Quantenkryptographie (Teil 2) - CHSH Ungleichung – Quanten-Version

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik

Hasso Plattner Institut
Digital Engineering • Universität Potsdam

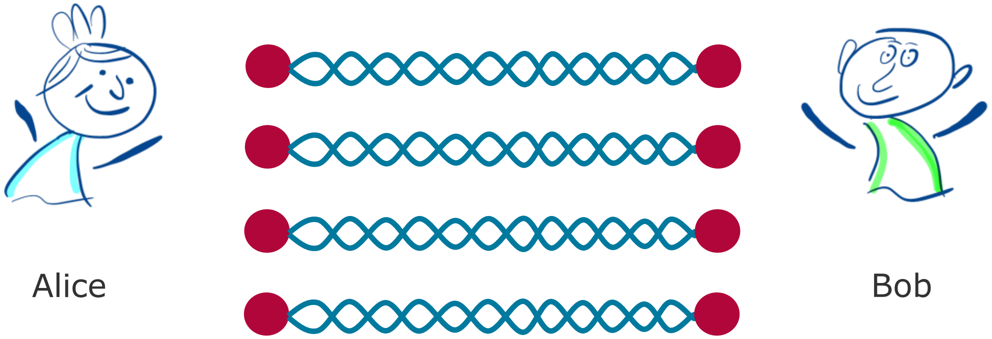
Agenda

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

Quanten-Strategie

- Alice und Bob teilen sich verschränkte 2-Qubit-Quantensysteme, jeweils im Zustand

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



Auswahl der Messbasen

- Je nach gestellter Aufgabe führen Alice und Bob eine Messung ihres Qubits unter einem bestimmten Winkel durch.
- Hierzu nutzen Sie folgende gedrehte Basen:

$$\begin{aligned}|0\rangle_A &= \cos(\phi)\,|\phi\rangle_A - \sin(\phi)\,|\phi^\perp\rangle_A\\ |1\rangle_A &= \sin(\phi)\,|\phi\rangle_A + \cos(\phi)\,|\phi^\perp\rangle_A\end{aligned}$$

$$\begin{aligned}|0\rangle_B &= \cos(\theta)\,|\theta\rangle_B - \sin(\theta)\,|\theta^\perp\rangle_B\\ |1\rangle_B &= \sin(\theta)\,|\theta\rangle_B + \cos(\theta)\,|\theta^\perp\rangle_B\end{aligned}$$

- Messergebnis $|\phi\rangle_A$ bzw. $|\theta\rangle_B$ entspricht hebe rechte Hand bzw. Fuß
- Messergebnis $|\phi^\perp\rangle_A$ bzw. $|\theta^\perp\rangle_B$ entspricht hebe linke Hand bzw. Fuß

Rechnung: Zustand in neuer Basis

$$
\begin{aligned}
|\Psi\rangle_{AB} &= \frac{1}{\sqrt{2}}\left(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B\right) \\
&= \frac{1}{\sqrt{2}}\Big(\left(\cos(\phi)\,|\phi\rangle_A - \sin(\phi)\,|\phi^\perp\rangle_A\right)\left(\cos(\theta)\,|\theta\rangle_B - \sin(\theta)\,|\theta^\perp\rangle_B\right) \\
&\qquad + \left(\sin(\phi)\,|\phi\rangle_A + \cos(\phi)\,|\phi^\perp\rangle_A\right)\left(\sin(\theta)\,|\theta\rangle_B + \cos(\theta)\,|\theta^\perp\rangle_B\right)\Big) \\
&= \frac{1}{\sqrt{2}}\Big((\cos(\phi)\cos(\theta) + \sin(\phi)\sin(\theta))\,|\phi\rangle_A\,|\theta\rangle_B \\
&\qquad + (-\cos(\phi)\sin(\theta) + \sin(\phi)\cos(\theta))\,|\phi\rangle_A\,|\theta^\perp\rangle_B \\
&\qquad + (-\sin(\phi)\cos(\theta) + \cos(\phi)\sin(\theta))\,|\phi^\perp\rangle_A\,|\theta\rangle_B \\
&\qquad + (\sin(\phi)\sin(\theta) + \cos(\phi)\cos(\theta))\,|\phi^\perp\rangle_A\,|\theta^\perp\rangle_B\Big)
\end{aligned}
$$

Transformation

- Als Gesamtsystem erhält man aus $|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)$

$$
\begin{aligned}
|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}\Big(& \cos(\phi-\theta)\ |\phi\rangle_A |\theta\rangle_B + \sin(\phi-\theta)\ |\phi\rangle_A |\theta^\perp\rangle_B \\
& -\sin(\phi-\theta)\ |\phi^\perp\rangle_A |\theta\rangle_B + \cos(\phi-\theta)\ |\phi^\perp\rangle_A |\theta^\perp\rangle_B \Big)
\end{aligned}
$$

- Die Wahrscheinlichkeiten für eine Messung ergeben sich aus:

$$
\begin{aligned}
P(|\phi\rangle_A |\theta\rangle_B) &= \frac{1}{2}\cos^2(\phi-\theta) \\
P(|\phi\rangle_A |\theta^\perp\rangle_B) &= \frac{1}{2}\sin^2(\phi-\theta) \\
P(|\phi^\perp\rangle_A |\theta\rangle_B) &= \frac{1}{2}\sin^2(\phi-\theta) \\
P(|\phi^\perp\rangle_A |\theta^\perp\rangle_B) &= \frac{1}{2}\cos^2(\phi-\theta)
\end{aligned}
$$

Wahrscheinlichkeiten für:

- Alice rechts, Bob rechts
- Alice rechts, Bob links
- Alice links, Bob rechts
- Alice links, Bob links

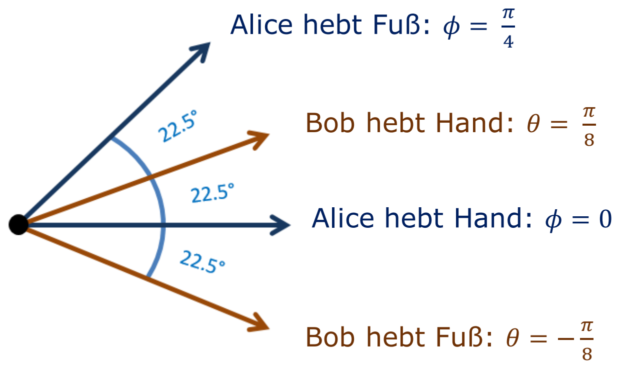
Korrelationsfunktion

Als Korrelationsfunktion erhält man

$$
\begin{aligned}
E(\phi,\theta) &= \underbrace{P(|\phi\rangle_A|\theta\rangle_B) + P(|\phi^\perp\rangle_A|\theta^\perp\rangle_B)}^{\text{Korreliert (+1)(+1) bzw. (-1)(-1)}} \underbrace{- P(|\phi\rangle_A|\theta^\perp\rangle_B) - P(|\phi^\perp\rangle_A|\theta\rangle_B)}^{\text{Antikorreliert (-1)(+1) bzw. (+1)(-1)}} \\
&= \frac{1}{2}\cos^2(\phi-\theta) + \frac{1}{2}\cos^2(\phi-\theta) - \frac{1}{2}\sin^2(\phi-\theta) - \frac{1}{2}\sin^2(\phi-\theta) \\
&= \cos^2(\phi-\theta) - \sin^2(\phi-\theta) \\
&= \cos\left(2(\phi-\theta)\right)
\end{aligned}
$$

Auswahl der Messbasen

- Alice und Bob wählen nun folgende konkrete Messbasen (Winkel):
  - Wenn Alice ihre Hand heben soll, wählt sie als Winkel: $\phi = 0$
  - Wenn Alice ihren Fuß heben soll, wählt sie als Winkel: $\phi = \frac{\pi}{4}$
  - Wenn Bob seine Hand heben soll, wählt er als Winkel: $\theta = \frac{\pi}{8}$
  - Wenn Bob seinen Fuß heben soll, wählt er als Winkel: $\theta = -\frac{\pi}{8}$



Ergebnis

- Somit ergibt sich

$$
\begin{aligned}
S &= E(0,\frac{\pi}{8}) + E(0,-\frac{\pi}{8}) + E(\frac{\pi}{4},\frac{\pi}{8}) - E(\frac{\pi}{4},-\frac{\pi}{8}) \\
&= \cos\left(2(0-\frac{\pi}{8})\right) + \cos\left(2(0+\frac{\pi}{8})\right) + \cos\left(2(\frac{\pi}{4}-\frac{\pi}{8})\right) - \cos\left(2(\frac{\pi}{4}+\frac{\pi}{8})\right) \\
&= \cos(-\frac{\pi}{4}) + \cos(\frac{\pi}{4}) + \cos(\frac{\pi}{4}) - \cos(\frac{3\pi}{4}) \\
&= 3\cos(\frac{\pi}{4}) - \cos(\frac{3\pi}{4}) \\
&= 3\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} \\
&= 2\sqrt{2} \approx 2,828427
\end{aligned}
$$

Zusammenfassung

- Haben Alice und Bob in jeder Spielrunde die "Korrelation" eines maximal verschränkten Qubit-Paars zur Verfügung, können sie für

$$S = < A_H \cdot B_H > + \ < A_H \cdot B_F > + \ < A_F \cdot B_H > - \ < A_F \cdot B_F >$$

  den Wert $|S| = 2\sqrt{2}$ erreichen!
  - Im klassischen Fall gilt immer $|S| \leq 2$.

- Es kann gezeigt werden, dass $2\sqrt{2}$ ein Maximalwert (ober Schranke) ist.
  - Stichwort: Tsirelson's Bound

HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

Vielen Dank für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik