Introduction to Quantum Technologies

Ilkka Tittonen

Micro and Quantum System Group (MQS)

Department of Electronics and Nanoengineering &
Center for Quantum Engineering (CQE)

Aalto University

Topics

- General remarks of using light
- A few “simple” quantum-mechanical cases
- Basics of quantum communication
- Principles of encryption
- Some international examples
- Examples of Quantum Computation
- Big Data applications
- Quantum radar/Illumination in a noisy environment

Assume a communication laser: wavelength = 1550 nm, power 10 mW

$$H = \frac{1}{2}\int_V dV(\epsilon_0 \mathbf{E}^2 + \mu_0^{-1}\mathbf{B}^2)$$

$$\begin{aligned} H_{\mathbf{k}}|n\rangle_{\mathbf{k}} &= \hbar\omega_{\mathbf{k}}(n+1/2)|n\rangle_{\mathbf{k}} \\ a_{\mathbf{k}}|0\rangle_{\mathbf{k}} &= 0 \\ a_{\mathbf{k}}|n\rangle_{\mathbf{k}} &= \sqrt{n}|n-1\rangle_{\mathbf{k}} \\ a_{\mathbf{k}}^{\dagger}|n\rangle_{\mathbf{k}} &= \sqrt{n+1}|n+1\rangle_{\mathbf{k}} \end{aligned}$$

$$E = hf = h\frac{c}{\lambda} = 3.14 \times 10^{-19} J \qquad P = \frac{nE}{t}$$

$$n = P\frac{t}{E} = 10 \times 10^{-3} W \frac{1s}{3.14 \times 10^{-19} J} = 3.18 \times 10^{16}$$

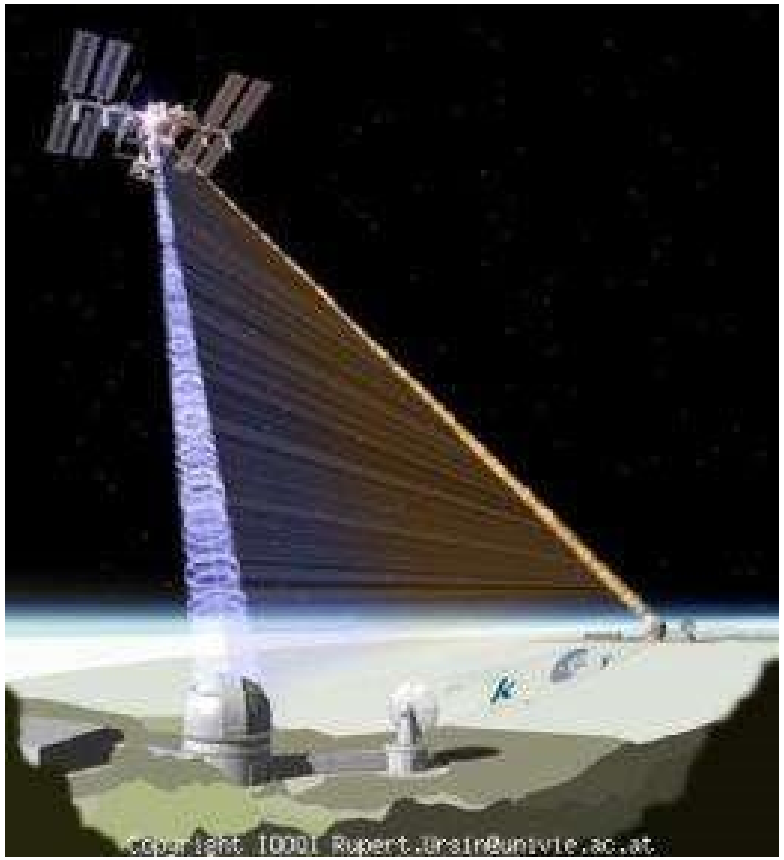
photons in a second!!

- A single photon has just three properties:
  colour/energy, polarization, direction/momentum

- Its quantum state can be described as a superposition of these properties

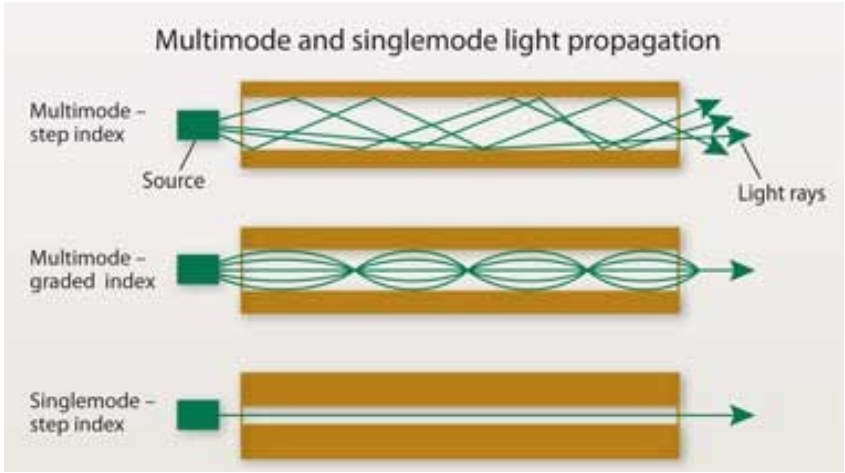
Communication using light

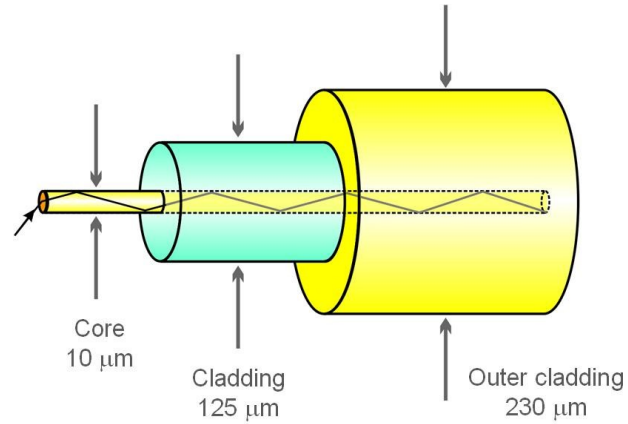
Either free space

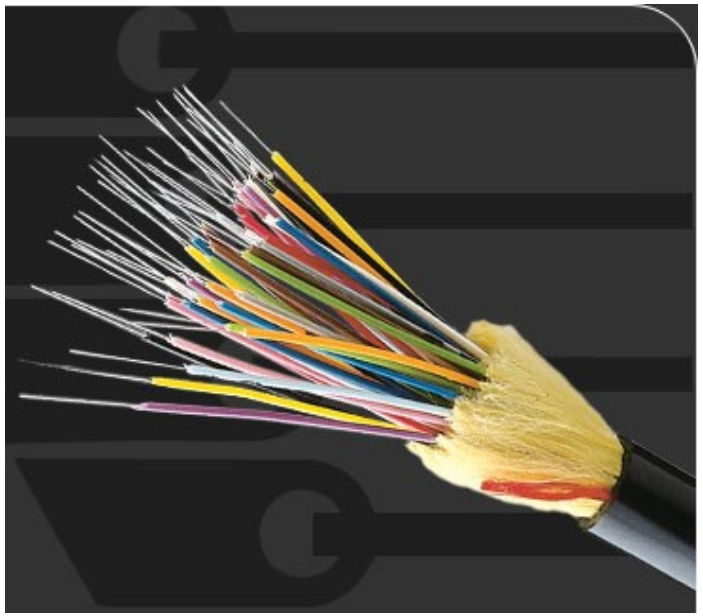


Distribution of Entanglement from the ISS. [Copyright ESA]

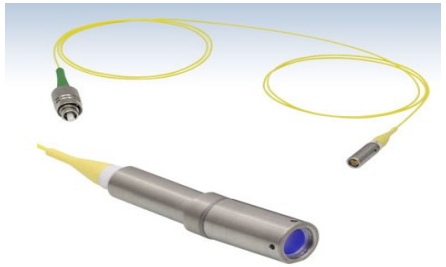
or in optical fiber



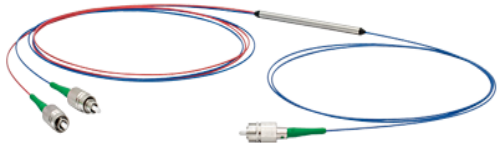




Advantages of fiber integration, many commercial "cheap" components readily available

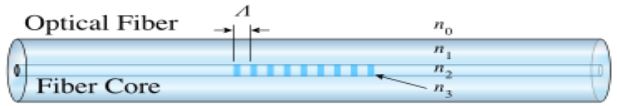


Fiber collimator



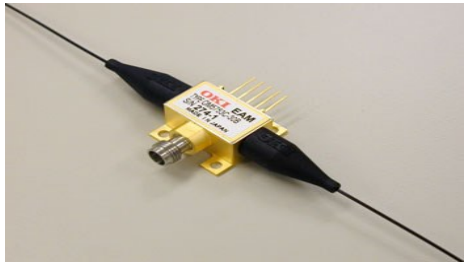
WDM

Fiber Reflector



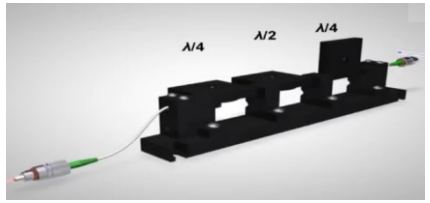
Fiber Bragg Grating

Isolators



Modulators

Circulators



Polarization Controllers

Safety?

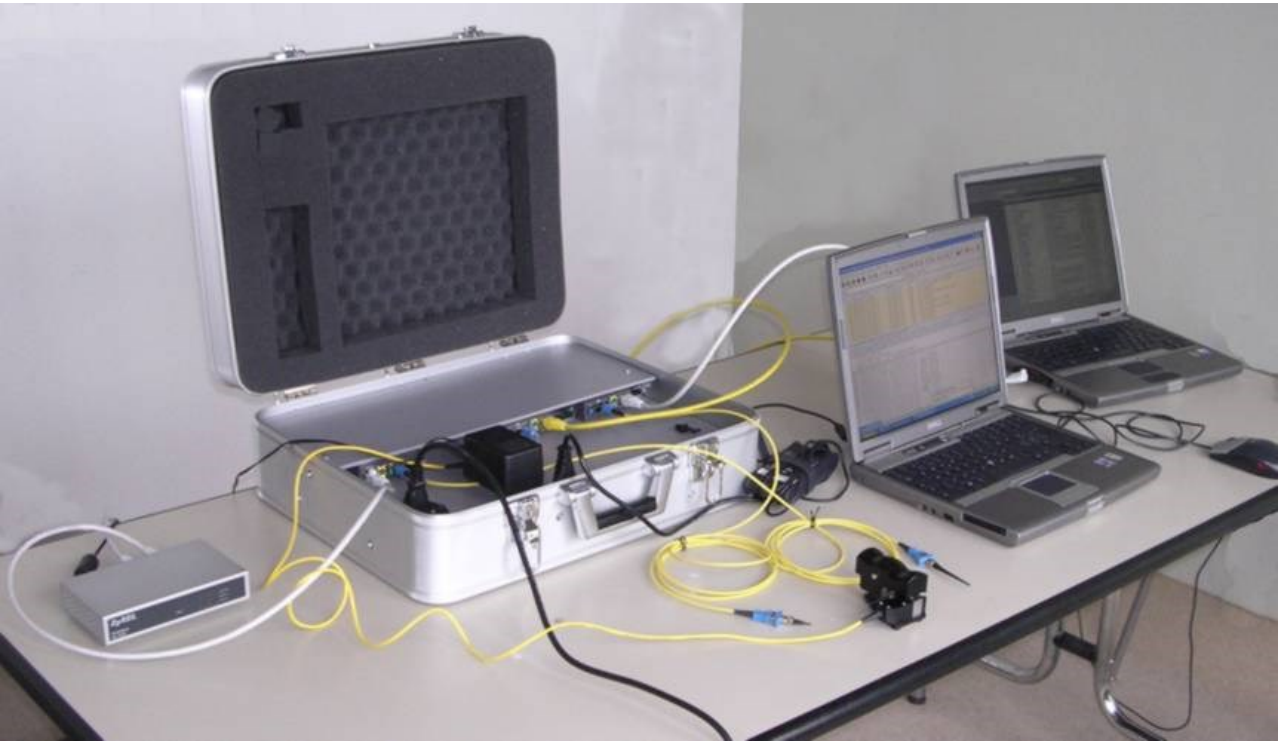
In fiber applications, one needs to have a physical contact with the fiber, which is in principle easy and invisible

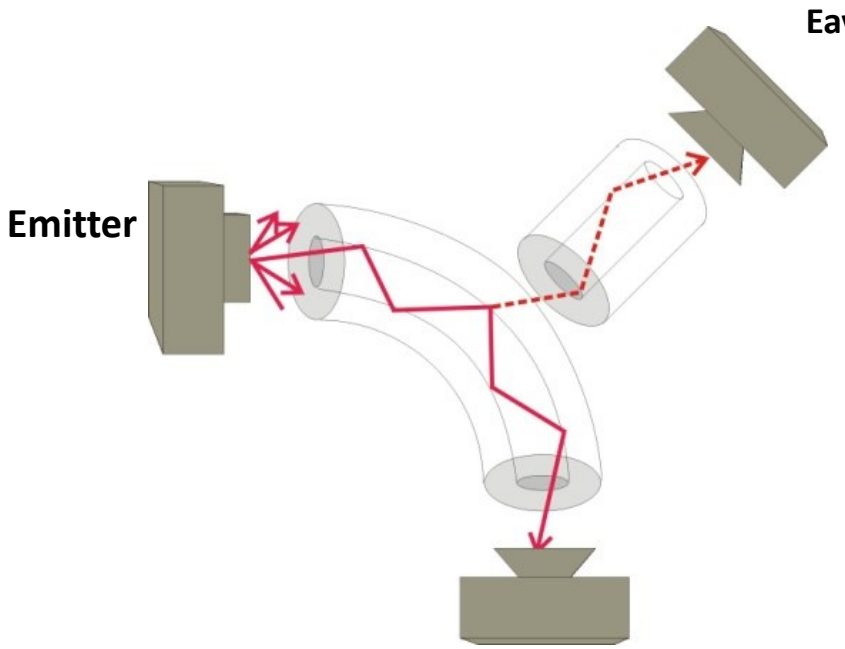
In free space between the top of mountains, between buildings, ground station-satellite, the evesdropper needs to be physically close to the optical beam, in the middle and possibly easily detectable

Copying video signal from someone else' fiber is very easy!!!

Optical Tapping for under €500

- **Optical fiber bending & coupling**
- **Buy an optical tap**
  - http://www.fods.com/optic_clip_on_coupler.html





Receiver

Quantum Mechanics

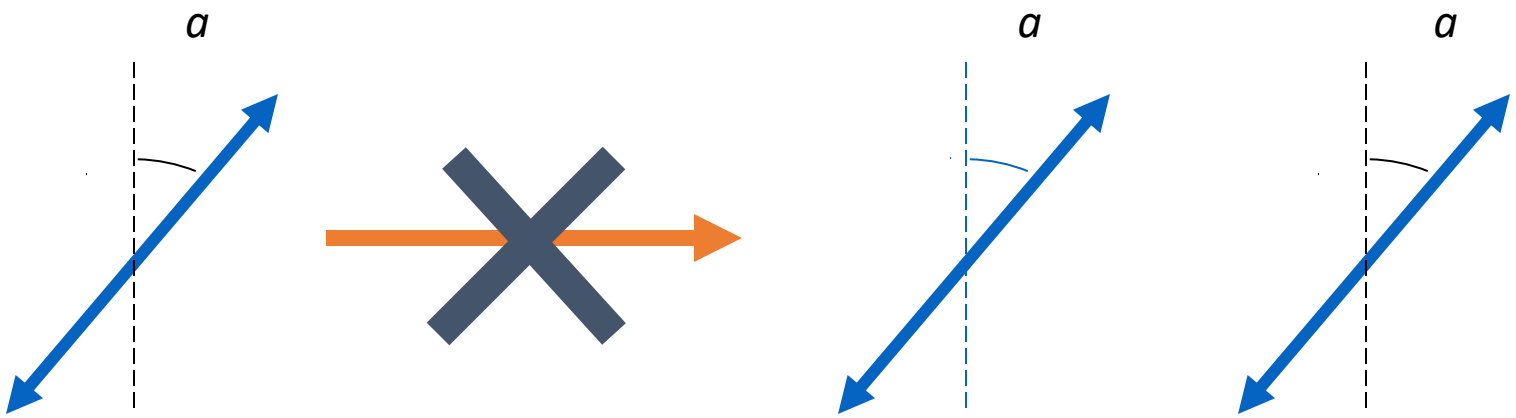
Quantum concepts such as:

- Uncertainty,
- Superposition,
- Entanglement,
- No-cloning,

do not have a correspondent in classical physics

Reminder: Quantum No-cloning Theorem

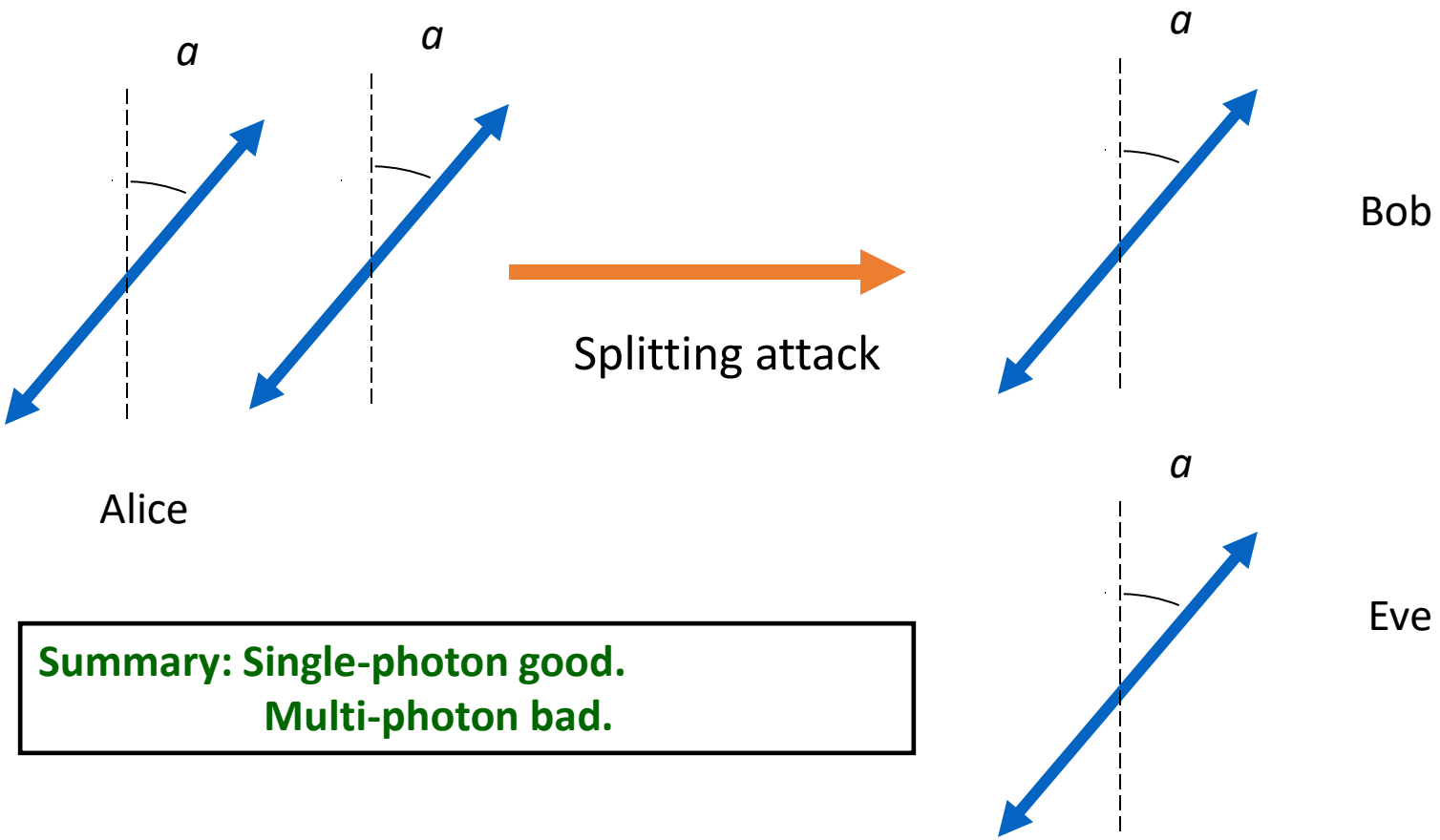
- An unknown quantum state **CANNOT** be cloned. Therefore, eavesdropper, Eve, cannot have the same information as Bob.
- Single-photon signals are secure.



IMPOSSIBLE

Photon-number splitting attack against multi-photons

A multi-photon signal CAN be split. (Therefore, insecure.)



Summary: Single-photon good.
Multi-photon bad.

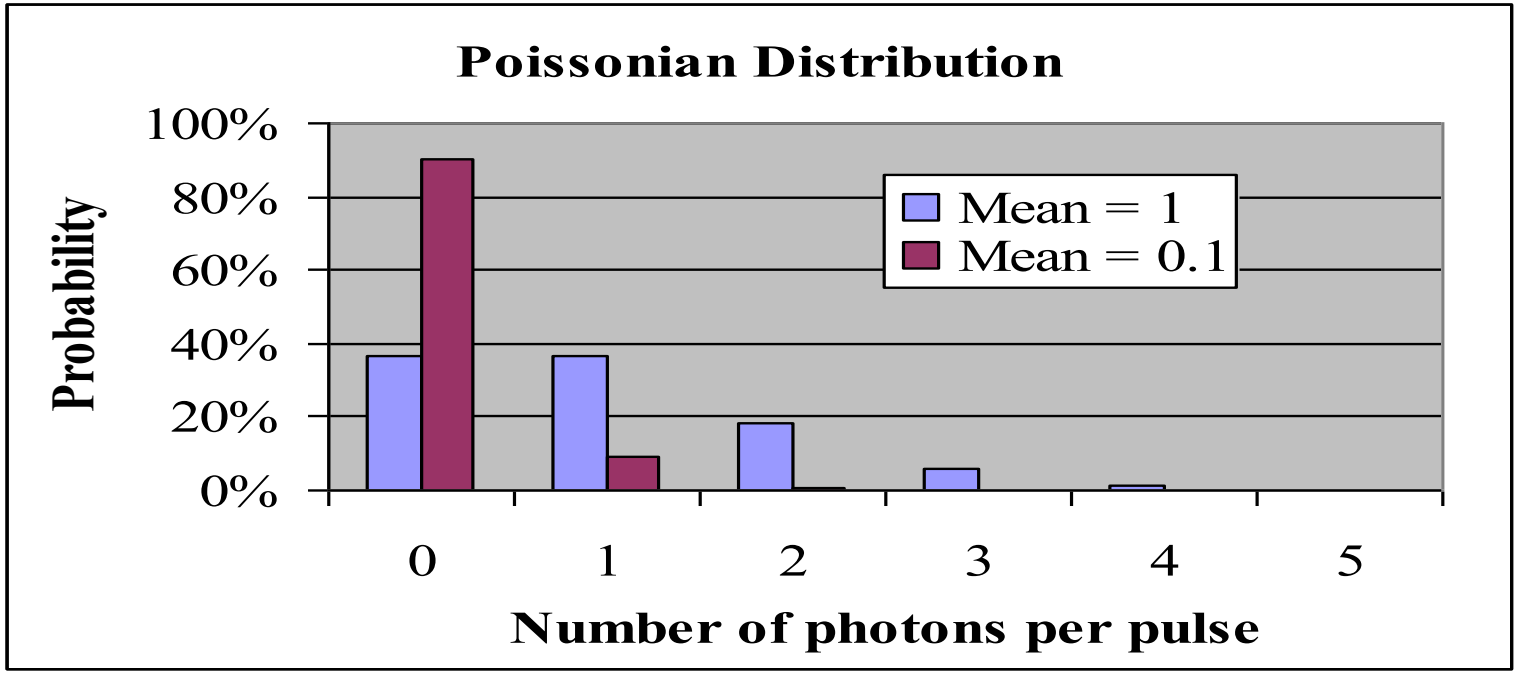
Pseudo-Single-Photon Source

- Realised with standard semiconductor lasers and calibrated attenuators (low cost, triggered, room T...)

probability of finding n photons in a pulse follows the Poisson Statistics

$$P(n,\mu) = \frac{\mu^n}{n!} \exp(-\mu)$$

μ mean photon number



Secure communication and QKD

Alice

Eve

Bob

Basic Idea of QKD, optics brings along a new way of hard ware encrypting

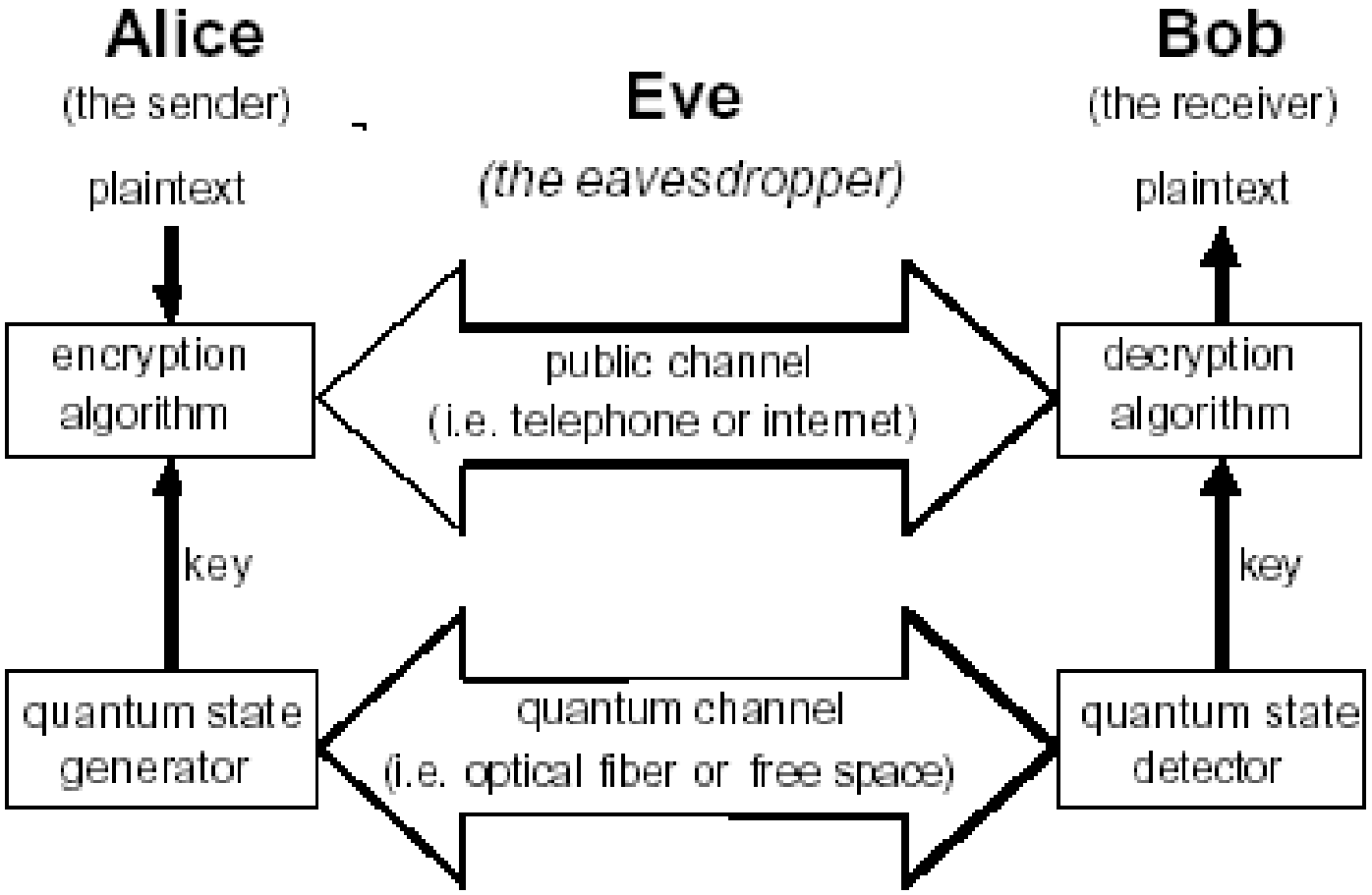


Figure 1. Quantum Key Distribution.

The goal is to exchange keys for hiding the message (OTP example)

• message	M	O	I
	01001101	01001111	01001001
• Key	01110110	01100010	01100101
• Secret msg	00111011	00101111	00101100

XOR

Inputs		Outputs
X	Y	Z
0	0	0
0	1	1
1	0	1
1	1	0

Examples of classical logic gates

AND gate

2 Input AND gate		
A	B	A.B
0	0	0
0	1	0
1	0	0
1	1	1

OR gate

2 Input OR gate		
A	B	A+B
0	0	0
0	1	1
1	0	1
1	1	1

NOT gate

NOT gate	
A	$\overline{A}$
0	1
1	0

NAND gate

2 Input NAND gate		
A	B	$\overline{A.B}$
0	0	1
0	1	1
1	0	1
1	1	0

NOR gate

2 Input NOR gate		
A	B	$\overline{A+B}$
0	0	1
0	1	0
1	0	0
1	1	0

EXOR gate

2 Input EXOR gate		
A	B	A⊕B
0	0	0
0	1	1
1	0	1
1	1	0

Addition mod 2:

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$

XOR gate

$k \in \{0,1\}^n \ \ uniformly\ distributed$

m=original message to be sent,
k=secret code (here a secret random 8-bit string of 0's and 1's),
c=message to be sent from Alice to Bob

Alice sends c=m⊕k

Bob knows k:

c ⊕k=(m ⊕k) ⊕ k= m ⊕k ⊕k=m ⊕0=m

Example: letter Q corresponds to 01010001 =m,

let 00110111= k,

m ⊕k= 01100110

c ⊕k= 01010001

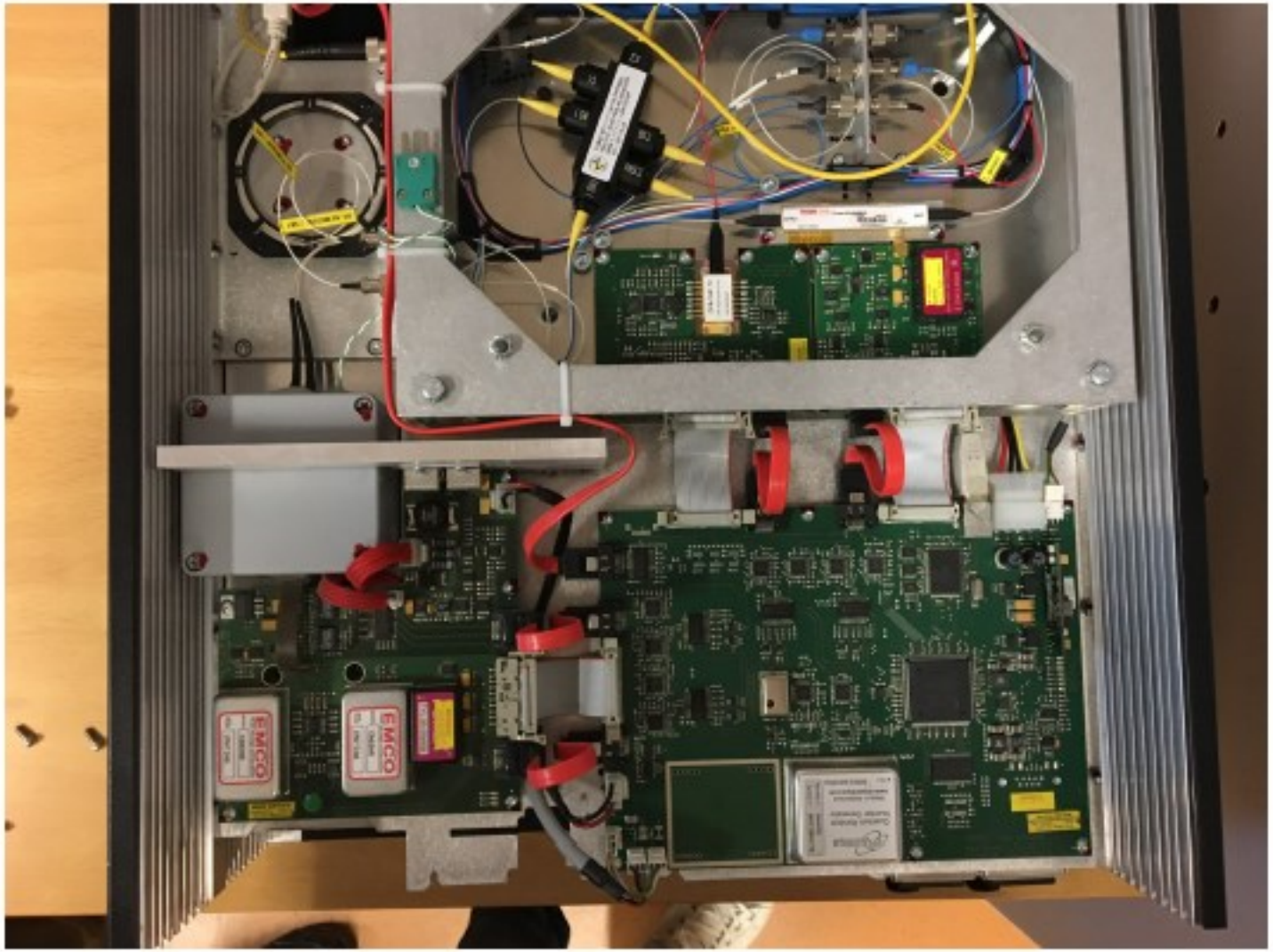
IDQuantique QKD setup

(MATINE project)


PLASMA
LG

Alice

Bob



Advantages of Quantum Cryptography

Long-term confidentiality of data

- Crypto based on computational complexity may be compromised by powerful supercomputers and/or cryptanalysis in future
- Quantum cryptography suitable for long term secrets

Security from quantum computer

- Quantum computer will severely weaken conventional public key cryptography
- Quantum crypto secure from all attacks by a quantum computer

High quality random number generation

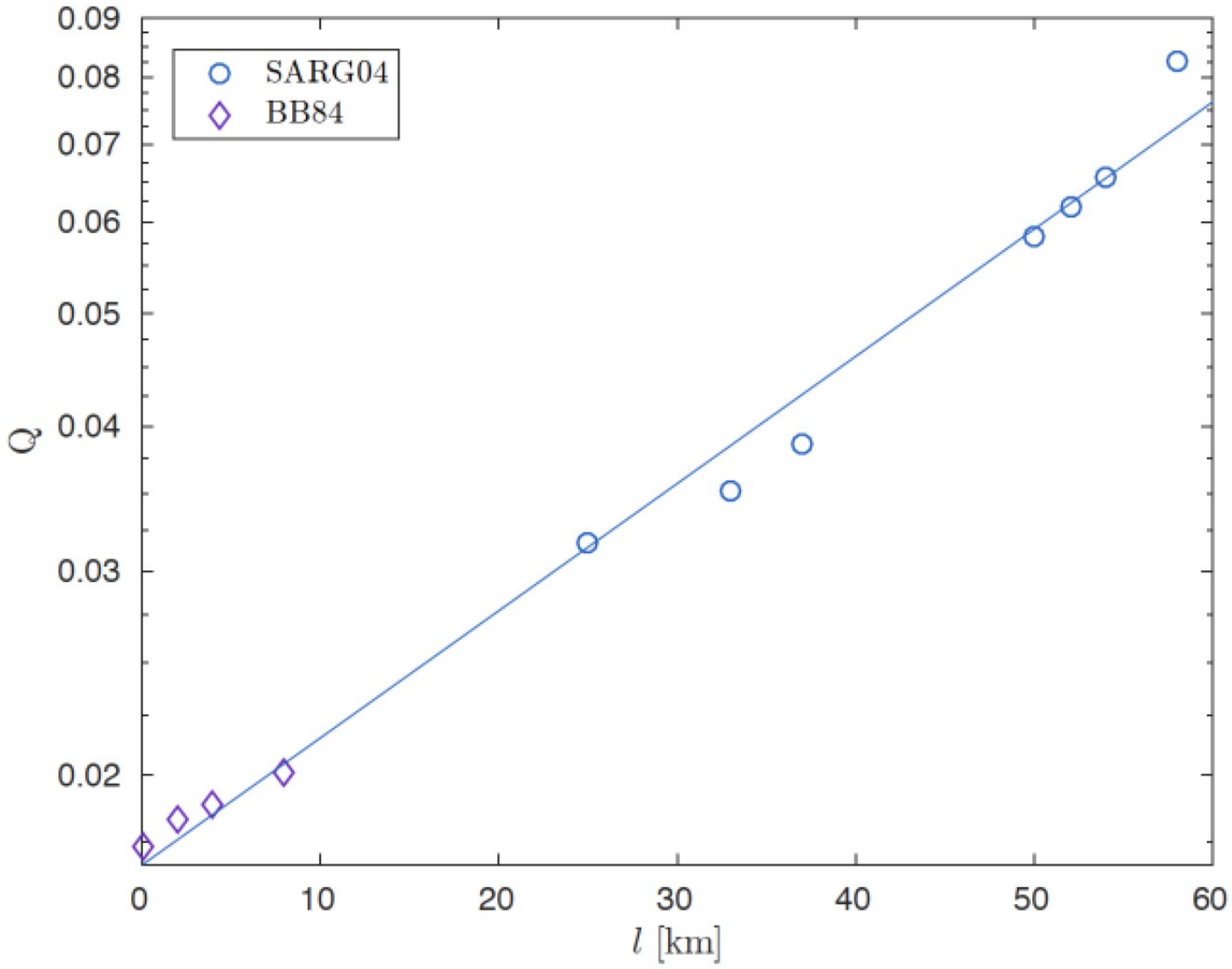
- High quality random numbers important for all cryptography
- Quantum processes are impossible to predict and well suited to generation of high quality random numbers at high rates

Physical layer security

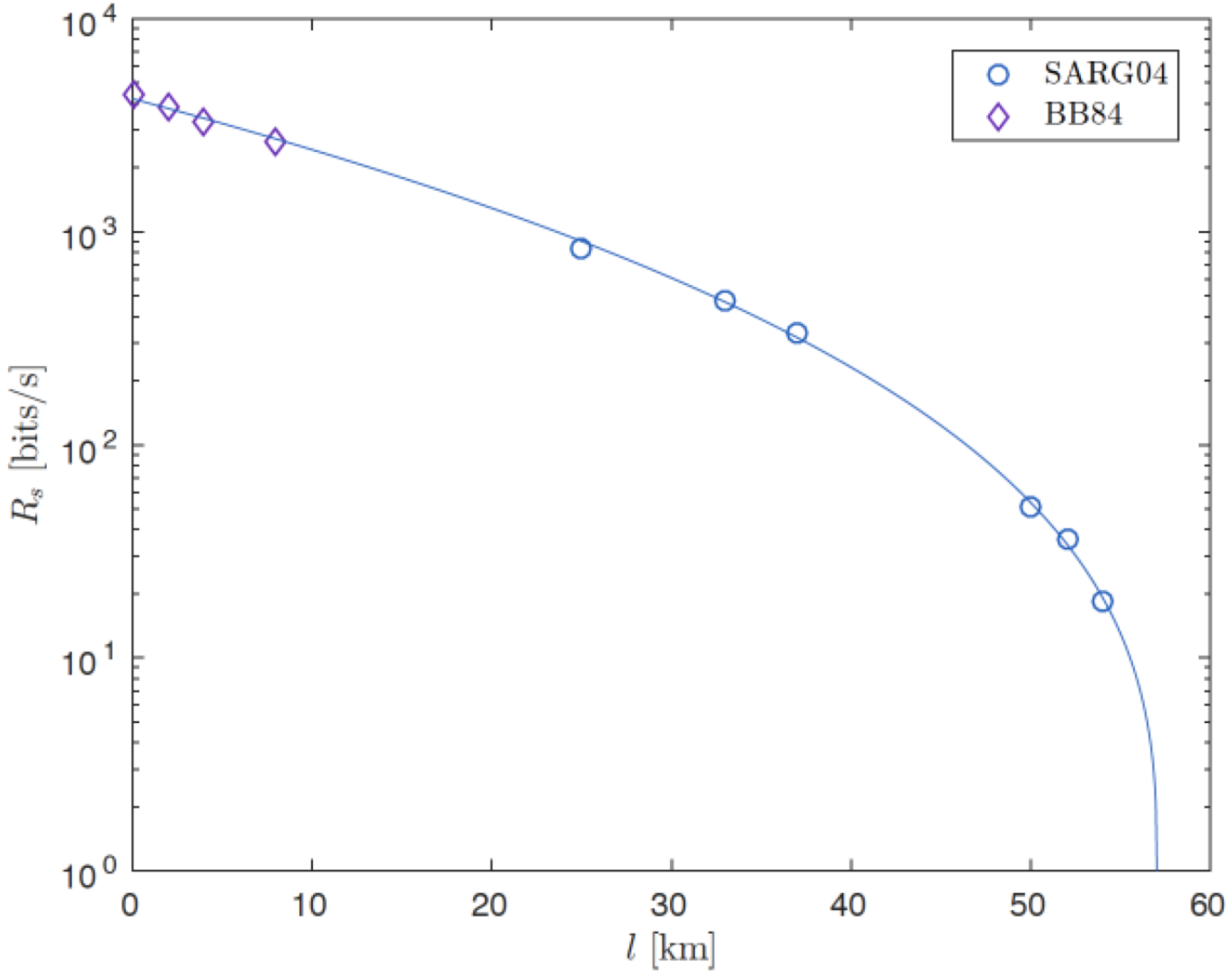
- Suitable for low latency, high bandwidth encryption.
- Use in conjunction with other ‘quantum-safe’ technologies
- Stronger crypto through multi-layer approach

Not an algorithm,
high-entropy rnd’s

QBER as a function of distance

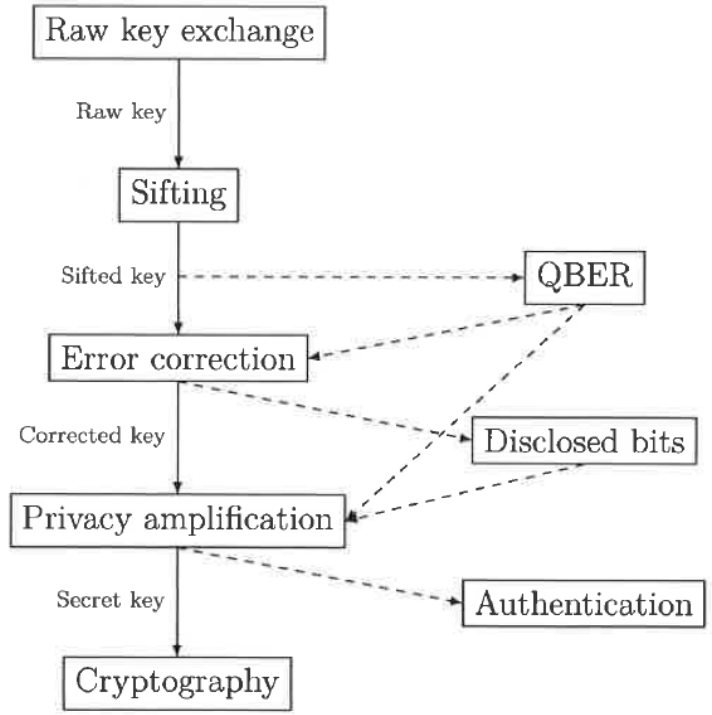


Keyrate as a function of distance



Different stages of QKD

- Raw key exchange and comparison of bases
- Some error correction protocol, QBER must be less than 11%
  unideal detectors and scattering create errors
- Privacy amplification
  key is made shorter by a hash-function
- Authentication
- Bit sifting is an important step in the post-processing of quantum key distribution.
  Its function is to sift out the undetected original keys.
- Hash functions (hashing algorithms) used in computer cryptography are known as "cryptographic hash functions".
  An example of such functions is for example **SHA-256, a** hash function is **a mathematical function that converts any digital data into an output string with a fixed number of characters**. Hashing is the one-way act of converting the data (called a message) into the output (called the hash).
- https://emn178.github.io/online-tools/sha256.html



One example of a practical test, the distance was chosen to be 25 km (quite normal)

Alice's key	5.14×10^8	100%
Bob's key	4.00×10^6	0.778%
Sifted key	9.95×10^5	0.194%
Final key	2.39×10^5	0.0466%

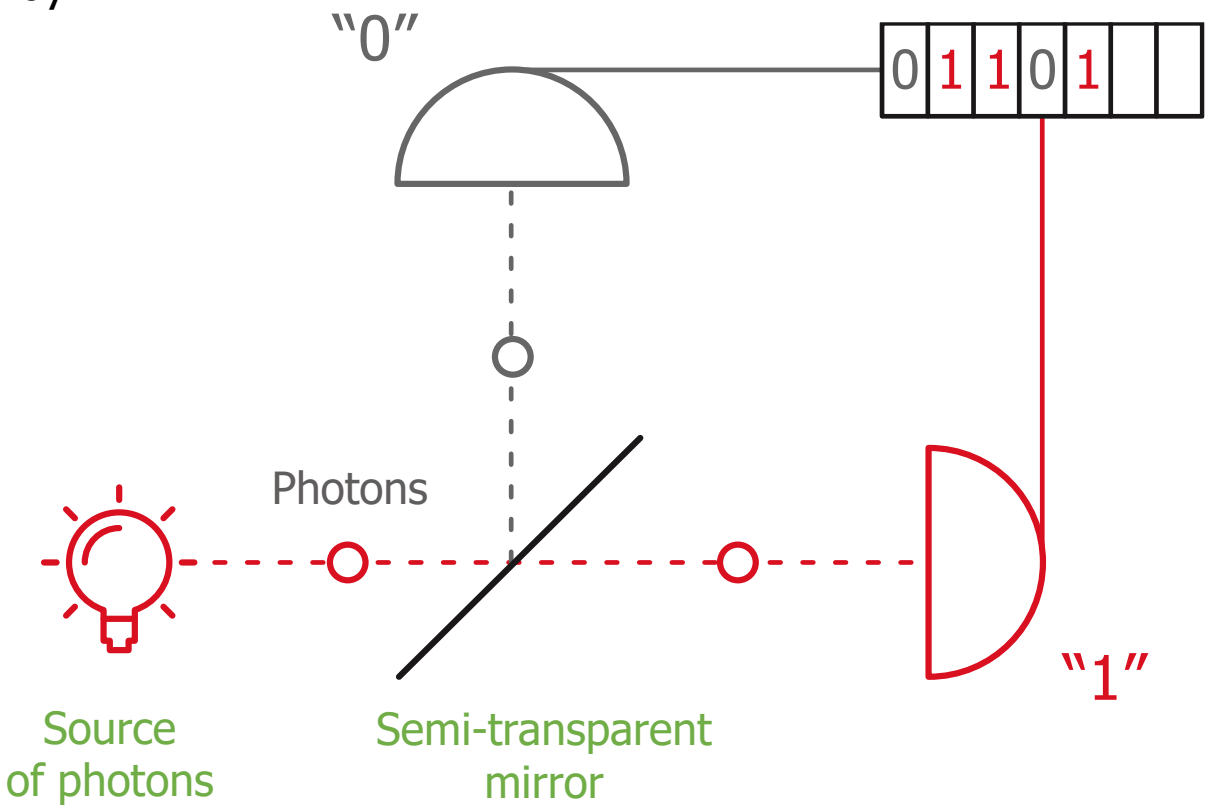
In error correction, 28% of the key is lost, one bit of key corresponds to the 2100 sent pulses.

Possible attacks: partly personal view

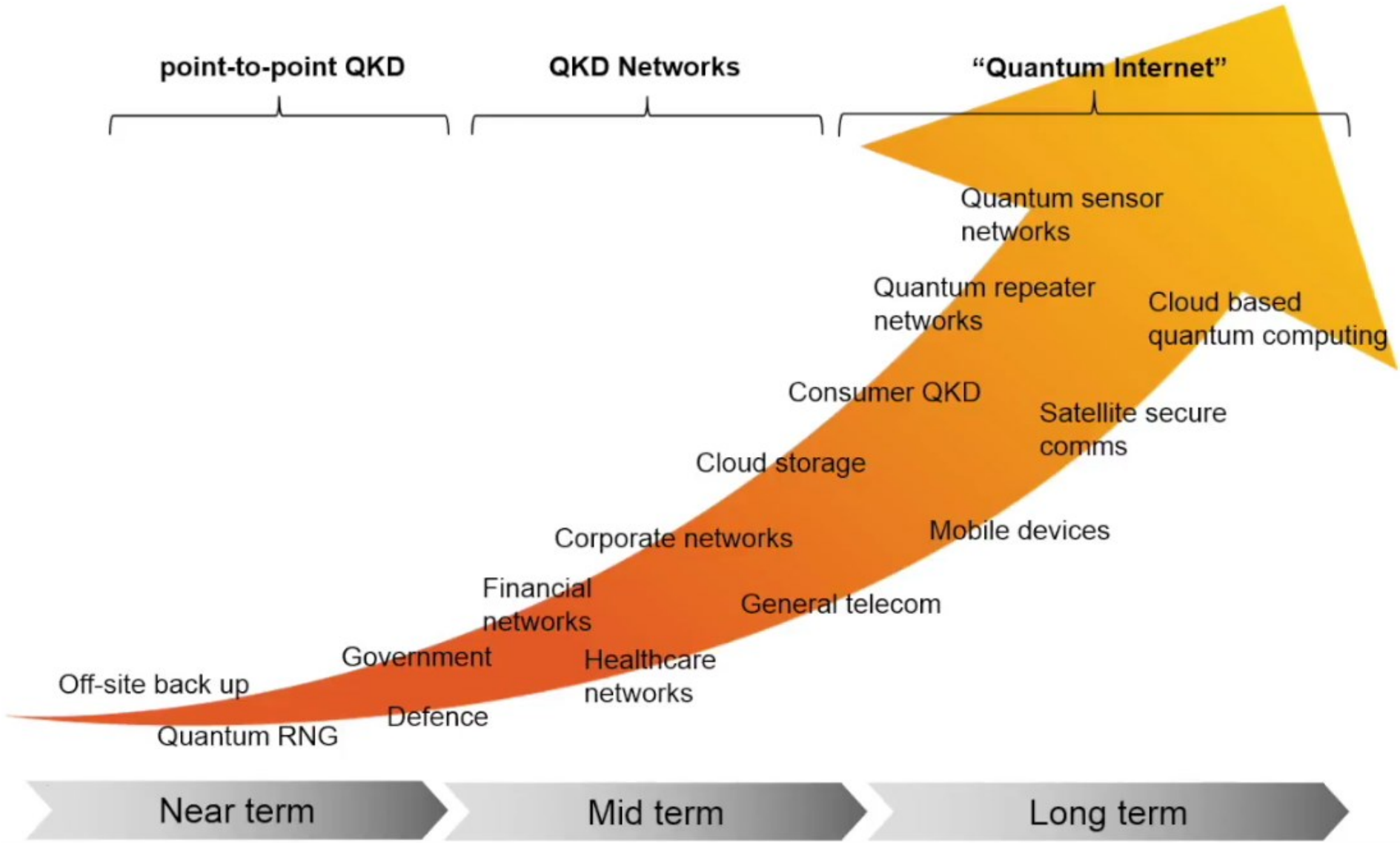
- Quantum mechanics is not correct: very unlikely
- The system under use is not behaving according to the theory: quite likely, needs to be characterized
- Photon source is not working in a single photon mode: possible
- Physical access to the transmitter is always dangerous
- Crosstalk or fiber listening impossible
- Quantum repeaters need to secured, needed after every 100 km?
- Detectors always a problem, APD’s can be driven into linear mode
- Long distances…?

True Random Number Generatorbased on Quantum Physics

- Physical Random Number Generator exploiting a phenomenon described by quantum physics:
- Provably random



Applications



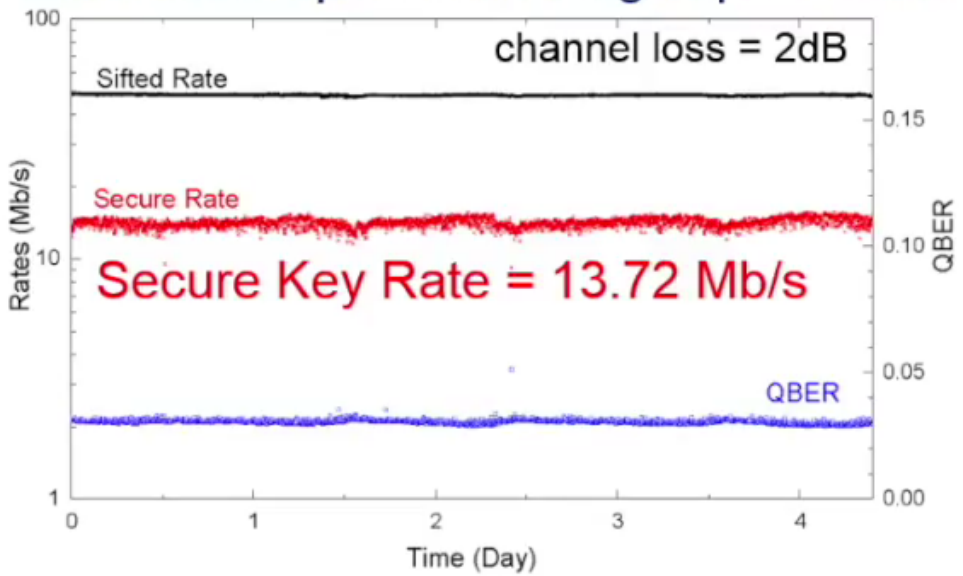
Quantum Technologies: Blackett Review, GO Science, Nov 16.

Overcoming the Processing Bottleneck

First 10 Mb/s QKD System

- Room temperature self-differencing APD detectors
- High photon throughput sifting electronics (250 Mc/s)
- Hardware based error correction and privacy amplification (> 100 Mc/s)

continuous operation of high speed QKD

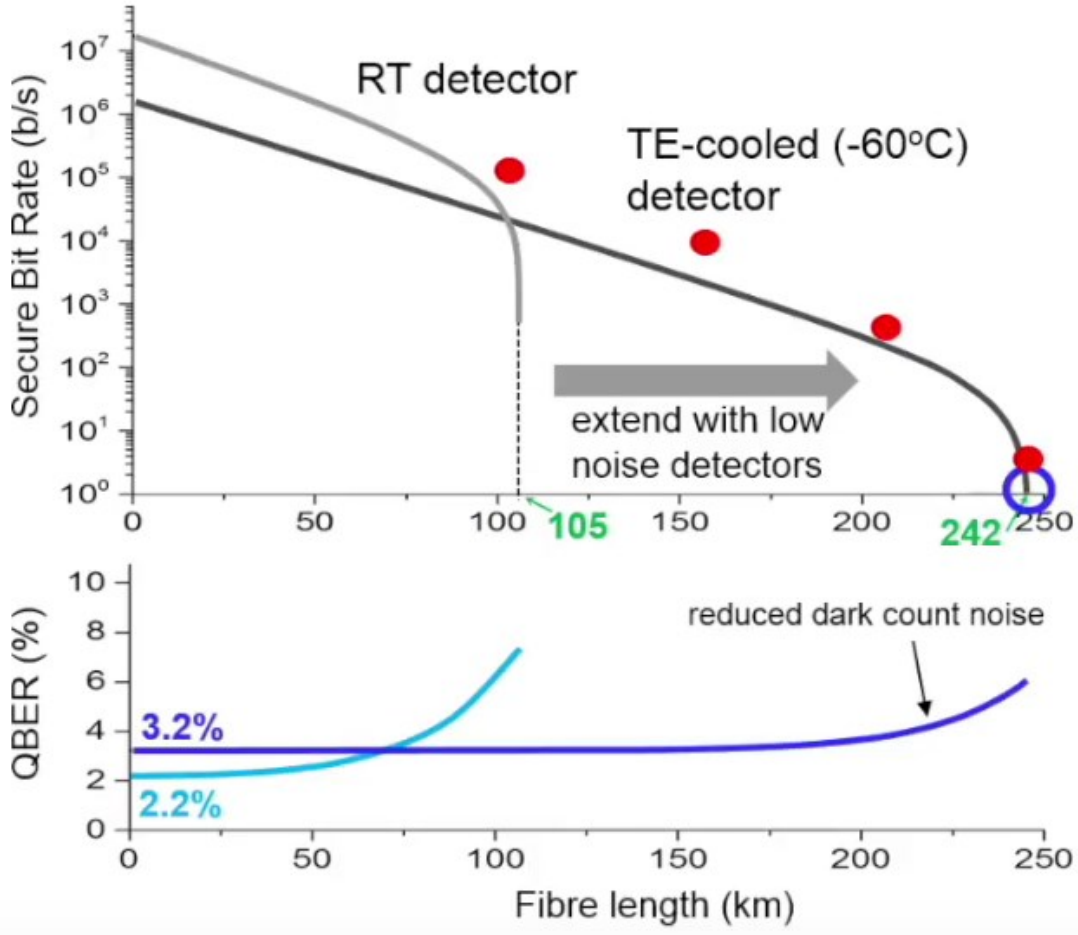


Further details

- Yuan et al, talk Th12 (Thurs, 9.35am)
- Demonstration during lab tour (Tues, 2pm)

Range of a Single QKD Link

- Extend range of QKD system by thermo-electric cooling SD-APD detector (-60°C)
- Detector dark count rate reduced to ~ 10c/s



- Reduced dark count noise extends range of *practical* QKD to 240 km

- Expt. points (●) use detector temp optimized for each distance

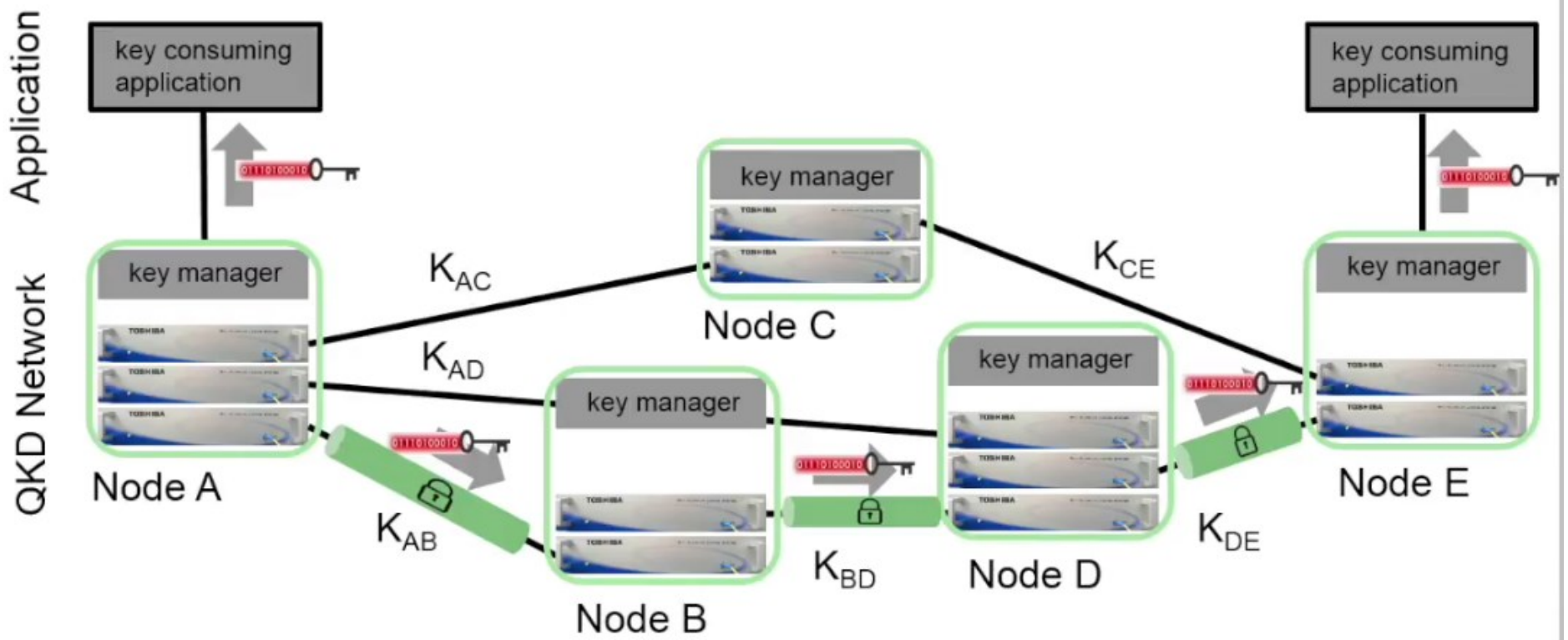
  Frohlich et al, *Optica* **4**, 163 (2017)

  See also Lim et al (Geneva), *Nat. Phot.* **9**, 163 (2015) for COW protocol

- Even longer range possible with superconducting detectors
- USTC reported 404km using MDI-QKD, superconducting detectors and ultra-low loss fibre.

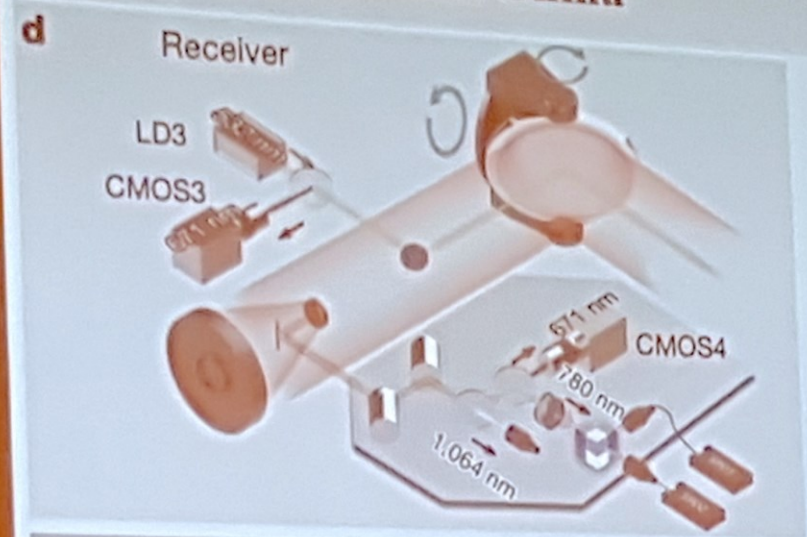
Trusted Node Networks

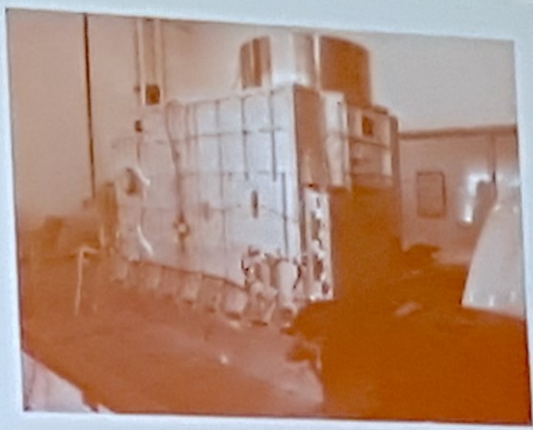
- Deliver *application keys* between any two nodes on network
  - Using key relay (QKD + OTP tunnels for application key)

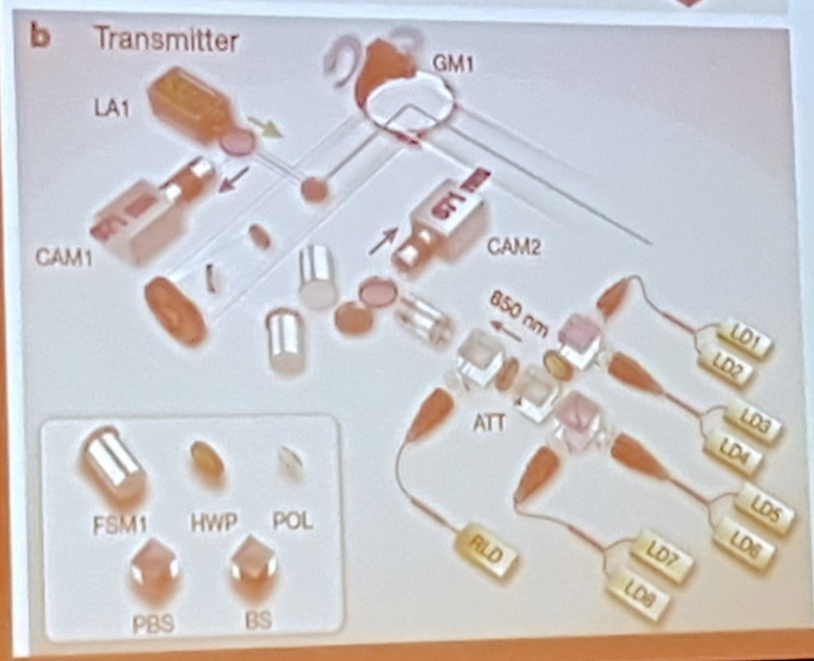


Chengzhi Peng

Quantum Satellite in China

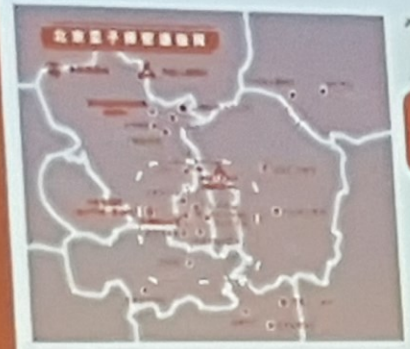






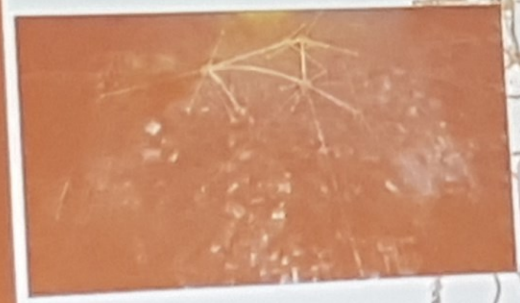
- ☑ 532nm beacon and synchrotron laser source
- ☑ 850nm synchrotron laser source
- ☑ 850nm decoy state source
- ☑ 671nm beacon laser detector
- ☑ 1064nm synchrotron laser detector
- ☑ 780nm quantum signal detector

Challenge of global quantum network -- Fiber network



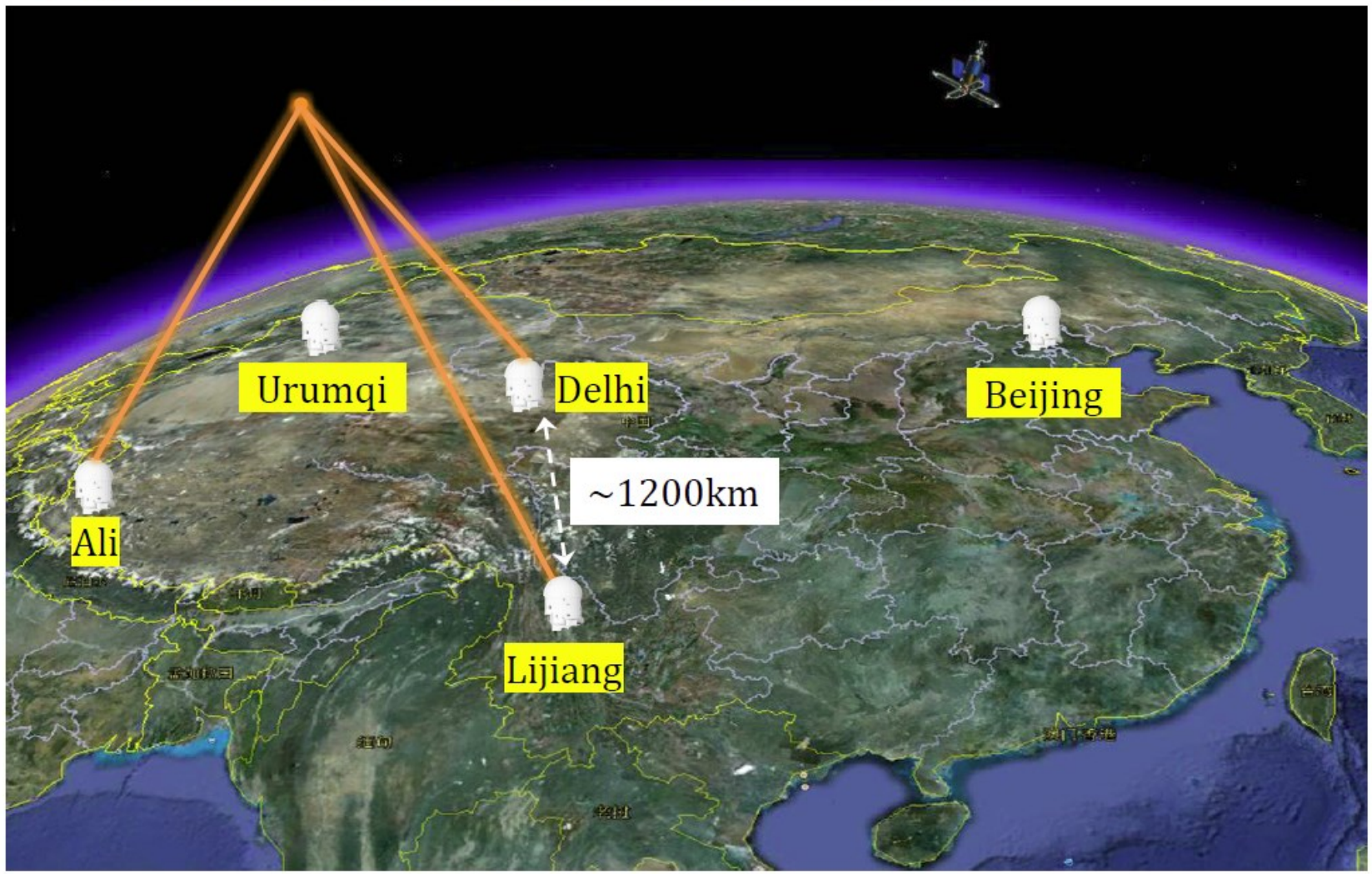
量子网络
CAS QUANTUMNET

国盾量子
QuantumCTek

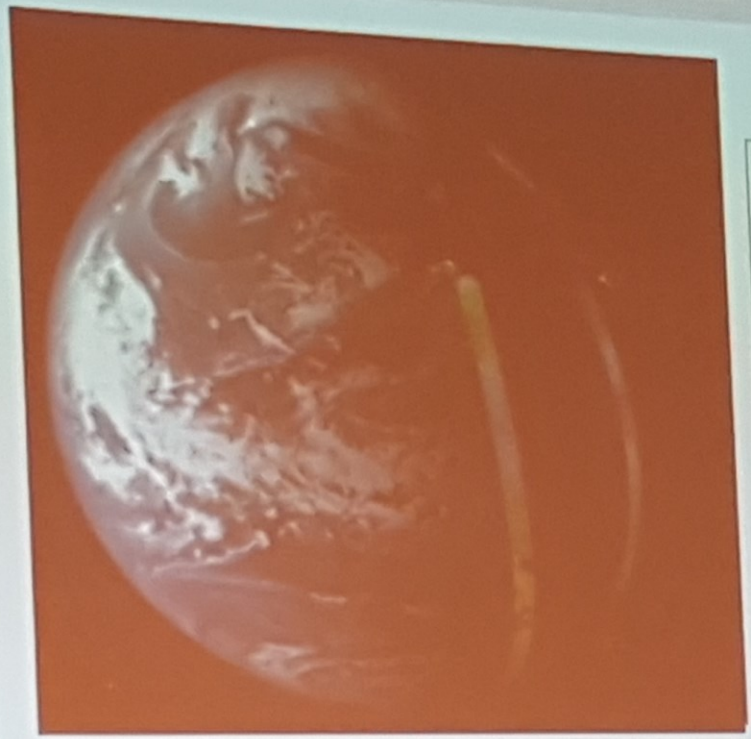


China's Quantum Experiments Plan in Space

- High-rate QKD between satellite and ground
- Quantum entanglement distribution from satellite, test of Bell's inequality over macro-scale
- Quantum teleportation between satellite and ground



Challenge of global quantum network



- Experiment time is ~ 6 minutes for each pass
- Coverage range is about 500km (Radius)
- Have to be in the shadow of earth
- Weather condition affects

What is a quantum computer?

- 1) In therms of hardware a device that is well-protected from the environment by freezing it to almost absolute zero temperature in a magnetically shielded environment. They are also relatively big.

Typical cryostat that creates millikelvin temperatures inside the chamber. Bluefors is a Finnish company, cost around 300k€ - 650 k€ depending on the number of wires.

IBM expects to improve quantum computers in part by making them much larger. This more spacious refrigeration chamber will to house them.

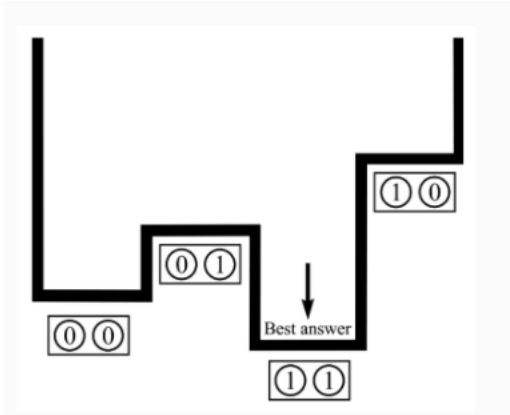
IBM Research

What is meant by annealing quantum computer? (DWave)

Quantum annealing simply uses quantum physics to find low-energy states of a problem and therefore the optimal or near-optimal combination of elements.

The challenge is that the problem and the data need to be mapped to the potential landscape, but we need only a rather good result for making big decisions, the perfect tedious calculation only takes time and costs money without giving any more significantly better information. => fast but robust cost-effective results good enough for many purposes!

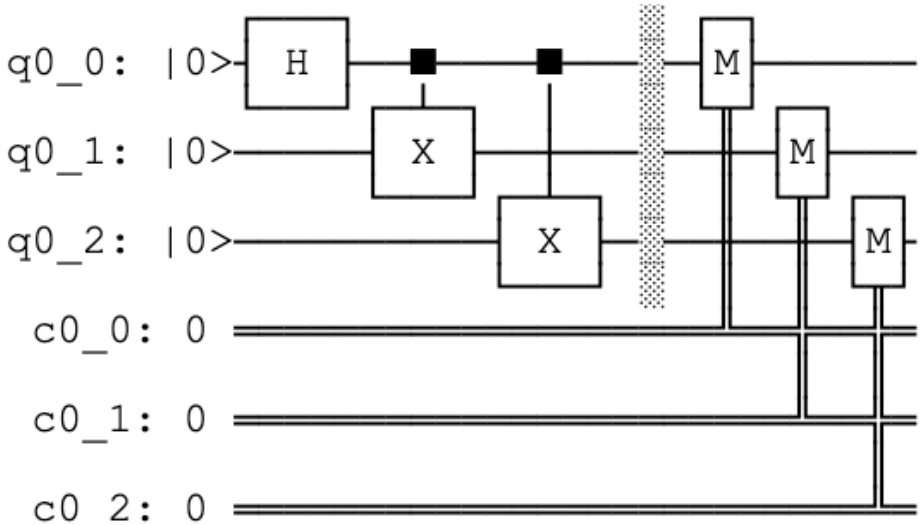
Think of snow starting to melt on the Alps, first water will flow into the local minimum and only finally to the bottom of the valley, the intermediate valley can already be quite a good solution and we get it much faster than the global final result!!!



Quantum bits: qubits

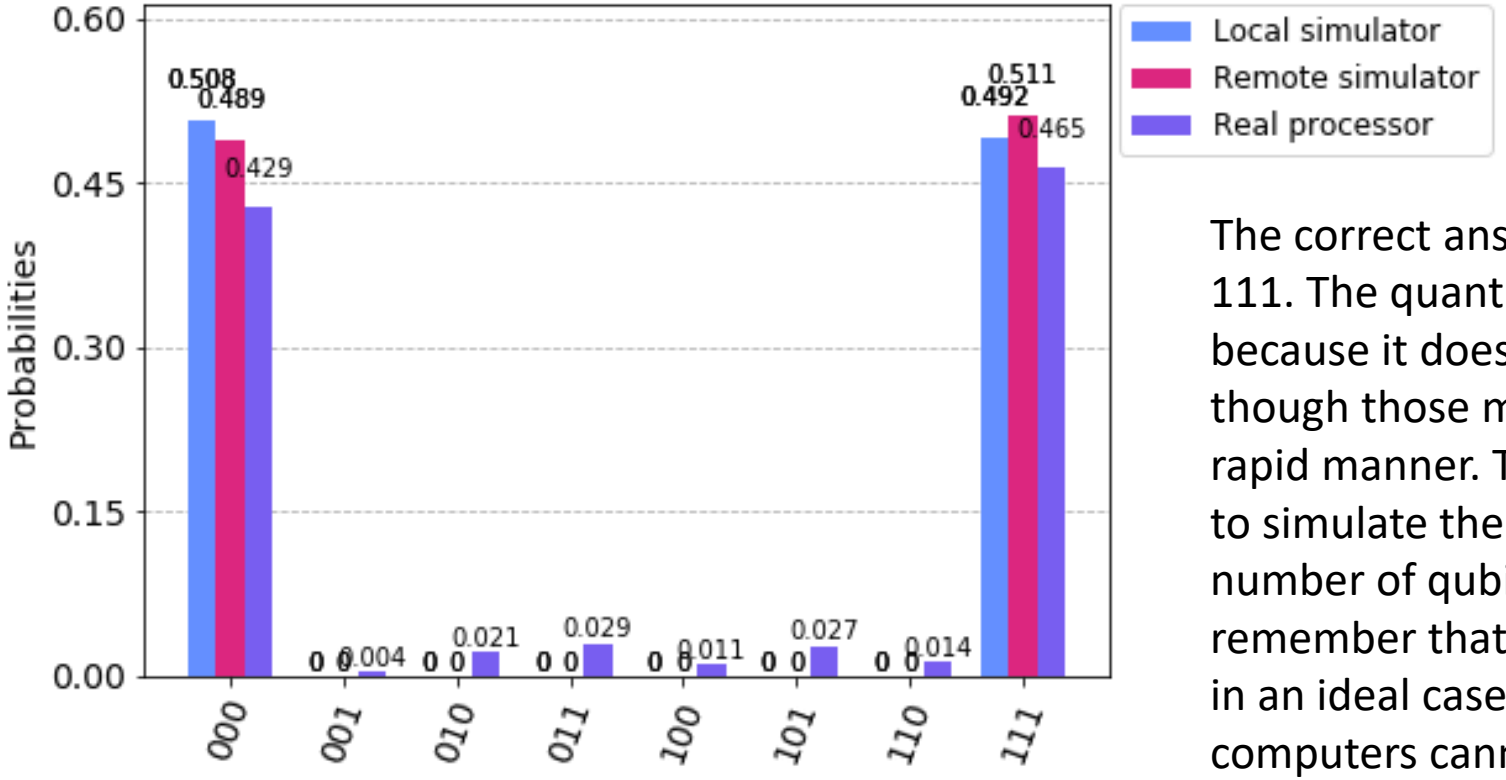
$$|\psi\rangle = a|0\rangle + b|1\rangle$$

This is one qubit, looks actually quite easy, but the secret is that it is not only in state 0 or in state 1 but in this kind of superposition, in a mixture state. a and b are real numbers.



This is an example of a very simple quantum code in a graphical representation, each horizontal line is one qubit, time flows from left to right, q0's are quantum bits and c0's are classical bits into which the quantum bits are read in the end of this super short program. H and X are different quantum gates, that can be also mathematically represented. M means measurement of the qubit state. So we start by three qubits and transfer the results to 3 classical bits. As long as we do not measure the quantum system it evolves in its own world (qubits + gates) without anybody hopefully disturbing it. When the measurement is done the qubit loses its quantum behaviour (coherence). However, the code can be restarted and run hundreds (thousands) of times.

Results of the previous code (less than 50 lines of python code):



The correct answers are the sequences 000 and 111. The quantum machine makes some errors, because it does not perform (yet) ideally, even though those machines become improved in a rapid manner. The classical machines can be used to simulate the quantum machine, when the number of qubits is rather small. We should remember that a quantum machine corresponds in an ideal case to 2^n classical bits. So big quantum computers cannot any more be simulated by classical machines. Remember: $2^{10} = 1024$, but $2^{53} = 10^{16}$ = ten million billion !!!

A classical computer solves way better than a real quantum computer this very simple problem.

What's the fuzz of all quantum things?

Are we saying that quantum gadgets are obviously useless?

Obviously, a quantum algorithm needs to be run many times in order to collect statistical result which at least so far contains some experimental noise.

Noise levels will go down as technologies are improved in the future

Finally, quantum computing has a different philosophy, results are statistical but computation is massively parallel

A kind of rule of thumb is that a quantum register of N qubits may be compared to a classical one so that 2^N equals the amount of corresponding classical bits

If for example N= 15, we get huge numbers…

IBM's quantum computing roadmap

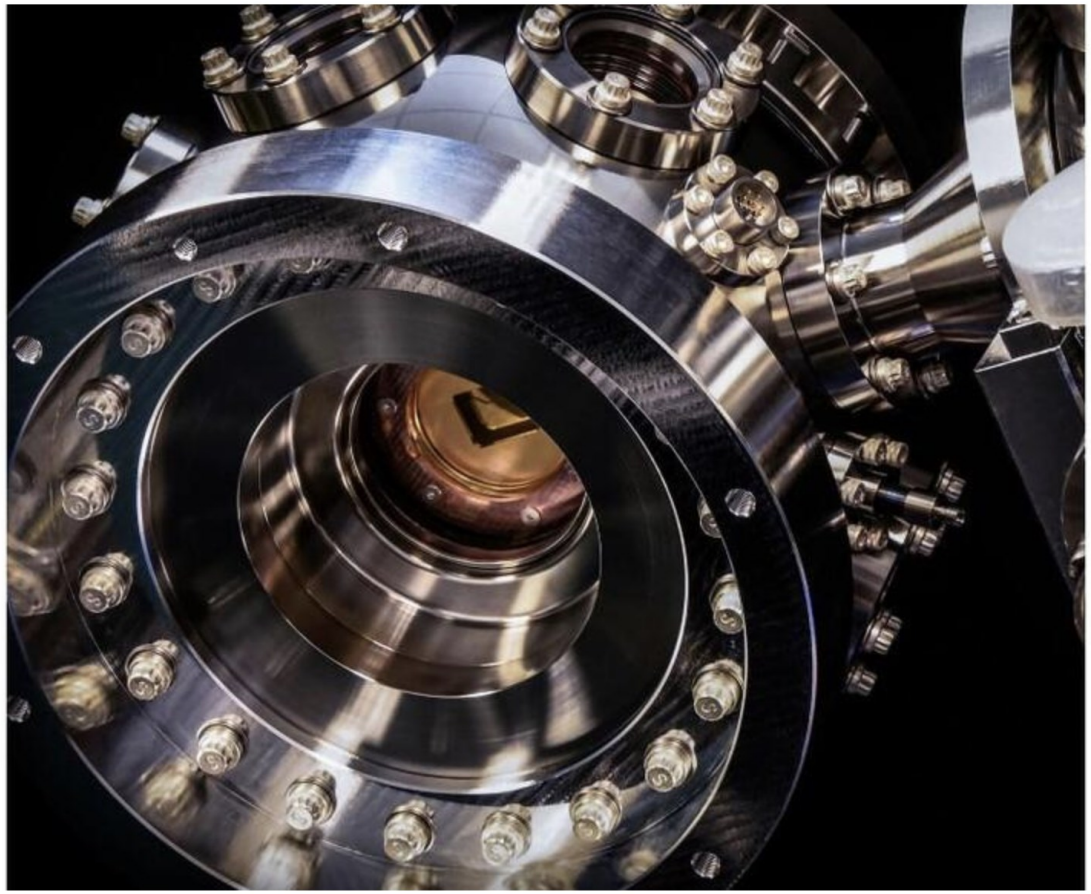
IBM Research

IBM tries to fulfill its promise to double every year its quantum volume, a measurement that captures not just the qubit total but also how capable the qubits are at performing a computation

Honeywell claims to surpass IBM with the world's fastest quantum computer

by **Macy Bayern** in **Innovation**
on June 19, 2020, 8:22 AM PST

The new device boasts a quantum volume of 64, double that of the industry alternative, the company says.



Inside Honeywell quantum computer chamber.

Honeywell declared on Thursday that it has the world's highest-performing quantum computer. Touting a quantum volume of 64—the metric used to convey the effectiveness of a quantum computer—the device is twice as powerful as IBM's supercomputer, which was the former industry leader.

SEE: Managing AI and ML in the enterprise 2020: Tech leaders increase project development and implementation (TechRepublic Premium)

The industrial giant pledged in March to have the most powerful quantum computer by the middle of 2020, fulfilling that promise only three months later.

The company also said in March that it would improve the performance of its quantum computers by a factor of 10 every year for the next five years, which means the computer could be 100,000 faster in 2025.

"What makes our quantum computers so powerful is having the highest quality qubits, with the lowest error rates," said Tony Uttley, president of Honeywell Quantum Solutions, in a press release. "This is a combination of using identical, fully connected qubits and precision control."

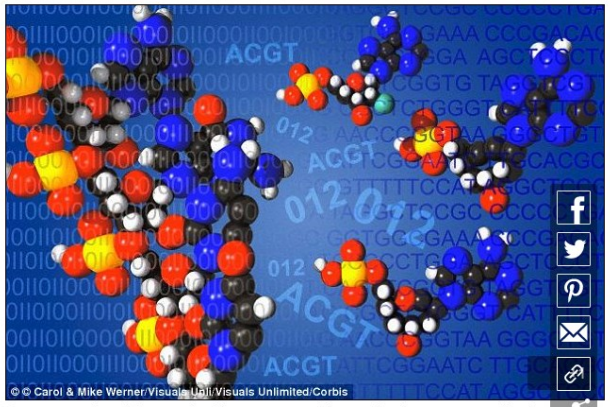
More about Innovation

- Automation, it's what's for dinner: "Robot-run" restaurant opens in China
- The future of farming: Building an agtech center in the heart of the Bluegrass State
- Augmented reality for business: Cheat sheet
- The Internet of Wild Things: Tech and the battle against biodiversity loss and climate change (PDF)

Where does the Big data come from?

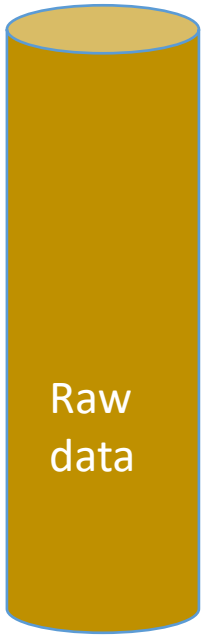
- Modern technology is gathering lots of all kinds of data.
- This is enormous amount of bits and they remain largely unprocessed but giving hugh promises to really big business.

Scanners, web crawlers, human genome, cameras,…



Human genetic code is contained in a sequence of four molecules, represented by letters A, T, G and C. Each can be encoded with two bits of binary information - 00, 10, 11, 01. When multiplied by 6 billion letters, and divided by eight bits per byte, a physician claims the entire code contains just 1.5GB of data

Analyzing huge datasets can help us identifying surprising patterns and regularities of incredible economical value.



"Data is being generated at the speed of business"
"Data grows fast"
"Companies do not know what to do with their own data"

More analyzed/engineered data/Extrapolation

Data for decision making

Leadership trust level goes up with using the big data

- Flexibility a big issue: who has access to what data
- In an ideal case self-service should be possible inside the company
- Use of data should benefit the customer, better service in all aspects without losing safety
- New technologies go beyond any human performance: machine learning, quantum computation
- Big data tells the story of the company

The challenge:

- A word quantum computer refers to the general theory developed in the beginning of 1900's but one can find different physical systems that follow the same universal theory
- one can use
  - superconducting circuit based machines
  - annealing machines
  - also other systems exist
- All these machines are mutually totally different and are best also for different kinds of problems

Circuit-based quantum processors [edit]

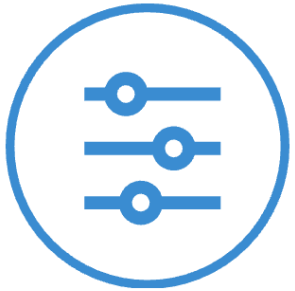
These QPUs are based on the quantum circuit and quantum logic gate-based model of computing.

Manufacturer	Name/Codename/Designation	Architecture	Layout	Socket	Fidelity	Qubits	Release date
Google	N/A	Superconducting	N/A	N/A	99.5%[1]	20 qb	2017
Google	N/A	Superconducting	7×7 lattice	N/A	99.7%[1]	49 qb[2]	Q4 2017 (planned)
Google	Bristlecone	Superconducting	6×12 lattice	N/A	99% (readout) 99.9% (1 qubit) 99.4% (2 qubits)	72 qb[3][4]	5 March 2018
Google	Sycamore	Nonlinear superconducting resonator	N/A	N/A	N/A	54 transmon qb 53 qb effective	2019
IBM	IBM Q 5 Tenerife	Superconducting	bow tie	N/A	99.897% (average gate) 98.64% (readout)	5 qb	2016[1]
IBM	IBM Q 5 Yorktown	Superconducting	bow tie	N/A	99.545% (average gate) 94.2% (readout)	5 qb	
IBM	IBM Q 14 Melbourne	Superconducting	N/A	N/A	99.735% (average gate) 97.13% (readout)	14 qb	
IBM	IBM Q 16 Rüschlikon	Superconducting	2×8 lattice	N/A	99.779% (average gate) 94.24% (readout)	16 qb[5]	17 May 2017 (Retired: 26 September 2018)[6]
IBM	IBM Q 17	Superconducting	N/A	N/A	N/A	17 qb[5]	17 May 2017
IBM	IBM Q 20 Tokyo	Superconducting	5x4 lattice	N/A	99.812% (average gate) 93.21% (readout)	20 qb[7]	10 November 2017
IBM	IBM Q 20 Austin	Superconducting	5x4 lattice	N/A	N/A	20 qb	(Retired: 4 July 2018)[6]
IBM	IBM Q 50 prototype	Superconducting	N/A	N/A	N/A	50 qb[7]	
IBM	IBM Q 53	Superconducting	N/A	N/A	N/A	53 qb	October 2019
Intel	17-Qubit Superconducting Test Chip	Superconducting	N/A	40-pin cross gap	N/A	17 qb[8][9]	10 October 2017
Intel	Tangle Lake	Superconducting	N/A	108-pin cross gap	N/A	49 qb [10]	9 January 2018
Rigetti	8Q Agave	Superconducting	N/A	N/A	N/A	8 qb	4 June 2018[11]
Rigetti	16Q Aspen-1	Superconducting	N/A	N/A	N/A	16 qb	30 November 2018[11]
Rigetti	19Q Acorn	Superconducting	N/A	N/A	N/A	19 qb[12]	17 December 2017
IBM	IBM Armonk[13]	Superconducting	Single Qubit	N/A	N/A	1 qb	16 October 2019
IBM	IBM Ourense[13]	Superconducting	T	N/A	N/A	5 qb	03 July 2019
IBM	IBM Vigo[13]	Superconducting	T	N/A	N/A	5 qb	03 July 2019
IBM	IBM London[13]	Superconducting	T	N/A	N/A	5 qb	13 September 2019
IBM	IBM Burlington[13]	Superconducting	T	N/A	N/A	5 qb	13 September 2019
IBM	IBM Essex[13]	Superconducting	T	N/A	N/A	5 qb	13 September 2019

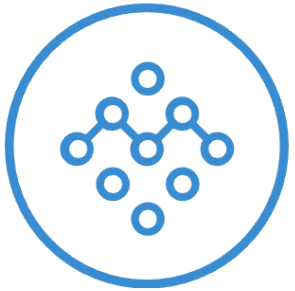
250+

User-developed early quantum applications on D-Wave systems, including airline scheduling, election modeling, quantum chemistry simulation, automotive design, preventative healthcare, logistics, and much more.

Optimization



Machine Learning



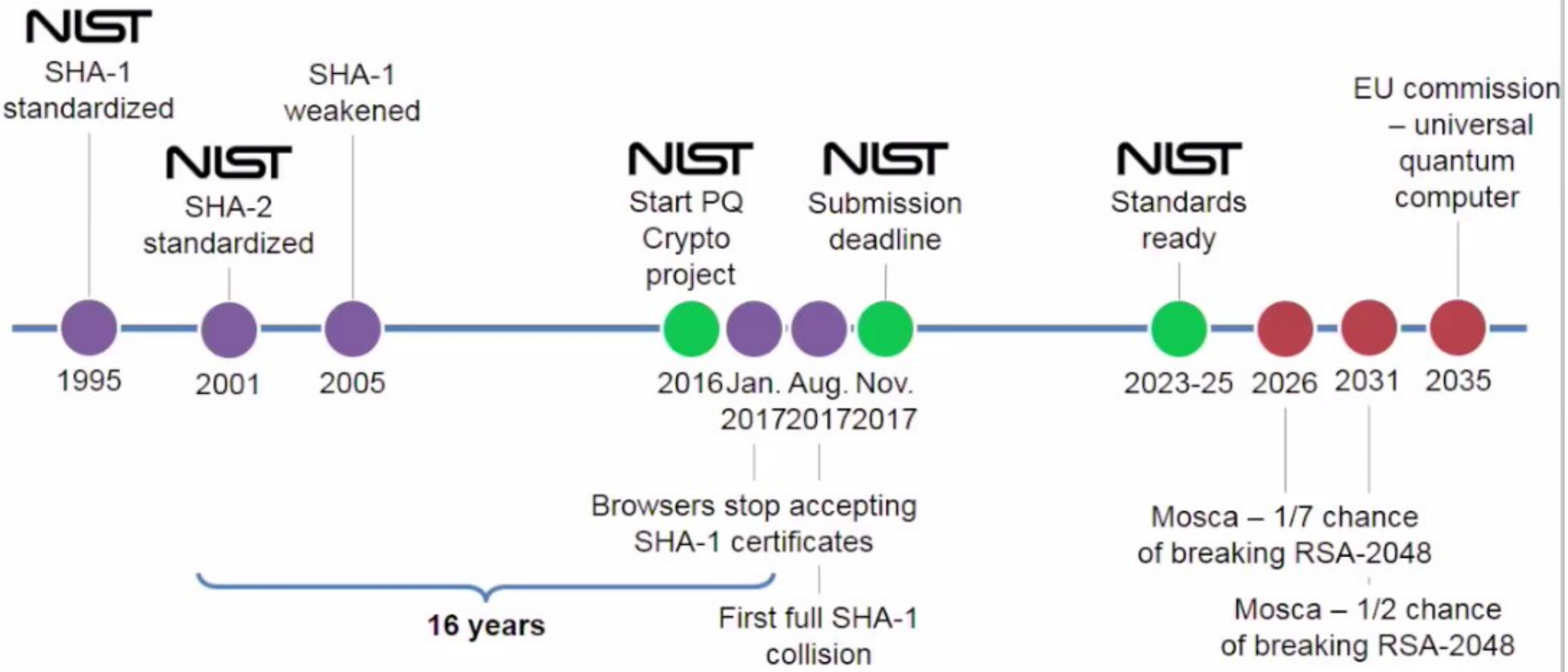
Materials Science

Annealing quantum processors [edit]

These QPUs are based on quantum annealing.

Manufacturer	Name/Codename/Designation	Architecture	Layout	Socket	Fidelity	Qubits	Release date
D-Wave	D-Wave One (Ranier)	Superconducting	N/A	N/A	N/A	128 qb	11 May 2011
D-Wave	D-Wave Two	Superconducting	N/A	N/A	N/A	512 qb	2013
D-Wave	D-Wave 2X	Superconducting	N/A	N/A	N/A	1152 qb	2015
D-Wave	D-Wave 2000Q	Superconducting	N/A	N/A	N/A	2048 qb	2017
D-Wave	D-Wave Advantage	Superconducting	N/A	N/A	N/A	5000 qb	2020

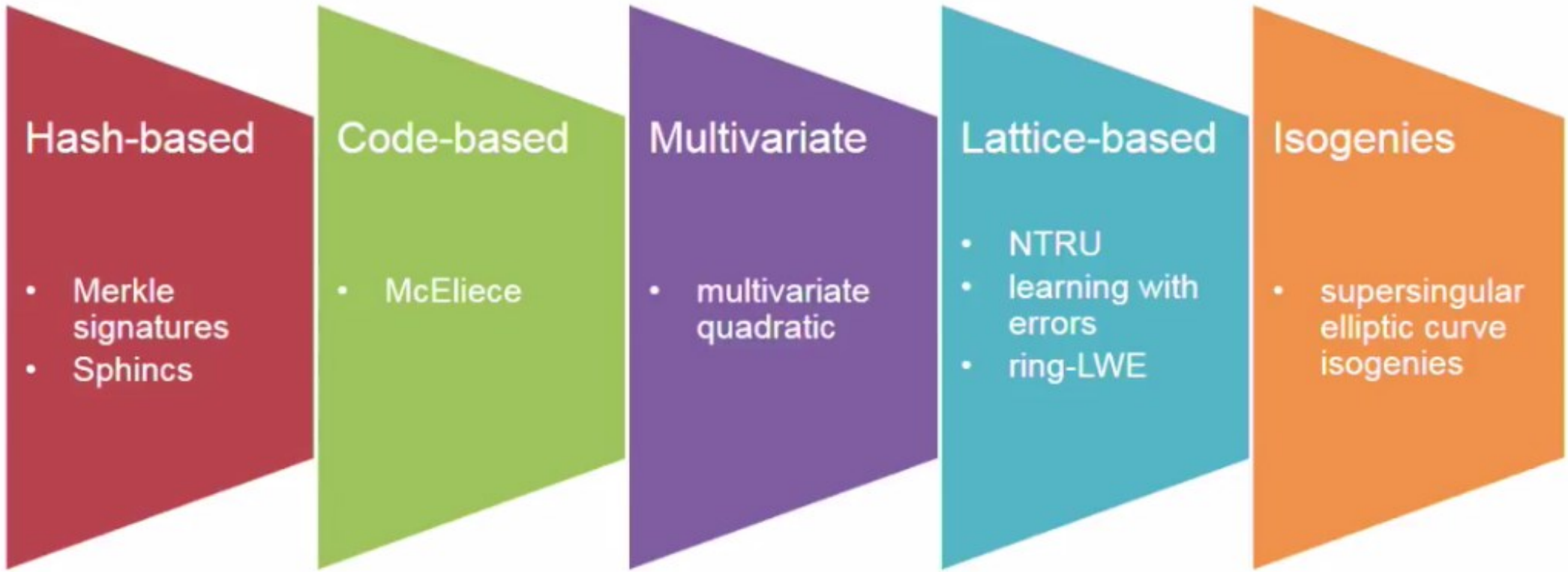
Timeline


NIST
SHA-1 standardized
1995
NIST
SHA-2 standardized
2001
SHA-1 weakened
2005
16 years
NIST
Start PQ Crypto project
2016
Jan. 2017
Browsers stop accepting SHA-1 certificates
Aug. 2017
First full SHA-1 collision
NIST
Submission deadline
Nov. 2017
NIST
Standards ready
2023-25
2026
Mosca – 1/7 chance of breaking RSA-2048
2031
Mosca – 1/2 chance of breaking RSA-2048
EU commission – universal quantum computer
2035

Post-quantum crypto

a.k.a. quantum-resistant algorithms

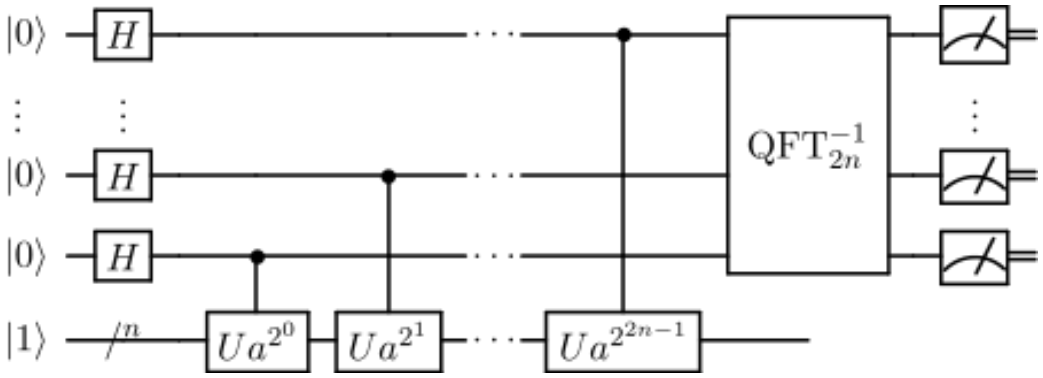
Classical crypto with no known exponential quantum speedup



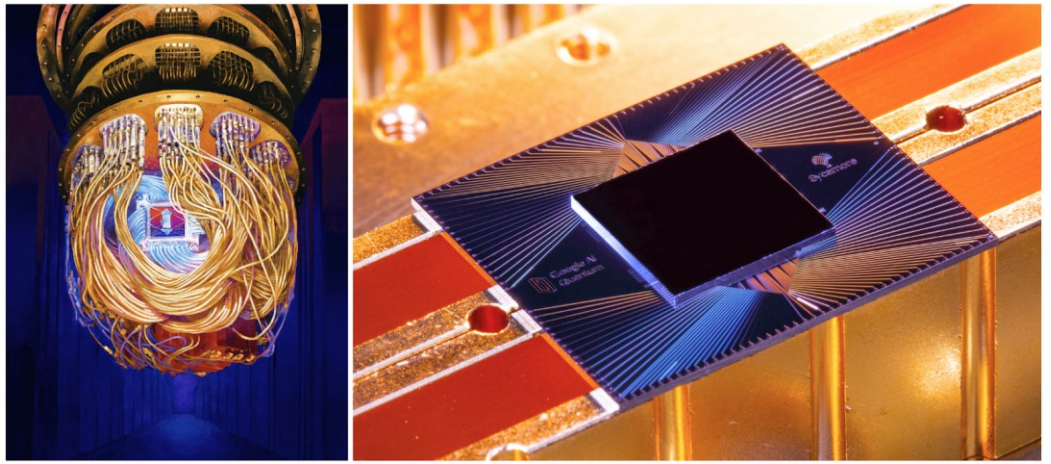
Post Quantum Cryptography

- Quantum computers can efficiently solve **integer factorization** and **discrete logarithm** problems with Shor's algorithm.
- Safety of popular crypto protocols (e.g. RSA, Diffie-Hellman) under threat, when large quantum computers become available.
- Currently, push to develop **quantum-safe** cryptosystems based on mathematical problems hard even for quantum computers.

Circuit representation of Shor's algorithm



Google's Sycamore quantum processor



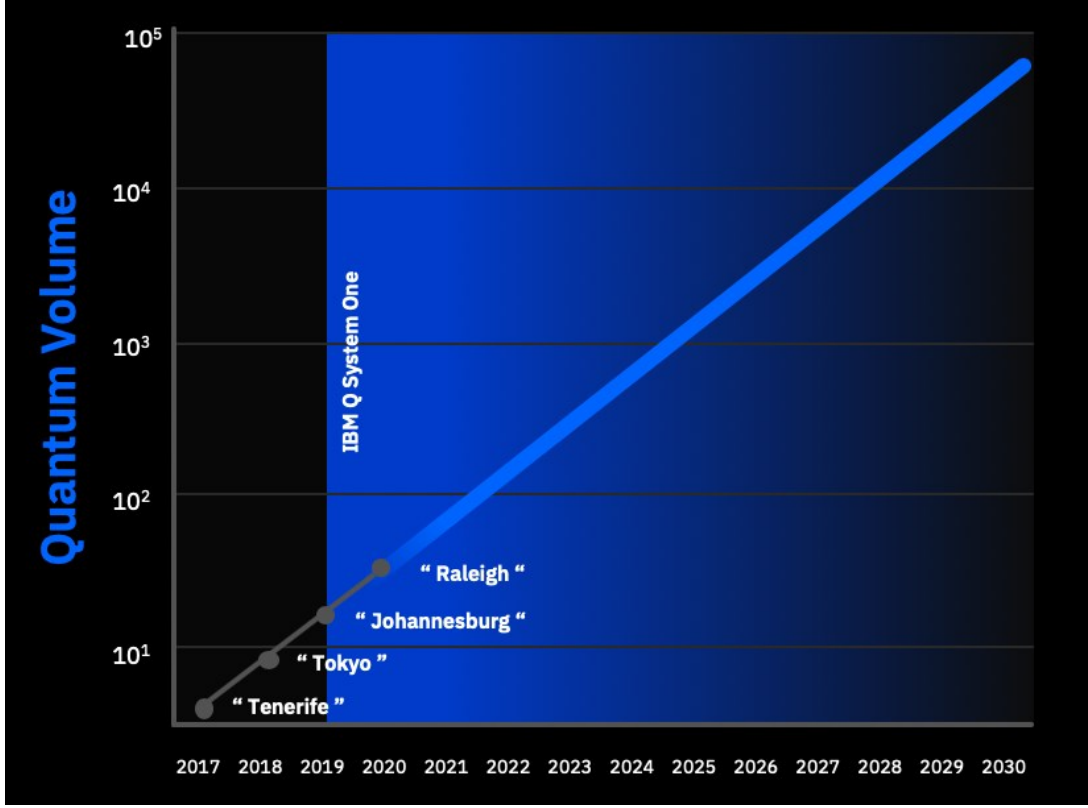
Key research questions

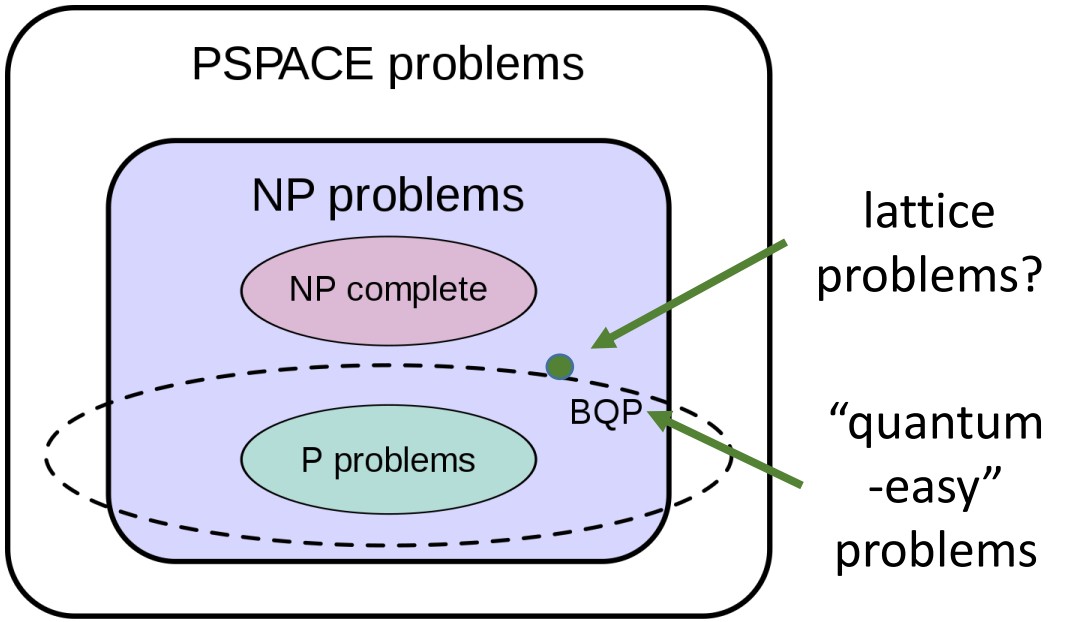
1. When will the current cryptosystems break?

- Recent estimates suggest that breaking 2048 bit RSA takes 20 million physical qubits. (arXiv:1905.09749)
- **Quantum volume** of processors grows exponentially at the moment. Quantum Moore's law?
- We will develop up-to-date estimates for the **future development of quantum computers & software.**
  ⇒ **Timeline of the threat.**

2. How safe are the proposed PQC protocols?

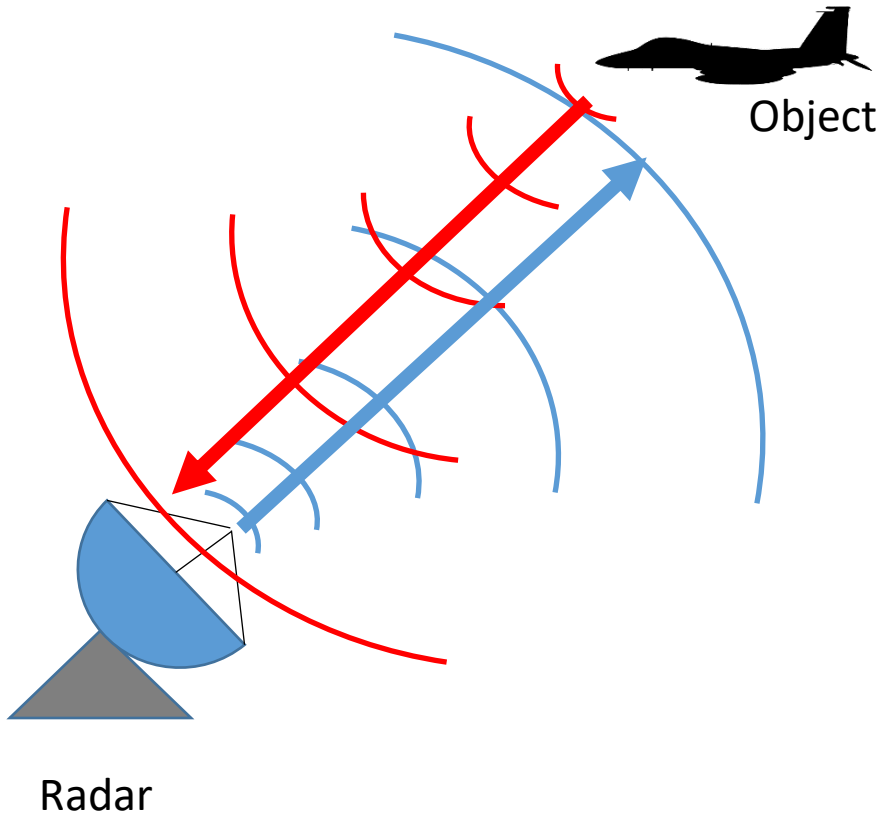
- Protocols based on various mathematical problems. Most succesful ones based on **lattice problems**.
- **Subexponential** quantum algorithms known for some lattice problems. (arXiv:1112.3333)
- One solution could be **automated quantum algorithm discovery** to PQC problems. (arXiv:1812.04458)
  ⇒ **Assess the optimality of current algorithms.**
  ⇒ **Find new (better?) algorithms for PQC problems.**





What is meant by Backscatter Communication?

- **Backscatter** – reflection of EM-waves back to the position where they are coming from.
- **Quantum radar** makes use of quantum entanglement for detecting low reflectivity objects under noisy and lossy environments
- **Quantum backscatter communication:** Information may be transmitted by transforming the signal in some way while it is being reflected back. Entanglement may be used to reduce errors, and make the communication secure against evesdropping.



What is quantum entanglement?

- Tangle/entangle – twisting together/ tie / intertwine, etc..
- **Quantum entanglement** - strong correlation between the two separated photons (distance independent, in principle)
- Given an **entangled pair of photons**, by performing a measurement on one of the photons gives you the ability to predict the value of the related property on the other photon with 100% certainty.
- For example, we know the wavelength, time window and polarization state of the returning photon after detecting the other photon of the entangled pair.

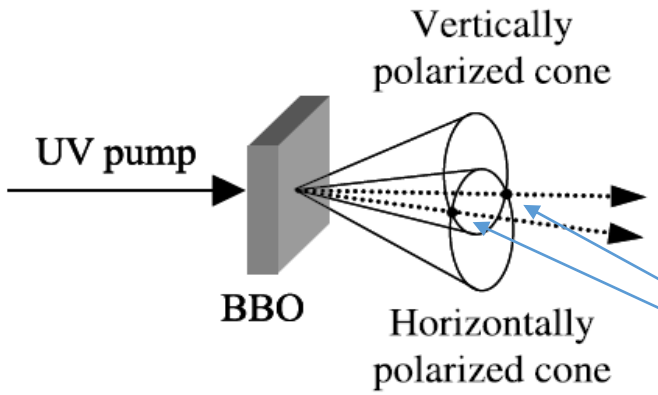
Creating entangled photons

There are two well-known methods to create photon pairs with a mutual quantum correlation (entanglement) in nonlinear optics.

Method 1: a pump UV laser shot into a physical crystal (e.g. barium borate)

Type II SPDC

4 Bell States



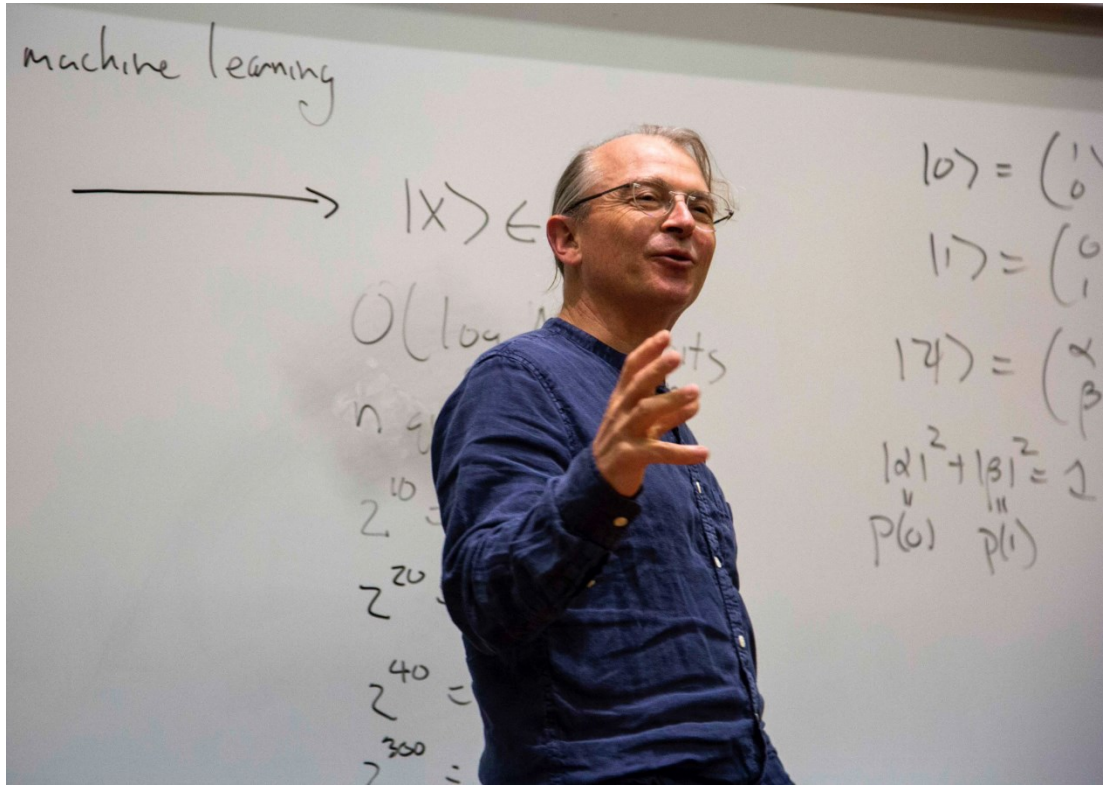
Positive correlation $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0_1, 0_2\rangle \pm |1_1, 1_2\rangle\right),$

Negative correlation $|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0_1, 1_2\rangle \pm |1_1, 0_2\rangle\right),$

- Conversion efficiency is low
- Highest efficiency confirmed is 4×10^{-6}
- In our system, the target is 10^5 photons/s/pm
- One needs to select the photons in **the intersection points** by pinholes, since in this case one does not know to which cone they were emitted, and thus they form of **superposition** of different possibilities.

- **Quantum illumination** was introduced by Prof. S. Lloyd (MIT) in the setting of detecting the presence of a low-reflective target in a noisy environment using entangled photons as probes.

[1] Lloyd, S.: Enhanced sensitivity of photodetection via quantum illumination. Science **321**, 1463–1465 (2008)



Applications

- Quantum secure communication
- Quantum radar
- Detection for cloaked objects
- Quantum imaging

Advantages

- Lower error probability
- Enhancement of signal-to-noise ratio
- Two-photon entanglement in ghost imaging improves the spatial resolution of an image.

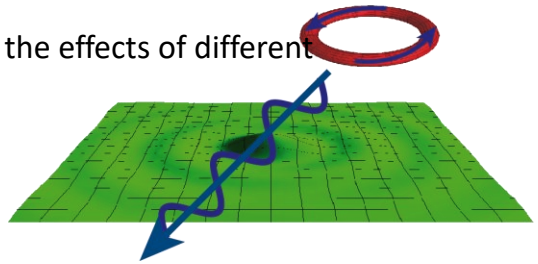
Quantum optical effects in quantum rings - Quantum information processing

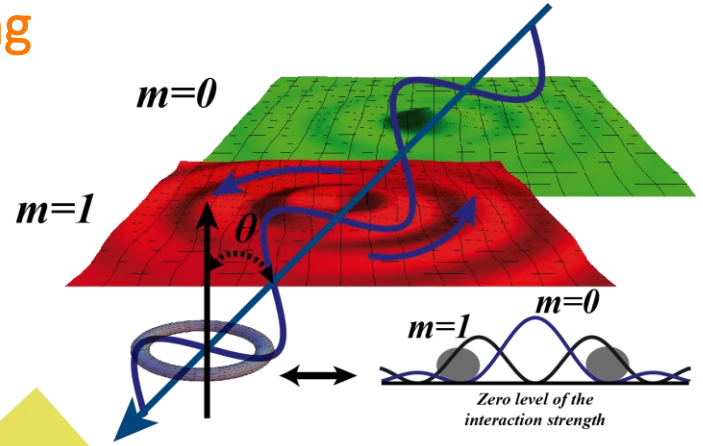
❖ Any optical plane wave consists of an infinite number of orbital angular momentum (OAM) modes:

$$e^{i\mathbf{q}\cdot\mathbf{r}} \propto \sum_{m=-\infty}^{\infty} J_m(q\sin(\theta)r_{||})e^{im\varphi}.$$

❖ Usually this is only a mathematical construction and the detection of individual OAM components is almost impossible

- In extremely small structures, only m=0 mode is effective.
- In large structures, the effects of different modes are mixed.





LIGHT-MATTER INTERACTION

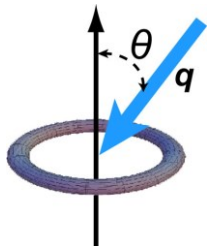
❖ Quantum rings are ideal for discrete detection of different m modes:

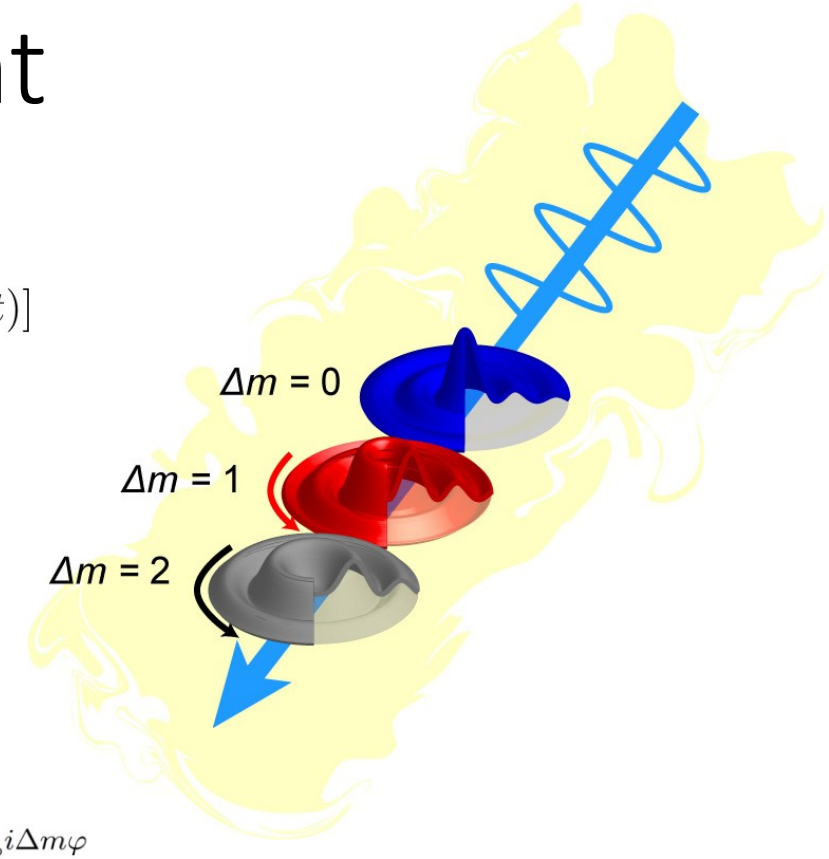
- Size can be large enough to allow $m\neq0$ modes to interact
- Volume is small enough to provide fully quantized spectrum
- Phys. Rev. B 84, 165317 (2011)

Decomposition of light

• Total angular momentum of light:

$$\boldsymbol{J}_f = \epsilon_0 \int d^3r \boldsymbol{r} \times [\boldsymbol{E}(\boldsymbol{r},t) \times \boldsymbol{B}(\boldsymbol{r},t)]$$





An expansion into cylindrical waves:

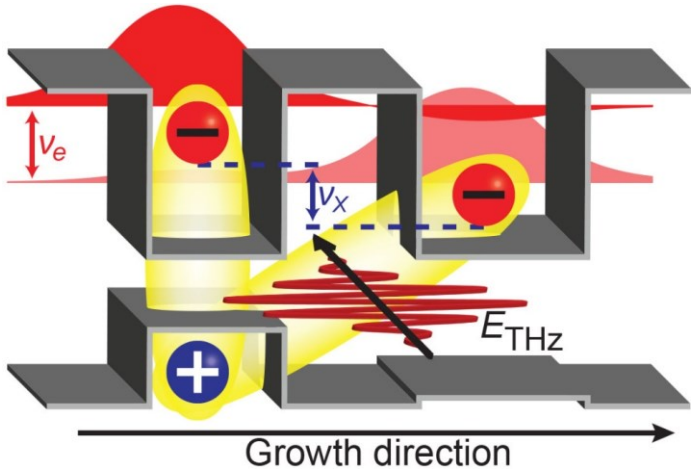
$$e^{i\boldsymbol{q}\cdot\boldsymbol{r}} = e^{iq_z z} \sum_{\Delta m=-\infty}^{\infty} i^{\Delta m} J_{\Delta m}(rq\sin\theta) e^{i\Delta m\varphi}.$$

PHYSICAL REVIEW B **84**, 165317 (2011)

Indirect interband optical transitions in a semiconductor quantum ring with submicrometer dimensions

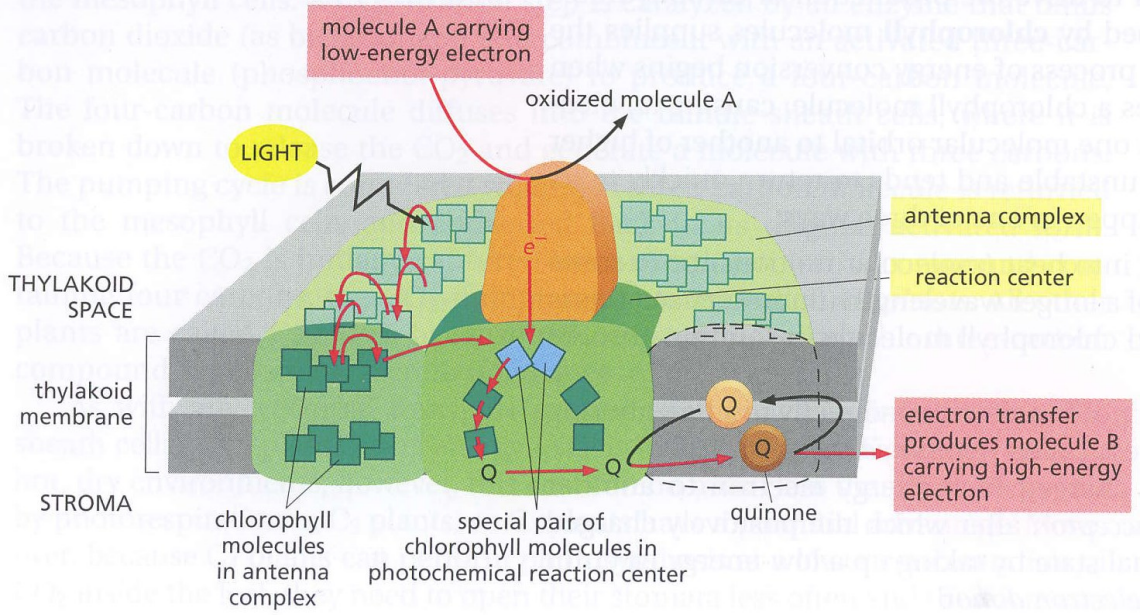
O. Vänskä,[1] M. Kira,[2] I. Tittonen,[1] and S. W. Koch[2]
[1]*Department of Micro- and Nanosciences, Aalto University, P.O. Box 13500, FI-00076 Aalto, Finland*
[2]*Department of Physics and Materials Sciences Center, Philipps-University Marburg, Renthof 5, D-35032 Marburg, Germany*
(Received 31 August 2011; published 12 October 2011; corrected 19 October 2011)

Tunneling of exitonic correlations (only)

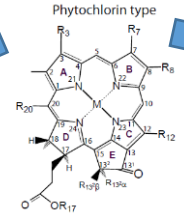


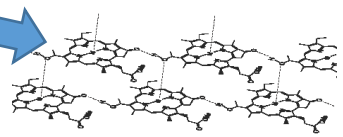
Coherent Terahertz Control of Vertical Transport in Semiconductor Heterostructures
O. Vänskä, I. Tittonen, S.W. Koch, and M. Kira, Physical Review Letters 114, 116802 (2015)

Photosynthetic process



Biomimicry

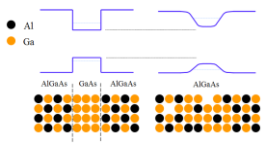




- molecular excitation
- decay channels
- stability
- losses & efficiency
- aggregation
- functionalization
- quantum effects

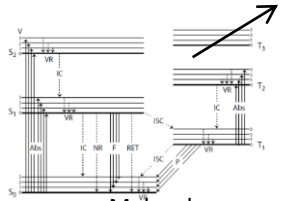
Epitaxial growth @ Micronova

Extraction of molecules, functionalization



quantum wells

Energetic matching



Molecular transitions

Charge transfer

devices

Thank you!