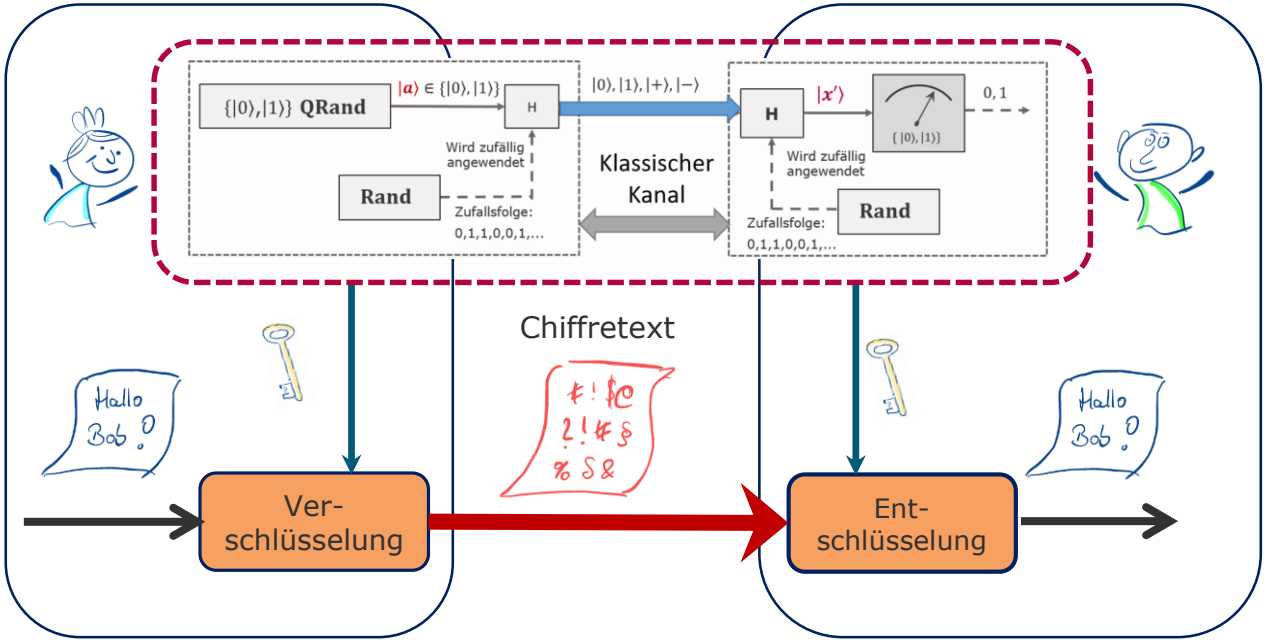
Quantenkryptographie (Teil 2)
- Wiederholung BB84-Protokoll

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik

Agenda

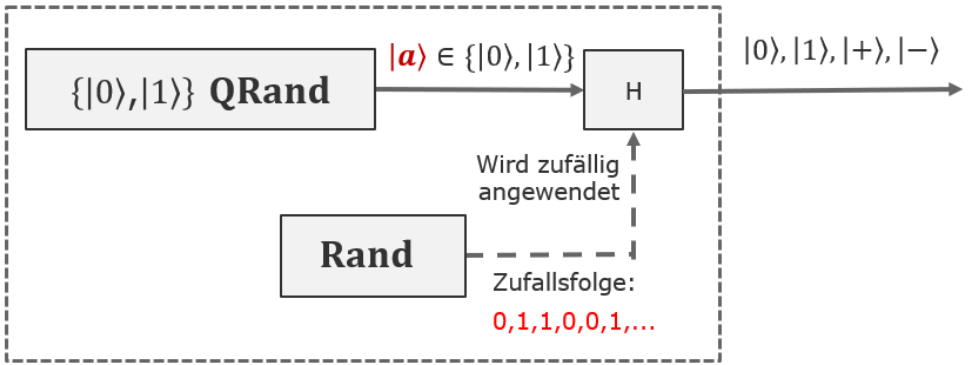
1. Einführung
2. **Wiederholung BB84**
3. Qubits und Messbasen
4. Zusammengesetzte Systeme
5. Verschränkung
6. Anwendung von Verschränkung
7. Shared Randomness
8. Schmidt-Darstellung
9. Dichtematrizen
10. Partielle Spur
11. Verschränkungsmaß
12. Entropie und Monogamie
13. Entanglement Swapping
14. Entanglement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

BB84 Schematische Übersicht



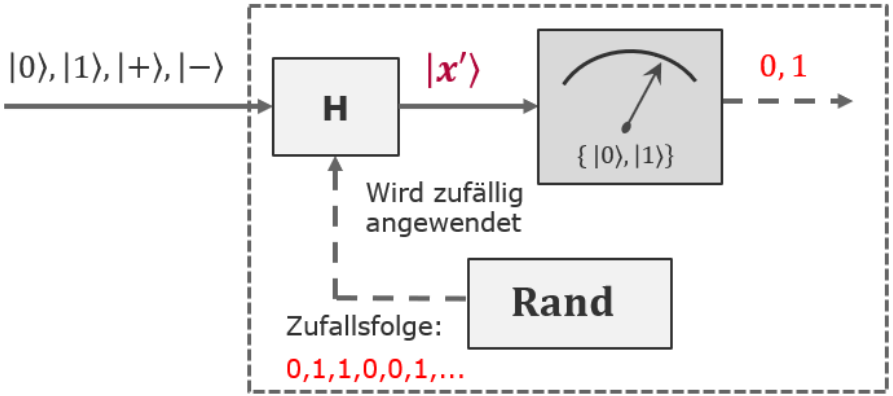
BB84-Protokoll: *Preparation*

- Alice erzeugt zufällig Qubits in einem der Zustände $|0\rangle, |1\rangle, |+\rangle, |-\rangle$
  - **Wichtig**: Die Sequenz der erzeugten Qubits enthält bereits den zukünftigen Schlüssel als Teilsequenz.
    - "Der Schlüssel wird im Labor von Alice erzeugt!"



BB84-Protokoll: *Measurement*

- Bob wendet zufällig eine Hadamard-Operation auf die erhaltenen Qubits an und führt anschließend eine Messung durch.



BB84-Protokoll: *Sifting*

- Nach der Übertragung der Qubits tauschen Alice und Bob über den klassischen Kanal aus, bei welchen Qubits sie die Hadamard-Operation angewendet haben (Vergleich der Zufallsbits).

Qubit $\|a\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	...
Alice Zahl	1	0	1	0	1	1	1	0	1	0	...
$\|x\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	...
Bobs Zahl	0	0	1	1	1	0	1	1	0	0	...
$\|x'\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	...
Schlüssel	-	1	1	-	0	-	0	-	-	1	...

Schema des BB84-Protokolls

- *Preparation*: Alice erzeugt zufällig *2n* Qubits in einem der Zustände $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ und sendet die Qubits zu Bob.
- *Measurement*: Für jedes Qubit, das Bob erhält, wählt er zufällig die Anwendung von Hadamard und misst das Qubit.
- *Sifting*: Alice kommuniziert Bob über den klassischen Kanal, wann sie ihre Hadamard-Operationen angewendet hat.
  Bob und Alice berücksichtigen nur die Qubits, bei denen sie beide Hadamard oder beide nicht Hadamard angewendet haben.
- Alice und Bob wählen einen Teil des Schlüssels aus und vergleichen (öffentlich) die Werte. Wenn es zu viele Abweichungen gibt, brechen sie das Protokoll ab.
  Ansonsten führen sie *Error Correction* und *Privacy Amplification* durch, um die Qualität des Schlüssels zu steigern.

Sicherheit des Protokolls

- Die Sicherheit beruht darauf, dass ein Lauscher beim Vergleich von Schlüsselbits detektiert werden kann.
  - Zugrunde liegende quantenphysikalische Prinzipien:
    - Nicht-Unterscheidbarkeit von nicht-orthogonalen Zuständen.
      Bsp.: $|0\rangle$ und $|+\rangle$ können nicht zuverlässig durch eine Messung unterschieden werden.
    - No-Cloning Theorem.
      Qubits können (in der Regel) nicht kopiert werden.

- Getroffene Annahmen:
  - Alle Geräte (Photonenquelle, Detektoren, Quantenkanal, etc.) arbeiten zuverlässig und störungsfrei.

Zusammenfassung

- Durch den Austausch von Qubits kann ein "sicherer" Schlüsseltausch realisiert werden.
- Das BB84-Protokoll ist ein *prepare-and-measure*-Protokoll.
  - Ist für Point-to-Point-Verbindungen bereits kommerziell verfügbar.
- Der ausgetauschte Schlüssel kann dann z.B. für eine Verschlüsselung mit dem One-Time-Pad benutzt werden.
- Neben dem "Quanten-Kanal" wird auch ein authentifizierender "klassischer" Kanal benötigt.
  - Authentifizierung ist aber getrennt von der Schlüsselgenerierung.
    - Späteres brechen eines zur Authentifizierung verwendeten öffentlichen Schlüssels hat keinen Einfluss auf die Verschlüsselung.
    - Wichtiger Unterschied zu klassischen Verfahren.

Vielen Dank
für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik