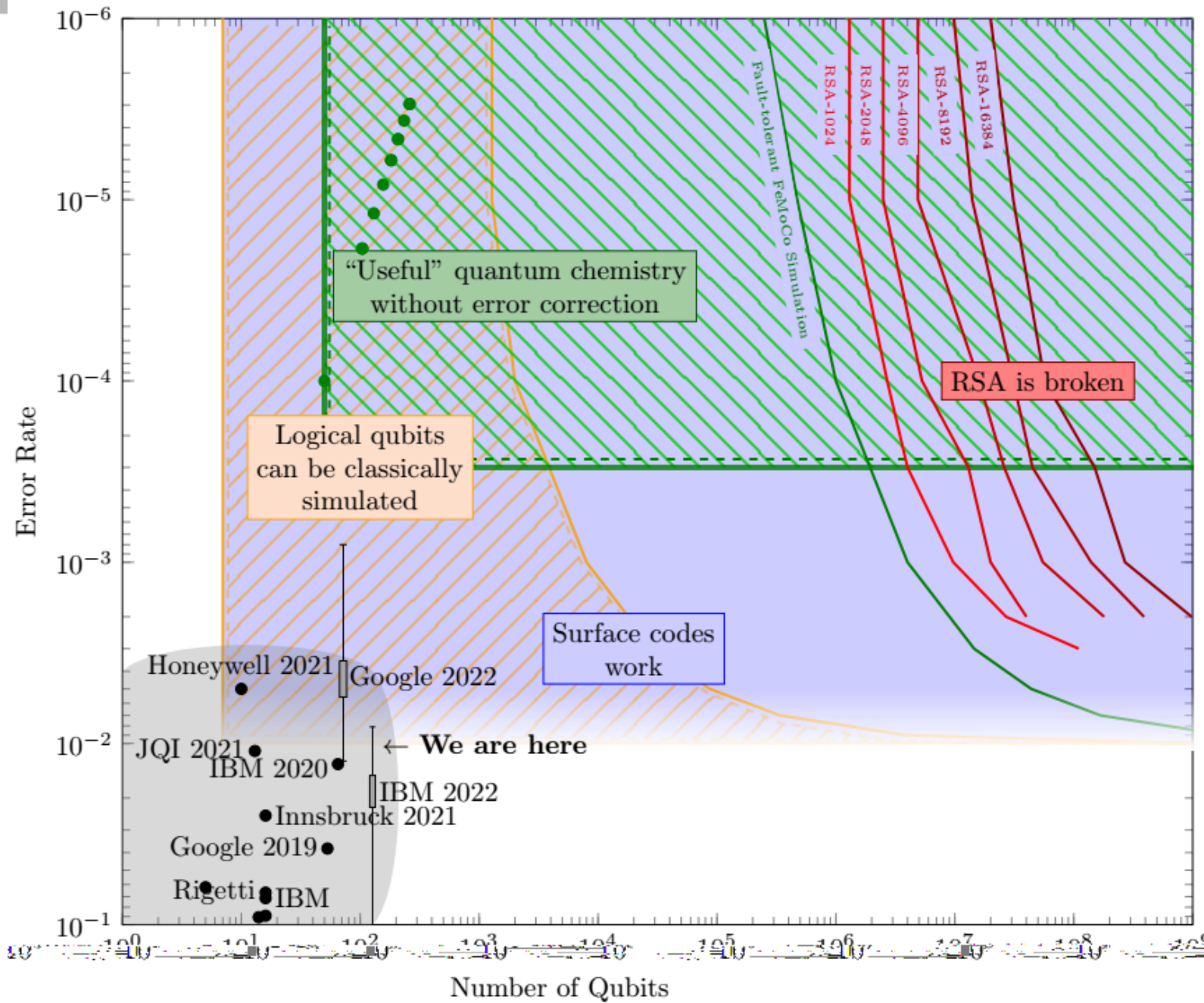
<https://avs.scitation.org/doi/10.1116/5.0073075>



**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 algorithms 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](https://sam-jaques.appspot.com/quantum_landscape_2022)

## 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

**INCORRECT CLAIMS!**

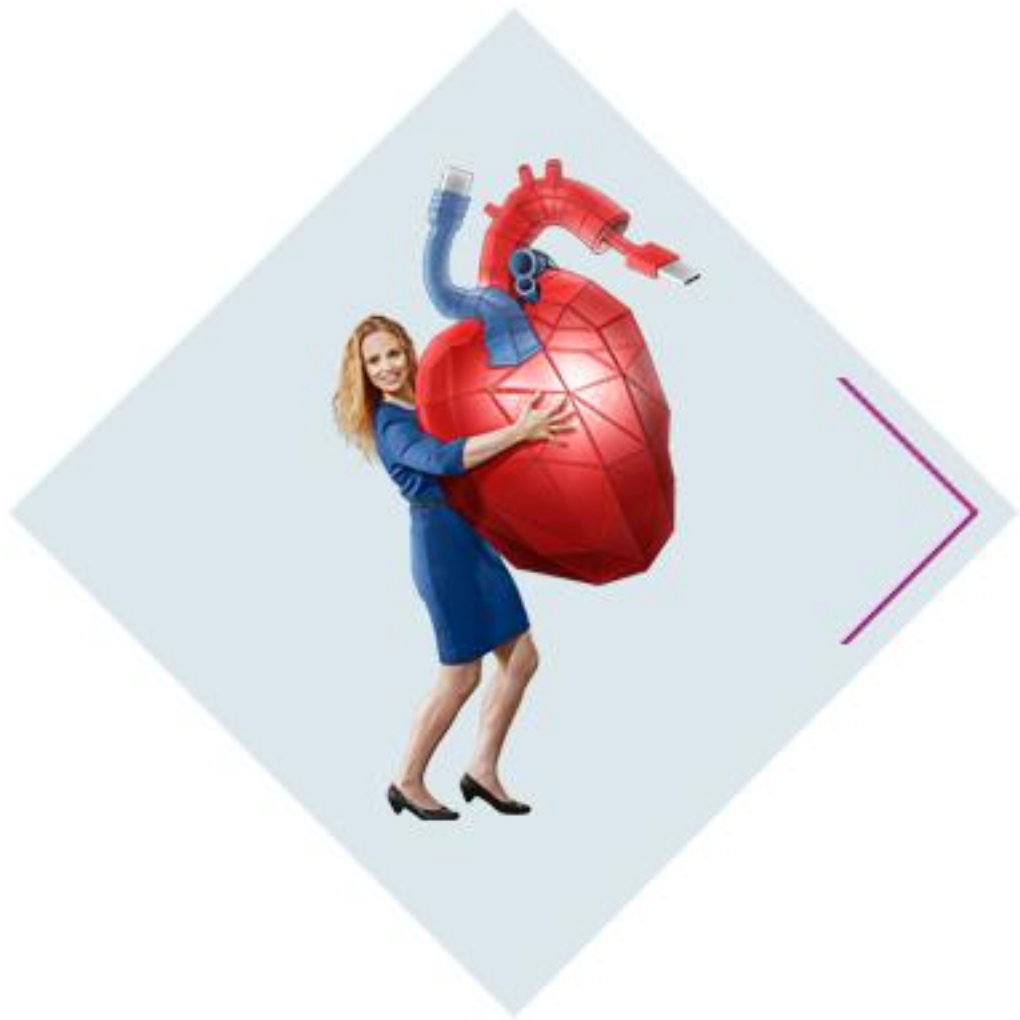
#### Sources

<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.moodyanalytics.com/articles/2023/rsa-and-diffie-hellman-cryptosystems-under-threat-sooner-than-previously-thought>



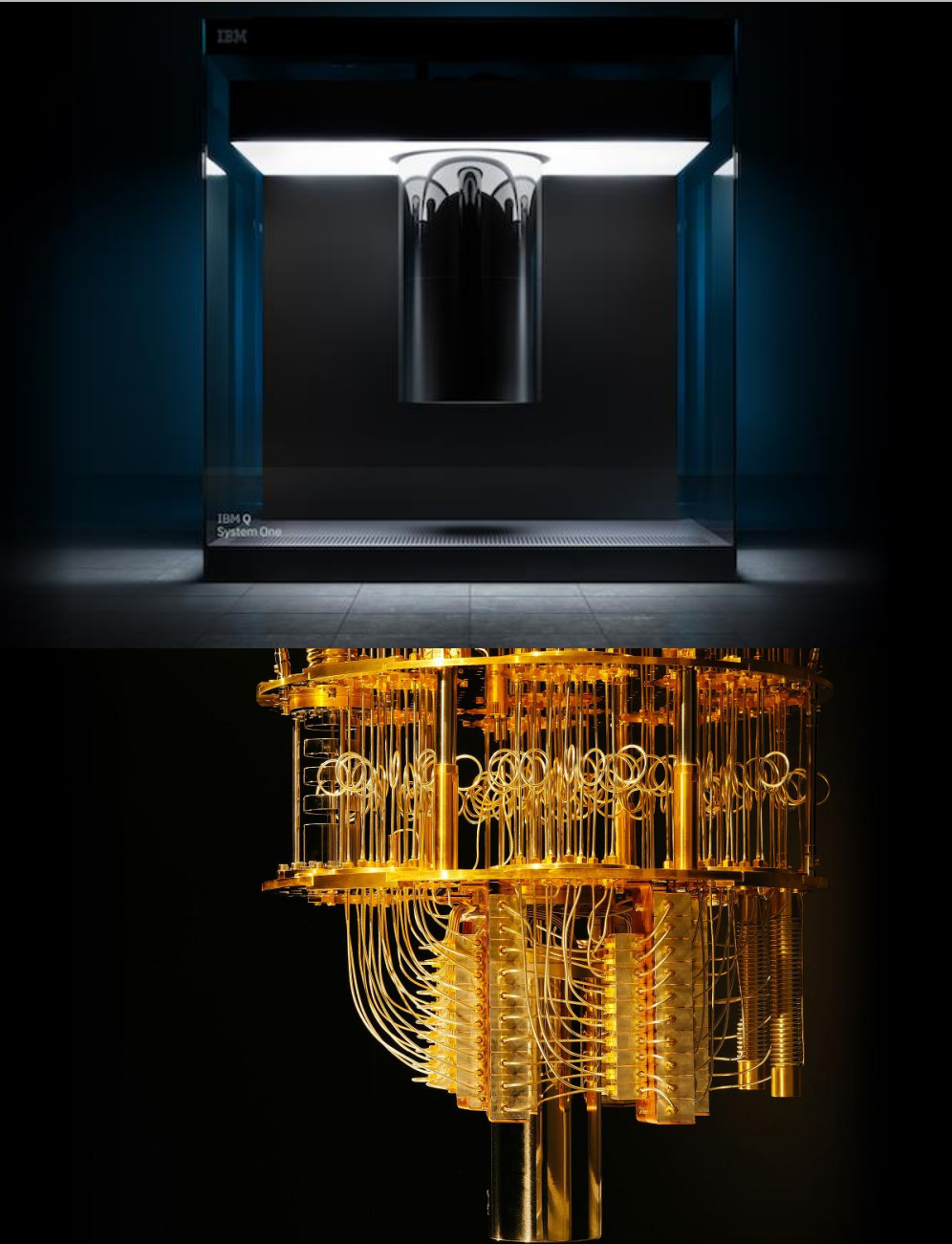
# Agenda

Quantum computers in theory

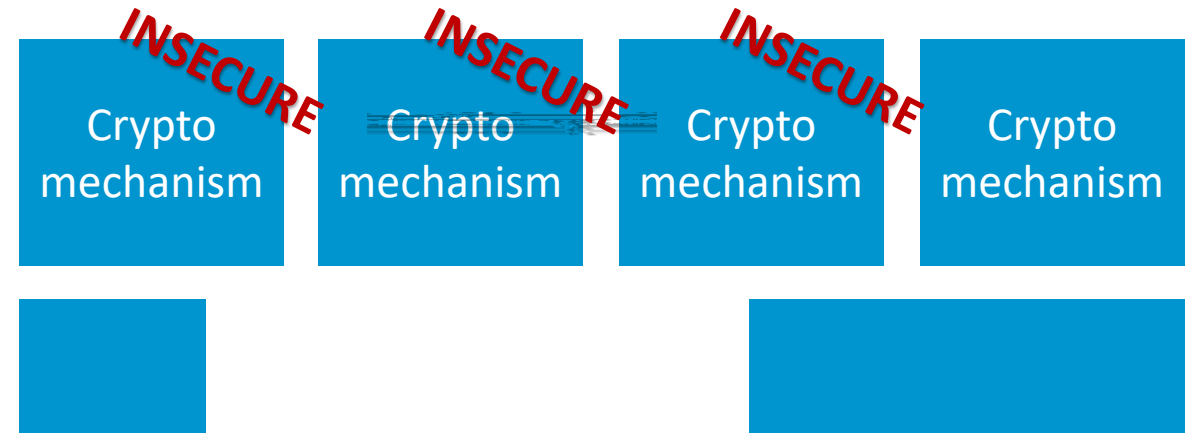
Quantum computers in practice

Crypto-apocalypse now?

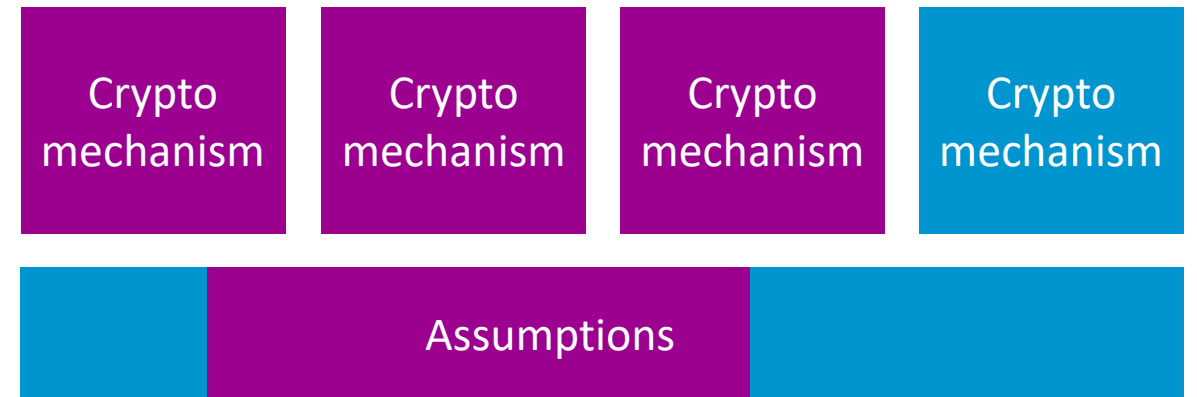
**Quantum-resistant cryptography**



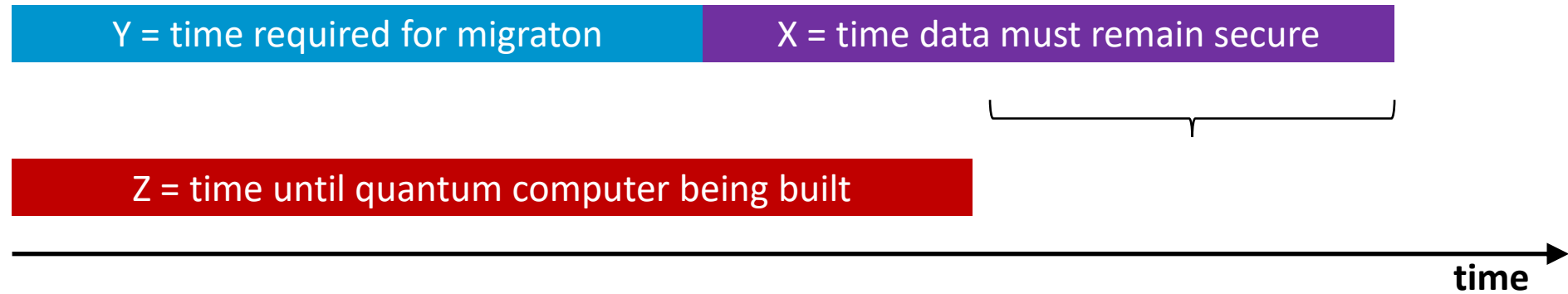
## MODERN PUBLIC-KEY CRYPTOGRAPHY



## QUANTUM RESISTANT CRYPTOGRAPHY



# Mosca's Theorem

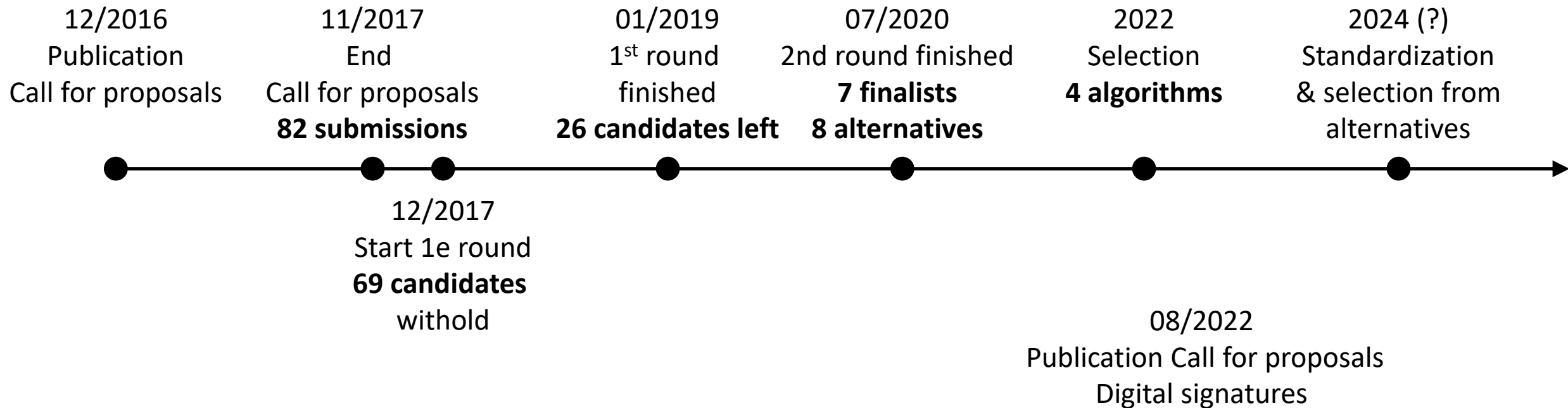


**if**  
**then**

**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)


## 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



The image shows a screenshot of a news article from the website Wired. At the top left, there is a menu icon (three horizontal lines) followed by the 'WIRED' logo in a bold, black, sans-serif font. To the right of the logo, the text 'SIGN IN' is visible, followed by a vertical line and a magnifying glass icon representing a search function. Below the header, the author's name 'DAN GOODIN, ARS TECHNICA' is displayed in white text on a black rectangular background. To the right of the author's name, the category 'SECURITY' and the date and time 'AUG 3, 2022 9:00 AM' are shown in a smaller, black, sans-serif font. The main title of the article is 'A New Attack Easily Knocked Out a Potential Encryption Algorithm', written in a large, bold, black, sans-serif font. Below the title, a short paragraph of text reads: 'SIKE was a contender for post-quantum-computing encryption. It took researchers an hour and a single PC to break it.'



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.

**Correction**  
Not the algorithm was cracked, but an implementation of it contained vulnerabilities



By Kevin Townsend  
February 21, 2023



## 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**





- **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**



## Hybrid encryption

*The quantum-safe algorithms that are currently being standardized are not yet as well researched as the "classical" methods*

*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*

## Cryptographic agility

*making cryptographic mechanisms as flexible as possible in order to be able to react to developments, implement upcoming recommendations and standards*

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



## ❖ **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 ...

❖ ...

”

**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

# Thanks for your attention

---

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

✉ [kristof.verslype@smals.be](mailto:kristof.verslype@smals.be)

☎ +32(0)2 7875376

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



[www.smals.be](http://www.smals.be)

[www.smalsresearch.be](http://www.smalsresearch.be)

[www.cryptov.net](http://www.cryptov.net)

DEVOXX™



- 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](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/>