# Quantenkryptographie (Teil 2) - Zusammenfassung

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik

# Agenda

1. Einführung
2. Wiederholung BB84
3. Qubits und Messbasen
4. Zusammengesetzte Systeme
5. Verschränkung
6. Anwendung von Verschränkung
7. Shared Randomness
8. Schmidt-Darstellung
9. Dichtematrizen
10. Partielle Spur
11. Verschränkungsmaß
12. Entropie und Monogamie
13. Entanglement Swapping
14. Entanglement Distillation
15. CHSH-Ungleichung (klassisch)
16. CHSH-Ungleichung (Quantenversion)
17. CHSH-Ungleichung (Simulation)
18. Ekert-Protokoll
19. Sicherheit und DIQKD
20. **Zusammenfassung**

# Zusammenfassung

- Einsatz von Kryptographie ist essentiell für die sichere Datenübertragung und den Schutz der Privatsphäre.
  - Es existieren viele etablierte klassische Verfahren.
    - Symmetrische und asymmetrische
    - Asymmetrische Systeme bilden Grundlage für den Schlüsseltausch bei der Anwendung von symmetrischen Krypto-Systemen.

- Verfahren sind in der Regel nur "berechnungssicher".
  - Außer One-Time-Pad, das perfekt sicher ist!

# Zusammenfassung

- Quantencomputer können die heute verwendeten asymmetrischen Systeme brechen.

- Zwei Lösungsvarianten:
  - Einsatz von Post-Quantum-Kryptographie.
    - Algorithmen sind nach wie vor "berechnungssicher".
    - Kein echter Sicherheitsbeweis möglich. Beruhen auf nicht-beweisbaren Annahmen.
  - Einsatz von Quanten Key Distribution.
    - Basiert auf sicherem Schlüsseltausch (Detektion eines Lauschers).
    - Es existieren Sicherheitsbeweise!

# Verschränkung als Ressource

- Verschränkung ist eine universelle Ressource, die kein klassisches Äquivalent besitzt.
  - Verschränkung ist experimentell beherrschbar.
  - Bei Zwei-Qubit-Systemen ist die Verschränkung "gut verstanden".
  - Maximal verschränkte Qubits sind "monogam".
  - Verschränkung stellt eine neue Art von Korrelation dar.
    - Grundlage verschiedener Protokolle.
  - Maximale Verschränktheit kann überprüft werden.
    - CHSH-Ungleichung ist nur eine von vielen sogenannten Bell-Ungleichungen.
  - Für verschränkungsbasierte Protokolle existieren Sicherheitsbeweise.

# Das Ekert-Protokoll

- QKD-Protokoll auf Basis von Verschränkung (Ekert 1991)
  - Es gibt mittlerweile verschiedene Varianten.
- Zur Schlüsselgenerierung werden maximal verschränkte Qubits im folgenden Zustand benutzt

$$|\Psi\rangle = \frac{1}{\sqrt{2}}( |00\rangle + |11\rangle )$$

  - Ressource für *Shared Randomness*
    - Erzeugung des Schlüssels
    - Schlüssel wird erst bei der Messung generiert!
    - Detektion eines Lauschers basiert auf der Überprüfung der CHSH-Ungleichung.
  - "Klassische" Nachbearbeitung wie bei BB84.

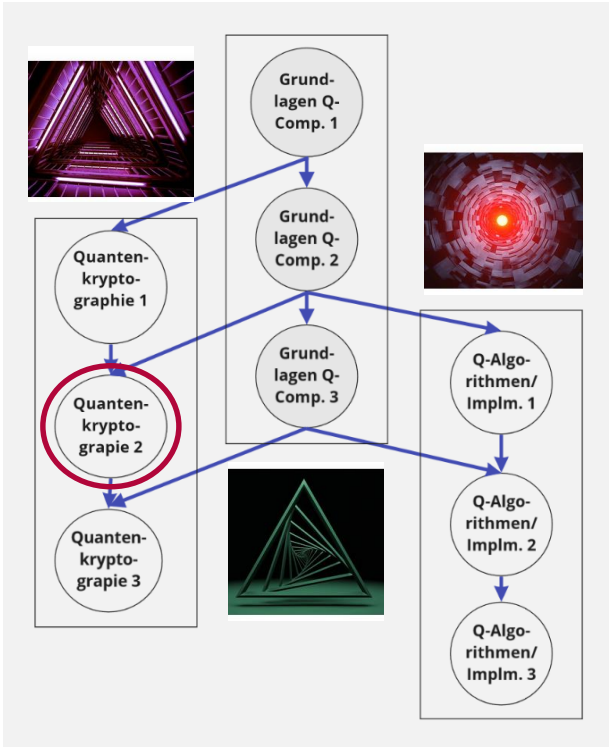
# Literatur zu QKD

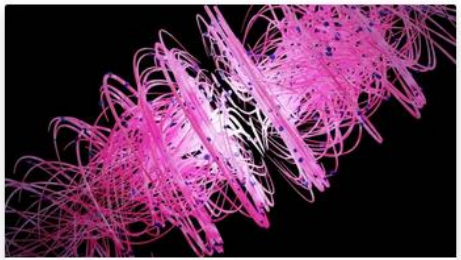
- Primärquelle sind die Originalveröffentlichungen.
  - Oft zu finden auf https://arxiv.org/

- Viele Bücher zum Thema Quantum Computing enthalten einführende Kapitel zur QKD.

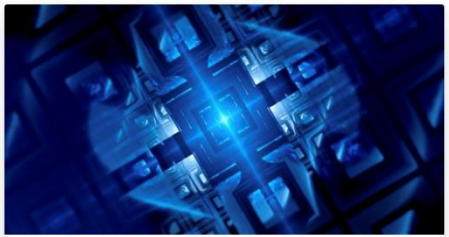
- Kleine Auswahl an Lehrbüchern speziell zum Thema (QKD):
  - Loepp und Wooters: *Protecting Information. From Classical Error Correction to Quantum Cryptography*, Cambridge (2006)
  - Kollmitzer et al: *Applied Quantum Cryptography*, Lecture Notes in Physics, Springer (2010)
  - Ramona Wolf: *Quantum Key Distribution. An Introduction with Exercises*, Springer (2021)

# Agenda Gesamtkursprogramm

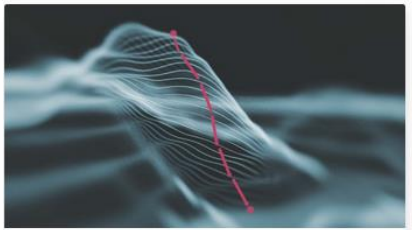


Quantum Computing Forum



Introduction to Quantum Computing with Qiskit (with IBM Quantum...



Quantum Machine Learning (with IBM Quantum Research)

**Quanten-kryptographie**

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern

# Vielen Dank
# für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik