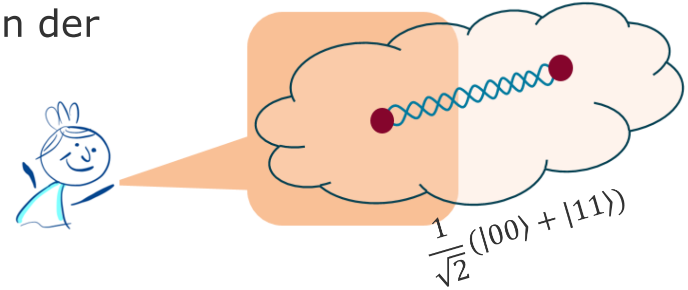
Quantenkryptographie (Teil 2) - Partielle Spur

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik

Agenda

Extraktion einer Teilsicht

- Aus einer Dichtematrix eines Quentensystems kann durch Bildung einer "partiellen Spur" die "Sicht" auf ein Teilsystem extrahiert werden.
  - Idee: Sammlung aller möglichen Zustände, wenn der "Rest" des Systems gemessen wird.



- Beispiel: Das Gesamtsystem sei in dem Zustand

$$\frac{1}{\sqrt{2}}\left(|0\rangle_A \, |0\rangle_B + |1\rangle_A |1\rangle_B \right)$$

- Aus Alice Sicht besitzt sie einen gemischten Zustand
  - $|0\rangle$ oder $|1\rangle$ jeweils mit Wahrscheinlichkeit $\frac{1}{2}$

$$\rho_A = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Partielle Spur

- Formale Definition der "Extraktion" (partielle Spur)

- Beispiel: Betrachte ein (allgemeines) Zwei-Qubit-System

$$|\Psi\rangle = c_{00}\,|0\rangle_1\,|0\rangle_2 + c_{01}\,|0\rangle_1\,|1\rangle_2 + c_{10}\,|1\rangle_1\,|0\rangle_2 + c_{11}\,|1\rangle_1\,|1\rangle_2$$

- Dichtematrix

$$\begin{pmatrix} c_{00}\overline{c_{00}} & c_{00}\overline{c_{01}} & c_{00}\overline{c_{10}} & c_{00}\overline{c_{11}} \\ c_{01}\overline{c_{00}} & c_{01}\overline{c_{01}} & c_{01}\overline{c_{10}} & c_{01}\overline{c_{11}} \\ c_{10}\overline{c_{00}} & c_{10}\overline{c_{01}} & c_{10}\overline{c_{10}} & c_{10}\overline{c_{11}} \\ c_{11}\overline{c_{00}} & c_{11}\overline{c_{01}} & c_{11}\overline{c_{10}} & c_{11}\overline{c_{11}} \end{pmatrix}$$

Partielle Spur: Extraktion der Teilsysteme

- Zur Extraktion des Teilsystems 1 wird Teilsystem 2 "quasi gemessen".

$$|\Psi\rangle = c_{00}\,|0\rangle_1\,|0\rangle_2 + c_{01}\,|0\rangle_1\,|1\rangle_2 + c_{10}\,|1\rangle_1\,|0\rangle_2 + c_{11}\,|1\rangle_1\,|1\rangle_2$$

- Partielle Spur

$$\begin{array}{c|cccc} & \langle 00| & \langle 01| & \langle 10| & \langle 11| \\ \hline |00\rangle & c_{00}\overline{c_{00}} & c_{00}\overline{c_{01}} & c_{00}\overline{c_{10}} & c_{00}\overline{c_{11}} \\ |01\rangle & c_{01}\overline{c_{00}} & c_{01}\overline{c_{01}} & c_{01}\overline{c_{10}} & c_{01}\overline{c_{11}} \\ |10\rangle & c_{10}\overline{c_{00}} & c_{10}\overline{c_{01}} & c_{10}\overline{c_{10}} & c_{10}\overline{c_{11}} \\ |11\rangle & c_{11}\overline{c_{00}} & c_{11}\overline{c_{01}} & c_{11}\overline{c_{10}} & c_{11}\overline{c_{11}} \end{array}$$

$$\begin{aligned} \rho_1 &= {}_2\langle 0|\rho\,|0\rangle_2 + {}_2\langle 1|\rho\,|1\rangle_2 \\ &= \begin{pmatrix} c_{00}\overline{c_{00}} & c_{00}\overline{c_{10}} \\ c_{10}\overline{c_{00}} & c_{10}\overline{c_{10}} \end{pmatrix} + \begin{pmatrix} c_{01}\overline{c_{01}} & c_{01}\overline{c_{11}} \\ c_{11}\overline{c_{01}} & c_{11}\overline{c_{11}} \end{pmatrix} \\ &= \begin{pmatrix} c_{00}\overline{c_{00}} + c_{01}\overline{c_{01}} & c_{00}\overline{c_{10}} + c_{01}\overline{c_{11}} \\ c_{10}\overline{c_{00}} + c_{11}\overline{c_{01}} & c_{10}\overline{c_{10}} + c_{11}\overline{c_{11}} \end{pmatrix} \end{aligned}$$

Partielle Spur

- Analog: Extraktion von Teilsystem 2

$$|\Psi\rangle = c_{00}\,|0\rangle_1\,|0\rangle_2 + c_{01}\,|0\rangle_1\,|1\rangle_2 + c_{10}\,|1\rangle_1\,|0\rangle_2 + c_{11}\,|1\rangle_1\,|1\rangle_2$$

- Partielle Spur

$$\begin{array}{c|c} & \begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \end{array} \\ \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} & \begin{pmatrix} c_{00}\overline{c_{00}} & c_{00}\overline{c_{01}} & c_{00}\overline{c_{10}} & c_{00}\overline{c_{11}} \\ c_{01}\overline{c_{00}} & c_{01}\overline{c_{01}} & c_{01}\overline{c_{10}} & c_{01}\overline{c_{11}} \\ c_{10}\overline{c_{00}} & c_{10}\overline{c_{01}} & c_{10}\overline{c_{10}} & c_{10}\overline{c_{11}} \\ c_{11}\overline{c_{00}} & c_{11}\overline{c_{01}} & c_{11}\overline{c_{10}} & c_{11}\overline{c_{11}} \end{pmatrix} \end{array}$$

$$\begin{aligned} \rho_2 &= {}_1\langle 0|\rho\,|0\rangle_1 + {}_1\langle 1|\rho\,|1\rangle_1 \\ &= \begin{pmatrix} c_{00}\overline{c_{00}} & c_{00}\overline{c_{01}} \\ c_{01}\overline{c_{00}} & c_{01}\overline{c_{01}} \end{pmatrix} + \begin{pmatrix} c_{10}\overline{c_{10}} & c_{10}\overline{c_{11}} \\ c_{11}\overline{c_{10}} & c_{11}\overline{c_{11}} \end{pmatrix} \\ &= \begin{pmatrix} c_{00}\overline{c_{00}} + c_{10}\overline{c_{10}} & c_{00}\overline{c_{01}} + c_{10}\overline{c_{11}} \\ c_{01}\overline{c_{00}} + c_{11}\overline{c_{10}} & c_{01}\overline{c_{01}} + c_{11}\overline{c_{11}} \end{pmatrix} \end{aligned}$$

Beispiel: Separierbarer Zustand

- Beispiel aus dem vorherigen Video zu "Dichtematrizen"

$$
\begin{aligned}
|\Psi\rangle &= \left(\frac{2}{3}|0\rangle_1 + \frac{\sqrt{5}}{3}|1\rangle_1\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle_2 + \frac{1}{\sqrt{2}}|1\rangle_2\right) \\
&= \frac{2}{3\sqrt{2}}|0\rangle_1|0\rangle_2 + \frac{2}{3\sqrt{2}}|0\rangle_1|1\rangle_2 + \frac{\sqrt{5}}{3\sqrt{2}}|1\rangle_1|0\rangle_2 + \frac{\sqrt{5}}{3\sqrt{2}}|1\rangle_1|1\rangle_2
\end{aligned}
$$

$$
\begin{array}{cc}
 & \begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \end{array} \\
\begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} &
\begin{pmatrix}
\frac{4}{18} & \frac{4}{18} & \frac{2\sqrt{5}}{18} & \frac{2\sqrt{5}}{18} \\
\frac{4}{18} & \frac{4}{18} & \frac{2\sqrt{5}}{18} & \frac{2\sqrt{5}}{18} \\
\frac{2\sqrt{5}}{18} & \frac{2\sqrt{5}}{18} & \frac{5}{18} & \frac{5}{18} \\
\frac{2\sqrt{5}}{18} & \frac{2\sqrt{5}}{18} & \frac{5}{18} & \frac{5}{18}
\end{pmatrix}
\end{array}
$$

Extraktion der Teilsysteme

- Teilsystem 1

$$\rho_1 = \mathrm{Tr}_2(\rho) = {}_2\langle 0|\rho\,|0\rangle_2 + {}_2\langle 1|\rho\,|1\rangle_2 = \frac{1}{9}\begin{pmatrix} 4 & 2\sqrt{5} \\ 2\sqrt{5} & 5 \end{pmatrix}$$

$$\begin{array}{c c} & \begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \end{array} \\ \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} & \begin{pmatrix} \frac{4}{18} & \frac{4}{18} & \frac{2\sqrt{5}}{18} & \frac{2\sqrt{5}}{18} \\ \frac{4}{18} & \frac{4}{18} & \frac{2\sqrt{5}}{18} & \frac{2\sqrt{5}}{18} \\ \frac{2\sqrt{5}}{18} & \frac{2\sqrt{5}}{18} & \frac{5}{18} & \frac{5}{18} \\ \frac{2\sqrt{5}}{18} & \frac{2\sqrt{5}}{18} & \frac{5}{18} & \frac{5}{18} \end{pmatrix} \end{array}$$

- Teilsystem 2

$$\rho_2 = \mathrm{Tr}_1(\rho) = {}_1\langle 0|\rho\,|0\rangle_1 + {}_1\langle 1|\rho\,|1\rangle_1 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{array}{c c} & \begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \end{array} \\ \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} & \begin{pmatrix} \frac{4}{18} & \frac{4}{18} & \frac{2\sqrt{5}}{18} & \frac{2\sqrt{5}}{18} \\ \frac{4}{18} & \frac{4}{18} & \frac{2\sqrt{5}}{18} & \frac{2\sqrt{5}}{18} \\ \frac{2\sqrt{5}}{18} & \frac{2\sqrt{5}}{18} & \frac{5}{18} & \frac{5}{18} \\ \frac{2\sqrt{5}}{18} & \frac{2\sqrt{5}}{18} & \frac{5}{18} & \frac{5}{18} \end{pmatrix} \end{array}$$

Berechnung mit Qiskit

Partielle Spur

```
# Dichtematrix für System A
rho_A = qi.partial_trace(rho,[0]) # BEACHTE: Interne Reihenfolge B-A
display( rho_A.draw('latex',prefix='\\rho_{A} = ') )
```

$$\rho_A = \begin{bmatrix} \frac{4}{9} & 0.4969 \\ 0.4969 & \frac{5}{9} \end{bmatrix}$$

```
# Dichtematrix für System B
rho_B = qi.partial_trace(rho,[1]) # BEACHTE: Interne Reihenfolge B-A
display( rho_B.draw('latex',prefix='\\rho_{B} = ') )
```

$$\rho_B = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

```
# Berechnung der Dichtematrix
rho = qi.DensityMatrix(psi_AB)
display( rho.draw('latex',prefix='\\rho_{AB} = ') )
```

$$\rho_{AB} = \begin{bmatrix} \frac{2}{9} & \frac{2}{9} & 0.24845 & 0.24845 \\ \frac{2}{9} & \frac{2}{9} & 0.24845 & 0.24845 \\ 0.24845 & 0.24845 & 0.27778 & 0.27778 \\ 0.24845 & 0.24845 & 0.27778 & 0.27778 \end{bmatrix}$$

Bell-Zustand

- Alice Sicht auf "ihr Teilsystem" von $|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B\right)$

- Berechnung der partiellen Spur

$$\rho_{AB} = |\Psi\rangle_{AB\;AB}\langle\Psi| = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{aligned} \rho_A = \mathrm{Tr}_B(\rho_{AB}) &= {}_B\langle 0|\rho|0\rangle_B + {}_B\langle 1|\rho|1\rangle_B \\ &= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

- Alice sieht einen gemischten Zustand: $\left\{\left\{\frac{1}{2}, |0\rangle\right\}; \left\{\frac{1}{2}, |1\rangle\right\}\right\}$
  - Ein System in einem von zwei möglichen Zuständen

Vergleich

- Alice Sicht auf "ihr Teilsystem" eines verschränkten Systems.
  - Gemischter Zustand

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B\right)$$

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}) = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

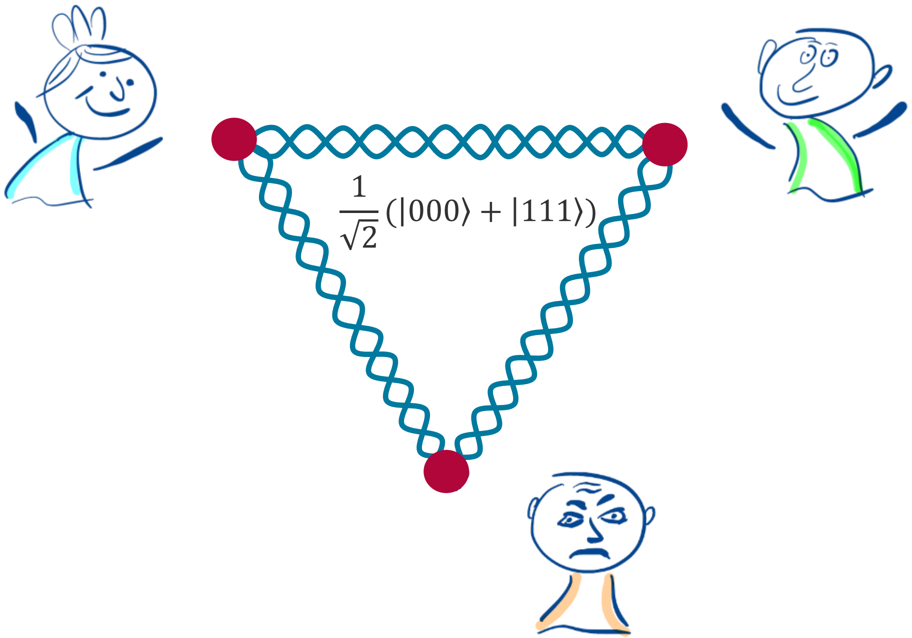
- Alice Sicht auf ein Qubit in Superposition

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$\rho = |\Psi\rangle\langle\Psi| = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Verschränktes 3-Qubit-System

- Betrachte folgende Situation (GHZ-Zustand)



Partielle Spur

- Sicht auf das "Teilsystem" von Alice und Bob bei dem Zustand

$$|\Psi\rangle_{ABE} = \frac{1}{\sqrt{2}}\Big(|0\rangle_A |0\rangle_B |0\rangle_E + |1\rangle_A |1\rangle_B |1\rangle_E \Big)$$

- Berechnung der partiellen Spur (*partial trace*)
  - Resultat ist ein gemischter Zustand.

$$\begin{aligned} \rho_{AB} = \mathrm{Tr}_E(\rho) &= {}_E\langle 0|\rho\,|0\rangle_E + {}_E\langle 1|\rho\,|1\rangle_E \\ &= \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

Berechnung mit Qiskit

```python
# Erzeugung des Zustandsvektors
psi = np.array([1,0,0,0,0,0,0,1])/np.sqrt(2)
psi_GHZ = qi.Statevector(psi)
display( psi_GHZ.draw('latex') )
```

$$\frac{\sqrt{2}}{2}|000\rangle + \frac{\sqrt{2}}{2}|111\rangle$$

```python
# Berechnung der Dichtematrix
rho_ABC = qi.DensityMatrix(psi_GHZ)
display( rho_ABC.draw('latex',prefix='\\rho_{ABE} = ') )
```

$$\rho_{ABE} = \begin{bmatrix} \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \end{bmatrix}$$

```python
# Dichtematrix für System AB
rho_AB = qi.partial_trace(rho_ABC,[0]) # Umgekehre Reihenfolge E-B-A
display( rho_AB.draw('latex',prefix='\\rho_{AB} = ') )
```

$$\rho_{AB} = \begin{bmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{bmatrix}$$

```python
# Dichtematrix für System E
rho_E = qi.partial_trace(rho_ABC,[1,2])  # Umgekehre Reihenfolge E-B-A
display( rho_E.draw('latex',prefix='\\rho_{E} = ') )
```

$$\rho_{E} = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}$$

Zusammenfassung

- Mit Hilfe der partiellen Spur kann die "Sicht" auf ein Teilbereich eines Quantensystems beschrieben werden.
- Bei separierbaren Systemen erhält man die Ausgangszustände.
- Bei verschränkten Systemen erhält man einen "gemischten Zustand".

Vielen Dank
für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik