Quantenkryptographie (Teil 2)
- Entanglement Distillation

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik

Agenda

Entanglement Distillation

- Maximal verschränkte Qubit-Paare sind eine wichtige Ressource.
- Werden benötigt für:
  - Teleportation
  - Dichtekodierung
  - Ekert-Protokoll
  - und vieles mehr

- In der Realität sind verschränkte Qubit-Paare oft nicht maximal verschränkt.
  - "Fehlerhafte" Produktion
  - Übertragungsfehler beim Versenden
- Es wird eine Art "Verschränkungskorrektur" benötigt.

Die Frage bzw. Idee

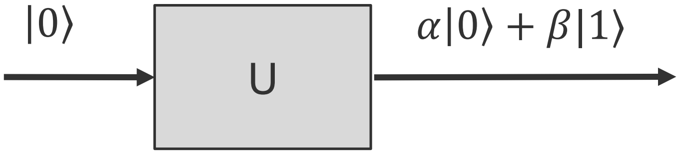
- Kann man aus nicht-maximal verschränkten Qubit-Paaren maximal verschränkte Qubit-Paare erzeugen?
  - Antwort lautet "Ja, das geht!"

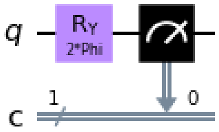
- Betrachte im Folgenden zwei einfache Verfahren:
  1. Erzeugung eines maximal verschränkten Qubit-Paares, wenn z.B. ein Baustein keine echt gleichverteilte Superposition liefert.
  2. Erzeugung eines Qubit-Paares mit höherem Verschränkungsgrad aus zwei "weniger gut" verschränkten Qubit-Paaren.

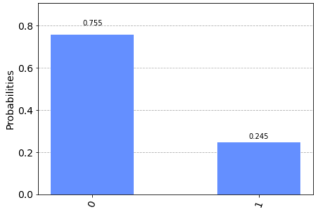
Erzeugung eines maximal verschränktes Qubit-Paar

- Angenommen, wir haben einen Baustein, der keine gleichverteilte Superposition liefert, sondern

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{mit} \quad \alpha \neq \beta, |\alpha|^2 + |\beta|^2 = 1$$



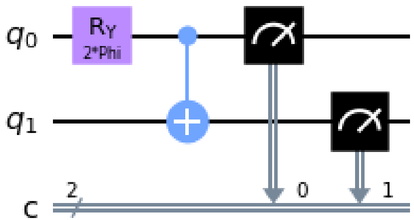


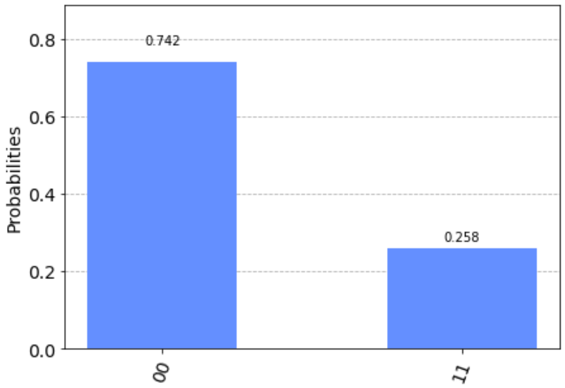


Anwendung eines Bell-Schalkreis

- Aus dem Qubit $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ wird:

$$\alpha|00\rangle + \beta|11\rangle$$

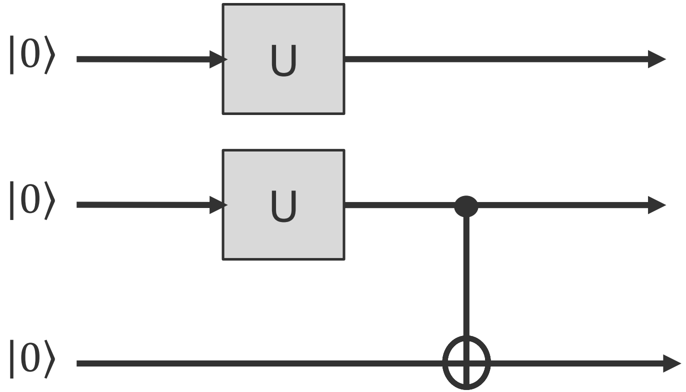




Schaltkreis (1)

- Zwei nicht-gleichverteilte Qubits plus ein $|0\rangle$ werden wie folgt kombiniert:

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|00\rangle + \beta|11\rangle)$$
$$= \alpha^2 \, |0\rangle|00\rangle + \alpha\beta|0\rangle|11\rangle + \alpha\beta|1\rangle|00\rangle + \beta^2|1\rangle|11\rangle$$

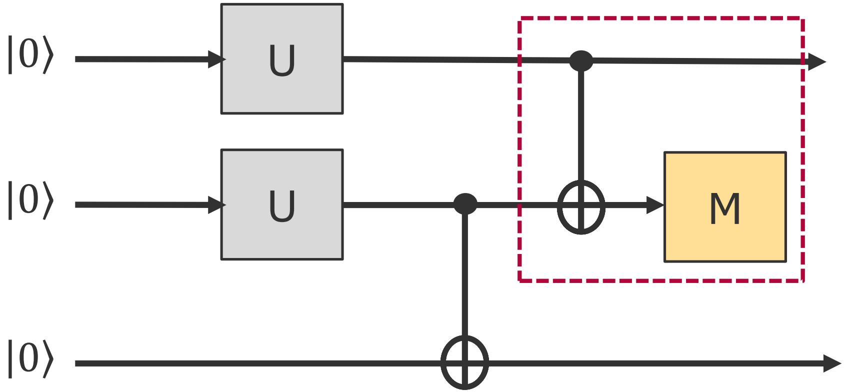


Schaltkreis (2)

- Anwendung eines CNOT-Gatter

$$\alpha^2\ |0\rangle|00\rangle + \alpha\beta|0\rangle|11\rangle + \ \alpha\beta|1\rangle|00\rangle + \beta^2|1\rangle|11\rangle$$
$$\Longrightarrow\ \ \alpha^2\ \ |0\rangle|00\rangle + \alpha\beta|0\rangle|11\rangle + \ \alpha\beta|1\rangle|10\rangle + \beta^2|1\rangle|01\rangle$$

- und anschließende Messung des mittleren Qubits



Auswertung

- Ausgangszustand vor der Messung

$$\alpha^2 \,|0\rangle|00\rangle + \alpha\beta|0\rangle|11\rangle + \alpha\beta|1\rangle|10\rangle + \beta^2|1\rangle|01\rangle$$

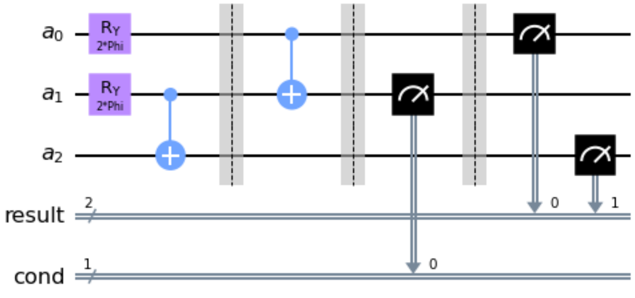
- Messergebnis "0" erzeugt mit Wahrscheinlichkeit $\alpha^4 + \beta^4$ den Zustand zwischen erstem und dritten Qubit

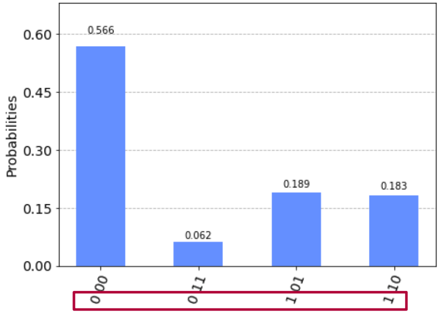
$$\frac{\alpha^2|00\rangle + \beta^2|11\rangle}{\sqrt{\alpha^4 + \beta^4}}$$

- Messergebnis "1" erzeugt mit Wahrscheinlichkeit $2\alpha\beta$ den Zustand:

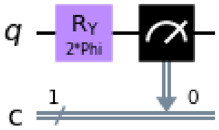
$$\frac{1}{\sqrt{2}}(\,|01\rangle + |10\rangle)$$

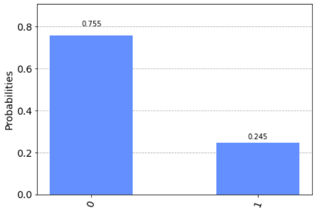
Simulation mit Qiskit





Mit dem "verzerrenden" Baustein Ry

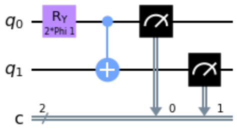




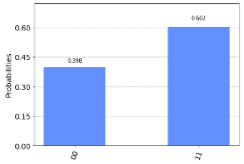
Entanglement "Concentration"

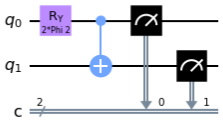
- Aus zwei "wenig" verschränkten Qubit-Paaren kann ein "besser" verschränktes Paar erzeugt werden.
  - Iterative Anwendung des Prozesses möglich.
  - Man benötigt aber dann zu Beginn entsprechend viele Qubit-Paare.

- Ausgangspunkt des Beispiels

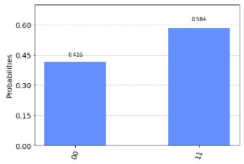


$$|\Psi_{01}\rangle \;=\; \alpha_0\,|00\rangle + \beta_0\,|11\rangle$$

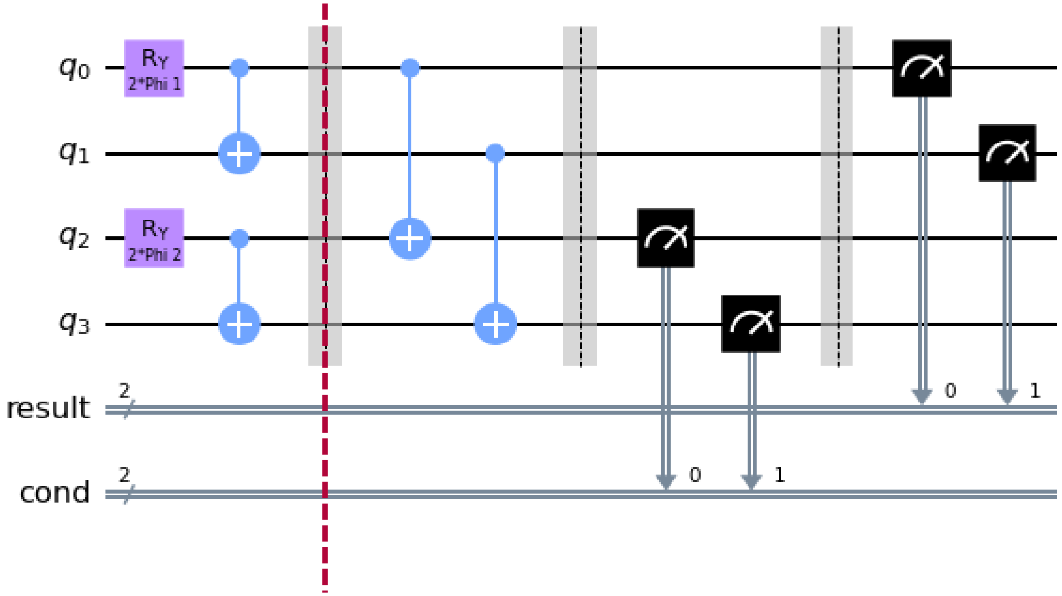




$$|\Psi_{23}\rangle \;=\; \alpha_2\,|00\rangle + \beta_2\,|11\rangle$$



Schaltkreis (mit Qiskit)



$$|\Psi_{0123}\rangle = |\Psi_{01}\rangle \otimes |\Psi_{23}\rangle = \alpha_0\alpha_2\,|00\rangle\,|00\rangle + \alpha_0\beta_2\,|00\rangle\,|11\rangle + \beta_0\alpha_2\,|11\rangle\,|00\rangle + \beta_0\beta_2\,|11\rangle\,|11\rangle$$

Analyse

- Anwendung von $CNOT_{0\to2}$ und $CNOT_{1\to3}$liefert

$$\begin{aligned}|\Psi_{0123}\rangle &= \alpha_0\alpha_2\,|00\rangle\,|00\rangle + \alpha_0\beta_2\,|00\rangle\,|11\rangle + \beta_0\alpha_2\,|11\rangle\,|11\rangle + \beta_0\beta_2\,|11\rangle\,|00\rangle \\ &= (\alpha_0\alpha_2\,|00\rangle + \beta_0\beta_2\,|11\rangle)\,|00\rangle + (\alpha_0\beta_2\,|00\rangle + \beta_0\alpha_2\,|11\rangle)\,|11\rangle\end{aligned}$$

- Messung von q_2 und q_3 liefert "00"

$$|\Psi_{12}\rangle = \frac{\alpha_0\alpha_2\,|00\rangle + \beta_0\beta_2\,|11\rangle}{\sqrt{(\alpha_0\alpha_2)^2 + (\beta_0\beta_2)^2}} \qquad p = (\alpha_0\alpha_2)^2 + (\beta_0\beta_2)^2$$

- Messung von q_2 und $q_3$liefert "11"

$$|\Psi_{12}\rangle = \frac{\alpha_0\beta_2\,|00\rangle + \beta_0\alpha_2\,|11\rangle}{\sqrt{(\alpha_0\beta_2)^2 + (\beta_0\alpha_2)^2}} \qquad p = (\alpha_0\beta_2)^2 + (\beta_0\alpha_2)^2$$

Konkretes Rechenbeispiel

- Ausgangspaare

$$|\Psi_0\rangle = \alpha_0 |0\rangle + \beta_0 |1\rangle \quad \alpha_0 = 0.678264 \quad \beta_0 = 0.734818$$
$$|\Psi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle \quad \alpha_2 = 0.450083 \quad \beta_2 = 0.549917$$

- Concurrence

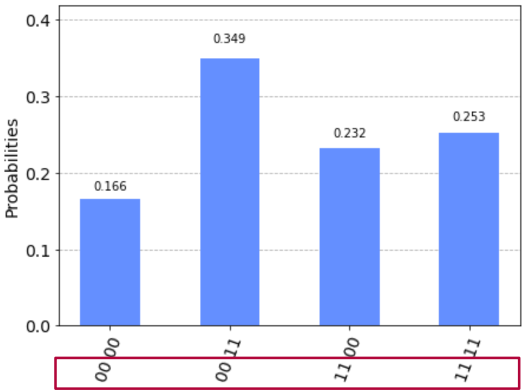
$$C(|\Psi_{01}\rangle) = 0.980067$$
$$C(|\Psi_{23}\rangle) = 0.987227$$

- Concurrence bei "00"-Messung

$$C(|\Psi_{12}\rangle) = 0.937864$$

- Concurrence bei "11"-Messung

$$C(|\Psi_{12}\rangle) = 0.999174$$



Zusammenfassung

- Aus nicht maximal verschränkten Qubits können mit Hilfe verschiedener Manipulationen und Messungen maximal verschränkte Qubits erzeugt werden.
  - Neben den hier vorgestellten Verfahren existieren auch noch weitere.

Hasso Plattner Institut
Digital Engineering · Universität Potsdam

Vielen Dank
für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik