Chapter 1 - Introduction and Motivation

Jan Bouda

PV275 Quantum Programming

2019

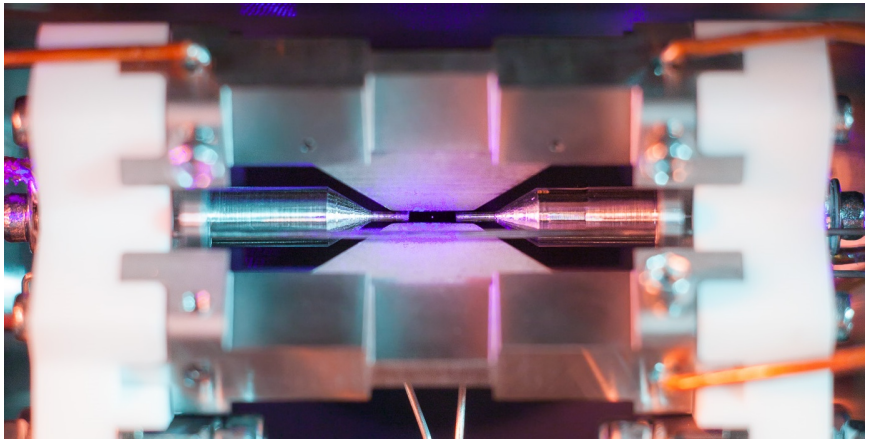
Part I

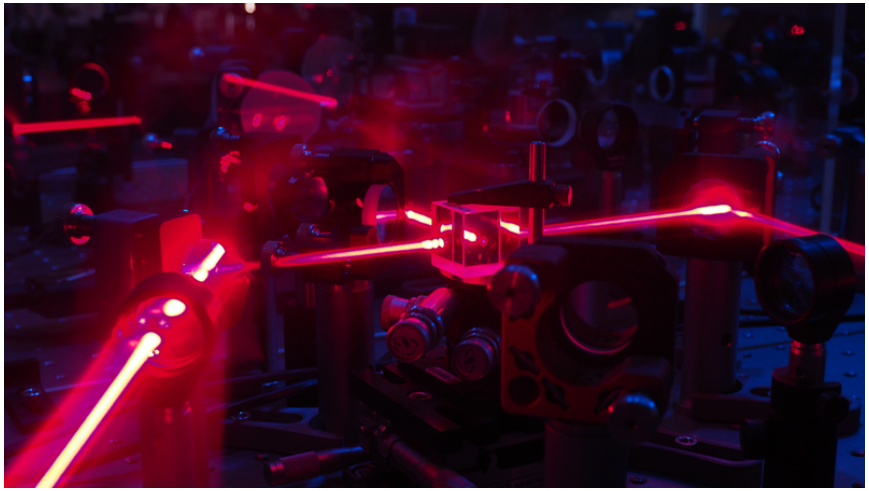
What is quantum information processing

Classical vs. Quantum computer

Classical computer

Quantum computer





Classical vs. Quantum computer

Classical computer

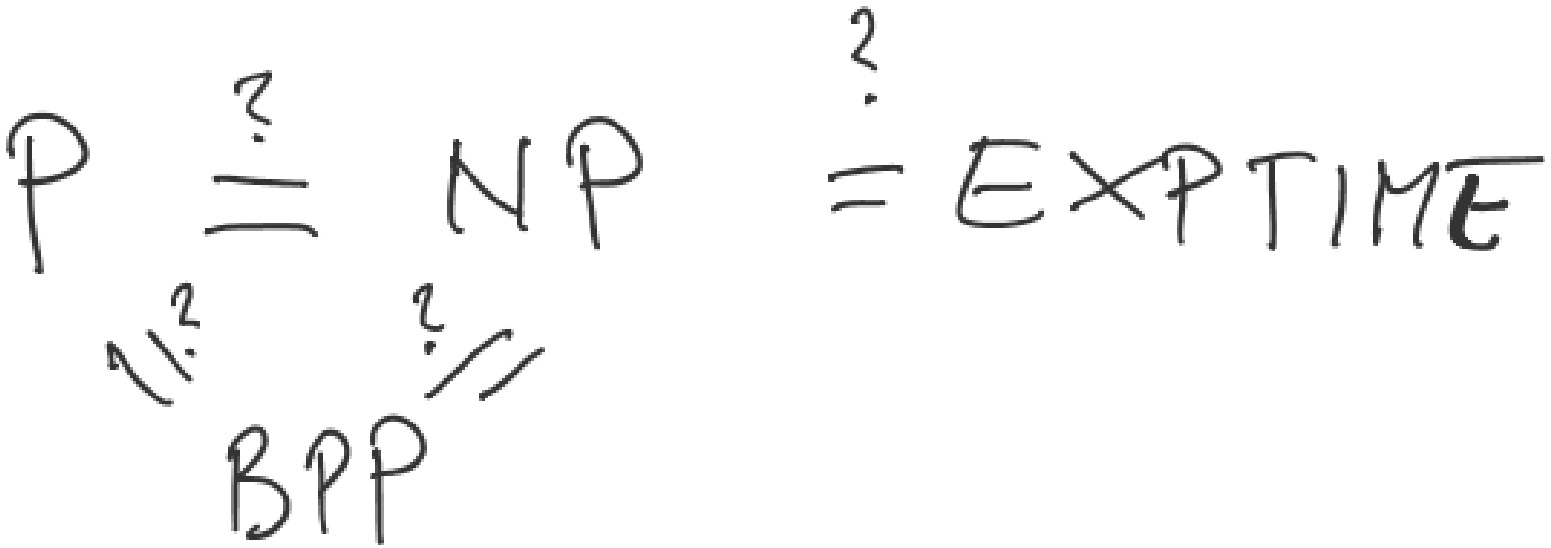
- classical bit
- computation - boolean function, boolean gate
- reading information

Quantum computer

- quantum bit
- computation - unitary matrix, unitary gate
- reading information - quantum measurement

Does it make difference?

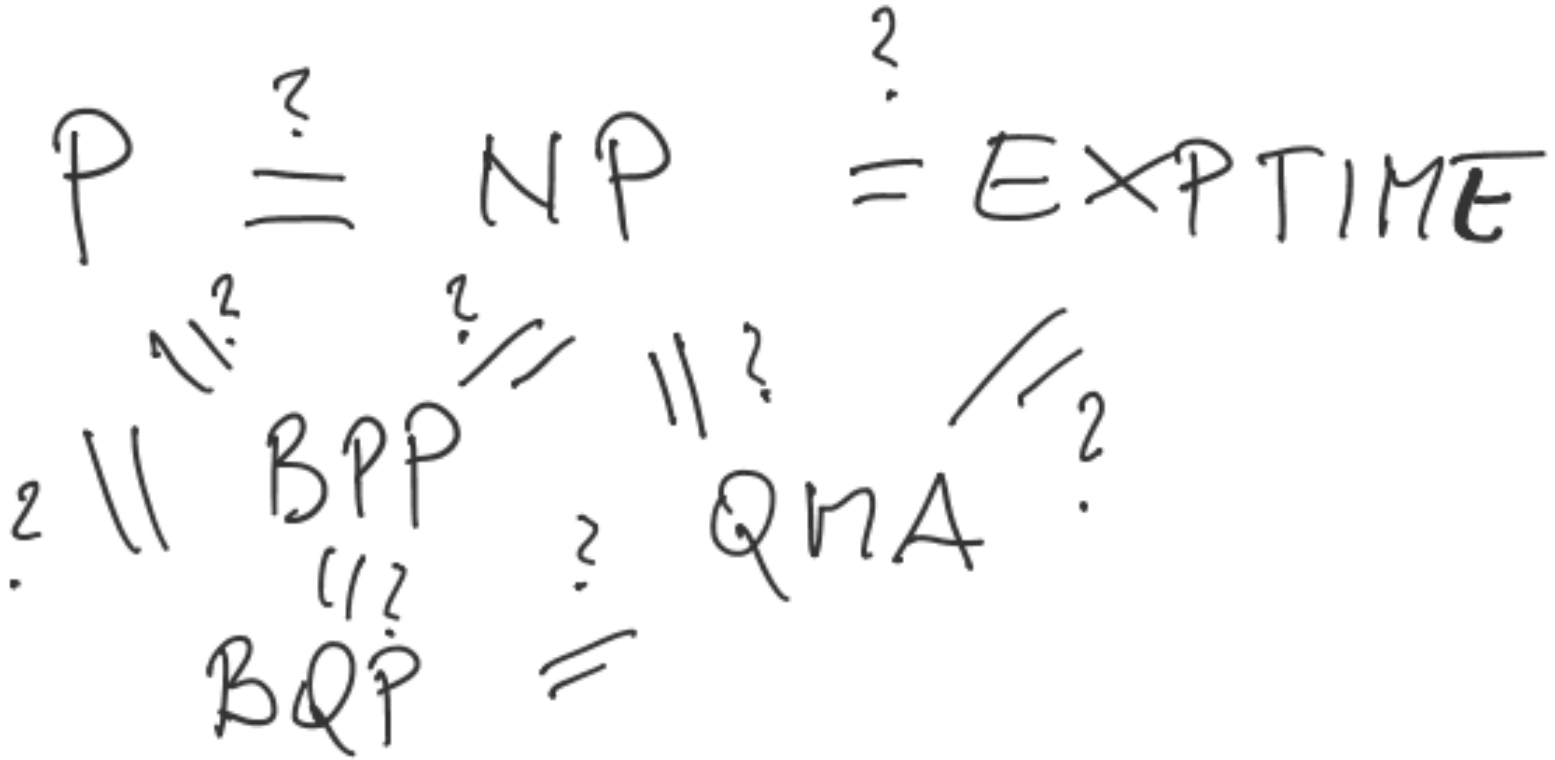
Computational complexity



Complexity zoo: https://complexityzoo.uwaterloo.ca/Complexity_Zoo

Does it make difference?

Computational complexity



Does it make difference?

Cryptography

- YES
- QKD, QRNG, DI
- RSA, Diffie-Hellman, El Gamal...
- Post-quantum cryptography

Communication complexity

- YES
- Some (!) problems have different classical and quantum CC

Information theory

- YES
- Information theory no longer independent on information carrier.

Algorithms

- Probably

NIST (National Institute of Standards and Technology)

- NIST is currently performing post-quantum cryptography standardization
- The goal is to chose asymmetric encryption systems and digital signatures that are likely to be secure against quantum computers.
- Must be adopted as soon as possible - adversary may store messages transmitted today and decrypt them in the future.
- Second round "winners" announced on January 30, 2019
- Previously recommended algorithms are vulnerable

NIST (National Institute of Standards and Technology)

NISTIR 8105 Report on Post-Quantum Cryptography

Cryptographic algorithm	**Type**	**Purpose**	**Impact from large-scale quantum computer**
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	——	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Part II

Prominent applications of quantum information processing

Random number generators

- Random numbers are critical especially for cryptographic applications
- Classical random number generators are not random.
  - Classical physics does not have random events.
  - Randomness is our ignorance about the parameters of the system.
  - Chaotic system - even small ignorance about initial parameters means large ignorance of the output.
- Quantum measurement - truly random.
  - If the quantum physics is right ...

Quantum key distribution

Shared (symmetric) secret key is indispensable for a number of cryptoapplications.

- encryption
- message authentication
- digital pseudosignatures
- secure multi-party computation in general

Classical case

- Computational security only.
- Many solutions later shown insecure.
- Even more solutions insecure against quantum computer.

Quantum case

- unconditionally secure
- different technologies
  - BB84 - single photons
  - E91, BBM92 - entanglement
  - COW - continuous variables

Device-independent technologies

Random number generators and key distribution can be "device independent".

- Device can be tested by user for security.
  - Tested as a blackbox using external random number generator.
- Secure against quantum hacking.
- Secure against incorrect design.
- Secure against fradulent producer.
  - Huawei
  - Many US companies - wikileaks, snowden
- eDICT project.

More cryptographic applications

Quantum information can be encrypted!

- Quantum one-time pad
- Non-malleable encryption

Limited quantum storage models

- coin tossing
- bit commitment
- secure multi-party computation

Weak coin tossing

Quantum algorithms

Grover

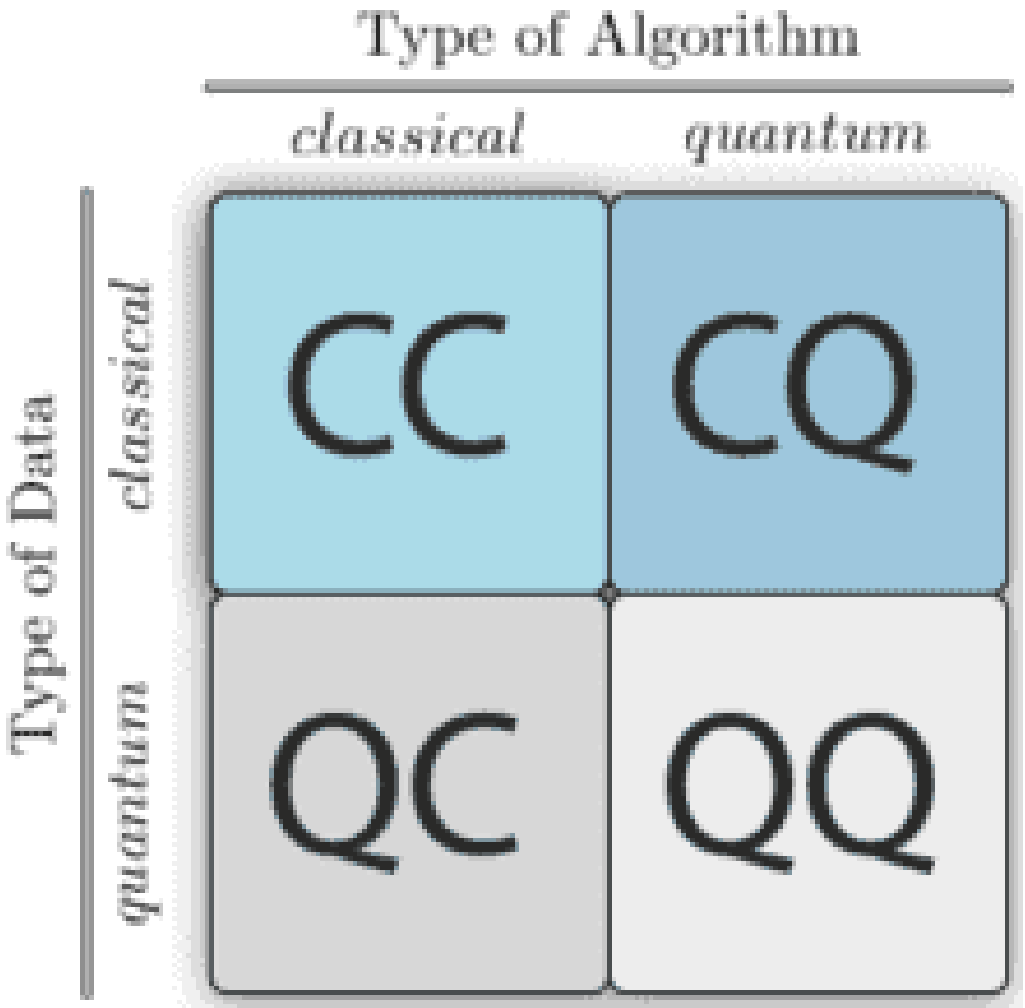
- Searching in unordered list (database)
- quadratic speedup
- Bad for symmetric ciphers
- Key length efficiently reduce to half

Shor-type algorithms

- Most general version solves hidden subgroup problem for Abelian groups.
- Exponential speedup.
- RSA - integer factorization
- El Gamal - discrete logarithm
- Some eliptic curve ciphers.

\+ Approximating NP-complete problems

Machine learning algorithms



Simulating quantum systems

Simulations are cheaper and faster than experimental trials:

- sound systems, photography lenses, aerodynamic simulations
- drug invention:
  - developing a new drug and bringing it to market can take 15 years and cost more than $ 1 billion
  - simulations maximize commercial potential, while reducing the costs and minimizing risks
- (car) batteries:
  - Computer Michael @ University College London
  - £1.6M, 265 TFLOPS
- (nano)-materials
- Agriculture fertilizers
- Chemical compounds

Quantum technologies vs. Quantum information processing

- accelerometers - navigation devices without external help
- solid-state quantum sensors for sensitive measurements of magnetic field
  - inside human body biosensors
  - magnetic resonance
- entanglement — increased resolution in imaging, quantum clock
- squeezed light: LIGO – Laser Interferometer Gravitational-Wave Observatory
  - Do not mistake with LEGO – Leg Godt (Danish: Play Well)
- measuring voids under the ground and to detect mineral deposits
- providing non-invasive point-of-care diagnosis.

Part III

Existing quantum devices

ID Quantique Quantis QRNG

- The first quantum random number generator commercially available.
- Internal design not know. Is it random?
- Early versions suffered from problems with postprocessing.
  - Resulted in bad randomness.
- Not clear whether postprocessing issues were resolved.

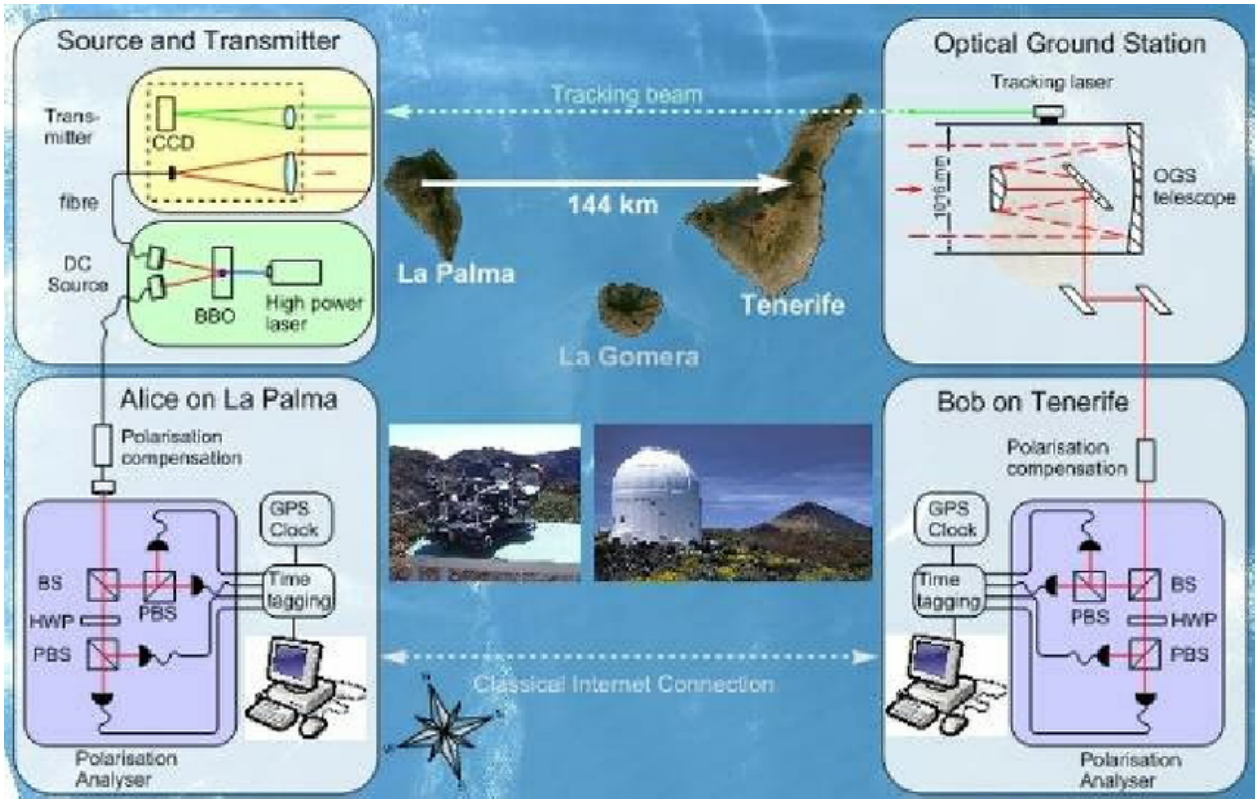
Australian National University

Online access to quantum randomness

ID Quantique Cerberis QKD

Commercial QKD system. Communication via optical fibre.

Tenerife-La Palma experiment



Open air quantum key distribution. 144km distance.

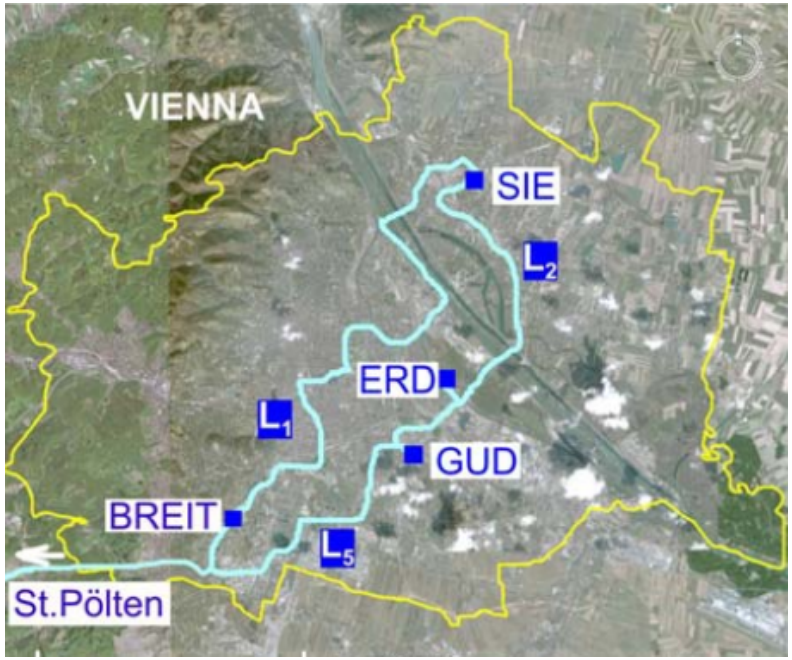
Tenerife-La Palma experiment

SECOQC project

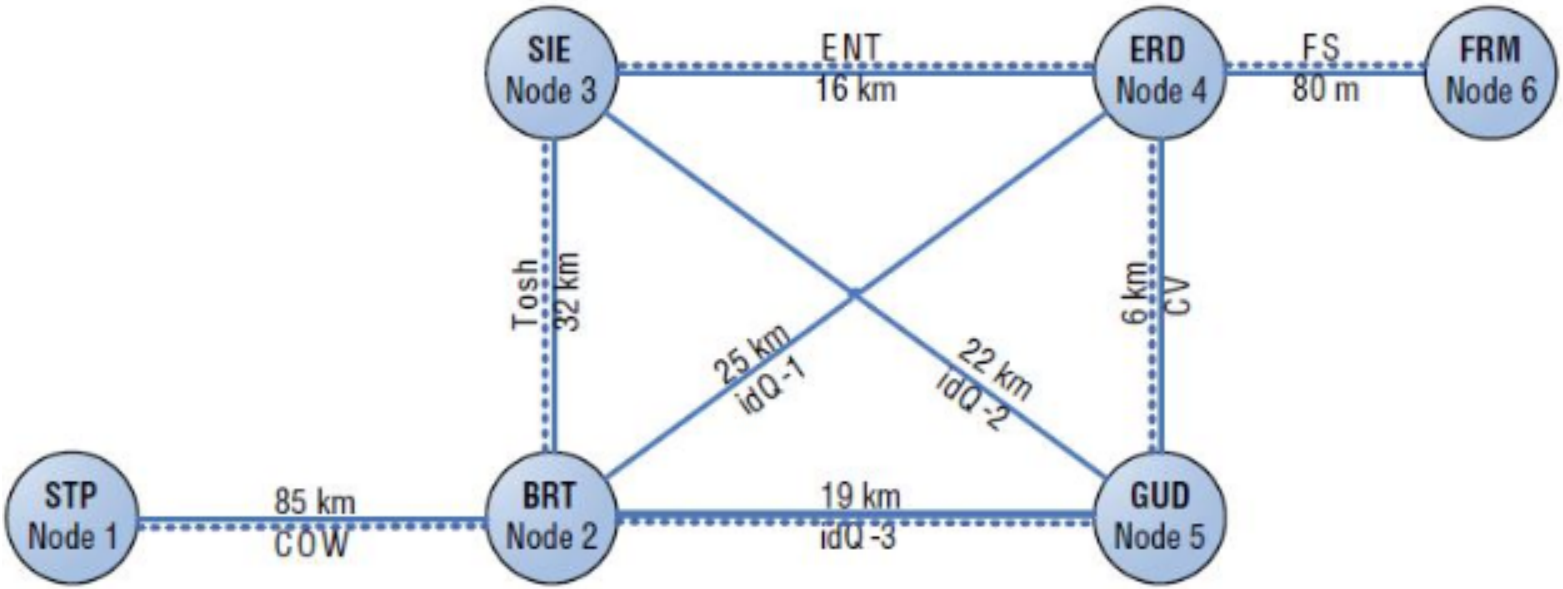
- European project culminating in creating experimental quantum network around and inside Vienna.
- 2008

Consortium of more than 40 partners including:

- AIT (Austrian Institute of technology), coordinator.
- Siemens
- Toshiba
- Hewlett-Packard
- Thales France
- ID Quantique



SECOQC project

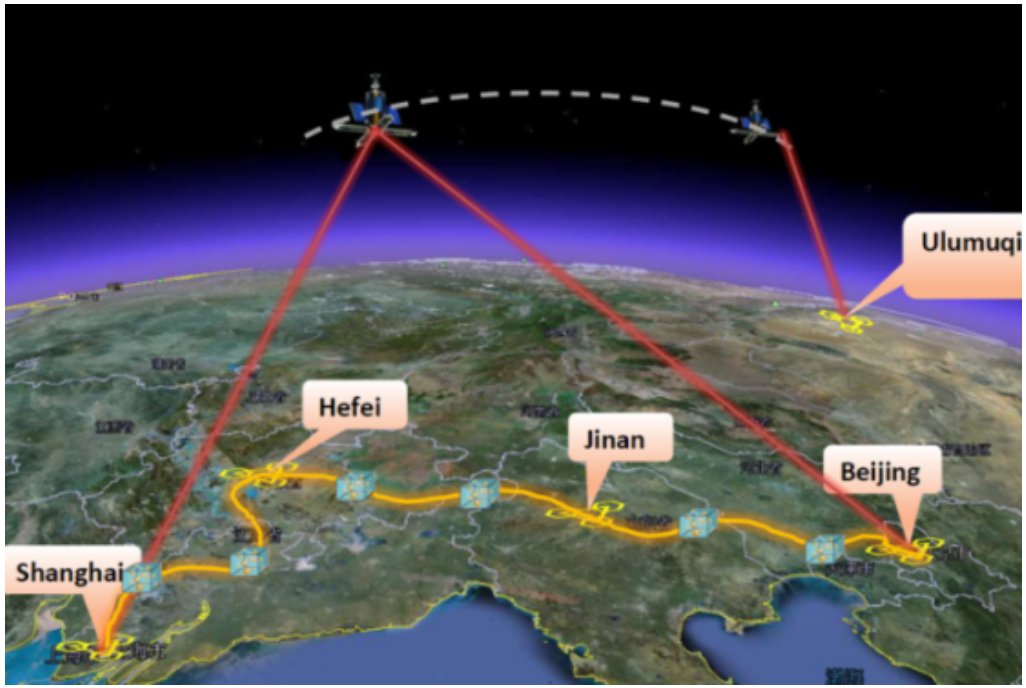


- BB84, BBM92 (entanglement), COW (coherent one-way)

Chinese QKD backbone

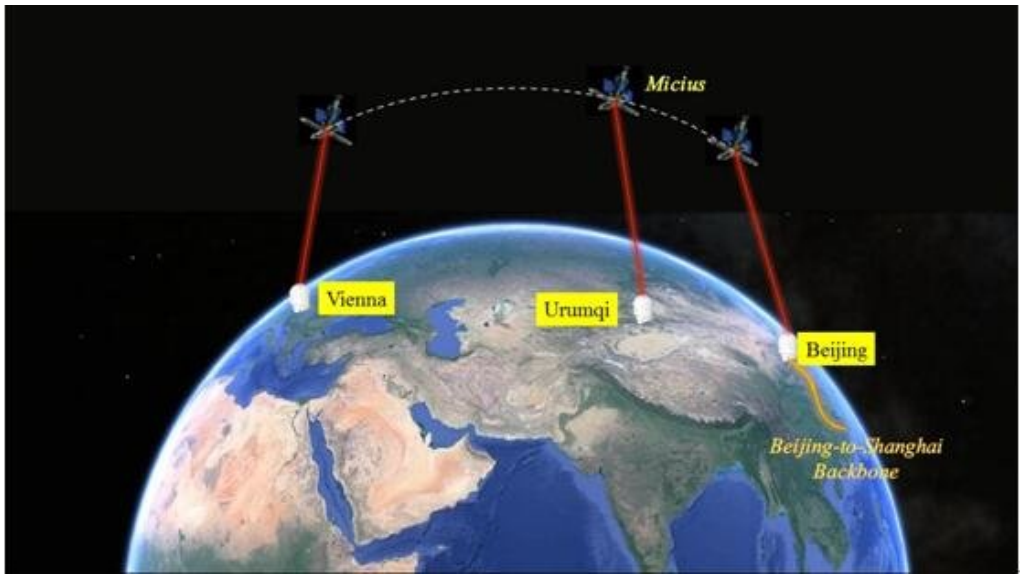
2000km backbone QKD network from Beijing to Shanghai.

- Opened September 2017.
- Connects local quantum networks in
  - Beijing
  - Shanghai
  - Hefei
  - Jinan
- 32 trusted nodes used as repeaters.
- Connects critical government and military installations.



Chinese Quantum satellite Micius

- Launched August 2016.
- Quantum-enabled satellite.

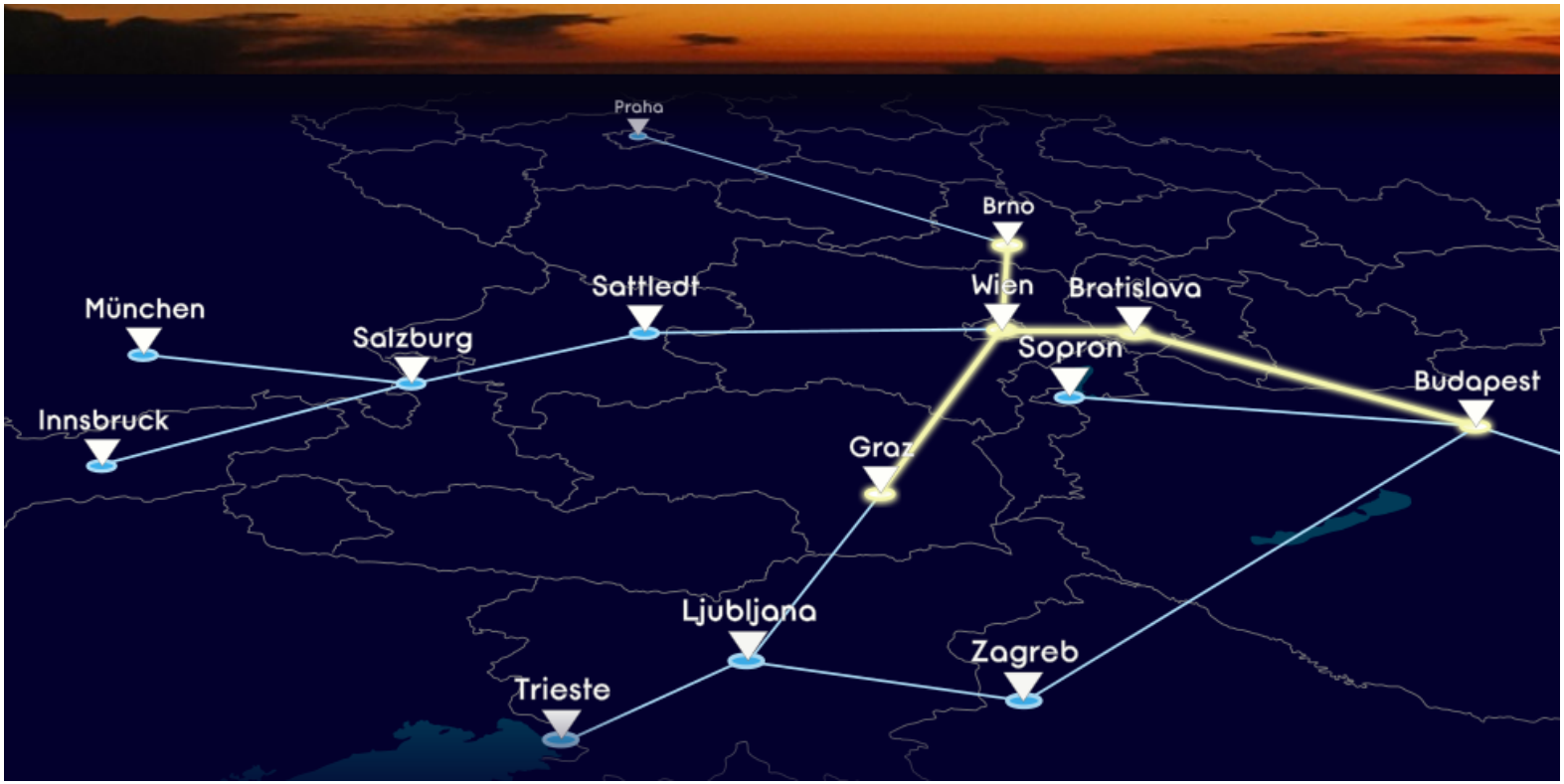


- Distributes entangled pair to a pair of selected ground stations.
- Connects the military installation in Ulumuqi to the Chinese backbone network.
- Connects to some ground installations in Austria
  - Graz OGS
  - In future Vienna as well, to connect Chinese quantum backbone network and European Quapital network.

Quapital project

- Plan to connect European Capitals using a QKD network.
- Entanglement-based QKD.
- Also serves as an out-of-lab practical test of entanglement technology.
- Uses rented standard commercial optical fibres (Turkish telecom, CESNET, ...).
- Link between Vienna and Bratislava almost finished.
- Next should be connected Budapest, Brno, and Graz.

Quapital project



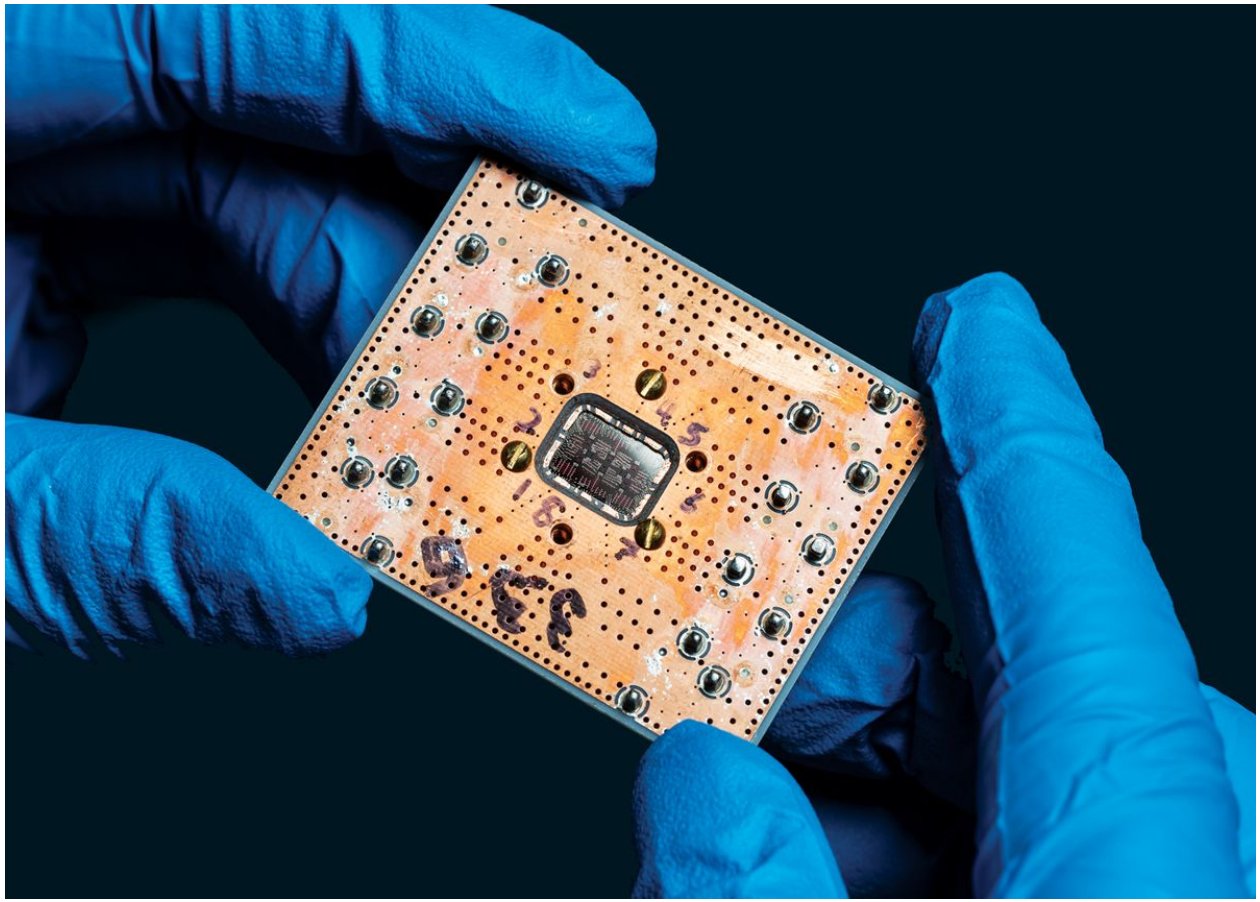
Quantum technologies in space: ESA

Telescope in La Palma receiving laser beacon from ESA OGS (optical ground station) at Tenerife. Preparation for quantum teleportation experiment.

Quantum technologies in space: ESA

Graz OGS tracks Chinese Micius satellite. Green beacon laser from satellite, red beacon laser from ground station.

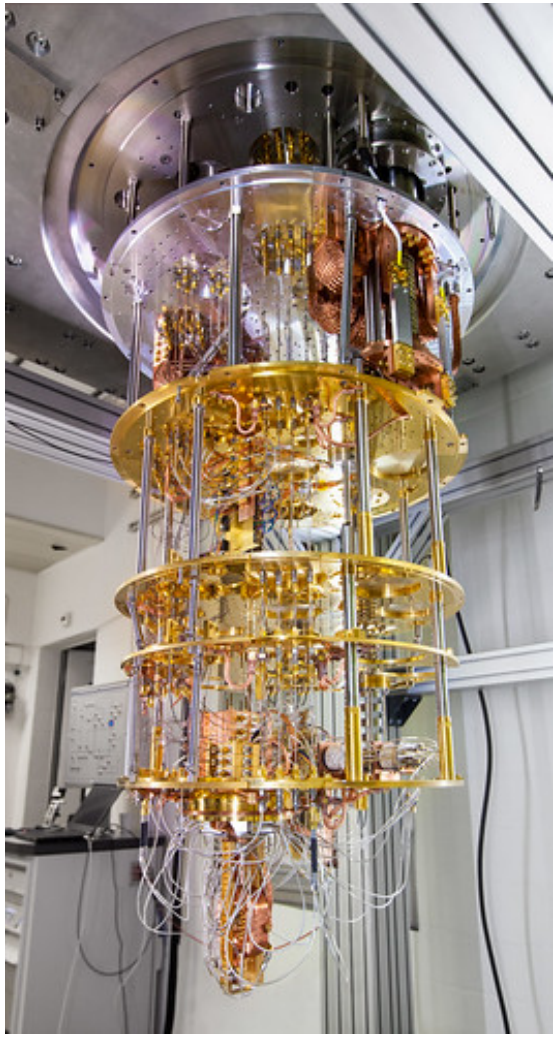
IBM quantum chip



IBM quantum computer

How did IBM start designing quantum computer ...?

- The actual quantum chip you cannot see at the bottom.
- The rest is mainly cooling.
- How to make something really cool?
  - You can e.g. bring helium to a rapid boil (under pressure) ;-).



IBM quantum computer

20 qubit computer System one

IBM quantum commerce

IBM Q Network clients include

- JPMorgan Chase
- Daimler AG
- Samsung
- JSR Corporation
- Barclays
- Hitachi Metals
- Honda
- Nagase

Other quantum computers

- Google's Bristlecone quantum processor
  - 9 qubits
- Microsoft 10 qubit processor.
  - Microsoft Quantum development kit.
  - The Q# language.
- Apple announced no quantum computer ...
- Intel is testing quantum processor ...

D-wave device

- Special purpose device
- Not general quantum computer
- 2000 qubits
  - What does that mean?
- Represent computational problem as a specific parameter of a suitable physical process.
- Run quantum annealing to calculate the value of this parameter.
- The value of the parameter is the solution of the computational problem.

Part IV

Course outline

What is this course about

- To provide a (relatively) easy and friendly introduction to quantum programming.
- Sequentially introduce simple applications
- Gradually introduce, explain and practice necessary mathematical
- Gradually introduce, explain and practice necessary quantum information processing
- At each moment only necessary mathematics and quantum info

You will learn

- How to program IBM quantum computer using Qiskit library.
- Understand the applications you are programming.

You will not

- learn how to create your own quantum algorithms
- be able to understand more advanced quantum applications

Follow-up courses

At the moment

- IA082 Physical concepts of quantum information processing
- Spring

Curicullum design under consideration:

I This course.

II Quantum information theory course
  - Builds sufficient knowledge of quantum information
  - Builds sufficient knowledge of mathematical aspects
  - Builds sufficient knowledge of physical aspects
  - Includes e.g. Shor's algorithm

III Quantum programming
  - Includes machine learning algorithms.
  - Includes explanation how to program d-Wave and similar devices.

How to study the course

As smooth as possible learning curve

- If you attend lectures and tutorials
- Learn and practice the skills right after they are presented
- Tutorials require knowledge from lecture
- **Lectures require knowledge from tutorials!**

Mathematics

- is simple.
- complex numbers
- finite-dimensional complex vector spaces
- but we need intuitive and confident knowledge.
- you must be able to actually perform the calculations.

Tutorials

- Refreshing mathematics
- Calculation drill
- Calculating/solving quantum information processing tasks
- Programming using Python and Qiskit

Attendance of lectures and tutorials

- 2h lectures each week
- 1h tutorials each week

Tutorial attendance is compulsory

- If you cannot attend tutorial for a legitimate reason, deliver appropriate documents to the study department.
- Such a non-attendance won't be penalized.

Penalty:

- Skip one tutorial: no penalty
- Skip two tutorials: -5 penalty points
- Skip more than two tutorials: -10 penalty points
  - Counts only towards the pass/fail limits.
  - Does not influence the final grade above E.

Examination

How to get points:

- 4 minitests at random tutorials, 5 points each
  - define 2-dimensional quantum state
  - calculate an inverse of a given matrix
  - Learn regularly both the lectures and tutorials.
- Solve problems during tutorials
  - Number of points depends on difficulty of the task.
  - Everybody will get chance to obtain at least 15 points.
  - Learn regularly both the lectures and tutorials
- Final exam

Part I Written test. No materials are allowed.

Part II Program (solve) a simple task on a computer. Online access to Qiskit reference and tutorials.

  - 70 points together

- Subsequent oral exam necessary to get "A" or "B"

Evaluation and Grading

Points are (almost) everything

Type of Completion	Grade	minimal number of points	tutorial attendance penalty applies
credit ("zápočet")	z	20	Yes
colloquium	k	45	Yes
Exam	E	50	Yes
	D	60	No
	C	68	No
	B	$75^{(*1)}$	No
	A	$85^{(*2)}$	No

$^{(*1)}$ Oral exam mandatory, C guaranteed. No oral exam - C.

$^{(*2)}$ Oral exam mandatory, B guaranteed. No oral exam - C.

Course content

Course divided into 10 chapters

- See interactive syllabus in IS for details

Each chapter combines

- explanation of particular quantum information processing applications
- refreshing relevant mathematics
- presenting relevant quantum information principles
- learning relevant quantum programming skills
- implementing application(s) using the IBM Qiskit.

Chapters are introduced in the order they will be presented.
Some of them will span more than one lecture.

Example:

Lecture 2:

- Quantum bit - qubit.
- Quantum register, quantum measurement
- Quantum random number generator
- QRNG implementation
- BB84 quantum key distribution.
- Simplified BB84 implementation

Lecture 3:

- Tensor products.
- Herminian matrices
- Quantum entangement

Lecture 5,6:

- Quantum gates
- Unitary operations
- (relatively) full BB84 implementation