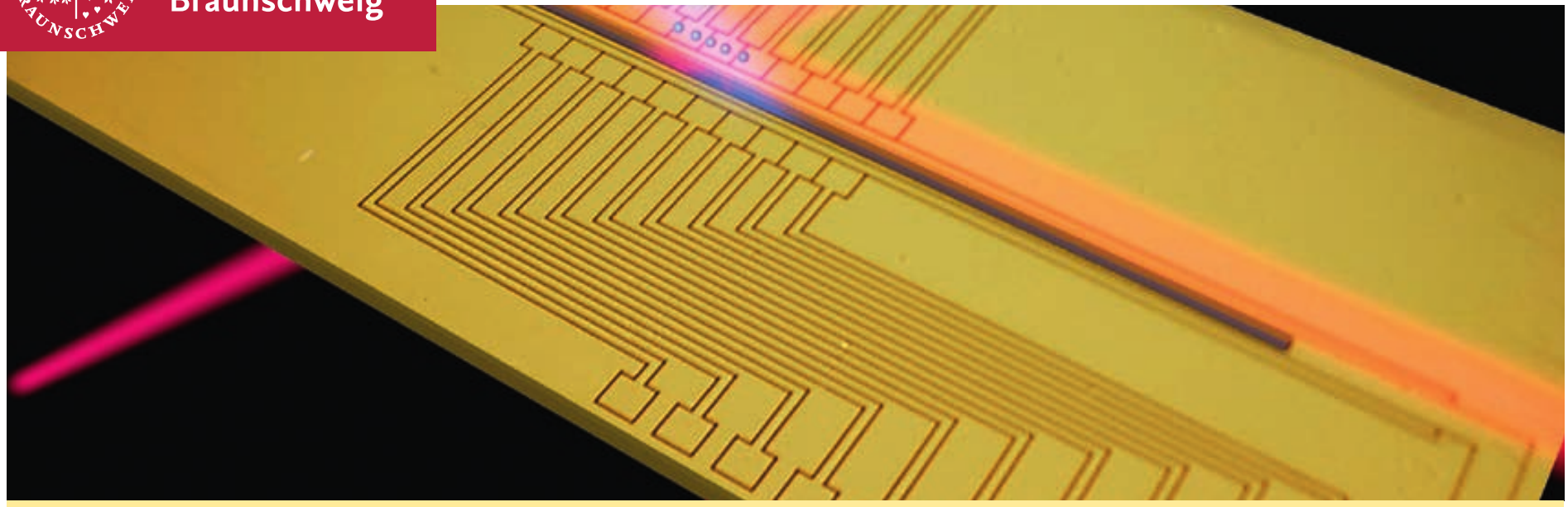


Quanteninformation und mögliche Anwendungen in der Kommunikationstechnik

David Hellmers, 14. Juni 2016

Übersicht

- **Motivation**
- **Quanteninformatik**
  - Qubits
  - Quanten-Gates
- **Quantenkommunikation**
  - Quantenkanal
  - Quantenkryptographie
- **Fazit**

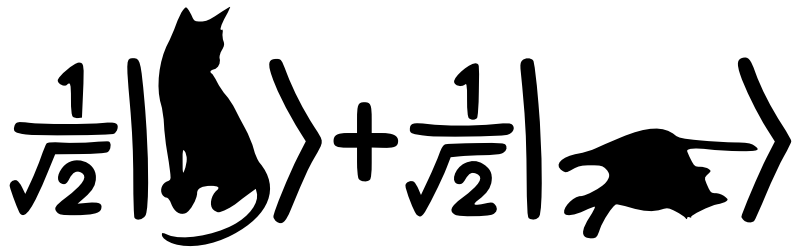
Übersicht

- **Motivation**
- **Quanteninformatik**
  - Qubits
  - Quanten-Gates
- **Quantenkommunikation**
  - Quantenkanal
  - Quantenkryptographie
- **Fazit**

Die Idee der Quanteninformatik

Computer mit quantenphysikalischen Eigenschaften:

- Superposition (Schrödingers Katze)
- Verschränkung



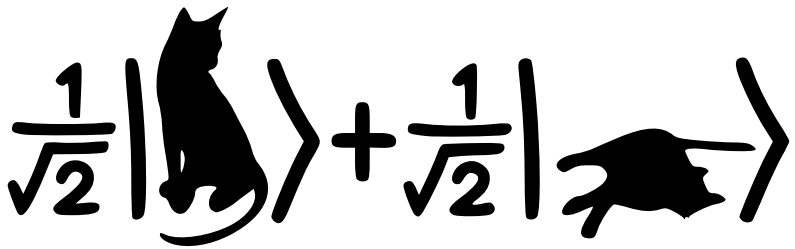
Die Idee der Quanteninformatik

Computer mit quantenphysikalischen Eigenschaften:

- Superposition (Schrödingers Katze)
- Verschränkung

Dadurch können Quantencomputer:

- Laufzeit klassischer Algorithmen bis zu exponentiell verbessern
- Lauschangriffe auf einen Kommunikationskanal erkennen



Aktuelle Forschung

In den letzten Jahren ist viel passiert, allein im Jahr 2016:

Aktuelle Forschung

In den letzten Jahren ist viel passiert, allein im Jahr 2016:

- Die ersten programmierbaren (universellen) Quantencomputer

Aktuelle Forschung

In den letzten Jahren ist viel passiert, allein im Jahr 2016:

- Die ersten programmierbaren (universellen) Quantencomputer
- IBM stellt Quantencomputer zur Verfügung

Aktuelle Forschung

In den letzten Jahren ist viel passiert, allein im Jahr 2016:

- Die ersten programmierbaren (universellen) Quantencomputer
- IBM stellt Quantencomputer zur Verfügung
- EU hat Forschungspaket für Quantencomputer vorgestellt

Übersicht

- Motivation
- **Quanteninformatik**
  - Qubits
  - Quanten-Gates
- Quantenkommunikation
  - Quantenkanal
  - Quantenkryptographie
- Fazit

Vom Bit zum Qubit

Klassische Informatik:
Bit ist 0 oder 1

Vom Bit zum Qubit

Klassische Informatik:
Bit ist 0 oder 1

Quanteninformatik:
$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ und $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

$|\psi\rangle$ heißt *Ket*.

Spin und Superposition

$|0\rangle$ und $|1\rangle$ sind *reine* Zustände eines Quantenteilchens.

Beispiel Spin:
Teilchen dreht sich im ($|0\rangle$) oder gegen ($|1\rangle$) den Uhrzeigersinn.

Spin und Superposition

$|0\rangle$ und $|1\rangle$ sind *reine* Zustände eines Quantenteilchens.

Beispiel Spin:
Teilchen dreht sich im ($|0\rangle$) oder gegen ($|1\rangle$) den Uhrzeigersinn.

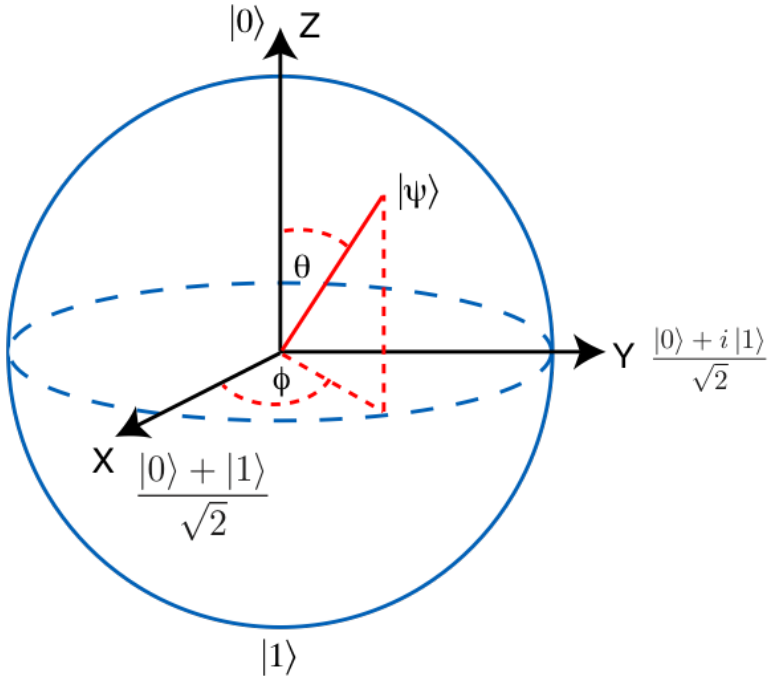
Superposition $\rightarrow$ beides gleichzeitig (Schrödingers Katze).

$$|\psi\rangle = \begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = c_0 \cdot |0\rangle + c_1 \cdot |1\rangle \text{ mit } c_0, c_1 \in \mathbb{C}$$

Definition Qubit

Qubit ist normalisierter Ket $|\psi\rangle$:

$$||\psi\rangle| = |c_0|^2 + |c_1|^2 = 1$$

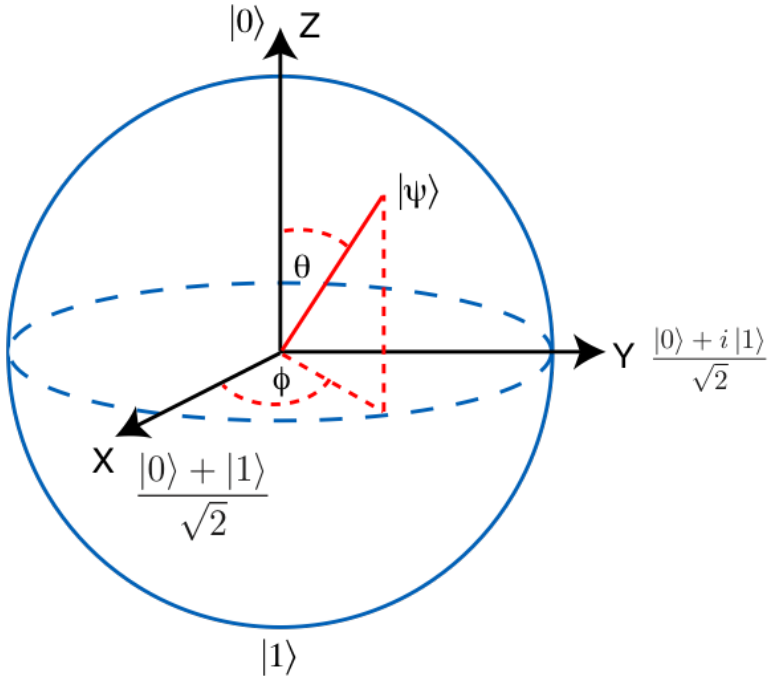


Definition Qubit

Qubit ist normalisierter Ket $|\psi\rangle$:

$$||\psi\rangle| = |c_0|^2 + |c_1|^2 = 1$$

$|c_0|^2$ und $|c_1|^2$ ist Wahrscheinlichkeit $|0\rangle$ bzw. $|1\rangle$ zu messen.



Systeme mit mehreren Qubits

Kombination von Qubits mit dem Tensorprodukt:

Systeme mit mehreren Qubits

Kombination von Qubits mit dem Tensorprodukt:

$$|0\rangle \otimes |1\rangle = |01\rangle = \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix}^T = 0 \cdot |00\rangle + 1 \cdot |01\rangle + 0 \cdot |10\rangle + 0 \cdot |11\rangle .$$

Beispiel: 2 Qubits

$$|00\rangle = \begin{matrix} \mathbf{00} \\ \mathbf{01} \\ \mathbf{10} \\ \mathbf{11} \end{matrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad |01\rangle = \begin{matrix} \mathbf{00} \\ \mathbf{01} \\ \mathbf{10} \\ \mathbf{11} \end{matrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad |10\rangle = \begin{matrix} \mathbf{00} \\ \mathbf{01} \\ \mathbf{10} \\ \mathbf{11} \end{matrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad |11\rangle = \begin{matrix} \mathbf{00} \\ \mathbf{01} \\ \mathbf{10} \\ \mathbf{11} \end{matrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

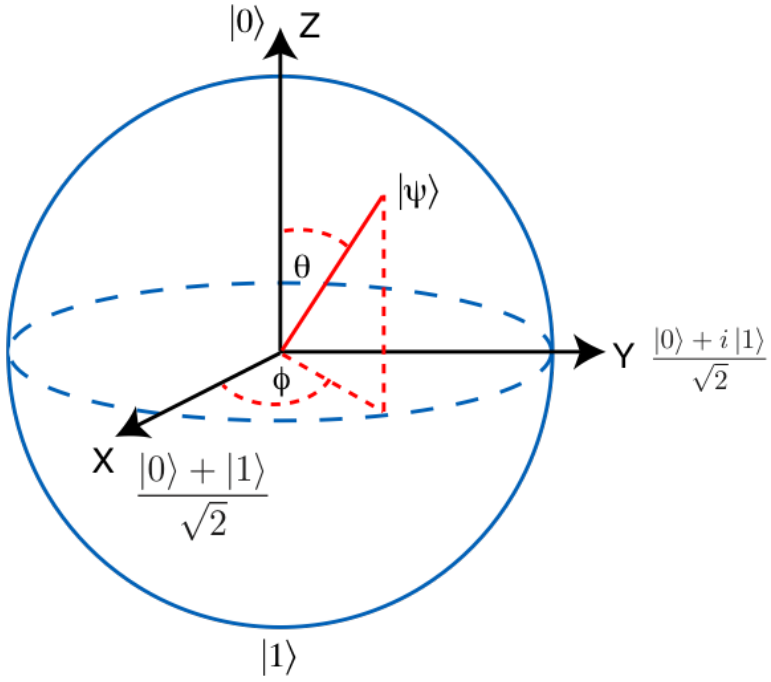
Übersicht

- Motivation
- **Quanteninformatik**
  - Qubits
  - Quanten-Gates
- Quantenkommunikation
  - Quantenkanal
  - Quantenkryptographie
- Fazit

Bloch-Kugel

Darstellung eines Qubits:

Quanten-Gates sind Rotations-matrizen auf der Bloch-Kugel.



Bloch-Kugel

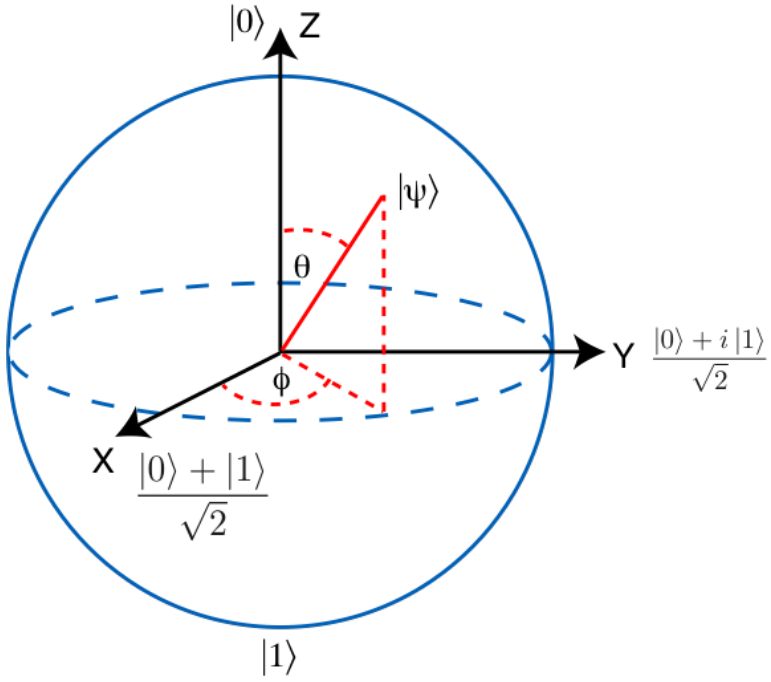
Darstellung eines Qubits:

Quanten-Gates sind Rotationsmatrizen auf der Bloch-Kugel.

Jedes Quanten-Gate muss umkehrbar sein.

Klassisches AND geht nicht!

$$AND = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$



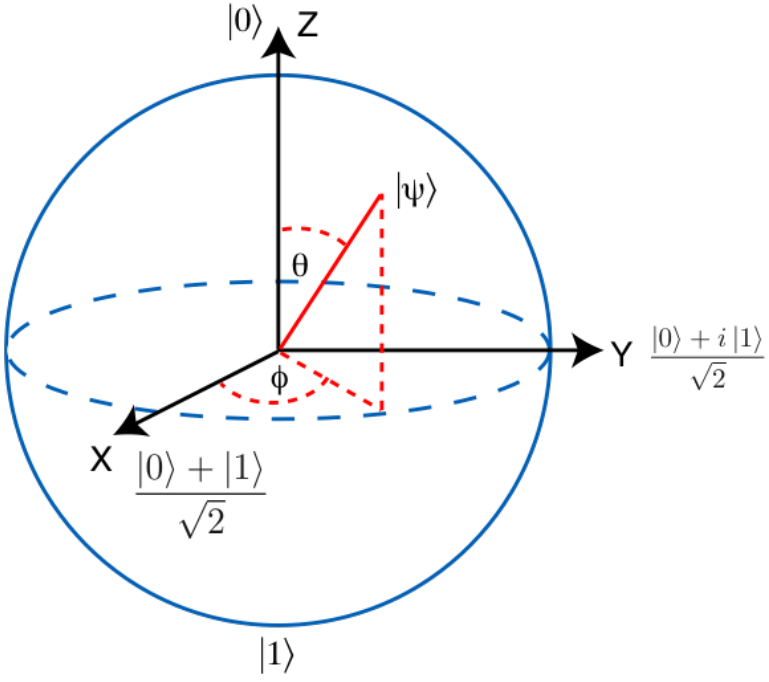
Pauli-Gates

Pauli-Gates rotieren Bloch-Kugel um eine Achse

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

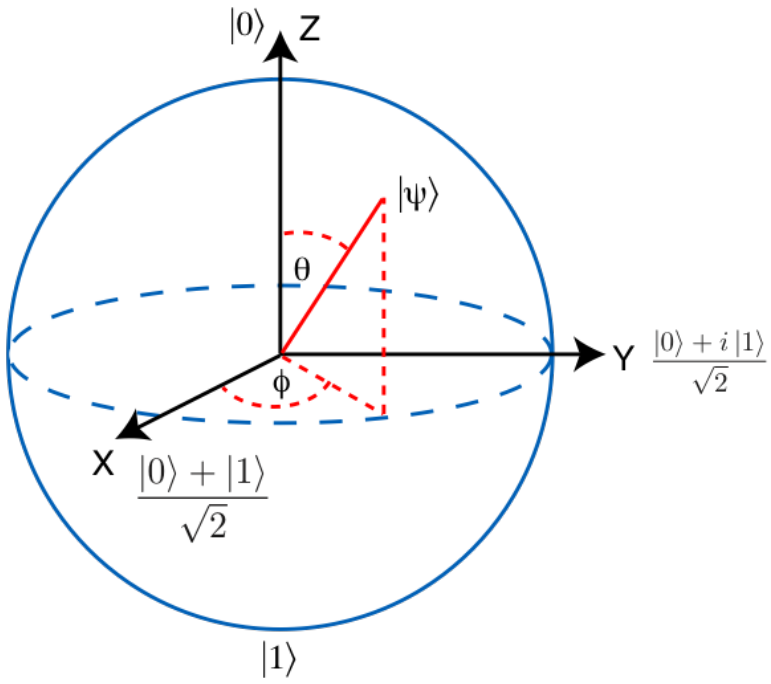
$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



Hadamard-Gate

Hadamard erzeugt gleichverteilte Superposition

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$



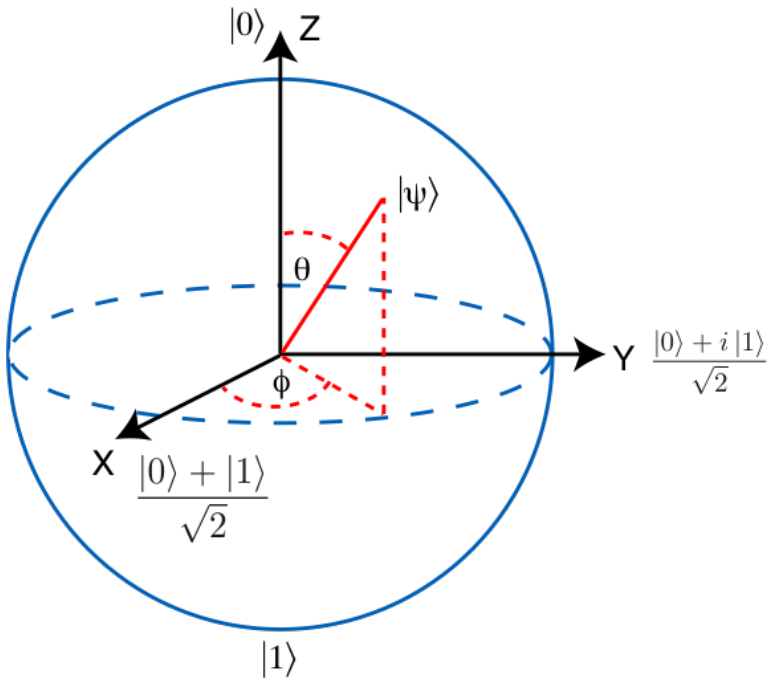
Hadamard-Gate

Hadamard erzeugt gleichverteilte Superposition

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H \cdot |0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$H \cdot |1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

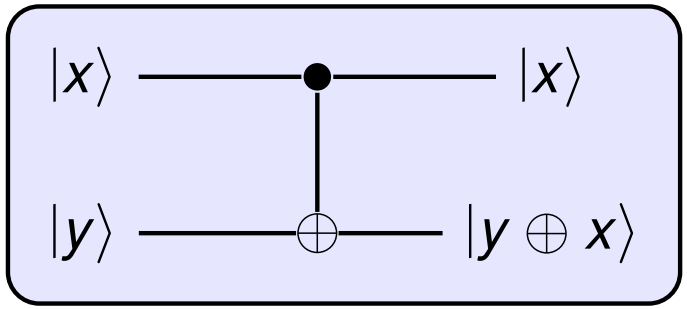


CNOT-Gate (Controlled-NOT)

CNOT ist 2-Qubit Operation.

Oberer Input $|x\rangle$ unverändert.
Unterer Input $|y\rangle$ wird zu $|y \oplus x\rangle$

$$\text{C-NOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



Übersicht

- Motivation
- Quanteninformatik
  - Qubits
  - Quanten-Gates
- **Quantenkommunikation**
  - Quantenkanal
  - Quantenkryptographie
- Fazit

Quantenkanal

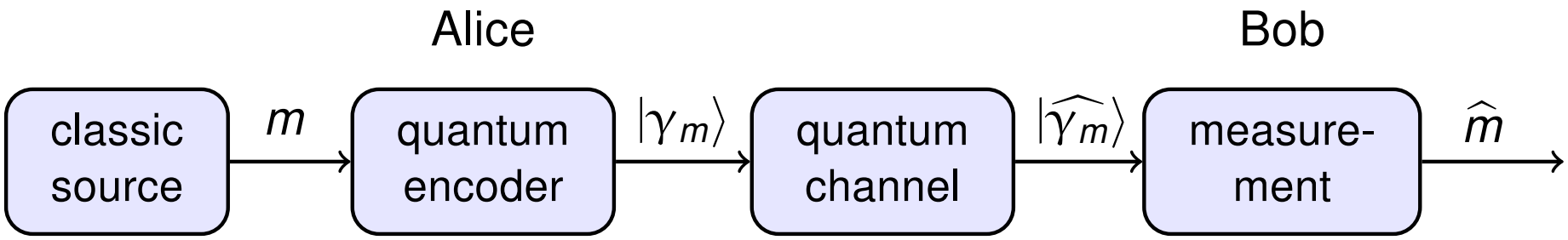


Abbildung 1 : Modell eines rauschenden Quantenkanals

Nachricht m wird in reine Zustände encoded. (z.B: $|0\rangle$ und $|1\rangle$).
Bob decoded reine Zustände, erhält modifiziertes Signal $\widehat{m}$.

Quantenkanal

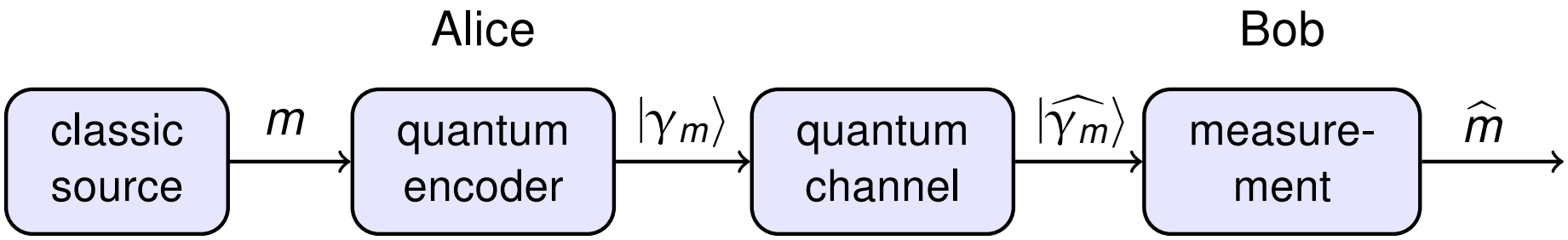


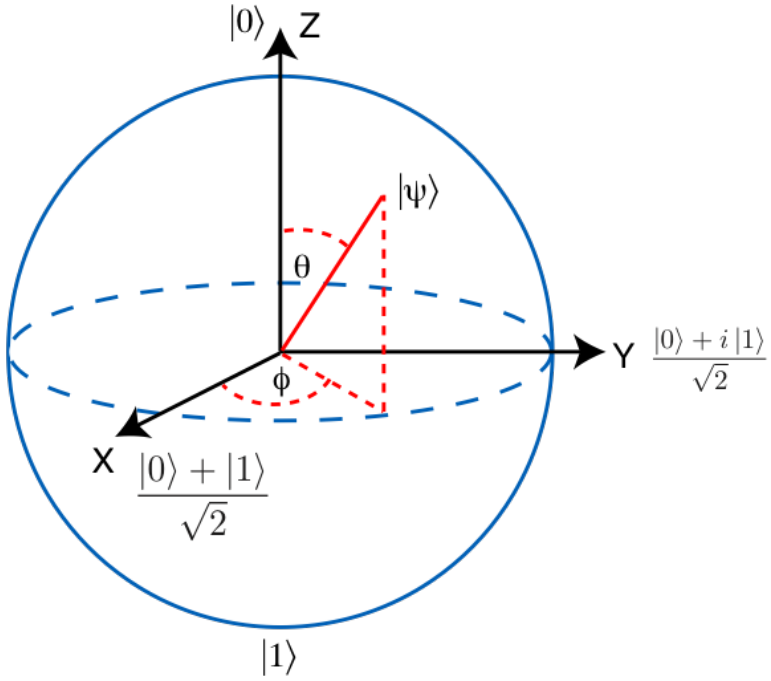
Abbildung 1 : Modell eines rauschenden Quantenkanals

Nachricht m wird in reine Zustände encoded. (z.B: $|0\rangle$ und $|1\rangle$).
Bob decoded reine Zustände, erhält modifiziertes Signal $\widehat{m}$.
Quantenzustände werden mittels Photonen verschickt.

Encoding von Nachrichten

Binäres Encoding von m:

Eine beliebige Basis in der Bloch-Kugel.

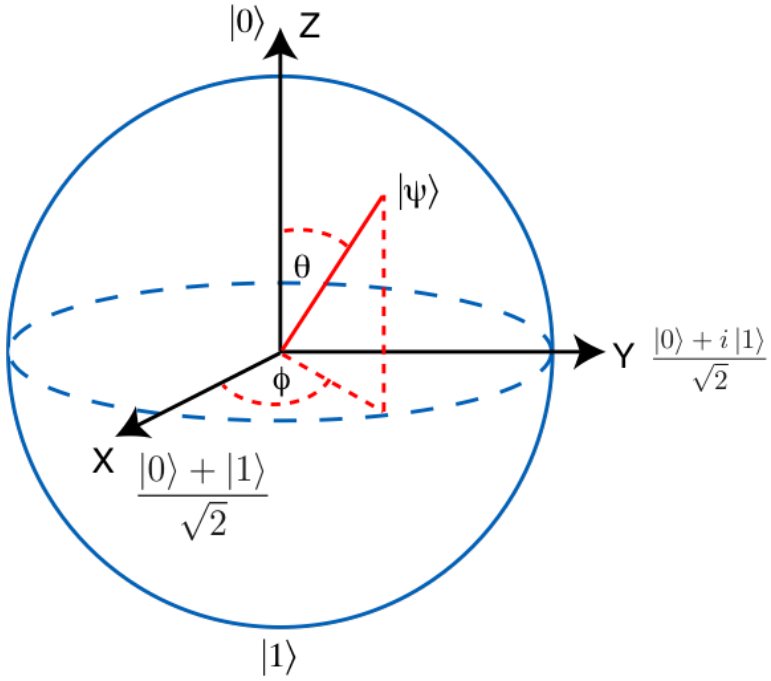


Encoding von Nachrichten

Binäres Encoding von m:

Eine beliebige Basis in der Bloch-Kugel.

Unterschiedliche Basen bei
En- und Decoding:
$\rightarrow$ großer Fehler beim Decodieren.



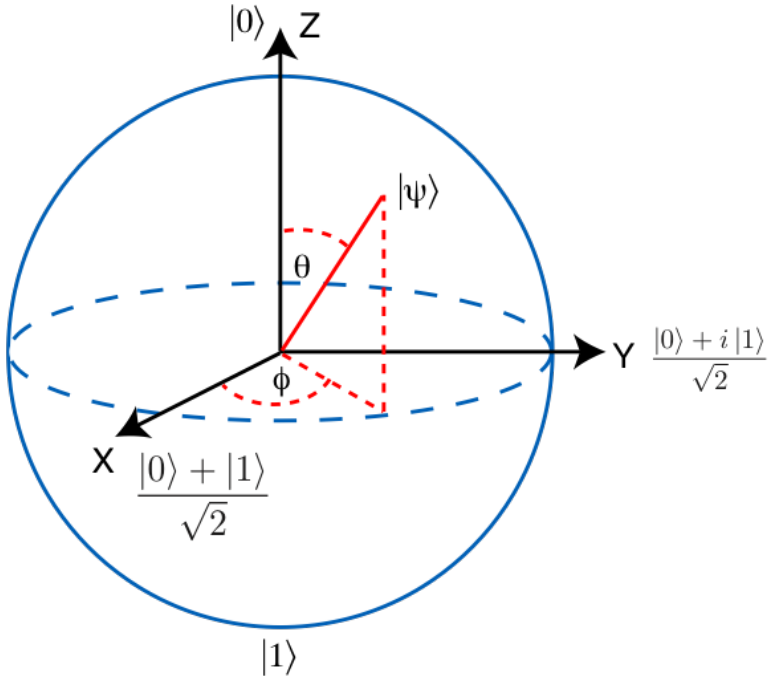
Encoding von Nachrichten

Binäres Encoding von m:

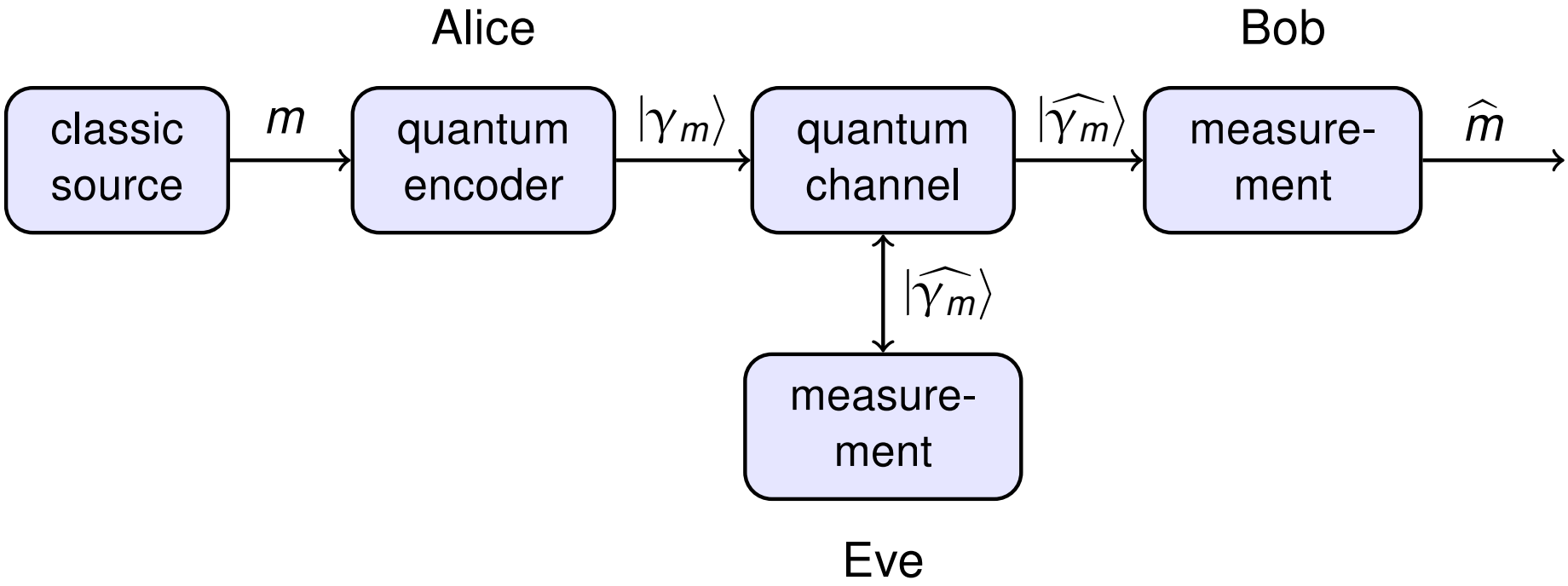
Eine beliebige Basis in der Bloch-Kugel.

Unterschiedliche Basen bei En- und Decoding:
$\rightarrow$ großer Fehler beim Decodieren.

$\Rightarrow$Erkennung von Lauschangriffen.



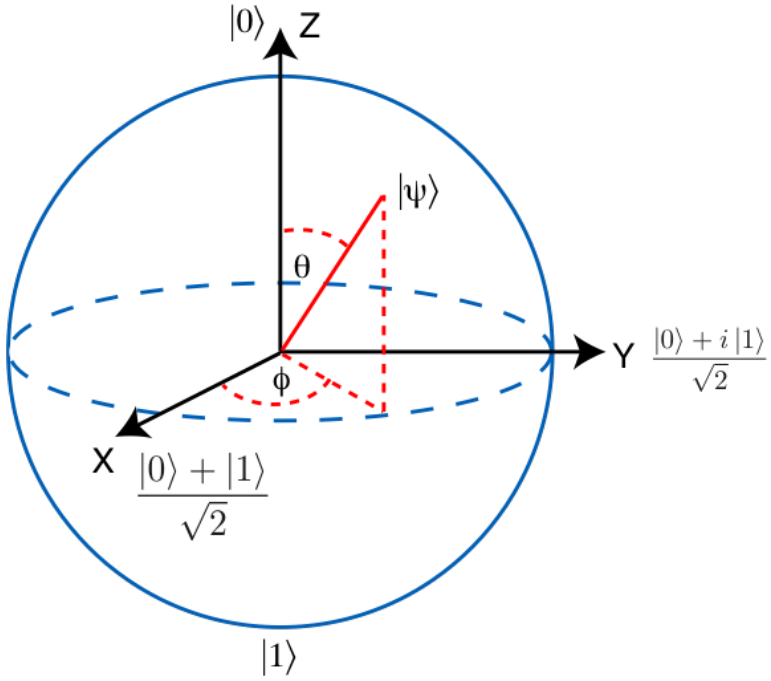
Eve im Quantenkanal



Gleiche Basis $\rightarrow$ kein Problem.

BB84 Protokoll - Konzept

Alice und Bob einigen sich auf 2 Basen.
z.B. $\{|\uparrow\rangle, |\downarrow\rangle\}$ und $\{|\leftarrow\rangle, |\rightarrow\rangle\}$

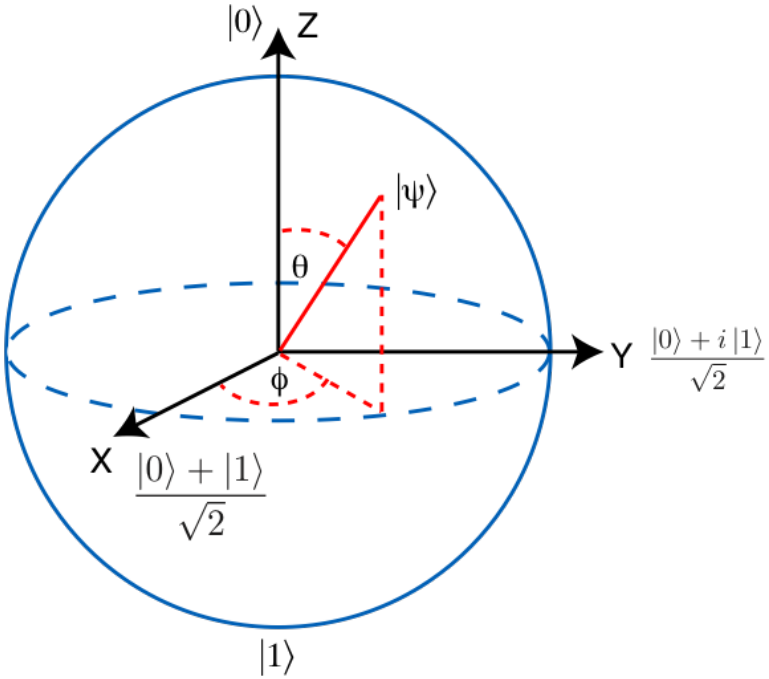


BB84 Protokoll - Konzept

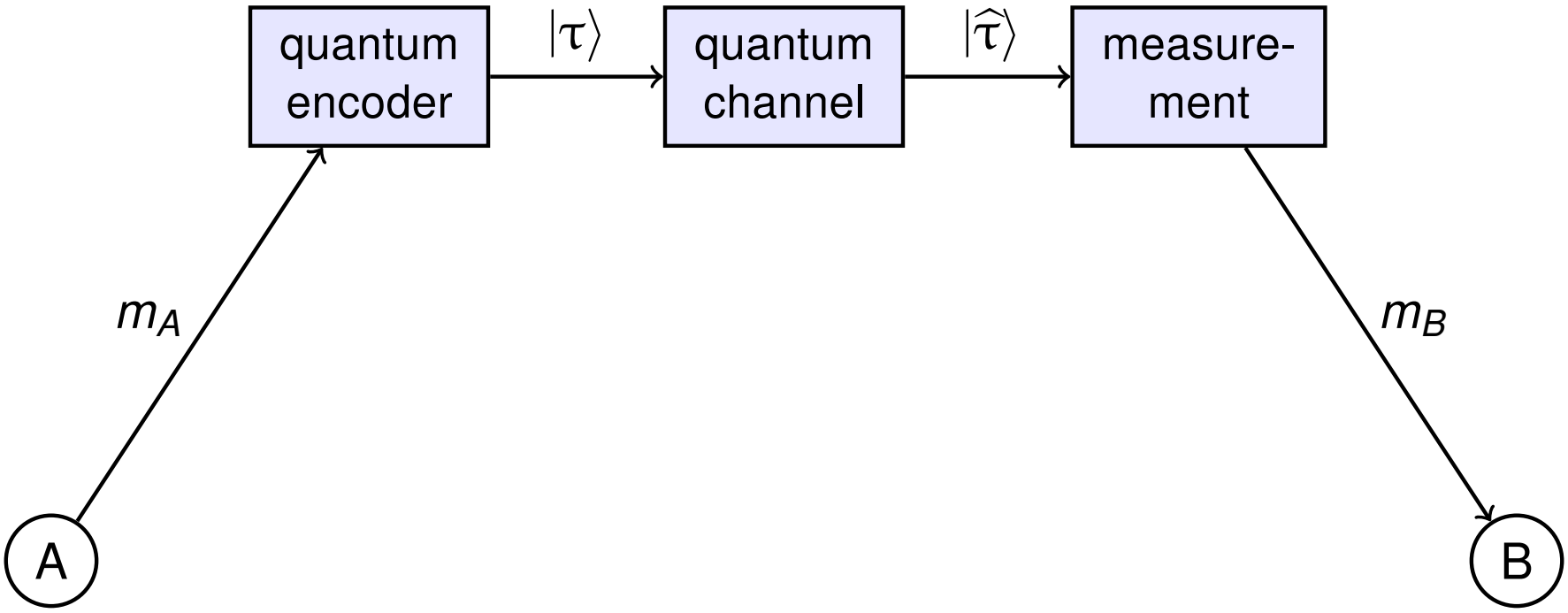
Alice und Bob einigen sich auf 2 Basen.
z.B. $\{|\uparrow\rangle, |\downarrow\rangle\}$ und $\{|\leftarrow\rangle, |\rightarrow\rangle\}$

Alice schickt zufällige Bitfolge.
Beim Encoding und Decoding für jedes Bit zufällige Basis.

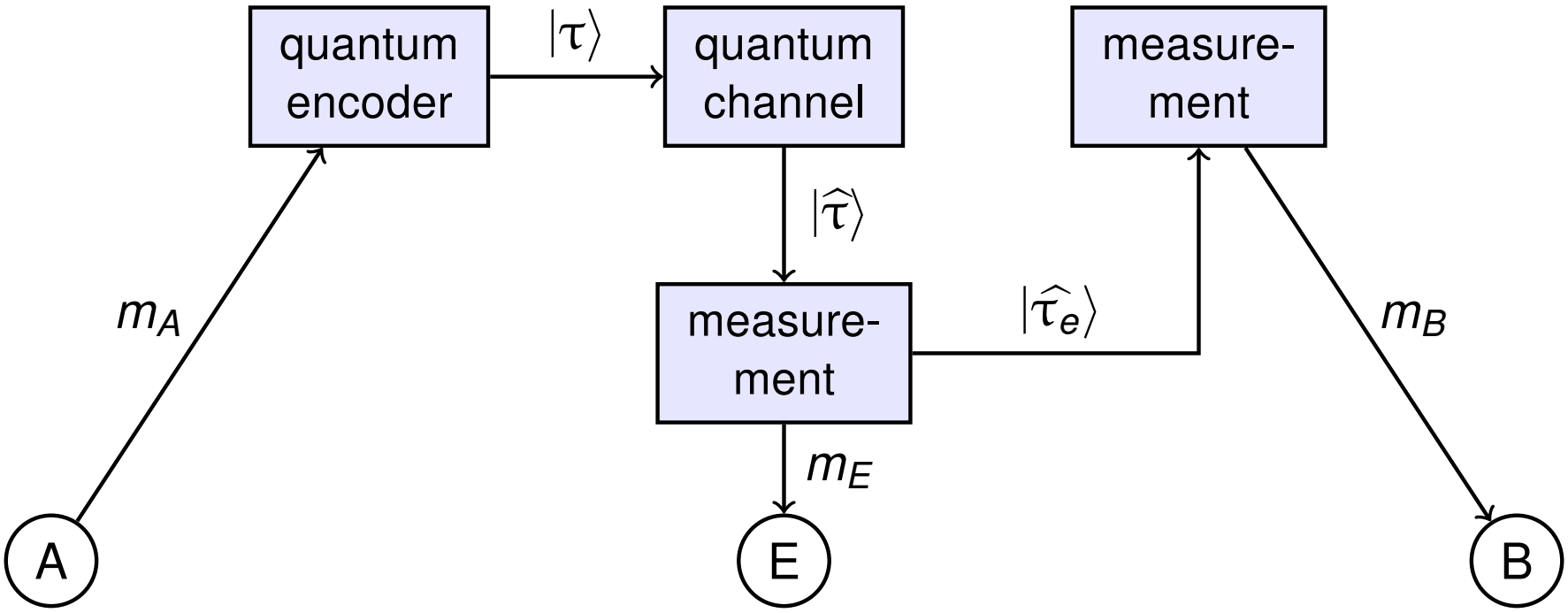
Hinterher Ergebnisse vergleichen.



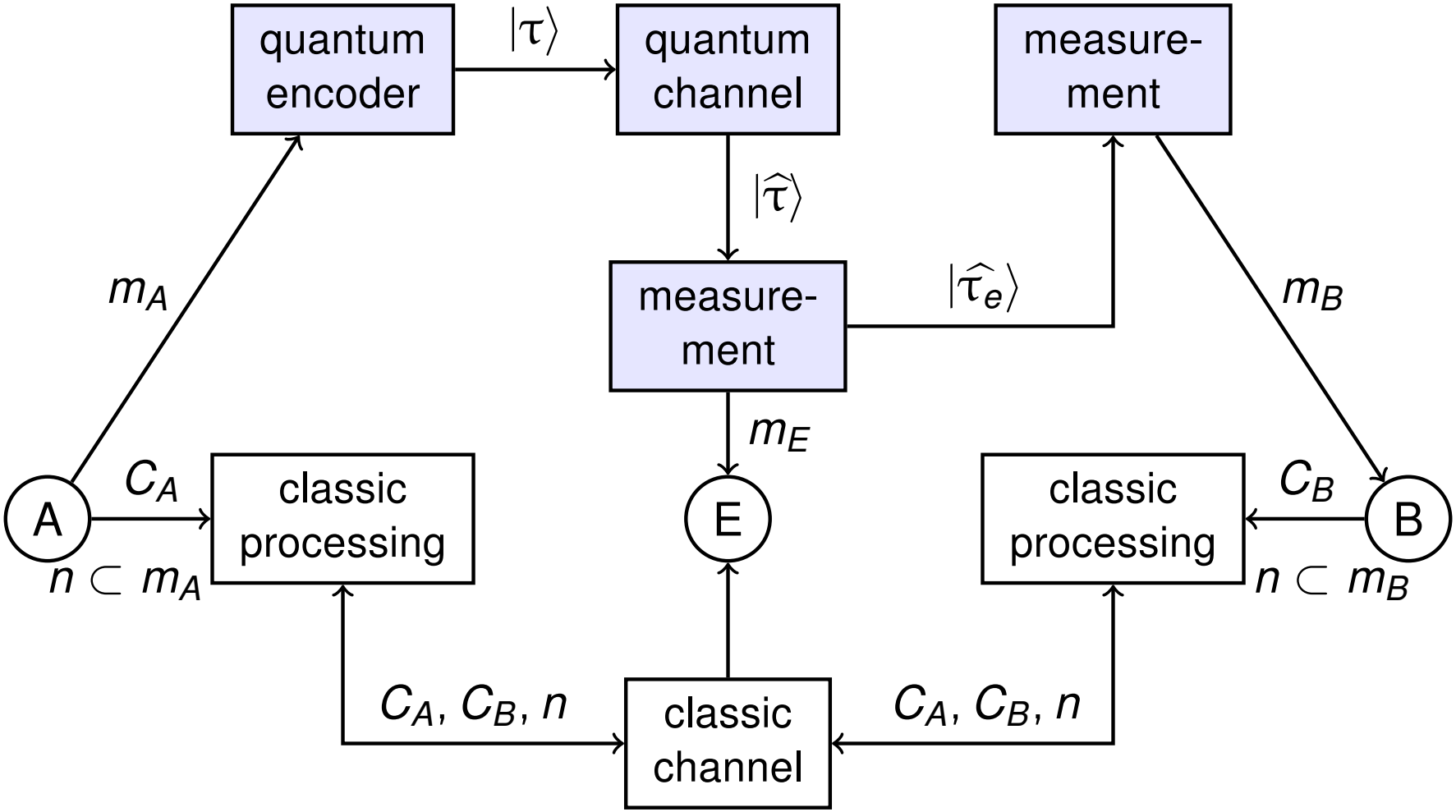
BB84 Protokoll



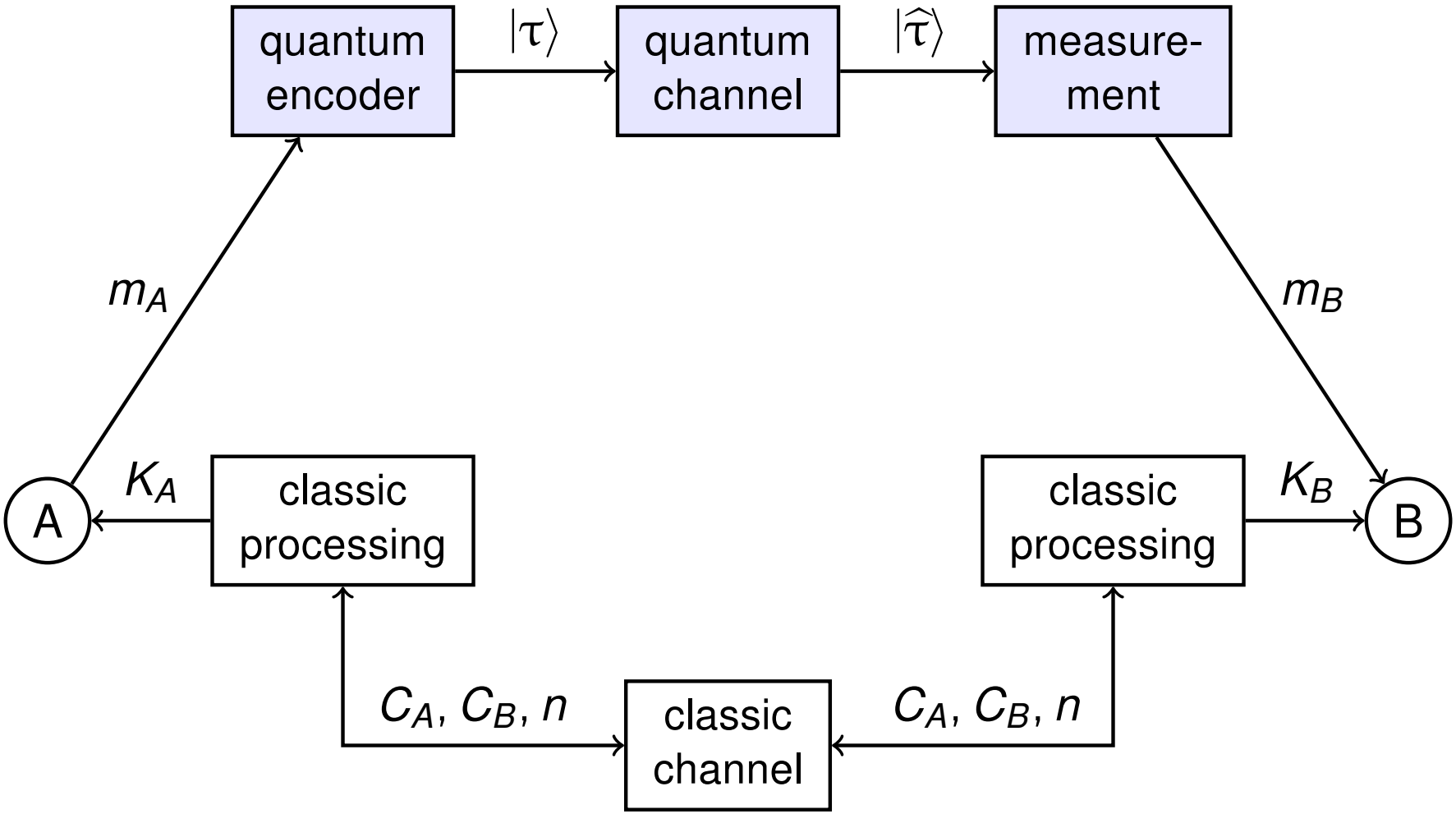
BB84 Protokoll



BB84 Protokoll



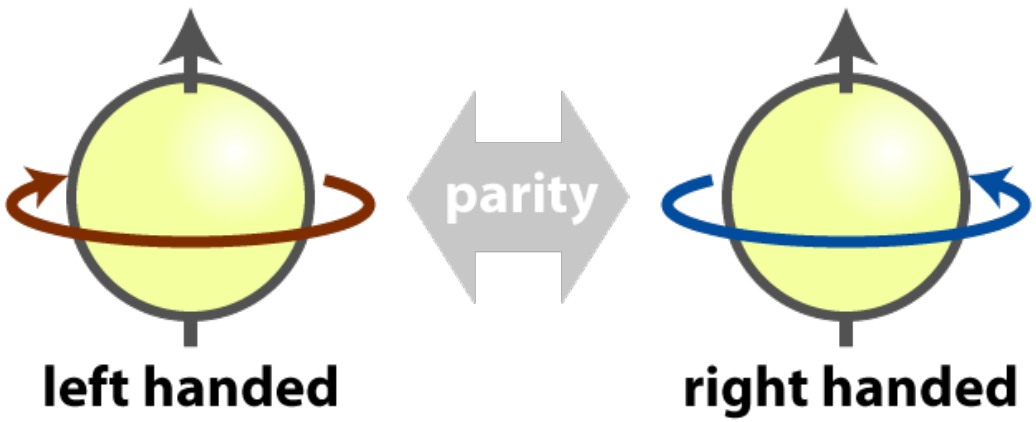
BB84 Protokoll



Exkurs: Verschränkung

Quantenzuständen können korreliert sein.

Beispiel Spin:
Ein Teilchen im, anderes gegen den Uhrzeigersinn.
$\rightarrow$ Gesamtspin 0.



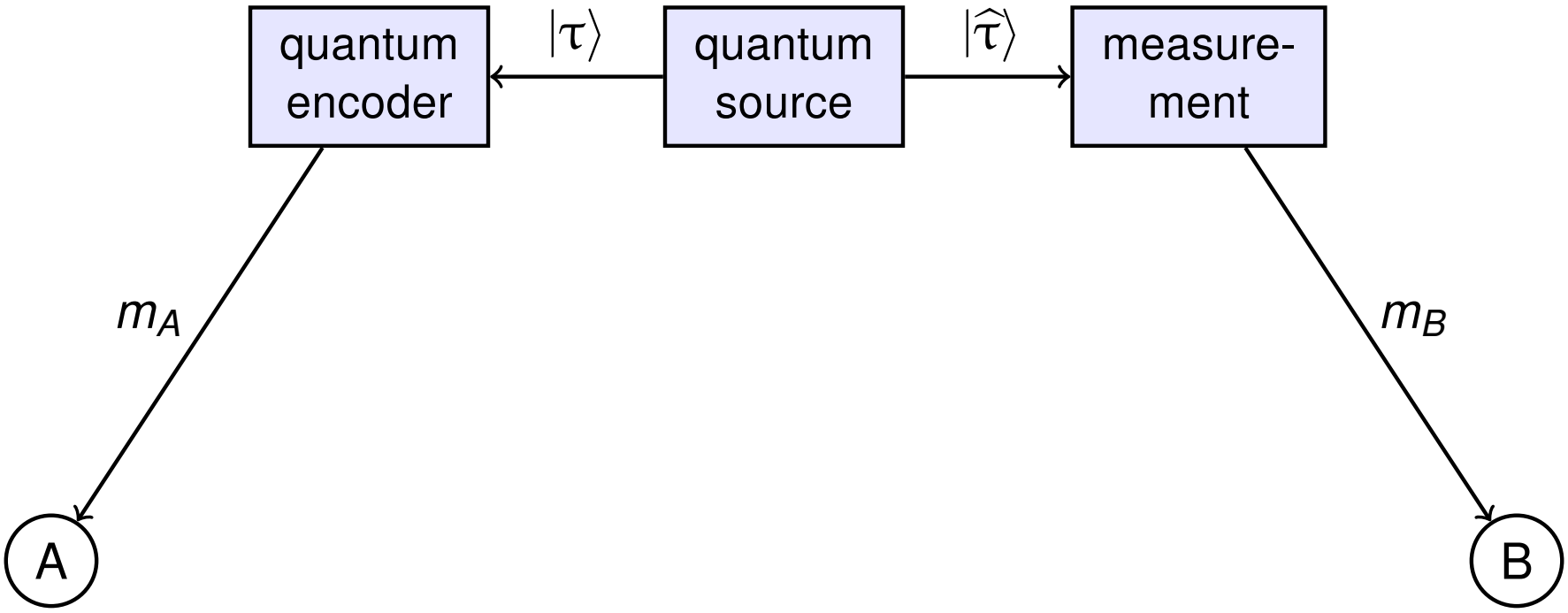
BBM92 Protokoll - Konzept

Gemeinsame Quelle von zufällig verschränkten Zuständen.

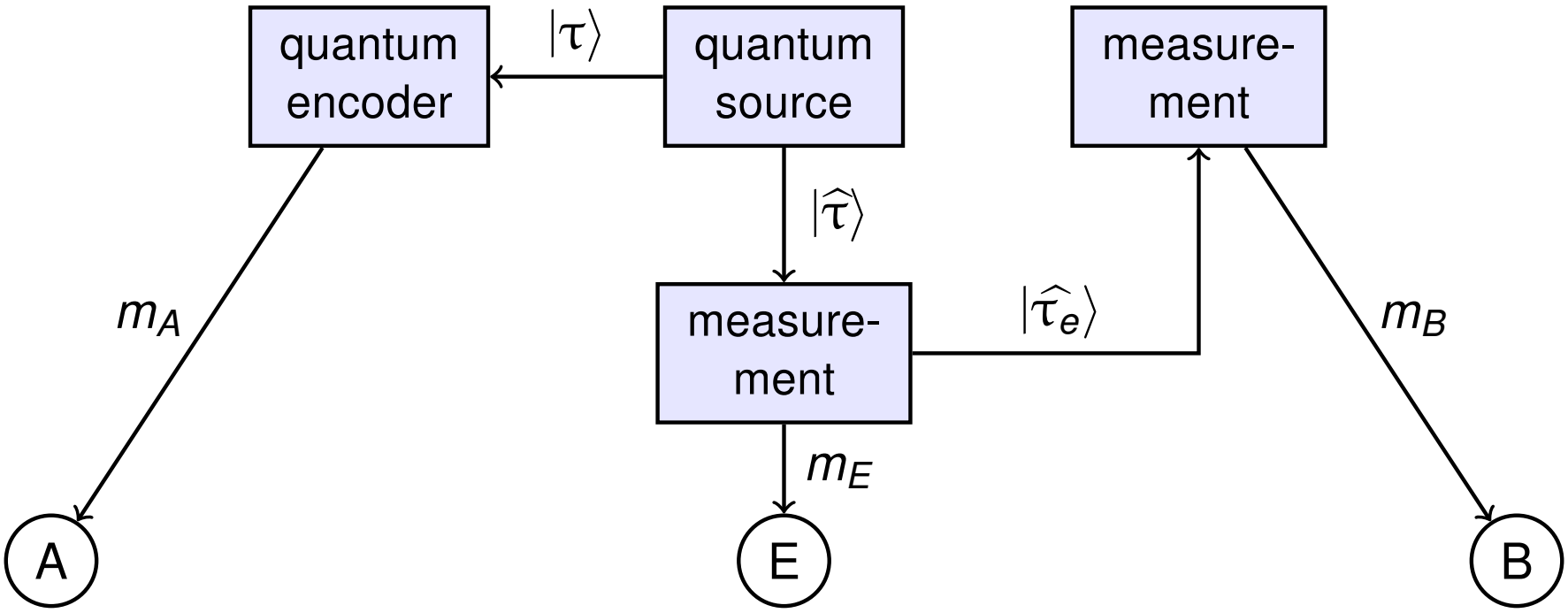
Messung hebt Verschränkung auf.
$\rightarrow$ Eve wird entdeckt.

Rest wie beim BB84.

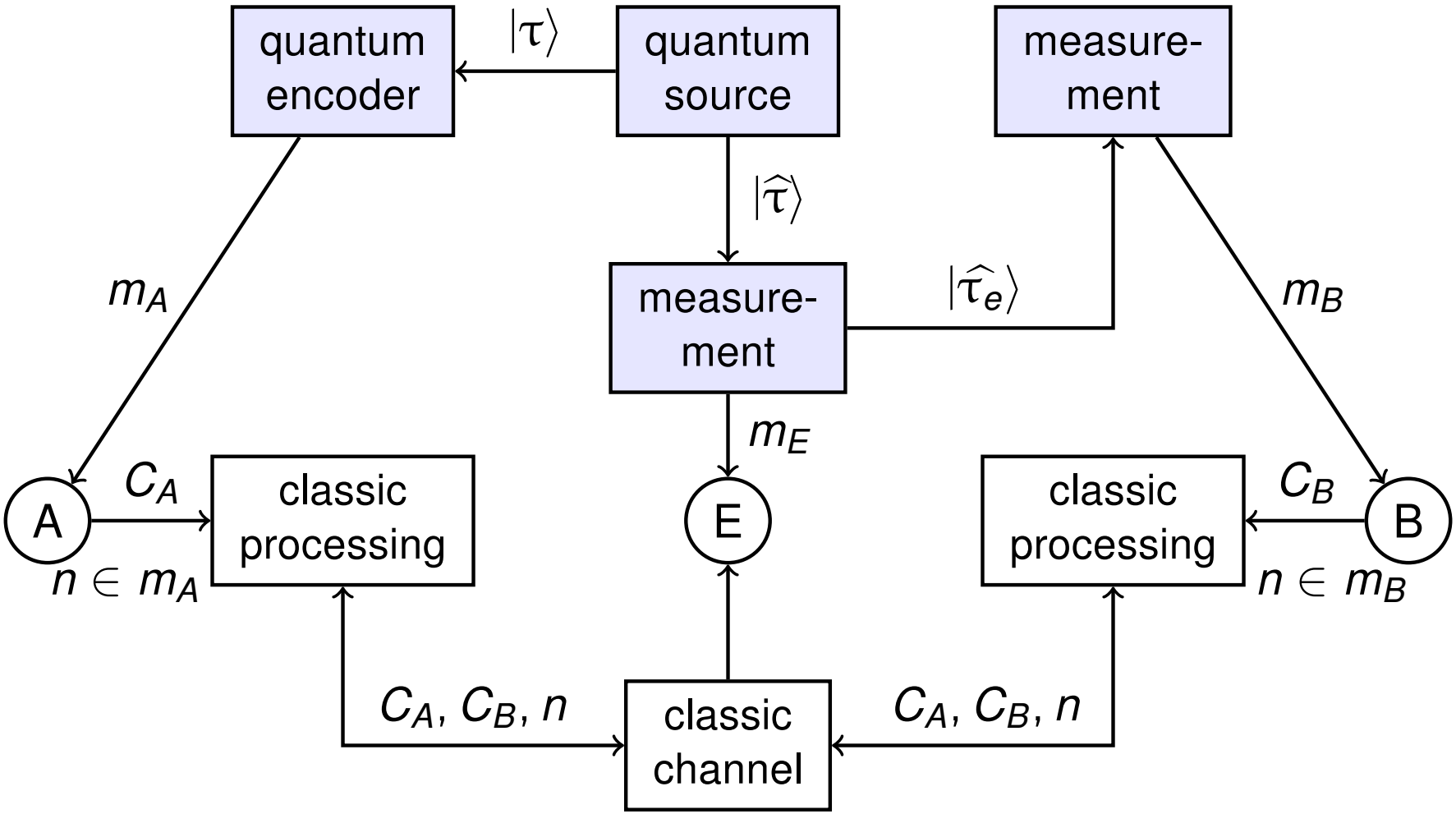
BBM92 Protokoll



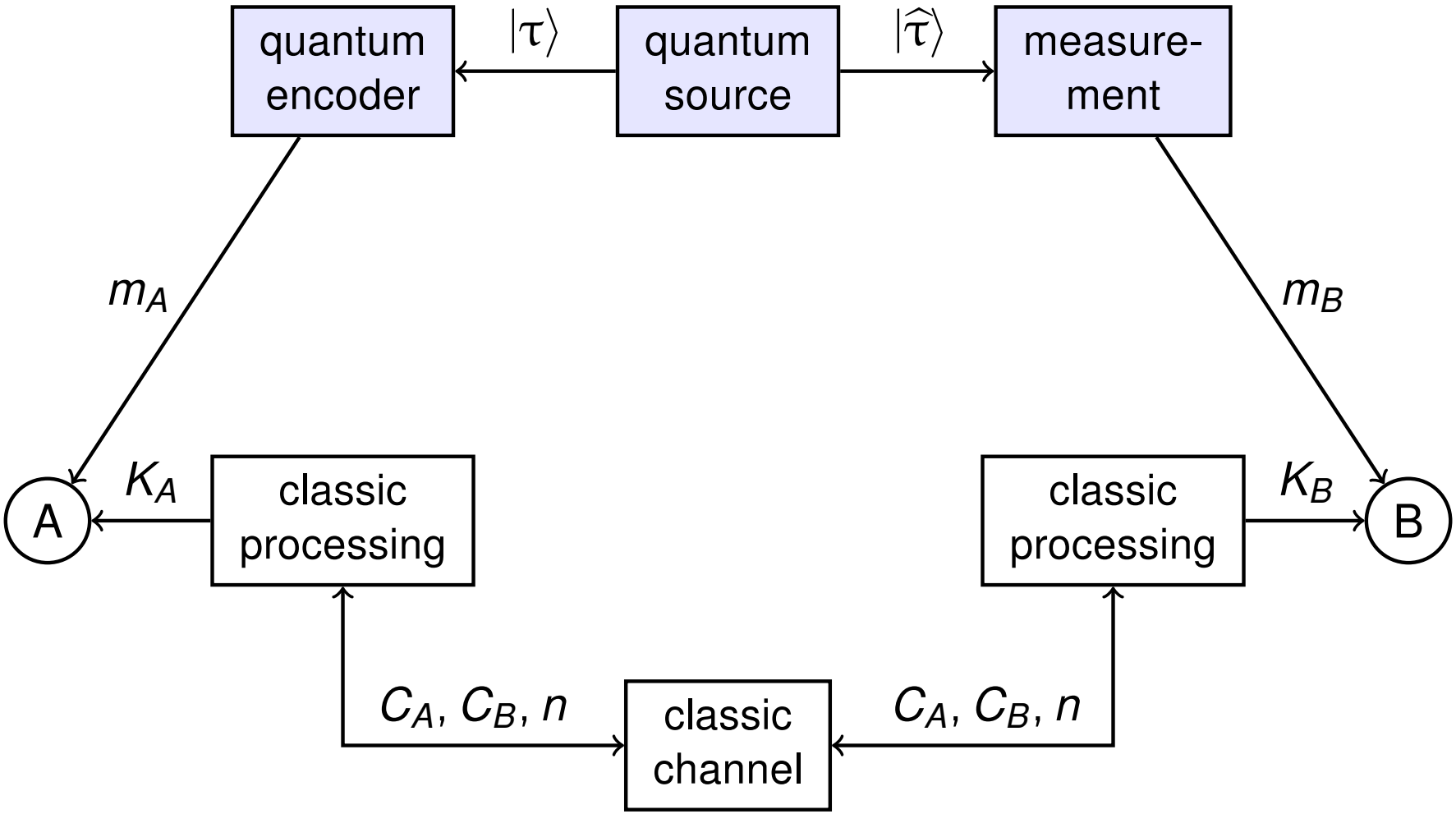
BBM92 Protokoll



BBM92 Protokoll



BBM92 Protokoll



Probleme

- klassischer Kanal
- Infrastruktur (Router, ISP, etc.)
- praktische Umsetzung

Übersicht

- Motivation
- Quanteninformatik
  - Qubits
  - Quanten-Gates
- Quantenkommunikation
  - Quantenkanal
  - Quantenkryptographie
- **Fazit**

Fazit

Quanteninformatik verspricht großen Fortschritt,

Fazit

Quanteninformatik verspricht großen Fortschritt, aber:

Technische Hürden

IBM Quantencomputer hat nur 5 Qubits

Fazit

Quanteninformatik verspricht großen Fortschritt, aber:

Technische Hürden

IBM Quantencomputer hat nur 5 Qubits

Struktur des Internets (Router, ISP) $\rightarrow$ unerwünschte Messungen

Fazit

Quanteninformatik verspricht großen Fortschritt, aber:

Technische Hürden

IBM Quantencomputer hat nur 5 Qubits

Struktur des Internets (Router, ISP) $\rightarrow$ unerwünschte Messungen

Theoretische Hürden

Bisher sehr wenig praktische Algorithmen

Fazit

Quanteninformatik verspricht großen Fortschritt, aber:

Technische Hürden
IBM Quantencomputer hat nur 5 Qubits
Struktur des Internets (Router, ISP) $\rightarrow$ unerwünschte Messungen

Theoretische Hürden
Bisher sehr wenig praktische Algorithmen
Quanteninformatik noch sehr jung (ca. 30 Jahre)

$\rightarrow$ noch viel zu erforschen!

Deutsch-Jozsa - Problemstellung

Eine Funktion $f : \{0,1\}^n \rightarrow \{0,1\}$ heißt *konstant* wenn

$$\forall x \in \{0,1\}^n : f(x) = c,\ c \in \{0,1\},$$

Deutsch-Jozsa - Problemstellung

Eine Funktion $f : \{0,1\}^n \rightarrow \{0,1\}$ heißt *konstant* wenn

$$\forall x \in \{0,1\}^n : f(x) = c,\ \ c \in \{0,1\},$$

oder balanciert wenn

$$|\{x \in \{0,1\}^n : f(x) = 0\}| = |\{y \in \{0,1\}^n : f(y) = 1\}|$$

Deutsch-Jozsa - Problemstellung

Eine Funktion $f : \{0,1\}^n \to \{0,1\}$ heißt *konstant* wenn

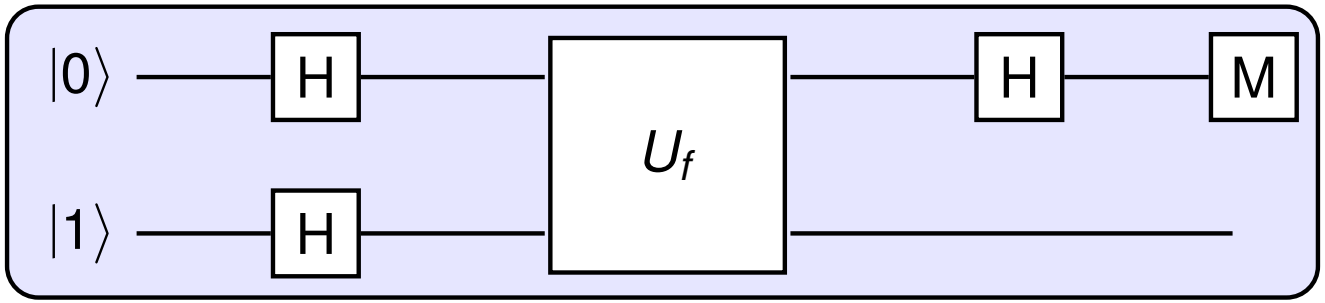
$$\forall x \in \{0,1\}^n : f(x) = c,\ c \in \{0,1\},$$

oder balanciert wenn

$$|\{x \in \{0,1\}^n : f(x) = 0\}| = |\{y \in \{0,1\}^n : f(y) = 1\}|$$

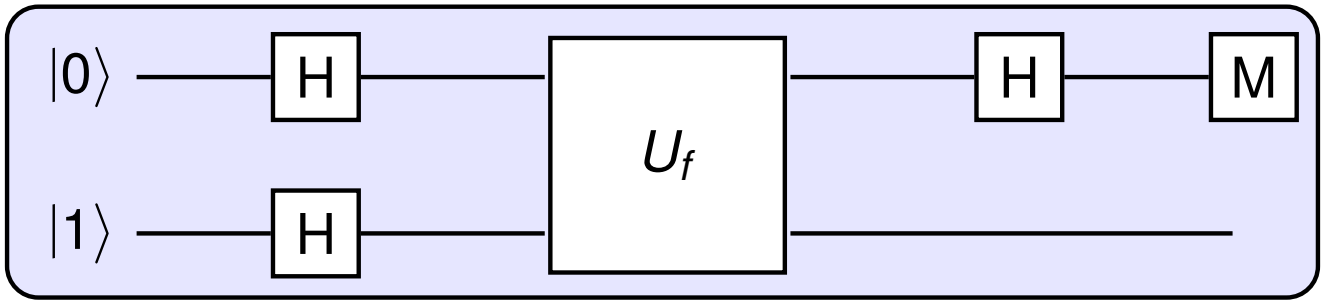
Klassische Vorgehensweise: $2^{n-1} + 1$ mal evaluieren.
Quanteninformatik: *Eine* Evaluation!

Deutsch Algorithmus



Vereinfachte Version des Deutsch-Jozsa Algorithmus,
$f : \{0, 1\} \rightarrow \{0, 1\}$

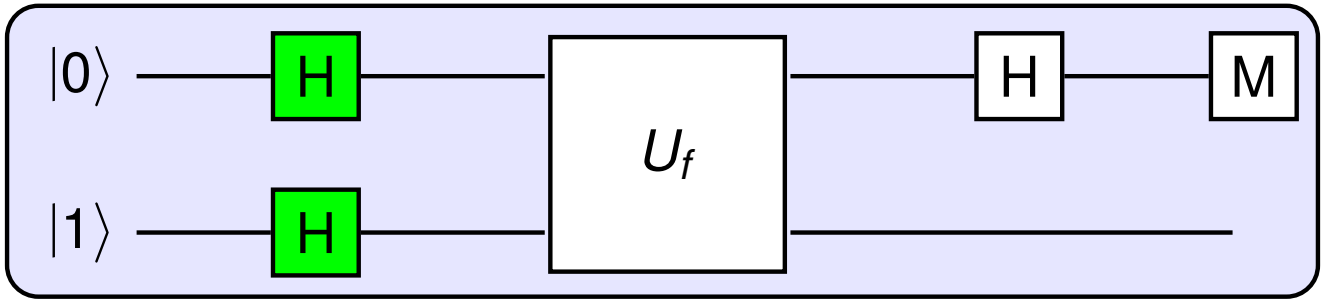
Deutsch Algorithmus



Vereinfachte Version des Deutsch-Jozsa Algorithmus,
$f : \{0, 1\} \rightarrow \{0, 1\}$

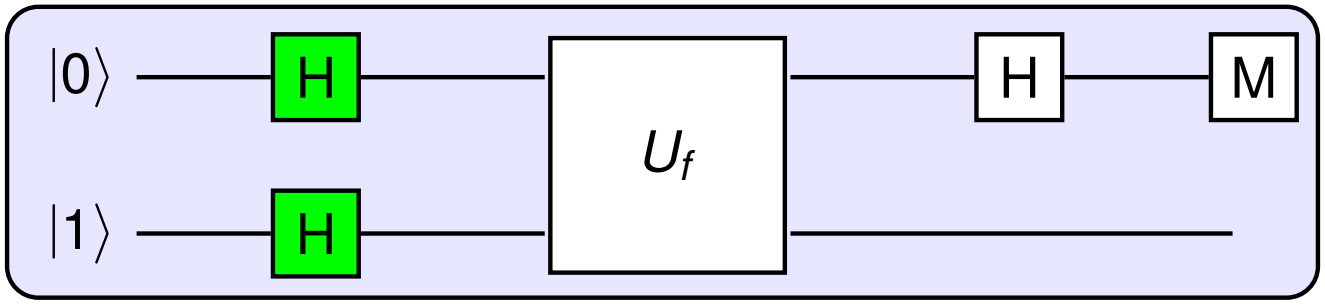
U_f ist modifiziertes CNOT-Gate:
Oberer Input $|x\rangle$ unverändert, unterer Input $|y\rangle$ wird zu $|y \oplus f(x)\rangle$

Deutsch - Schritt 1



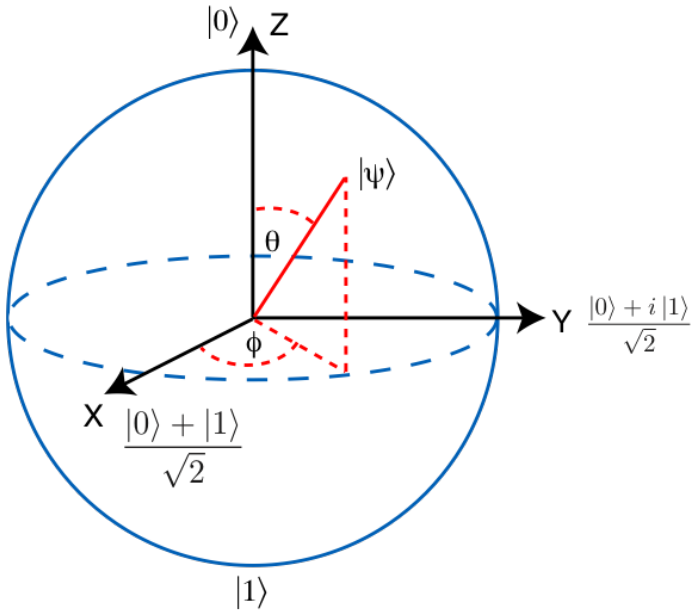
Erzeuge Superposition mit H.

Deutsch - Schritt 1

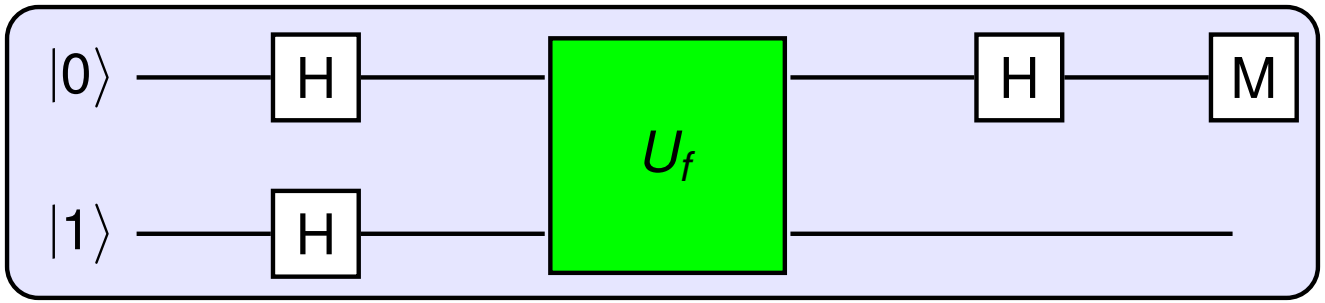


Erzeuge Superposition mit H.

$$|\psi\rangle = (H \cdot |0\rangle) \cdot (H \cdot |1\rangle)$$
$$= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \cdot \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$
$$= \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

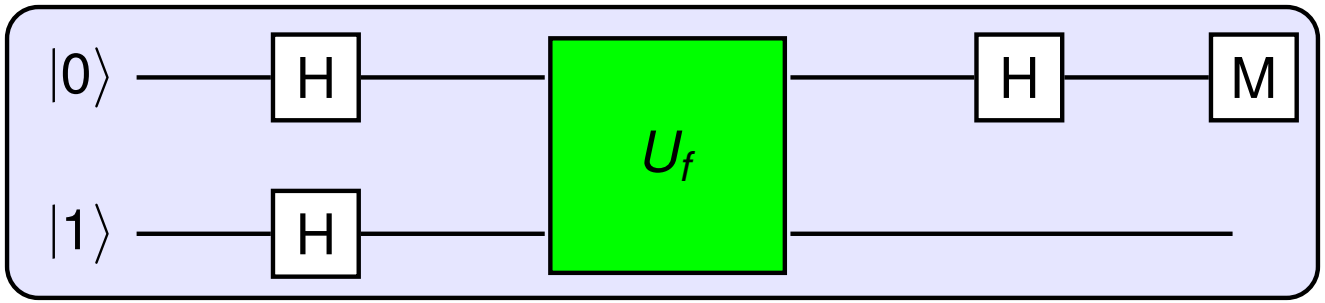


Deutsch - Schritt 2



$$\frac{\left(|0\rangle \cdot (-1)^{f(0)} + |1\rangle \cdot (-1)^{f(1)}\right) \cdot (|0\rangle - |1\rangle)}{2}$$

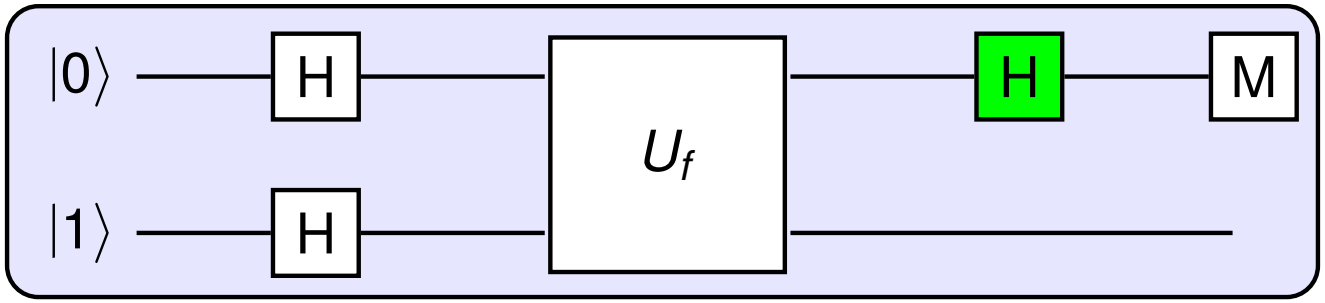
Deutsch - Schritt 2



$$\frac{\left(|0\rangle \cdot (-1)^{f(0)} + |1\rangle \cdot (-1)^{f(1)}\right) \cdot (|0\rangle - |1\rangle)}{2}$$

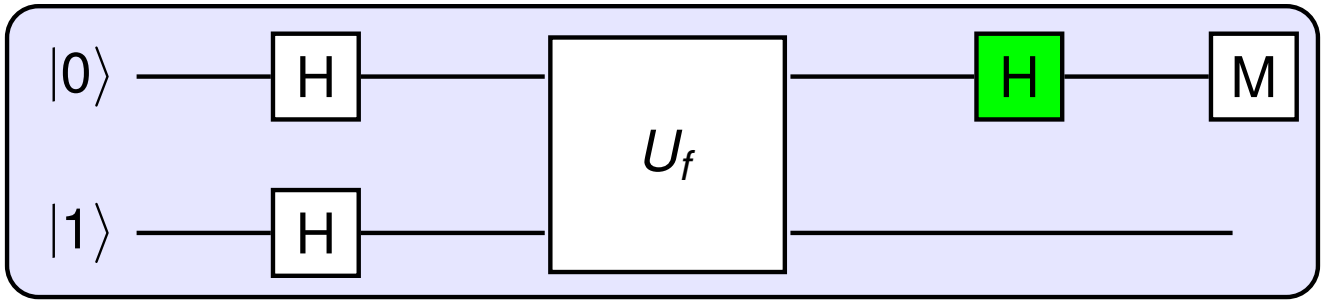
- $f(x)$ verändert nur Vorzeichen
- Vorzeichen in den oberen Qubit gezogen

Deutsch - Schritt 3



$$H \cdot \frac{\left(|0\rangle \cdot (-1)^{f(0)} + |1\rangle \cdot (-1)^{f(1)}\right)}{\sqrt{2}}$$

Deutsch - Schritt 3

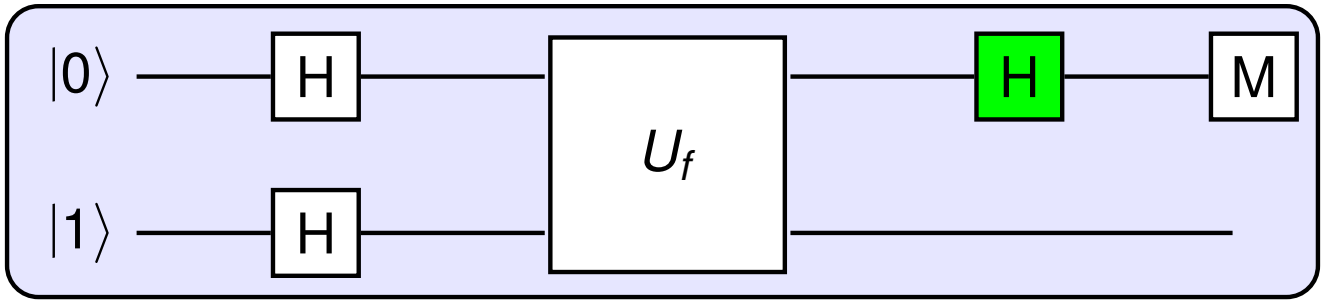


$$H \cdot \frac{\left(|0\rangle \cdot (-1)^{f(0)} + |1\rangle \cdot (-1)^{f(1)}\right)}{\sqrt{2}}$$

f konst.: $(-1)^{f(0)} = (-1)^{f(1)}$

$\Rightarrow H \cdot \pm\frac{|0\rangle+|1\rangle}{\sqrt{2}} = \pm|0\rangle$

Deutsch - Schritt 3



$$H \cdot \frac{\left(|0\rangle \cdot (-1)^{f(0)} + |1\rangle \cdot (-1)^{f(1)}\right)}{\sqrt{2}}$$

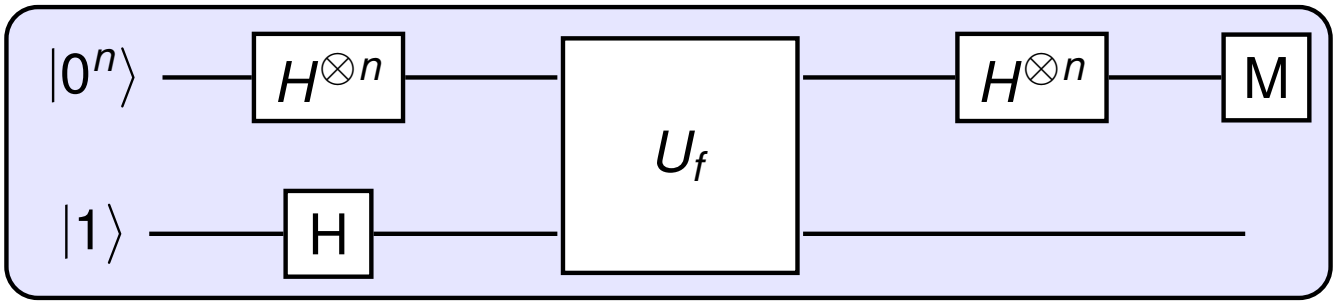
f konst.: $(-1)^{f(0)} = (-1)^{f(1)}$

$\Rightarrow H \cdot \pm\frac{|0\rangle+|1\rangle}{\sqrt{2}} = \pm|0\rangle$

f balanciert: $(-1)^{f(0)} ! = (-1)^{f(1)}$

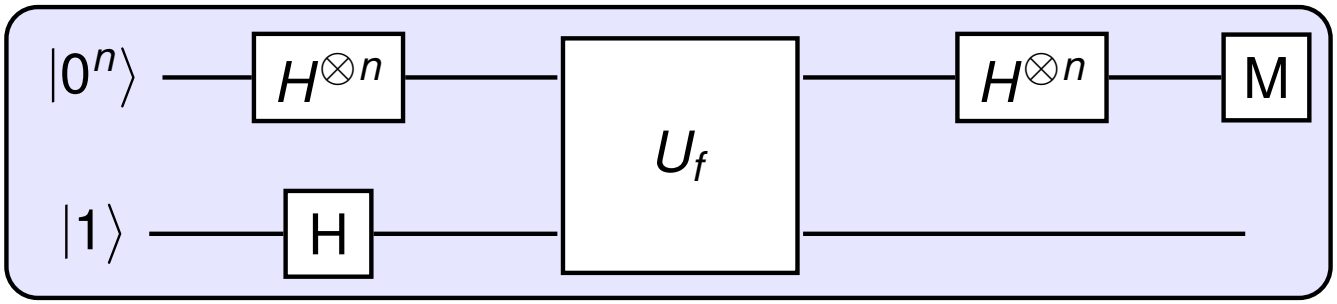
$\Rightarrow H \cdot \pm\frac{|0\rangle-|1\rangle}{\sqrt{2}} = \pm|1\rangle$

Deutsch-Jozsa - Ergebnis



Deutsch-Jozsa funktioniert analog mit n Qubits.

Deutsch-Jozsa - Ergebnis



Deutsch-Jozsa funktioniert analog mit n Qubits.

Problem zwar sehr künstlich, aber Grundlage für viele Quantenalgorithmen. (Shor, Grover)

Das Entscheidende ist die Nutzung des Phasenunterschieds.