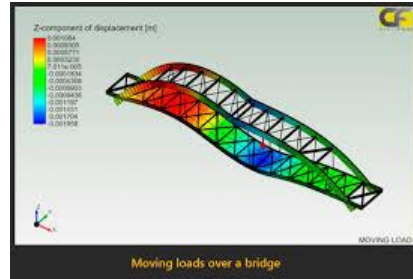
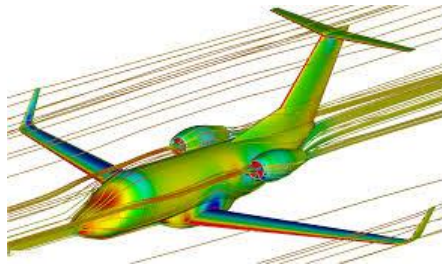
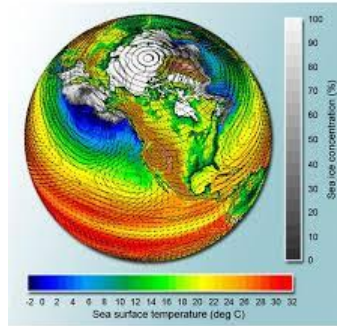
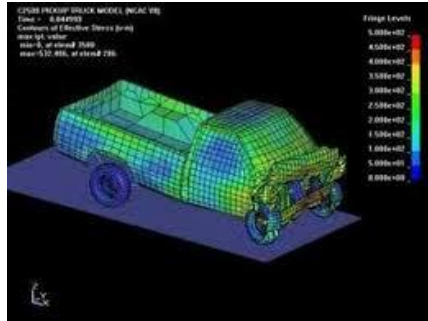


› **QUANTUM TECHNOLOGY
APPLICATIONS -
MARAN.VANHEESCH@TNO.NL**

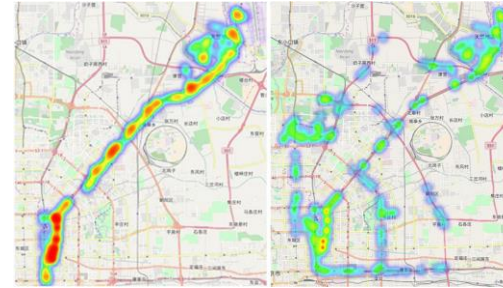
Drs. ir. M.P.P. van Heesch

TNO innovation
for life

VISION OF QUANTUM COMPUTING



Classic Computers



Optimization



Medicine production

Quantum Machine learning

Breaking cryptography

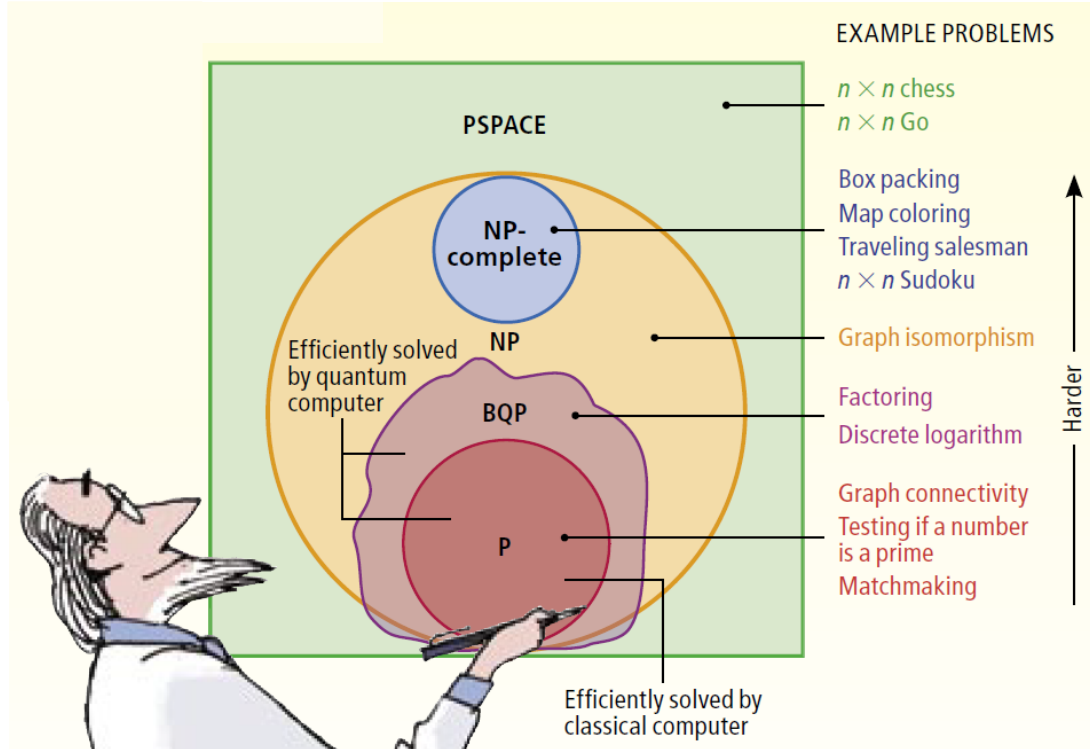


Quantum Computers

A 3D maze with white walls and a blue floor. The maze is complex and winding, with many paths and dead ends. In the center of the maze, the text "QUtech" is written in white. The maze is viewed from a slightly elevated perspective, showing the depth of the walls.

QUtech

QC AND COMPLEXITY



PSPACE = the set of all problems that can be solved using a polynomial amount of space (but possibly an exponential number of steps).

NP = Problems with efficient algorithms for which a given solution can be verified as a solution in polynomial time.

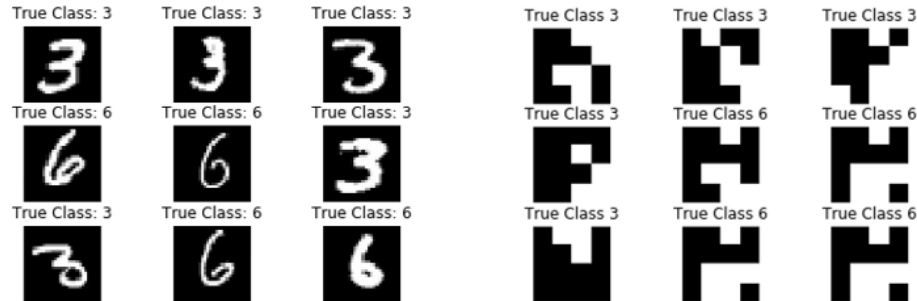
NP-complete = Class of decision problems which contains the hardest problems in NP. Each NP-complete problem has to be in NP.

P = Problems with efficient algorithms for finding solutions, these algorithms use at most polynomial amount of computational resources.

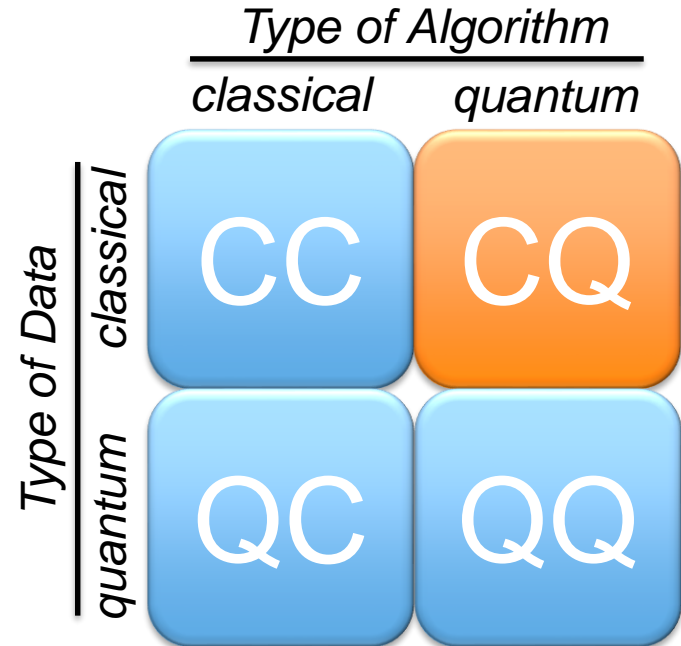
BQP = The class of decision problems solvable in polynomial, with at most 1/3 probability of error.

QUANTUM ENHANCEMENTS FOR ML

- › Quantum effects helping us solve classical learning tasks more efficiently.
- › Possible benefits:



quantum annealers, use of quantum sampling in generative models, Quantum ML algorithms (e.g., SVM using Grover's algorithm)



Quantum Inspire



- › A quantum computing platform
- › Try yourself!

```

1 version 1.0
2 # The circuit for the Quantum Fourier Transform on 6 qubits, using only elementary gates
3 qubits 6
4
5 # start writing your code here
6 H q[0]
7 CR q[1],q[0],0.25
8 CR q[2],q[0],0.125
9 CR q[3],q[0],0.0625
10 CR q[4],q[0],0.03125
11 CR q[5],q[0],0.015625
12 H q[1]
13 CR q[2],q[1],0.25
14 CR q[3],q[1],0.125
15 CR q[4],q[1],0.0625
                
```

Pauli-Z gate

Hadamard gate

The Hadamard gate is a single-qubit operation that maps the basis state $|0\rangle$ to $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|1\rangle$ to $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, thus creating an equal superposition of the two basis states.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

[Learn more](#)

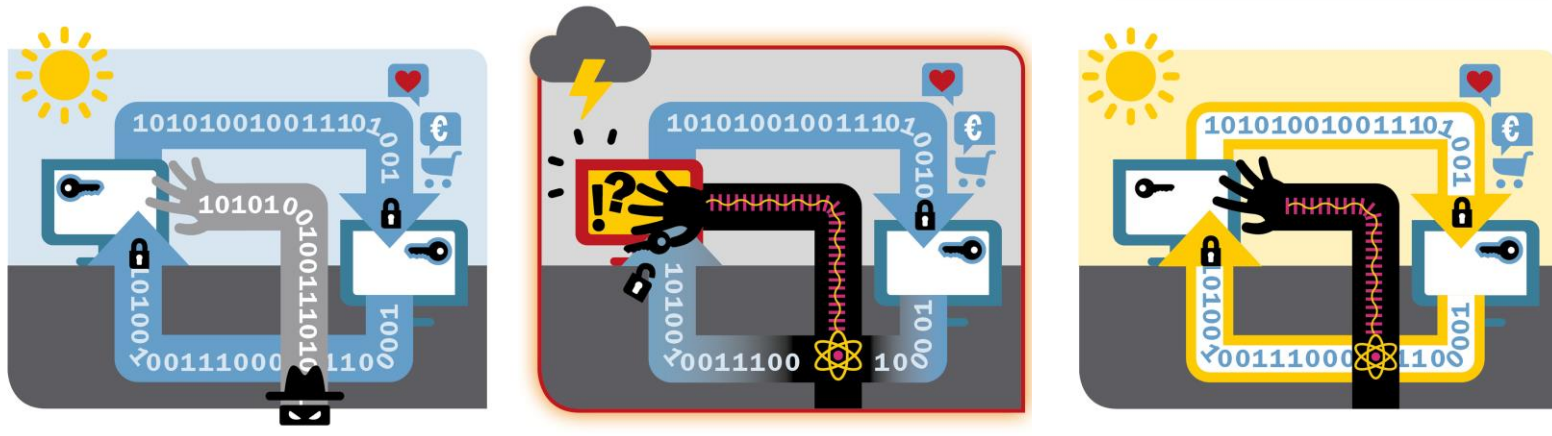
1 H q[0] #execute Hadamard gate on qubit 0

Copy to clipboard

IMPACT OF QUANTUM COMPUTING ON SECURITY

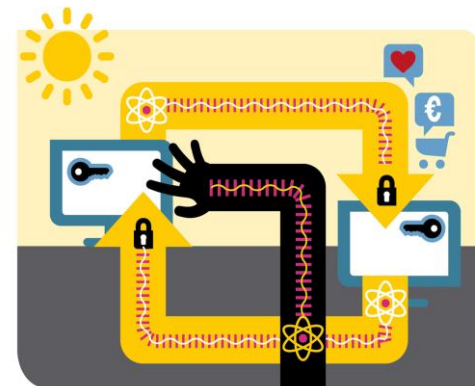
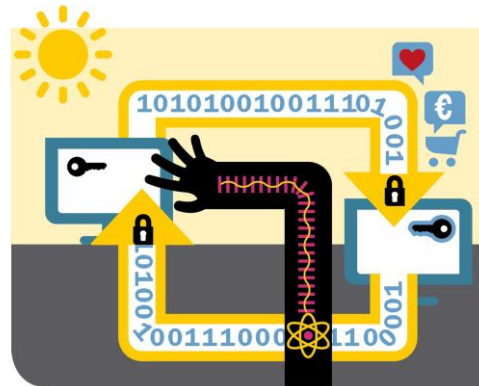
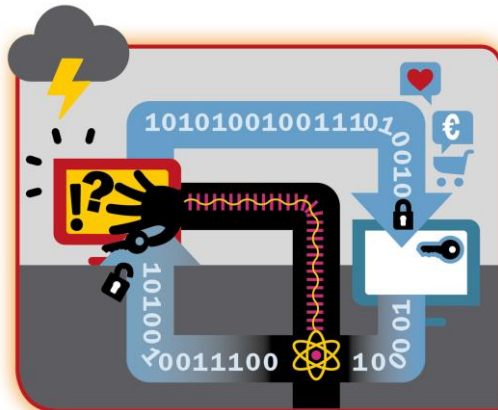
Store now, decrypt later

- › Shor's factoring algorithm (1994)
- › Grover's search algorithm (1996)
- › Most of the currently used asymmetric cryptography is broken.
- › This affects our digital infrastructure (data transfer, transactions, signatures).



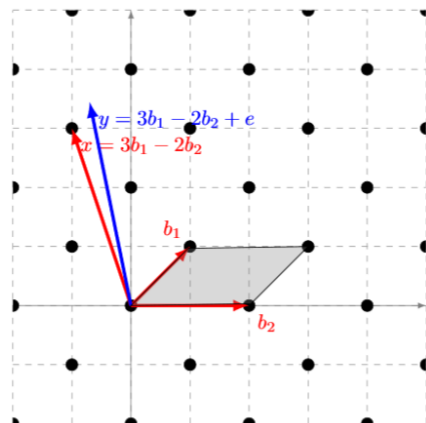
GETTING QUANTUM-READY

- › Need to **diversify** the cryptographic protocols and solutions
- › Important to think about strategies to become quantum-safe now, and introduce flexible solutions.
- › Both post-quantum and quantum cryptography (QKD) can be used to become quantum safe.

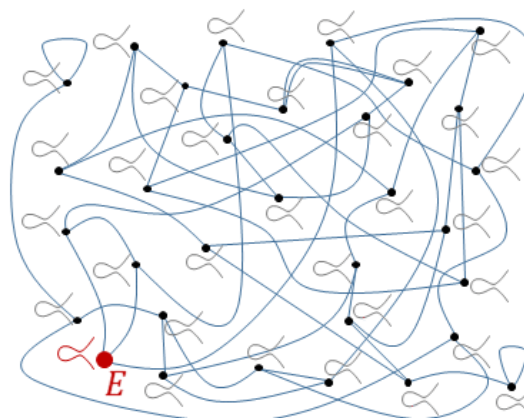


POST-QUANTUM CRYPTOGRAPHY

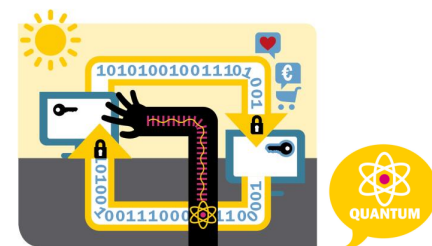
- › Need to **diversify** the cryptographic protocols and associated mathematical problems.



Lattices



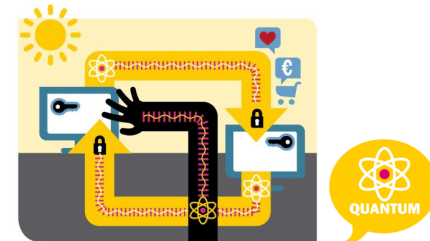
Supersingular Isogenies



QUANTUM KEY DISTRIBUTION

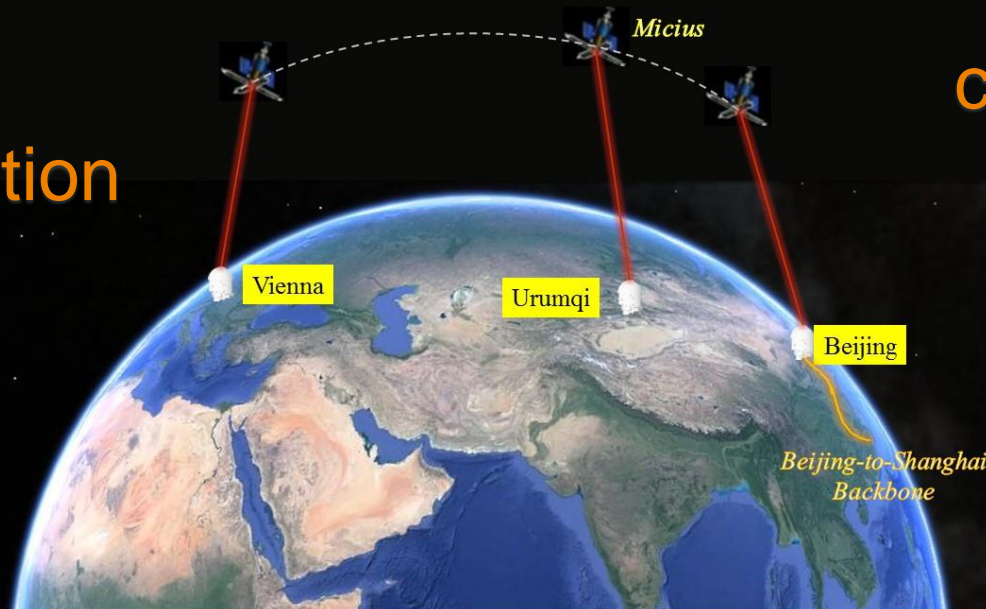


- › Provides: A point-to-point solution.
- › Promise: Information theoretic secure key exchange if implemented perfectly.
- › Need: classical authentication and post processing.
- › To consider: distance limitations.



QUANTUM NETWORKS

For
secure
communication



For
computation

For
sensors

TAKEAWAYS

- › Quantum technology offers both opportunities and threats
- › Quantum computing offers possible breakthroughs in the fields of
 - › Simulation of quantum physics and chemistry
 - › Machine Learning, optimization problems and other hard problems
- › To be quantum safe; one can use post-quantum cryptography or quantum communication
- › To **get quantum ready** it is important
 - › to investigate possible use cases of the quantum computer and experiment on the current hardware.
 - › to take the security threat into consideration and start planning

Drs. Ir. Maran van Heesch
maran.vanheesch@tno.nl

A nighttime photograph of a city street. In the foreground, a metal railing runs across the frame. Behind it, a road with light trails from moving vehicles is visible. In the background, several multi-story buildings are lit up, with windows glowing. A prominent feature is a curved, modern building with a glass facade and a balcony area. The overall scene is illuminated by city lights, creating a vibrant urban atmosphere.

› **THANK YOU FOR YOUR
ATTENTION**

Take a look:

TNO.NL/TNO-INSIGHTS

TNO innovation
for life

Drs. Ir. Maran van Heesch
maran.vanheesch@tno.nl