



universität  
wien



# Quantum Computing and Data Security

Marie-Christine Röhsner

Quantum Information Science and Quantum Computation  
Group, Faculty of Physics, University of Vienna

IPEN workshop

09.06.2017

# Overview

---

## | Quantum Computers

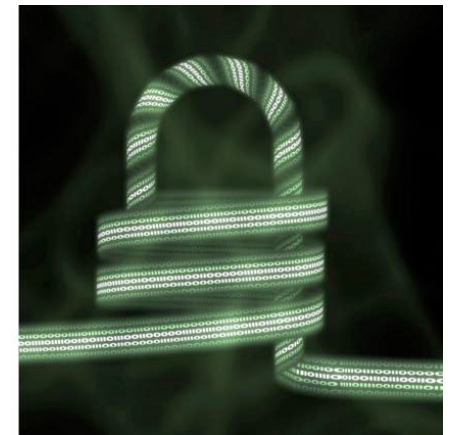
| A threat to classical cryptography

## | Quantum Cryptography

| Security guaranteed by the laws of physics

## | Blind Quantum Computing

| Perfect data privacy in cloud computing



# Quantum Computers

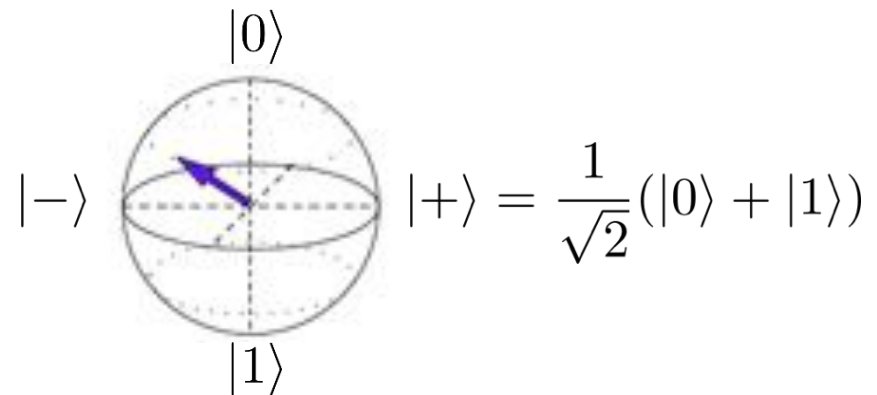
- Computers based on the laws of quantum physics

Bit



Easy readout

Qubit



$N$  qubits –  $2^N$  basis states

Need measurement to readout →  
collapse the state

# Quantum Computers

---

## Disadvantages

- Instable
  - Errors
  - Loss of quantum properties
- Hard to build
  - Isolation
  - Up-scaling
  - Memories

## Advantages

- New resources
  - Parallelism
  - Interference
  - Entanglement
- Fast solutions for
  - Quantum Simulation
  - Search (Grover)
  - Factorization (Shor)

# Shor's Algorithm

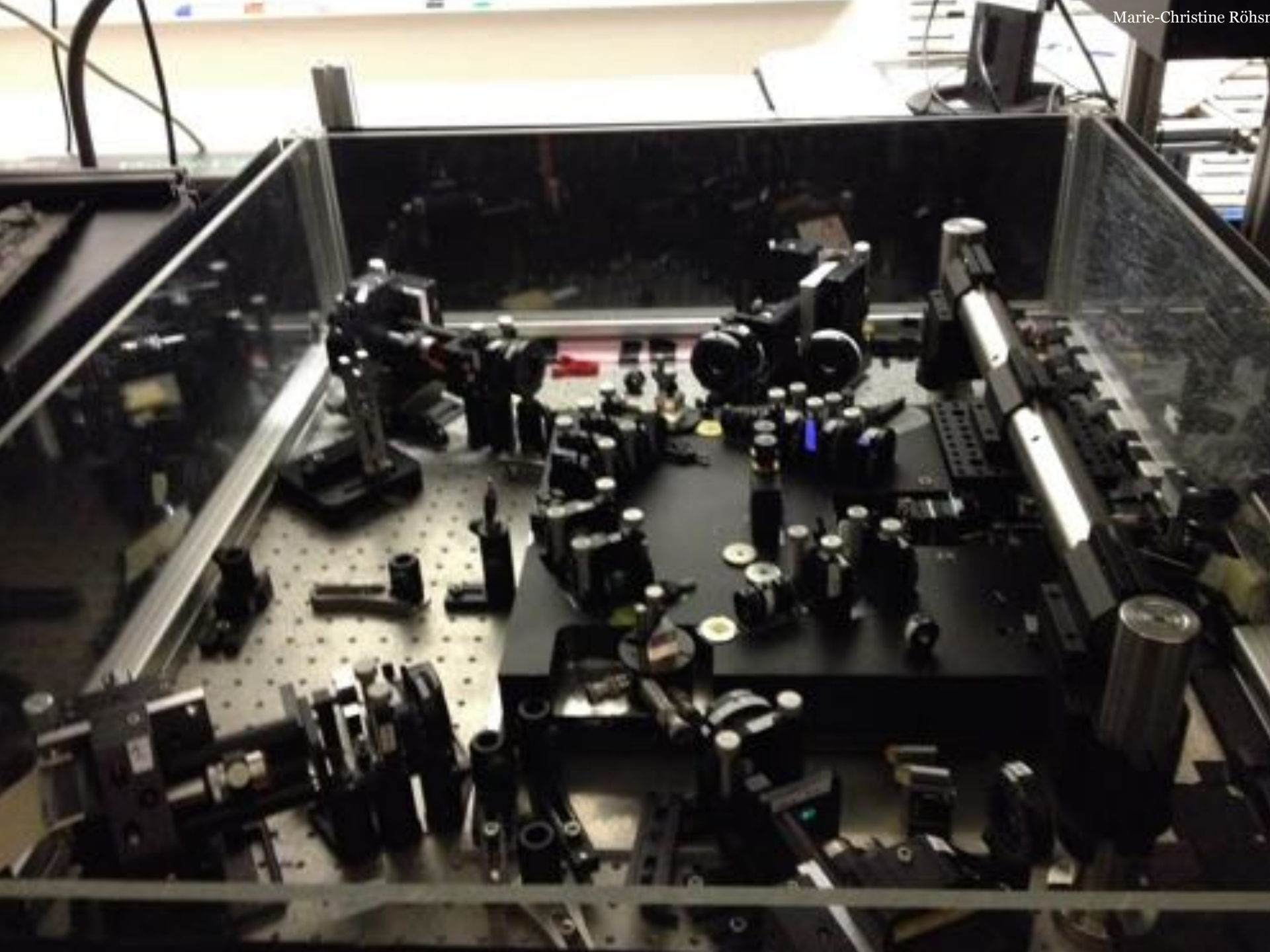
---

- Algorithm for integer factorization ( $N=p*q$ )
- RSA encryption is based on assumption that factoring is hard
- Quantum computer can solve it in polynomial time (BQP)
- Relies on superposition and quantum Fourier transform
- Therefore a large, universal quantum computer would break RSA

# Quantum Computers - state of the art

---

- Different implementations
  - Photons (~10 qubits)
  - Ions (~14 qubits)
  - Superconductors (IBM: 17 qubits)
- Specialized machines (e.g. D-Wave >2000 “qubits”)



# Solution

---

## Post quantum cryptography

- Classical Cryptography
- Not breakable by any known quantum algorithm
- Security not proven

## Quantum cryptography

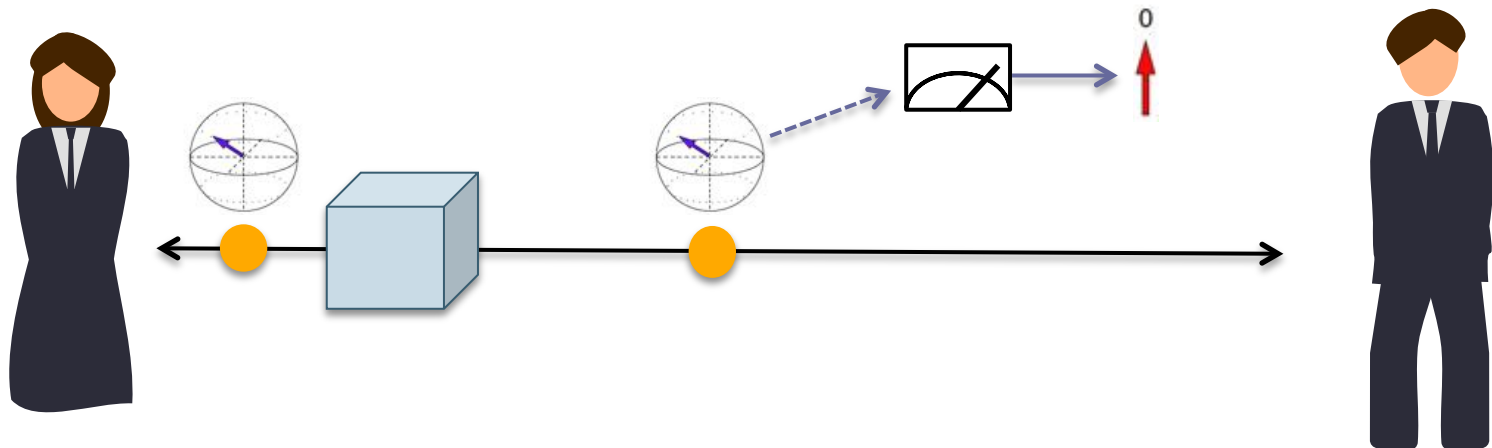
- Based on quantum systems
- Security theoretically guaranteed by the laws of physics
- First systems are commercially available



# Quantum Cryptography

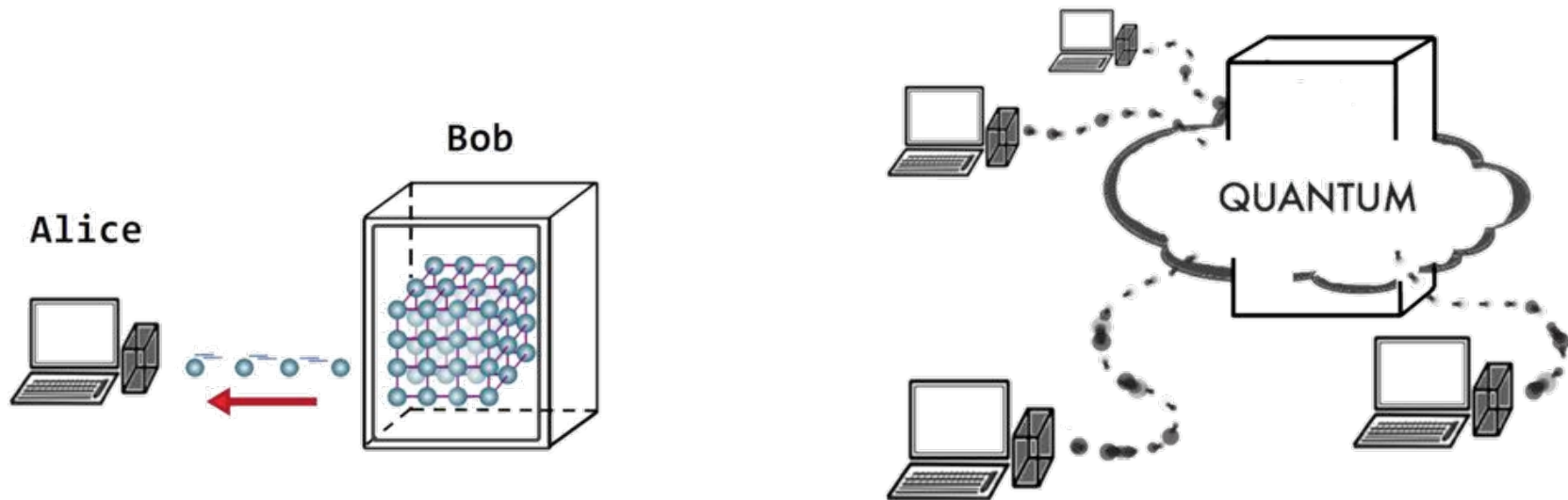
---

- Quantum Key Distribution (QKD)
- Distribution of a random one-time-pad
- Alice and Bob can find out if someone is listening

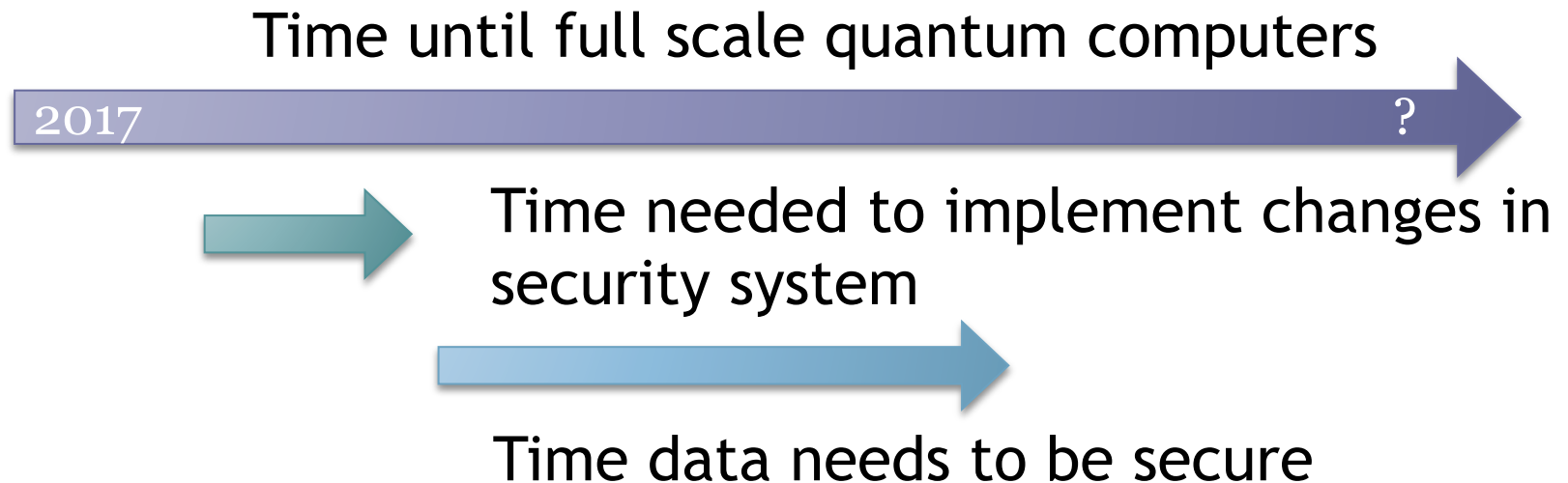


# Quantum Cloud Computation

- Nearly classical clients can evaluate quantum algorithms
- Without leaking input, output or algorithm



# When will this become a problem?



# Thank you!



