Quantenkryptographie für die Schule

Claus Lämmerzahl
15. Februar 2022

Fundamentale Fragen der Physik
Highlights aus der Forschung
Bremen, 15. Februar 2022

GOC
Gauss-Olbers Space Technology Transfer Center

DFG
Research Training Group
Graduiertenkolleg
Models of Gravity

Universität Bremen*

CENTER OF
APPLIED SPACE TECHNOLOGY
AND MICROGRAVITY
ZARM

Inhalt

Quantentechnologien – Praktische Anwendungen der Quantenmechanik

Inhalt

Quantentechnologien – Praktische Anwendungen der Quantenmechanik

Quantencomputer

Inhalt

Quantentechnologien – Praktische Anwendungen der Quantenmechanik

Quantencomputer

Die quantenmechanische Messung

Inhalt

ZARM

Inhalt

ZARM

Inhalt

ZARM

Inhalt

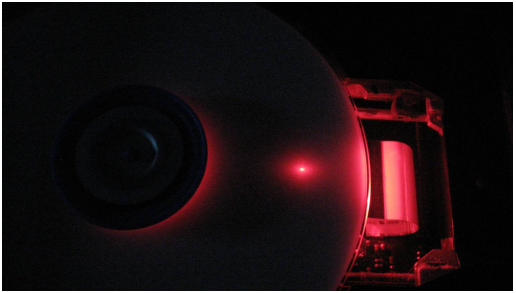
ZARM

Inhalt

ZARM

Praktische Anwendungen der Quantenmechanik

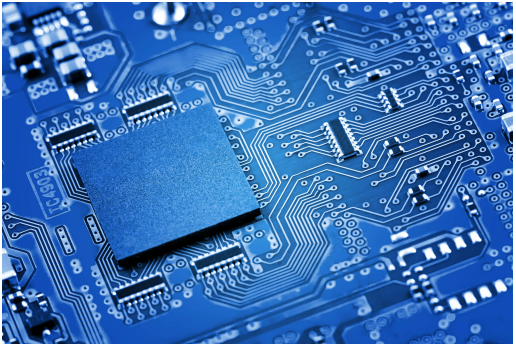
- Laser (CD, Laserpointer, Laserschweissen, ...)



Welt der Physik

Praktische Anwendungen der Quantenmechanik

- Laser (CD, Laserpointer, Laserschweissen, ...)
- Halbleiter (Transistoren, Dioden, elektrische Schaltkreise, Quantenelectronik, Chips, ...)



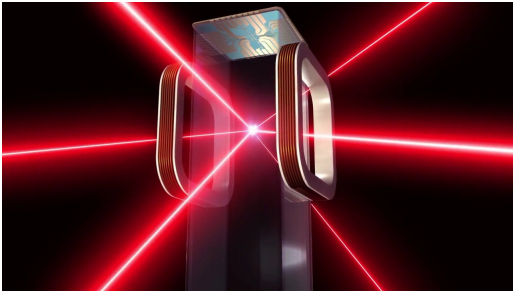
Praktische Anwendungen der Quantenmechanik

- Laser (CD, Laserpointer, Laserschweissen, ...)
- Halbleiter (Transistoren, Dioden, elektrische Schaltkreise, Quantenelectronik, Chips, ...)
- Uhren – Messung der Zeit (Atomuhr, international Atomzeit TAI, Positioning, Geodäsie, ...)

PTB

Praktische Anwendungen der Quantenmechanik

- Laser (CD, Laserpointer, Laserschweissen, ...)
- Halbleiter (Transistoren, Dioden, elektrische Schaltkreise, Quantenelectronik, Chips, ...)
- Uhren – Messung der Zeit (Atomuhr, international Atomzeit TAI, Positioning, Geodäsie, ...)
- Quantensensors (SQUID, Atominterferometer, ...)



Praktische Anwendungen der Quantenmechanik

- Laser (CD, Laserpointer, Laserschweissen, ...)
- Halbleiter (Transistoren, Dioden, elektrische Schaltkreise, Quantenelectronik, Chips, ...)
- Uhren – Messung der Zeit (Atomuhr, international Atomzeit TAI, Positioning, Geodäsie, ...)
- Quantensensors (SQUID, Atominterferometer, ...)
- Quantenmetrologie (neues SI-System)

PTB

ZARM

Praktische Anwendungen der Quantenmechanik

- Laser (CD, Laserpointer, Laserschweissen, ...)
- Halbleiter (Transistoren, Dioden, elektrische Schaltkreise, Quantenelectronik, Chips, ...)
- Uhren – Messung der Zeit (Atomuhr, international Atomzeit TAI, Positioning, Geodäsie, ...)
- Quantensensors (SQUID, Atominterferometer, ...)
- Quantenmetrologie (neues SI-System)

unser tägliches Leben basiert essentiell auf den Quantentechnologien

PTB

ZARM

Praktische Anwendungen der Quantenmechanik

1. Quantenrevolution: die Physik der Quantenenergien

- Laser (CD, Laserpointer, Laserschweissen, ...)
- Halbleiter (Transistoren, Dioden, elektrische Schaltkreise, Quantenelectronik, Chips, ...)
- Uhren – Messung der Zeit (Atomuhr, international Atomzeit TAI, Positioning, Geodäsie, ...)
- Quantensensors (SQUID, Atominterferometer, ...)
- Quantenmetrologie (neues SI-System)

unser tägliches Leben basiert essentiell auf den Quantentechnologien

PTB

ZARM

Praktische Anwendungen der Quantenmechanik

1. Quantenrevolution: die Physik der Quantenenergien

- Laser (CD, Laserpointer, Laserschweissen, ...)
- Halbleiter (Transistoren, Dioden, elektrische Schaltkreise, Quantenelectronik, Chips, ...)
- Uhren – Messung der Zeit (Atomuhr, international Atomzeit TAI, Positioning, Geodäsie, ...)
- Quantensensors (SQUID, Atominterferometer, ...)
- Quantenmetrologie (neues SI-System)

unser tägliches Leben basiert essentiell auf den Quantentechnologien

2. Quantenrevolution: die Physik der Quantenzustände

- Quantencomputer
- Quanteninformation
- Quantenkommunication
- Quantenkryptographie
- Quanteninternet
- Quantenbildgebung
- Quantenradar

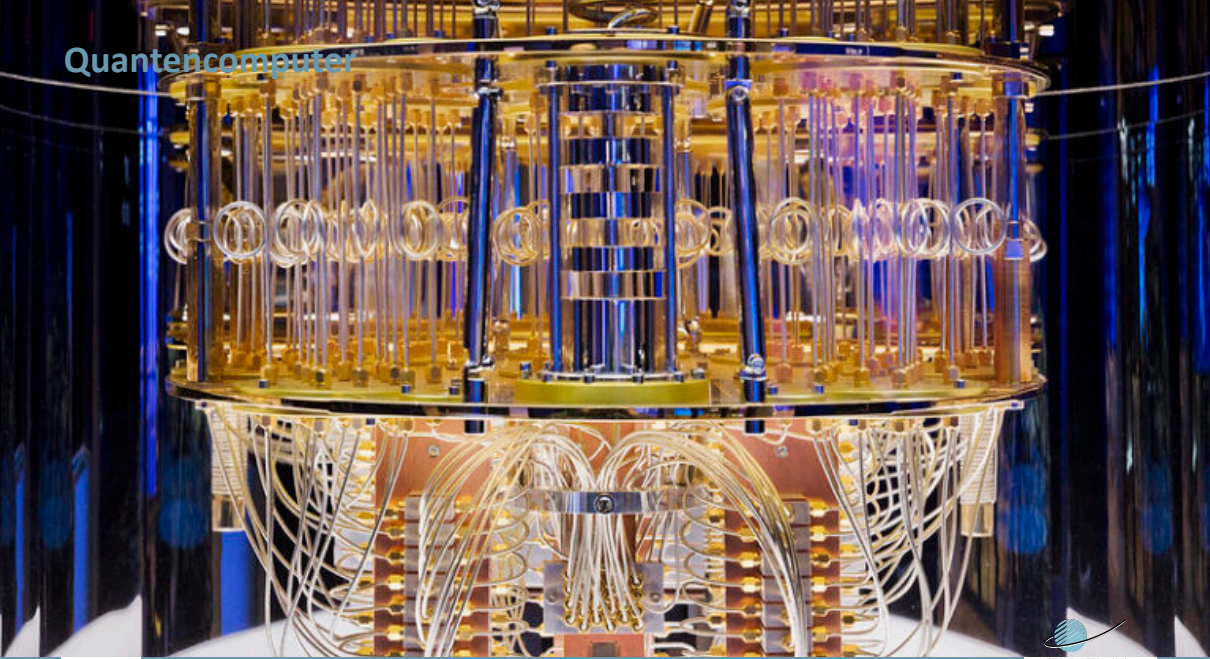
$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)$$

ZARM

Inhalt

ZARM

Quantencomputer



ZARM

Qanteninformation

Das Quanten-Bit

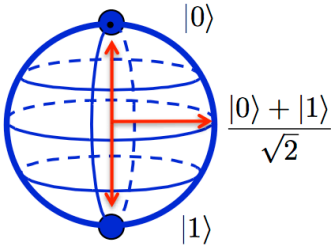
klassische Informationseinheit

- 0 und 1

quantenmechanische Informationseinheit

- alle komplexe Zahlen $|\alpha|^2 + |\beta|^2 = 1$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$



Classical Bit **Qubit**

$$|\psi\rangle = \cos\vartheta|0\rangle + e^{i\varphi}\sin\vartheta|1\rangle$$

Superpositionsprinzip

Quibits = Atome mit Spin, Photonen, ... (sehr kleine Systeme)

ZARM

Zahlen

binäre Darstellung
von Zahlen

0 00000

Zahlen

binäre Darstellung
von Zahlen

0 00000
1

Zahlen

binäre Darstellung
von Zahlen

0	00000
1	00001

Zahlen

binäre Darstellung
von Zahlen

0	00000
1	00001
2	

ZARM

Zahlen

binäre Darstellung
von Zahlen

0	00000
1	00001
2	00010

Zahlen

binäre Darstellung
von Zahlen

0	00000
1	00001
2	00010
3	

Zahlen

binäre Darstellung
von Zahlen

0	00000
1	00001
2	00010
3	00011

ZARM

Zahlen

binäre Darstellung
von Zahlen

0	00000
1	00001
2	00010
3	00011
4	

Zahlen

binäre Darstellung
von Zahlen

0	00000
1	00001
2	00010
3	00011
4	00100

Zahlen

binäre Darstellung
von Zahlen

0	00000
1	00001
2	00010
3	00011
4	00100
5	00101

Zahlen

binäre Darstellung
von Zahlen

0	00000
1	00001
2	00010
3	00011
4	00100
5	00101
6	00110

ZARM

Zahlen

binäre Darstellung
von Zahlen

0	00000
1	00001
2	00010
3	00011
4	00100
5	00101
6	00110
7	00111
8	01000
9	01001
10	01010

Zahlen

binäre Darstellung von Zahlen		klassisch-physikalische Darstellung Schalter ein oder aus		
0	00000	0	00000	○ ○ ○ ○ ○
1	00001	1	00001	○ ○ ○ ○ ●
2	00010	2	00010	○ ○ ○ ● ○
3	00011	3	00011	○ ○ ○ ● ●
4	00100	4	00100	○ ○ ● ○ ○
5	00101	5	00101	○ ○ ● ○ ●
6	00110	6	00110	○ ○ ● ● ○
7	00111	7	00111	○ ○ ● ● ●
8	01000	8	01000	○ ● ○ ○ ○
9	01001	9	01001	○ ● ○ ○ ●
10	01010	10	01010	○ ● ○ ● ○

Zahlen

binäre Darstellung von Zahlen

0	00000
1	00001
2	00010
3	00011
4	00100
5	00101
6	00110
7	00111
8	01000
9	01001
10	01010

klassisch-physikalische Darstellung
Schalter ein oder aus

0	00000	○ ○ ○ ○ ○
1	00001	○ ○ ○ ○ ●
2	00010	○ ○ ○ ● ○
3	00011	○ ○ ○ ● ●
4	00100	○ ○ ● ○ ○
5	00101	○ ○ ● ○ ●
6	00110	○ ○ ● ● ○
7	00111	○ ○ ● ● ●
8	01000	○ ● ○ ○ ○
9	01001	○ ● ○ ○ ●
10	01010	○ ● ○ ● ○

quantenmechanische Darstellung mittels Qubits

0	00000	$\|0\rangle\|0\rangle\|0\rangle\|0\rangle\|0\rangle = \|0\rangle$
1	00001	$\|0\rangle\|0\rangle\|0\rangle\|0\rangle\|1\rangle = \|1\rangle$
2	00010	$\|0\rangle\|0\rangle\|0\rangle\|1\rangle\|0\rangle = \|2\rangle$
3	00011	$\|0\rangle\|0\rangle\|0\rangle\|1\rangle\|1\rangle = \|3\rangle$
4	00100	$\|0\rangle\|0\rangle\|1\rangle\|0\rangle\|0\rangle = \|4\rangle$
5	00101	$\|0\rangle\|0\rangle\|1\rangle\|0\rangle\|1\rangle = \|5\rangle$
6	00110	$\|0\rangle\|0\rangle\|1\rangle\|1\rangle\|0\rangle = \|6\rangle$
7	00111	$\|0\rangle\|0\rangle\|1\rangle\|1\rangle\|1\rangle = \|7\rangle$
8	01000	$\|0\rangle\|1\rangle\|0\rangle\|0\rangle\|0\rangle = \|8\rangle$
9	01001	$\|0\rangle\|1\rangle\|0\rangle\|0\rangle\|1\rangle = \|9\rangle$
10	01010	$\|0\rangle\|1\rangle\|0\rangle\|1\rangle\|0\rangle = \|10\rangle$

ZARM

Parallelismus I

man kann in einem Quantenzustand mehrere Zahlen speichern

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|9\rangle + |5\rangle\right) = \frac{1}{\sqrt{2}}\left(|1\rangle|0\rangle|1\rangle|0\rangle + |0\rangle|1\rangle|0\rangle|1\rangle\right)$$

- mit 1 Qubit kann man 2 Zahlen darstellen
- mit 2 Qubits kann man $2 \cdot 2 = 2^2 = 4$ Zahlen darstellen
- mit 53 Qubits kann man $2^{52} \sim 10^{17}$ Zahlen darstellen (Grenzen der klassischen Rechenanlagen)
- mit 100 Qubits kann man $2^{100} \sim 10^{30}$ Zahlen darstellen = Anzahl der Sterne im Universum
- mit 1000 Qubits kann man $2^{1000} \sim 10^{300}$ Zahlen darstellen, weit mehr als alle Teilchen im Universum

enorm große Darstellungspotential

ZARM

Parallelismus II

mit n Qubits kann man nun $2^n - 1$ Zahlen gleichzeitig darstellen

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

- alle Zahlen von 0 bis $2^n - 1$ sind in diesem Zustand drin
- dies kann man durch bestimmte “Schaltkreise” erzeugen

man kombiniert diesen Zustand mit einem Null-Zustand eine bestimmten Länge

$$|\psi, 0\rangle = |\psi\rangle|0\rangle \qquad \text{mit} \qquad |0\rangle = |0\rangle|0\rangle \cdots |0\rangle$$

man kann nun rechnen: $x \to f(x)$ und erhält

$$f|\psi, 0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle$$

- d.h. in dem Endzustand sind alle Funktionswerte drin
- den gesuchten Funktionswert muss man “nur noch” ausmessen

Parallelismus II

mit n Qubits kann man nun $2^n - 1$ Zahlen gleichzeitig darstellen

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

- alle Zahlen von 0 bis $2^n - 1$ sind in diesem Zustand drin
- dies kann man durch bestimmte “Schaltkreise” erzeugen

man kombiniert diesen Zustand mit einem Null-Zustand eine bestimmten Länge

$$|\psi, 0\rangle = |\psi\rangle|0\rangle \qquad \text{mit} \qquad |0\rangle = |0\rangle|0\rangle \cdots |0\rangle$$

man kann nun rechnen: $x \to f(x)$ und erhält

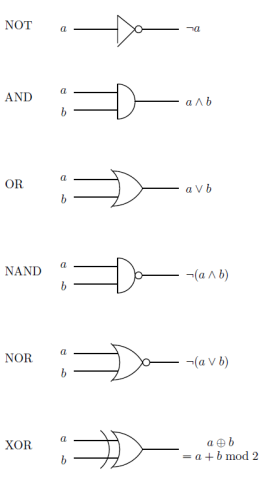
$$f|\psi, 0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle$$

massive Parallelität im Rechnen

- d.h. in dem Endzustand sind alle Funktionswerte drin
- den gesuchten Funktionswert muss man “nur noch” ausmessen

ZARM

Klassische und Quantengatter



a	$\neg a$
0	1
1	0

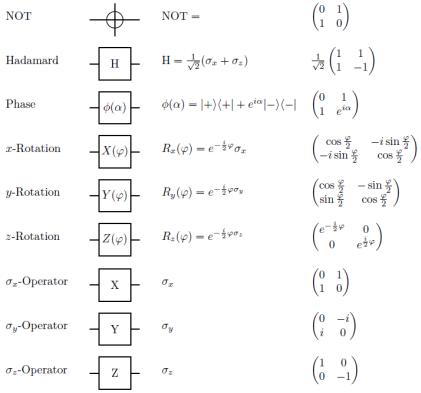
a	b	$a \wedge b$
0	0	0
1	0	0
0	1	0
1	1	1

a	b	$a \vee b$
0	0	0
1	0	1
0	1	1
1	1	1

a	b	$\neg(a \wedge b)$
0	0	1
1	0	1
0	1	1
1	1	0

a	b	$\neg(a \vee b)$
0	0	1
1	0	0
0	1	0
1	1	0

a	b	$a \oplus b$
0	0	0
1	0	1
0	1	1
1	1	0



wenn in der Schule Matrizen behandelt werden,
kann man auch Quantencomputing machen

ZARM

Quantencomputer

basiert auf

- volle Quantenmechanik
- Quantengatter (logische Schaltelemente AND, OR, NOT, ...)
- Quanten-Fehlerkorrektur

quantum supremacy

- zumindest verschiedene Klassen von Problemen können mit Quantencomputer schneller berechnet werden
- klassische Verschlüsselung kann geknackt werden
- Quantenverschlüsselung

großer Markt

- Optimierung
- Sicherheit
- Künstliche Intelligenz

Quantencomputer

basiert auf

- volle Quantenmechanik
- Quantengatter (logische Schaltelemente AND, OR, NOT, ...)
- Quanten-Fehlerkorrektur

quantum supremacy

- zumindest verschiedene Klassen von Problemen können mit Quantencomputer schneller berechnet werden
- klassische Verschlüsselung kann geknackt werden
- Quantenverschlüsselung

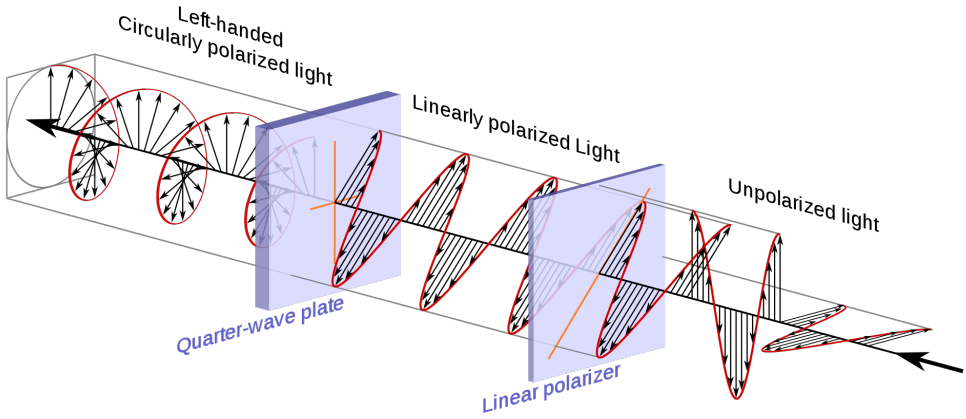
großer Markt

- Optimierung
- Sicherheit
- Künstliche Intelligenz

Inhalt

ZARM

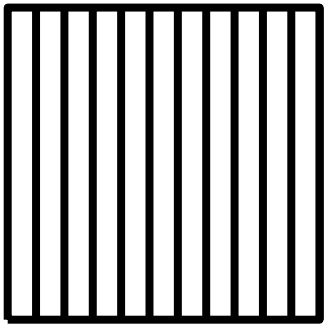
Polarisation von Photonen / Wellen



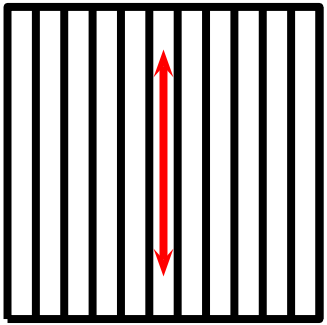
Messung der Polarisation von Lichtwelle

Polarisation

Polarisationsfilter / - messgerät



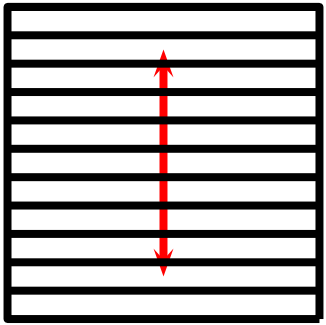
Messung der Polarisation von Lichtwellen



Polarisation vertikal
Filter vertikal

$\Rightarrow$ Licht kommt durch

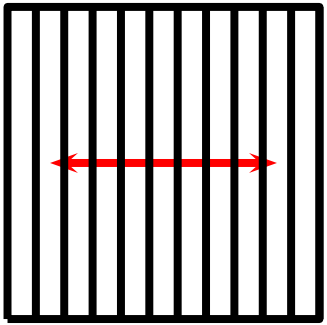
Messung der Polarisation von Lichtwellen



Polarisation vertikal
Filter horzontal

$\Rightarrow$ Licht kommt nicht durch

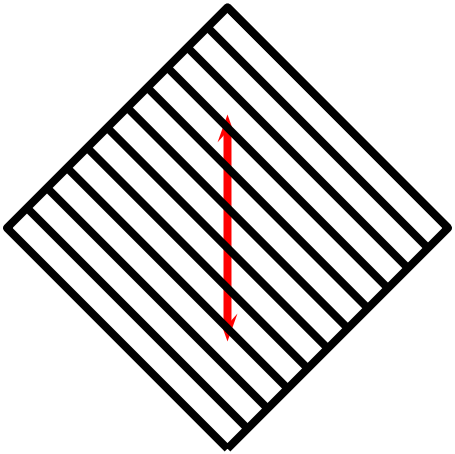
Messung der Polarisation von Lichtwellen



Polarisation horizontal
Filter vertikal

$\Rightarrow$ Licht kommt nicht durch

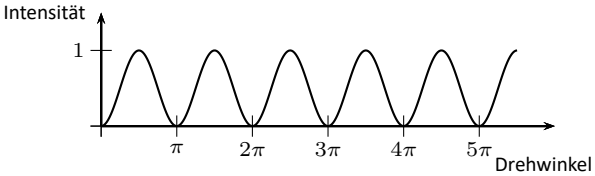
Messung der Polarisation von Lichtwellen



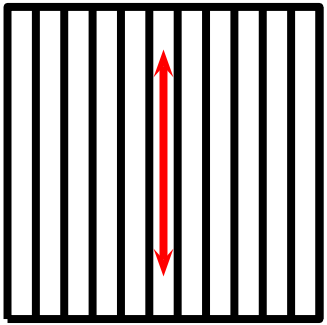
Polarisation vertikal
Filter diagonal

$\Rightarrow$ Licht kommt zu 50% durch

Intensität als Funktion des Drehwinkels



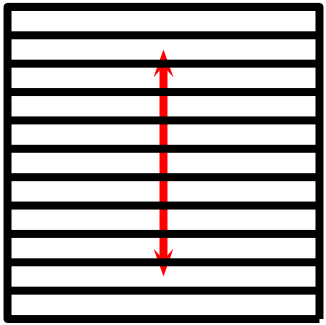
Messung der Polarisation von einzelnen Photonen



Polarisation vertikal
Filter vertikal

$\Rightarrow$ Photon kommt durch

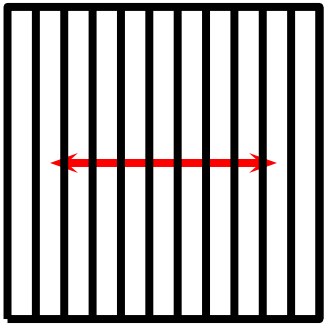
Messung der Polarisation von einzelnen Photonen



Polarisation vertikal
Filter horzontal

$\Rightarrow$ Photon kommt nicht durch

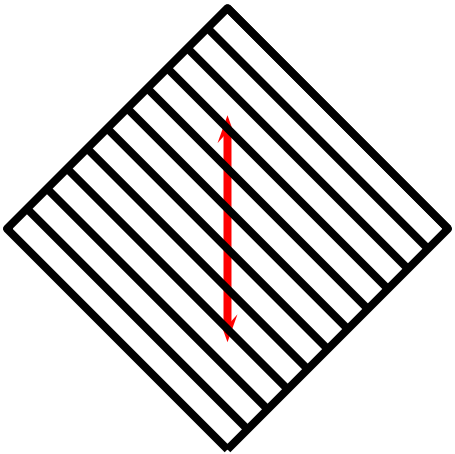
Messung der Polarisation von einzelnen Photonen



Polarisation horizontal
Filter vertikal

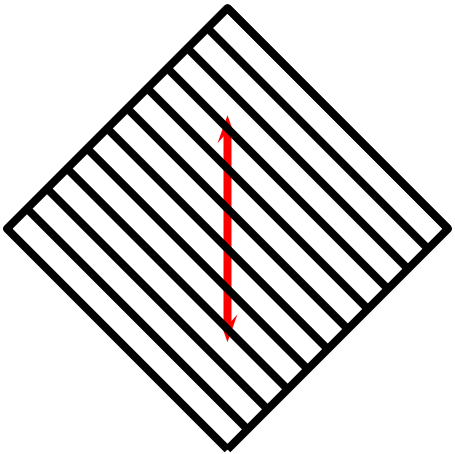
$\Rightarrow$ Photon kommt nicht durch

Messung der Polarisation von einzelnen Photonen



Polarisation vertikal + Filter diagonal
$\Rightarrow$ Photon kommt zu 50% durch ???????

Messung der Polarisation von einzelnen Photonen

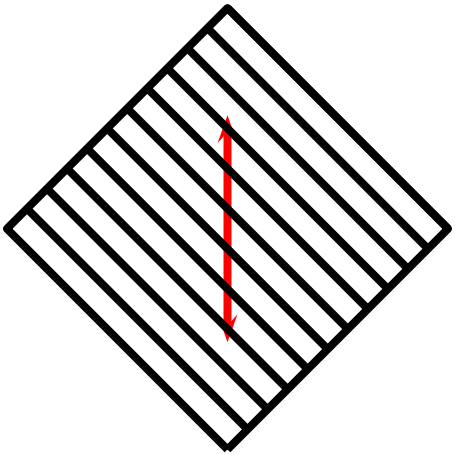


Polarisation vertikal + Filter diagonal
$\Rightarrow$ Photon kommt zu 50% durch ???????

Photon kann nicht zerteilt werden: daher nur "Durchkommen´´ oder "nicht Durchkommen´´

kann nicht vorhergesagt werden, ob Photon durchkommt oder nicht (man kann nur Wahrscheinlichkeit angeben, die aber für die Einzelmessung belanglos ist)

Messung der Polarisation von einzelnen Photonen



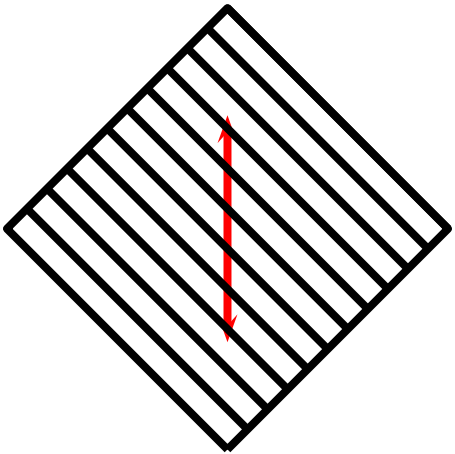
Polarisation vertikal + Filter diagonal
$\Rightarrow$ Photon kommt zu 50% durch ???????

Photon kann nicht zerteilt werden: daher nur "Durchkommen´´ oder "nicht Durchkommen´´

kann nicht vorhergesagt werden, ob Photon durchkommt oder nicht (man kann nur Wahrscheinlichkeit angeben, die aber für die Einzelmessung belanglos ist)

ein Beispiel des quantenmechanischen Messprozesses

Messung der Polarisation von einzelnen Photonen



Polarisation vertikal + Filter diagonal
⇒ Photon kommt zu 50% durch ???????

Photon kann nicht zerteilt werden: daher nur "Durchkommen´´ oder "nicht Durchkommen´´

kann nicht vorhergesagt werden, ob Photon durchkommt oder nicht (man kann nur Wahrscheinlichkeit angeben, die aber für die Einzelmessung belanglos ist)

ein Beispiel des quantenmechanischen Messprozesses

Frage: wie erzeugt man einzelne Photonen?

