Quantenkryptographie (Teil 2)
- Anwendung von Verschränkung

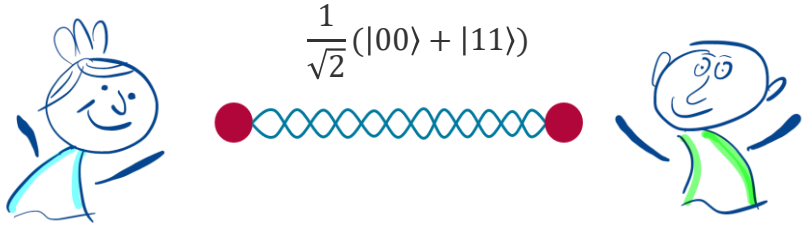
Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik

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

Dense Coding (1)

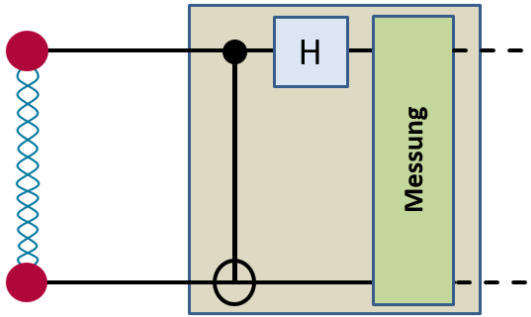
- Bob kann mit Hilfe eines Bell-Zustands durch Übermittlung seines Qubits an Alice 2 Bit Information (z.B. Buchstabe *a,b,c*, oder *d*) übertragen.
  - Bob führt hierzu davor eine entsprechende Operation (Manipulation seines Qubits) durch und sendet Alice danach sein Qubit.



$$
\begin{array}{lcll}
a & \Longrightarrow & (\mathbb{1} \otimes \mathbb{1}) & \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
b & \Longrightarrow & (\mathbb{1} \otimes Z) & \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
c & \Longrightarrow & (\mathbb{1} \otimes X) & \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
d & \Longrightarrow & (\mathbb{1} \otimes XZ) & \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{array}
$$

Dense Coding (2)

- Alice führt dann eine Bell-Messung an den beiden Qubits durch. Sie erhält eines von vier möglichen Ergebnissen.
  - Ergebnis kann dann entsprechend interpretiert werden.



$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow (0,0) \Longrightarrow a$$
$$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \rightarrow (1,0) \Longrightarrow b$$
$$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \rightarrow (0,1) \Longrightarrow c$$
$$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \rightarrow (1,1) \Longrightarrow d$$

Teleportation

Bei der Teleportation überträgt Alice mit Hilfe eines verschränkten 2-Qubit-Systems den Zustand eines Qubits an Bob

- Alice und Bob müssen sich hierzu einen Bell-Zustand "teilen".
- Alice Qubit "verliert" bei dem Vorgang seinen Zustand!

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle)$$

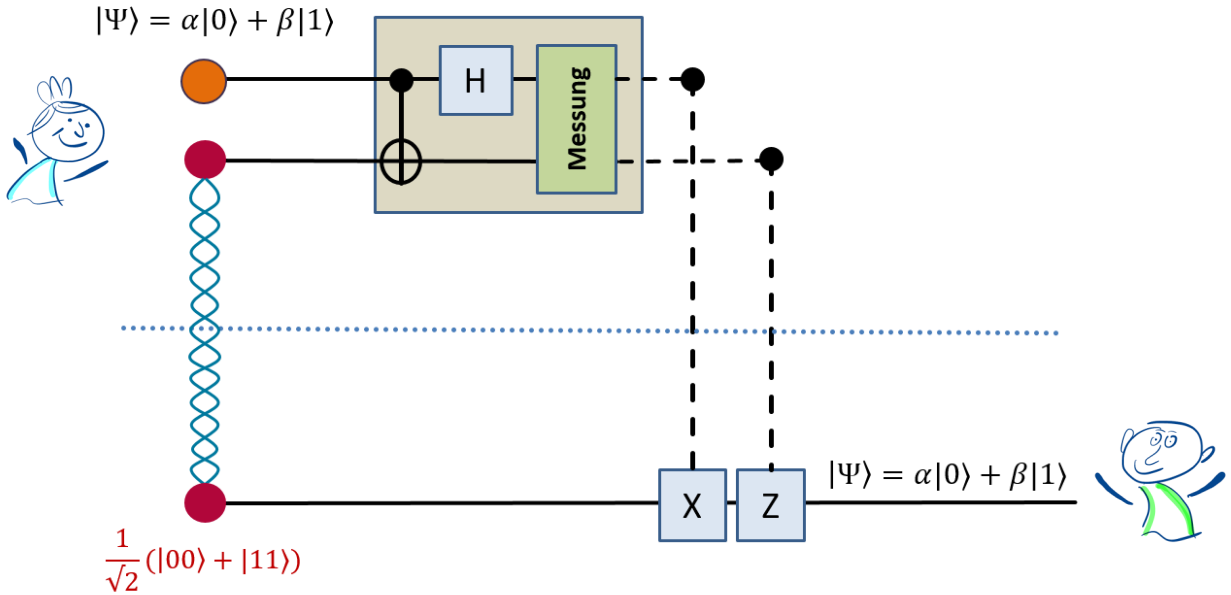
Alice

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

Bob

Beschreibung des Prozess

Alice führt mit ihren beiden Qubits eine Bell-Messung durch und teilt Bob das Messergebnis über einen klassischen Kanal mit.



Mathematische Beschreibung

Bildung des Gesamtsystems (3 Qubits) und Anwendung von CNOT:

$$
\begin{aligned}
|\Psi\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
&= \frac{1}{\sqrt{2}}(\alpha|000\rangle + \beta|100\rangle + \alpha|011\rangle + \beta|111\rangle) \\
\xrightarrow{CNOT_{1\mapsto 2}} & \frac{1}{\sqrt{2}}(\alpha|000\rangle + \beta|110\rangle + \alpha|011\rangle + \beta|101\rangle) \\
= & \frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle))
\end{aligned}
$$

Mathematische Beschreibung

Anwendung von Hadamard auf das erste Qubit:

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

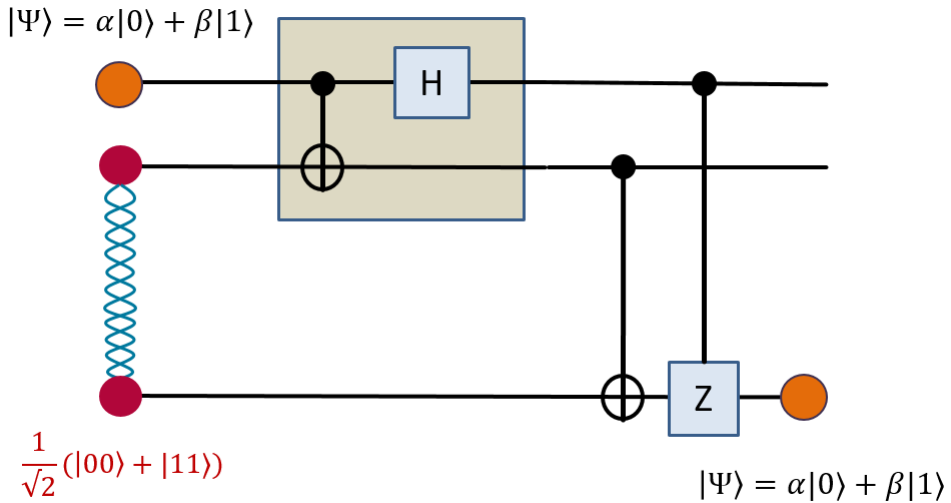
Mathematische Beschreibung

- Alice misst ihre beiden Qubits und meldet Bob das Messergebnis. Bob muss dann sein Qubit entsprechend nachbearbeiten.
  - Ursprüngliches Qubit von Alice wird hierdurch "zerstört".

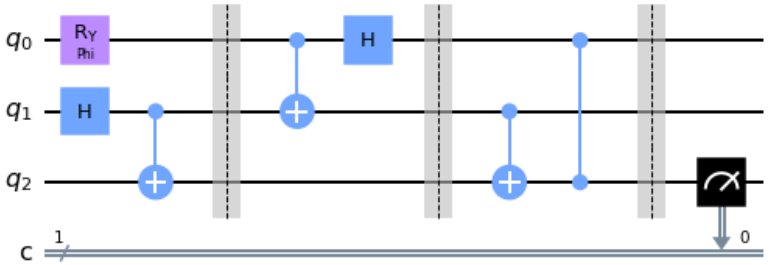
Alice Messergebnis		Bobs Nachbearbeitung		
$0,0$	$\longrightarrow$	$\mathbb{1}(\alpha\|0\rangle + \beta\|1\rangle)$	$=$	$\alpha\|0\rangle + \beta\|1\rangle$
$0,1$	$\longrightarrow$	$X(\alpha\|1\rangle + \beta\|0\rangle)$	$=$	$\alpha\|0\rangle + \beta\|1\rangle$
$1,0$	$\longrightarrow$	$Z(\alpha\|0\rangle - \beta\|1\rangle)$	$=$	$\alpha\|0\rangle + \beta\|1\rangle$
$1,1$	$\longrightarrow$	$ZX(\alpha\|1\rangle - \beta\|0\rangle)$	$=$	$\alpha\|0\rangle + \beta\|1\rangle$

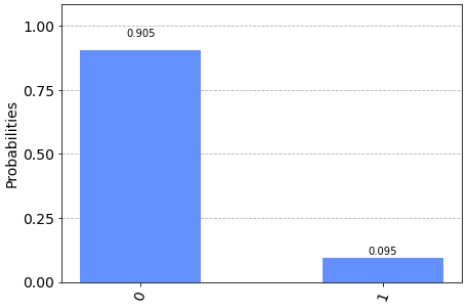
Intraportation

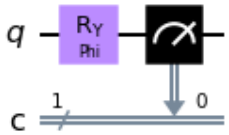
- Hat man Zugriff auf alle Qubits, kann der Zustand eines Qubits direkt portiert werden.
  - Man spricht dann von Intraportation.

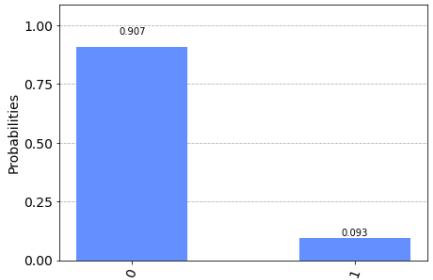


Simulation mit Qiskit









Zusammenfassung

- Bekannte Anwendung von zwei verschränkten Qubits:
  - Dense Coding (dichte Kodierung)
  - Teleportation

Vielen Dank
für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik