Quantenkryptographie (Teil 2) - Einführung

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik

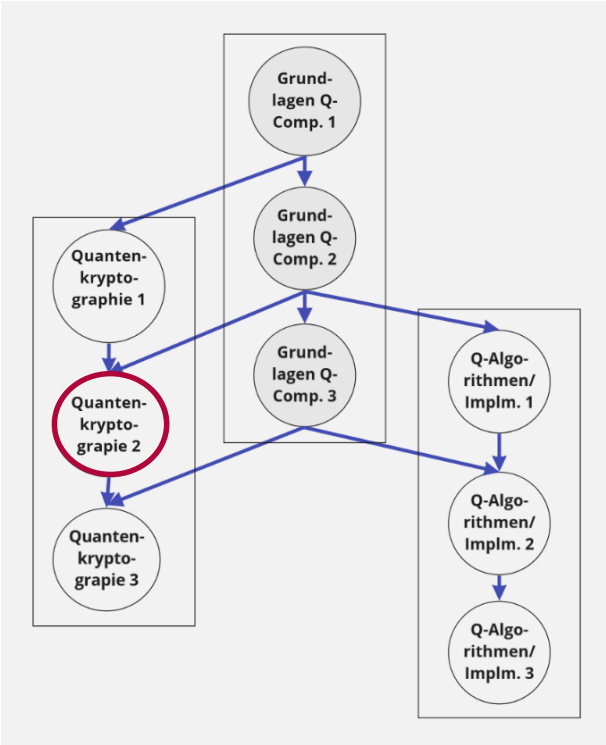
Dozent

- Jörg Hettel
- Professor an der Hochschule Kaiserslautern,
- Fachbereich Informatik und Mikrosystemtechnik,
- Seit über 10 Jahren Vorlesungen zu den Themen:
  - Quanteninformation,
  - Quantencomputing.

Hochschule Kaiserslautern
University of Applied Sciences

Informatik und Mikrosystemtechnik
Zweibrücken

Agenda Gesamtkursprogramm



Grundlagen des Quantencomputing, 1-3

Prof. Dr. Bettina Just, THM

Quantenkryptographie 1-3

Prof. Dr. Jörg Hettel,
HS Kaiserslautern

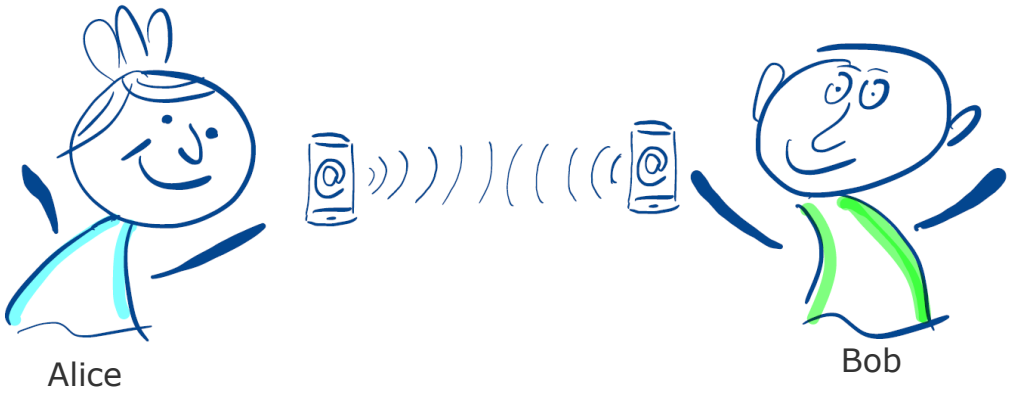
Quantenalgorithmen und Implementierung 1-3

Prof. Dr. Gerhard Hellstern,
DHBW Ravensburg

Worum geht es in dem Kurs?

Sichere Kommunikation durch Anwendung kryptographischer Methoden.

- Quantencomputer können die heute verwendeten asymmetrischen Systeme brechen.



Lösungsmöglichkeiten

- Zwei Lösungsvarianten:
  - Einsatz von Post-Quantum-Kryptographie.
    - Algorithmen sind nach wie vor "berechnungssicher".
    - Kein echter Sicherheitsbeweis vorhanden. Beruhen bis jetzt auf (noch) nicht-beweisbaren Annahmen.
  - Einsatz von Quanten Key Distribution (QKD).
    - Realisiert einen "sicheren" Schlüsseltausch.
    - Sicherheit basiert auf der Detektion eines Lauschers.
    - Sicherheitsbeweise existieren unter bestimmten Annahmen.

Quanten Key Distribution

- Zwei Varianten:
  - *Prepare-and-Measure*-Protokolle, wie das BB84 (Kurs 1).
  - ***Entanglement*-basierte Protokolle.**

- Legen den Schwerpunkt auf die **Verschränkung (Entanglement)!**

- Phänomenologische Beschreibung steht im Mittelpunkt.
  - Darstellung nicht immer exakt.
  - Es wird dieses Mal mehr gerechnet.
  - Zeige auch (Rechen-) Beispiele mit Qiskit.
    - Das ist keine Qiskit-Einführung

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

Vielen Dank
für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik