Abhörsichere Kommunikation über Quanten-Repeater

Christian Deppe

November 2017

Outline

Outline

Outline

Outline

Outline

Outline

Outline

Outline

Historischer Überblick

- “Klassische” Modellierung der Informationsübertragung: Shannon 1948.

Historischer Überblick

- “Klassische” Modellierung der Informationsübertragung: Shannon 1948.
- Ideen:
  - lokale Berechnungen sind “frei”, Übertragungen sind “teuer”.
  - Quantifizierung von Datenübertragung und Datenkompression.

Historischer Überblick

- “Klassische” Modellierung der Informationsübertragung: Shannon 1948.
- Ideen:
  - lokale Berechnungen sind “frei”, Übertragungen sind “teuer”.
  - Quantifizierung von Datenübertragung und Datenkompression.
- Die wichtigsten Kommunikationsalgorithmen beruhen immer noch auf Shannons Grundideen.

Historischer Überblick

- “Klassische” Modellierung der Informationsübertragung: Shannon 1948.
- Ideen:
  - lokale Berechnungen sind “frei”, Übertragungen sind “teuer”.
  - Quantifizierung von Datenübertragung und Datenkompression.
- Die wichtigsten Kommunikationsalgorithmen beruhen immer noch auf Shannons Grundideen.
- Planck, Einstein, Bohr, de Broglie, Born, Heisenberg, Schrödinger, Pauli, Dirac, und von Neumann sind die Pioniere der Quantentheorie (1920er und 1930er).

Historischer Überblick

- “Klassische” Modellierung der Informationsübertragung: Shannon 1948.
- Ideen:
  - lokale Berechnungen sind “frei”, Übertragungen sind “teuer”.
  - Quantifizierung von Datenübertragung und Datenkompression.
- Die wichtigsten Kommunikationsalgorithmen beruhen immer noch auf Shannons Grundideen.
- Planck, Einstein, Bohr, de Broglie, Born, Heisenberg, Schrödinger, Pauli, Dirac, und von Neumann sind die Pioniere der Quantentheorie (1920er und 1930er).
- Fannes, Holevo (erste Forscher in der Quanteninformationstheorie, 1970er)

Historischer Überblick

- “Klassische” Modellierung der Informationsübertragung: Shannon 1948.
- Ideen:
  - lokale Berechnungen sind “frei”, Übertragungen sind “teuer”.
  - Quantifizierung von Datenübertragung und Datenkompression.
- Die wichtigsten Kommunikationsalgorithmen beruhen immer noch auf Shannons Grundideen.
- Planck, Einstein, Bohr, de Broglie, Born, Heisenberg, Schrödinger, Pauli, Dirac, und von Neumann sind die Pioniere der Quantentheorie (1920er und 1930er).
- Fannes, Holevo (erste Forscher in der Quanteninformationstheorie, 1970er)
- 1980er: NoCloning Theorem (Wootters, Zurek, 1982), BB84 (Bennett, Brassard, 1984).

Historischer Überblick

- “Klassische” Modellierung der Informationsübertragung: Shannon 1948.
- Ideen:
  - lokale Berechnungen sind “frei”, Übertragungen sind “teuer”.
  - Quantifizierung von Datenübertragung und Datenkompression.
- Die wichtigsten Kommunikationsalgorithmen beruhen immer noch auf Shannons Grundideen.
- Planck, Einstein, Bohr, de Broglie, Born, Heisenberg, Schrödinger, Pauli, Dirac, und von Neumann sind die Pioniere der Quantentheorie (1920er und 1930er).
- Fannes, Holevo (erste Forscher in der Quanteninformationstheorie, 1970er)
- 1980er: NoCloning Theorem (Wootters, Zurek, 1982), BB84 (Bennett, Brassard, 1984).
- seit 1990: Stetig steigende Forschungsaktivität.

Highlights der Quanteninformationstheorie seit 1990

- QKD (Eckert, Bennett, ...)

Highlights der Quanteninformationstheorie seit 1990

- QKD (Eckert, Bennett, ...)
- Teleportationsprotokol (Bennett, Peres, Wootters, Brassard, Josza, Crepeau, 1993)

Highlights der Quanteninformationstheorie seit 1990

- QKD (Eckert, Bennett, ...)
- Teleportationsprotokol (Bennett, Peres, Wootters, Brassard, Josza, Crepeau, 1993)
- Faktorzerlegung in polynomieller Zeit (Shor, 1994)

Highlights der Quanteninformationstheorie seit 1990

- QKD (Eckert, Bennett, ...)
- Teleportationsprotokol (Bennett, Peres, Wootters, Brassard, Josza, Crepeau, 1993)
- Faktorzerlegung in polynomieller Zeit (Shor, 1994)
- Quantenfehlerkorrigierende Codes (Shor, 1995)

Highlights der Quanteninformationstheorie seit 1990

- QKD (Eckert, Bennett, ...)
- Teleportationsprotokol (Bennett, Peres, Wootters, Brassard, Josza, Crepeau, 1993)
- Faktorzerlegung in polynomieller Zeit (Shor, 1994)
- Quantenfehlerkorrigierende Codes (Shor, 1995)
- HSW Theorem (Holevo, Schumacher, Westmoreland, 1997) (Holevo 1973)

Highlights der Quanteninformationstheorie seit 1990

- QKD (Eckert, Bennett, ...)
- Teleportationsprotokol (Bennett, Peres, Wootters, Brassard, Josza, Crepeau, 1993)
- Faktorzerlegung in polynomieller Zeit (Shor, 1994)
- Quantenfehlerkorrigierende Codes (Shor, 1995)
- HSW Theorem (Holevo, Schumacher, Westmoreland, 1997) (Holevo 1973)
- Superdichte Codes (Bennett, Holevo, 2002)

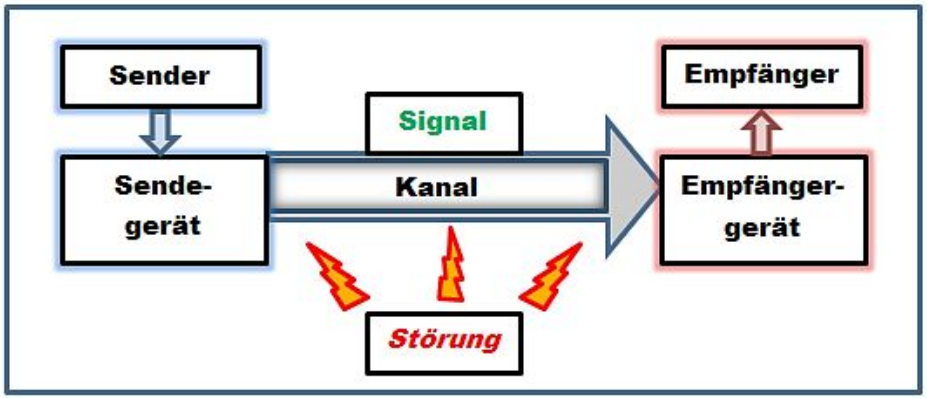
Highlights der Quanteninformationstheorie seit 1990

- QKD (Eckert, Bennett, ...)
- Teleportationsprotokol (Bennett, Peres, Wootters, Brassard, Josza, Crepeau, 1993)
- Faktorzerlegung in polynomieller Zeit (Shor, 1994)
- Quantenfehlerkorrigierende Codes (Shor, 1995)
- HSW Theorem (Holevo, Schumacher, Westmoreland, 1997) (Holevo 1973)
- Superdichte Codes (Bennett, Holevo, 2002)
- Superaktivierung von Quantenkanälen (Smith, Yard, 2008)

Highlights der Quanteninformationstheorie seit 1990

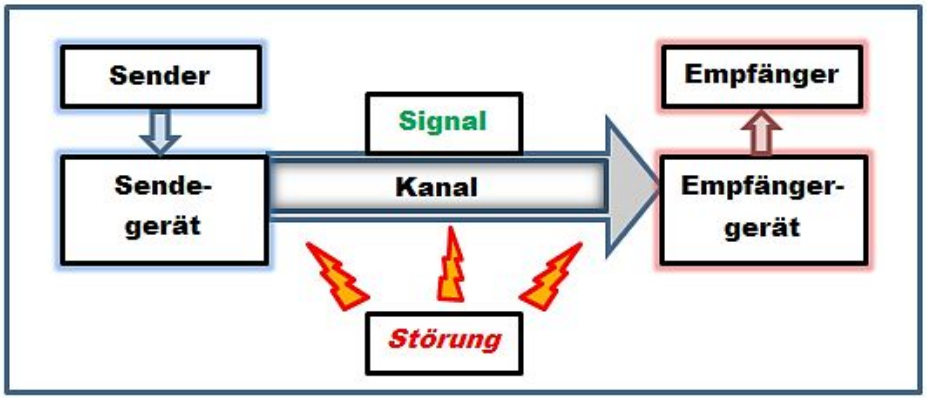
- QKD (Eckert, Bennett, ...)
- Teleportationsprotokol (Bennett, Peres, Wootters, Brassard, Josza, Crepeau, 1993)
- Faktorzerlegung in polynomieller Zeit (Shor, 1994)
- Quantenfehlerkorrigierende Codes (Shor, 1995)
- HSW Theorem (Holevo, Schumacher, Westmoreland, 1997) (Holevo 1973)
- Superdichte Codes (Bennett, Holevo, 2002)
- Superaktivierung von Quantenkanälen (Smith, Yard, 2008)
- Bielefelder Beiträge: Ahlswede, Blinovsky, D., Cai, Winter (Identifikation, Codes mit variabler Länge, Datenkompression, ...)

Klassische Kommunikation



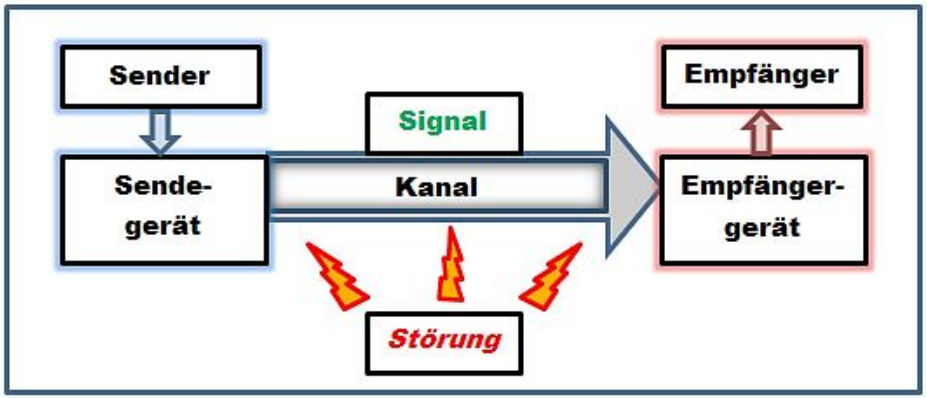
- Daten oder Nachrichten $\mathcal{M} = \{1, \ldots, M\}$.

Klassische Kommunikation



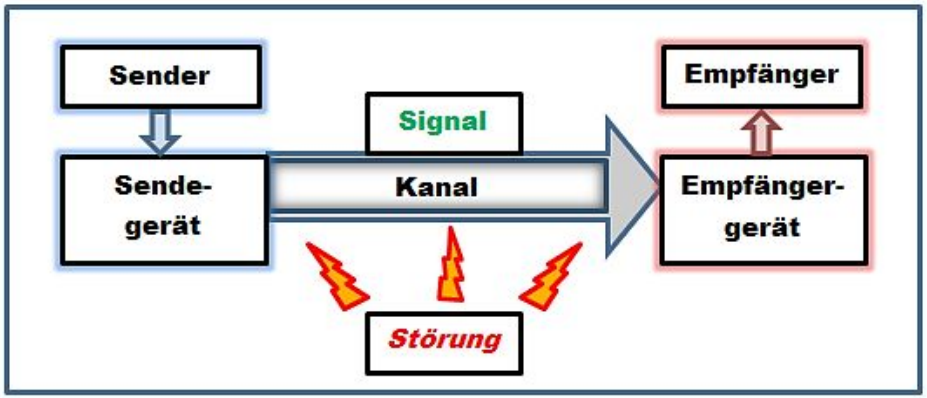
- Daten oder Nachrichten $\mathcal{M} = \{1, \ldots, M\}$.
- Sender sendet Signale $\mathcal{X} = \{0, \ldots, d_1\}$ ($d_1 = 1$, Bits).

Klassische Kommunikation



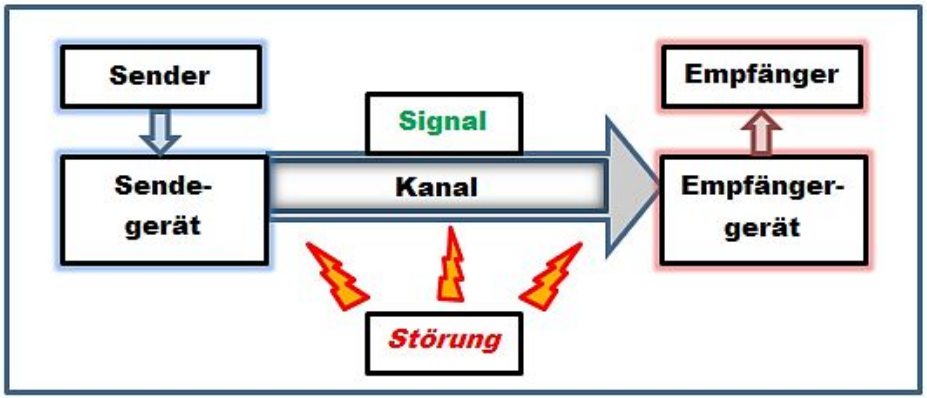
- Daten oder Nachrichten $\mathcal{M} = \{1, \ldots, M\}$.
- Sender sendet Signale $\mathcal{X} = \{0, \ldots, d_1\}$ ($d_1 = 1$, Bits).
- Empfänger empfängt Signale $\mathcal{Y} = \{0, \ldots, d_2\}$.

Klassische Kommunikation

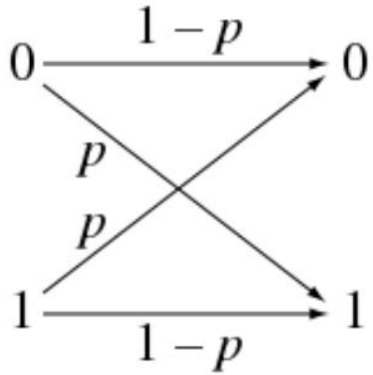


- Daten oder Nachrichten $\mathcal{M} = \{1, \ldots, M\}$.
- Sender sendet Signale $\mathcal{X} = \{0, \ldots, d_1\}$ ($d_1 = 1$, Bits).
- Empfänger empfängt Signale $\mathcal{Y} = \{0, \ldots, d_2\}$.
- Praktische Annahme: $|\mathcal{X}| = |\mathcal{Y}| = 2$.

Klassische Kommunikation



- Daten oder Nachrichten $\mathcal{M} = \{1, \ldots, M\}$.
- Sender sendet Signale $\mathcal{X} = \{0, \ldots, d_1\}$ ($d_1 = 1$, Bits).
- Empfänger empfängt Signale $\mathcal{Y} = \{0, \ldots, d_2\}$.
- Praktische Annahme: $|\mathcal{X}| = |\mathcal{Y}| = 2$.
- Störungen:



Klassische Kommunikation: Blockkodierung

- $c : \mathcal{M} \to \{0,1\}^n$ Einkodierungsfunktion.

Klassische Kommunikation: Blockkodierung

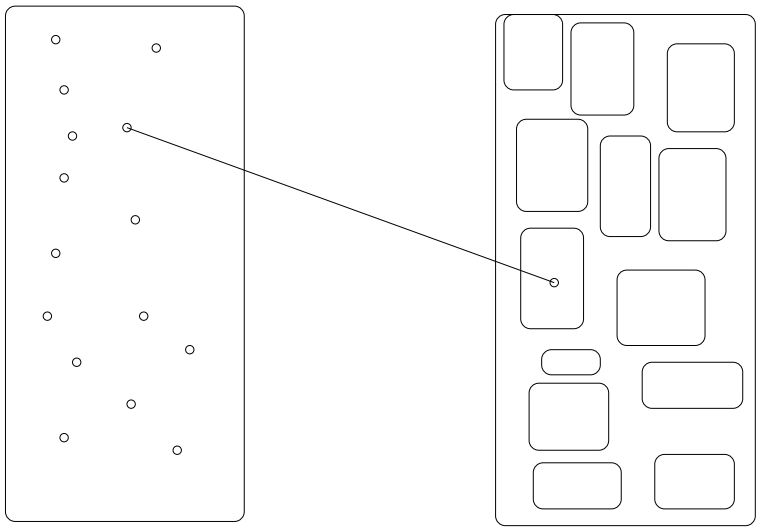
- $c : \mathcal{M} \to \{0,1\}^n$ Einkodierungsfunktion.
- $\{\mathcal{D}_i : 1 \leq i \leq M\}$ disjunkte Dekodiermengen.

Klassische Kommunikation: Blockkodierung

- $c : \mathcal{M} \to \{0,1\}^n$ Einkodierungsfunktion.
- $\{\mathcal{D}_i : 1 \leq i \leq M\}$ disjunkte Dekodiermengen.
- **Was sollte für einen “guten” Code gelten?**

Klassische Kommunikation: Blockkodierung

- $c : \mathcal{M} \to \{0,1\}^n$ Einkodierungsfunktion.
- $\{\mathcal{D}_i : 1 \leq i \leq M\}$ disjunkte Dekodiermengen.
- **Was sollte für einen "guten" Code gelten?**
- $P(D_i|c(i)) \geq 1 - \lambda$
  Korrekter Empfang mit hoher Wahrscheinlichkeit !!
- Dies nennt man einen (M, n, λ) Code.



Klassische Kommunikation: Blockkodierung bei binären Kanälen

- **Ein Ziel (Shannon):** Maximiere bei gegebenem Kanal die Anzahl der möglichen Nachrichten, so dass die Fehlerwahrscheinlichkeit gegen 0 geht, wenn die Blocklänge gegen unendlich geht.

Klassische Kommunikation: Blockkodierung bei binären Kanälen

- **Ein Ziel (Shannon):** Maximiere bei gegebenem Kanal die Anzahl der möglichen Nachrichten, so dass die Fehlerwahrscheinlichkeit gegen 0 geht, wenn die Blocklänge gegen unendlich geht.
- Man betrachtet die Rate eines (M, n, λ) Codes:

$$R = \frac{\log_2 M}{n}.$$

- Offensichtlich hat ein binärer fehlerfreier Code die Rate 1.

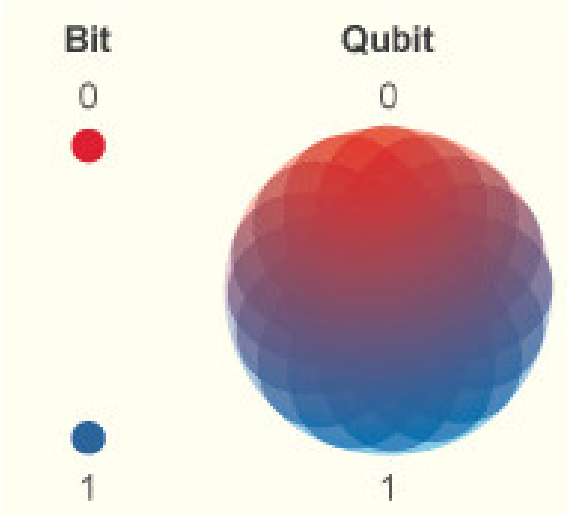
Klassische Kommunikation: Blockkodierung bei binären Kanälen

- **Ein Ziel (Shannon):** Maximiere bei gegebenem Kanal die Anzahl der möglichen Nachrichten, so dass die Fehlerwahrscheinlichkeit gegen 0 geht, wenn die Blocklänge gegen unendlich geht.
- Man betrachtet die Rate eines (M, n, λ) Codes:

$$R = \frac{\log_2 M}{n}.$$

- Offensichtlich hat ein binärer fehlerfreier Code die Rate 1.
- Die maximale Rate eines Codes für einen gegebenen Kanal, so dass die Fehlerwahrscheinlichkeit gegen 0 geht nennt man die Kapazität des Kanals.

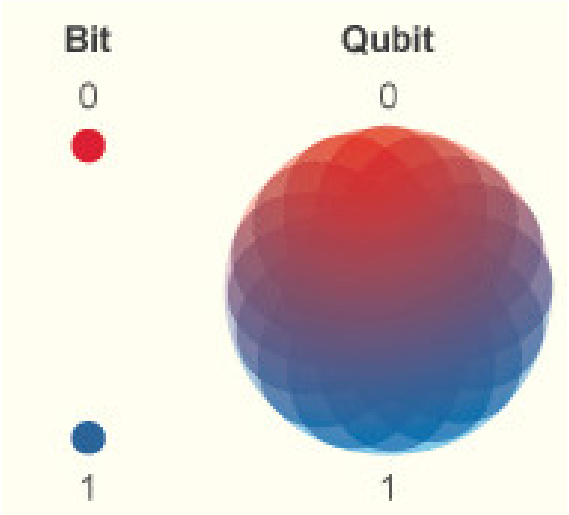
Bits vs. Qubits



$$x \in \{0,1\} \longleftrightarrow |\psi\rangle \equiv \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

- α und β sind komplexe Zahlen mit $|\alpha|^2 + |\beta|^2 = 1$

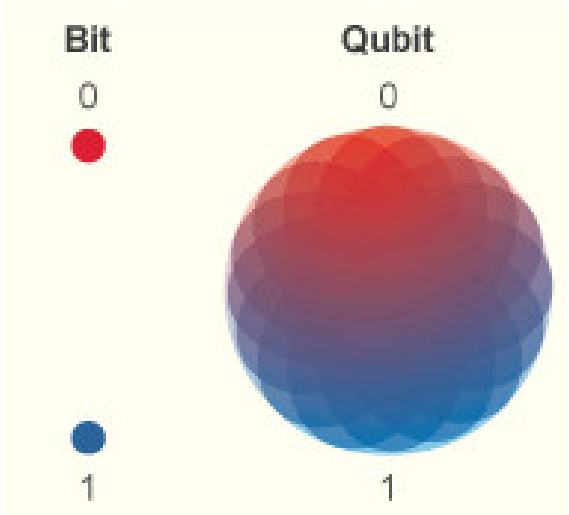
Bits vs. Qubits



$$x \in \{0,1\} \longleftrightarrow |\psi\rangle \equiv \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

- α und β sind komplexe Zahlen mit $|\alpha|^2 + |\beta|^2 = 1$
- $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Bits vs. Qubits



$$x \in \{0,1\} \longleftrightarrow |\psi\rangle \equiv \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

- α und β sind komplexe Zahlen mit $|\alpha|^2 + |\beta|^2 = 1$
- $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ Element eines zweidimensionalen Hilbertraumes.

Qubits

- Erste Besonderheit von Qubits: Darstellung zu jeder Orthonormalen Basis möglich.
- $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha\,|0\rangle + \beta\,|1\rangle = \frac{\alpha+\beta}{\sqrt{2}}\,|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}\,|-\rangle$
- $|+\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ und $|-\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$
- Diese Basis nennt man die Hadamard Basis.

Qubits

- Der Sender stellt ein Qubit zu einer Basis her.
- $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$
- Der Empfänger kann eine beliebige Basis wählen und “misst” zu dieser Basis.
- Wenn er die Standardbasis wählt, misst er mit der Wahrscheinlichkeit $|\alpha|^2$ ($|\beta|^2$) das Qubit $|0\rangle$ ($|1\rangle$).
- Dannach ist das Qubit in diesem Zustand!
- Er kann jedoch auch jede andere Basis wählen und erhält die entsprechenden Messergebnisse.

Stern Gerlach Experiment

- Im Labor erzeugt man den Zustand $|0\rangle$.

Stern Gerlach Experiment

- Im Labor erzeugt man den Zustand $|0\rangle$.
- Falls man diesen Zustand in der Standard-Basis misst, erhalten wir immer den gleichen Zustand $|0\rangle$.

Stern Gerlach Experiment

- Im Labor erzeugt man den Zustand $|0\rangle$.
- Falls man diesen Zustand in der Standard-Basis misst, erhalten wir immer den gleichen Zustand $|0\rangle$.
- Was passiert wenn wir diesen Zustand in der Hadamard Basis messen?

Stern Gerlach Experiment

- Im Labor erzeugt man den Zustand $|0\rangle$.
- Falls man diesen Zustand in der Standard-Basis misst, erhalten wir immer den gleichen Zustand $|0\rangle$.
- Was passiert wenn wir diesen Zustand in der Hadamard Basis messen?
- Der Zustand $|0\rangle$ ist äquivalent zu einer gleichverteilten Superposition der Zustände $|+\rangle$ und $|-\rangle$.

Stern Gerlach Experiment

- Im Labor erzeugt man den Zustand $|0\rangle$.
- Falls man diesen Zustand in der Standard-Basis misst, erhalten wir immer den gleichen Zustand $|0\rangle$.
- Was passiert wenn wir diesen Zustand in der Hadamard Basis messen?
- Der Zustand $|0\rangle$ ist äquivalent zu einer gleichverteilten Superposition der Zustände $|+\rangle$ und $|-\rangle$.
- Aufgrund des Messpostulats erhalten wir den Zustand $|+\rangle$ oder $|-\rangle$ mit gleicher Wahrscheinlichkeit nach dem Messen.

Stern Gerlach Experiment

- Im Labor erzeugt man den Zustand $|0\rangle$.
- Falls man diesen Zustand in der Standard-Basis misst, erhalten wir immer den gleichen Zustand $|0\rangle$.
- Was passiert wenn wir diesen Zustand in der Hadamard Basis messen?
- Der Zustand $|0\rangle$ ist äquivalent zu einer gleichverteilten Superposition der Zustände $|+\rangle$ und $|-\rangle$.
- Aufgrund des Messpostulats erhalten wir den Zustand $|+\rangle$ oder $|-\rangle$ mit gleicher Wahrscheinlichkeit nach dem Messen.
- Nun messen wir wieder in der Standardbasis.

Stern Gerlach Experiment

- Im Labor erzeugt man den Zustand $|0\rangle$.
- Falls man diesen Zustand in der Standard-Basis misst, erhalten wir immer den gleichen Zustand $|0\rangle$.
- Was passiert wenn wir diesen Zustand in der Hadamard Basis messen?
- Der Zustand $|0\rangle$ ist äquivalent zu einer gleichverteilten Superposition der Zustände $|+\rangle$ und $|-\rangle$.
- Aufgrund des Messpostulats erhalten wir den Zustand $|+\rangle$ oder $|-\rangle$ mit gleicher Wahrscheinlichkeit nach dem Messen.
- Nun messen wir wieder in der Standardbasis.
- Das Ergebnis der Messung ist $|0\rangle$ oder $|1\rangle$ mit gleicher Wahrscheinlichkeit, wenn das Ergebnis vorher $|+\rangle$ war.
- Das gleiche gilt, falls das Ergebnis vorher $|-\rangle$ war.

Stern Gerlach Experiment

- Im Labor erzeugt man den Zustand $|0\rangle$.
- Falls man diesen Zustand in der Standard-Basis misst, erhalten wir immer den gleichen Zustand $|0\rangle$.
- Was passiert wenn wir diesen Zustand in der Hadamard Basis messen?
- Der Zustand $|0\rangle$ ist äquivalent zu einer gleichverteilten Superposition der Zustände $|+\rangle$ und $|-\rangle$.
- Aufgrund des Messpostulats erhalten wir den Zustand $|+\rangle$ oder $|-\rangle$ mit gleicher Wahrscheinlichkeit nach dem Messen.
- Nun messen wir wieder in der Standardbasis.
- Das Ergebnis der Messung ist $|0\rangle$ oder $|1\rangle$ mit gleicher Wahrscheinlichkeit, wenn das Ergebnis vorher $|+\rangle$ war.
- Das gleiche gilt, falls das Ergebnis vorher $|-\rangle$ war.
- Dies zeigt, dass die 2. Messung die 1. Messung vergisst.

Stern Gerlach Experiment

- Im Labor erzeugt man den Zustand $|0\rangle$.
- Falls man diesen Zustand in der Standard-Basis misst, erhalten wir immer den gleichen Zustand $|0\rangle$.
- Was passiert wenn wir diesen Zustand in der Hadamard Basis messen?
- Der Zustand $|0\rangle$ ist äquivalent zu einer gleichverteilten Superposition der Zustände $|+\rangle$ und $|-\rangle$.
- Aufgrund des Messpostulats erhalten wir den Zustand $|+\rangle$ oder $|-\rangle$ mit gleicher Wahrscheinlichkeit nach dem Messen.
- Nun messen wir wieder in der Standardbasis.
- Das Ergebnis der Messung ist $|0\rangle$ oder $|1\rangle$ mit gleicher Wahrscheinlichkeit, wenn das Ergebnis vorher $|+\rangle$ war.
- Das gleiche gilt, falls das Ergebnis vorher $|-\rangle$ war.
- Dies zeigt, dass die 2. Messung die 1. Messung vergisst.
- Es war eines der ersten Experimente, welches die Quantentheorie in der Praxis bestätigt.

Qubit Folgen

Seien zwei Qubits zur Standardbasis gegeben:

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix}, \qquad \begin{pmatrix} a_2 \\ b_2 \end{pmatrix}. \tag{1}$$

Die Folge dieser Vektoren wird durch das Tensorprodukt dargestellt:

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \otimes \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} \equiv \begin{pmatrix} a_1 \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} \\ b_1 \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} a_1 a_2 \\ a_1 b_2 \\ b_1 a_2 \\ b_1 b_2 \end{pmatrix}. \tag{2}$$

Für die Basen gilt:

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{3}$$

Qubit Folgen

Wir erhalten durch zwei zusammengesetzte Qubits:

$$|\xi\rangle \equiv \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle\,. \tag{4}$$

Qubit Folgen

Wir erhalten durch zwei zusammengesetzte Qubits:

$$|\xi\rangle \equiv \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle\,. \tag{4}$$

Die Physiker können jedoch auch besondere zusammengesetzte Zustände erstellen:

$$\left|\Phi^{+}\right\rangle^{AB} \equiv \frac{|0\rangle^{A}\,|0\rangle^{B} + |1\rangle^{A}\,|1\rangle^{B}}{\sqrt{2}}. \tag{5}$$

Qubit Folgen

Wir erhalten durch zwei zusammengesetzte Qubits:

$$|\xi\rangle \equiv \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle\,. \tag{4}$$

Die Physiker können jedoch auch besondere zusammengesetzte Zustände erstellen:

$$\left|\Phi^{+}\right\rangle^{AB} \equiv \frac{|0\rangle^{A}\,|0\rangle^{B} + |1\rangle^{A}\,|1\rangle^{B}}{\sqrt{2}}. \tag{5}$$

- Zustände dieser Art heißen verschränkte Zustände.
- Es gibt kein Tensorprodukt zweier Qubits mit dem man diesen Zustand erreichen kann.

Verschränkte Qubits

Betrachten wir nochmal:

$$\left|\Phi^{+}\right\rangle^{AB} \equiv \frac{|0\rangle^{A}|0\rangle^{B} + |1\rangle^{A}|1\rangle^{B}}{\sqrt{2}}. \tag{6}$$

Verschränkte Qubits

Betrachten wir nochmal:

$$\left|\Phi^{+}\right\rangle^{AB} \equiv \frac{|0\rangle^{A}|0\rangle^{B} + |1\rangle^{A}|1\rangle^{B}}{\sqrt{2}}. \tag{6}$$

- Nehmen wir an, dass Alice und Bob jeweils ein Qubit dieses verschränkten Qubitpärchens bekommen.

Verschränkte Qubits

Betrachten wir nochmal:

$$\left|\Phi^{+}\right\rangle^{AB} \equiv \frac{|0\rangle^{A}|0\rangle^{B} + |1\rangle^{A}|1\rangle^{B}}{\sqrt{2}}. \tag{6}$$

- Nehmen wir an, dass Alice und Bob jeweils ein Qubit dieses verschränkten Qubitpärchens bekommen.
- Was ist das besondere?

Verschränkte Qubits

Betrachten wir nochmal:

$$\left|\Phi^{+}\right\rangle^{AB} \equiv \frac{|0\rangle^{A}|0\rangle^{B} + |1\rangle^{A}|1\rangle^{B}}{\sqrt{2}}. \tag{6}$$

- Nehmen wir an, dass Alice und Bob jeweils ein Qubit dieses verschränkten Qubitpärchens bekommen.
- Was ist das besondere?
- Wenn Alice ihr Qubit zur Standardbasis misst, misst sie mit Wahrscheinlichkeit $\frac{1}{2}$: $|0\rangle^{A}|0\rangle^{B}$
- oder mit Wahrscheinlichkeit $\frac{1}{2}$: $|1\rangle^{A}|1\rangle^{B}$

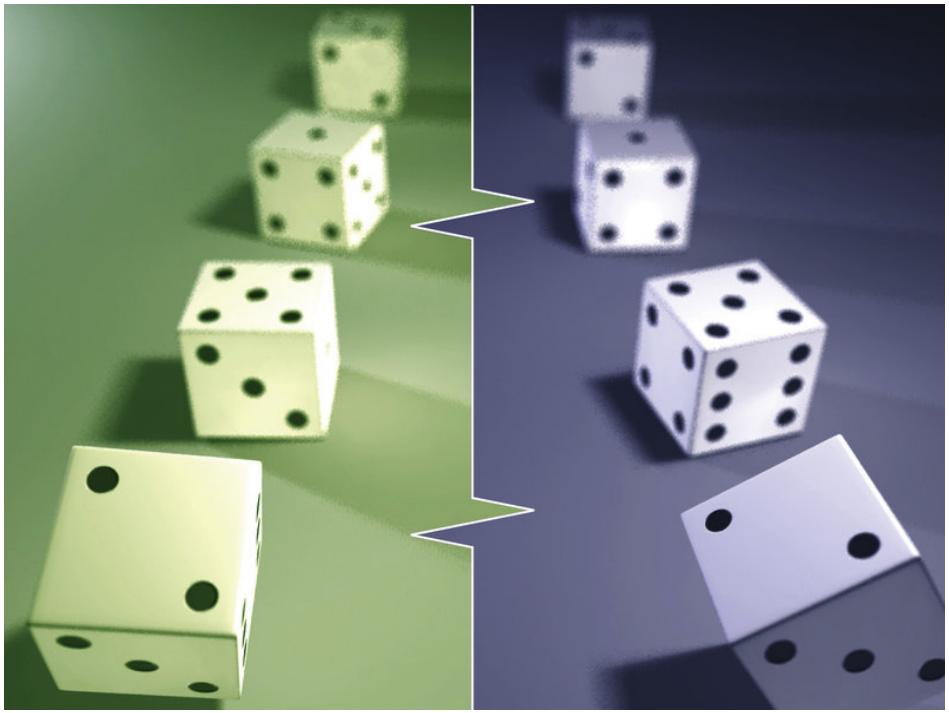
Verschränkte Qubits

Betrachten wir nochmal:

$$\left|\Phi^{+}\right\rangle^{AB} \equiv \frac{|0\rangle^{A}|0\rangle^{B} + |1\rangle^{A}|1\rangle^{B}}{\sqrt{2}}. \tag{6}$$

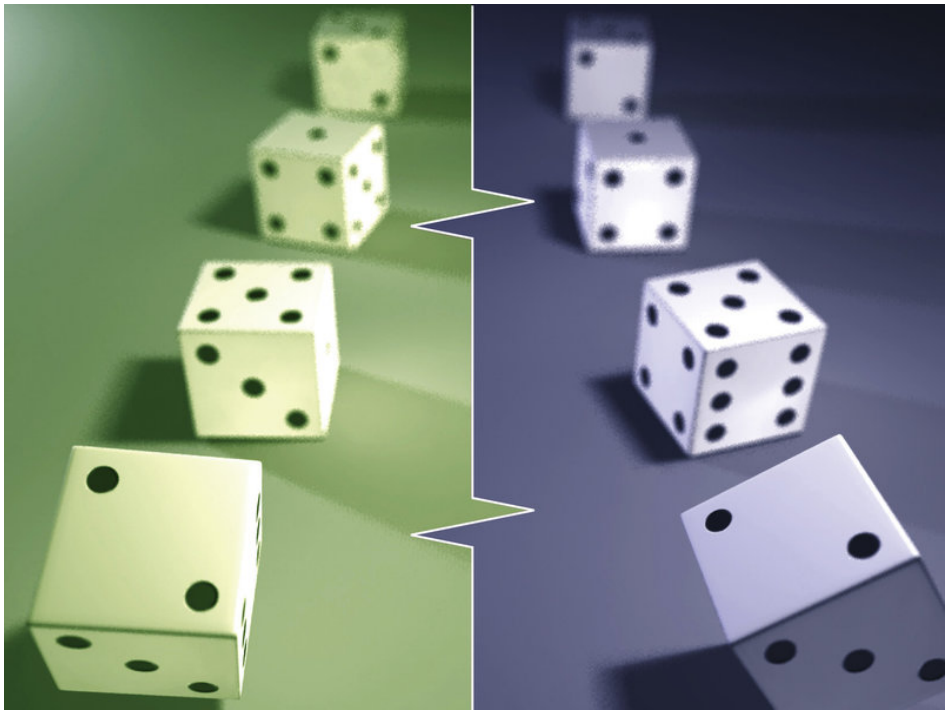
- Nehmen wir an, dass Alice und Bob jeweils ein Qubit dieses verschränkten Qubitpärchens bekommen.
- Was ist das besondere?
- Wenn Alice ihr Qubit zur Standardbasis misst, misst sie mit Wahrscheinlichkeit $\frac{1}{2}$: $|0\rangle^{A}|0\rangle^{B}$
- oder mit Wahrscheinlichkeit $\frac{1}{2}$: $|1\rangle^{A}|1\rangle^{B}$
- Damit steht nach dieser Messung das Messergebnis von Bob schon fest!!!!!!

Verschränkte Qubits



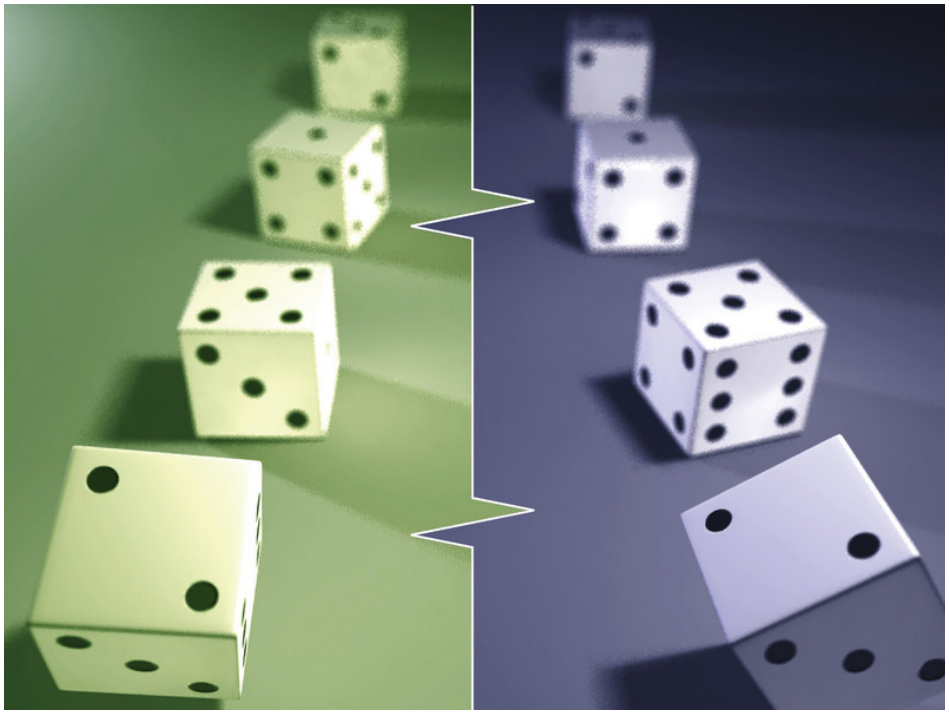
- Dies wurde praktisch nachgewiesen.

Verschränkte Qubits



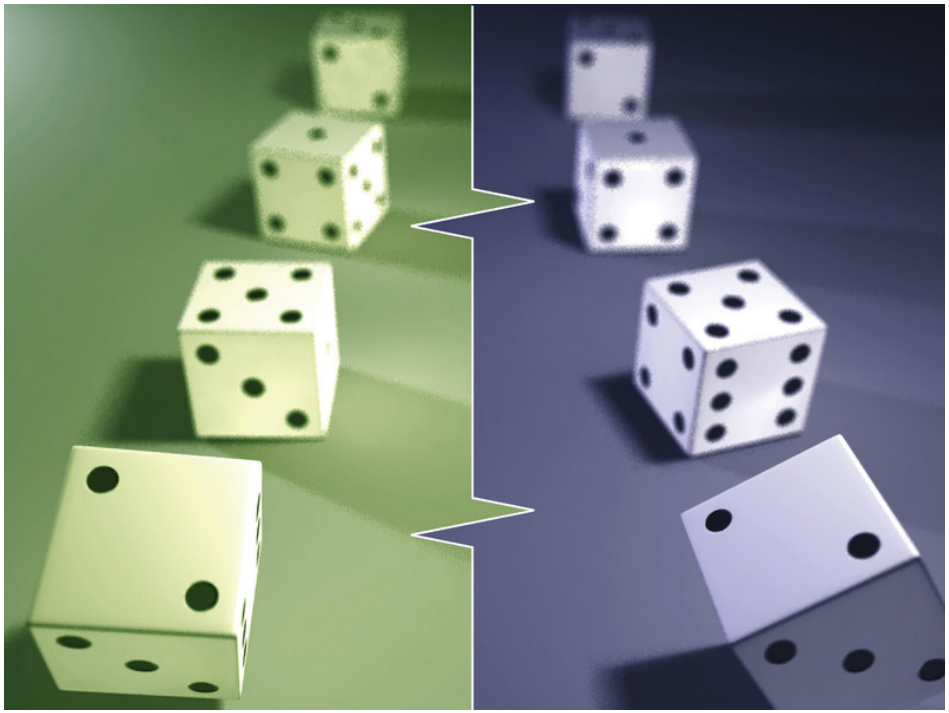
- Dies wurde praktisch nachgewiesen.
- Wir haben einen Münzwurf, der auf beiden Seiten das gleiche Ergebnis zeigt.

Verschränkte Qubits



- Dies wurde praktisch nachgewiesen.
- Wir haben einen Münzwurf, der auf beiden Seiten das gleiche Ergebnis zeigt.
- Sehr interessant für den Schlüsselaustausch in der Kryptographie.

Verschränkte Qubits



- Dies wurde praktisch nachgewiesen.
- Wir haben einen Münzwurf, der auf beiden Seiten das gleiche Ergebnis zeigt.
- Sehr interessant für den Schlüsselaustausch in der Kryptographie.
- “Entdecker”: Einstein, Podolski und Rosen (spukhafte Fernwirkung).

Teleportation eines Qubits

- Alice besitzt Qubit $|\xi>=\alpha|0>+\beta|1>$.

Teleportation eines Qubits

- Alice besitzt Qubit $|\xi>=\alpha|0>+\beta|1>$.
- Amplituden α, β sind Alice unbekannt.

Teleportation eines Qubits

- Alice besitzt Qubit $|\xi>=\alpha|0>+\beta|1>$.
- Amplituden α, β sind Alice unbekannt.
- Alice kann über einen klassischen Kanal mit Bob kommunizieren.

Teleportation eines Qubits

- Alice besitzt Qubit $|\xi>=\alpha|0>+\beta|1>$.
- Amplituden α, β sind Alice unbekannt.
- Alice kann über einen klassischen Kanal mit Bob kommunizieren.
- Alice und Bob teilen sich das Ebit $|e>=\frac{|00>^{AB}+|11>^{AB}}{\sqrt{2}}$.

Teleportation eines Qubits

- Alice besitzt Qubit $|\xi>=\alpha|0>+\beta|1>$.
- Amplituden α, β sind Alice unbekannt.
- Alice kann über einen klassischen Kanal mit Bob kommunizieren.
- Alice und Bob teilen sich das Ebit $|e>=\frac{|00>^{AB}+|11>^{AB}}{\sqrt{2}}$.
- **Ziel:** Alice sendet $|\xi>$ an Bob.

Teleportation eines Qubits

- Alice besitzt Qubit $|\xi>=\alpha|0>+\beta|1>$.
- Amplituden α, β sind Alice unbekannt.
- Alice kann über einen klassischen Kanal mit Bob kommunizieren.
- Alice und Bob teilen sich das Ebit $|e>=\frac{|00>^{AB}+|11>^{AB}}{\sqrt{2}}$.
- **Ziel:** Alice sendet $|\xi>$ an Bob.
- **Probleme:**
  - Alice kennt Amplituden nicht und eine Messung zerstört das Qubit.
  - Alice kann keine Kopien von $|\xi>$ erzeugen, um die Amplituden durch hinreichend viele Messungen zu approximieren.
  - Gäbe es einen Algorithmus zur Rekonstruktion von Quantenbits aus klassischer Information, so existiert ein Quanten-Kopierer.

Teleportation eines Qubits

- Alice besitzt Qubit $|\xi>=\alpha|0>+\beta|1>$.
- Amplituden α, β sind Alice unbekannt.
- Alice kann über einen klassischen Kanal mit Bob kommunizieren.
- Alice und Bob teilen sich das Ebit $|e>=\frac{|00>^{AB}+|11>^{AB}}{\sqrt{2}}$.
- **Ziel:** Alice sendet $|\xi>$ an Bob.
- **Probleme:**
  - Alice kennt Amplituden nicht und eine Messung zerstört das Qubit.
  - Alice kann keine Kopien von $|\xi>$ erzeugen, um die Amplituden durch hinreichend viele Messungen zu approximieren.
  - Gäbe es einen Algorithmus zur Rekonstruktion von Quantenbits aus klassischer Information, so existiert ein Quanten-Kopierer.
- **Lösung:** Setze $|\xi>$ und $|e>$ zusammen:

$$|\xi>\otimes|e>=\frac{\alpha|000>^{AAB}+\alpha|011>^{AAB}+\beta|100>^{AAB}+\beta|111>^{AAB}}{\sqrt{2}}$$

- Man beachte: Alice hat Zugriff auf die ersten beiden Qubits, Bob auf das 3. Qubit.

Teleportation eines Qubits

1. Alice wendet CNOT auf das 1. Qubit und 2. Qubit an:

$$CNOT|\xi e> \rightarrow \frac{\alpha|000> +\alpha|011> +\beta|110> +\beta|101>}{\sqrt{2}}$$

Teleportation eines Qubits

1. Alice wendet CNOT auf das 1. Qubit und 2. Qubit an:

$$CNOT|\xi e> \rightarrow \frac{\alpha|000> +\alpha|011> +\beta|110> +\beta|101>}{\sqrt{2}}$$

2. Alice wendet nun auf das 1. Qubit den Hadamard Operator an:

$$\frac{\alpha\frac{|0>+|1>}{\sqrt{2}}|00> +\alpha\frac{|0>+|1>}{\sqrt{2}}|11> +\beta\frac{|0>-|1>}{\sqrt{2}}|10> +\beta\frac{|0>-|1>}{\sqrt{2}}|01>}{\sqrt{2}}$$

$$= \frac{1}{2}(|00>(\alpha|0> +\beta|1>)+|01>(\alpha|1> +\beta|0>)+|10>(\alpha|0> -\beta$$

Teleportation eines Qubits

1. Alice wendet CNOT auf das 1. Qubit und 2. Qubit an:

$$CNOT|\xi e> \rightarrow \frac{\alpha|000> +\alpha|011> +\beta|110> +\beta|101>}{\sqrt{2}}$$

2. Alice wendet nun auf das 1. Qubit den Hadamard Operator an:

$$\frac{\alpha\frac{|0>+|1>}{\sqrt{2}}|00> +\alpha\frac{|0>+|1>}{\sqrt{2}}|11> +\beta\frac{|0>-|1>}{\sqrt{2}}|10> +\beta\frac{|0>-|1>}{\sqrt{2}}|01>}{\sqrt{2}}$$

$$= \frac{1}{2}(|00>(\alpha|0> +\beta|1>)+|01>(\alpha|1> +\beta|0>)+|10>(\alpha|0> -\beta$$

3. Alice misst die ersten beiden Qubits.

Qubit	Zustand nach Messung
$\|00>$	$\|00>(\alpha\|0> +\beta\|1>$
$\|01>$	$\|01>(\alpha\|1> +\beta\|0>$
$\|10>$	$\|10>(\alpha\|0> -\beta\|1>$
$\|11>$	$\|11>(\alpha\|1> -\beta\|0>$

Teleportation eines Qubits

Abhängig von Messergebnis führt Bob folgende Operation aus:

- $|00>$: Bobs Qubit ist bereits im gewünschten Zustand.
- $|01>$: NOT Operation: NOT $\alpha|1> + \beta|0> \longrightarrow \alpha|0> + \beta|1>$.
- $|10>$: Flip Operation: FLIP $\alpha|0> - \beta|1> \longrightarrow \alpha|0> + \beta|1>$.
- $|11>$: Flip $\circ$ NOT: FLIPNOT $\alpha|1> - \beta|0> \longrightarrow \alpha|0> + \beta|1>$.

Teleportation eines Qubits

Abhängig von Messergebnis führt Bob folgende Operation aus:

- $|00>$: Bobs Qubit ist bereits im gewünschten Zustand.
- $|01>$: NOT Operation: NOT $\alpha|1> + \beta|0> \longrightarrow \alpha|0> + \beta|1>$.
- $|10>$: Flip Operation: FLIP $\alpha|0> - \beta|1> \longrightarrow \alpha|0> + \beta|1>$.
- $|11>$: Flip $\circ$ NOT: FLIPNOT $\alpha|1> - \beta|0> \longrightarrow \alpha|0> + \beta|1>$.

Beobachtung: Alices Zustand $|\xi>$ wird nicht kopiert. Bob benötigt Alices Messung, um $|\xi>$ zu erhalten.

Vor- und Nachteile der Kommunikation mit Qubits

Vorteile:

- Wenn der Sender nur $|0\rangle$, $|1\rangle$ sendet und der Empfänger nur zur Standardbasis misst, gilt die klassische Theorie.
- Es gibt mittlerweile mehrere Protokolle (BB84) mit nachweisbarer Sicherheit (man merkt, wenn jemand abhört).
- Es wird weniger Energie benötigt (Laser, Glasfaser, polarisierte Photonen).

Vor- und Nachteile der Kommunikation mit Qubits

Vorteile:

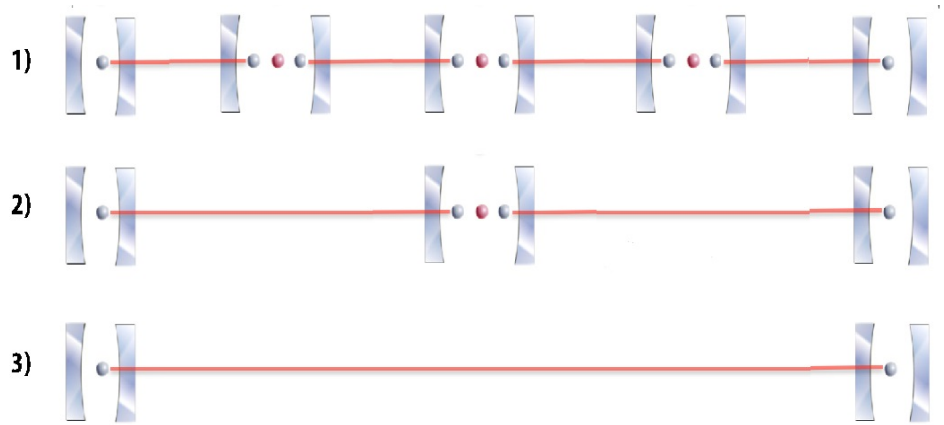
- Wenn der Sender nur $|0\rangle$, $|1\rangle$ sendet und der Empfänger nur zur Standardbasis misst, gilt die klassische Theorie.
- Es gibt mittlerweile mehrere Protokolle (BB84) mit nachweisbarer Sicherheit (man merkt, wenn jemand abhört).
- Es wird weniger Energie benötigt (Laser, Glasfaser, polarisierte Photonen).

Nachteile:

- Praktische Kommunikation nur von Punkt zu Punkt realisiert.
- Aufgrund des NoCloning Theorems gibt es keinen Verstärker.
- Die Kommunikation ist auf ca. 200 km via Glasfaser beschränkt.

Ansatz zur Lösung des Entfernungsproblems

Der Quantenrepeater



Forschung in Deutschland (BMBF)

- **Verbundprojekt Quantenkommunikation (2010-2013)**
  Projektpartner erforschten die notwendigen Komponenten eines zukünftigen Quantenrepeaters auf der Basis von Methoden und Systemen der Quantenoptik und der Halbleiterphysik.

Forschung in Deutschland (BMBF)

- **Verbundprojekt Quantenkommunikation (2010-2013)** Projektpartner erforschten die notwendigen Komponenten eines zukünftigen Quantenrepeaters auf der Basis von Methoden und Systemen der Quantenoptik und der Halbleiterphysik.
- **Q.com Projekt (2014-2018)** Mit diesem Projekt wurden die Quantentechnologien weiter an die Verwertung herangeführt.

Forschung in Deutschland (BMBF)

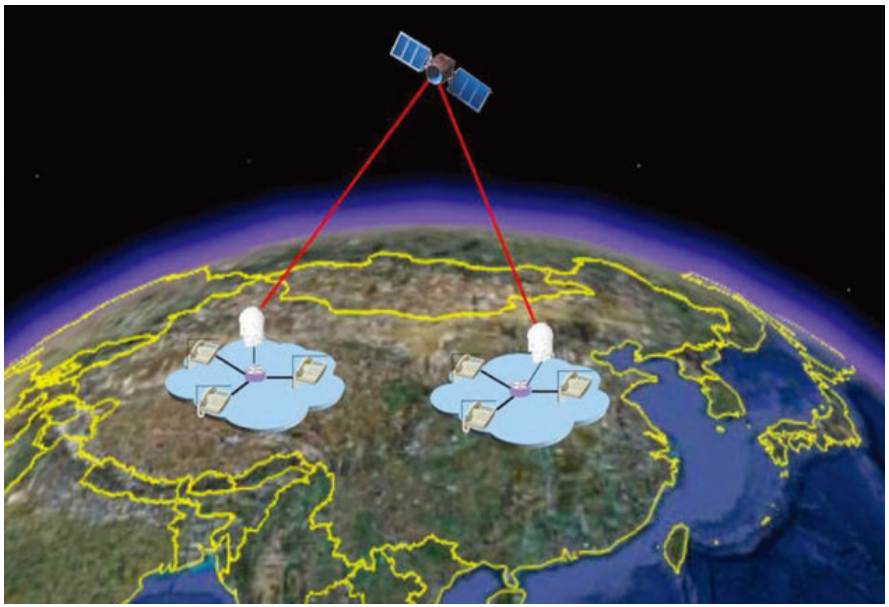
- **Verbundprojekt Quantenkommunikation (2010-2013)** Projektpartner erforschten die notwendigen Komponenten eines zukünftigen Quantenrepeaters auf der Basis von Methoden und Systemen der Quantenoptik und der Halbleiterphysik.
- **Q.com Projekt (2014-2018)** Mit diesem Projekt wurden die Quantentechnologien weiter an die Verwertung herangeführt.
- **Q.link.X Projekt (beantragt von 2018-2021)** Der geplante Q.Link.X-Verbund schlägt vor, drei Systeme zur faserbasierten Quantenschlüsselverteilung (Quantum Key Distribution, QKD) mittels Quantenrepeatern mit komplementären wissenschaftlich-technischen Ansätzen aufzubauen.

Forschung in China

- **2016** China hat den weltweit ersten Quanten-Satelliten (Micius) ins All geschickt, der abhörsichere Kommunikation und Datenübertragung ermöglichen soll.

Forschung in China

- **2016** China hat den weltweit ersten Quanten-Satelliten (Micius) ins All geschickt, der abhörsichere Kommunikation und Datenübertragung ermöglichen soll.
- **2017** Chinesische Wissenschaftler haben sogenannte verschränkte Photonen über eine Rekorddistanz von 1200 Kilometer verteilt.



Forschung in China

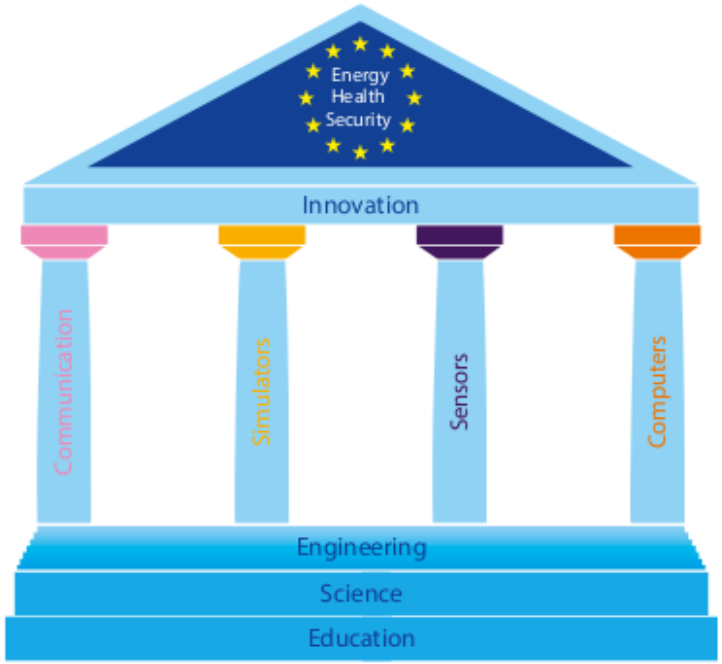
China stellt die längste hochsichere Quantenkommunikationsleitung der Welt vor

Achtung: Trusted Nodes !!

Forschung in Europa

2017: EU verkündet Flagship-Initative mit 1 Milliarde Euro für Quantentechnologie

Auf der Quantum Europe Conference im Mai wurde verkündet, dass die Europäische Kommission eine neue Initiative zur Förderung von Quantentechnologien im Rahmen des Programms Future and Emerging Technologies (FET) ins Leben ruft.



Elements of a European programme in quantum technologies.


Geschafft
Vielen Dank für Ihre Aufmerksamkeit
MEME-GENERATOR.DE