Quantenkryptographie (Teil 2)
- Entanglement Swapping

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

Entanglement Swapping

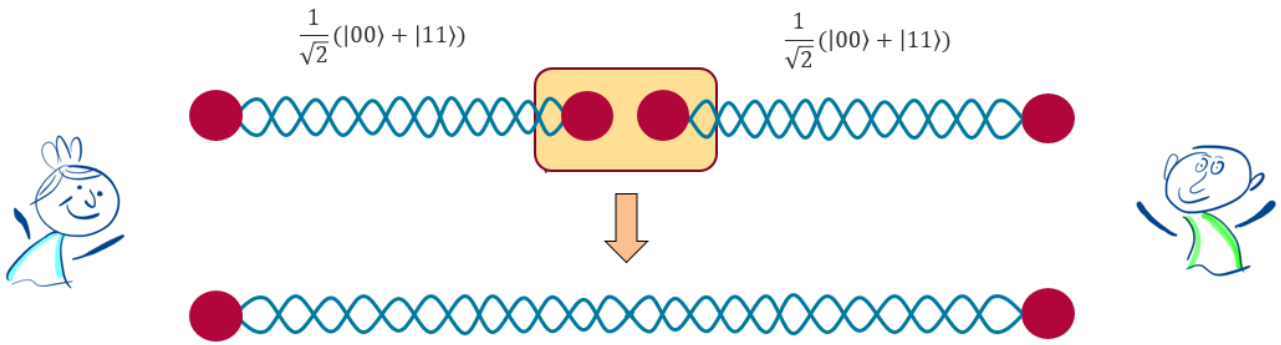
- Die "Einzelteile" eines verschränkten Qubit-Paars müssen oft über weite Strecken transportiert werden.
  - Als "Endstationen" für eine Teleportation
  - Beim Ekert-Protokoll zur Schlüsselgenerieung
  - und vieles mehr

- Qubits können aber nicht kopiert und verstärkt werden.
  - Transport von Qubits ist somit wegen "Störungen" limitiert.

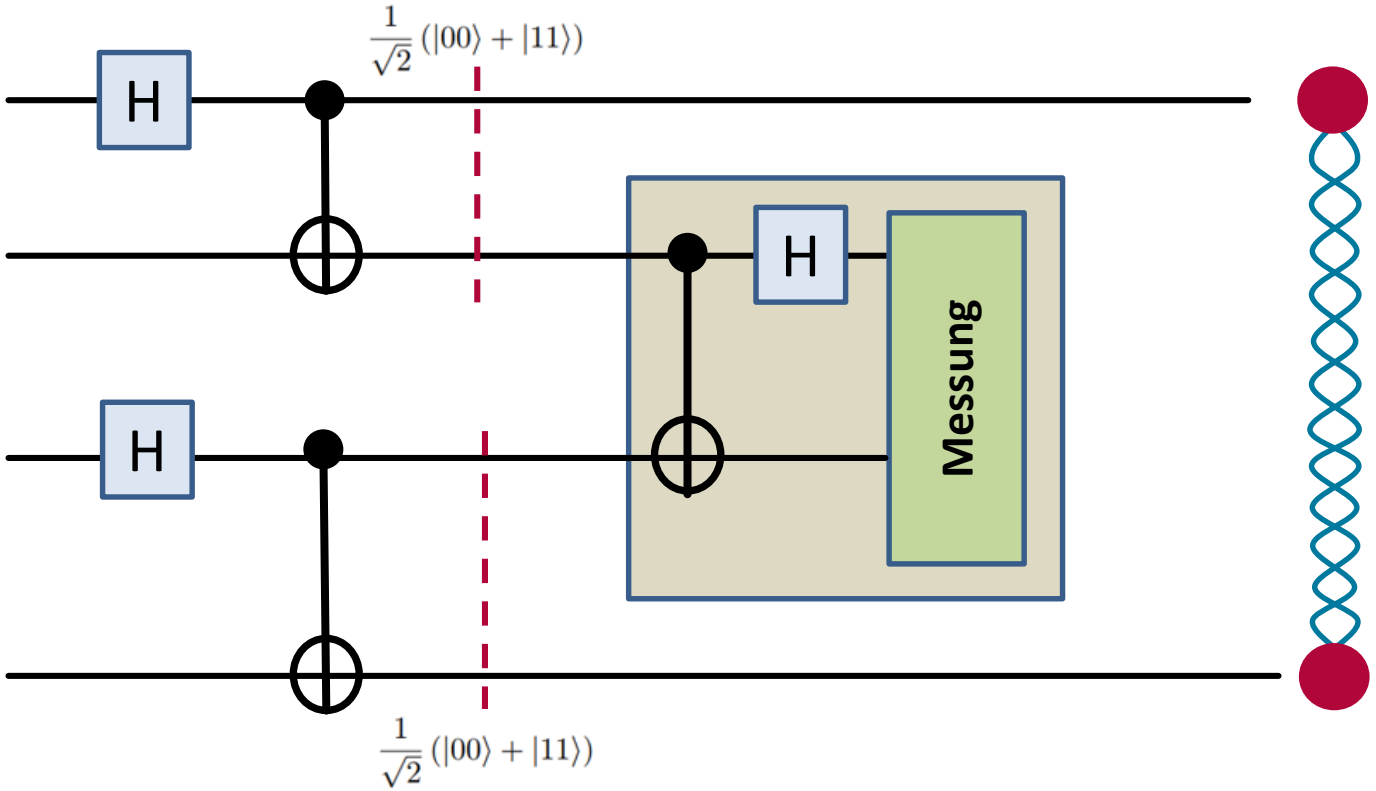
- Frage: Wie kann eine Verschränkung von zwei Qubits über weite Strecken erreicht werden?

Die Idee

- Man vereinigt zwei verschränkte Qubit-Paare durch geschickte Manipulation zu einem verschränkten Qubit-Paar.
  - Vergrößerung der Distanz der verschränkten Qubits.



Schaltkreis



Analyse (1)

- Ausgangspunkt sind zwei verschränkte Qubit-Paare

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\Psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

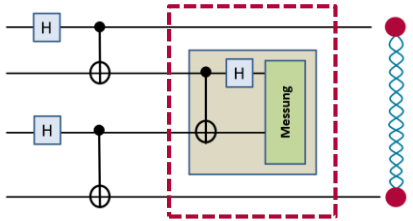
- Die zu einem Gesamtsystem zusammengefügt werden

$$|\Psi_1\rangle \otimes |\Psi_2\rangle = \frac{1}{2}(|00\rangle\,|00\rangle + |00\rangle\,|11\rangle + |11\rangle\,|00\rangle + |11\rangle\,|11\rangle)$$

Analyse (2)

- Anwendung von CNOT auf $\frac{1}{2}(|00\rangle|00\rangle + |00\rangle|11\rangle + |11\rangle|00\rangle + |11\rangle|11\rangle)$

$$|\Psi_1\rangle \otimes |\Psi_2\rangle = \frac{1}{2}(|00\rangle|00\rangle + |00\rangle|11\rangle + |11\rangle|10\rangle + |11\rangle|01\rangle)$$



- Anwendung von Hadamard auf das zweite Qubit

$$\begin{aligned}|\Psi_1\rangle \otimes |\Psi_2\rangle = \frac{1}{2\sqrt{2}}\big(&|0\rangle(|0\rangle + |1\rangle)|00\rangle \\ &+ |0\rangle(|0\rangle + |1\rangle)|11\rangle \\ &+ |1\rangle(|0\rangle - |1\rangle)|10\rangle \\ &+ |1\rangle(|0\rangle - |1\rangle)|01\rangle\big)\end{aligned}$$

$$\begin{aligned}|\Psi_1\rangle \otimes |\Psi_2\rangle = \frac{1}{2\sqrt{2}}\big(&|00\rangle|00\rangle + |01\rangle|00\rangle \\ &+ |00\rangle|11\rangle + |01\rangle|11\rangle \\ &+ |10\rangle|10\rangle - |11\rangle|10\rangle \\ &+ |10\rangle|01\rangle - |11\rangle|01\rangle\big)\end{aligned}$$

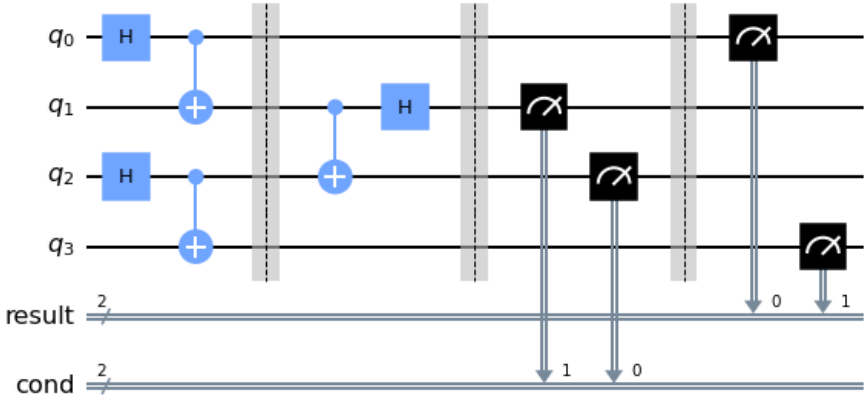
Analyse (3)

