

Gesche Pospiech
TU Dresden, Fakultät Physik, Professur Didaktik der Physik

Die zweite Quantenrevolution - Quanteninformation im Physikunterricht

Überblick

- **Die 2. Quantenrevolution**
- **Quantentechnologie und Allgemeinbildung**
- **Der Kern der Quantenphysik**
- **Anregung:
Quantenkryptographie**
- **Mittel zur Umsetzung**
- **Ausblick**



Die 2. Quantenrevolution

- **... kam auf leisen Sohlen**
 - getrieben von Fragen nach den Grundlagen der Quantenphysik und ihrer Bedeutung für unser Weltverständnis
 - Und (zunächst) **nicht**: weil man konkrete Anwendungen entwickeln wollte.
- **Erkenntnisgewinnung mit ungeahnten Auswirkungen**
 - Klassische Instrumente führen zur Entdeckung der Quantenphysik, der 1. Quantenrevolution
 - Quantenphysikalische Instrumente führen zur 2. Quantenrevolution: Quantensensoren, Quantenmetrologie, Quanteninformation ...
 - **Quantenkryptographie**, Quantencomputer

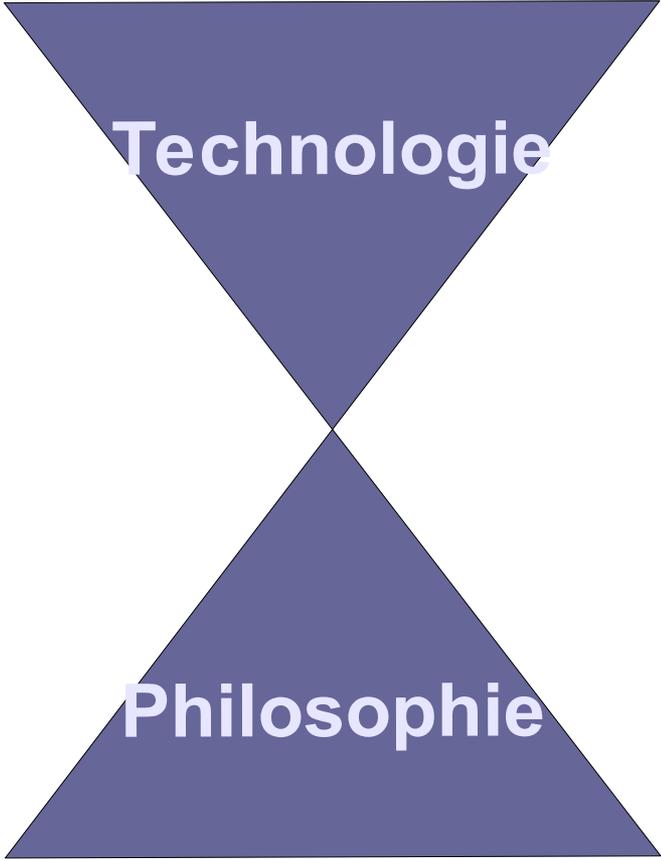
Und konkret: Philosophie oder Technologie?

Schwerpunkt 1. Quantenrevolution

- Neue Grundlagen der Physik: Unbestimmtheit, Messprozess und Verschränkung
- Diskussion über Interpretation und Weltbild
- Philosophische Fragen

Schwerpunkt 2. Quantenrevolution

- Technologische Anwendungen
- Quantenphysik als politischer und wirtschaftlicher Faktor
- Soziale, ökonomische, strategische Fragen



Technologie

Philosophie

Bedeutung für den Quantenphysikunterricht

- **Ziel: Vermittlung der Grundlagen von klassischer und quantenphysikalischer Beschreibung**
- **„Demystifizierung“ der Quantenphysik im Rahmen pragmatischer Anwendung**
 - Quantenphysik ist Teil unserer Welt, nicht ein „Alien“

„..... we always have had a great deal of difficulty in understanding the world view that quantum mechanics represents. At least I do, because I'm an old enough man that I haven't got to the point that this stuff is obvious to me. Okay, I still get nervous with it. And therefore, some of the younger students ... you know how it always is, every new idea, it takes a generation or two until it becomes obvious that there's no real problem. It has not yet become obvious to me that there's no real problem.....“

(Feynman 1982)

Akzeptanz der Quantentheorie

- **Eigenschaften der Quantenobjekte charakterisieren**
 - Mathematische Beschreibung interpretieren
- **„Wesenszüge“**
 - Überlagerung/ Interferenzfähigkeit
 - Unbestimmtheit/ Komplementarität
 - Stochastische, eindeutige Messergebnisse
 - (Ausschließliche) Vorhersagbarkeit von Wahrscheinlichkeiten

Quantenphysik als Teil unserer Welt

Nicht gegen die Quantenphysik kämpfen, sondern sie nutzen, d.h. quantenphysikalisch denken:

- **Kryptographie:** Zufall des Messergebnisses für Erzeugung einer perfekten Zufallsfolge nutzen
- **Quantenkryptographie** (Sicherheit der Kommunikation): Auch ein Spion kann die Unbestimmtheit nicht überlisten
- **Quantenteleportation:** nicht messen, sondern verschränken
- **Quantencomputer:** Quantenobjekte gezielt manipulieren mit dem Ziel, die Wahrscheinlichkeit des korrekten Resultats zu erhöhen

Was sollen Schüler:innen über Quantenphysik wissen:

welche Kompetenzen benötigen sie,
um sich mit dieser Entwicklung
auseinandersetzen zu können?

Bildung in Bezug auf Quantentechnologien

- **Allgemeinbildung: Wechselspiel Quantentheorie und Quantentechnologie**
 - Anwendungen, Alltagsbezug (Einordnen von Zeitungsberichten)
- **Berufs-(Zukunfts)orientierung: Grundlagen und Denkweisen**
 - Quantentechnologien als interdisziplinäres Gebiet
 - Zusammenarbeit von Physik, Informatik, Ingenieurwissenschaften, Chemie, ...
 - Vielfältige Kenntnisse und Fähigkeiten erforderlich
 - Hoher Spezialisierungsgrad der einzelnen Beteiligten
 - Ausbildungs- und Studieninitiativen erforderlich

Was sollen die Schüler:innen lernen? - Die Bildungsstandards



Begründung für Quanteninformatik in der Schule

- **Faszinierendes Thema**
- **Quanteninformatik beruht auf den Besonderheiten der Quantenphysik**
 - Dicht an quantenphysikalischen Grundlagen und zentralen Begriffen
- **Quanteninformatik lässt sich mit einfachen Spielzeugsystemen einführen**
 - Nutzung von Zwei-Zustandssystemen
- **Erweiterbar in mehreren Richtungen**
 - Informatische Kompetenz, Philosophische Überlegungen, Technische Realisierung
- **Medienberichte fordern Kommunikationskompetenz heraus**
 - Was kann ein Quantencomputer, was kann er nicht, was unterscheidet klassische und Quantencomputer?

Didaktische Rekonstruktion

- **Zentrale physikalische Inhalte**

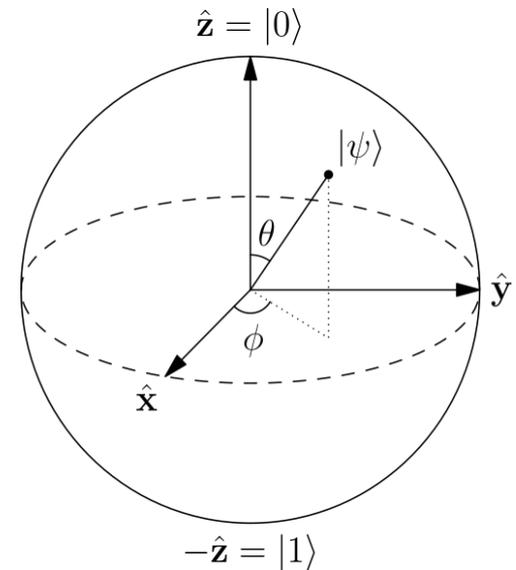
- Überlagerung, Unbestimmtheit, Messprozess, Verschränkung
- „Spielzeugsystem“: Zwei-Zustandssystem Polarisation (als Modell für Spin)
- Bewusste Nutzung von Modellen zur Beschreibung quantenphysikalischer Sachverhalte

- **Lernendenperspektive**

- Starkes Interesse an Anwendungen aus der Quanteninformatik, v. a. Quantencomputer
- Lernschwierigkeiten:
 - Empfinden der Quantenphysik als unanschaulich
 - „position first“-Zugang führt zu inadäquatem Verständnis der Konzepte

Vorteile von Zwei-Zustandssystemen

- **Mathematisch einfach**
 - Zweidimensionaler Zustandsraum, Darstellung auf Blochkugel
 - Diskrete Eigenwerte
- **Physikalisch vielseitig einsetzbar**
 - Übertragbar auf zahlreiche (stark vereinfachte) Beispiele
 - Relevant für aktuelle Anwendungen, v.a. Quantencomputer und Quantenalgorithmen
- **Vorteile für das Lernen**
 - Prinzipien der Quantenphysik klar sichtbar
 - Keine Interferenz mit klassischen Begriffen/ Modellen wie Welle und Teilchen



Quantenkryptographie

Quantenkommunikation als Teil der Quanteninformation



<https://www.faz.net/aktuell/wissen/physik-mehr/internet-4-0-quantencodes-spukten-jetzt-auch-zwischen-peking-und-wien-15227444.html>; Jian-Wei Pan

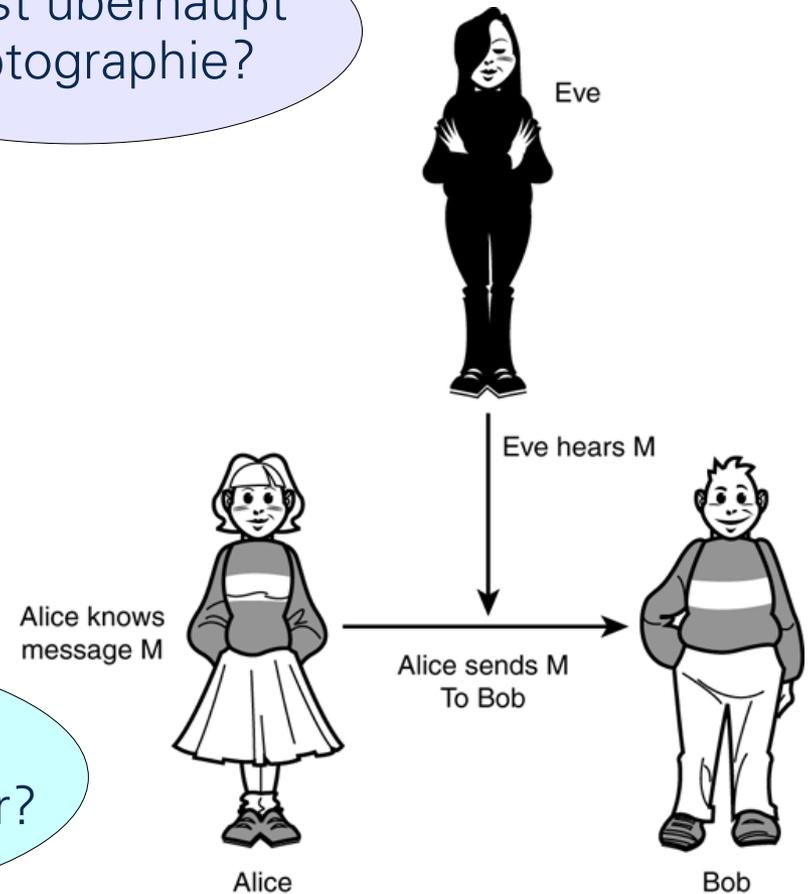
Problemstellung: Wie kann Kommunikation sicher werden?

Können Nachrichten so verschlüsselt werden, dass man ein mögliches Abhören entdeckt?

Was ist überhaupt Kryptographie?

Wie funktioniert Quantenkryptographie?

Warum ist Quantenkryptographie so sicher?



Kryptographie

- **Lehre vom "Verschlüsseln"**
- **One-Time-Pad**
 - Wird nur einmal verwendet
 - Schlüssel ist mindestens so lang wie die Nachricht
- **Bedingungen für sicheres Verschlüsseln**
 - **Schlüssel** ist geheim
 - **Schlüssel** ist zufällig

Es geht um Schlüsselaustausch

QUANTENPHYSIK

A=1=00001, B=2=00010, C=3=00011 etc.

Q	U	A	N	T	E	N
10001	10101	00001	01110	10100	00101	01110
P	H	Y	S	I	K	
10000	01000	11001	10011	01001	01011	

00010	01111	10101	00000	11101	01000	11100
10101	01010	10100	00101	01011	10101	etc.

Aufaddieren von Textziffern und Zufallsfolge nach der Regel: $(0+1=1)(0+0=0)(1+0=1)(1+1=0)$

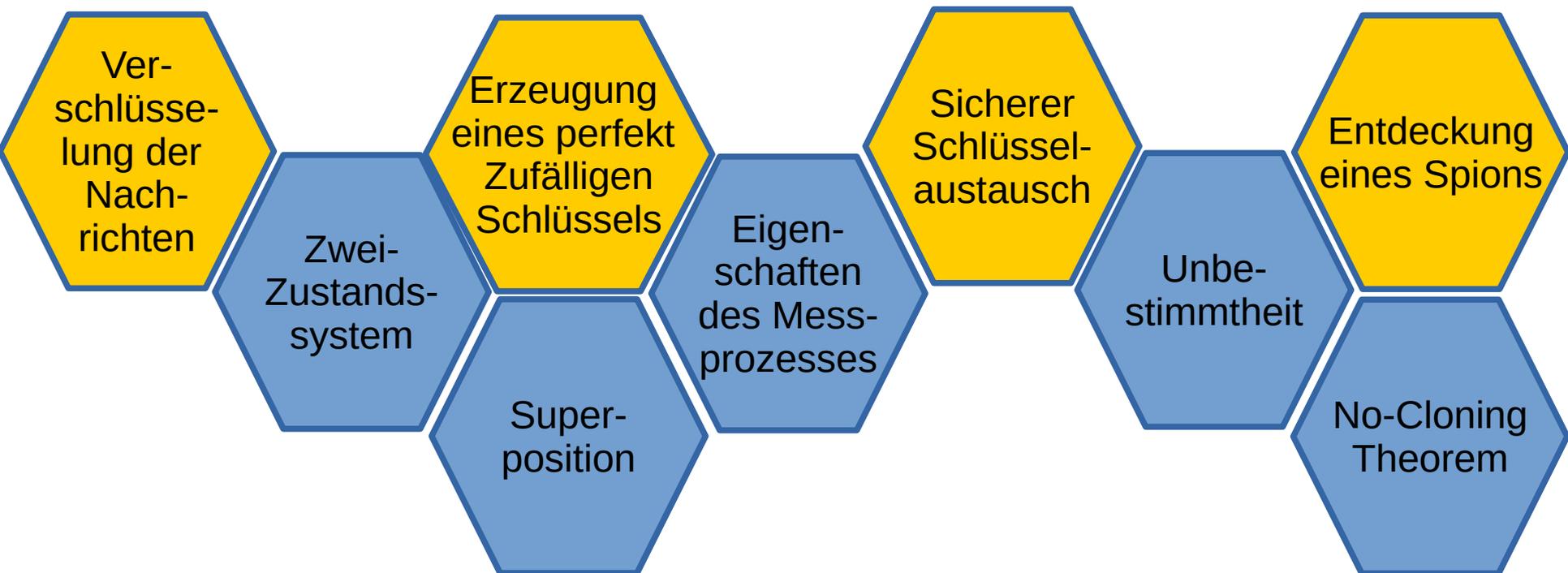
10011	11010	10100	01110	01001	01101	10010
(S	Z	T	N	I	M	R
00101	00010	01101	10110	00010	11110	
E	B	M	V	B	?)	

10001	10101	00001	01110	10100	00101	01110
Q	U	A	N	T	E	N
10000	01010	11001	10011	01001	01011	
P	H	Y	S	I	K	

Verknüpfung von Konzepten und Anwendung



Beispiel Quantenkryptographie



Instrumente und Experimente zur Quantenkryptographie

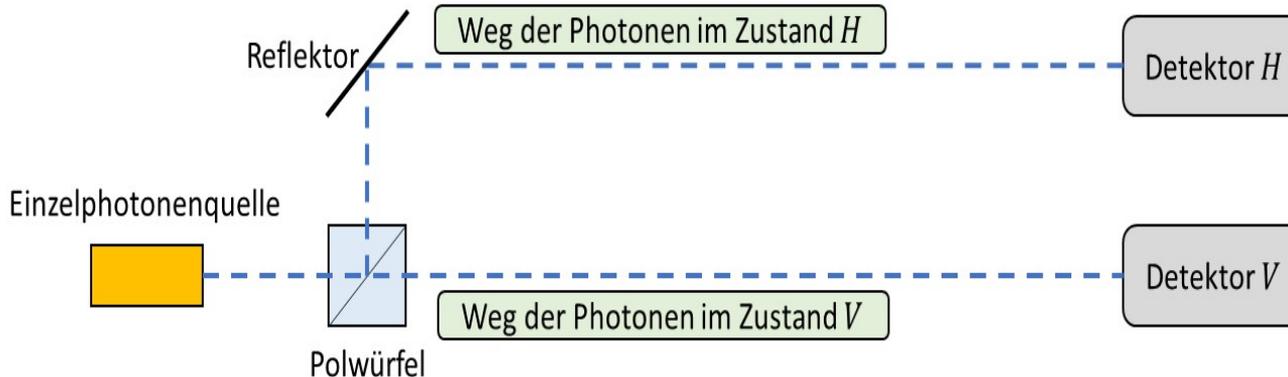
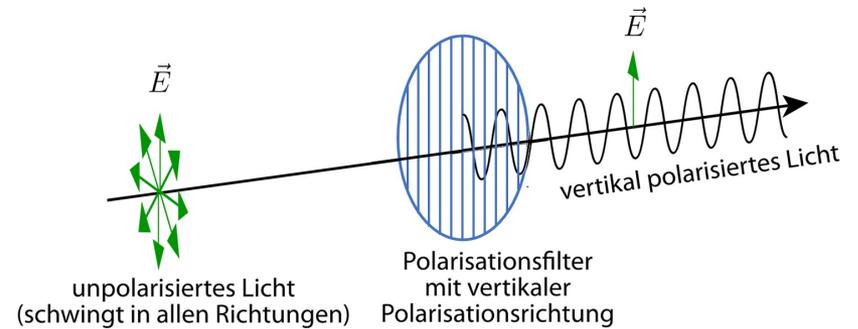


https://www.idquantique.com/quantum-safe-security/products/#quantum_key_distribution

https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=9869

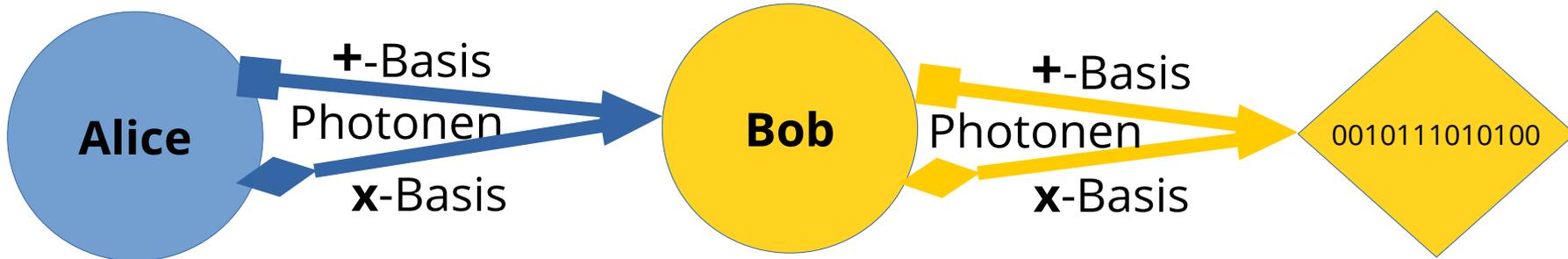
Erzeugung der Zufallsfolge

- **Zwei-Zustandssystem:**
 - Polarisation von Photonen
 - Zwei mögliche Basiszustände
- **Überlagerung nutzen**
- **Messprozess:**
 - Absolut zufällige Ergebnisse
 - Zwei mögliche Messergebnisse



Polarisationszustand	Signal
V	1
H	0

Ablauf des Schlüsselaustauschs



1	+
2	x
3	x
4	+
5	x
6	x
	.

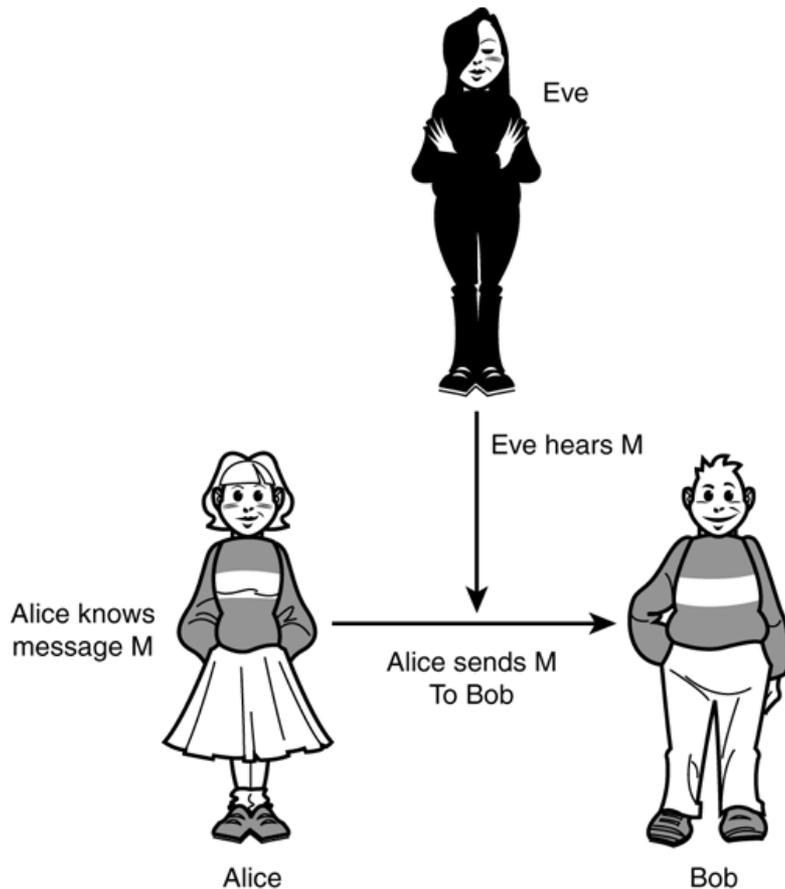
Austausch über öffentlichen Kanal

1	+
2	+
3	x
4	x
5	+
6	x
	.

Schlüssel:

0 _ 1 _ 1

Spion auf der Leitung?



- Eve fängt das von Alice an Bob gesandte Photon ab.
- Was kann sie tun?
 - Sie kann seinen Zustand **nicht** kopieren (No-Cloning-Theorem) und den Austausch abwarten.
 - Sie misst das Photon in einer selbst gewählten Basis und sendet es dann an Bob weiter.

Nutzen der Unbestimmtheit für die Quantenkryptographie (BB84 Protokoll)

Wie kann "Unbestimmtheit" dazu dienen, einen Spion zu finden?

- **Ausgangslage:** Wenn Alice und Bob bei einem Photon die gleiche Basis verwendet haben, sind automatisch auch ihre Messresultate gleich.
- **Bedingung:** Wenn Eve nicht weiß, welche gemeinsame Basis verwendet wurde, wählt sie mit gewisser Wahrscheinlichkeit eine „falsche“ Basis.
 - No-Cloning-Theorem verhindert grundsätzlich Wissen um gemeinsame Basis
- **Folgerung:** Die zwischengeschaltete Messung durch Eve bewirkt, dass die Messresultate von Alice und Bob nicht mehr immer übereinstimmen
- **Abwehr:** Alice und Bob vergleichen einen Teil (ca 10-20%) ihrer Messresultate.

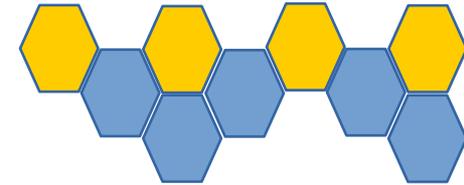
Metapher zur Unbestimmtheit bei Quantenobjekten

Ein Bauer hat eine Herde mit **weißen und schwarzen Kühen und Pferden**. Diese möchte er jetzt zählen. Er treibt alle Tiere durch ein Doppel-Gatter: Links können nur die **Kühe**, rechts nur die **Pferde** hindurchgehen. In einem zweiten Schritt bringt er die **Pferde** unwiderruflich weg und sortiert danach die **Kühe** der **Farbe** nach, um eine Herde mit **weißen Kühen** zu erhalten. Nun möchte er sich vergewissern, daß er richtig sortiert hat, schaut nach, indem er nur die **weißen Kühe** wieder durch das Doppel-Gatter schickt, und entdeckt plötzlich **Pferde** darunter.

Einführung der Quantenkryptographie – Piloterprobung

- **Konzeption und Planung**

- Konzeption entlang des beschriebenen Interlacing
- Anknüpfen an klassische Kryptographie
- Berücksichtigung der Akzeptanzbefragung zur Dirac-Notation



- **Ergebnisse**

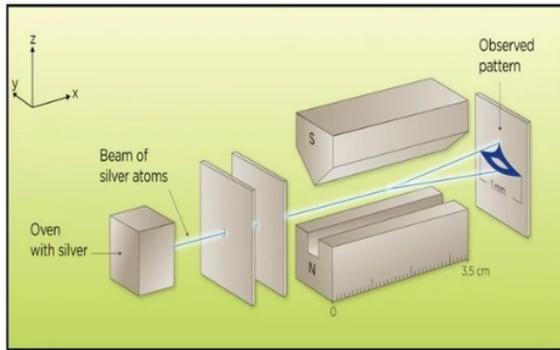
- Auch Interesse an technischer Realisierung
- Verständnis von Unbestimmtheit und Messprozess benötigt mehr Zeit als zuvor geplant
- Kleinschrittiges Vorgehen wichtig, keine Probleme mit der Mathematisierung

Mittel zur Umsetzung

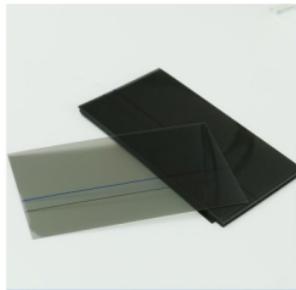
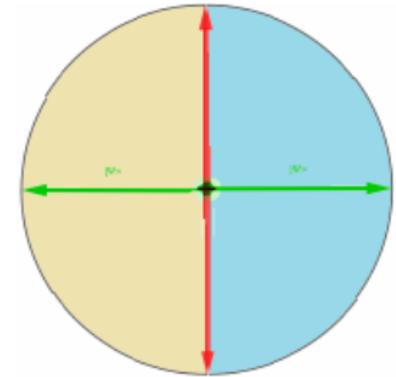
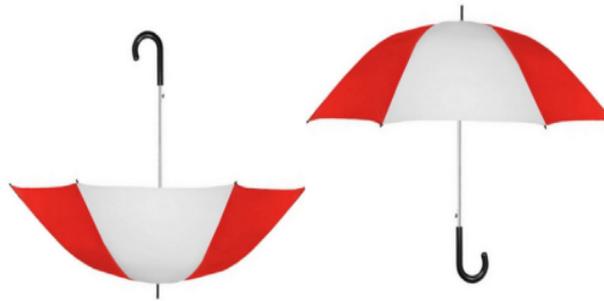
Nutzung von Modellen

- **Modelle, Analogien, Metaphern**
 - Modelle beschreiben oder veranschaulichen
 - Analogien (innerhalb der Physik) verfügen über ähnliche (physikalische oder mathematische) Strukturen
 - Metaphern nutzen Vergleiche aus physikfremden Bereichen
- **Konkret: Polarisation als Analogie zum Spin**
 - Blochkugel resp. Blochkreis eigentlich zur Beschreibung der Polarisation eingeführt, wird für Beschreibung des Spins und des Q-Bits verwendet

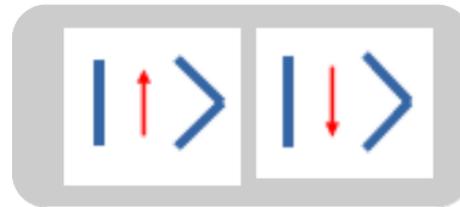
Repräsentationen – von gegenständlich bis mathematisch



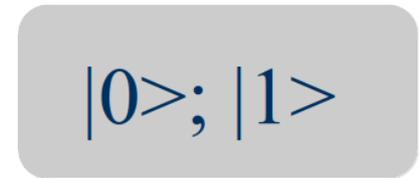
<https://www.mdpi.com/1099-4300/19/5/186/html>
by Håkan Wennerström and Per-Olof Westlund



Gedanken- oder
Analogieexperiment

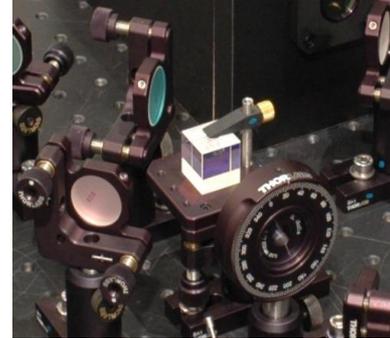


Symbolisch-bild-
liche Darstellung



Symbolisch-mathe-
matische Darstellung

Simulationen

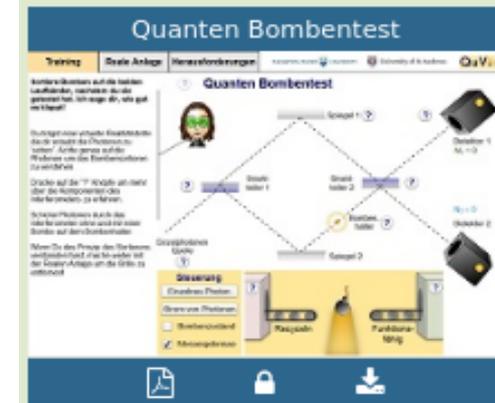
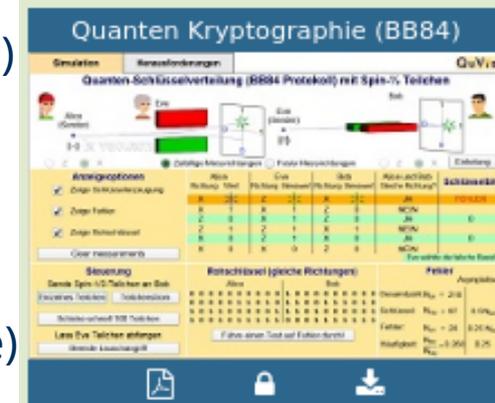
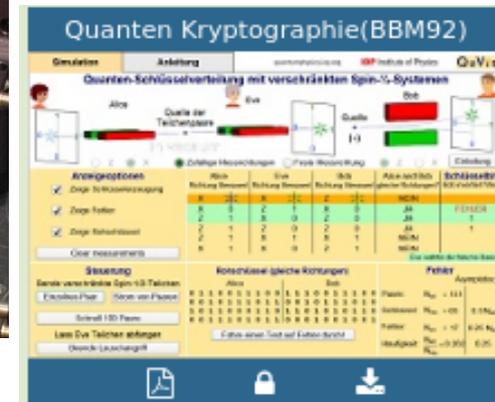


- **Typen von Simulationen**

- Interaktive Bildschirmexperimente (www.quantumlab.de)
- Simulationen in einer symbolischen Darstellung (<https://www.st-andrews.ac.uk/physics/quvis/>)

- **Einbettung von Simulationen mit Tutorials (A. Kohnle)**

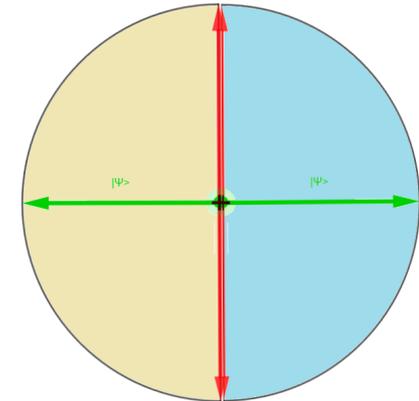
- Vertrautmachen mit der Simulation
- Systematisch mit der Simulation arbeiten
- Aufgaben bearbeiten und Probleme lösen



Einführung der Dirac-Notation – Akzeptanzbefragung

- **Inhalt des Kurses**

- Einführung der Schreibweise und Rechenregeln
- Veranschaulichung mit Hilfe des Blochkreises (Verzicht auf komplexe Zahlen)
- Einführung Wahrscheinlichkeit und Messprozess
- Ausblick: No-Cloning-Theorem



- **Durchführung der Befragung**

- Teilnahme: Wenige Schüler:innen aus Klassenstufe 10-12
- Jeweils alleine oder zu zweit

$$\alpha|\uparrow\rangle + \alpha|\downarrow\rangle = |\rightarrow\rangle$$

ODER:

$$\alpha|\rightarrow\rangle + \alpha|\leftarrow\rangle = |\uparrow\rangle$$

Müller, Christian 2019: Planung Einer Unterrichtseinheit Zur Quantenkryptografie Und Akzeptanzanalyse Der Dirac-Notation. Wissenschaftliche Abschlussarbeit, TU Dresden.

Wichtigste Ergebnisse der Akzeptanzbefragung

- **Visualisierungen wichtig und hilfreich**
 - Darstellung am Blochkreis wird gut akzeptiert
 - Darstellung mit Hilfe von Koordinatensystemen dient zur konkreteren Vorstellung
- **Berechnungen mit der Notation**
 - Schreibweise als eingängig empfunden
 - Kleinschrittiges Vorgehen und Üben ist notwendig
 - Wichtig: Wiederholung von Rechenregeln für das Rechnen mit Klammern
 - Umgang mit dem Blochkreis fiel Schüler:innen aus 10. Klasse leichter als älteren Schüler:innen

Ausblick

Quantenphysik und Allgemeinbildung

- **Technologiebildung zusammen mit Allgemeinbildung gedacht**
- **Jenseits der Mystifizierung**
 - Klärung grundlegender Begriffe: **Superposition, Unbestimmtheit, Verschränkung** sowie **Messprozess**
 - Interpretation und Nutzung der mathematisch-physikalischen Beschreibung
 - Systematische Nutzung des Modellbegriffs
- **Beschreibung des Messprozesses**
 - Kern der Unvereinbarkeit von klassischer und Quantenphysik
 - Teil-Erläuterung durch Dekohärenz

Mögliche Unterrichtsstruktur zum Quantencomputer

