Quantenkryptographie (Teil 2)
- CHSH Ungleichung – Klassische Version

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

Ein Spiel

Alice und Bob nehmen an einem Gewinnspiel teil.

- Alice und Bob werden räumlich getrennt. Sie dürfen während des Spiels nicht kommunizieren.
- Alice und Bob wird zufällig jeweils eine von zwei Aufgaben gestellt.
  - Hebe eine Hand oder hebe einen Fuß.
- Alice und Bob wählen jeweils eine aus zwei vorgegebenen Optionen aus.
  - Linke oder rechte Hand bzw. Fuß
  - Zufällig oder nach einer vorher abgesprochenen Strategie.
- Aus dem gezeigten Verhalten wird eine Punktzahl berechnet.
- Das Spiel hat sehr viele Runden.

- Ziel ist es, gemeinsam eine möglichst hohe Punktzahl zu erreichen.

Alice

Bob

Aufgaben und Antworten

- Alice und Bob wird zufällig z.B. folgende Aufgaben gestellt:
  - Alice: Hebe eine deiner Hände!
  - Bob: Hebe einer deiner Füße an!

- Bemerkung: Es gibt vier Aufgabenkombinationen:
  (*Aufgabe an Alice*, *Aufgabe an Bob*)
  - (A_H,B_H), (A_H,B_F), (A_F,B_H), (A_F,B_F)

- Alice und Bob wählen eine der folgenden Möglichkeiten:
  - Hand: rechts (+1) oder links (-1)
  - Fuß: rechts (+1) oder links (-1)

Beispiel

- Erste Runde:
  - Alice soll eine Hand heben und Bob einen Fuß.
  - Alice hebt die rechte Hand, Bob hebt den rechten Fuß.
  - Punktzahl: $(A_H,B_F) = (+1,+1) \Rightarrow (+1)*(+1) = +1$

- Zweite Runde:
  - Alice und Bob sollen beide ihre Hand heben.
  - Alice und Bob heben beide die linke Hand.
  - Punktzahl: $(A_H,B_H) = (-1,-1) \Rightarrow (-1)*(-1) = +1$

Beispiel für einen Spielverlauf

Alice	Antwort	Bob	Antwort	Punkte
Hand	+1	Fuß	+1	**+1**
Hand	-1	Hand	-1	**+1**
Fuß	+1	Hand	-1	**-1**
Hand	+1	Fuß	+1	**+1**
Fuß	-1	Hand	-1	**+1**
Fuß	+1	Fuß	-1	**-1**
Hand	+1	Fuß	-1	**-1**
…	…	…	…	…

Spielauswertung

- Nach dem Spiel werden die Mittelwerte gebildet
  - $< A_H \cdot B_H >, < A_H \cdot B_F >, < A_F \cdot B_H >, < A_F \cdot B_F >$

  und folgender Wert berechnet:
  - $S = < A_H \cdot B_H > + < A_H \cdot B_F > + < A_F \cdot B_H > - < A_F \cdot B_F >$

- Beispiel

Alice	Antwort	Bob	Antwort	Punkte
Hand	+1	Fuß	+1	**+1**
Hand	-1	Hand	-1	**+1**
Fuß	+1	Hand	-1	**-1**
Hand	+1	Fuß	+1	**+1**
Fuß	-1	Hand	-1	**+1**
Fuß	+1	Fuß	-1	**-1**
Hand	+1	Fuß	-1	**-1**
…	…	…	…	…

$$< A_H \cdot B_H > = \frac{(+1)}{1} = 1$$

$$< A_H \cdot B_F > = \frac{(+1)+(+1)+(-1)}{3} = \frac{1}{3}$$

$$< A_F \cdot B_H > = \frac{(-1)+(+1)}{2} = 0$$

$$< A_F \cdot B_F > = \frac{(-1)}{1} = 1$$

$$\boldsymbol{S = 1 + \frac{1}{3} + 0 - 1 = \frac{1}{3}}$$

Spielziel

- **Frage:** Können Alice und Bob |S| > 2 erreichen?

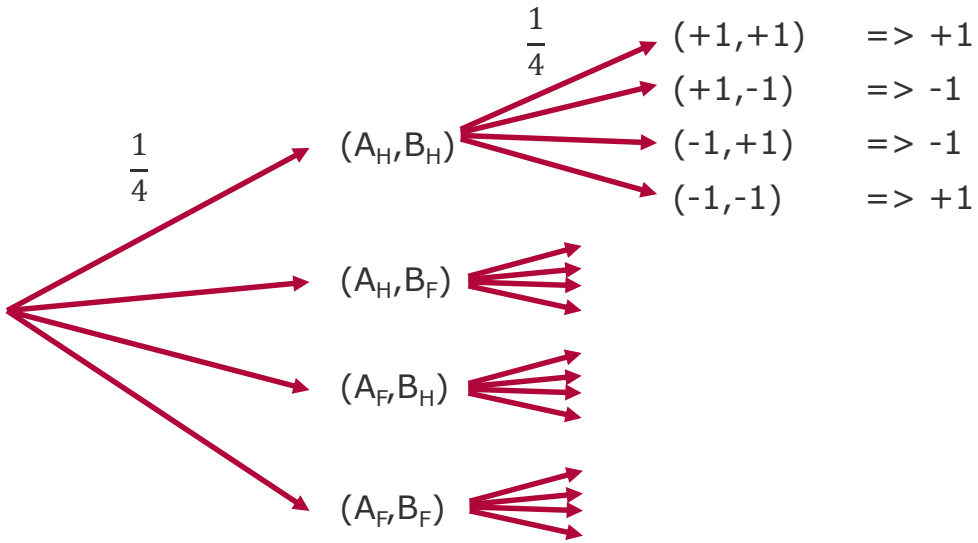
- Randbedingungen
  - Aufgaben für Alice und Bob werden zufällig gewählt.
  - Runden werden sehr oft wiederholt, sodass jede Fragekonstellation

    (A_H,B_H), (A_H,B_F), (A_F,B_H), (A_F,B_{FS})

    (ungefähr) gleich häufig vorkommt.

Spielstrategie: Random

- Alice und Bob ihre Gliedmaßen zufällig.
  - In dem Fall gilt: S = 0



Erwartungswert:

$$< A_H \cdot B_H > = \frac{1}{4}(+1) + \frac{1}{4}(-1) + \frac{1}{4}(-1) + \frac{1}{4}(+1) = 0$$

Spielstrategie: Deterministisch

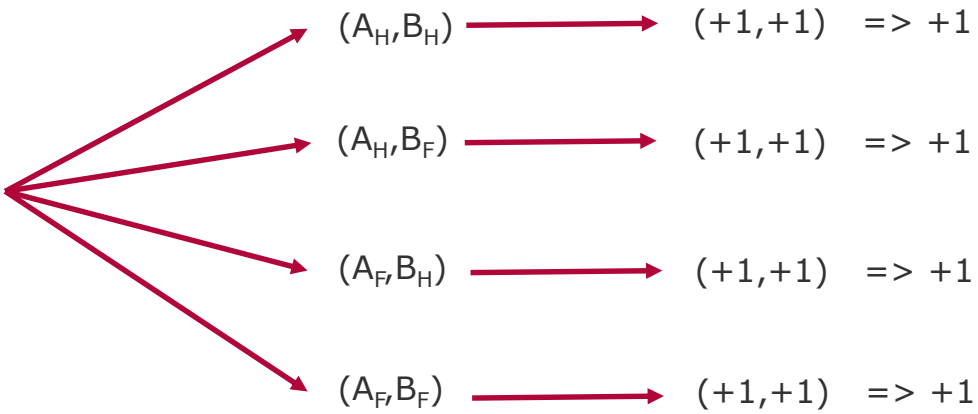
- Alice und Bob sprechen sich im Vorfeld ab.
  - Es gibt 16 verschiedene (feststehende) Strategien

		R1	R2	R3	R4	R5	R6	R7	R8
Alice	Hand	+1	-1	+1	-1	+1	-1	+1	-1
	Fuß	+1	+1	-1	-1	+1	+1	-1	-1
Bob	Hand	+1	+1	+1	+1	-1	-1	-1	-1
	Fuß	+1	+1	+1	+1	+1	+1	+1	+1

		R9	R10	R11	R12	R13	R14	R15	R16
Alice	Hand	+1	-1	+1	-1	+1	-1	+1	-1
	Fuß	+1	+1	-1	-1	+1	+1	-1	-1
Bob	Hand	+1	+1	+1	+1	-1	-1	-1	-1
	Fuß	-1	-1	-1	-1	-1	-1	-1	-1

Spielstrategie: Deterministisch

- Beispiel: Alice und Bob haben sich z.B. auf Strategie R1 verständigt:
  - Haben immer die rechte Hand bzw. den rechten Fuß.
  - Gesucht: $S = < A_H \cdot B_H > + < A_H \cdot B_F > + < A_F \cdot B_H > - < A_F \cdot B_F >$



Erwartungswerte:

$$< A_H \cdot B_H > = 1,$$
$$< A_H \cdot B_F > = 1,$$
$$< A_F \cdot B_H > = 1,$$
$$< A_F \cdot B_F > = 1$$

Und somit gilt:

$$S = 2$$

Ergebnisse für deterministische Spielstrategien

- Alice und Bob erhalten jenachdem $S = \pm 2$

		R1	R2	R3	R4	R5	R6	R7	R8
Alice	Hand	+1	-1	+1	-1	+1	-1	+1	-1
	Fuß	+1	+1	-1	-1	+1	+1	-1	-1
Bob	Hand	+1	+1	+1	+1	-1	-1	-1	-1
	Fuß	+1	+1	+1	+1	+1	+1	+1	+1
	S	+2	-2	+2	-2	-2	-2	+2	+2

		R9	R10	R11	R12	R13	R14	R15	R16
Alice	Hand	+1	-1	+1	-1	+1	-1	+1	-1
	Fuß	+1	+1	-1	-1	+1	+1	-1	-1
Bob	Hand	+1	+1	+1	+1	-1	-1	-1	-1
	Fuß	-1	-1	-1	-1	-1	-1	-1	-1
	S	+2	+2	-2	-2	-2	+2	-2	+2

Ergebnisse für deterministische Spielstrategien

- Allgemeine Erklärung: $A_H, A_F, B_H, B_F \in \{-1, +1\}$

- Wenn Fragekombinationen gleichhäufig sind, dann gilt:

$$\begin{aligned} S &= < A_H \cdot B_H > + < A_H \cdot B_F > + < A_F \cdot B_H > - < A_F \cdot B_F > \\ &= < A_H \cdot B_H + A_H \cdot B_F + A_F \cdot B_H - A_F \cdot B_F > \\ &= < A_H \cdot (B_H + B_F) + A_F \cdot (B_H - B_F) > \end{aligned}$$

- Wenn $B_H = B_F$ gilt, dann ist $S = < A_H \cdot (B_H + B_F) > = \pm 2$

- Wenn $B_H \neq B_F$ gilt, dann ist $S = < A_F \cdot (B_H - B_F) > = \pm 2$

Zusammenfassung

- Alice und Bob erhalten für

$$< A_H \cdot B_H > \; + \; < A_H \cdot B_F > \; + < A_F \cdot B_H > \; - \; < A_F \cdot B_F >$$

  immer $|S| \leq 2$.
  - Unabhängig von der zugrundeliegenden Spielstrategie.

- $|S| \leq 2$ wird CHSH-Ungleichung genannt.
  - CHSH – Clauser, Horne, Shimony, Holt, 1969
    - Gehört zu den sogenannten Bell-Ungleichungen.

Vielen Dank
für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik