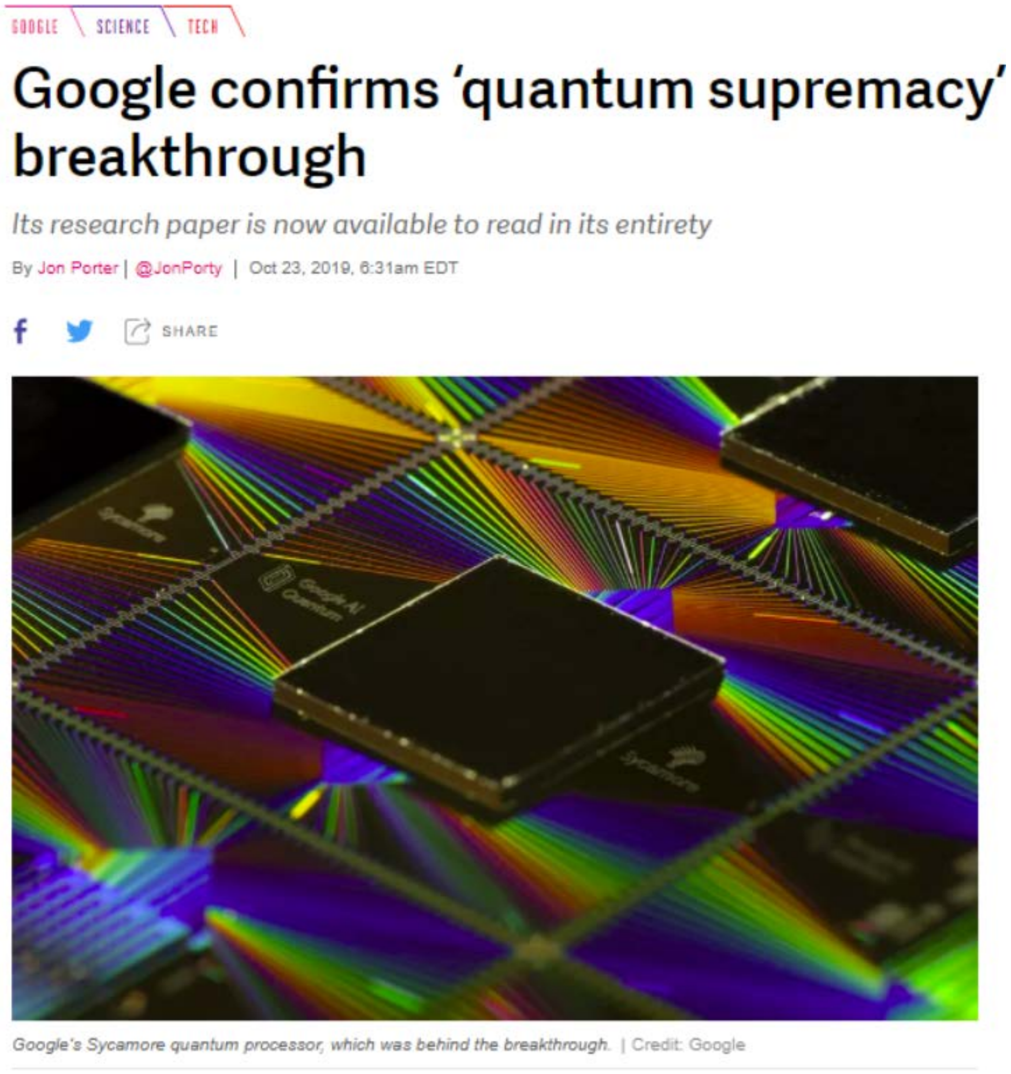
Quantum supremacy and Digital security

Simona Samardjiska
Digital Security Group – Radboud University

Quantum supremacy…

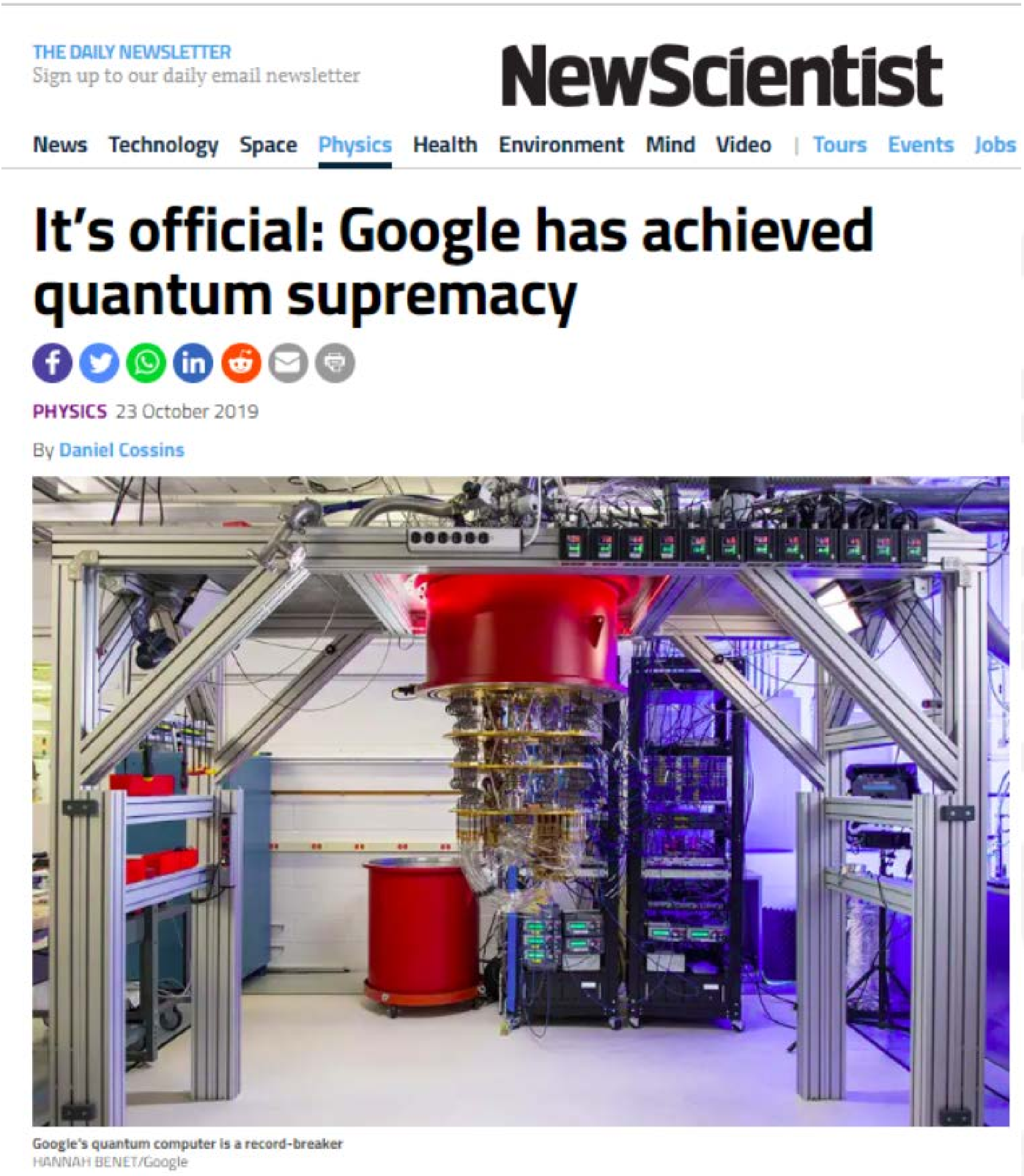


Google confirms ‘quantum supremacy’ breakthrough

Its research paper is now available to read in its entirety

By Jon Porter | @JonPorty | Oct 23, 2019, 6:31am EDT

Google's Sycamore quantum processor, which was behind the breakthrough. | Credit: Google



THE DAILY NEWSLETTER
Sign up to our daily email newsletter
NewScientist
News Technology Space Physics Health Environment Mind Video | Tours Events Jobs

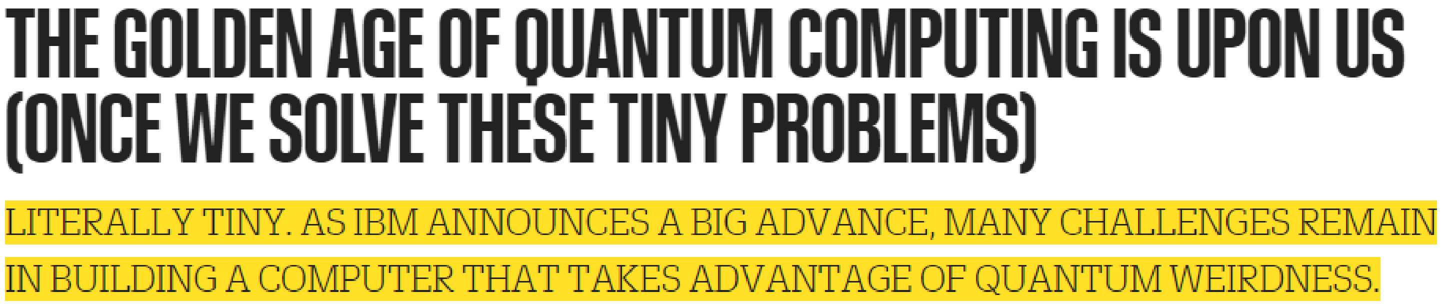
It’s official: Google has achieved quantum supremacy

PHYSICS 23 October 2019

By Daniel Cossins

Google’s quantum computer is a record-breaker
HANNAH BENET/Google

The last few years…



THE GOLDEN AGE OF QUANTUM COMPUTING IS UPON US (ONCE WE SOLVE THESE TINY PROBLEMS)

LITERALLY TINY. AS IBM ANNOUNCES A BIG ADVANCE, MANY CHALLENGES REMAIN IN BUILDING A COMPUTER THAT TAKES ADVANTAGE OF QUANTUM WEIRDNESS.

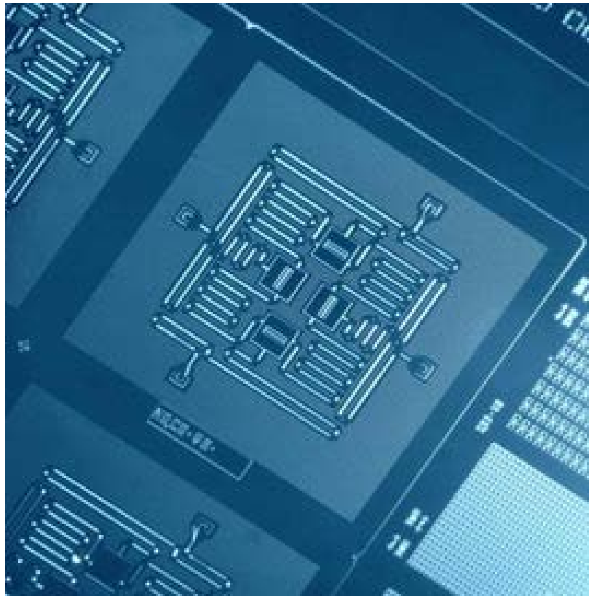
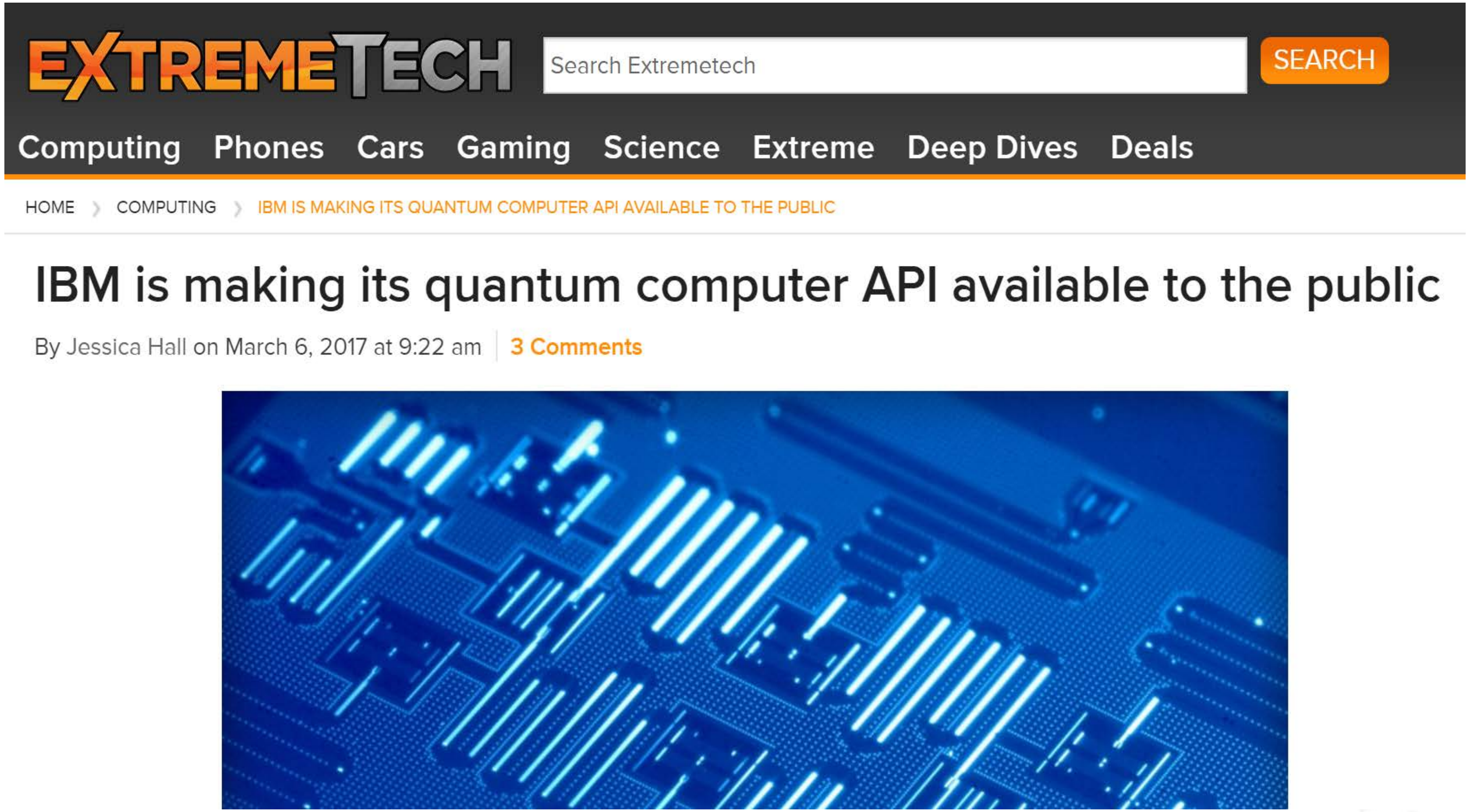


Photo: IBM Research

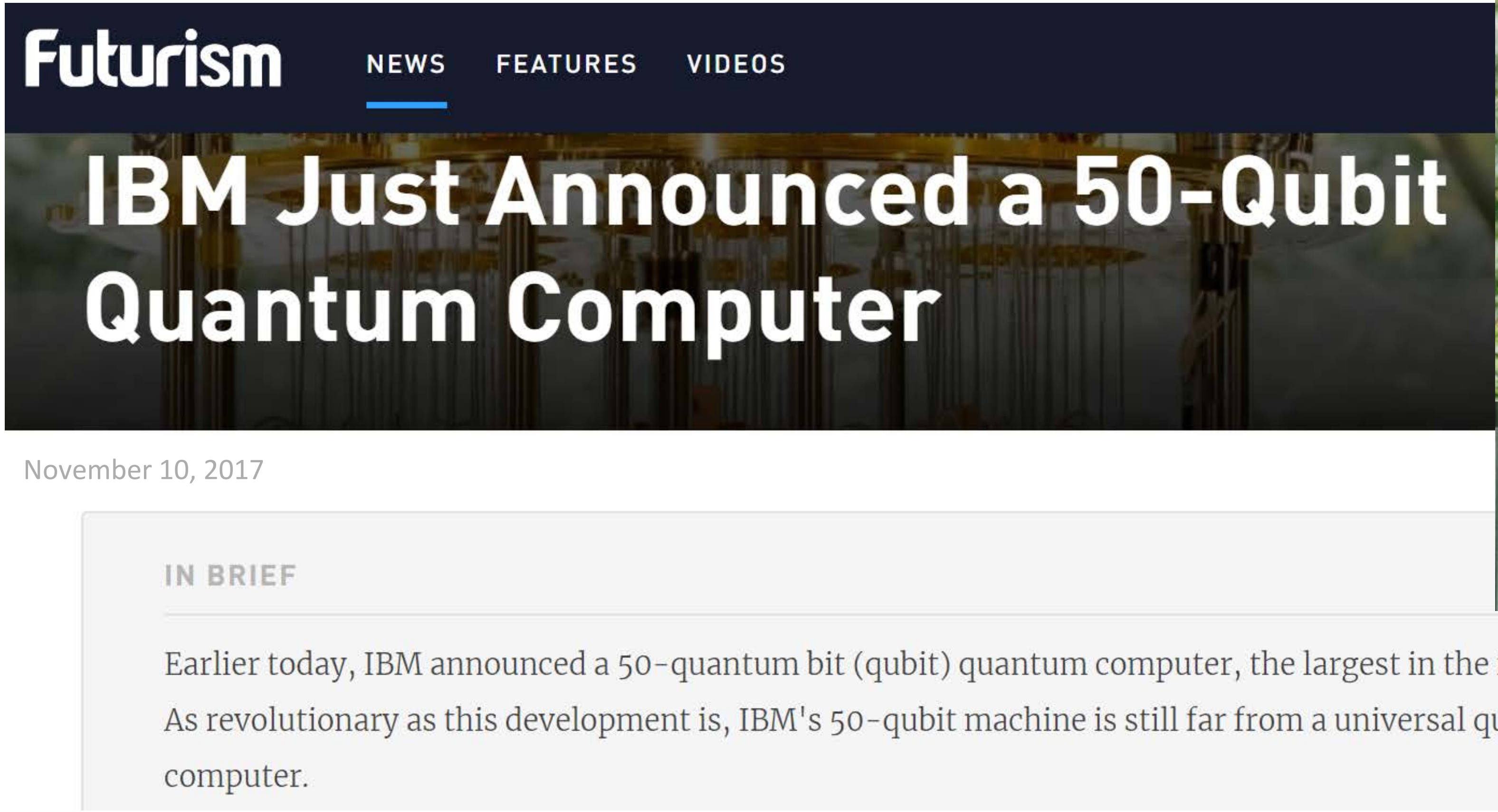
The last few years…



IBM is making its quantum computer API available to the public

By Jessica Hall on March 6, 2017 at 9:22 am | 3 Comments

The last few years…

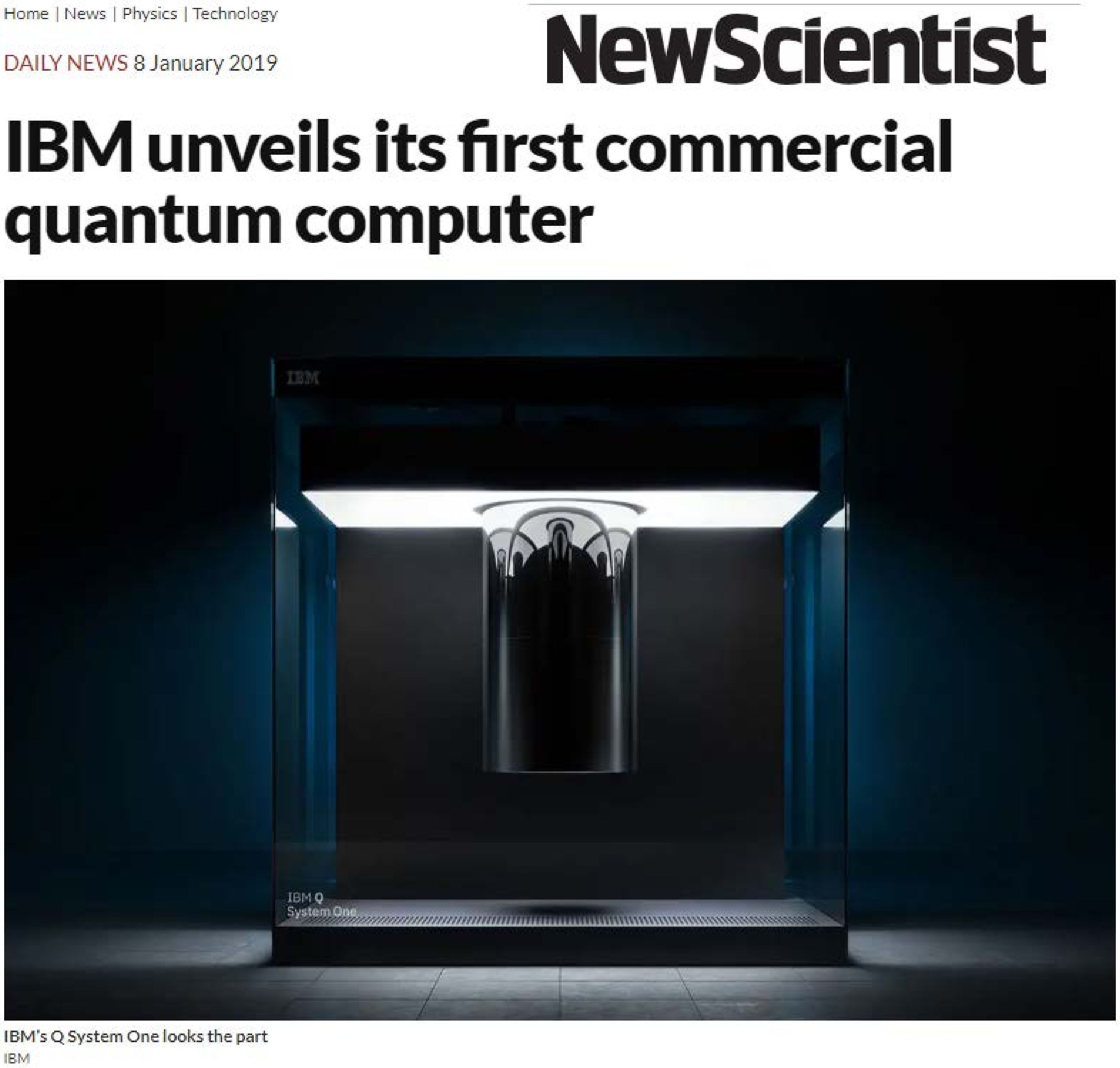


IBM Just Announced a 50-Qubit Quantum Computer

November 10, 2017

IN BRIEF

Earlier today, IBM announced a 50-quantum bit (qubit) quantum computer, the largest in the industry so far. As revolutionary as this development is, IBM's 50-qubit machine is still far from a universal quantum computer.



Home | News | Physics | Technology

DAILY NEWS 8 January 2019

NewScientist

IBM unveils its first commercial quantum computer

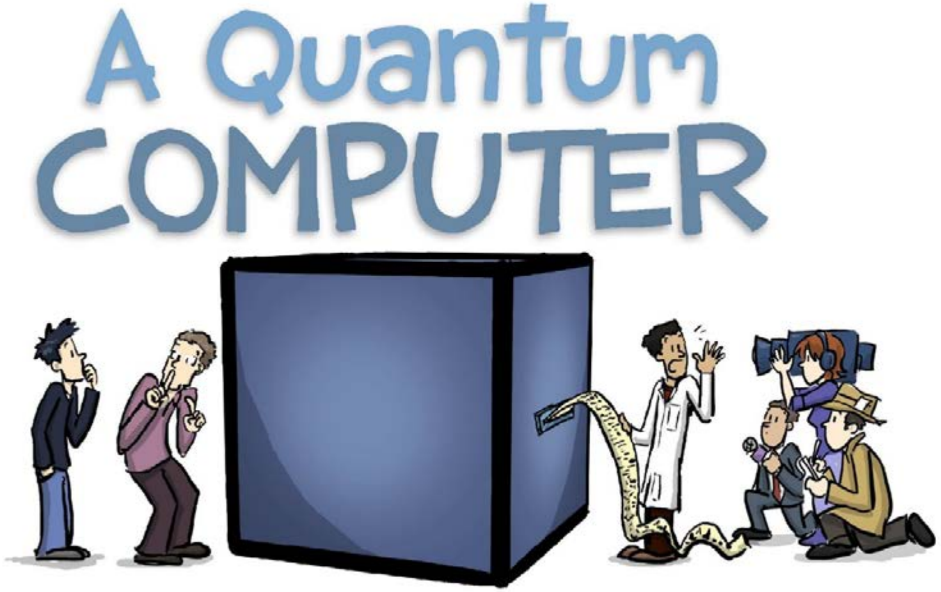
IBM's Q System One looks the part

IBM

What does Quantum supremacy even mean?

Showing experimentally that quantum computers are better than classical computers by performing a task that can not be simulated on a classical computer

What is



???

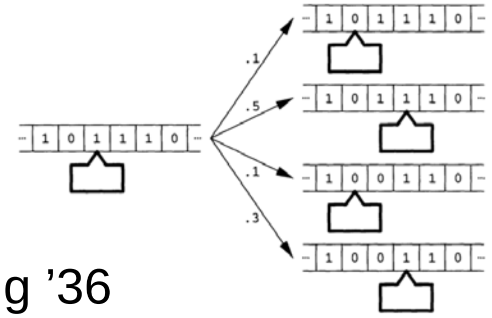
The origins…

Probabilistic Turing Machine

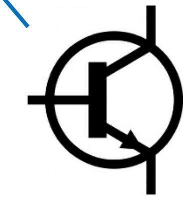
Any randomized algorithmic process can be simulated efficiently using a Probabilistic Turing machine

Turing '36

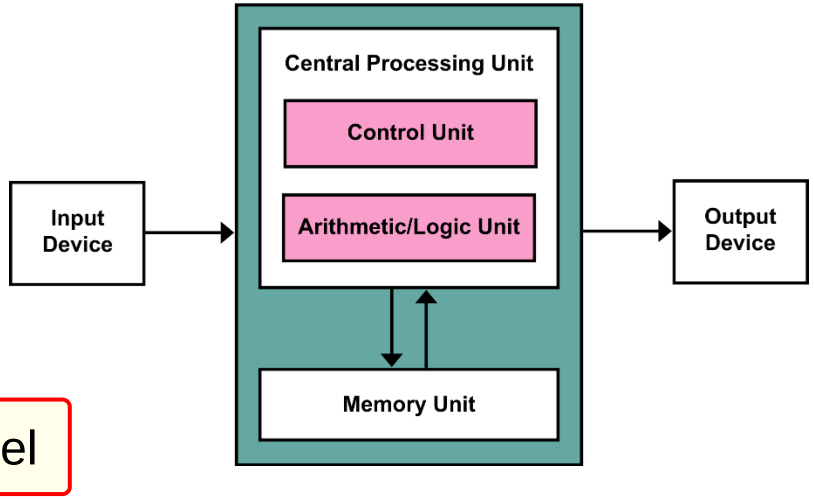
Gill '77



The classical computer


Transistors

Hardware


Central Processing Unit

Control Unit

Arithmetic/Logic Unit

Memory Unit

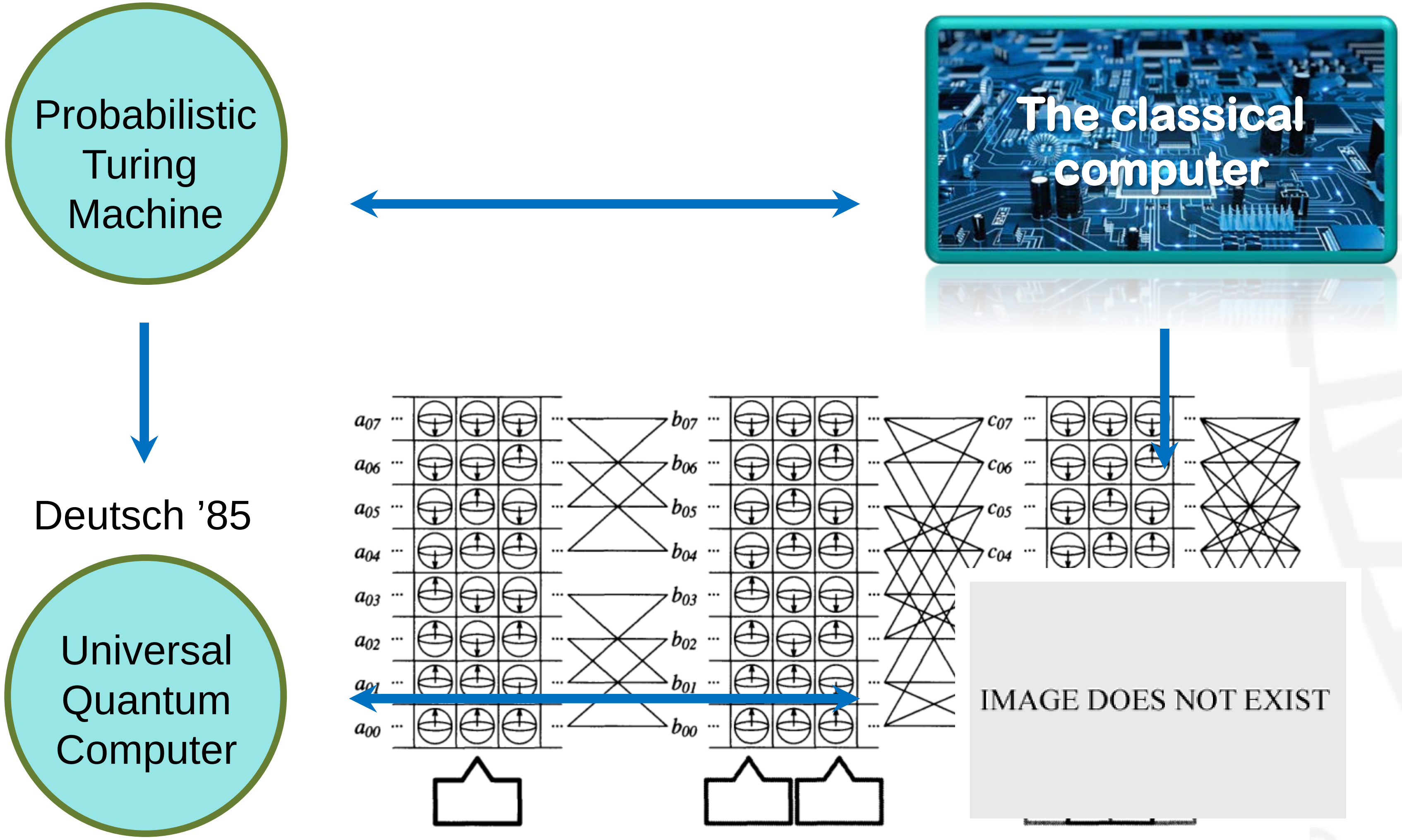
Input Device

Output Device

Theoretical model

von Neumann architecture

The origins…



Probabilistic Turing Machine

The classical computer

Deutsch ’85

Universal Quantum Computer

IMAGE DOES NOT EXIST

The qubit…

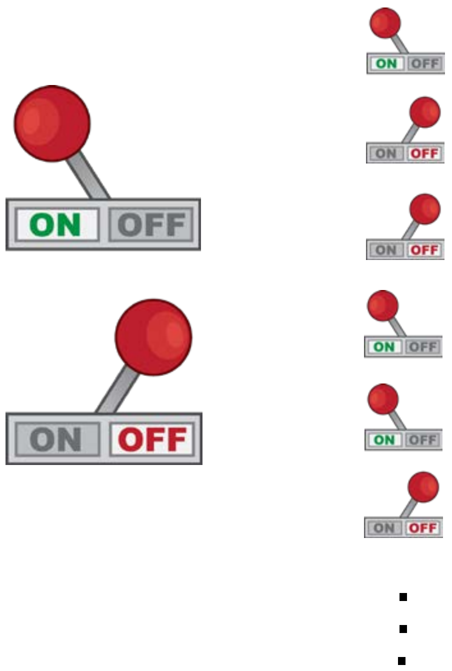
Bit – the unit of classical information

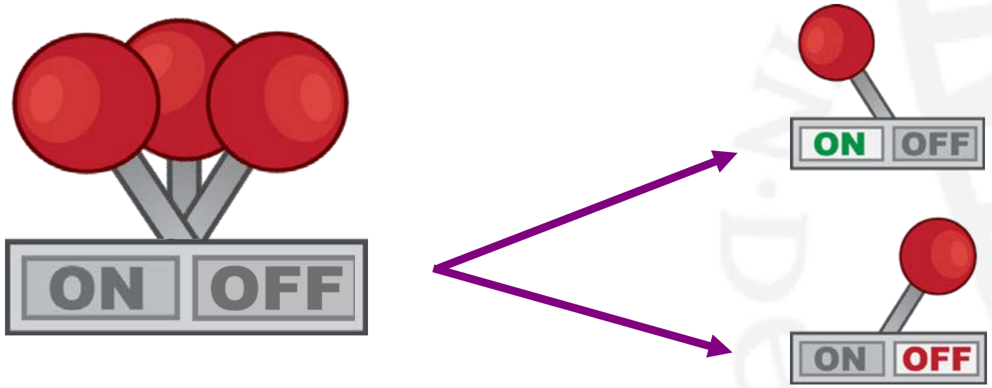
0 or 1

vs

Qubit – the unit of quantum information

A combination of 0 and 1





Measurement

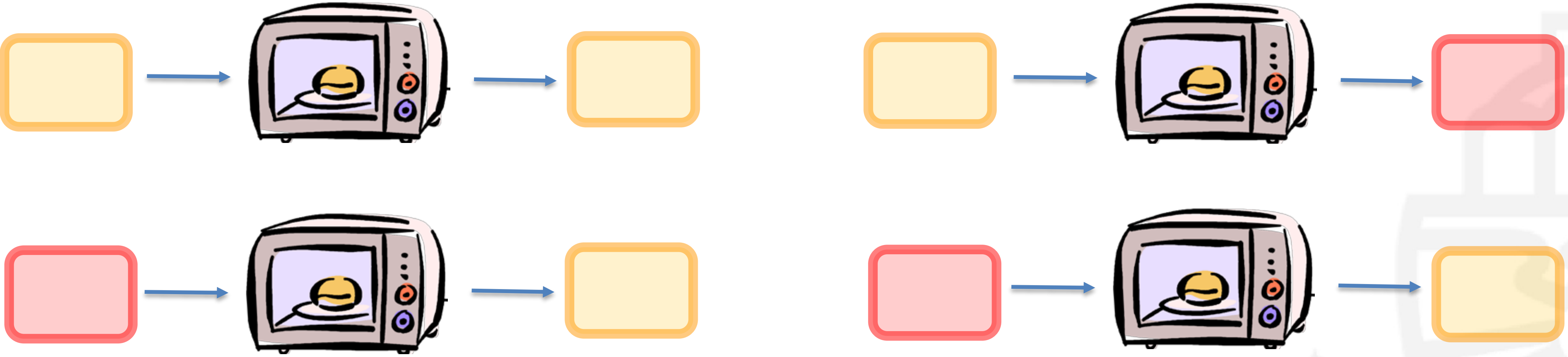
What can we do using quantum computers?

- Everything that a classical computer can do!
- Can we do more?

Deutsch-Jozsa Algorithm

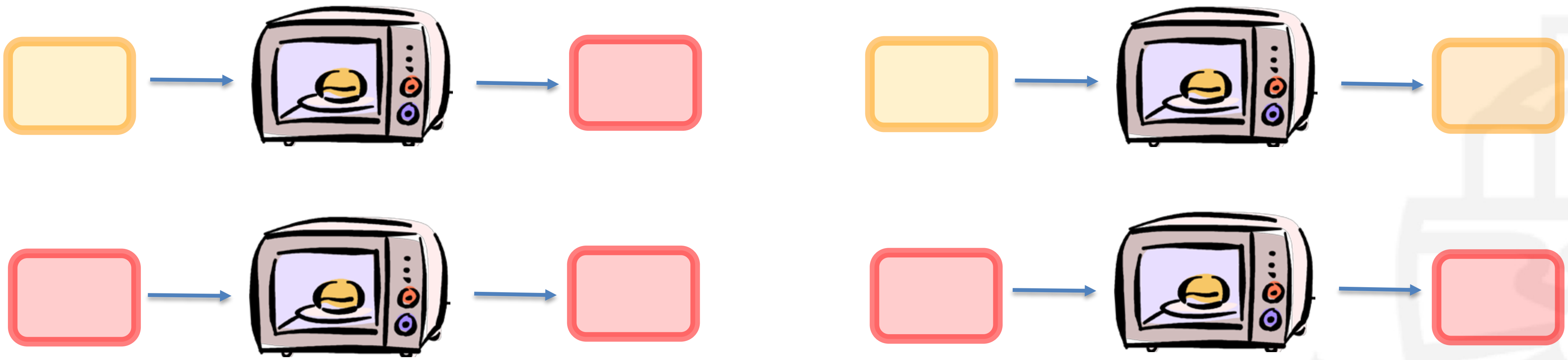
- Decide whether a function is constant or balanced

Deutsch-Jozsa Algorithm

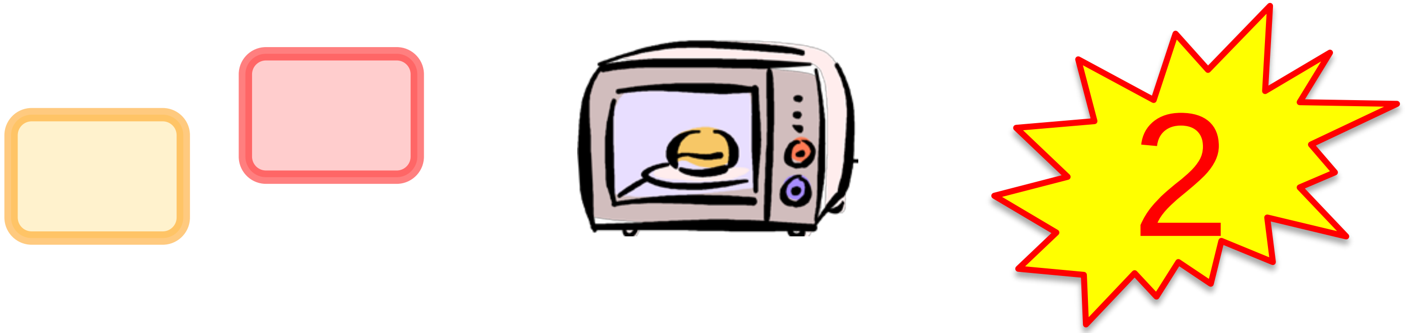


IN·DEI·NOMINE

Deutsch-Jozsa Algorithm

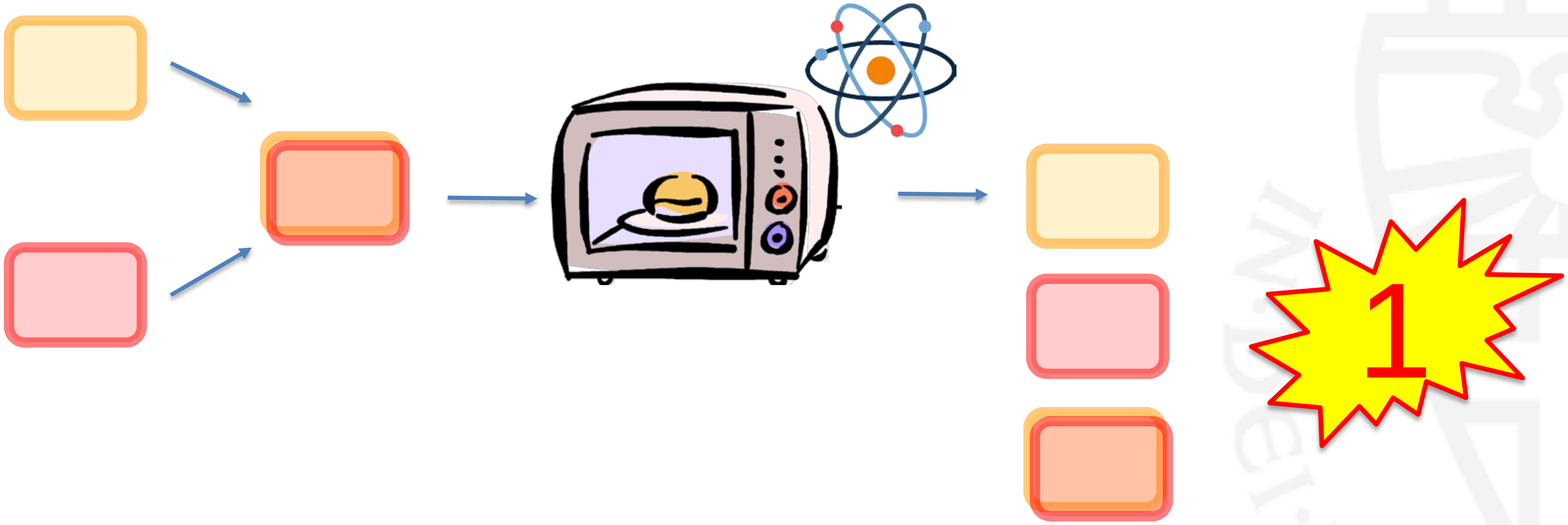


How many times do we need to use the oven in order to find out what it does?

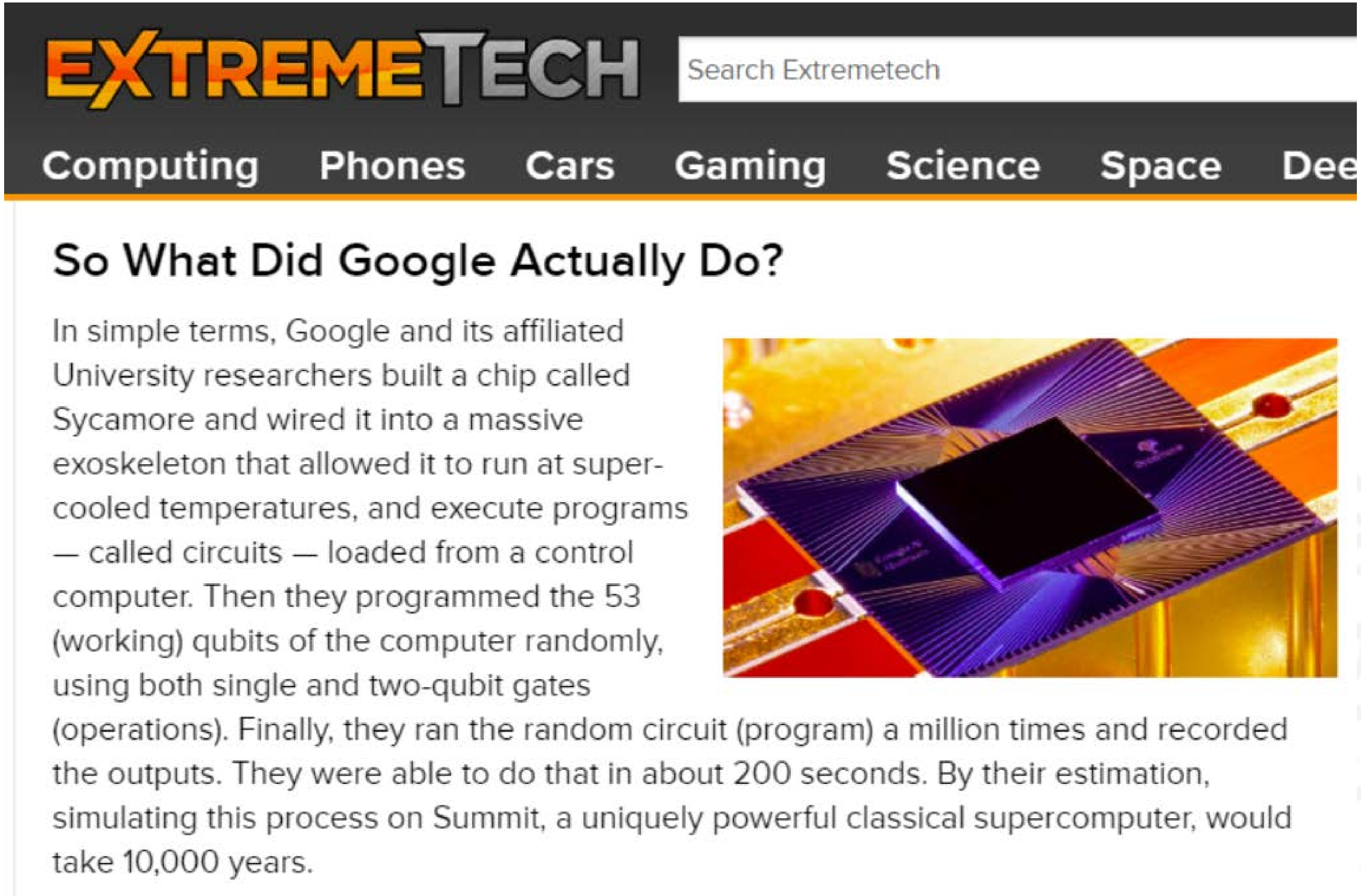


Deutsch-Jozsa Algorithm

- **If we had a quantum oven….**



How many times do we need to use the oven in order to find out what it does?



So What Did Google Actually Do?

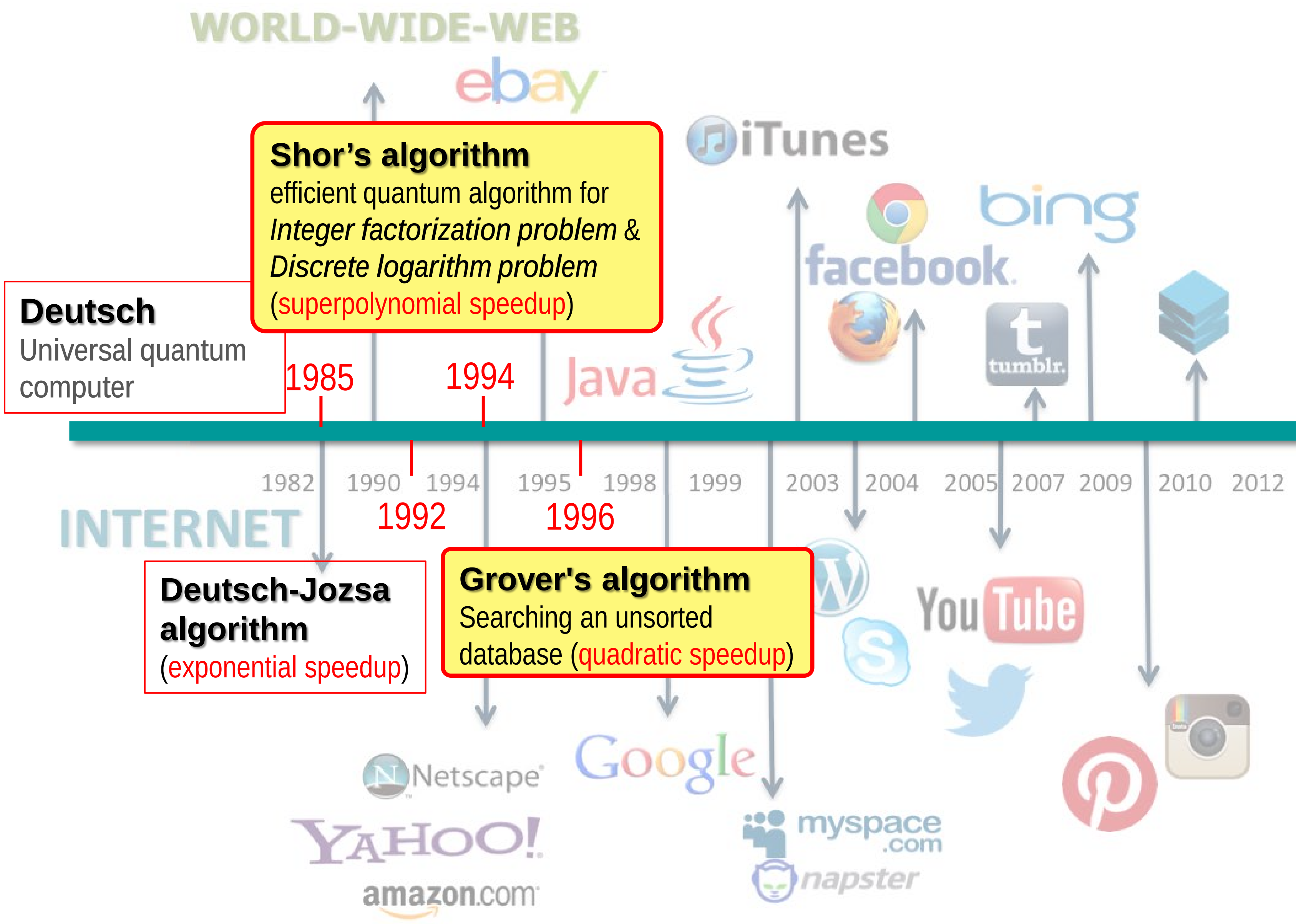
In simple terms, Google and its affiliated University researchers built a chip called Sycamore and wired it into a massive exoskeleton that allowed it to run at super-cooled temperatures, and execute programs — called circuits — loaded from a control computer. Then they programmed the 53 (working) qubits of the computer randomly, using both single and two-qubit gates (operations). Finally, they ran the random circuit (program) a million times and recorded the outputs. They were able to do that in about 200 seconds. By their estimation, simulating this process on Summit, a uniquely powerful classical supercomputer, would take 10,000 years.

More useful stuff we can do using quantum computers?

- **Simulations of systems**
  - in chemistry, physics, biology, medicine, finance
- **Searching for the best solution of a problem**
- **Optimization**
- **Machine learning and AI**
- …
- The sky is the limit ☺

IN·DEI·NOMINE

What does quantum supremacy mean to us…



Deutsch
Universal quantum computer

1985

Shor's algorithm
efficient quantum algorithm for *Integer factorization problem* & *Discrete logarithm problem* (superpolynomial speedup)

1994

1992

Deutsch-Jozsa algorithm
(exponential speedup)

1996

Grover's algorithm
Searching an unsorted database (quadratic speedup)

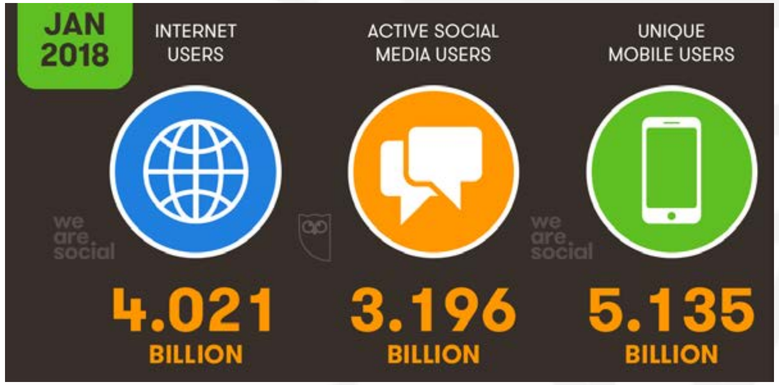
THE DAILY NEWSLETTER
Sign up to our daily email newsletter

NewScientist

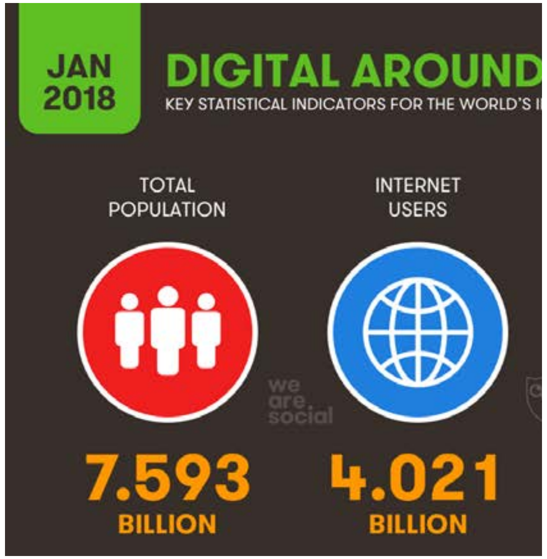
News | Technology | Space | Physics | Health | Environment | Mind | Video | Tours | Events | Jobs

It's official: Google has achieved quantum supremacy

October, 2019



How do we make this world secure?



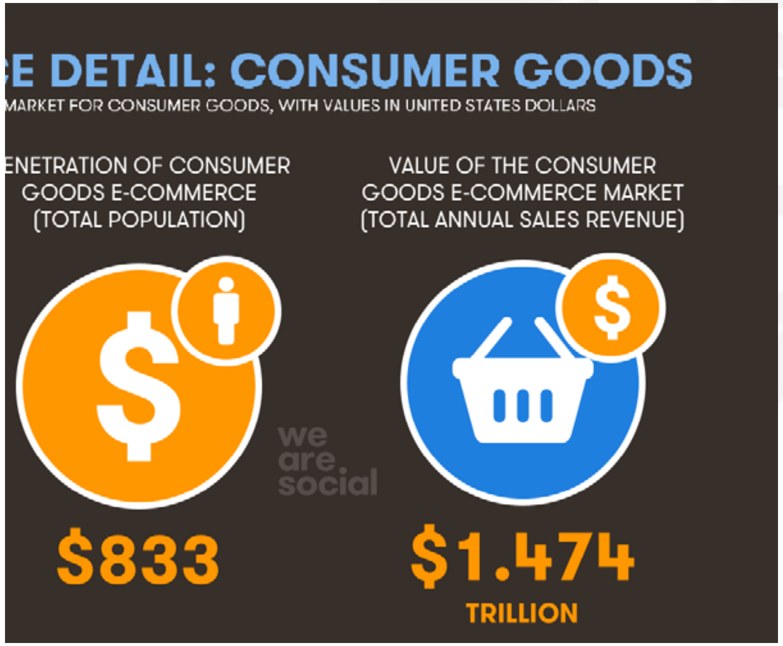
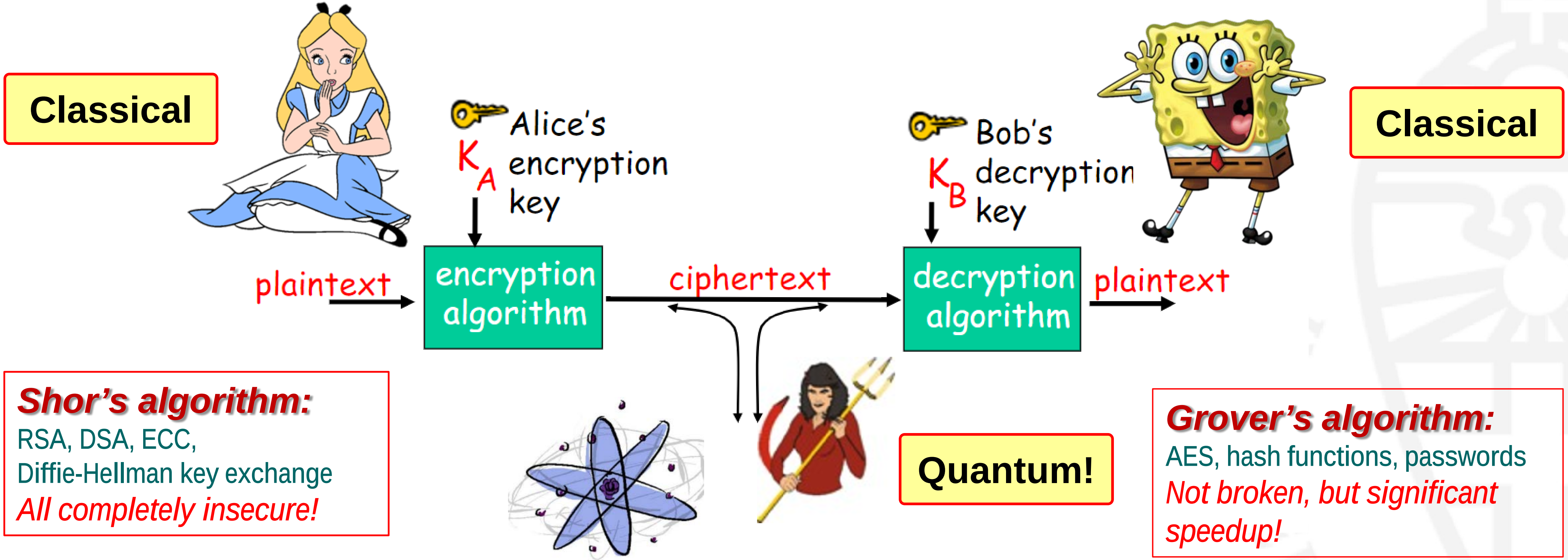


Image source: www.bandicoot.co.uk

So what happens when we have big enough quantum computers ?



Shor's algorithm:

RSA, DSA, ECC,
Diffie-Hellman key exchange

All completely insecure!

Grover's algorithm:

AES, hash functions, passwords

Not broken, but significant speedup!

Factor a 2048 bit number: < 1 second
(classically ~ 150,000 years)

Break a 8 character password of lowercase letters: < 5 days
(classically ~ 4,13 years)

Quantum computers vs Digital security

IN·DEI·NOMINE

Solution?

Post Quantum Cryptography!

Classical Cryptosystems believed to be secure against quantum computer attacks

NIST PQ standardization process:

- *NOT a competition*
- *82 submissions*
- Radboud involved in 8 ! (all in Round 2)

Timeline:

- *Fall 2016 – call for proposals*
- *November 2017 – deadline for submissions*
- *January 2019 – second round candidates*
- *2-4 years from now – results*
- *2 years later – Draft standard ready*
- *Deployment ?*

Digital Security Group – Radboud University involved in 8 Post Quantum Crypto candidates

KEMs

- **Classic McEliece**
  - Code-based

Lattice based

- **CRYSTALS-KYBER**
- **NTRU-HRSS-KEM**
- **New Hope**
  - Implemented and tested by Google

- **SIKE**
  - Isogeny-based

Signatures

- **CRYSTALS-DILITHIUM**
  - Lattice based

- **SPHINCS+**
  - Hash based

- **MQDSS**
  - [Chen, Hülsing, Rijneveld, S, Schwabe, 16]
  - NIST candidate
  - **First provably secure MQ signature scheme**
  - Hard problem: Solving systems of quadratic equations (MQ problem)

Some final words

If computers that you build are quantum,
Then spies everywhere will all want 'em.
Our codes will all fail,
And they'll read our email,
Till we get crypto that's quantum,
and daunt 'em.
Jennifer and Peter Shor

To read our E-mail, how mean
of the spies and their quantum
machine;
be comforted though,
they do not yet know
how to factorize twelve or fifteen.
Volker Strassen

Thank you for listening!

?