Quantenkryptographie (Teil 2)
- Ekert-Protokoll

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

Das Ekert-Protokoll (E91)

- QKD-Protokoll auf Basis von Verschränkung.
  - Vorgeschlagen von Artur Ekert 1991.
    - Intuitives Sicherheitsargument
  - Es gibt mittlerweile verschiedene Varianten.

- Detektion eines Lauschers basiert auf der Überprüfung der CHSH-Ungleichung.
  - Ansonsten Funktionsweise recht ähnlich zu BB84.

Austauschformat

- Zur Schlüsselgenerierung werden maximal verschränkte Qubit-Paare im folgenden Zustand benutzt:

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

- Bemerkung: Verschränkung zeigt sich in jedem (gedrehten) Basissystem

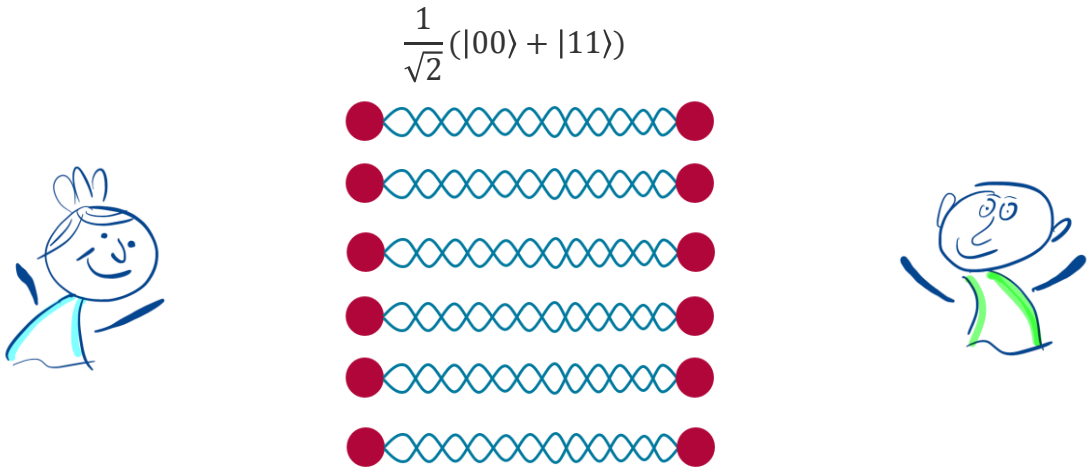
$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|\phi\rangle_A|\phi\rangle_B + |\phi^\perp\rangle_A|\phi^\perp\rangle_B)$$

Bei "unterschiedlichen" Drehungen

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

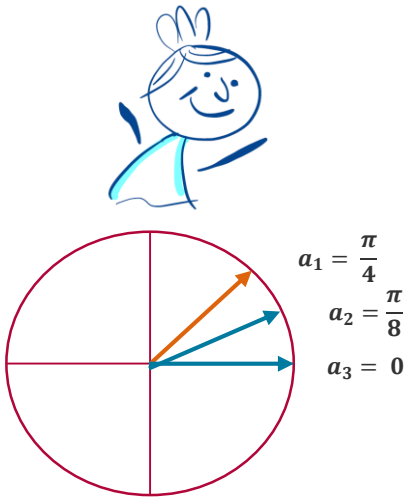
Präparation

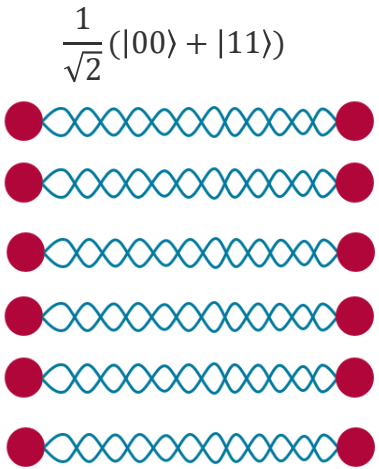
- Alice erzeugt verschränkte Qubit-Paare und übermittelt jeweils ein Qubit davon an Bob.

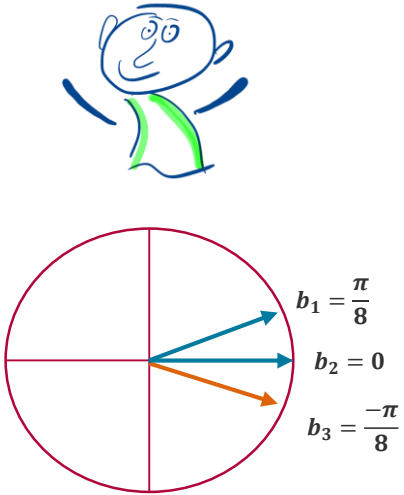


Schlüsselerzeugung (1)

- Alice und Bob messen nun ihre Qubits zufällig und gleichverteilt in verschiedenen Basen (Richtungen).
  - Alice und Bob protokollieren ihre Wahl (Winkel).







Schlüsselerzeugung (2)

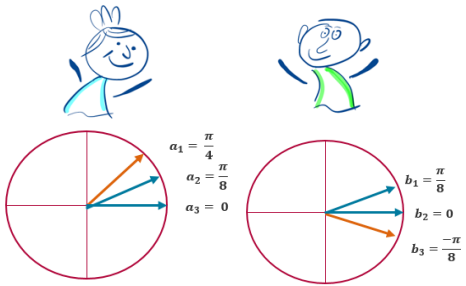
- Beispiel:
  - Alice: $a_2, a_1, a_1, a_3, a_2, a_1, a_2, a_1, a_3, a_2, a_2, a_3, a_3, a_2, \cdots$
  - Bob: $b_1, b_1, b_2, b_3, b_1, b_3, b_3, b_1, b_2, b_3, b_2, b_1, b_2, b_2, \cdots$

- Alice und Bob gleichen nach der Messung Ihre Messbasen ab.
  - Benutzen hierzu klassische Kommunikation über authentifizierenden Kanal.
  - Dadurch ergeben sich folgende Messkombinationen:
    $(a_2, b_1), (a_1, b_1), (a_1, b_2), (a_3, b_3), (a_2, b_1), (a_1, b_3), (a_2, b_3,), (a_1, b_1), (a_3, b_2),$
    $(a_2, b_3), (a_2, b_2), (a_3, b_1), (a_3, b_2), (a_1, b_2), \cdots$

Sifting und Sicherheitsprüfung

- Sifting Prozess
  - Haben Alice und Bob die selbe Basis gewählt, erhalten Sie bei einer Messung die selben Werte (jeweils 0 oder 1 mit 50% Wahrscheinlichkeit)
  - Hieraus wird der Schlüssel erzeugt

$(a_2, b_1), (a_1, b_1), (a_1, b_2), (a_3, b_3), \mathbf{(a_2, b_1)}, (a_1, b_3), (a_2, b_3,), (a_1, b_1), \mathbf{(a_3, b_2)},$
$(a_2, b_3), (a_2, b_2), (a_3, b_1), \mathbf{(a_3, b_2)}, (a_1, b_2), \cdots$



- Prüfung
  - Die anderen Messergebnisse werden (zum Teil) zur Berechnung der CHSH-Gleichung benutzt

$(a_2, b_1), (a_1, b_1), (a_1, b_2), (a_3, b_3), (a_2, b_1), (a_1, b_3), (a_2, b_3,), (a_1, b_1), (a_3, b_2),$
$(a_2, b_3), (a_2, b_2), (a_3, b_1), (a_3, b_2), (a_1, b_2), \cdots$

CHSH-Ungleichung

- Bestimmung der CHSH-Ungleichung
  - Zähle jeweils die Paare

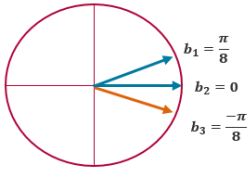
$$(a_3, b_1), (a_3, b_3), (a_1, b_1), (a_1, b_3)$$

    und bestimme deren durchschnittliches Vorkommen.
  - Entspricht den Winkelkombinationen: $(0, \frac{\pi}{8}), (0, \frac{-\pi}{8}), (\frac{\pi}{4}, \frac{\pi}{8}), (\frac{\pi}{4}, \frac{-\pi}{8})$

- Bestimmung der CHSH-Ungleichung

$$S = Avg(a_3, b_1) + Avg(a_3, b_3) + Avg(a_1, b_1) - Avg(a_1, b_3)$$

- Es muss gelten: $S > 2$ (optimal $S = 2\sqrt{2}$)



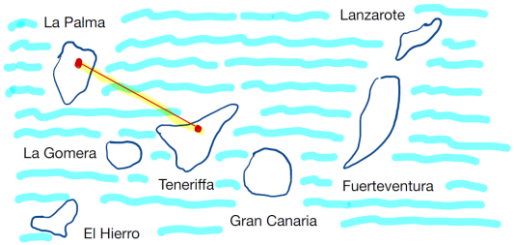
Weitere Schritte

- Da man in der Realität immer Störungen und Rauschen hat, muss auch beim Ekert-Protokoll eine Nachverarbeitung erfolgen.
- Dies kann analog zum BB84-Protokoll erfolgen:
  - Bestimmung der Fehlerrate
  - Durchführung einer Fehlerkorrektur (Error Correction)
  - Privacy Amplification

- Alternativen
  - Zur Verbesserung der Verschränkungsgüte kann vor der Messung z.B. auch ein Entanglement Distillation Protokoll durchgeführt werden.

Implementierungsbeispiele

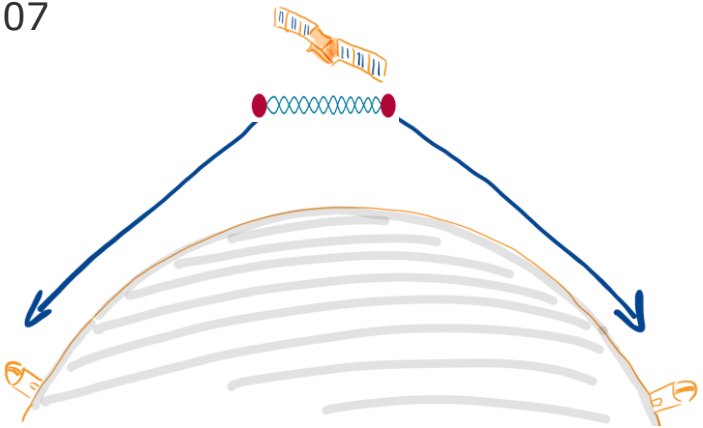
- 2007, Ursin et al. (Laserstrahl)
  - Distanz 144 km
  - CHSH-Wert: S = 2,508 ± 0,037



- 2016, Yin et al. (Glasfaser)
  - Distanz 311 km (Standardglasfaser) bzw. 404 km (Spezialfaser)
  - Glasfaserspule im Labor
  - Bitrate $2{,}6 \cdot 10^{-3}$ bps bzw. $3{,}2 \cdot 10^{-4}$ bps

Implementierungsbeispiele

- 2020, Yin et al. (Satellitenbasiert)
  - Satellit produziert verschränkte Photonenpaare
  - Distanz 1120 km
    - Überwindung der Erdkrümmung
  - CHSH-Wert: S = 2,56 ± 0,07
  - Bitrate: 0,12 bps



Zusammenfassung

- Das Ekert-Protokoll (E91) basiert auf dem Phänomen der Verschränkung.
  - Lauscherdetektion durch Bestimmung der CHSH-Ungleichung.
- Schlüssel wird erst zum Zeitpunkt der Messung erzeugt.
  - Nach dem Austausch der Qubits!
- Experimentelle Realisierungen vorhanden.
  - Noch nicht so ausgereift wie BB84.

Vielen Dank
für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik