Quantenkryptographie (Teil 2) - Shared Randomness

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik

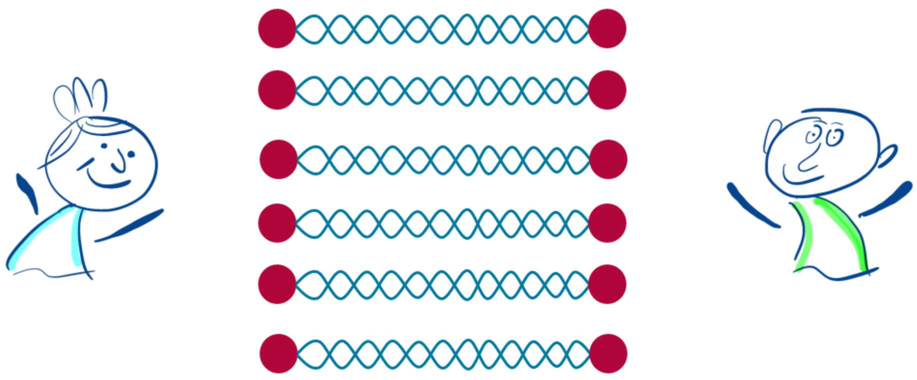
Agenda

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

Shared Randomness

- Alice und Bob teilen sich viele Bell-Zustände.
  - Beispiel: Alice erzeugt verschränkte Photonenpaare und gibt jeweils eines der Photonen (Qubits) an Bob.

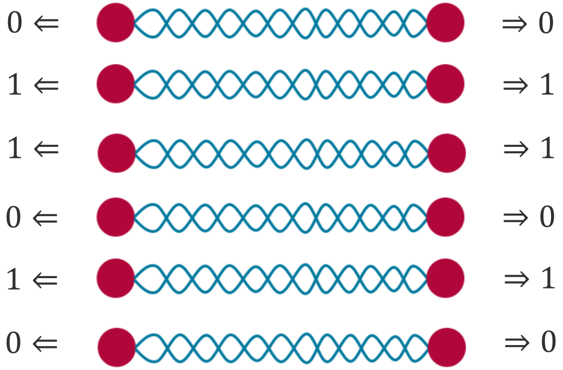
$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



Shared Randomness

- Alice und Bob messen beide ihre Qubits in der Standardbasis.
  - Beide erhalten dieselbe Zufallssequenz.
  - Es wird aber <u>keine</u> Information (Bit-Werte) übertragen.

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



Messung in einer anderen Basis

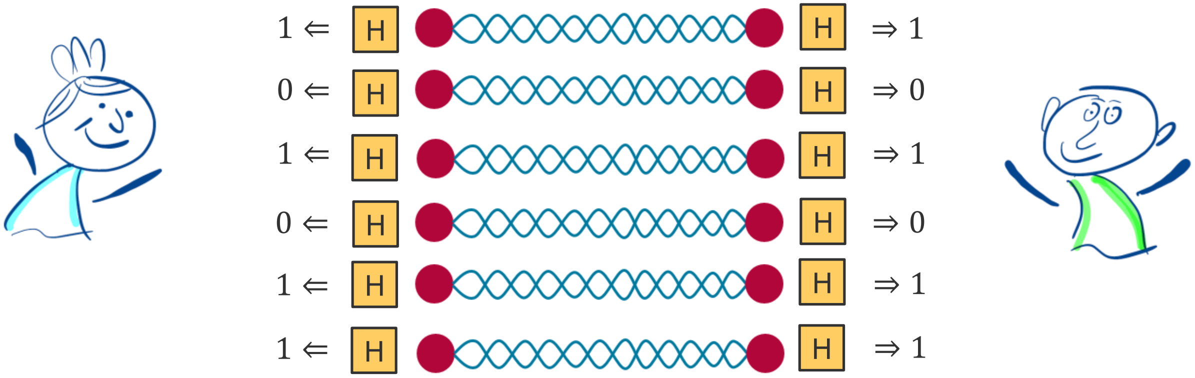
- Alice und Bob wenden vor der Messung jeweils Hadamard an:

$$
\begin{aligned}
|\Psi\rangle = \quad & \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
\xrightarrow{H \otimes H} \quad & \frac{1}{2\sqrt{2}}\Big((|0\rangle + |1\rangle)(|0\rangle + |1\rangle) + (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)\Big) \\
= \quad & \frac{1}{2\sqrt{2}}\Big((|00\rangle + |01\rangle + |10\rangle + |11\rangle) + (|00\rangle - |01\rangle - |10\rangle + |11\rangle) \Big) \\
= \quad & \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big)
\end{aligned}
$$

Messung in einer anderen Basis

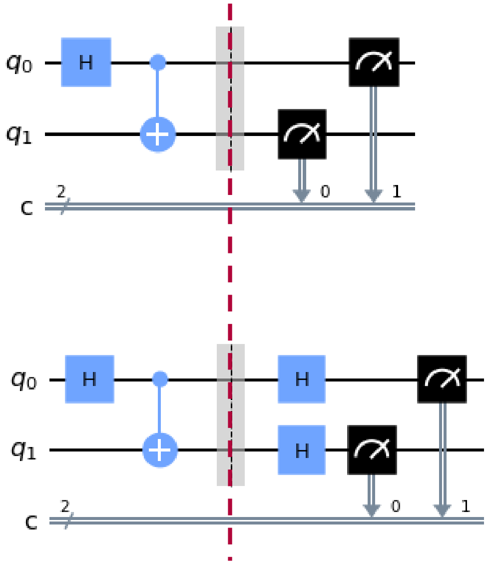
- Alice und Bob erhalten auch jetzt eine perfekt korrelierte Zufallssequenz.

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

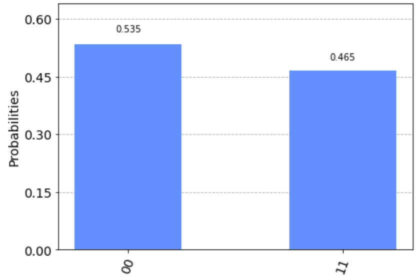


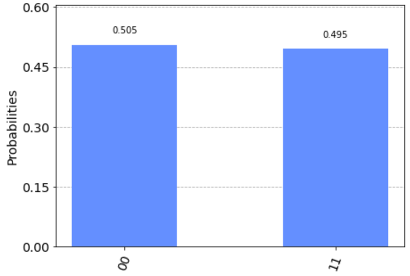
Simulation (mit Qiskit)

Messung in der Standardbasis versus Hadamard-Basis



$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

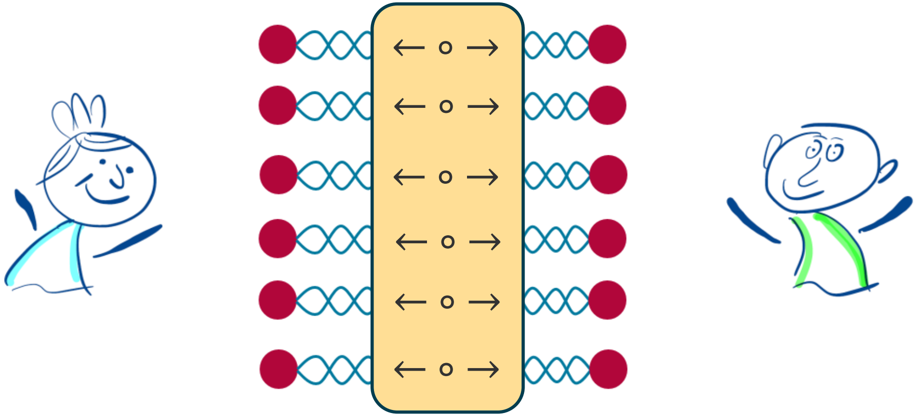




Shared Randomness

- Alice und Bob erhalten verschränkte Photonenpaare aus einer externen Quelle.
  - Frage: Können Alice und Bob feststellen, ob sich ihre Photonen alle im Bell-Zustand $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ befinden?

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \;??$$



Shared Randomness

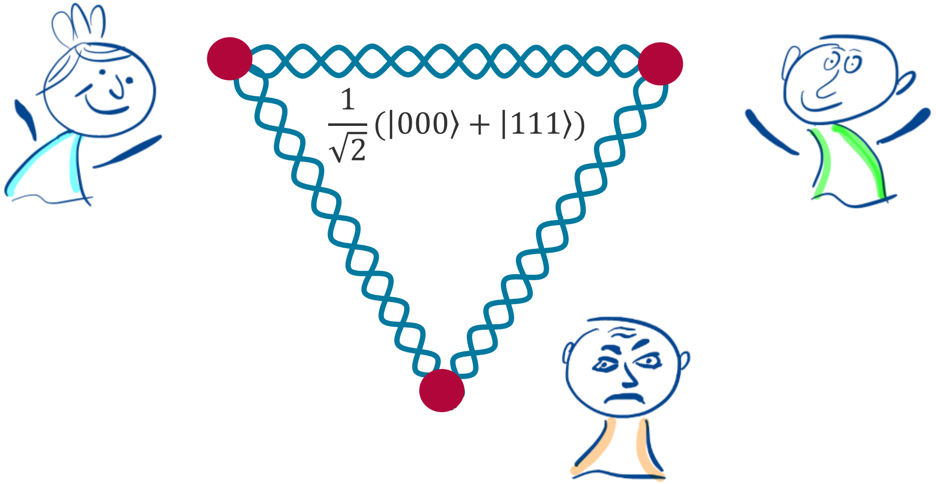
- Möglichkeiten für erhaltene Photonen

  - Erzeuger ist komplett entkoppelt:
    - $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes |\psi\rangle$
    - Alice und Bob erhalten bei einer Messung eine korrelierte Zufallssequenz.

  - Erzeuger ist mit den beiden Photonen von Alice und Bob verschränkt:
    - Beispiel: $\alpha|00\rangle|\psi_0\rangle + \beta|11\rangle|\psi_1\rangle$
    - Beispiel: $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$

Shared Randomness

- Beispiel: Alice und Bob erhalten Photonenpaar von Eve aus dem 3-Qubit Zustand $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$
  - Frage: Können Alice und Bob feststellen, dass sie kein Bell-Paar besitzen?



Shared Randomness

- Messen Alice und Bob ihre Qubits in der Standardbasis, erhalten sie eine korrelierte Zufallssequenz.
  - Auch Eve erhält dieselbe Zufallsfolge.
- Wenden Alice und Bob auf ihre Qubits z.B. Hadamard an, ändert sich der Gesamtzustand zu:

$$
\begin{aligned}
|\Psi\rangle = \quad & \frac{1}{\sqrt{2}}(|111\rangle + |000\rangle) \\
\xrightarrow{H\otimes H\otimes \mathbb{1}} \quad & \frac{1}{2\sqrt{2}}\Big((|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\,|0\rangle) + ((|0\rangle - |1\rangle)(|0\rangle - |1\rangle)\,|1\rangle) \Big) \\
= \quad & \frac{1}{2\sqrt{2}}\Big((|00\rangle + |01\rangle + |10\rangle + |11\rangle)\,|0\rangle + (|00\rangle - |01\rangle - |10\rangle + |11\rangle)\,|1\rangle \Big) \\
= \quad & \frac{1}{2\sqrt{2}}\Big(|000\rangle + |010\rangle + |100\rangle + |110\rangle + |001\rangle - |011\rangle - |101\rangle + |111\rangle \Big)
\end{aligned}
$$

Shared Randomness

- Misst Alice ihr Qubit und erhält z.B. 0, so bleibt folgender Zustand zurück

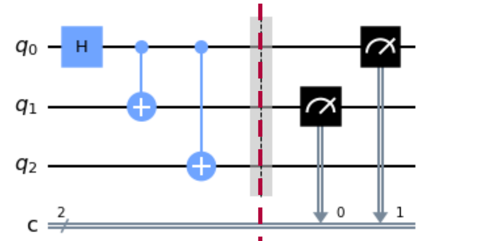
$$
\begin{aligned}
& \frac{1}{2}\Big(|00\rangle + |10\rangle + |01\rangle - |11\rangle \Big) \\
= \; & \frac{1}{2}\Big(|0\rangle \left(|0\rangle + |1\rangle\right) + |1\rangle \left(|0\rangle - |1\rangle\right)\Big)
\end{aligned}
$$

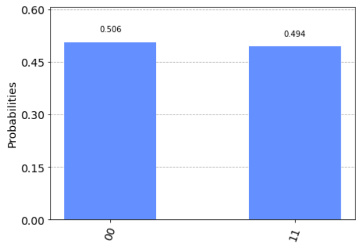
- Misst Bob nun sein Qubit erhält er 0 oder 1, je mit Wahrscheinlichkeit $\frac{1}{2}$
  - Es existiert keine Korrelation mehr zwischen Alice und Bobs Qubits in dieser Messbasis (Anwendung von Hadamard)!

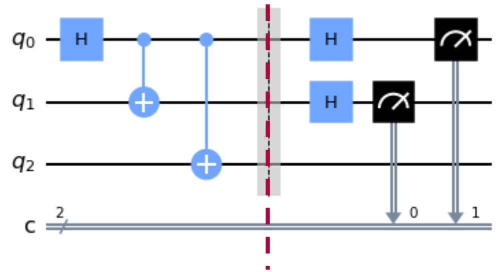
- Alice und Bob können, wenn sie viele gleich präparierte Qubits haben, durch Variierung der Messbasen feststellen, ob ihre zwei Photonen einem Bell-Zustand entsprechen!

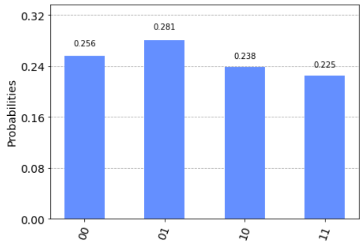
Simulation (mit Qiskit)

Messung in der Standardbasis versus Hadamard-Basis









$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

Zusammenfassung

- Zwei maximal verschränkte Qubits können als gemeinsamer "Zufallsgenerator" benutzt werden
- Wenn die beiden Qubits nicht maximal verschränkt sind, kann dies von Alice und Bob festgestellt werden.
  - Hierzu mehr in den nächsten Videos.

Vielen Dank
für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik