Quantum computer: What, Why, When?

János Asbóth[1,2]

1: Budapest University of Technology and Economics,
Dept. of Theoretical Physics;

2: Wigner Physics Research Centre,
Dept. of Quantum Optics and Quantum Information

CNUE Futurology Forum Budapest, 2020. September 14.

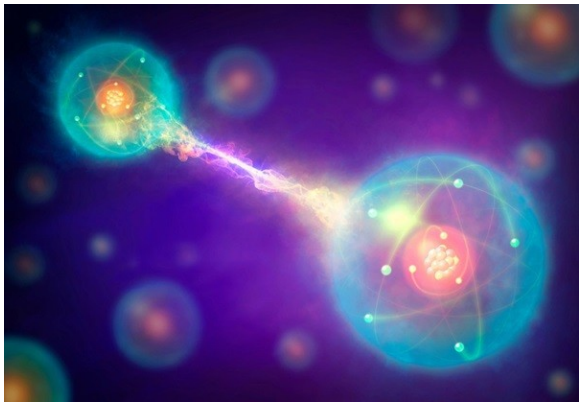
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL

AZ INNOVÁCIÓ LENDÜLETE

What is a quantum computer?

A machine using “quantum weirdness” for computation
- superposition, entanglement

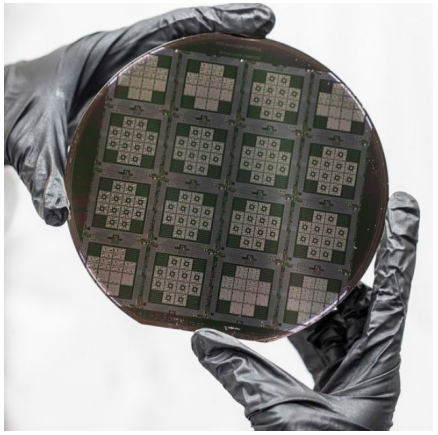


What is it good for?

Some exponentially hard problems
- Simulating molecular reactions
  (new medicine, better fertilizer)
- Breaking encryption (RSA)
- ??

When will I have one?

Early phase of research & development
- Different hardware approaches
- Best quantum chip has 53 bits (need ~1 million)
- IBM quantum computer accessible online

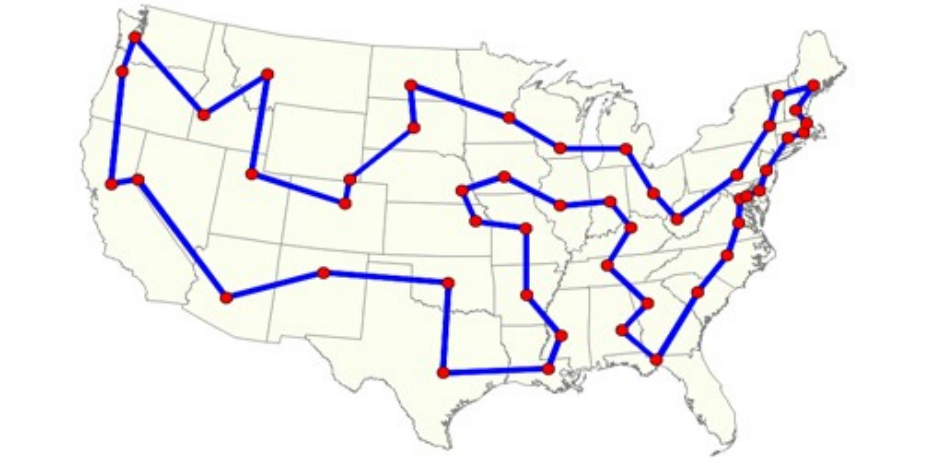


Hungarian research in quantum technology:
wigner.mta.hu/quantumtechnology

HUNQUTECH

There are exponentially hard problems, where having a faster computer does not help much

Traveling salesman: what is the shortest path passing through all cities?



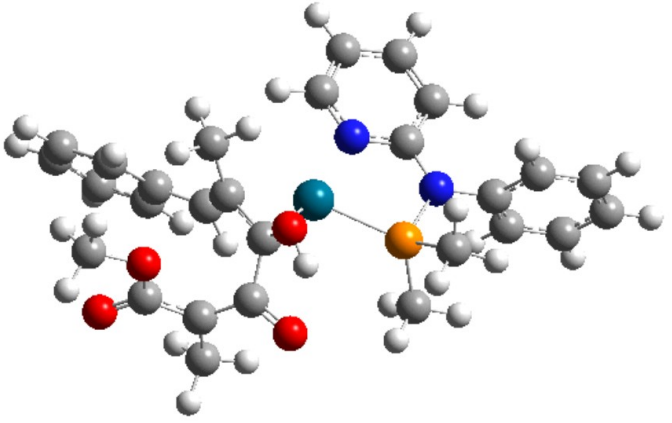
perfect solution:
2x computing power → +1 city

Prime factorization:
Big number, what are its prime divisors?

502 560 280 658 509 = 15 485 863 * 32 452 843

2x computing power → +1 digit

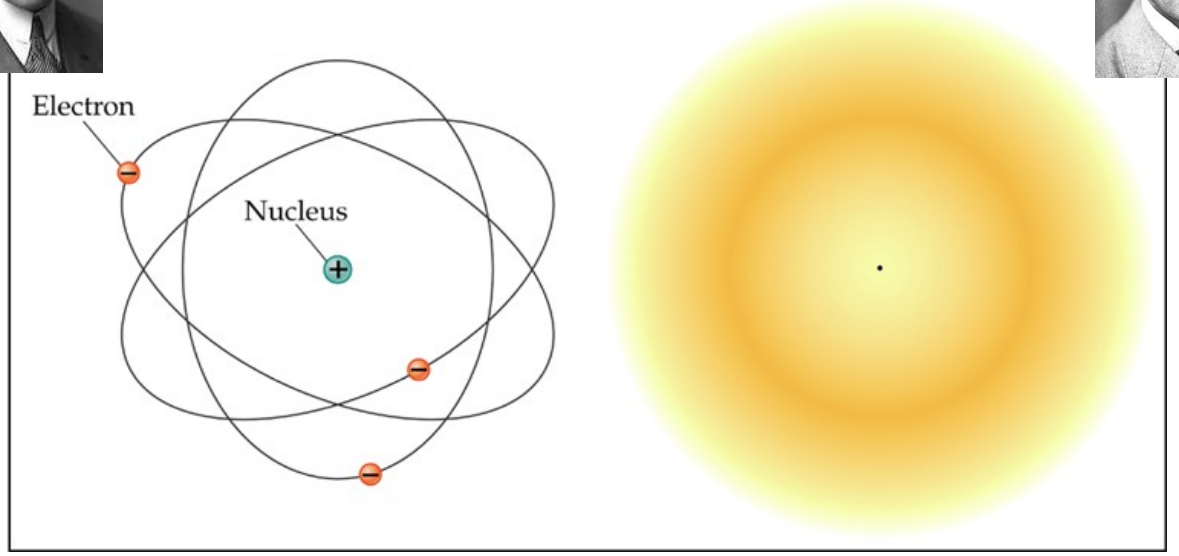
Precise modeling of chemical reactions

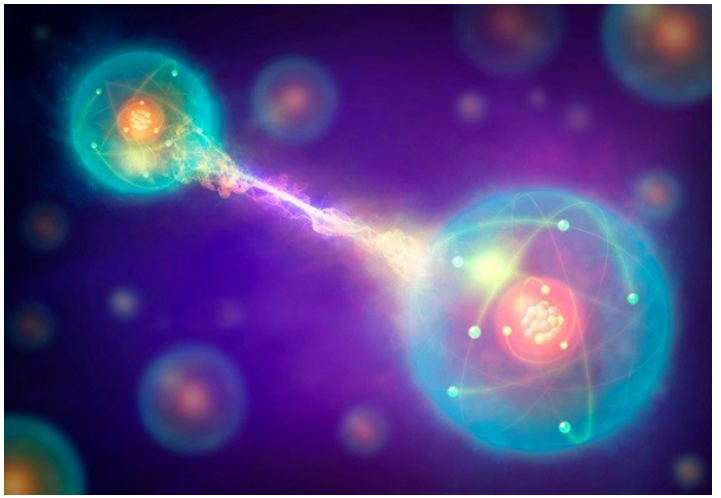


2x memory → +1 electron orbital

Precise modeling of chemical reactions is hard because of quantum weirdness: superposition, entanglement

Bohr 1913 → Schrödinger 1925





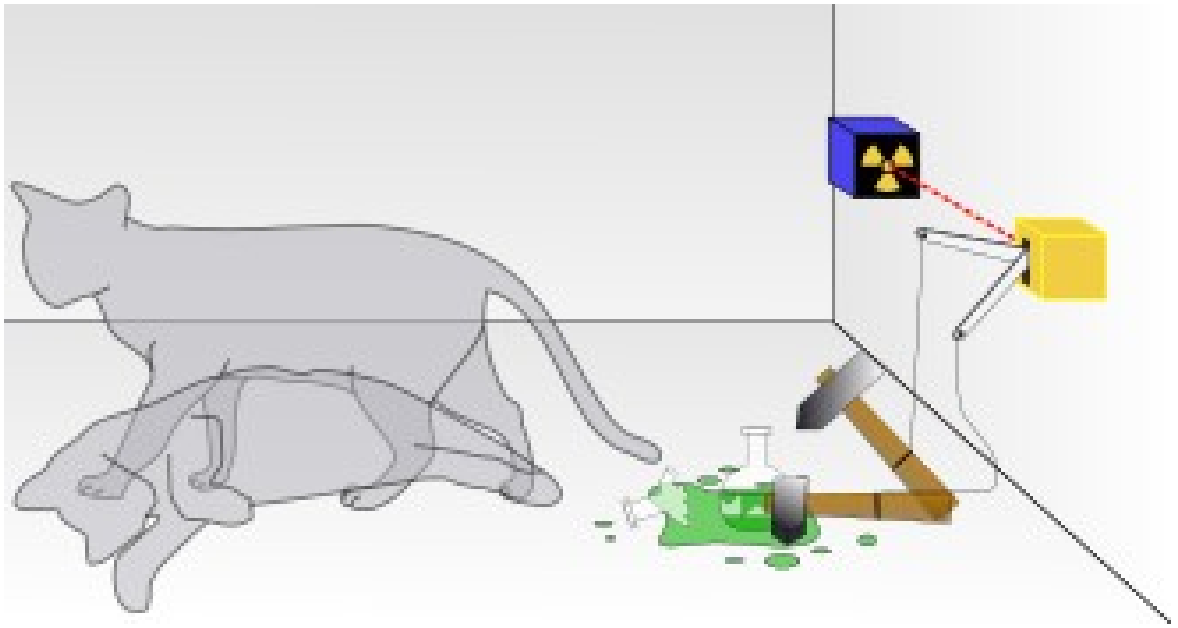
electron “in several places at once” – superposition

Needed to account for experiments

more electrons → superposition state of A depends on state of B = entanglement

→ exponential resources used → can find efficient reaction pathway

Quantum paradox 1:
Superposition of dead and alive cat - What would it mean?



1935: writing letters to Einstein,
"verschränkung" → entanglement

1933: for the foundations of quantum mechanics (Schrödinger's equation)

1935: Schrödinger's cat

[E. Schrödinger, "Die gegenwärtige Situation in der Quantenmechanik", Naturwissenschaften 23: pp.807-812; 823-828; 844-849 (1935)]

Quantum paradox 2:
Two entangled particles “stay in instant contact?”

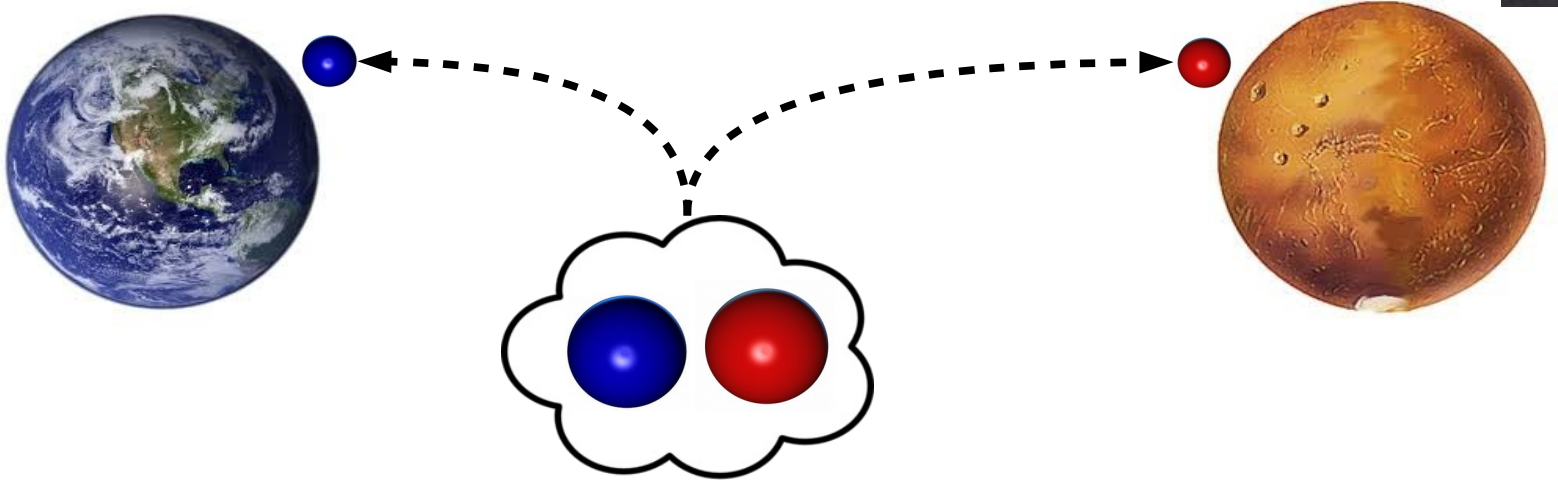
MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

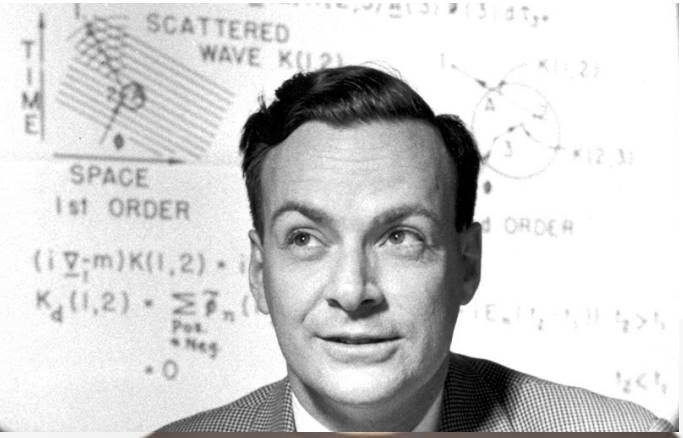
(Received March 25, 1935)

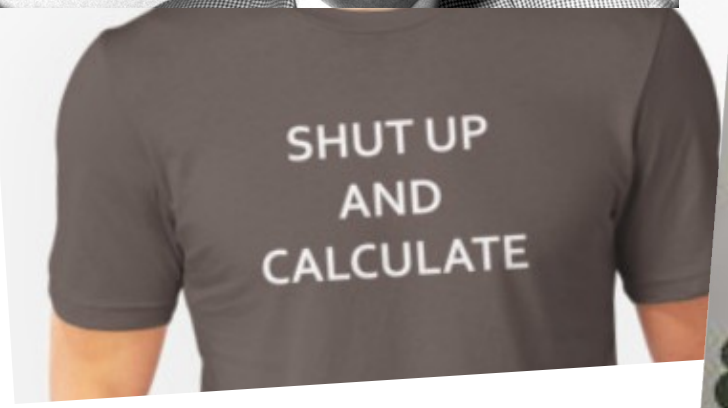
1. Prepare a pair of particles, using quantum tricks, Send A to Earth, B to Mars
2. Measuring A on Earth → instant effect on B on Mars
3. This conflicts with locality
   → quantum mechanics is missing something



1935- Despite paradoxes, quantum mechanics is the foundation of modern science and technology

R. Feynman: Quantum electrodynamics, 1965

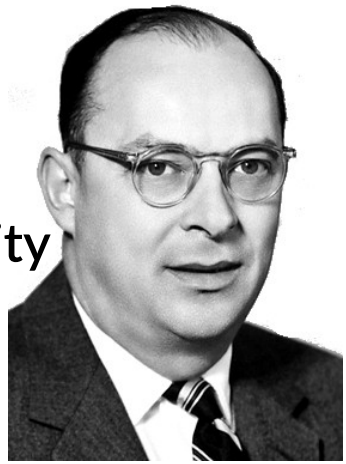


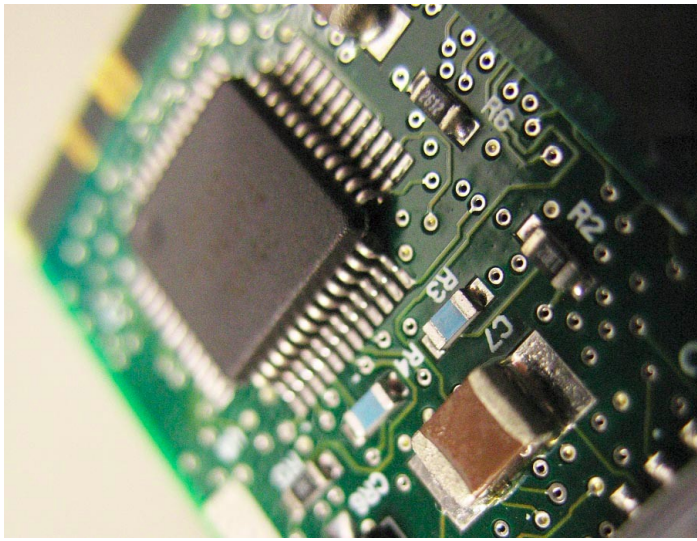


J. Bardeen

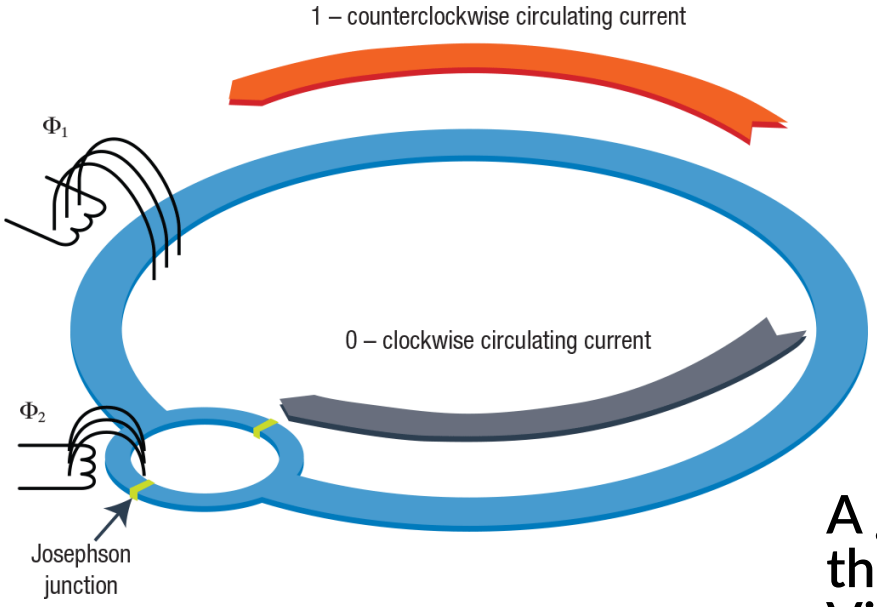
Transistor 1956

Theory of Superconductivity 1972



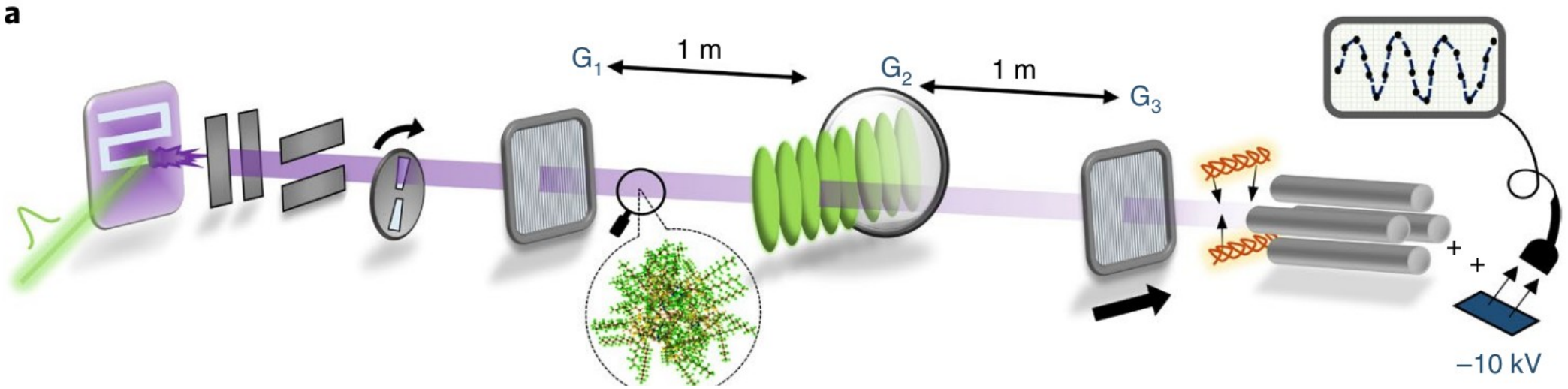


Since 1990's we can test "quantum paradoxes" directly, in the lab. Superposition...

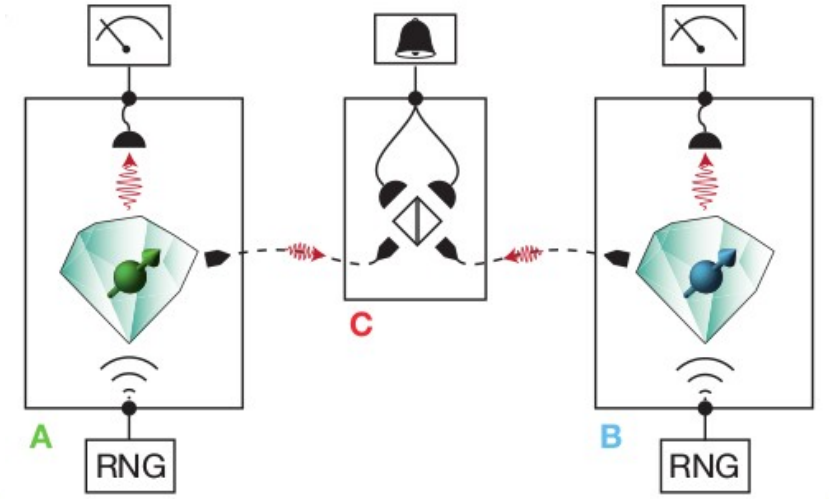


Superconducting ring carries current clockwise and counterclockwise "at the same time" [Mooij, Delft, 2001]

A giant molecules of 2000 atoms passes through two slits at the same time [Arndt, Vienna, 2019]

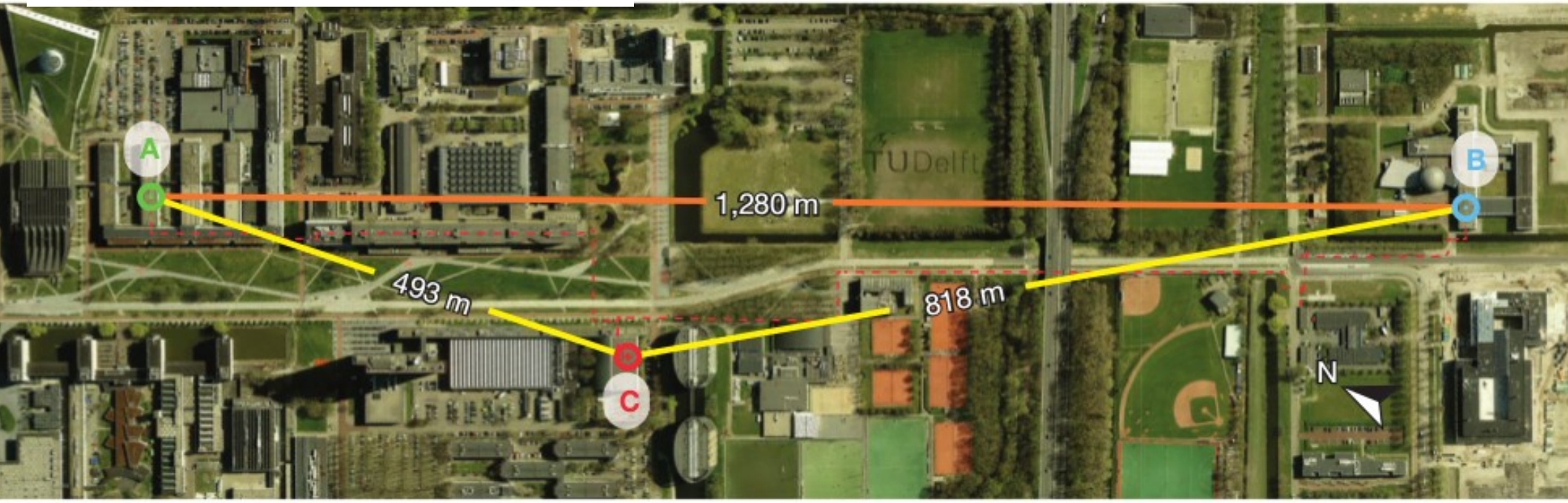


… and entanglement: “spooky action at a distance” exists!

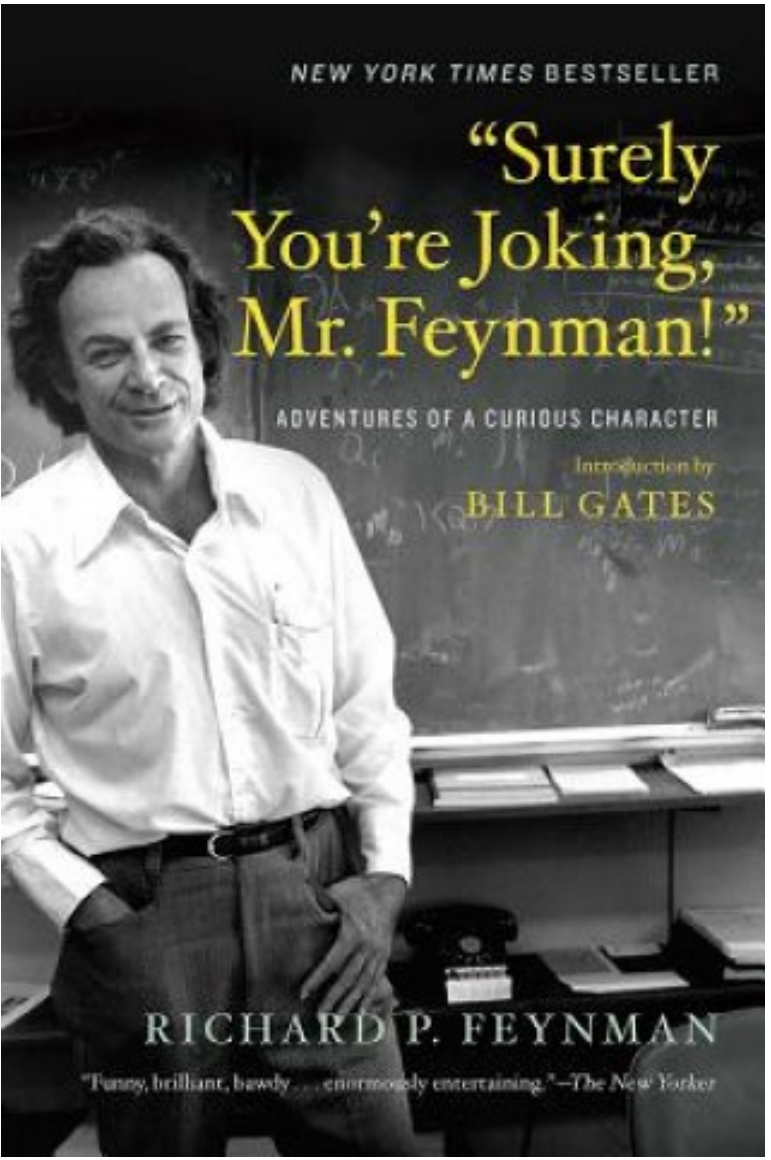


2015, TU Delft:
Long-range entanglement
using photons and defects in diamond

[Hensen et al, Nature (2015):
Experimental loophole-free violation of a Bell inequality using entangled electron spins separated by 1.3 km.]



Feynman, 1981: Since these quantum chemistry calculations are so hard, we need a quantum computer



. . trying to find a computer simulation of physics seems to me to be an excellent program to follow out. . . . the real use of it would be with quantum mechanics. . . .
if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.

Quantum simulator or digital computer?

What does a quantum bit mean?

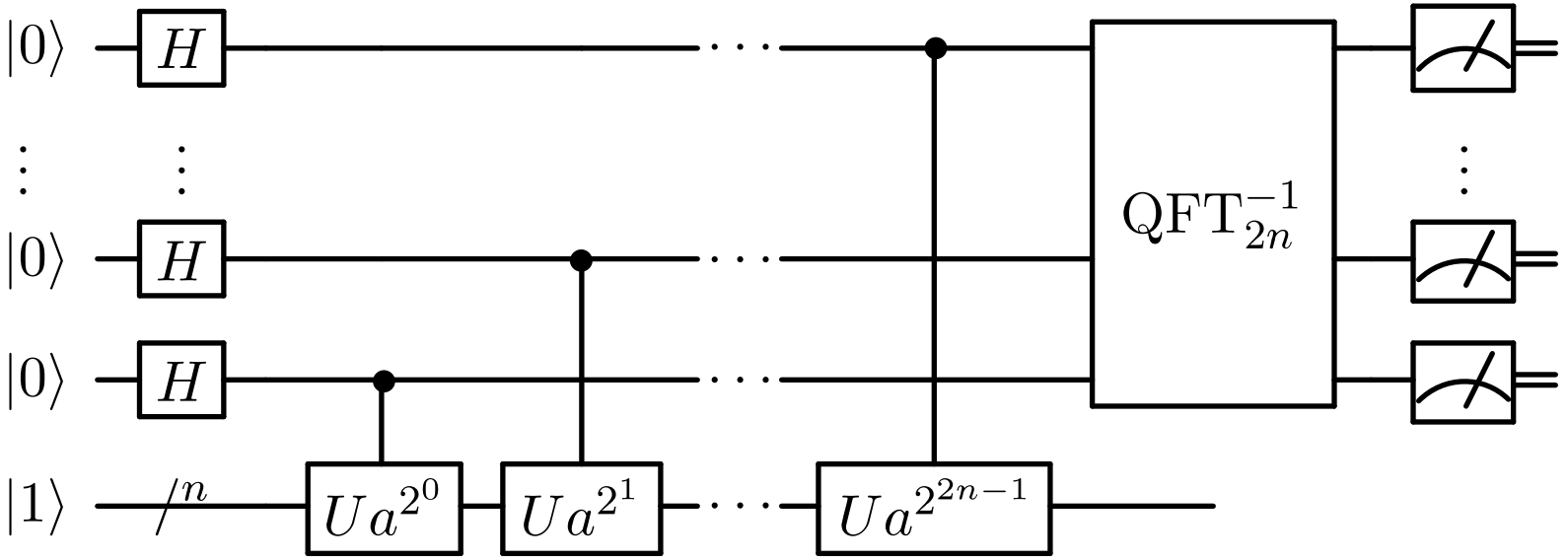
What does a program look like?

How to build the hardware?

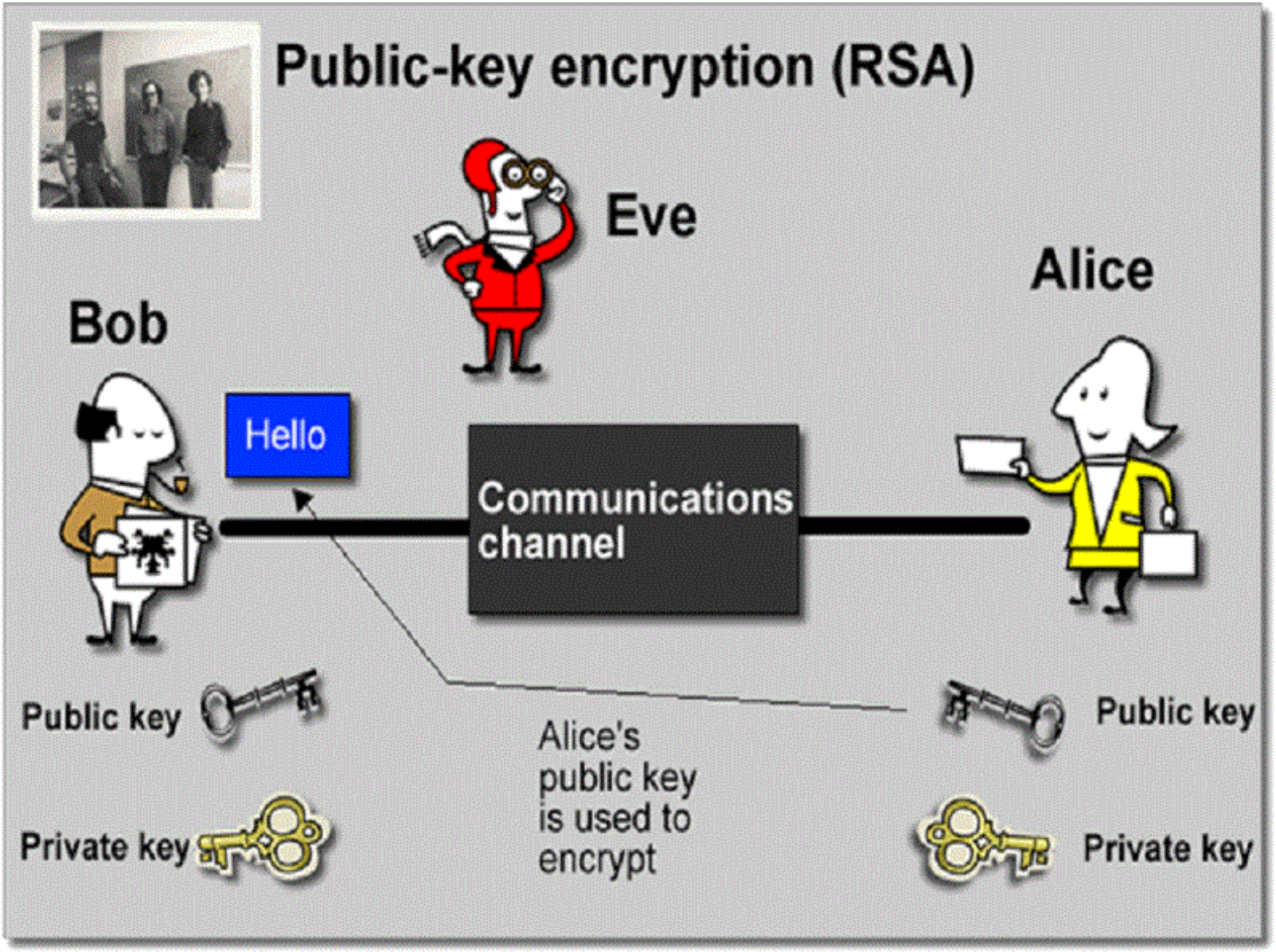
1994, Peter Shor (MIT): If we had a quantum computer, it could factorize large numbers quickly

Peter Shor, MIT (1959-)

- 1994: quantum algorithm for prime factorization
  - exponentially faster!
- 1996: quantum error correction



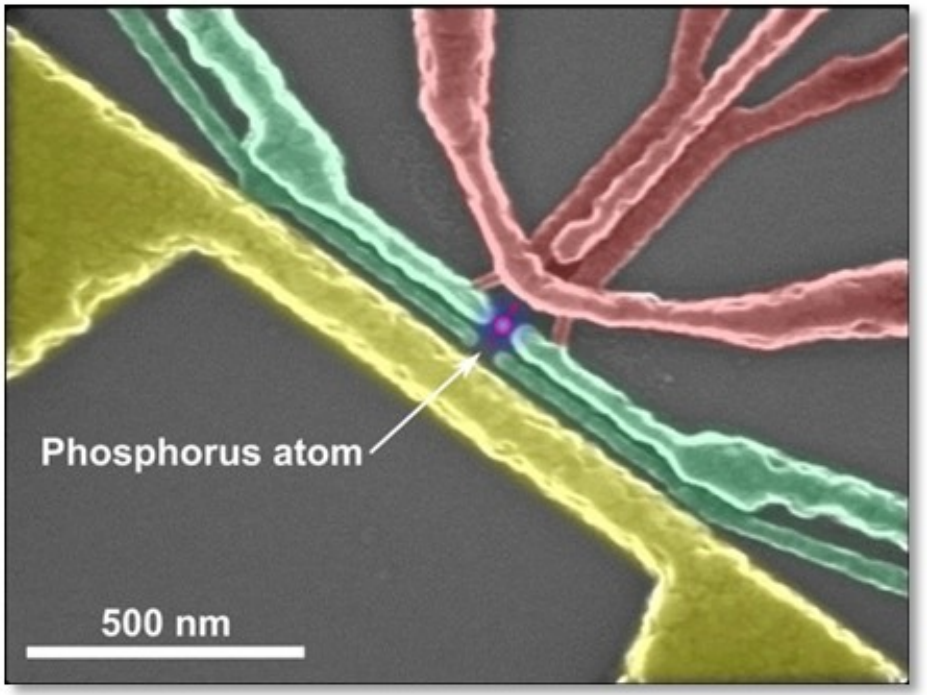
Shor's discovery attracted attention:
Can be used to break widespread encryption protocol (RSA)



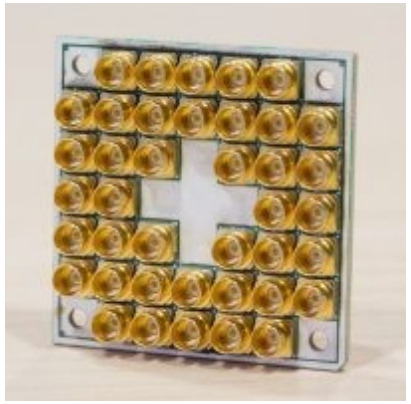
Quantum computer needs quantum bits.
Individual quantum systems, well isolated from environment, but controllable (initialization, logic gates, readout)

Chris Monroe, USA,
Joint Quantum Inst.:
Ions levitated in vacuum

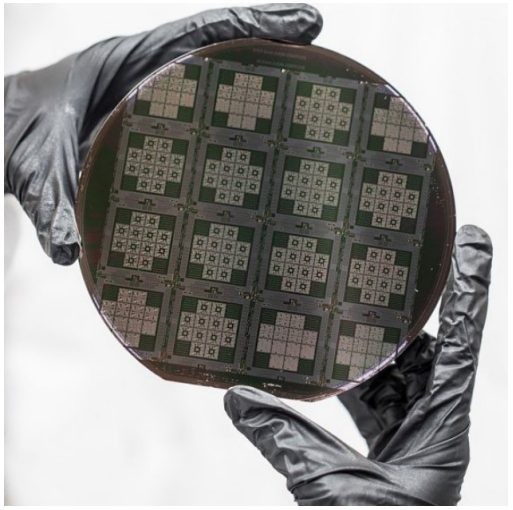
Australia (UNSW): nucleus
of phosphorus atoms
implanted in silicon



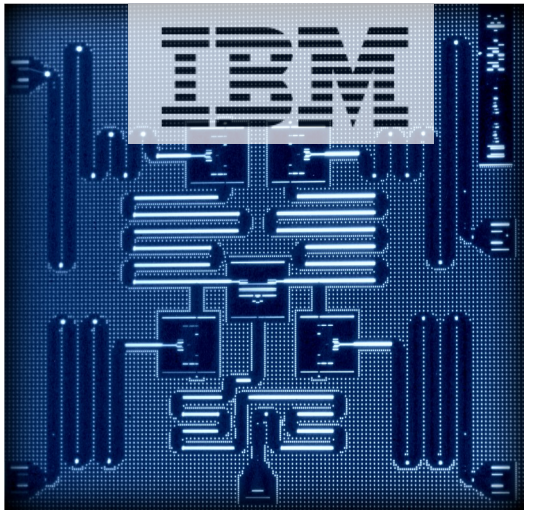
At the moment qubits made from superconducting integrated circuits seem most promising



TU Delft + Intel:
17 quantum bits,
low quality



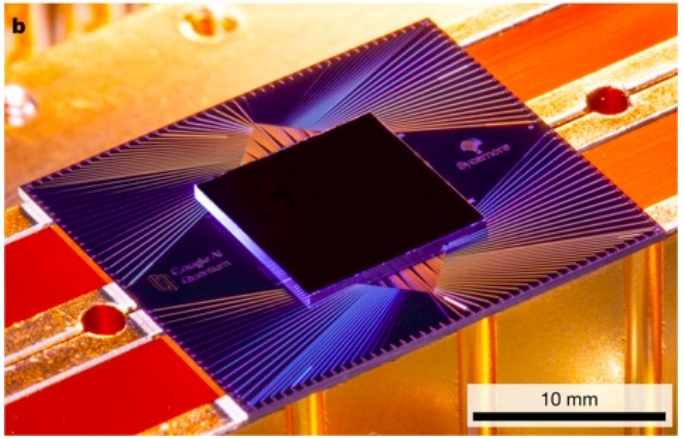
Rigetti: 19 quantum bits,
online for paying clients



IBM: 20 quantum bits,
online for free

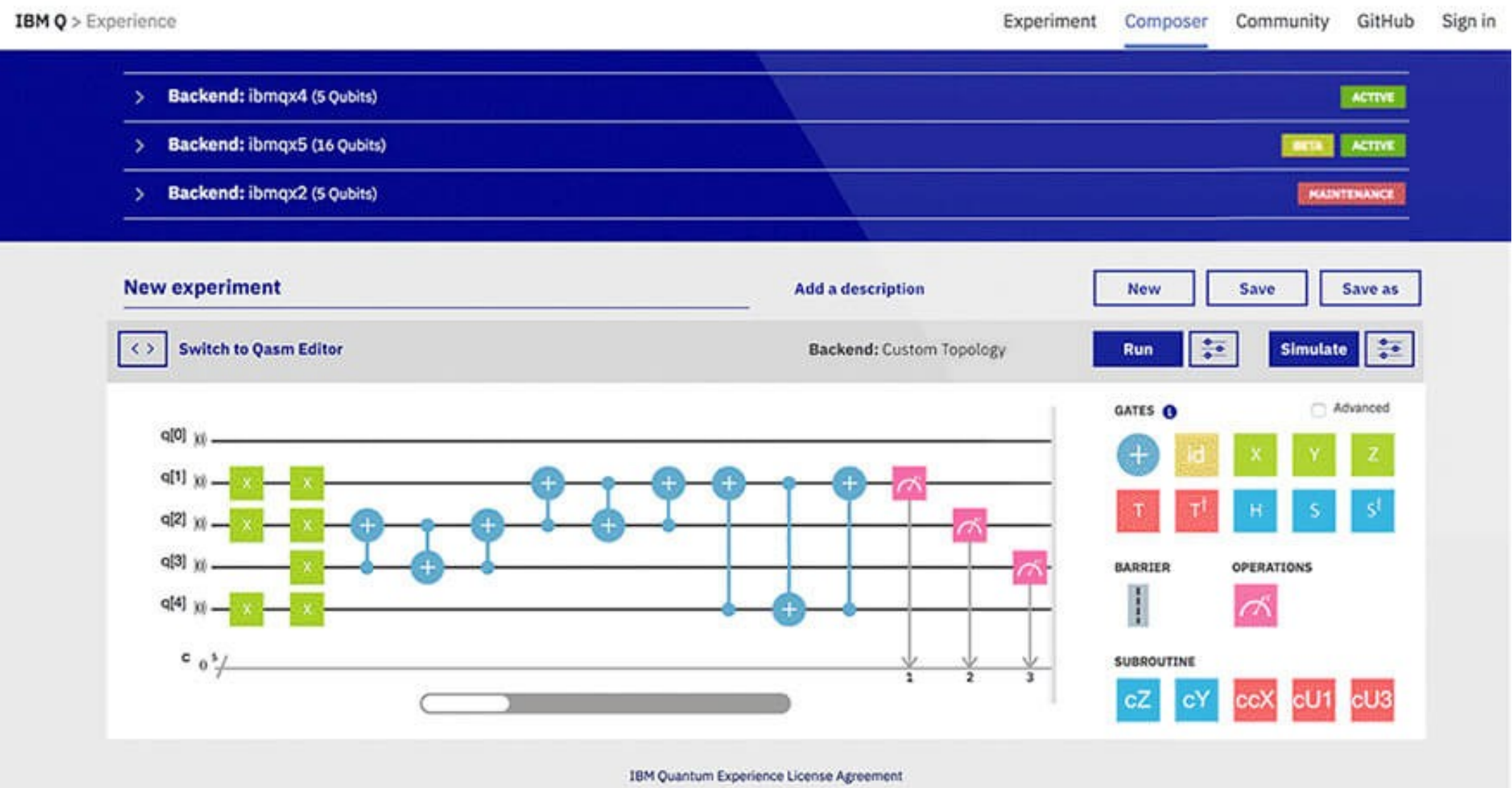
UCSB+Google:
53 quantum bits,
quantum supremacy

Google

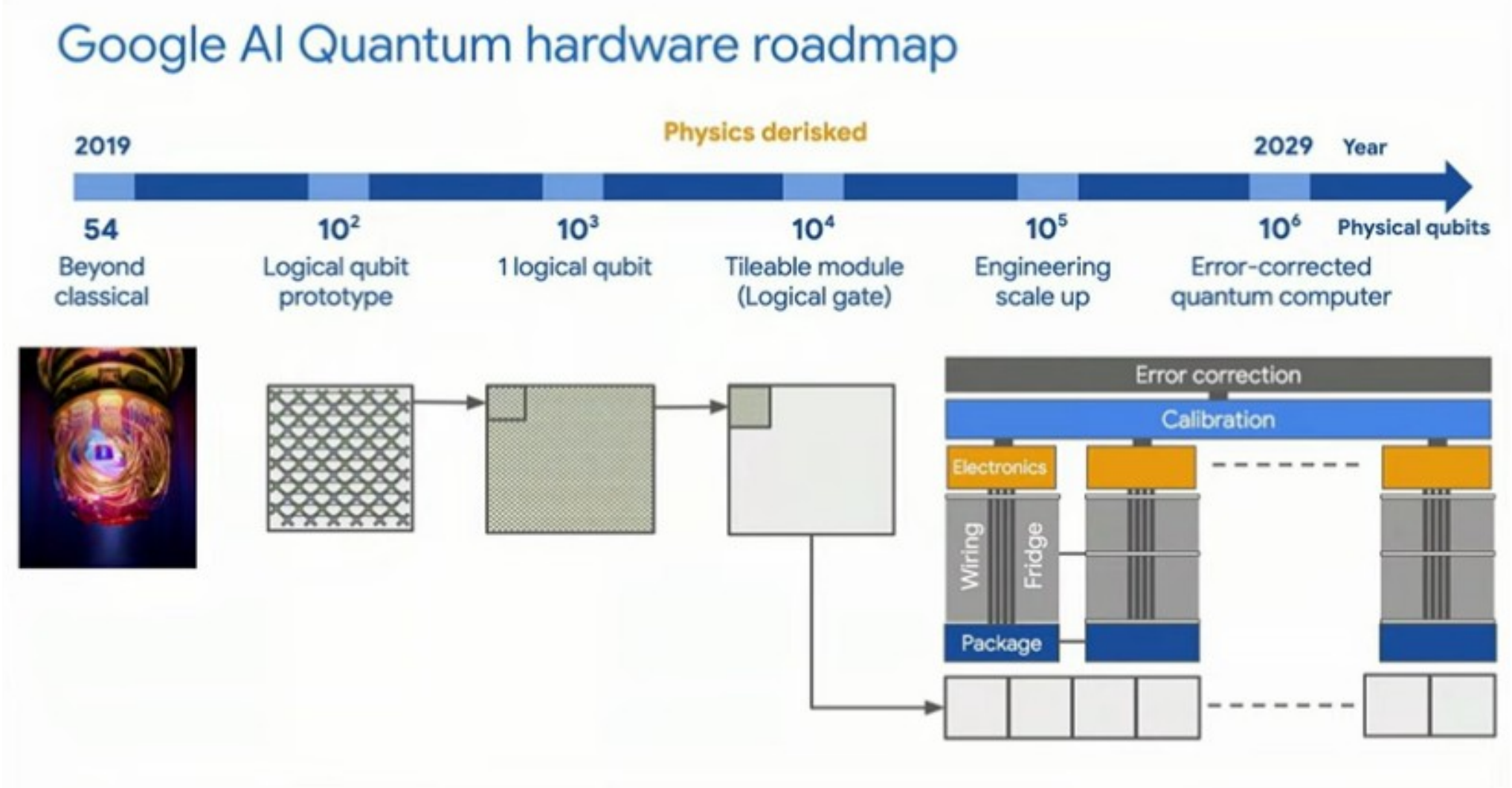


IBM's quantum computer is freely accessible, has user-friendly interface

https://quantum-computing.ibm.com/



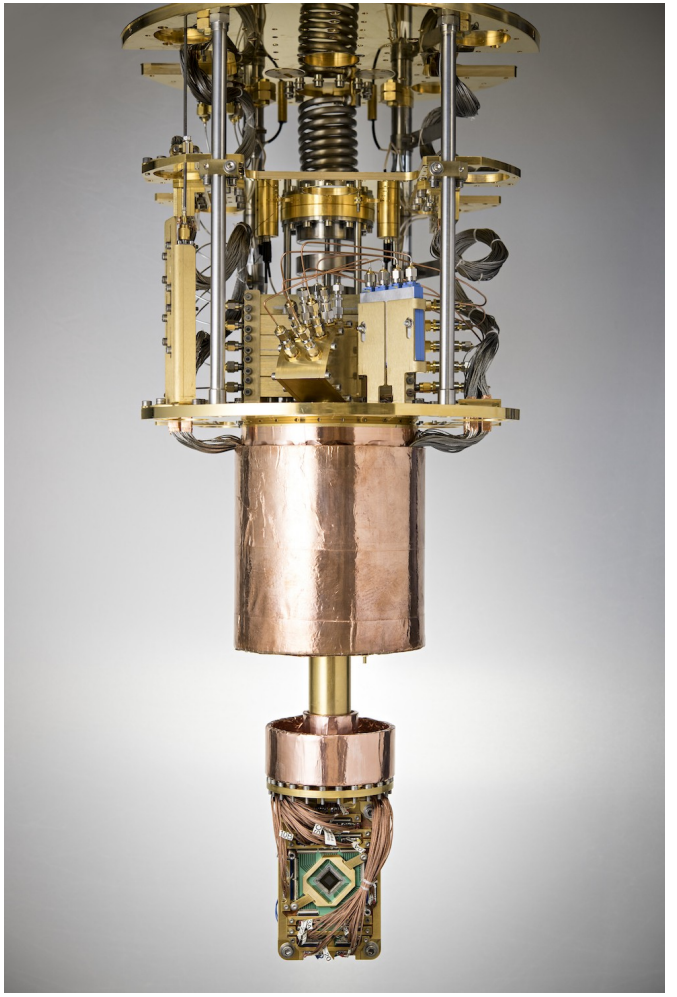
Google scaling up quantum computer building operation 1 million qubits before 2030?



[Hartmut Neven's talk on Google Summer Symposium 2020, https://www.youtube.com/playlist?list=PLQY2H8rRoyvx4VttfJOPRslw8XWT7yaBJ]

Off-the-shelf “quantum computer” : D-Wave quantum annealer (2000 bits, 15 million $)

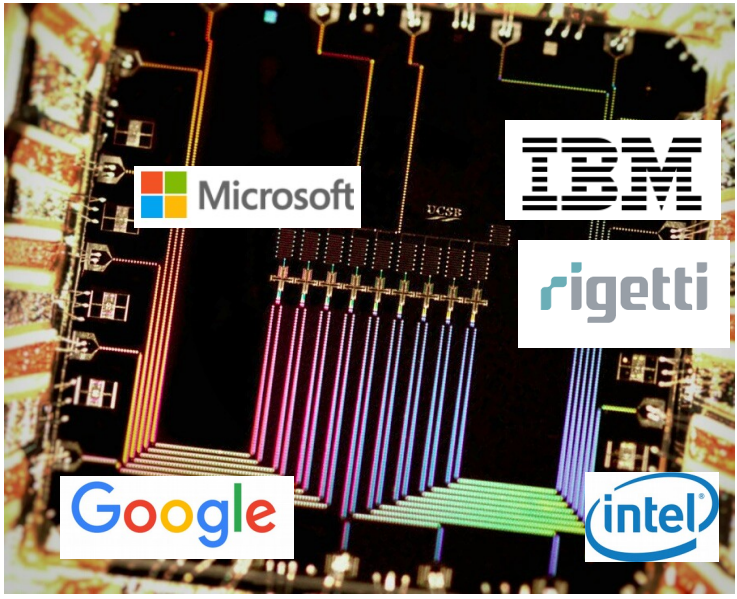
Can accelerate solution of traveling salesman problem, Google bought one for AI, but...



... not clear if better than desktop PC using clever algorithms(1 thousand $)

Summary:
using quantum weirdness for hard computing problems

- Some “hard problems” - faster computers do not help much to scale up solution
- Quantum world gives new opportunities (superposition, entanglement)
- Today: quantum processors with 10-50 bits, (Google, Intel, IBM, Rigetti, ...)
- Need: 1 million quantum bits to solve real-world problems
- Maybe in 10-20 years?



HUNQUTECH

How Quantum Physics changes Cryptography and Digital Signatures

János Asbóth[1,2]

1: Budapest University of Technology and Economics,
Dept. of Theoretical Physics;

2: Wigner Physics Research Centre,
Dept. of Quantum Optics and Quantum Information

UNL Budapest, 2020. September 14.

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL
AZ INNOVÁCIÓ LENDÜLETE
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Public key cryptosystems (Encryption & Digital Signature) work with trapdoor (one-way) functions: what one key locks, only other key can unlock

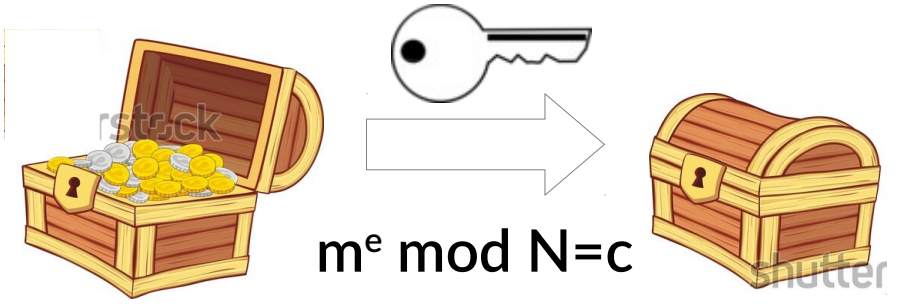
Alice

Manufactures:

Encoding key (e, N)

Decoding key (d, N)

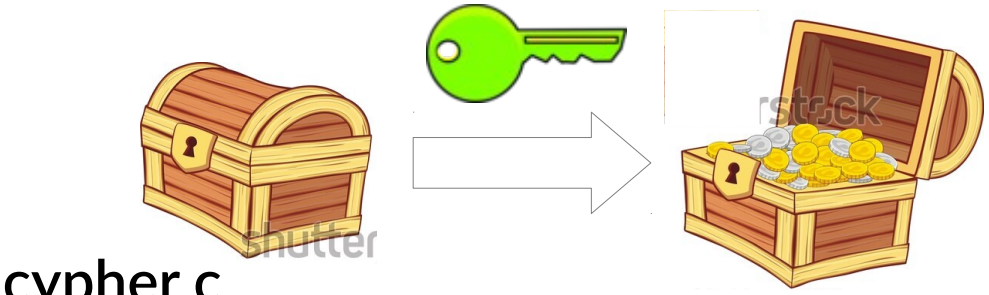
1. Two large primes p, q
2. N=pq
3. φ=(p-1)(q-1)
4. e coprime to φ
5. d = 1/e mod φ



message m

$m^e \bmod N = c$

cypher c



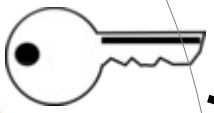
cypher c

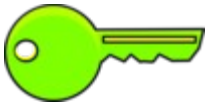
$c^d = m^{ed} \bmod N = m$

message m

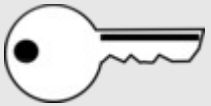
Cryptography: Alice publishes “locking” key, and keeps “unlocking” key. Anyone (e.g. Bob) can send secret messages to Alice

Alice

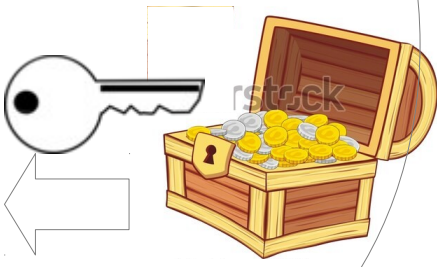


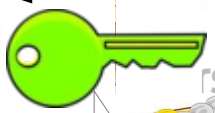


Public channel



Bob





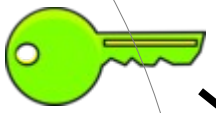
c=m^e mod N

Eve

Anyone can encode, only Alice can decode: Eavesdropper cannot open message

Digital signature: Alice publishes “unlocking” key, and unencoded document + encoded hash, keeps “locking” key. Alice’s signature can be identified by anyone

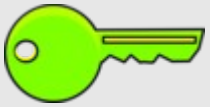
Alice



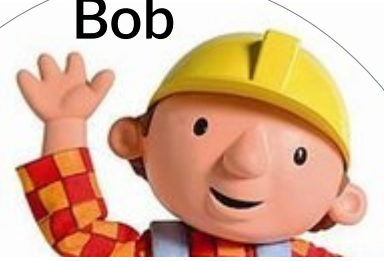
message m: hash of contract

$c=m^e \bmod N$

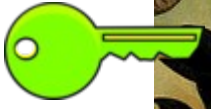
Public channel



Bob

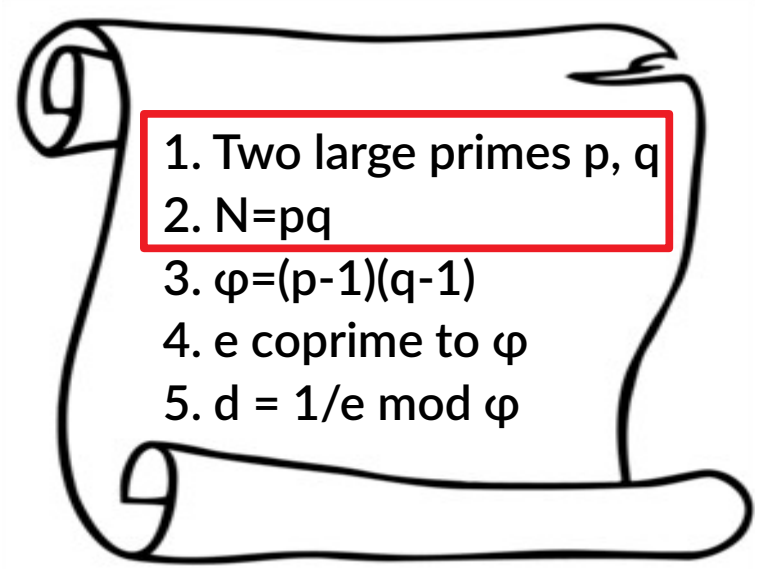


Eve



Anyone can decode, only Alice can encode: Eavesdropper cannot pretend to be Alice

Security of Public key cryptosystems: from 1 key, cannot reverse engineer the other key. Due to conjectured computational hardness of factoring.



easy

hard

Encoding key (e, N)

Decoding key (d, N)

$$\underbrace{15\,485\,863}_{p} \cdot \underbrace{32\,452\,843}_{q} = \underbrace{502\,560\,280\,658\,509}_{N}$$

Here, N has 15 digits = 50 bits.

RSA foundation of many publicly used cryptosystems (e.g. PKCS#1)

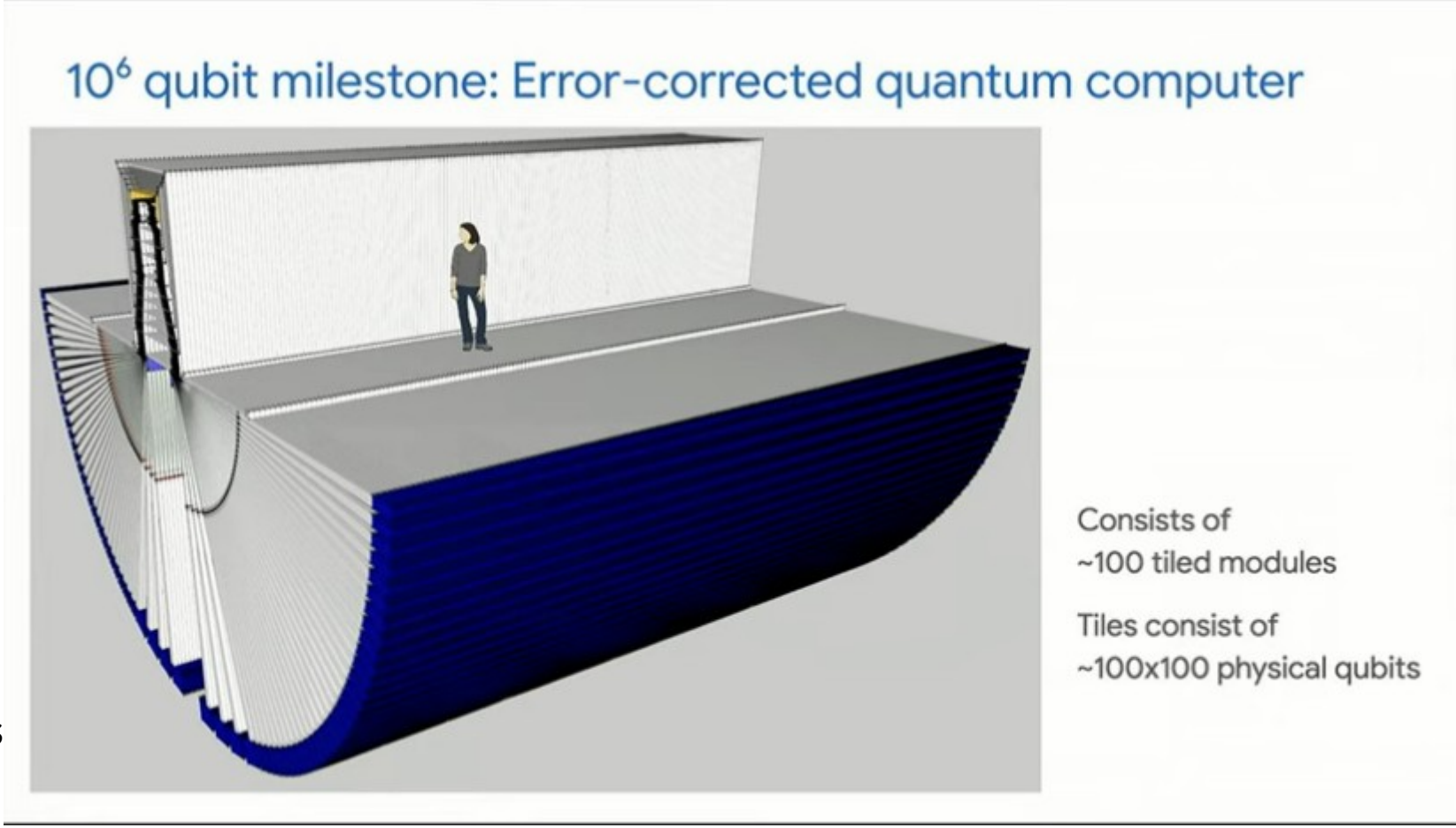
Recommendation (NIST, 2015) for N: 2048 bits = 615 digits

Quantum computers with ~20 million bits could factor 2048-bit numbers, and break RSA

2048-bit RSA :
1 hour,
20 million qubits

4096-bit RSA :
2 hours,
40 million qubits

65536-bit RSA:
4 days,
1000 million qubits



[Gidney & Ekera: How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, arXiv:1905.09749]

[Hartmut Neven's talk on Google Summer Symposium 2020, https://www.youtube.com/playlist?list=PLQY2H8rRoyvx4VttfJOPRslw8XWT7yaBJ]

Improve security of cryptography/digital signature:
1) Post-quantum cryptography

Post-quantum =quantum-proof = quantum-safe = quantum-resistant

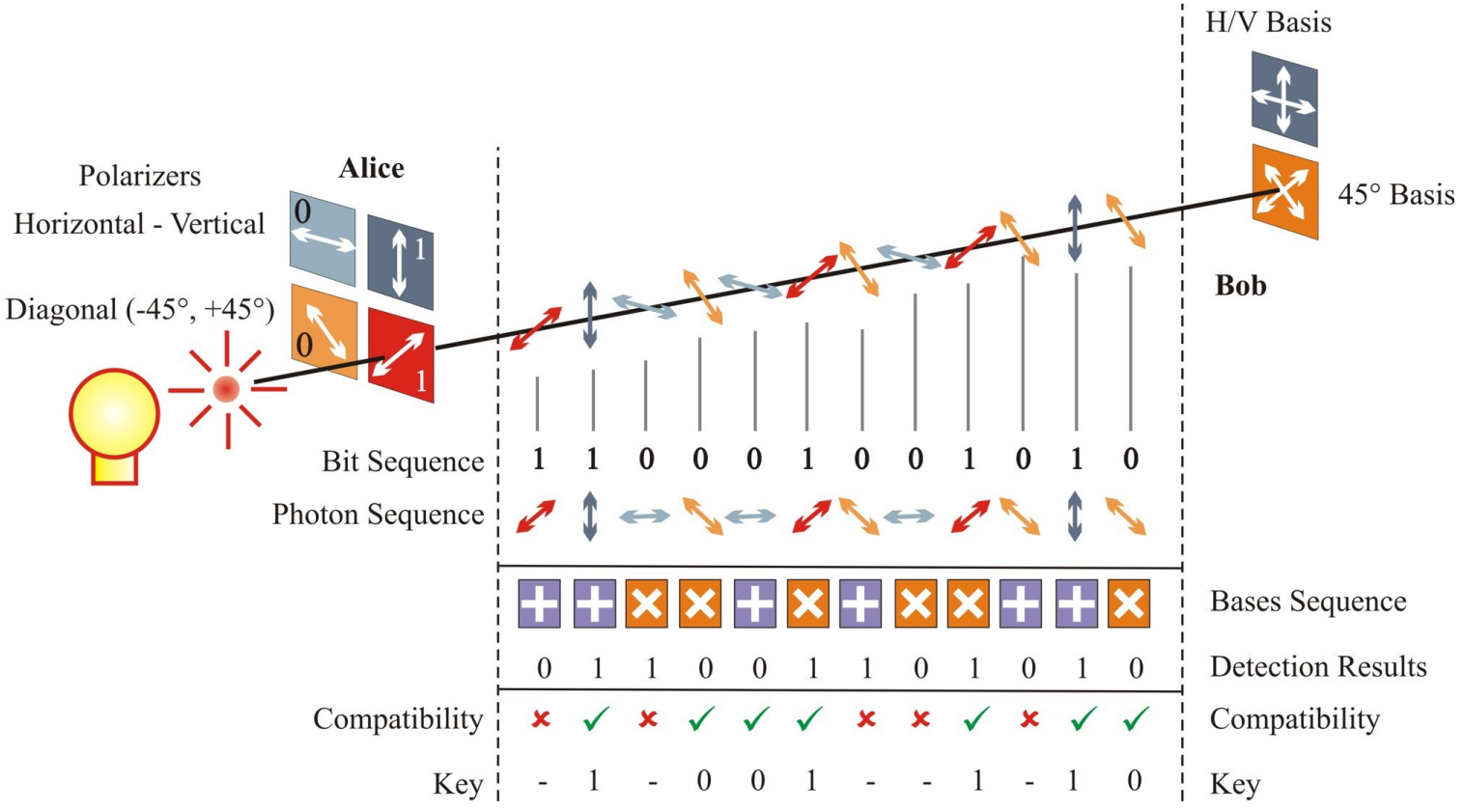
- symmetric cryptographic algorithms OK
- Existing technology, implementable
- Secure against existing quantum & classical algorithms
- Security due to conjectured computational hardness

Improve security of cryptography/digital signature: 2) Quantum cryptography, invented in 1984

Charles Bennett, IBM (1943-)

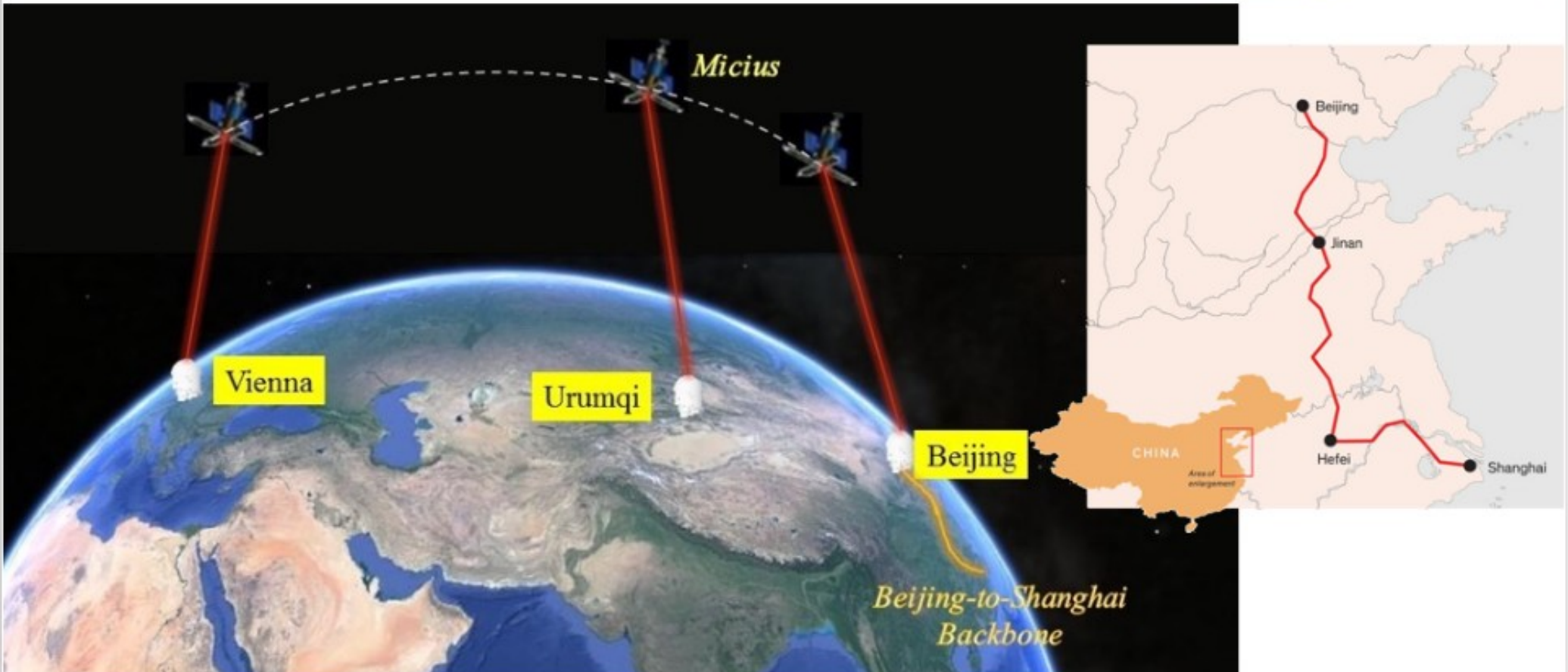
- 1972→ information theory
- 1984: BB84, first quantum cryptography protocol
- 1993: quantum teleportation

Gilles Brassard, Montreal

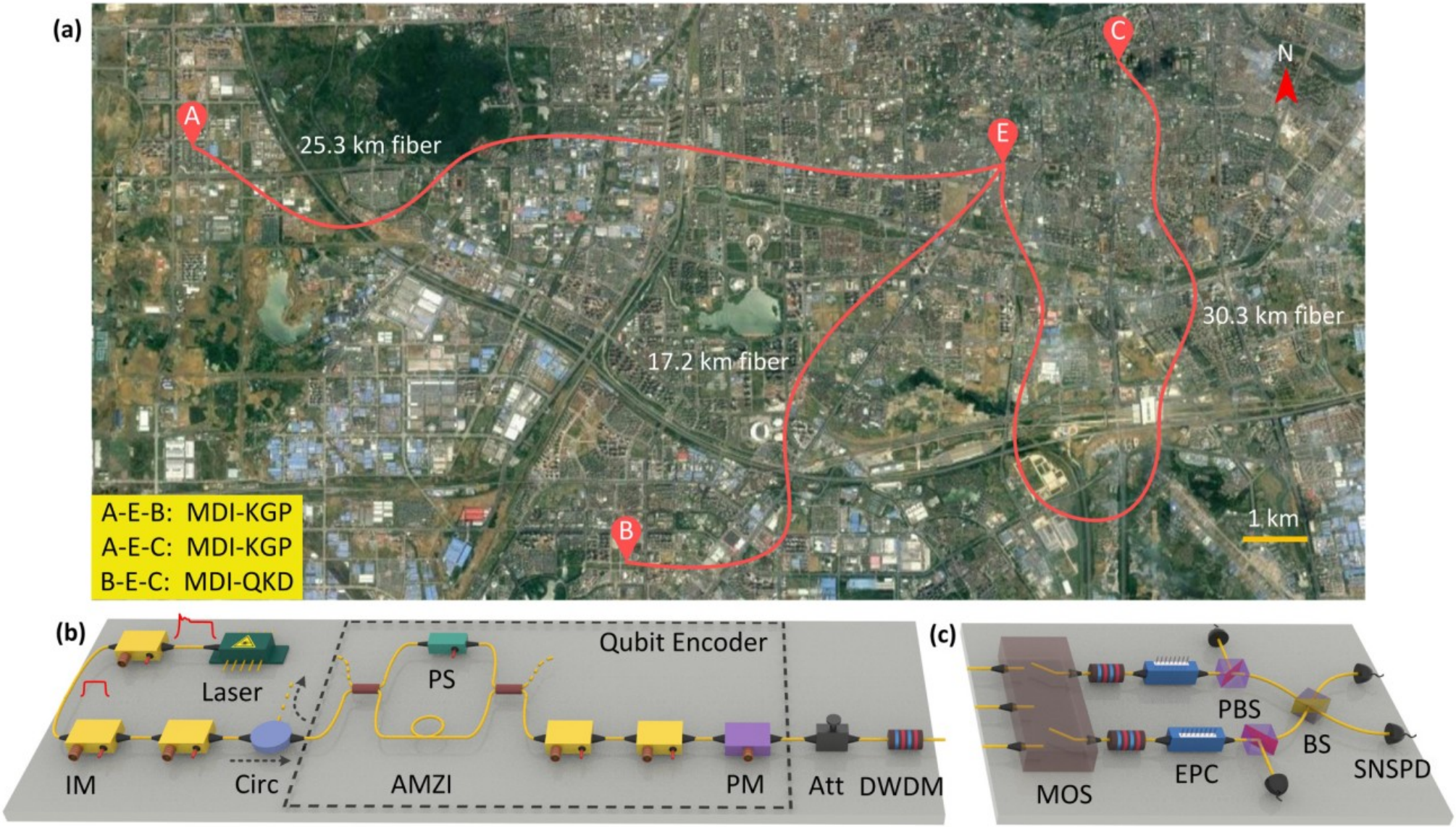


Quantum cryptography is already implemented, international networks being developed. Problems: short range, low bitrate

- IdQuantique
- Toshiba
- QuintessenceLabs
- Qubitekk
- QuantumCTek
- …



Quantum digital signature: signature fades quickly (no quantum memory, verification has to be fast). First demonstration experiments in Hefei, China, 2017



[Yin et al: Experimental measurement-device-independent quantum digital signatures over a metropolitan network, Phys. Rev. A (2017)]

Summary: How Quantum physics changes cryptography/ digital signatures

- Practical public-key cryptography/digital signature rely on conjectured computational hardness of factoring & related problems. Example: RSA
- Quantum computers in 10-20 years could break RSA-2048
- Post-quantum cryptography: more cumbersome algorithms that are conjectured more secure. Could be deployed right now
- Quantum cryptography:
  + security based on physics
  - short range, low bitrate
- Quantum digital signature:
  + security based on physics
  - short range, short lifetime

Only 53 quantum bits on the best quantum computer, because it is hard to protect fragile superposition states from the environment

- Dilution fridge using He3/He4 mixture (1 million $)
  → 10 mK (300x colder than outer space)
- Precise control & measurement difficult (1% error – slightly too much)
- Controlling 1 quantum bit → neighbor is affected