Quantenkryptographie (Teil 2)
- Zusammengesetzte Quantensysteme

Prof. Dr. Jörg Hettel

Hochschule Kaiserslautern

Fachbereich Informatik

Agenda

Zusammengesetzte Systeme

- Beschreibung eines Qubits:

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \qquad \alpha, \beta \in \mathbb{C} \qquad |\alpha|^2 + |\beta|^2 = 1$$

- Betrachte nun mehrere Qubits

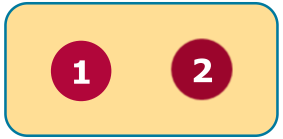
$$\begin{aligned} |\Psi\rangle_1 &= \alpha_1\,|0\rangle_1 + \beta_1\,|1\rangle_1 \\ |\Psi\rangle_2 &= \alpha_2\,|0\rangle_2 + \beta_2\,|1\rangle_2 \\ |\Psi\rangle_3 &= \alpha_3\,|0\rangle_3 + \beta_3\,|1\rangle_3 \\ \vdots &= \vdots \\ |\Psi\rangle_n &= \alpha_n\,|0\rangle_n + \beta_n\,|1\rangle_n \end{aligned}$$

Mathematische Beschreibung

- Beschreibung des Gesamtsystems zusammengesetzt aus mehreren Qubits.
  - Qubits (Teilsysteme) werden mit Hilfe des Tensorproduktes verknüpft.

$$\begin{aligned} |\Psi\rangle &= |\Psi\rangle_1 \otimes |\Psi\rangle_2 \otimes \ldots \otimes |\Psi\rangle_n \\ &= |\Psi\rangle_1 |\Psi\rangle_2 |\Psi\rangle_3 \ldots |\Psi\rangle_n \end{aligned}$$

- Beispiel für ein 2-Qubit-System



$$\begin{aligned} |\Psi\rangle &= |\Psi\rangle_1 \otimes |\Psi\rangle_2 \\ &= (\alpha_1 |0\rangle_1 + \beta_1 |1\rangle_1) \otimes (\alpha_2 |0\rangle_2 + \beta_2 |1\rangle_2) \\ &= \alpha_1\alpha_2 |0\rangle_1 \otimes |0\rangle_2 + \alpha_1\beta_2 |0\rangle_1 \otimes |1\rangle_2 + \beta_1\alpha_2 |1\rangle_1 \otimes |0\rangle_2 + \beta_1\beta_2 |1\rangle_1 \otimes |1\rangle_2 \\ &= \alpha_1\alpha_2 |0\rangle_1 |0\rangle_2 + \alpha_1\beta_2 |0\rangle_1 |1\rangle_2 + \beta_1\alpha_2 |1\rangle_1 |0\rangle_2 + \beta_1\beta_2 |1\rangle_1 |1\rangle_2 \\ &= \alpha_1\alpha_2 |00\rangle + \alpha_1\beta_2 |01\rangle + \beta_1\alpha_2 |10\rangle + \beta_1\beta_2 |11\rangle \end{aligned}$$

Mathematische Beschreibung

- In Vektorform:

$$\begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix} \otimes \begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix} = \begin{pmatrix}\alpha_1 \begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix}\\ \beta_1 \begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\alpha_1\alpha_2\\ \alpha_1\beta_2\\ \beta_1\alpha_2\\ \beta_1\beta_2\end{pmatrix}$$

- Wir erhalten ein 4-dim System mit den vier Basisvektoren:

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \quad |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \quad |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \quad |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

System aus 3 Qubits

- 3 Qubits ergeben ein 8-dim System:

$$
\begin{aligned}
|\Psi\rangle &= |\Psi\rangle_1 \otimes |\Psi\rangle_2 \otimes |\Psi\rangle_3 \\
&= (\alpha_1 |0\rangle_1 + \beta_1 |1\rangle_1) \otimes (\alpha_2 |0\rangle_2 + \beta_2 |1\rangle_2) \otimes (\alpha_3 |0\rangle_3 + \beta_3 |1\rangle_3) \\
&= \alpha_1\alpha_2\alpha_3 |000\rangle + \alpha_1\alpha_2\beta_3 |001\rangle + \alpha_1\beta_2\alpha_3 |010\rangle + \alpha_1\beta_2\beta_3 |011\rangle \\
&\quad + \beta_1\alpha_2\alpha_3 |100\rangle + \beta_1\alpha_2\beta_3 |101\rangle + \beta_1\beta_2\alpha_3 |110\rangle + \beta_1\beta_2\beta_3 |111\rangle
\end{aligned}
$$

$$
\begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} \otimes \begin{pmatrix} \alpha_3 \\ \beta_3 \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2\alpha_3 \\ \alpha_1\alpha_2\beta_3 \\ \alpha_1\beta_2\alpha_3 \\ \alpha_1\beta_2\beta_3 \\ \beta_1\alpha_2\alpha_3 \\ \beta_1\alpha_2\beta_3 \\ \beta_1\beta_2\alpha_3 \\ \beta_1\beta_2\beta_3 \end{pmatrix}
$$

Dimension des Systems

- Die Dimension des Systems (Hilbertraum) wächst exponentiell mit der Anzahl der Qubits:
  - 2-Qubit System: $2^2 = 4$ Dimensionen
  - 3-Qubit System: $2^3 = 8$ Dimensionen
  - 4-Qubit System: $2^4 = 16$ Dimensionen
  - … …
  - 10-Qubit System: $2^{10} = 1024$ Dimesionen
  - … …
  - 20-Qubit System: $2^{20} = 1.048.576$ Dimesionen
  - … …
  - 30-Qubit System: $2^{30} = 1.073.741.824$ Dimesionen
  - … …
  - 100-Qubit System: $2^{100} = 1.267.650.600.228.229.401.496.703.205.376$ Dimesionen

Separabel versus verschränkt

- Man nennt einen (Multi-Qubit-) Zustand ***separabel***, wenn sein Zustandsvektor als Tensorprodukt von einzelnen Qubits geschrieben werden kann.
  - Man nennt einen solchen Zustand auch Produktzustand.

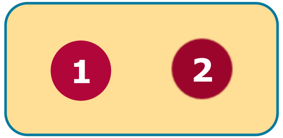
$$|\Psi\rangle \quad = \quad |\Psi\rangle_1 \otimes |\Psi\rangle_2 \otimes \ldots \otimes |\Psi\rangle_n$$

- Man nennt einen (Multi-Qubit-) Zustand **verschränkt** (entangled), wenn sein Zustandsvektor **nicht** als Tensorprodukt von einzelnen Qubits geschrieben werden kann.
  - Es existiert eine "Korrelation" zwischen den "Teilsystemen".

Beispiel: 2-Qubit-System

- Ein aus zwei einzelnen Qubits zusammen gesetzte System:

$$\begin{aligned} |\Psi\rangle_1 \otimes |\Psi\rangle_2 &= (\alpha_1 |0\rangle_1 + \beta_1 |1\rangle_1) \otimes (\alpha_2 |0\rangle_2 + \beta_2 |1\rangle_2) \\ &= \alpha_1\alpha_2 |00\rangle + \alpha_1\beta_2 |01\rangle + \beta_1\alpha_2 |10\rangle + \beta_1\beta_2 |11\rangle \end{aligned}$$



- Ein allgemeines 2-Qubit-System

$$|\Psi\rangle = c_{00} |00\rangle + c_{01} |01\rangle + c_{10} |10\rangle + c_{11} |11\rangle$$

- Frage: Wann kann ein Zustand als Tensorprodukt von zwei Qubits geschrieben werden?

$$|\Psi\rangle_1 \otimes |\Psi\rangle_2 \stackrel{?}{=} c_{00} |00\rangle + c_{01} |01\rangle + c_{10} |10\rangle + c_{11} |11\rangle$$

Beispiel: 2-Qubit-System

- Ein allgemeines 2-Qubit-System ist separierbar, falls folgende Gleichung gilt:

$$\begin{aligned} |\Psi\rangle &= c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle \\ &\stackrel{?}{=} \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle = |\Psi\rangle_1 \otimes |\Psi\rangle_2 \end{aligned}$$

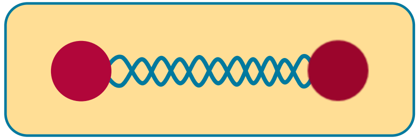
- Hierzu müssen folgende Bedingungen erfüllt sein:

$$\left.\begin{aligned} c_{00} &= \alpha_1\alpha_2 \\ c_{01} &= \alpha_1\beta_2 \\ c_{10} &= \beta_1\alpha_2 \\ c_{11} &= \beta_1\beta_2 \end{aligned}\right\} \Rightarrow \left.\begin{aligned} c_{00}c_{11} &= \alpha_1\alpha_2\beta_1\beta_2 \\ c_{01}c_{10} &= \alpha_1\alpha_2\beta_1\beta_2 \end{aligned}\right\} \Rightarrow \boxed{c_{00}c_{11} = c_{01}c_{10}}$$

$$c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$$

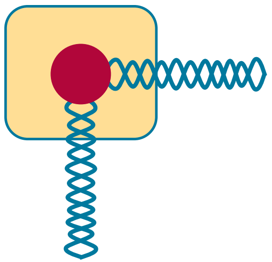
Verschränkung als Ressource

- Zusammengesetzte Systeme können verschränkt sein.
  - Dann ist das Ganze mehr als die Summe seiner Teile.
    - Hierzu später mehr.
  - Anwendungen:
    - Teleportation, Dense Coding, …
    - Quanten Computing
    - Quanten Kryptographie



Verschränkung als Ursache für Dekohärenz

- Oft verschränken sich Systeme mit der Umgebung
  - Bei unzureichender Kontrolle
    - Bezeichnung: Dekohärenz
    - Hier kommt die "*Quantum Error Correction*" ins Spiel.



Zusammenfassung

- Zusammengesetzte Quantensysteme können
  - separierbar
  - oder verschränkt sein.
- Dimension zusammengesetzter Qubit-Systeme wachsen exponentiell mit der Anzahl der beteiligten Qubits.
- Verschränkung ist eine sehr wichtige Ressource!
  - Ist ein reines Quantenphänomen!
  - Grundlage "moderner" QKD.

Vielen Dank
für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik