Quantenkryptographie (Teil 2)
- Qubits und Messbasen

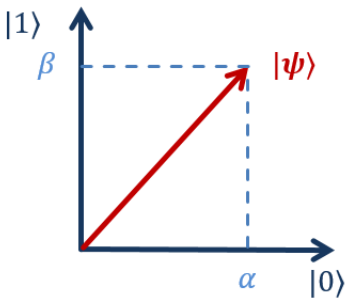
Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik

Agenda

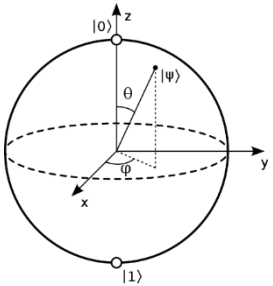
1. Einführung
2. Wiederholung BB84
3. **Qubits und Messbasen**
4. Zusammengesetzte Systeme
5. Verschränkung
6. Anwendung von Verschränkung
7. Shared Randomness
8. Schmidt-Darstellung
9. Dichtematrizen
10. Partielle Spur
11. Verschränkungsmaß
12. Entropie und Monogamie
13. Entanglement Swapping
14. Entanglement Distillation
15. CHSH-Ungleichung (klassisch)
16. CHSH-Ungleichung (Quantenversion)
17. CHSH-Ungleichung (Simulation)
18. Ekert-Protokoll
19. Sicherheit und DIQKD
20. Zusammenfassung

Qubits

- Qubits werden (immer) bezüglich einer Basis angegebe
- Darstellung eines Qubits bezüglich der Standardbasis:
  - $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
    - Bemerkung: $\alpha, \beta \in \mathbb{C}$ und $|\alpha|^2 + |\beta|^2 = 1$
  - Globale Phase ist weitere Freiheitsgrad
    - $|\Psi\rangle \equiv e^{i\gamma}|\Psi\rangle$
    - Hat physikalisch keine Relevanz.



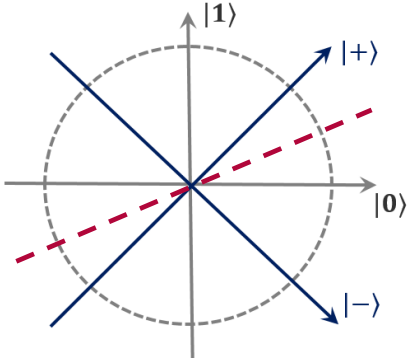
- Weitere gebräuchliche Darstellung
  - Bloch-Kugel-Darstellung
  - $|\Psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle$
  - Mit $0 \le \theta \le \pi$ und $0 \le \phi \le 2\pi$



Quelle: Wikipedia

Hadamard-Basis

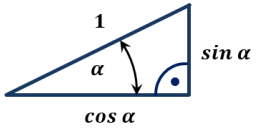
- Qubits können bezüglich verschiedener Basen dargestellt werden.
- Ein weitere oft verwendete Basis ist die Hadamard-Basis:
  - $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
  - Somit gilt: $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$, $|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$
  - $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle$

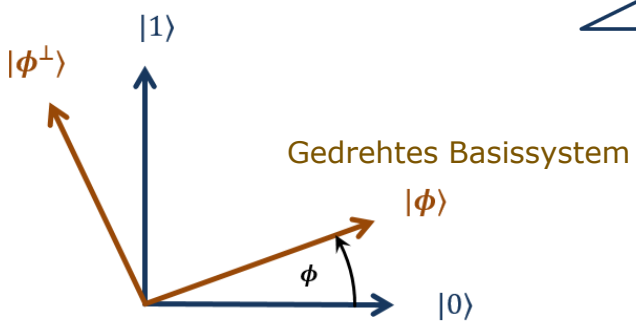


- Bemerkung zur Hadamard-Basis:
  - Spiegelung an Ursprungsgeraden mit Winkel $\alpha = \frac{\pi}{8} = 22{,}5°$ zur positiven x-Achse.

Basiswechsel

- Im Folgenden beschränken wir uns auf reelle Koeffizienten.
  - Bleiben in der (x,z)-Ebene der Blochkugel.
- Durch Drehung der Standardbasis entstehen ebenfalls neue Basen
  - $|\phi\rangle = \cos\phi\,|0\rangle + \sin\phi\,|1\rangle$
  - $|\phi^{\perp}\rangle = -\sin\phi\,|0\rangle + \cos\phi\,|1\rangle$

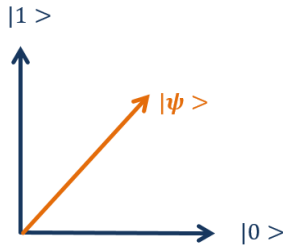


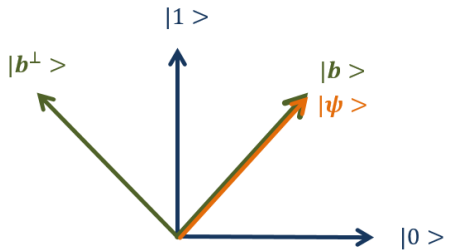


- Matrixoperation:
  - $\mathrm{R}(\phi) = \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix}$
  - Es gilt
    - $|\phi\rangle = R(\phi)|0\rangle$
    - $|\phi^{\perp}\rangle = R(\phi)|1\rangle$

Qubits: Eigenbasis

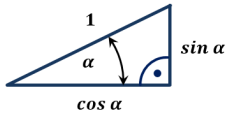
- Allgemeine Darstellung eines Qubits bezüglich der Standardbasis
  - $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
- Einführung einer speziellen (Eigen-) Basis
  - $|b\rangle = R(\phi)\,|0\rangle$
  - $|b^{\perp}\rangle = R(\phi)\,|1\rangle$
- Darstellung bezüglich $\{|\mathrm{b}\rangle, |\mathrm{b}^{\perp}\rangle\}$-Basis
  - $|\Psi\rangle = 1\,|b\rangle$



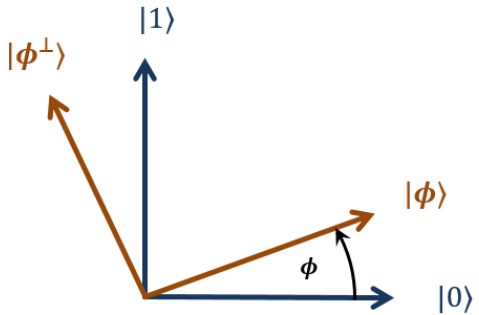


Basiswechsel

- Darstellung der $\{|\phi\rangle, |\phi^{\perp}\rangle\}$-Basis in der Standardbasis:
  - $|\phi\rangle = \cos\phi\,|0\rangle + \sin\phi\,|1\rangle$
  - $|\phi^{\perp}\rangle = -\sin\phi\,|0\rangle + \cos\phi\,|1\rangle$

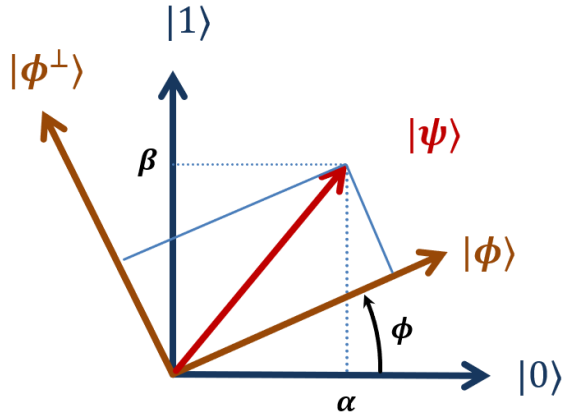


- Darstellung der Standardbasis in der $\{|\phi\rangle, |\phi^{\perp}\rangle\}$-Basis :
  - $|0\rangle = \cos\phi\,|\phi\rangle - \sin\phi\,|\phi^{\perp}\rangle$
  - $|1\rangle = \sin\phi\,|\phi\rangle + \cos\phi\,|\phi^{\perp}\rangle$



Beispiel

- Darstellung von
  $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- In der $\{|\phi\rangle, |\phi^{\perp}\rangle\}$-Basis:
  - $|\phi\rangle = \cos\phi\,|0\rangle + \sin\phi\,|1\rangle$
  - $|\phi^{\perp}\rangle = -\sin\phi\,|0\rangle + \cos\phi\,|1\rangle$

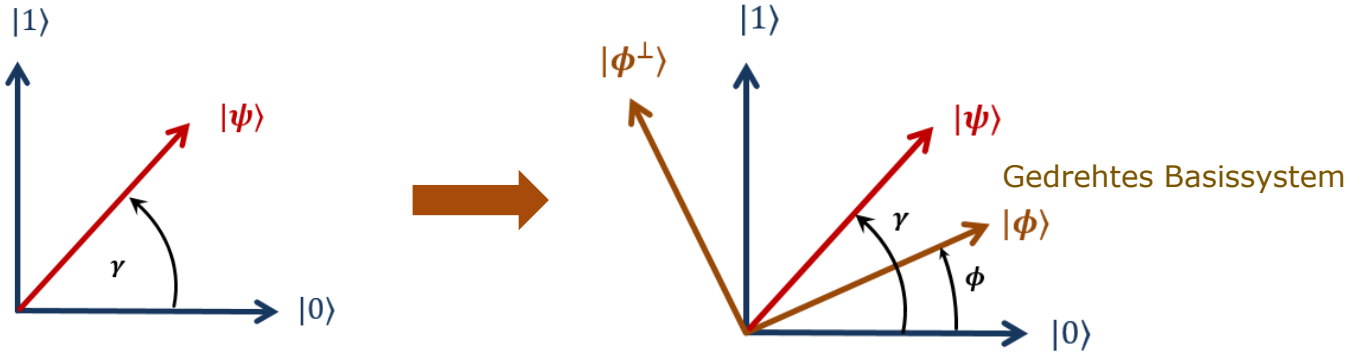


- Einsetzen von:
  - $|0\rangle = \cos\phi\,|\phi\rangle - \sin\phi\,|\phi^{\perp}\rangle$
  - $|1\rangle = \sin\phi\,|\phi\rangle + \cos\phi\,|\phi^{\perp}\rangle$

  ergibt
  - $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle = (\alpha\cos\phi + \beta\sin\phi)|\phi\rangle + (-\alpha\sin\phi + \beta\cos\phi)|\phi^{\perp}\rangle$

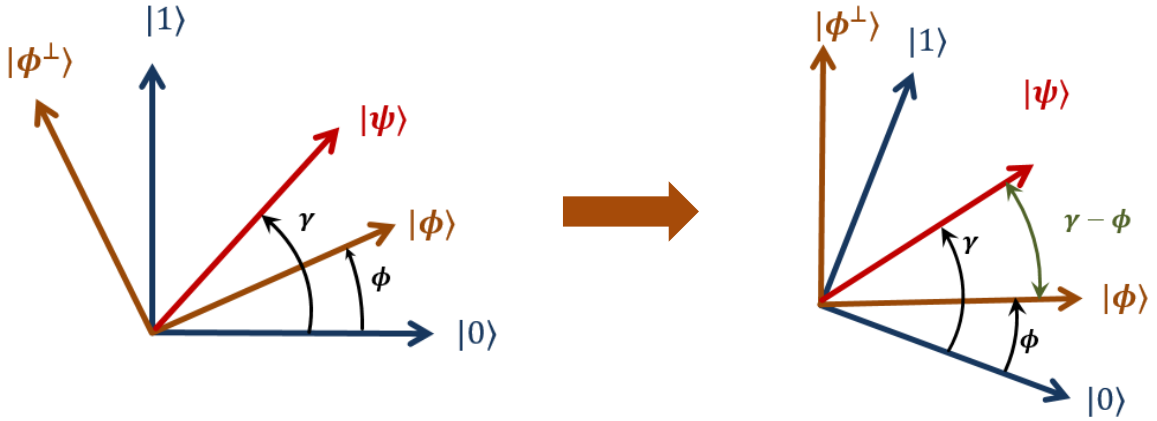
Messung bezüglich gedrehter Basis (1)

- Ein Qubit $|\Psi\rangle$ soll bezüglich einer gedrehten Basis gemessen werden.
  - Messen können wir aber (in vielen Fällen) nur in der Standardbasis.
- Idee: Gedrehtes Basissystem (plus Qubit $|\Psi\rangle$) zurückdrehen auf Standardbasis und Standardmessung vornehmen.



Messung bezüglich gedrehter Basis (2)

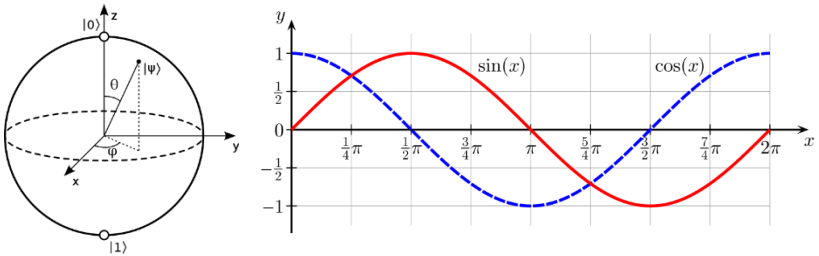
- Entspricht einer Drehung des Qubits $|\Psi\rangle$ nach rechts und Messung in der Standardbasis.



Rotationsgatter *RY(θ)*

- Qubit-Gatter werden oft (bei Qiskit) durch ihre Wirkung auf der Bloch-Kugel beschrieben.
- Mit Rotationsgattern kann man Zustandsvektoren um eine der drei Achsen der Bloch-Kugel drehen.
  - Das $RY(\theta)$ dreht einen Zustandsvektor um den Winkel θ um die y-Achse der Bloch-Kugel (Drehung in der (x,z)-Ebene).
    - Beachte: $0 \leq \theta \leq \pi$ und $0 \leq \phi \leq 2\pi$
  - Matrixdarstellung:

$$RY(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

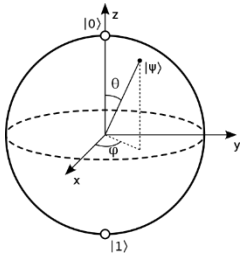


Quelle: Wikipedia

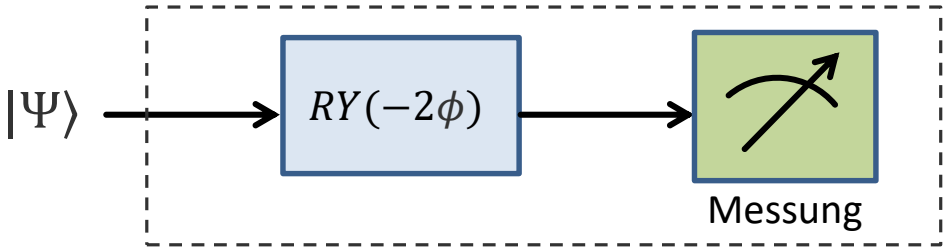
Messung in einer gedrehten Basis

- Rotation mit einem RY-Gatter (definiert auf der Bloch-Kugel)
  - Beachte: $0 \leq \theta \leq \pi$ (Drehung von $|0\rangle$ Richtung $|1\rangle$)

$$RY(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$



- Messung in eine um den Winkel ϕ gedrehte Basis entspricht einem Zurückdrehen um den "doppelten" Winkel mit $RY(\theta)$ und Messung in der Standardbasis.



Zusammenfassung

- Allgemeine Darstellung eines Qubits bezüglich der Standardbasis:

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

- Darstellung eines Qubits bezüglich einer gedrehten Basis:

$$|\Psi\rangle = \alpha_\phi|\phi\rangle + \beta_\phi|\phi^\perp\rangle$$

- Darstellung in der "Eigenbasis":

$$|\Psi\rangle = 1\,|b\rangle$$

- Messung in einer gedrehten Basis entspricht einer "Rückdrehung" und anschließender Messung in der Standardbasis.

Vielen Dank
für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik