UNIVERSITATEA LUCIAN BLAGA DIN SIBIU
HPI Hasso Plattner Institut Digital Engineering · Universität Potsdam
CLUJ IT
Sibiu IT Cluster
SID 2025
Sibiu Innovation Days
06-07 November, Sibiu - RO
EMERGING DISRUPTIVE TECHNOLOGIES:
Balancing Innovation, Risks, and Societal Impact

Secure Communication in the Quantum Era: Challenges, Promises, and Limits.

R. Schwonnek, Quantum Information Group,
Leibniz Universität Hannover

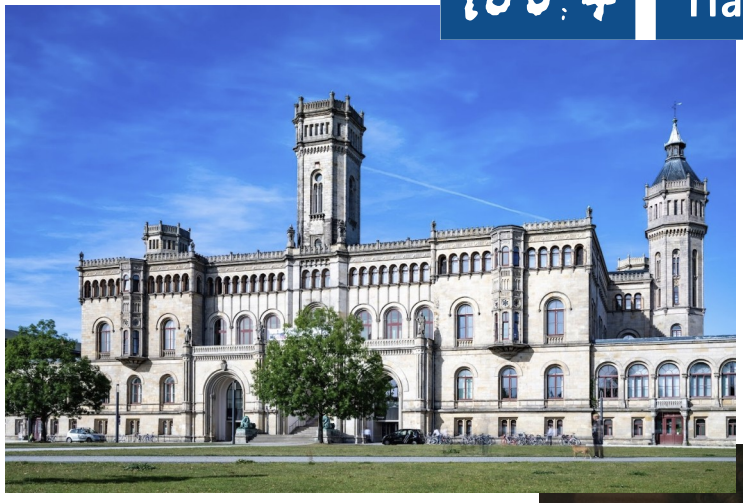
Leibniz Universität Hannover

- Leibniz University Hannover,

  26k students, 3 clusters of excellence

- Quantum Information Group
  - 3 Profs , 3 SRFs , 25 PhD and Post Docs
  - Quantum technology team

Leibniz Universität Hannover



Activities

- Quantum Frontiers Cluster of Excellence
  - Topical Group Quantum Computing Concepts
- Quantum Valley Lower Saxony
  - Industry - University partnership, research initiative
- ATIQ
  - Ion based quantum computer (50 M €)
- QUICs
  - Consultation Centre for SMUs
- SEQUIN and CBQD
  - Security proofs and certification for cryptographic devices

QF

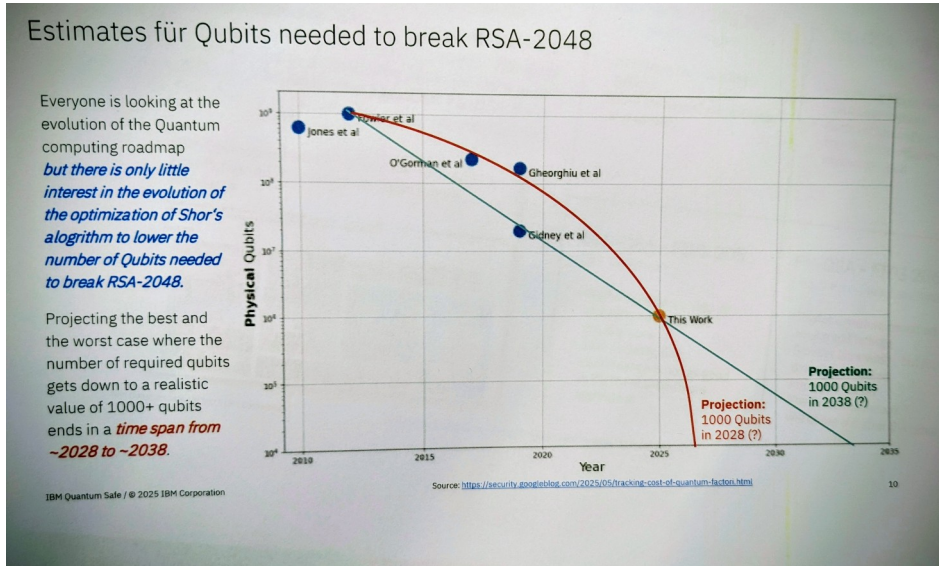
QVLS | Quantum Valley Lower Saxony

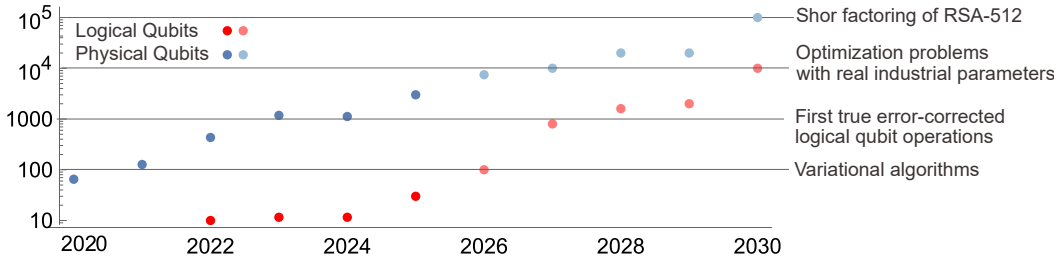
|ATIQ⟩

- Fact:

  Quantum computers can break existing public key cryptography (Shor)

- Should we worry?





Status of quantum computer development

Entwicklungsstand Quantencomputer

Federal Office for Information Security

~10 years

What can be done?

Post Quantum Cryptography (PQC)

- Protect data from decryption

Physical Layer Security (e.g. QKD)

- Protect data leaks to third parties

What is Post Quantum Cryptography ?

- Classical encryption algorithms that do not break on Shor's Algorithm
  - See talk by Florin Simedru
- Can be employed on standard IT-hardware
- Standardization in progress

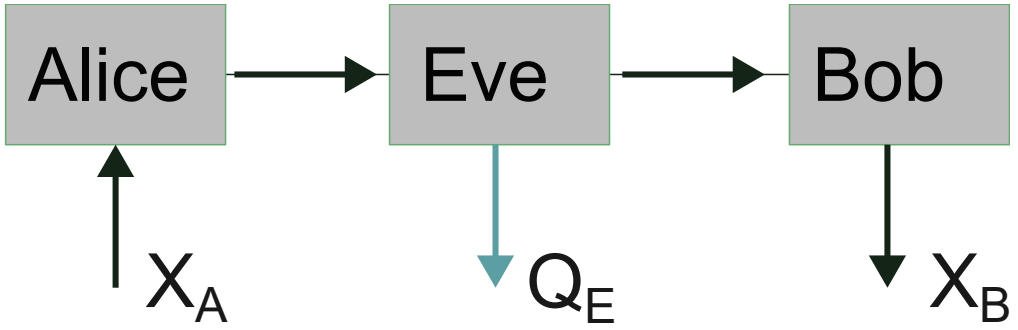
> **Post-Quantum Cryptography Standardization**
>
> *Short URL: https://csrc.nist.gov/pqc-standardization*
>
> ***HQC was selected for standardization on March 11, 2025. NIST IR 8545, Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process is now available.***
>
> ***FIPS 203, FIPS 204 and FIPS 205, which specify algorithms derived from CRYSTALS-Dilithium, CRYSTALS-KYBER and SPHINCS+, were published August 13, 2024.***

- The name is misleading
  - No security proof against quantum attacks !
  - Hinges on unproven (unprovable?) mathematical conjectures

What is Quantum Cryptography ?

- Use a quantum based communication link (usually photons)
  - Influence of an eavesdropper can be detected (no measurement without disturbance)
  - Secure exchange of secret keys → Quantum Key Distribution
- Rigorous security proofs possible (in theory)
- Rate-Distance tradeoff
  - e.g. 1000 km with 3mbit/s to 20 km with 1 Mbit/s
- Challenges:
  - Rely on correct hardware model (in practice)
  - New hardware infrastructure needed
- Need seed key for channel authentication

- Statistical Security statement



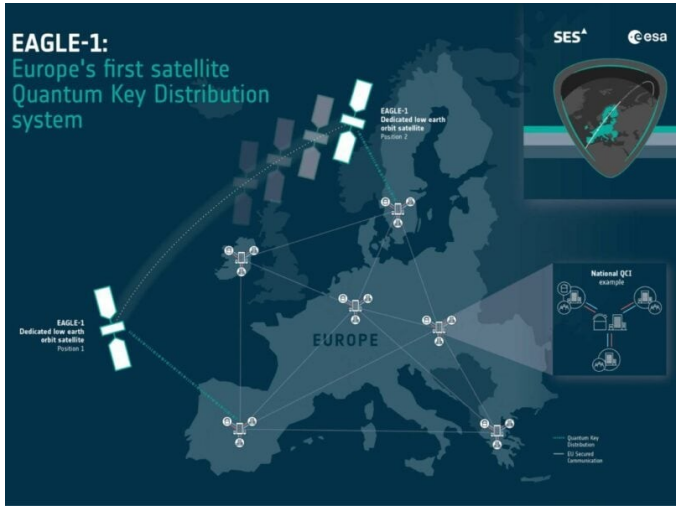
→ Estimate influence of Eve, ECC and hashing

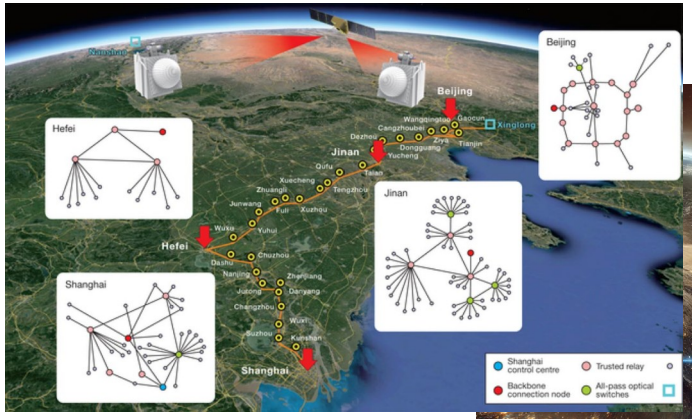
- After observing some data X_A X_B , we conclude:
  - with probability ε_{sec} is $|| \rho_{ABE}^{real} - \rho_{ABE}^{ideal} || \leq \delta_{quant}$
- Secure infrastructure: Every device is evaluated by an ε

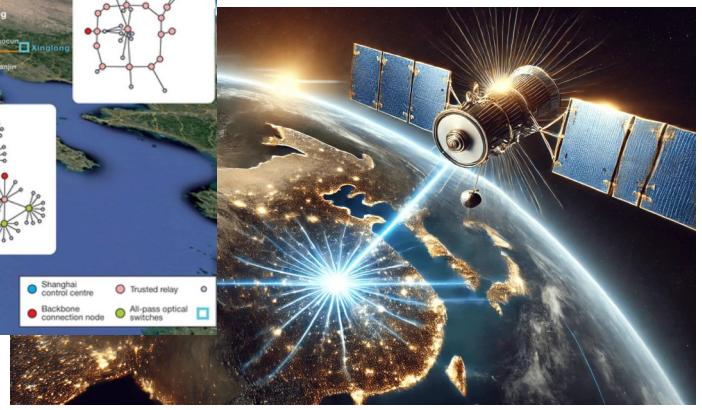
- Prepare and measure (e.g. BB84)
  - DV, single photons, qubits encoded in polarization
  - DV, mostly single photons, decoy states
  - CV, coherent continuous light sources
  - MDI, no trust on receiver
- Entanglement based (e.g. E91, DIQKD)
  - entangled single photons
  - DIQKD security based on Bell-Test

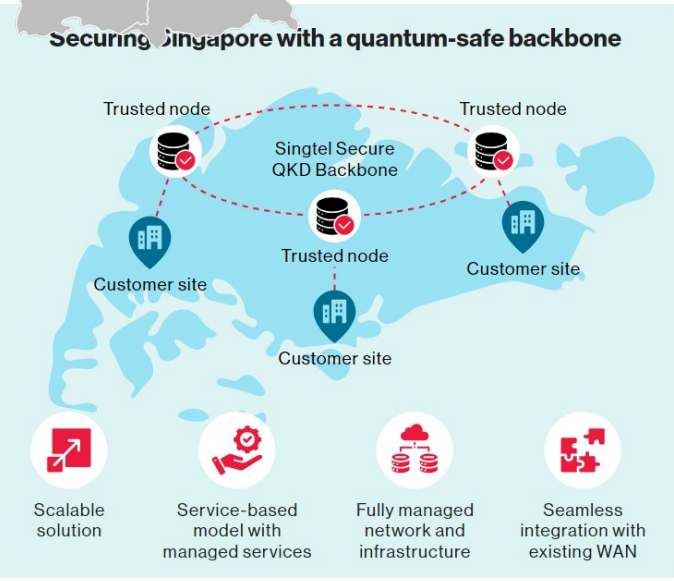
- QKD networks

EuroQCI

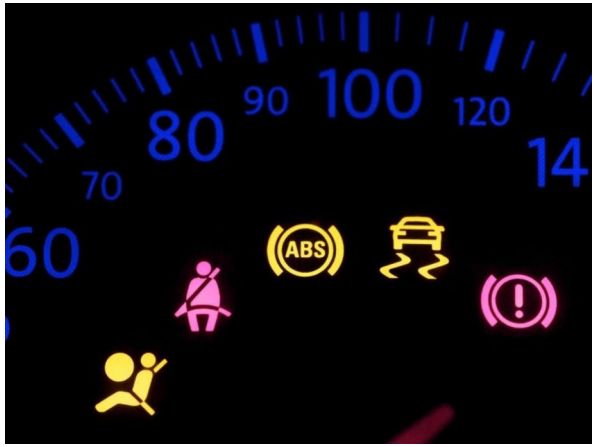








- PQC
  - Software upgrades
  - Trust your Mathematician



- QKD
  - Hardware investment
  - Trust your Engineers

- Things you can do now:
  - Ensure crypto agility
  - Bill of Materials
  - Talk to your local university

- Security is a process, not a product