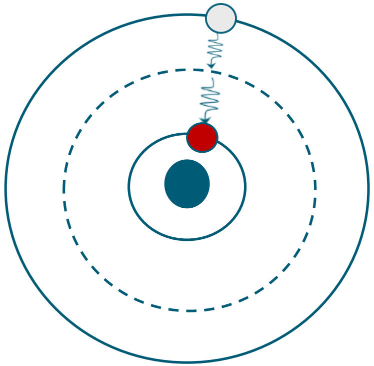
Quantenkryptographie (Teil 2) - Verschränkung

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik

Agenda

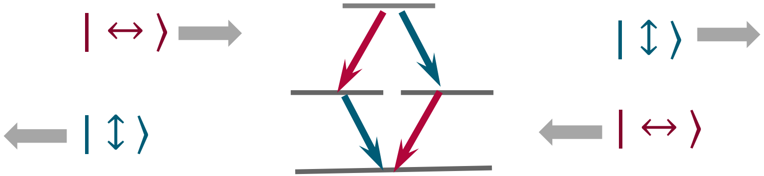
Erzeugung von verschränkten Photonen

- Angeregtes Cäsium-Atom



Möglichkeit 1

Möglichkeit 2

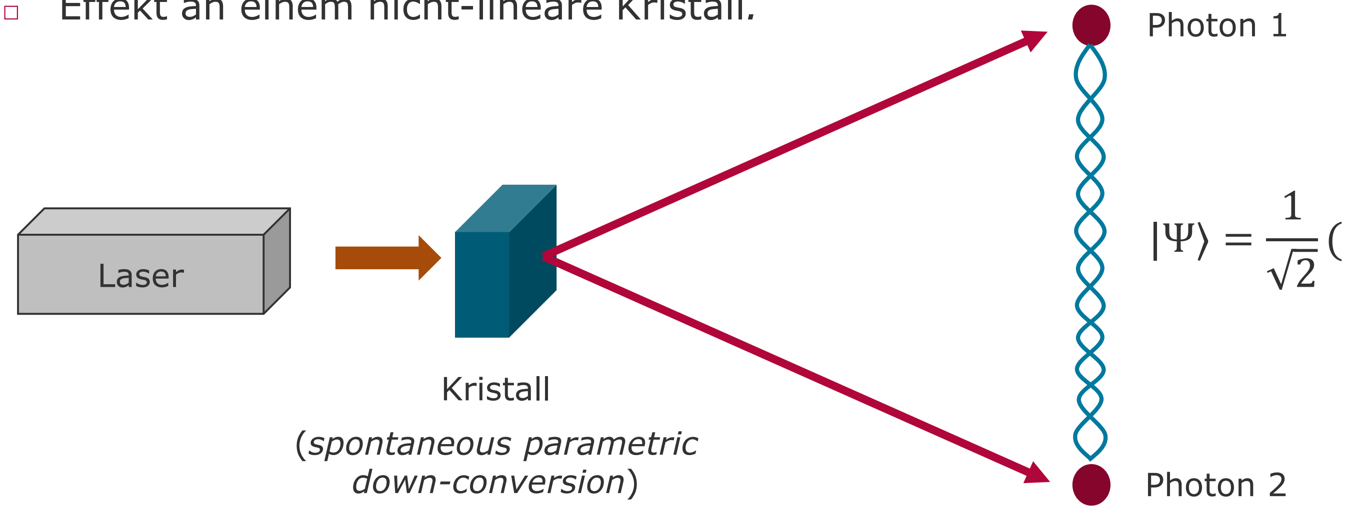


Überlagerung beider Möglichkeiten:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|\updownarrow\leftrightarrow\rangle + |\leftrightarrow\updownarrow\rangle\right)$$

Erzeugung von verschränkten Photonen

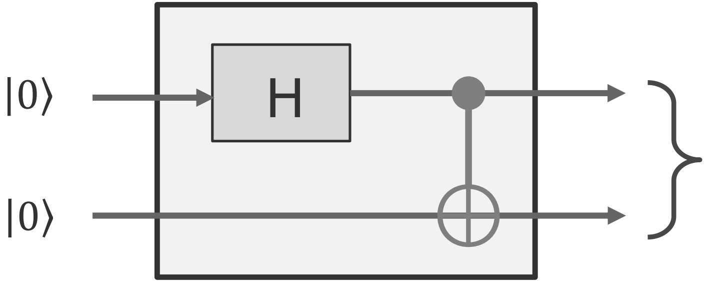
- *Parametric Down Conversion*.
  - Effekt an einem nicht-lineare Kristall.



$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

Erzeugung von verschränkten Qubits

- Schaltkreis



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

  - Erzeugung der Bellzustände:

$$|00\rangle \rightarrow |\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|10\rangle \rightarrow |\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|01\rangle \rightarrow |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|11\rangle \rightarrow |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

-

Verschränkung und Bell-Zustände

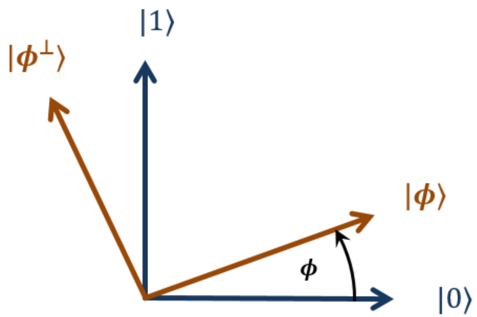
- Die vier Bell-Zustände $|\phi^+\rangle, |\phi^-\rangle, |\Psi^+\rangle$ und $|\Psi^-\rangle$ bilden eine Orthonormalbasis für ein Zwei-Qubit-System.
  - Zustandsvektoren stehen senkrecht aufeinander.
  - Es gilt $\langle\phi^+|\phi^+\rangle = \langle\phi^-|\phi^-\rangle = \langle\Psi^+|\Psi^+\rangle = \langle\Psi^-|\Psi^-\rangle = 1$
  - Und $\langle\phi^+|\phi^-\rangle = 0, \langle\phi^+|\Psi^+\rangle = 0, \langle\phi^+|\Psi^-\rangle = 0$, etc.

- Die in einem verschränkten Zustand enthaltene "Korrelation" ist unabhängig von der gewählten Basis.

- Die Bell-Zustände (auch ERP-Zustände genannt) sind *maximal verschränkt.*
  - Dazu später mehr.

Bellzustand in einer anderen Basis

- Darstellung von $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ in der $\{|\phi\rangle, |\phi^{\perp}\rangle\}$-Basis:
  - $|\phi\rangle = \cos\phi\,|0\rangle + \sin\phi\,|1\rangle$
  - $|\phi^{\perp}\rangle = -\sin\phi\,|0\rangle + \cos\phi\,|1\rangle$



- Transformation
  - $|0\rangle = \cos\phi\,|\phi\rangle - \sin\phi\,|\phi^{\perp}\rangle$
  - $|1\rangle = \sin\phi\,|\phi\rangle + \cos\phi\,|\phi^{\perp}\rangle$

Rechnung

$$
\begin{aligned}
|\Psi\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B\right) \\
&= \frac{1}{\sqrt{2}}\Bigg(\left(\cos(\phi)\,|\phi\rangle_A - \sin(\phi)\,|\phi^\perp\rangle_A\right)\left(\cos(\phi)\,|\phi\rangle_B - \sin(\phi)\,|\phi^\perp\rangle_B\right) \\
&\quad + \left(\sin(\phi)\,|\phi\rangle_A + \cos(\phi)\,|\phi^\perp\rangle_A\right)\left(\sin(\phi)\,|\phi\rangle_B + \cos(\phi)\,|\phi^\perp\rangle_B\right)\Bigg) \\
&= \frac{1}{\sqrt{2}}\Bigg(\cos^2(\phi)\,|\phi\rangle_A|\phi\rangle_B - \sin(\phi)\cos(\phi)\left(|\phi^\perp\rangle_A|\phi\rangle_B + |\phi\rangle_A|\phi^\perp\rangle_B\right) + \sin^2(\phi)\,|\phi^\perp\rangle_A|\phi^\perp\rangle_B \\
&\quad + \sin^2(\phi)\,|\phi\rangle_A|\phi\rangle_B + \sin(\phi)\cos(\phi)\left(|\phi^\perp\rangle_A|\phi\rangle_B + |\phi\rangle_A|\phi^\perp\rangle_B\right) + \cos^2(\phi)\,|\phi^\perp\rangle_A|\phi^\perp\rangle_B\Bigg) \\
&= \frac{1}{\sqrt{2}}\left(|\phi\rangle_A|\phi\rangle_B + |\phi^\perp\rangle_A|\phi^\perp\rangle_B\right)
\end{aligned}
$$

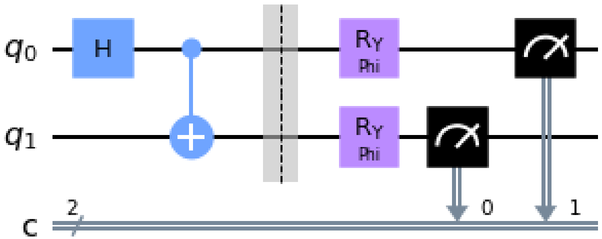
$$
\boxed{
\begin{aligned}
|0\rangle_A &= \cos(\phi)\,|\phi\rangle_A - \sin(\phi)\,|\phi^\perp\rangle_A \\
|1\rangle_A &= \sin(\phi)\,|\phi\rangle_A + \cos(\phi)\,|\phi^\perp\rangle_A \\
\\
|0\rangle_B &= \cos(\phi)\,|\phi\rangle_B - \sin(\phi)\,|\phi^\perp\rangle_B \\
|1\rangle_B &= \sin(\phi)\,|\phi\rangle_B + \cos(\phi)\,|\phi^\perp\rangle_B
\end{aligned}
}
$$

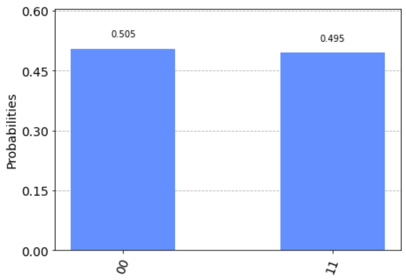
Messung in einer gedrehten Basis (mit Qiskit)

Erzeugung des Bell-Zustands

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

und Messung in einer gedrehten Basis:

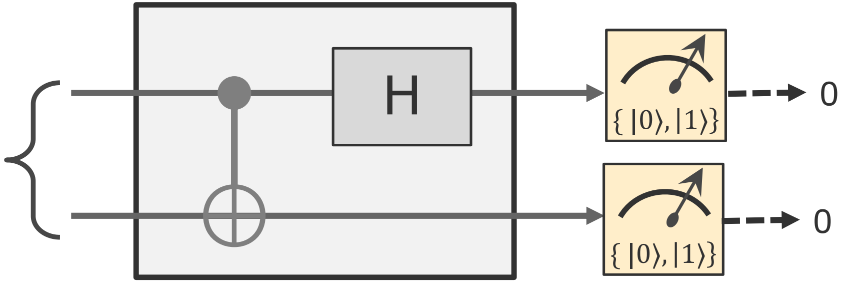




Analyse eines verschränkten Zustands

- Bell-Messung

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



  - Analyse der Bell-Zustände:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow 0{,}0$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \rightarrow 1{,}0$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \rightarrow 0{,}1$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \rightarrow 1{,}1$$

-

Verschränkung von drei Qubits

- Häufig vorkommende verschränkte Systemzustände mit 3 Qubits:
  - Zustände können auf noch mehr Qubits verallgemeinert werden.
  - GHZ-Zustand (Greenberger, Horne und Zeilinger)

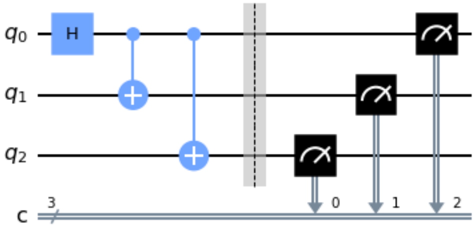
$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)$$

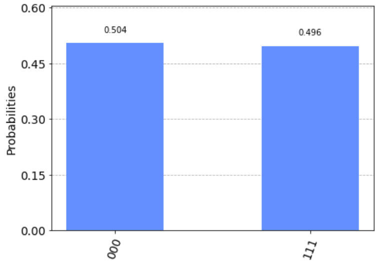
  - W-Zustand (Werner)

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|001\rangle + |010\rangle + |100\rangle\right)$$

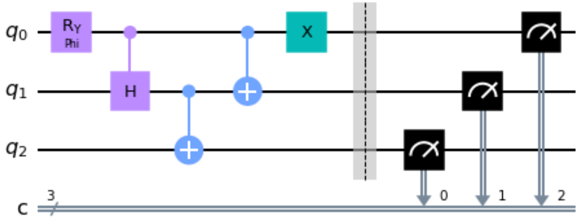
Verschränkung von drei Qubits (Simulation mit Qiskit)

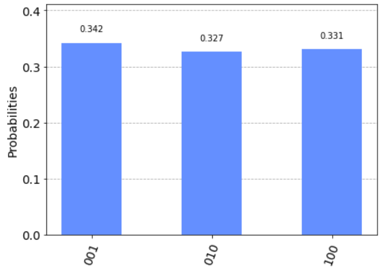
- Schaltkreis zur Erzeugung der Zustände
  - GHZ-Zustand





  - W-Zustand ($\phi = 2\arccos(\frac{1}{\sqrt{3}})$)





Zusammenfassung

- Verschränkte Systeme (Photonen) können physikalisch erzeugt werden.
- Bell-Zustände sind wichtige grundlegende Systeme.
  - Bilden eine Basis für Zwei-Qubit-Systeme.
  - Wir werden sehr oft mit $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ arbeiten.
- Die Verschränkung zeigt sich bei den Bellzuständen im jeder (gedrehten) Basis.

$$|00\rangle \to |\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|10\rangle \to |\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|01\rangle \to |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|11\rangle \to |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

- Es können auch mehrere Qubits miteinander verschränkt sein.
  - GHZ- und W-Zustände sind wichtige Beispiele.

Hasso Plattner Institut
Digital Engineering • Universität Potsdam

Vielen Dank
für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik