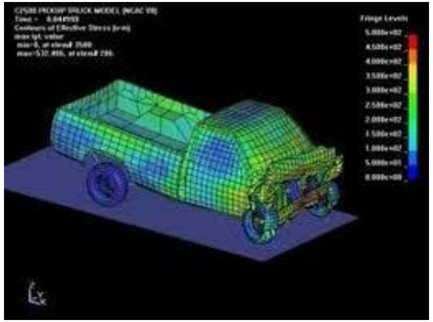
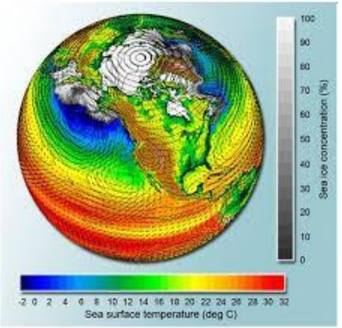
# QUANTUM TECHNOLOGY APPLICATIONS - MARAN.VANHEESCH@TNO.NL

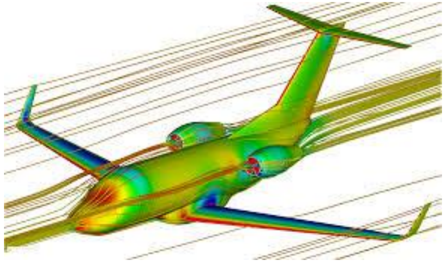
Drs. ir. M.P.P. van Heesch

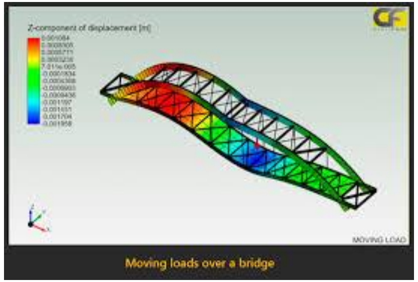
TNO innovation for life

# VISION OF QUANTUM COMPUTING

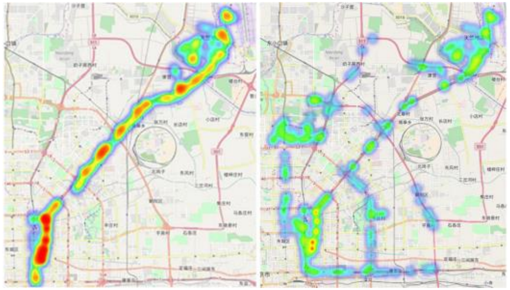




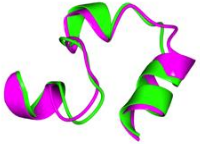



Classic Computers



Optimization

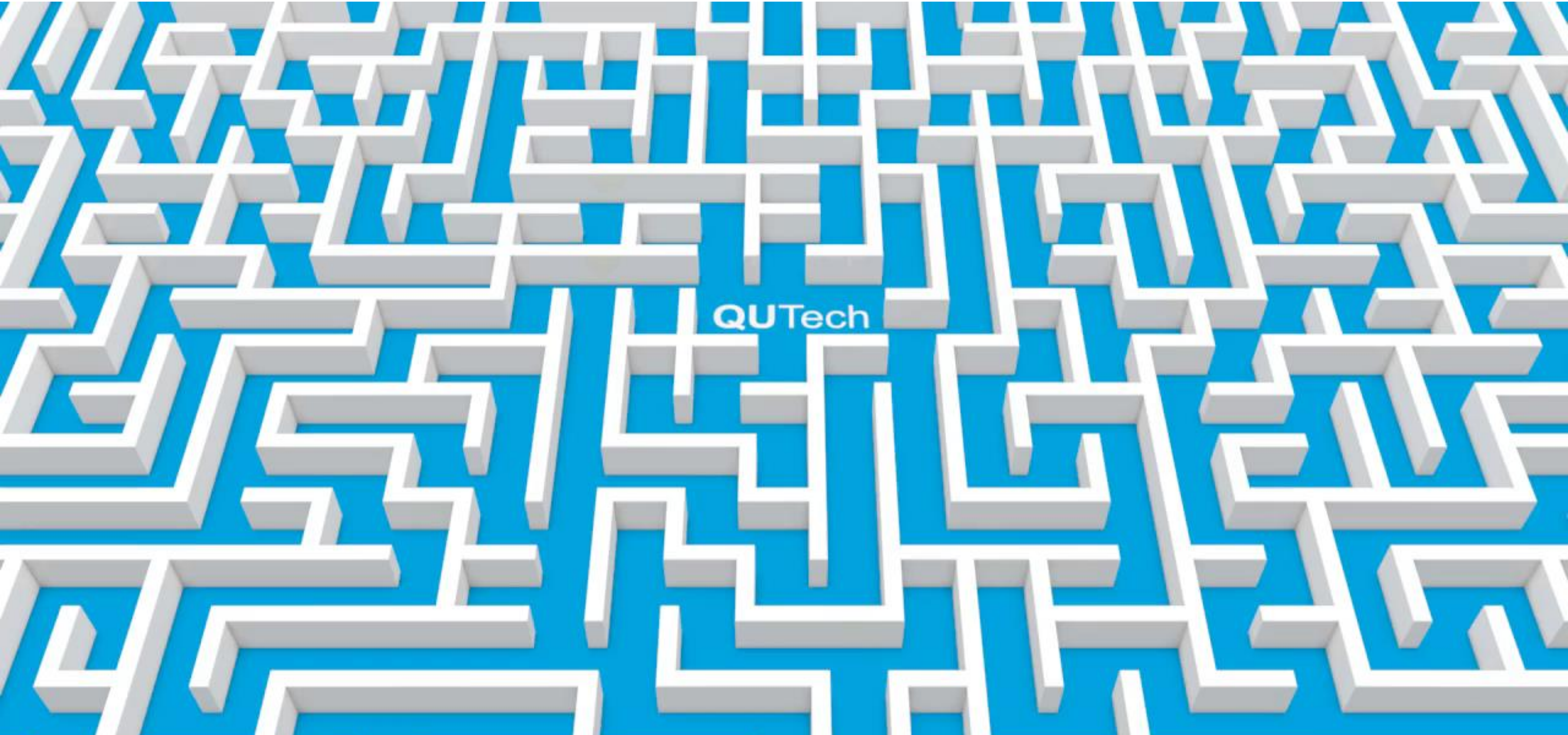
Quantum Machine learning



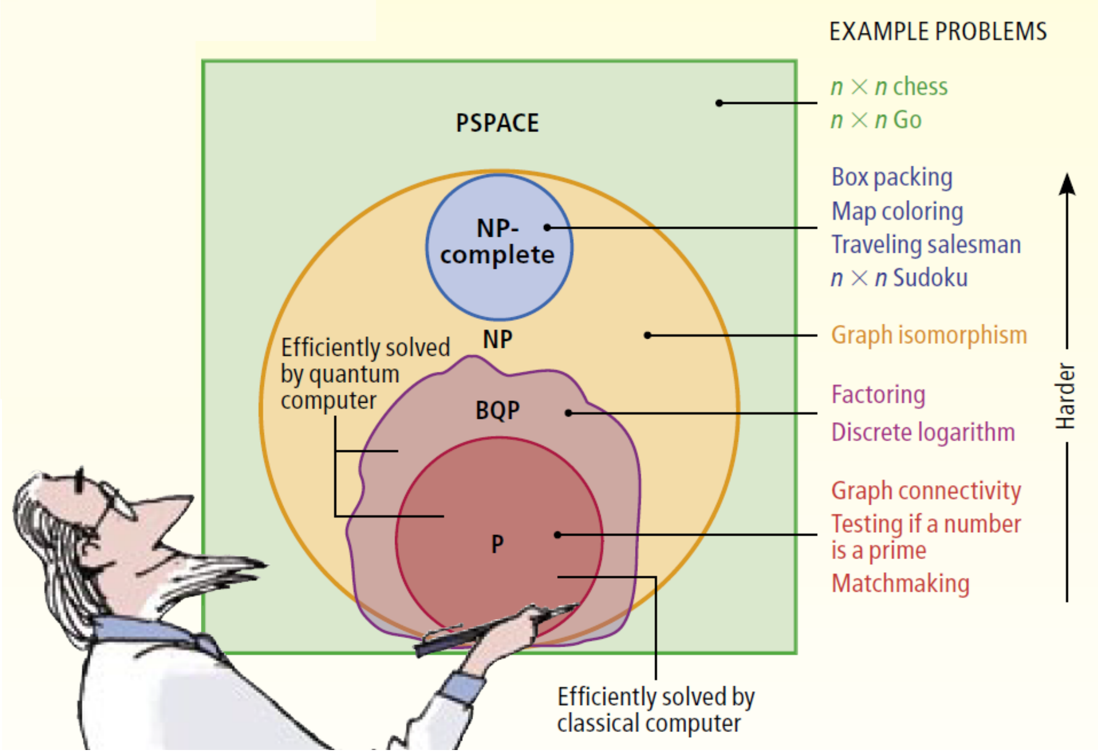
Medicine production

Breaking cryptography

Quantum Computers


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.

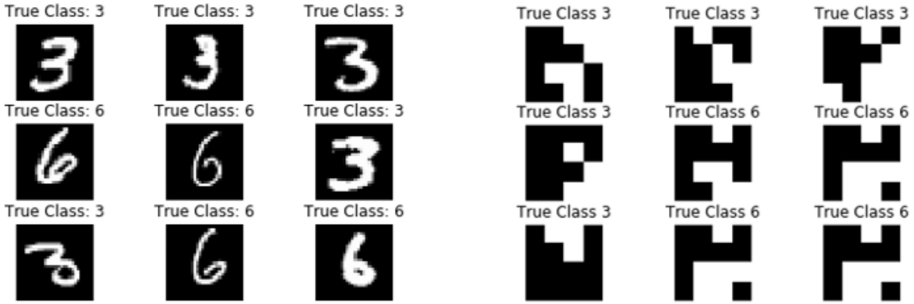
P = Problems with efficient algorithms for finding solutions, these algorithms use at most polynomial amount of computational resources.

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

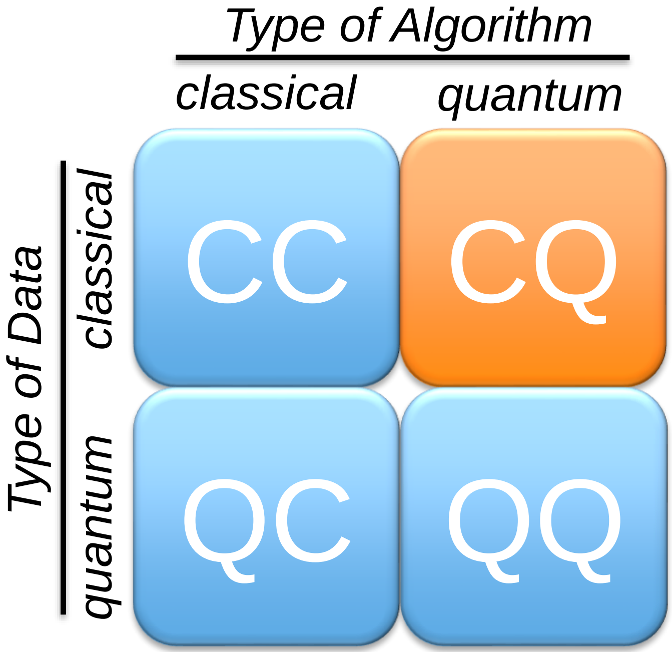
Source: The Limits of Quantum – Scott Aaronson

# QUANTUM ENHANCEMENTS FOR ML

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

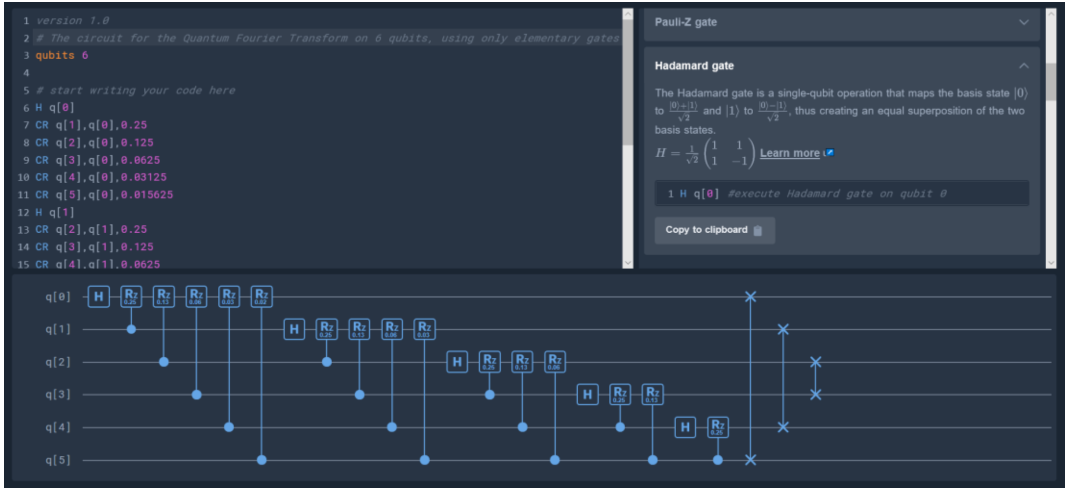



quantum annealers, use of quantum sampling in generative models, Quantum ML algorithms (e.g.,SVM using Grover's algorithm)



# Quantum Inspire

- A quantum computing platform
- Try yourself!

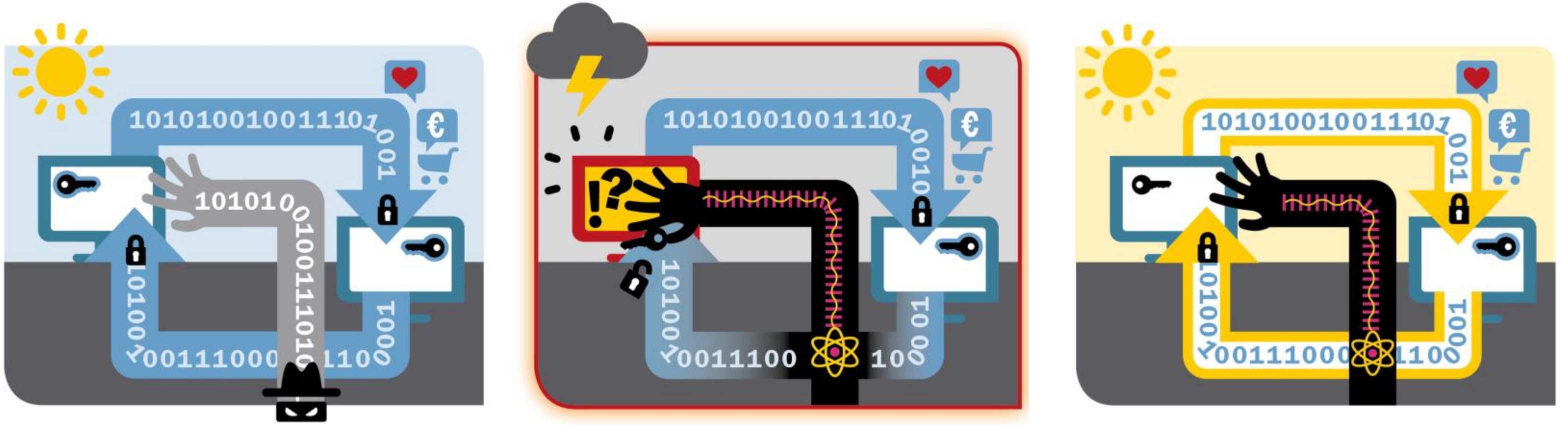


# IMPACT OF QUANTUM COMPUTING ON SECURITY

Store now, decrypt later

- Shor’s factoring algorithm (1994)
- Grover’s search algorithm (1996)

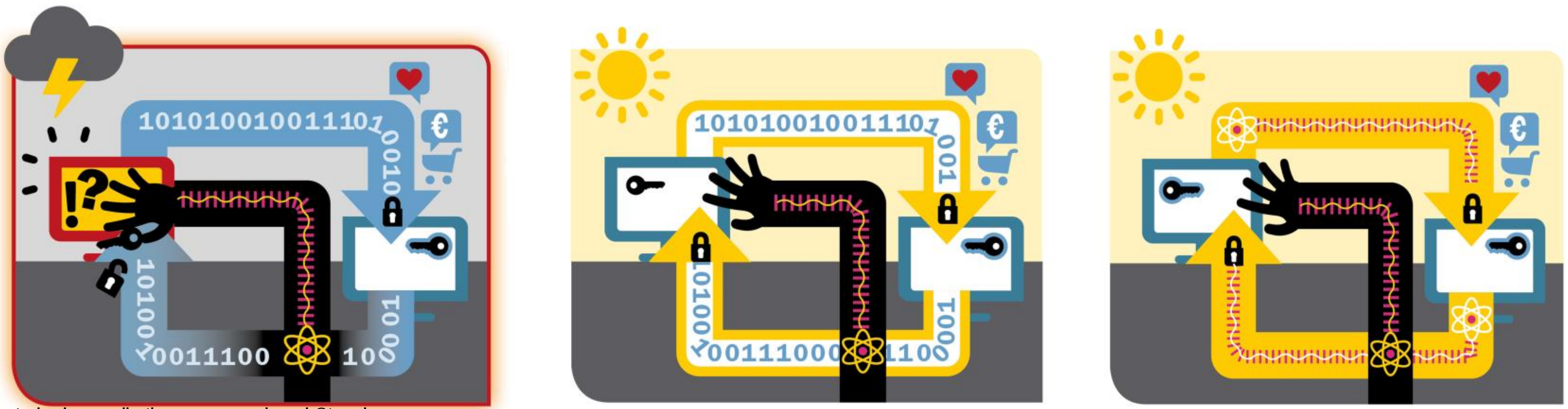
- Most of the currently used asymmetric cryptography is broken.
- This affects our digital infrastructure (data transfer, transactions, signatures).



# GETTING QUANTUM-READY

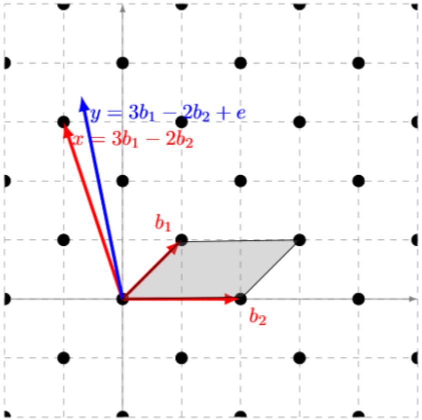
- Need to ***diversify*** the cryptographic protocols and solutions
- Important to think about strategies to be come quantum-safe now, and introduce flexible solutions.

- Both post-quantum and quantum cryptography (QKD) can be used to become quantum safe.

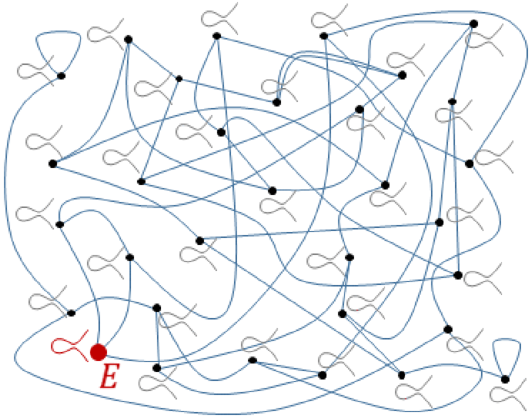


# POST-QUANTUM CRYPTOGRAPHY

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




Lattices




Supersingular Isogenies

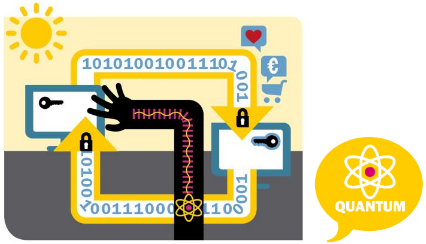
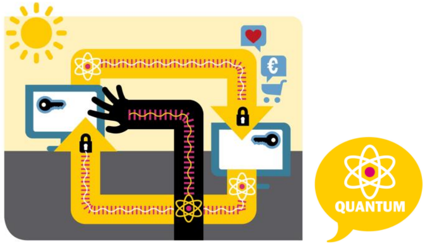





Figure: https://www.esat.kuleuven.be/cosic/elliptic-curves-are-quantum-dead-long-live-elliptic-curves/

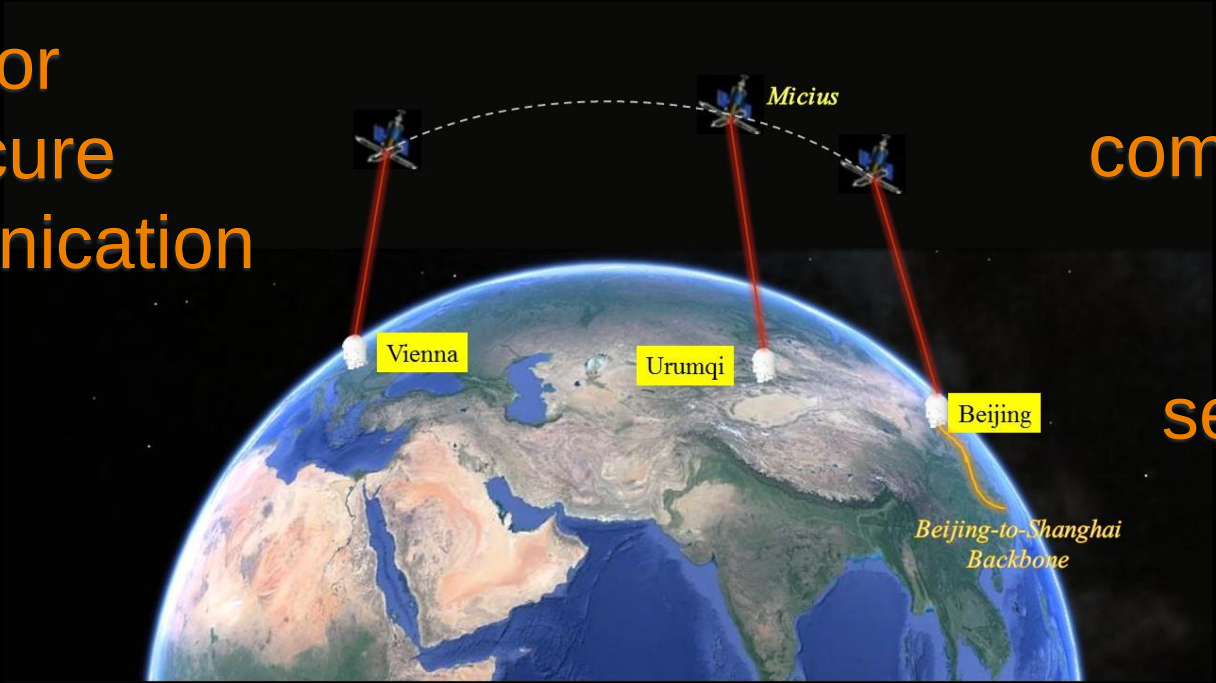
# QUANTUM KEY DISTRIBUTION


- 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

https://phys.org/news/2018-01-real-world-intercontinental-quantum-enabled-micius.html innovation for life

# 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**

# 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**