Inhalt

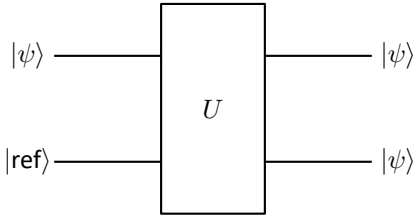
ZARM

Das no-cloning-Theorem

man kann von einem Quantenzustand $|\psi\rangle$ keine Kopie herstellen

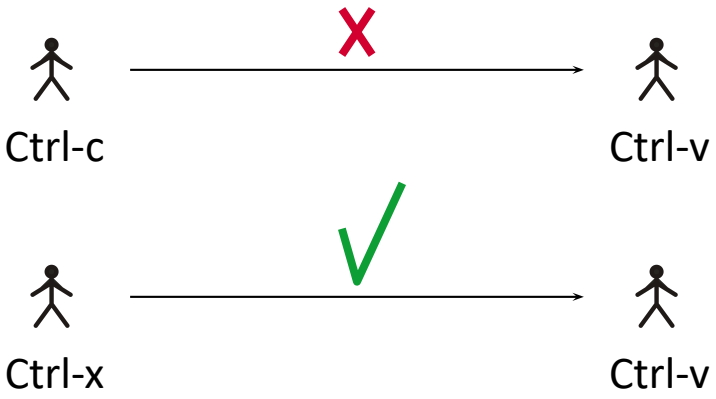
es existiert kein unitärer Operator, so dass

$$U(|\psi\rangle \otimes |\text{ref}\rangle) = \alpha|\psi\rangle \otimes |\psi\rangle$$



- verständlich wegen Messprozess: der Messprozess zerstört i.A. den auszumessenden Zustand ($\rightarrow$ Messpostulat)
- ist wesentlicher Aspekt bei Quanten-kommunikation: abhörsichere Kommunikation
- abhörsicher wegen physikalischer Grundgesetze, die nicht ausgeheblt werden können

Das no-cloning-Theorem



Inhalt

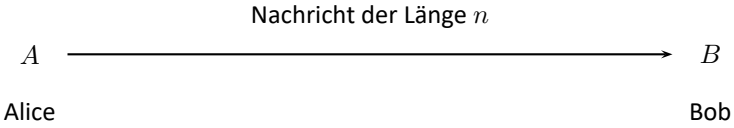
ZARM

Inhalt

ZARM

Nachrichtenübertragung

allgemeines setting



Abbildung

$$\begin{array}{cccc} 0 & 0 & \to & 0 \\ 0 & 1 & \to & 1 \\ 1 & 0 & \to & 1 \\ 1 & 1 & \to & 0 \end{array}$$

äquivalent zu $a + b \bmod 2 = a \oplus b$

Klassische Kryptographie

klassische Ver- und Entschlüsselung von Nachrichten

Vernan-Kodierung

Sender

Nachricht	00110111001010111101001
$\oplus$ Schlüssel	10111010001010111100110
Kryptogramm	10001101000000000001111

Empfänger

Kryptogramm	10001101000000000001111
$\oplus$ Schlüssel	10111010001010111100110
Nachricht	00110111001010111101001

Quantenkryptographie

- der Schlüssel ist vorgegeben oder man konstruiert ihn sich
- das Senden eines gegeben Schlüssels oder das sich per Konstruktion Einigen auf einen Schlüssel ist ein zutiefst quantenmechanischer Prozess (Messprozess)
- diese Verfahren sind absolut abhörsicher, wenn jemand abhört, kann das detektiert werden
- Grundlage ist das no-cloning-Theorem

Inhalt

ZARM

B92-Protokoll

hier *einigen* sich Alice und Bob auf einen gemeinsamen Schlüssel

es gibt zwei Sorten von Polarisationen $\uparrow, \rightarrow$ und $\nearrow, \searrow$, die beide $45°$ gegeneinander gedreht sind

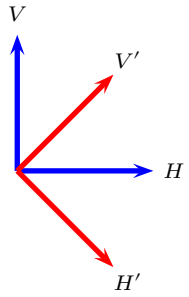
- Alice hat eine Zufallsreihe von 0 und 1, diese bestimmen die Polarisation der einzelnen Photonen

$$0 \rightarrow \uparrow \quad \text{und} \quad 1 \rightarrow \nearrow$$

die Alice zu Bob schickt

- Bob hat ebenfalls eine (andere) Zufallsreihe von 0 und 1, diese bestimmen den Gebrauch seines Polarisationsfilters

$$0 \rightarrow \searrow \quad \text{und} \quad 1 \rightarrow \rightarrow$$



Bennet 1992

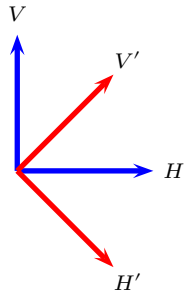
B92-Protokoll

Durchrechnen der Möglichkeiten

- Alice and Bob haben unterschiedliche Zufallszahlen
  - wenn Alice 0 und Bob 1 hat, dann misst $\rightarrow$ ein $\uparrow \Rightarrow$ kein Klick
  - wenn Alice 1 und Bob 0 hat, dann misst $\searrow$ ein $\nearrow \Rightarrow$ kein Klick
- Alice und Bob haben gleiche Zufallszahlen
  - wenn Alice und Bob beide 0 haben, dann misst $\searrow$ ein $\uparrow \Rightarrow$ Klick mit Wahrscheinlichkeit 50%
  - wenn Alice und Bob beide 1 haben, dann misst $\rightarrow$ ein $\nearrow \Rightarrow$ Klick mit Wahrscheinlichkeit 50%

nun kann Bob Alice öffentlich darüber informieren, wann sein Detektor Klick gemacht hat (ohne über die Polarisation zu reden) $\Rightarrow$

- immer, wenn der Detektor klick gemacht hat, haben Alice und Bob dieselben Zahlen
- bei welchen Zahlen es klickt, hängt von quantenmechanischen Messprozess ab



Bennet 1992

B92-Protokoll: Experiment

man gebe sich Alices und Bobs Zufalszahlen beliebig vor und verwende die obigen Regeln
die Messung muss dann den gemeinsamen Schlüssel ergeben

Nummer des Photons	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Alices Zufallszahlen															
Alices Polarisation															
Bobs Zufallszahlen															
Bobs Filter															
Klick des Detektors															

Alice und Bob müssen die gleichen Zahlen (= Schlüssel) haben

B92-Protokoll: Beispiel

Nummer des Photons	1	2	3	4	5	6	7	8	9
Alices Zufallszahlen	1	0	0	1	1	0	1	0	0
Alices Polarisation	↗	↑	↑	↗	↗	↑	↗	↑	↑
Bobs Zufallszahlen	0	0	1	0	1	0	1	0	1
Bobs Filter	↘	↘	→	↘	→	↘	→	↘	→
Klick des Detektors	n	j/n	n	n	j/n	j/n	j/n	j/n	n

- es werden nur die Messungen genommen, bei denen der Detektor geklickt hat
- j/n ist 50:50 Ergebnis einer Quantenmessung, nicht vorhersagbar
- ein Dritter kann auch nicht messen, da eine weitere Messung das Ergebnis verändert (das gesendete Photon auf dem Wege zu Bob würde dann i.d.R. verändert oder vernichtet, was Bob erkennen kann oder man in Fehlern bei der Ver- und Entschlüsselung erkennt)
- brauche viermal soviele Messungen, wie die Länge der zu verschlüsselnden Nachricht

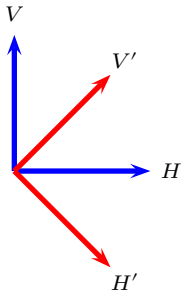
Inhalt

ZARM

BB84-Protokoll

ähnlich zum B92-Protokoll, hier wird *der Schlüssel von Alice zu Bob übermittelt*.

es gibt wieder zwei Sorten von Polarisationen $\uparrow, \rightarrow$ und $\nearrow, \searrow$, die beide 45° gegeneinander gedreht sind



- Alice hat eine erste Zufallsreihe s_i aus 0 und 1, soll an Bob als Schlüssel übermittelt werden
- Alice hat eine zweite Zufallsreihe b_i aus 0 und 1, zeigt die Wahl der Basis an
- Alice sendet nun ein Photon, und zwar mit folgender Zuordnung

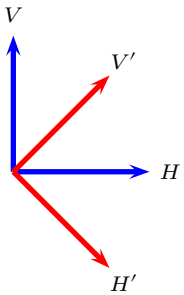
	$s_i = 0$	$s_i = 1$
$b_i = 0$	$\rightarrow$	$\uparrow$
$b_i = 1$	$\searrow$	$\nearrow$

Bennet & Brassard
1984

BB84-Protokoll

- Bob hat eine Zufallsreihe b_i' aus 0 und 1, die seinen Polarisationsfilter bestimmt: $0 \to \uparrow$, $1 \to \nearrow$
- Bob misst mit seiner Basis die Photonen von Alice, ohne die Basis von Alice zu kennen
- Analyse der Möglichkeiten:
  - hat Bob eine Basis gleicher Farbe gewählt, dann ist $s_i' = s_i$
  - hat Bob eine verschiedenfarbige Basis gewählt, dann ist $s_i' = s_i$ oder $s_i \neq s_i'$ mit 50:50-Wahrscheinlichkeit
- Bob und Alice gleichen öffentlich ihre Wahl der Basen ab
- es werden nur die Bits genommen, für die die Wahl der Basen von Alice und Bob gleich ist $\Rightarrow s_i' = s_i$.

Damit hat Alice Bob Teile ihres Schlüssels übertragen. Die Messwerte $s_i = s_i'$ entspringen einer Quantenmessung.



Bennet & Brassard
1984

Ein Experiment

man gebe sich zufällig vor s_i, b_i und b'_i und verwende die obigen Regeln
die Messung muss dann den gemeinsamen Schlüssel ergeben

Nummer des Photons		1	2	3	4	5	6	7	8	9	10	11	12	13	14
zu übertragender Schlüssel	s_i														
Alices zufällige Basiswahl	b_i														
Photonpolarisation															
Bobs zufällige Basiswahl	b'_i														
Detektorfilter															
Messwert von Bob	s'_i														
beibehaltene Bitsequenz	k														

Alice und Bob müssen die gleichen Zahlen (= Schlüssel) haben

Ein Beispiel

Nummer des Photons		1	2	3	4	5	6	7	8	9	10	11	12	13	14
zu übertragender Schlüssel	s_i	1	0	1	1	0	1	0	1	0	0	0	1	1	0
Alices zufällige Basiswahl	b_i	0	1	1	0	1	0	0	1	0	1	1	1	0	0
Photonpolarisation		↑	↘	↗	↑	↘	↑	→	↗	→	↘	↘	↗	↑	→
Bobs zufällige Basiswahl	b'_i	0	0	0	0	1	1	0	1	1	1	0	1	0	1
Detektorfilter		↑	↑	↑	↑	↗	↗	↑	↗	↗	↗	↑	↗	↑	↗
Messwert von Bob	s'_i	1	–	–	1	0	–	0	1	–	0	–	1	1	–
beibehaltene Bitsequenz	k	1			1	0		0	1		0		1	1	

- die beibehaltene Bitsequenz ist der gemeinsame Schlüssel k
- ein Lauschangriff kann wegen des No-Cloning-Theorems entdeckt werden

Ein Beispiel

man kann auch andere Identifizierungen nehmen

	$s_i = 0$	$s_i = 1$
$b_i = 0$	→	↑
$b_i = 1$	↘	↗

und

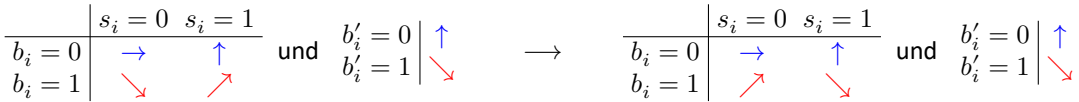
$b'_i = 0$	↑
$b'_i = 1$	↗

Nummer des Photons		1	2	3	4	5	6	7	8	9	10	11	12	13	14
zu übertragender Schlüssel	s_i	1	0	1	1	0	1	0	1	0	0	0	1	1	0
Alices zufällige Basiswahl	b_i	0	1	1	0	1	0	0	1	0	1	1	1	0	0
Photonpolarisation		↑	↘	↗	↑	↘	↑	→	↗	→	↘	↘	↗	↑	→
Bobs zufällige Basiswahl	b'_i	0	0	0	0	1	1	0	1	1	1	0	1	0	1
Detektorfilter		↑	↑	↑	↑	↗	↗	↑	↗	↗	↗	↑	↗	↑	↗
Messwert von Bob	s'_i	1	–	–	1	0	–	0	1	–	0	–	1	1	–
beibehaltene Bitsequenz	k	1			1	0		0	1		0		1	1	

ZARM

Ein Beispiel

man kann auch andere Identifizierungen nehmen



Nummer des Photons		1	2	3	4	5	6	7	8	9	10	11	12	13	14
zu übertragender Schlüssel	s_i	1	0	1	1	0	1	0	1	0	0	0	1	1	0
Alices zufällige Basiswahl	b_i	0	1	1	0	1	0	0	1	0	1	1	1	0	0
Photonpolarisation		↑	↗	↘	↑	↗	↑	→	↘	→	↗	↗	↘	↑	→
Bobs zufällige Basiswahl	b'_i	0	0	0	0	1	1	0	1	1	1	0	1	0	1
Detektorfilter		↑	↑	↑	↑	↘	↘	↑	↘	↘	↘	↑	↘	↑	↘
Messwert von Bob	s'_i	1	–	–	1	0	–	0	1	–	0	–	1	1	–
beibehaltene Bitsequenz	k	1			1	0		0	1		0		1	1	

Inhalt

ZARM

E91-Protokoll

- Protokoll verwendet Verschränkung
- Verwendung von 4 Basen: b_1, b_2, b_3 und b_4 nennen wollen
- Alice und Bob nutzen jeweils drei Basen, zwei stimmen überein – wählen z.B. $b^{(\text{Alice})} = \{b_1, b_2, b_3\}$ und $b^{(\text{Bob})} = \{b_2, b_3, b_4\}$

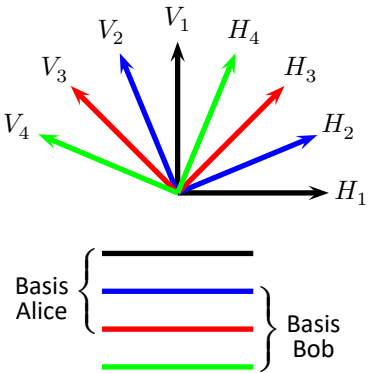
Es wird wieder in mehreren Schritten vorgegangen.

- eine Dritte erzeugt einen verschränkter Zustand aus zwei Teilchen (Photonen), wir wählen

$$|\Phi\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$$

Das erste Teilchen fliegt zu Alice, das zweite zu Bob.

- Wenn Alice und Bob die Teilchen in ihren Basen ausmessen, werden ihre Ergebnisse antikorreliert sein (beim Bell-Zustand mit $+$ wären die Ergebnisse korreliert)

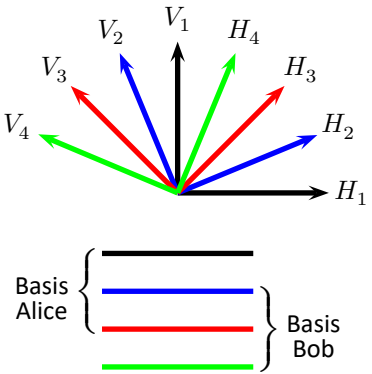


Die vier Basen von Alice und Bob

Eckart 1991

E91-Protokoll

- Alice wählt eine Zufallsfolge aus ihren Basen $\{\alpha_1, \alpha_2, \alpha_3\}$ mit $\alpha_i \in b^{(A)}$. Ebenfalls wählt Bob eine Zufallsfolge aus seiner Menge von Basen $\{\beta_1, \beta_2, \beta_3\}$ aus.
- Alice und Bob führen nun an den Bell-Teilchen Messungen in der gewählten Basen durch. Beide erhalten davon Messwerte $\{m_1^A, m_2^A, m_3^A, \ldots, m_N^A\}$ und $\{m_1^B, m_2^B, m_3^B, \ldots, m_N^B\}$.
- Alice und Bob gleichen ihre Basen über öffentlichen Kanal ab
- der Schlüssel ergibt sich wieder aus den Messwerten bei einer gemeinsamen Basis, wobei diese notwendigerweise wegen der Quantenmessung von Alice und Bob und wegen der Verschränkung gleich sein müssen



Die vier Basen von Alice und Bob

Eckart 1991

Ein Beispiel

Nummer der Messung	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Alice Zufallsbasis	α_1	α_1	α_2	α_1	α_3	α_1	α_1	α_2	α_1	α_3	α_2	α_1	α_2	α_2	α_1
Alice Messungen	0	0	1	0	1	1	0	0	1	0	1	1	0	0	0
Bobs Zufallsbasis	β_2	β_2	β_2	β_3	β_2	β_2	β_3	β_1	β_2	β_1	β_2	β_3	β_1	β_1	β_1
Bobs Messungen	1	0	1	1	1	0	0	8	0	1	1	1	0	0	0
Schlüssel k			1								1				0

Auch hier ergibt sich die Sicherheit der Erzeugung wieder aus den Prinzipien der Quantenmechanik. Hier kann man aber auch Kriterien, die auf der Bellschen Ungleichung beruhen, angeben, um zu sehen, ob man abgehört wurde oder nicht.

Bemerkungen

- Sicherheit beruht auf
  - quantenmechanischem Messprozess
  - no-cloning-Theorem
- da Schlüssel so lang sein soll wie die Nachricht, muss man insgesamt Nachrichten austauschen, die mehrfach so lang sind wie die zu verschlüsselnde Nachricht
- Fehlerkorrekturen verlangen zusätzlich Redundanz

$\Rightarrow$ gro□es Datenaufkommen

Inhalt

Inhalt

ZARM

Nachrichten

es geht um das effiziente Versenden von Nachrichten

Alphabet Ein Alphabet ist eine Menge X von K Zeichen $\{x_1, x_2, x_3, \dots, x_K\}$, die alle mit einer bestimmten Wahrscheinlichkeit $\{p_1, p_2, \dots p_K\}$ vorkommen.

Nachricht Eine Nachricht ist eine Menge von n Buchstaben $x_i \in X$, $i = 1, 2, \dots, n$. Die Menge der Nachrichten der Länge n ist N.

Shannon-Entropie Jedes Alphabet und jede Nachricht hat eine Entropie

$$H_X = -\sum_{i=1}^{K} p_i \log_2 p_i \qquad \text{und} \qquad H_N = -n \sum_{i=1}^{N} p_i \log_2 p_i \to n H_X$$

Anzahl der unterschiedlichen Nachrichten der Länge n bei K Buchstaben ist ungefähr $N \approx e^{2nH_X(p)}$. Jede Sprache hat ihre Entropie.

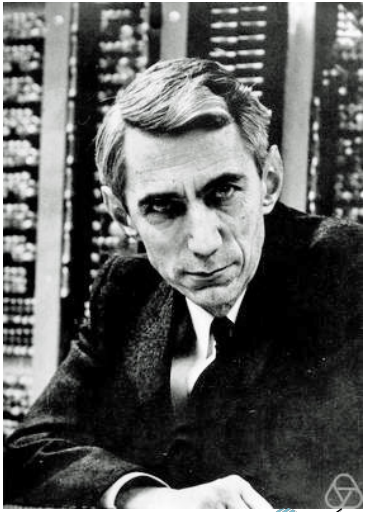
Nachrichten

Kompression Abbbildungen $C : \mathcal{N} \to \mathcal{M}$ und $D : \mathcal{M} \to \mathcal{N}$ mit $\mathcal{M} \subset \mathcal{N}$ nennt man Kompression und Dekompression, falls $D \circ C = \mathbb{1}$.

Erstes Shannon-Theorem

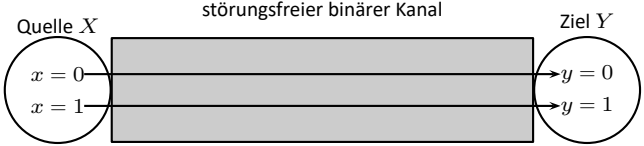
Eine Nachricht der Länge n aus einem Alphabet mit K Buchstaben kann von $n \log K$ Bits verlässlich auf $nH(p) \log K$ Bits komprimiert werden.

heisst auch Shannon's noiseless coding theorem

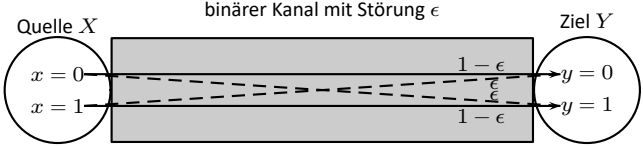


Verrauschte Nachrichten

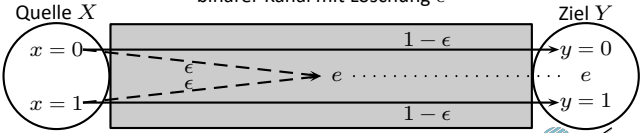
störungsfreier binärer Kanal



binärer Kanal mit Störung ϵ



binärer Kanal mit Löschung ϵ



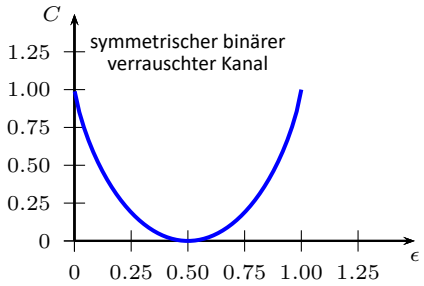
Kapazität eines Kanals

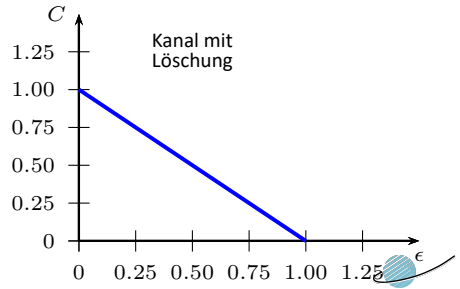
Kapazität

Die Kapazität gibt die bestmögliche Informationsübertragung bei einem gegebenen Kanal an

$$C := \max_{p_X} I(X;Y)$$

abstrahiert von der Information, charakterisiert ausschließlich die Übertragung (Kanal)





Kompression bei verrauschten Kanälen

Zweites Shannon-Theorem

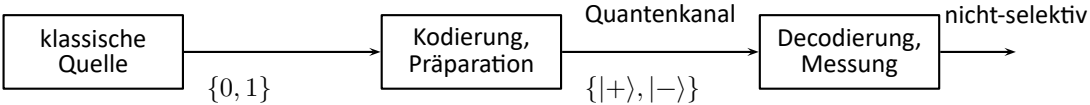
Durch Codierung einer Nachricht der Länge nR in 2^{nR} Codeworte der Länge n kann die Nachricht asymptotisch für $n \to \infty$ fehlerfrei übertragen werden, falls die Rate $0 \leq R \leq 1$ die Kapazität C nicht übersteigt, $R < C$.

dies heisst auch Shannon's noisy channel coding theorem

Inhalt

ZARM

Quantenkommunikation



Quantenalphabet ein Quantenbuchstabe ist ein Element von $\{|\psi_x\rangle, p_x\}$, d.h. ein Alphabet ist beschrieben durch

$$\rho = \sum_{i=1}^{K} p_i |\psi_i\rangle\langle\psi_i|$$

Quantennachricht der Länge n ist

$$\rho^n = \rho \otimes \rho \otimes \cdots \otimes \rho$$

von Neumann-Entropie Entropie eines Quantenalphabets bzw. -nachricht

$$S(\rho) = -\mathrm{tr}\,(\rho \log \rho) \qquad S(N) \to nS(\rho)$$

Schumacher's noiseless quantum coding theorem 1995

Man benötigt optimalerweise nur $nS(\rho)$ Qubits um n Qubits zu übertragen.

- Beweis analog zu Shannon's noiseless coding theorem, aber etwas komplizierter
- ist auch auf verrauschte Quantenkanäle übertragbar

Quantenkommunikation

für orthogonale Zustände gilt

$$H(p) = S(\rho)$$

d.h. Quanteninfomation = klassische Information
für nichtorthogonale Zustände, d.h. für

$$\rho = \sum p_x \rho_x$$

gilt

$$H(p) = S(\rho) - \sum_x p_x S(\rho_x) =: \chi(\mathscr{E})$$ mit Ensemble von Quantenzuständen $$\mathscr{E} = \{\rho_x, p_x\}$$

dies ist auch die maximal erreichbare Information = Holevo-Grenze = obere Schranken der Übertragungsrate

Quantenkommunikation

Quantenkapazität

$$C := \max_{\mathscr{E}} \chi(\mathscr{E})$$

dies ist die maximale Anzahl von klassischen bits pro Quantenbuchstabe, die durch einen Quantenkanal transportiert werden können

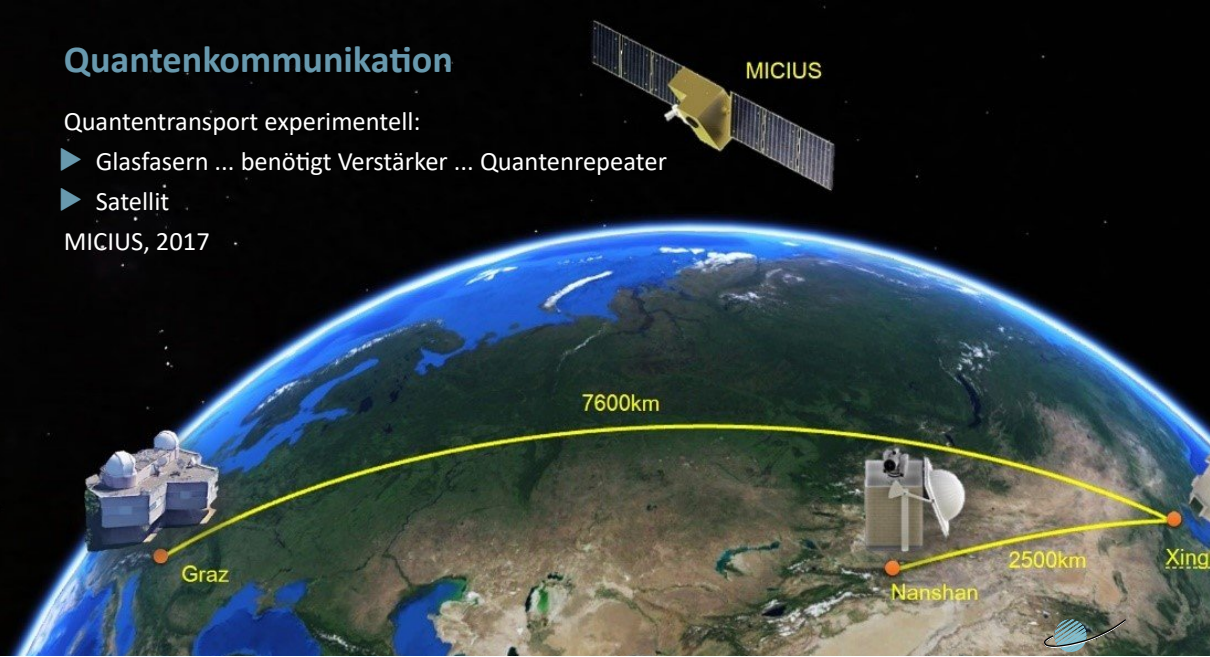
$\Rightarrow$ Schumacher's noisy channel coding theorem

Quantenkommunikation

Quantentransport experimentell:

- Glasfasern ... benötigt Verstärker ... Quantenrepeater
- Satellit

MICIUS, 2017



Inhalt

ZARM

Schlusswort

Quantentechnologien werden wichtiger

- Abhörsicherheit
- massive Rechenleistung
- grenzenlose Vielfältigkeit (Quanten(meta)materialien)
- Metrologie (Eindeutigkeit des Vergleichs)
- Quantenchemie
- quantum mashine learning, quantum based artificial intelligence ?

Schlusswort

Quantentechnologien werden wichtiger

- Abhörsicherheit
- massive Rechenleistung
- grenzenlose Vielfältigkeit (Quanten(meta)materialien)
- Metrologie (Eindeutigkeit des Vergleichs)
- Quantenchemie
- quantum mashine learning, quantum based artificial intelligence ?

Quantenmechanik

- ... übersteigt unser Vorstellungsvermögen
- ... kann von uns kontrolliert werden
- ... geht mit ihren Grundlagen direkt in die Technologien ein

Mögliche weitere Themen

- Bit und Qubit
- Quantengatter
- Quantencomputing
- Verschränkung und das Verständnis der Quantenmechanik
- klassische Informationstheorie
- Quanteninformationstheorie
- klassische Kommunikation
- Quantenkommunikation

und die jeweiligen experimentellen Realisierungen

Mögliche weitere Themen

- Bit und Qubit
- Quantengatter
- Quantencomputing
- Verschränkung und das Verständnis der Quantenmechanik
- klassische Informationstheorie
- Quanteninformationstheorie
- klassische Kommunikation
- Quantenkommunikation

und die jeweiligen experimentellen Realisierungen

Danke sehr!