

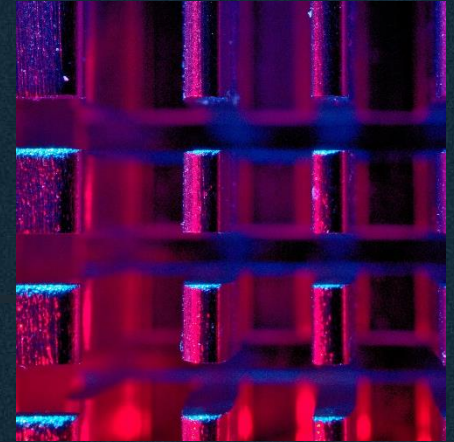
# Quantentechnologie

## Digi.Lab

# Quantentechnologie im Digi.Lab

## Quantenkryptographie

- **Postquantum Verschlüsselung**  
Postquanten - Software - Algorithmen
- **Quantenverschlüsselung**  
Quantenverschlüsselung auf Basis unumstößlicher physikalischer Gesetze

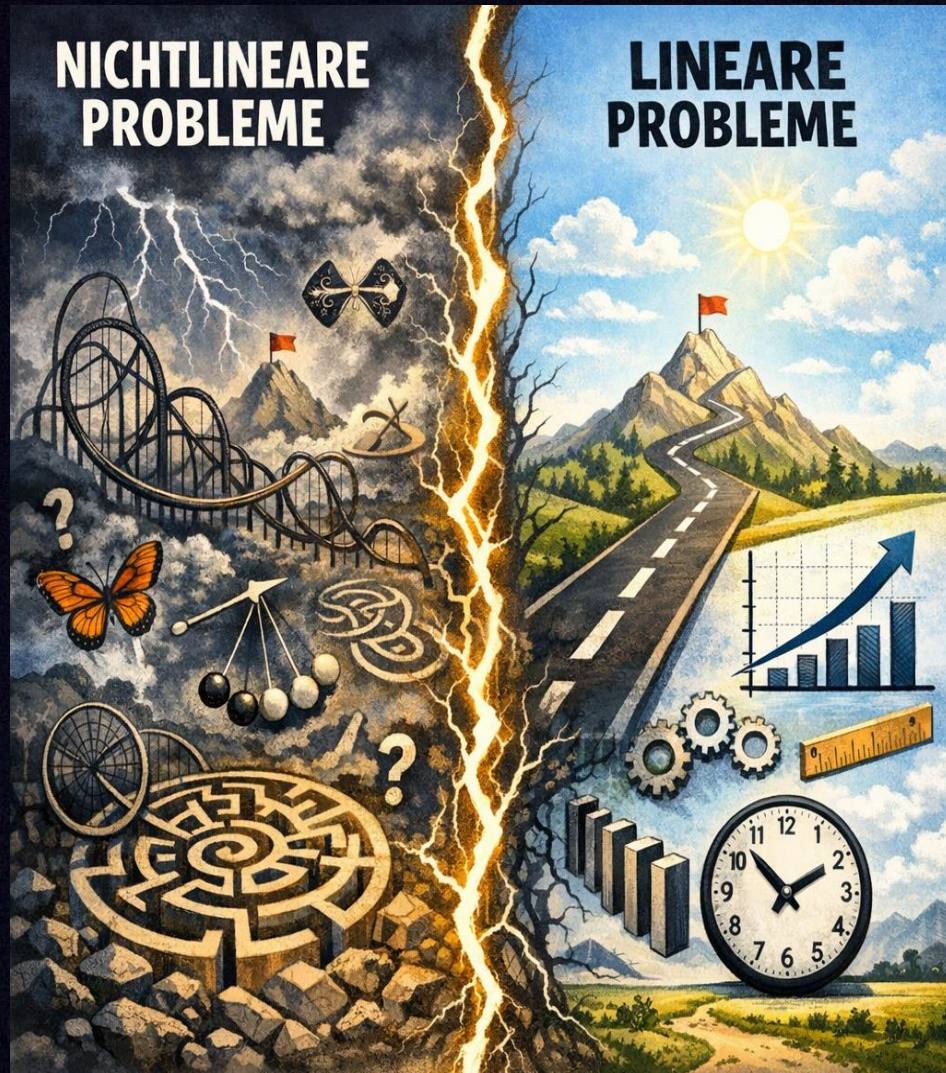


## Quantensensorik

- Nutzung der Gesetze der Quantenphysik
- Neue Wege zu hoher Präzession und Sensitivität
- Niedrige Nachweisgrenzen für kleinste Mengen
- Stabile Referenzen für belastbare Quantifizierung
- Perspektive für kompakte und besonders energieeffiziente Sensorik



# Quantencomputer versus Binärcomputer



KI-Generiert

Aktuelle Computer können sehr schnell und effektiv lineare Probleme lösen.

Messungen, Zeitreihenanalyse

Quantencomputer finden effizient Strukturen in sehr großen Datenmengen

Entschlüsselung von Daten

Quantencomputer können schnell und effektiv nicht lineare Probleme lösen

Simulation bei der Herstellung von neuen Molekülverbindungen (neue Materialien)



# Quantenkryptographie

Peter Shor Quantenalgorithmus

Algorithmus zum Brechen von aktuellen  
Verschlüsselungen

Realtime Entschlüsselung



# Quantenbegriffe

## Qubit

Informationseinheit die aufgrund der Quantenmechanik gleichzeitig mehrere Zustände annehmen kann.

Klassische Bits: 0 oder 1

Qubit: 0 oder 1 oder eine Überlagerung beider Zustände.

Logische Q-Bits: Rauschfrei, Nachvollziehbar, für Entschlüsselung anwendbar.

## Superposition

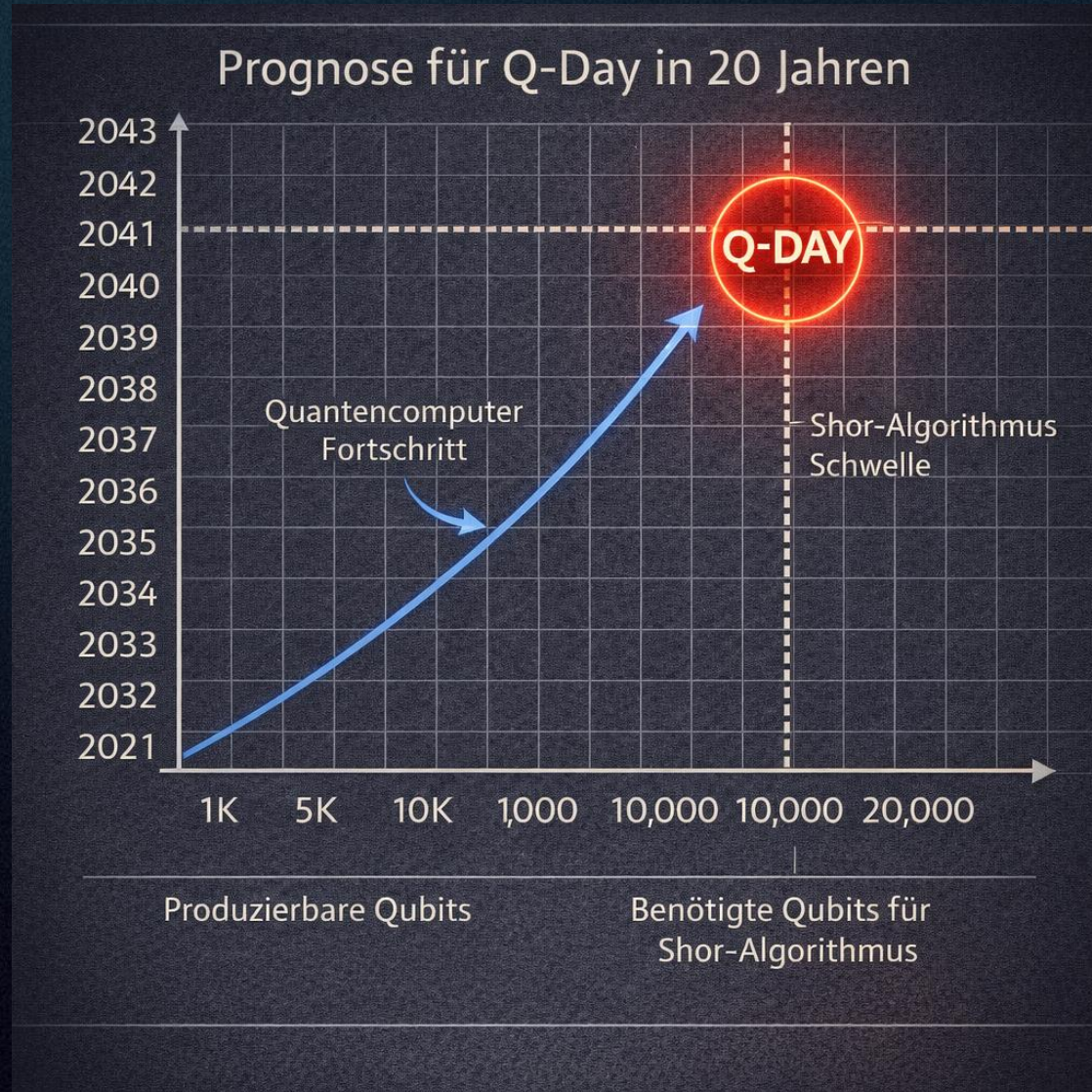
Ein Qubit kann gleichzeitig mehrere Zustände einnehmen, wodurch parallele Berechnungen möglich werden.

## Verschränkung

Zwei oder mehr Qubits können miteinander verbunden sein, sodass eine Änderung an einem Qubit sofort Auswirkungen auf die anderen hat, unabhängig von der Entfernung.



# Quantenentschlüsselung: Zeitachse



## Q-Day

Der Tag an dem Quantencomputer mit dem Peter Shor Algorithmus RSA Verschlüsselungen in Echtzeit hacken können.

## Q-Day Annahme vor 2-3 Jahren

Q-Day in 10 – 20 Jahren



# Quantenentschlüsselung: Zeitachse

## Verbesserung des Peter Shor Algorithmus

Benötigt weniger Q-Bits

## Anzahl logischer Q-Bits

Es werden immer mehr logische Q-Bits erzeugt + synthetische

## Q-Day rückt rasant näher

Aktuelle Schätzung 2-5 Jahre





Quantenkryptographie

**SNDL**



# Post Quantum Verschlüsselung

- Durch NIST verifizierte Algorithmen, welche aktuell als Quantensicher eingestuft sind.
- Softwarealgorithmen – keine physische quantenmechanische Sicherheit
- Aktuell haben wir Digi.Lab x WienIT folgende Post Quantum Algorithmen implementiert
- - Dilithium
  - Falcon
  - Kyber
  - McEliece
  - NTRU
  - Rainbow
  - Saber

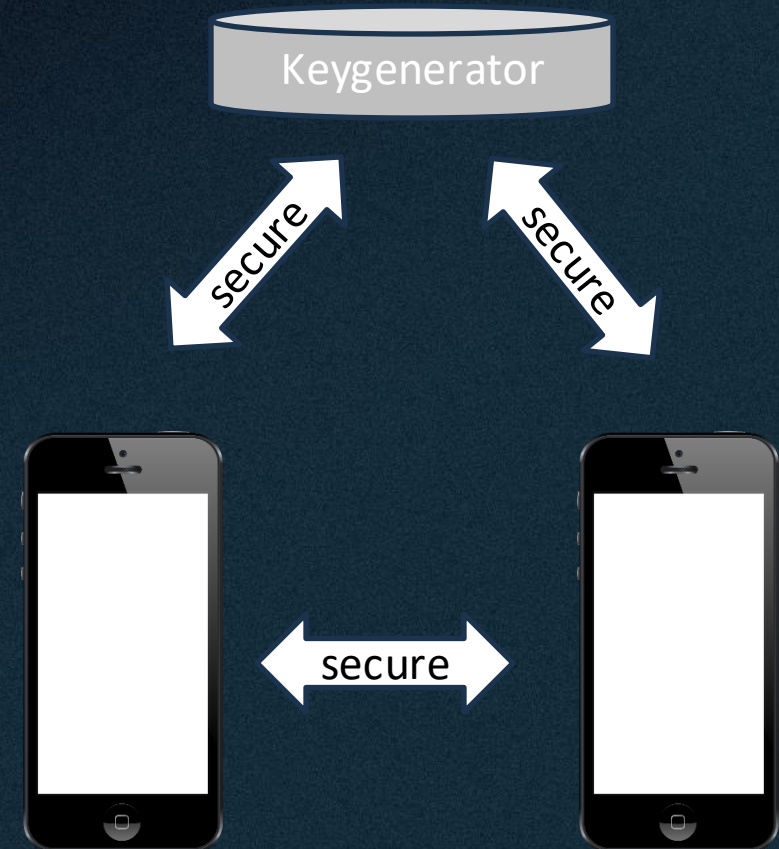


# Digi.Lab: Quantenkommunikation

## Quantenverschlüsselungs Demonstrator

Funktionierender Proof of Concept (POC)

- Aufbau einer quantenverschlüsselten Serververbindung
- Erzeugen eines asynchronen Quantenschlüsselpaares
- Mehrere postquantum Verschlüsselungsverfahren
- Asynchrone quantenverschlüsselte Kommunikation
- Peer to Peer Kommunikation
- Verfügbar auf Windows, Android, iPhone

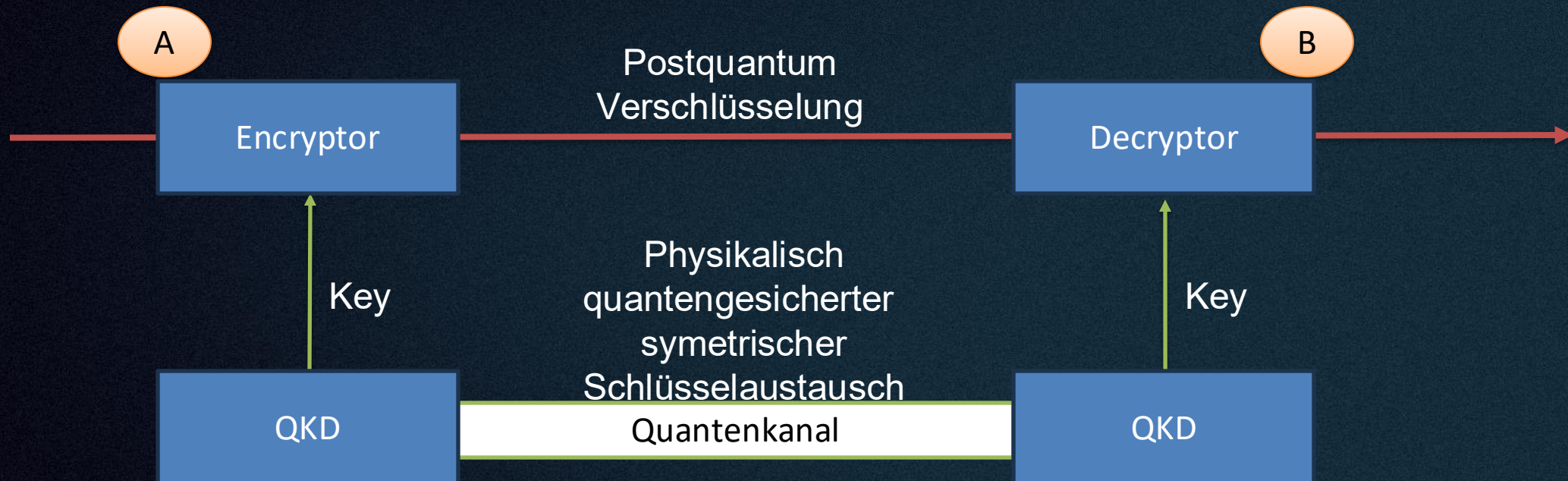




# Quantum Key Distribution

## Quantenverschlüsselung mit QKD

- Hardwarebasierter Quanten Schlüsselaustausch.
- Verwendet quantenmechanische Sicherheit  
Verschlüsselung auf Basis unumstößlicher physikalischer Gesetze





# Digi.Lab: Quantenkryptographie Phase 2

## Quantenverschlüsselung Konzernweit

- Aufbau mehrerer Quantenschlüsselserver
- Webschnittstelle für Quantenschlüssel
- SDK für Endgeräte zur lokalen Ver- und Entschlüsselung
- Verfügbar für alle unsere Partnerunternehmen





# Quantensensorik



## Quantensensorik

Nutzung der Quantenmechanik

- Quantenverschränkung
- Quanteninterferenz
- Quantenzustandsverkleinerung

Detektion magnetischer und elektrischer Felder mit einer räumlichen Auflösung von wenigen Nanometern bis hin zu einzelnen Elektronen- und Kernspins möglich

Molekülspezifische Erfassung erlaubt auch flüchtige organische Verbindungen (VOCs) zu identifizieren und zu quantifizieren

Erfassung auf größeren Distanzen

Übertrifft Leistung von klassischen Verfahren



# Quantensensorik

## Digi.Lab Methangas Quanten Sensoren

- Sehr geringe Nachweisgrenze
- Autonomes permanentes Monitoring
- Integrierte Referenzzelle  
bedeutet kalibriertes Messen  
Reduktion von Fehlalarmen
- Audit- und Reporting fähige Datenketten
- Akkubetrieb 10-12 Stunden





# Quantensensorik

## Digi.Lab Methangassensor

Optisch mit Referenzquelle

Präzise, stabilere Messung

Sehr gute Driftkompensation und Messstabilität

Quantifizierbar und Vertrauenswürdig

## Aktuelle Sensorik

MOX / Heizer

Metalloxid Semikonduktor mit beheizter Platte

Leckalarm erst zwischen 300 - 10.000 ppm

Beeinflussbar durch Feuchte, Temperatur und andere Gase

Grob erkennen



# Ready for takeoff!

digilab.wienit.at

✉ [digilab@wienit.at](mailto:digilab@wienit.at)

📷 [@lifeatwienit](https://www.instagram.com/@lifeatwienit)

🎵 [@wienit](https://www.tiktok.com/@wienit)

in [wienit](https://www.linkedin.com/company/wienit)

📄 [wienit.at/blog](https://wienit.at/blog)

📺 [wienit](https://www.youtube.com/wienit)

+43 5 90405 47603

Thomas-Klestil-Platz 13,  
1030 Wien

DIGI.LAB ×  WIEN IT