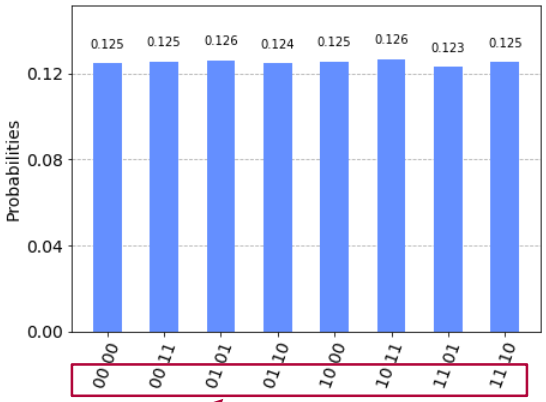
- Messung der beiden mittleren Qubits ergibt vier mögliche Ergebnisse.
  - Alle mit der Wahrscheinlichkeit ¼

$$
\begin{aligned}
00 &\rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
01 &\rightarrow \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
10 &\rightarrow \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
11 &\rightarrow \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned}
$$

- Je nach Messergebnis muss noch eine "Nachverarbeitung" erfolgen.
  - Anwendung eines X- oder Z-Gatter.
  - Klassische Kommunikation ist hierzu notwendig.

Simulation (Qiskit)

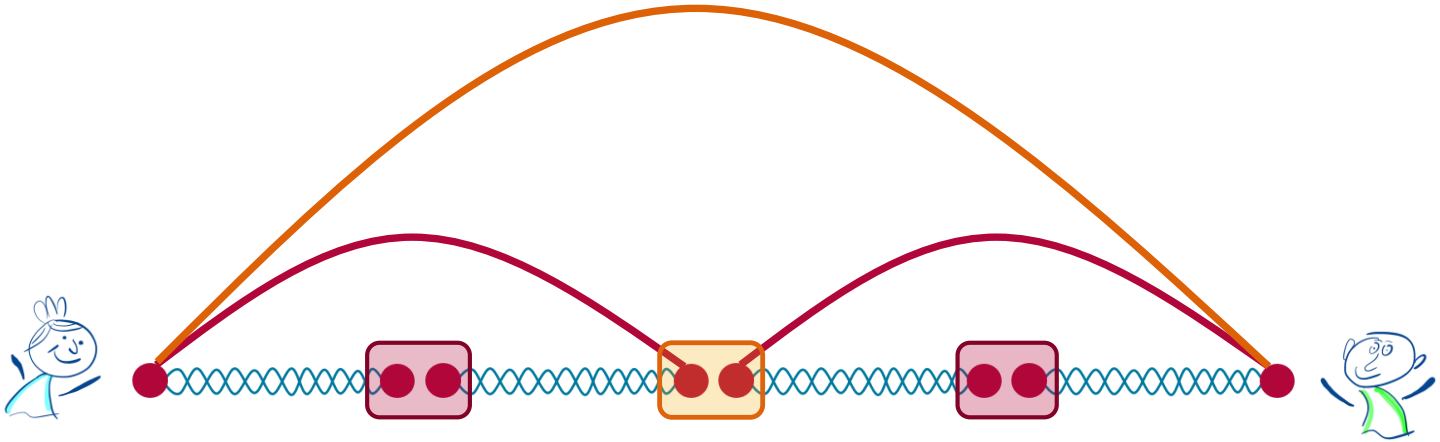




Messergebnis der mittleren Qubits

Erweiterung

- Durch eine "Reihenschaltung" können auch große Distanzen überbrückt werden.



Probleme

- Bei der hier vorgestelltem Verfahren müssen die beiden Qubits gleichzeitig in der "Austauschstation" vorliegen.
  - Bei Photonen (Lichtteilchen) ist das technisch sehr aufwendig bzw. schwierig.

- Für ein praktikables Entanglement Swapping wird eine Medium zur Speicherung von Qubits benötigt.
  - Ein sogenannter Quantenspeicher (QRAM).

Zusammenfassung

- Zwei verschränkte Qubit-Paare können so gekoppelt werden, dass ein neues verschränktes Paar entsteht.
  - Die zwei Qubits des neu erzeugten Verschränkungspaars müssen hierzu nicht lokal interagieren.
    - Müssen sich nicht treffen.
- Durch ein "Hintereinanderschalten" des Vorgangs können (theoretisch) weit entfernte Qubits verschränkt werden.
  - Das ist (aber noch) eine technische Herausforderung.
- Für eine praktikable Realisierung müssen Qubits gespeichert werden.
  - Grundlage für Quantum Repeater.

Vielen Dank
für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik