TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Physik, Professur Didaktik der Physik

Quanteninformation als Zugang zur Quantenphysik in der Schule

Gesche Pospiech, TU Dresden

Motivation

- **Quanteninformation ist aktuelles Thema**
- **Wesentliche Fakten der Quantenphysik werden angesprochen**
  - Superpositionsprinzip
  - Unbestimmtheit (resp. Unschärferelation)
  - Messprozess
  - ev. auch Verschränkung
- **Unterschiede zur klassischen Physik werden deutlich**

Zentrale Diskussionspunkte der Quantentheorie

- **Nicht-Determinismus**
- **Superposition**
- **Unbestimmtheit - Komplementarität (1927)**
  - Heisenberg, Bohr und Einstein auf der Suche nach einer Interpretation und Veranschaulichung der Quantentheorie
- **Verschränkung (1935)**
  - Begriff wurde von Schrödinger auf der Suche nach den Folgerungen aus der physikalischen Theorie geprägt

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 Quanten-kryptographie 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	?)	

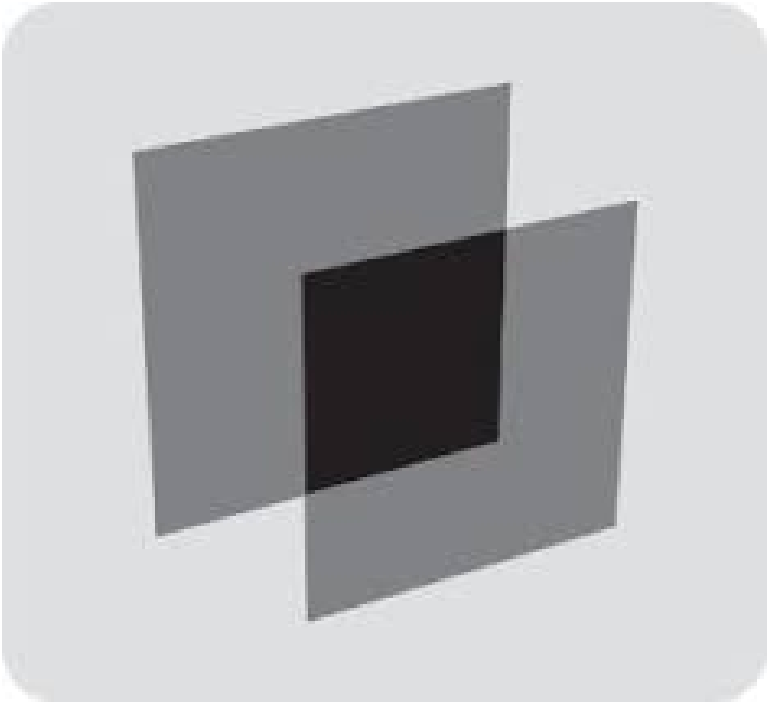
10001	10101	00001	01110	10100	00101	01110
Q	U	A	N	T	E	N
10000	01010	1100110011		01001	01011	
P	H	Y	S	I	K	

Quantenkryptographie

- **Es gibt bereits kommerzielle Geräte zur Quantenkryptographie**
- **Auch Lehrmittelfirmen fangen an, Lehrgeräte zu entwickeln, die sich dazu eignen, die Quantenkryptographie zumindest modellhaft in Experimenten zu demonstrieren**

Arbeiten mit Analogien und Modellexperimenten

- **Wir arbeiten nicht mit einzelnen Photonen, sondern mit “normalem” Licht oder Laser**
- **Damit lassen sich die Prozesse annähernd nachvollziehen**
- **Die hierzu wesentliche Eigenschaft des Lichts ist die Polarisation**



Element 0: Nachweis von Photonen

Experimental Evidence for a Photon Anticorrelation Effect on a Beam Splitter: A New Light on Single-Photon Interferences.

P. GRANGIER, G. ROGER and A. ASPECT (*)
Institut d'Optique Théorique et Appliquée, B.P. 43 - F 91406 *Orsay, France*

(received 11 November 1985; accepted in final form 20 December 1985)

When it comes to single-photon states of light, it is tempting to revisit the famous historical «single-photon interference experiments» [8]. One then finds that, in spite of their denomination ([1]), none has been performed with single-photon states of light. As a matter of fact, all have been carried out with chaotic light, for which it is well known that quantum second-order coherence properties cannot be distinguished from classical ones, even with a strongly attenuated beam [9]. This is why we have carried out an interference experiment with the same apparatus as used in the first experiment, *i.e.* with light for which we have demonstrated a property characteristic of single-photon states. This single-photon interference experiment is described in the second part of this letter.

([1]) Usually, the single-photon character is stated by showing that the amount of energy flowing during a certain characteristic time (coherence time, or time of flight between source and detector) is small compared to $h\nu$. The necessity of the concept of photon is thus postulated, probably on the basis that the detection process appears discrete. But it is well known that this argument is not fully conclusive, since all the characteristics of the photoelectric effect can be assigned to the fact that the «atomic detector is controlled by the laws of quantum mechanics» (see ref. [1], or: W. E. LAMB and M. O. SCULLY, in *Polarisation, Matière et Rayonnement*, ed. Société Française de Physique, Presses Universitaires de France, 1969).

Wie nutzt Quantenkryptographie die Eigenschaften der Quantentheorie?

- **Erzeugung von Schlüsseln**
  - Element 1: Nichtdeterminismus - Messprozess
  - Element 2: Superposition
- **Entdecken eines Spions**
  - Element 3: Unbestimmtheit
  - Element 4: Verschränkung

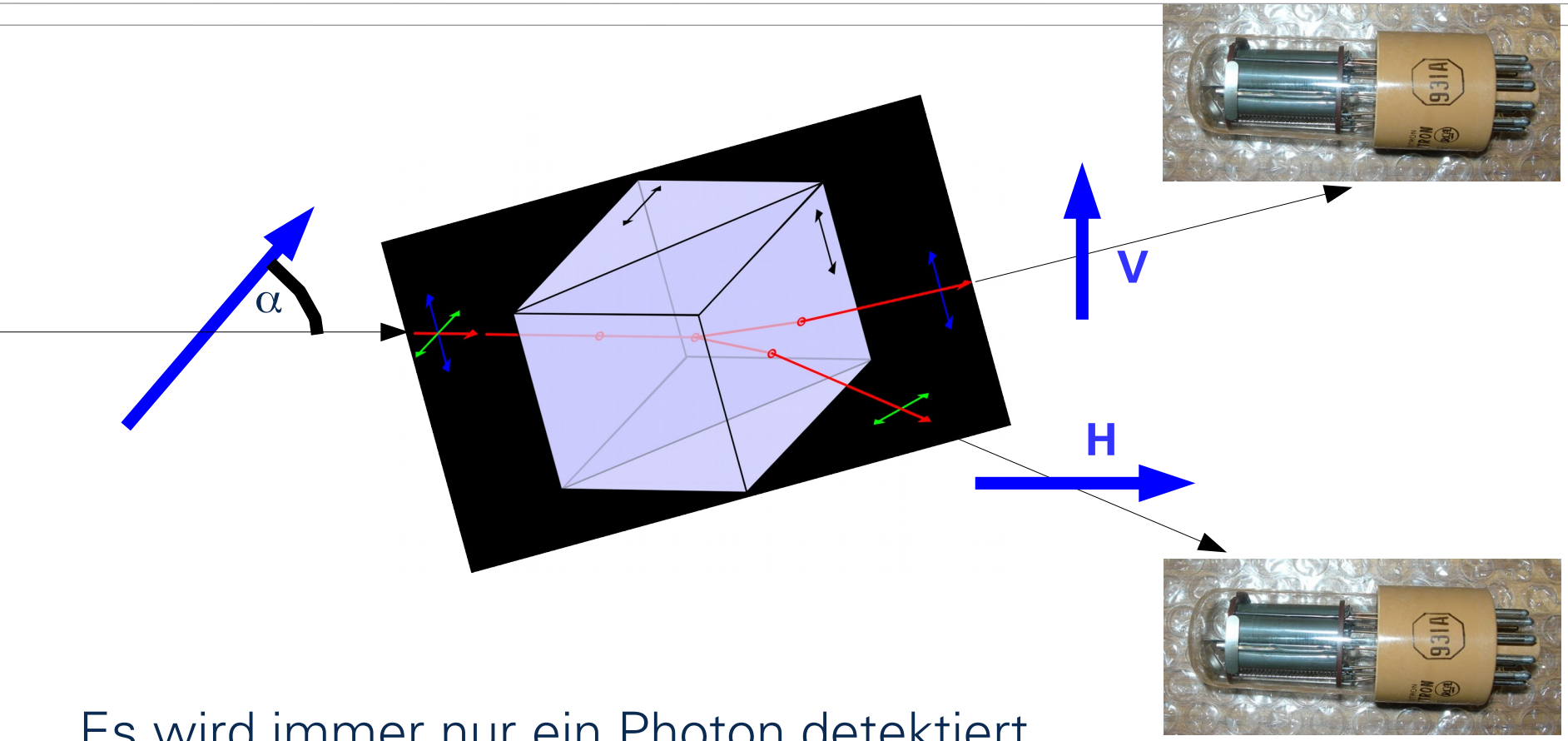
TECHNISCHE UNIVERSITÄT DRESDEN

Erzeugung und Austausch eines Quantenschlüssels

Element 1: Quantentheorie liefert perfekte Zufallsfolgen

- **Licht hat die Eigenschaft “Polarisation”. Diese kann man ohne großen Fehler auch einzelnen Photonen zuschreiben.**
  - Nicht polarisiertes Licht, z. B. einer Glühlampe, kann mit Hilfe von Polarisationsfiltern in einer festen Richtung polarisiert werden.
- **Photonen treten einzeln und quantenhaft auf.**
- **Es wird – je nach Messung – immer nur eines entweder registriert oder nicht registriert.**

Basiszustände von Photonen



Es wird immer nur ein Photon detektiert,
entweder im Zustand **H** oder **V**:

- Wenn α = 0° oder 90°: immer **H** oder **V**
- Wenn α = 45°: perfekte Zufallsfolge

Element 2: Möglichkeit von Zufallsfolgen beruht auf der Superposition

- **Jeden Polarisationszustand eines Photons kann man mit zwei Basiszuständen beschreiben**

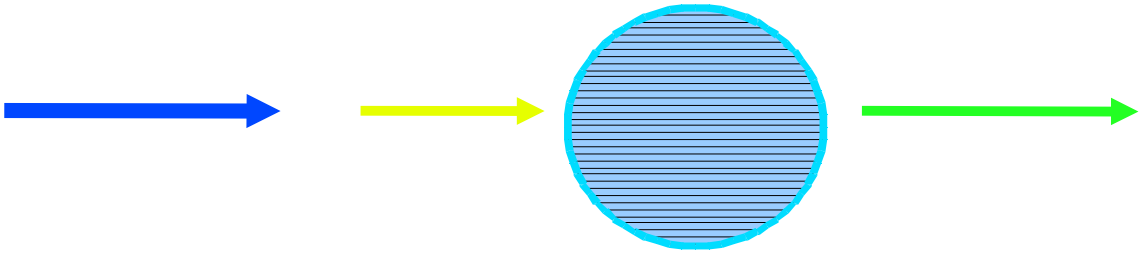
  *Basiszustände des Photons = horizontal polarisiert **(H)*** **oder** *vertikal polarisiert **(V)***

- **Eine Superposition der Basiszustände (H, V) führt zum Begriff des Q(uanten)-bit**

Wie messen wir die Überlagerung?

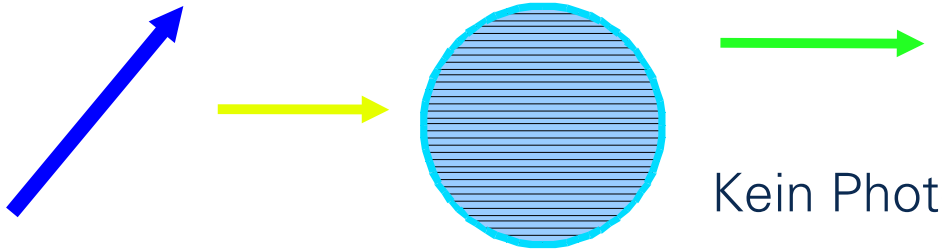
- Messapparat und Objekt sind im gleichen (Basis)Zustand

► Das Ergebnis steht mit Sicherheit fest:



- Messapparat ist in Basiszustand, Objekt nicht:

► Das Ergebnis kann nicht vorhergesagt werden.



Nur Wahr-
scheinlichkeit
angebbar

Das Superpositionsprinzip

Mathematische Beschreibung:
Vektorraumstruktur;
Zustände werden durch Vektoren beschrieben.

Graphische Darstellung:
Nutzung von Pfeilen, graphische Addition

ψ **= Spalt 1 + Spalt 2**

Verbale Umschreibung:
Überlagerung von Möglichkeiten, Gleichzeitig in 2 Zuständen

Metapher:
"Katalog der Möglichkeiten"

Quintessenz für die Schüler

- **Quantenphysik liefert nicht-deterministische Messergebnisse**
- **Zustände von Quantenobjekten (wie z. B. Photonen) können durch Überlagerung von Basiszuständen dargestellt werden**
- **Man kann den Messprozess als eine “Projektion” darstellen.**
- **Im Messprozess verändert das Quantenobjekt seinen Zustand**

Nutzen für Quantenkryptographie

- **Quantenschlüssel ist eine absolut zufällige Folge von Quanten-Bits in einem der Basis-Zustände**
- **Diese werden mit (H ; V) oder (0 ; 1) bezeichnet**
- **Weil eine wiederholte Messung den gleichen Zustand ergibt, kann der Schlüssel zwischen Alice und Bob ausgetauscht werden**

H, H, V, H, V, V, V, V, ..

TECHNISCHE UNIVERSITÄT DRESDEN

Wie entdeckt man einen Spion?

Element 3: Quantenphysik hilft beim Entdecken eines Spions

- **Aus den Eigenschaften der Quantenphysik ergibt sich ein mögliches Vorgehen, ein sog. Protokoll**
- **Das erste solcher Protokolle war BB84:**
  - Charles Bennett und Gilles Brassard haben es 1984 entwickelt.
  - Beruht auf Unbestimmtheit
- **Alternative: Ekert91 (EK91)**
  - Von Arthur Ekert 1991 entwickelt
  - Beruht auf Verschränkung, d.h. arbeitet mit Photonen-Paaren

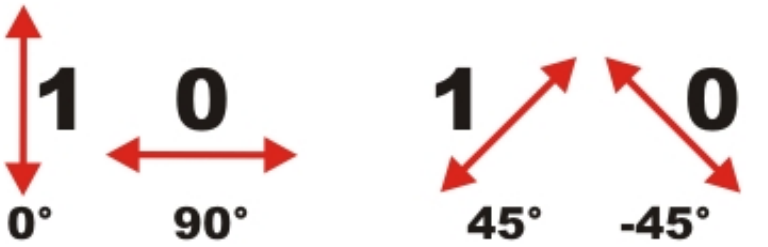
Wie nutzt das BB84-Protokoll die Unbestimmtheit?

Relevante Eigenschaft: Unbestimmtheit des Spins

- **Verhalten von Spins bei auf einander folgenden Messungen verschiedener Komponenten des Spins, z.B. σ_x und σ_z ist unbestimmt.**
- **Klassische Anordnung eines Gedankenexperiments:**
  - Drei hintereinander geschaltete Stern-Gerlach-Apparaturen
  - Gegeneinander gedrehte Messungen: ***x – z – x***

Zwei Eigenschaften – zwei Polarisationsbasen – Unbestimmtheit

- **Polarisation ist ein Modell für den Spin**
- **Zwei physikalische Eigenschaften des Spins von Photonen werden durch zwei verschiedene Basen der Polarisation dargestellt.**
  - Eigenschaft 1 (Basis 1): horizontal **(H)** oder vertikal **(V)**
  - Eigenschaft 2 (Basis 2): diagonal+ **(D+)** oder diagonal- **(D-)**



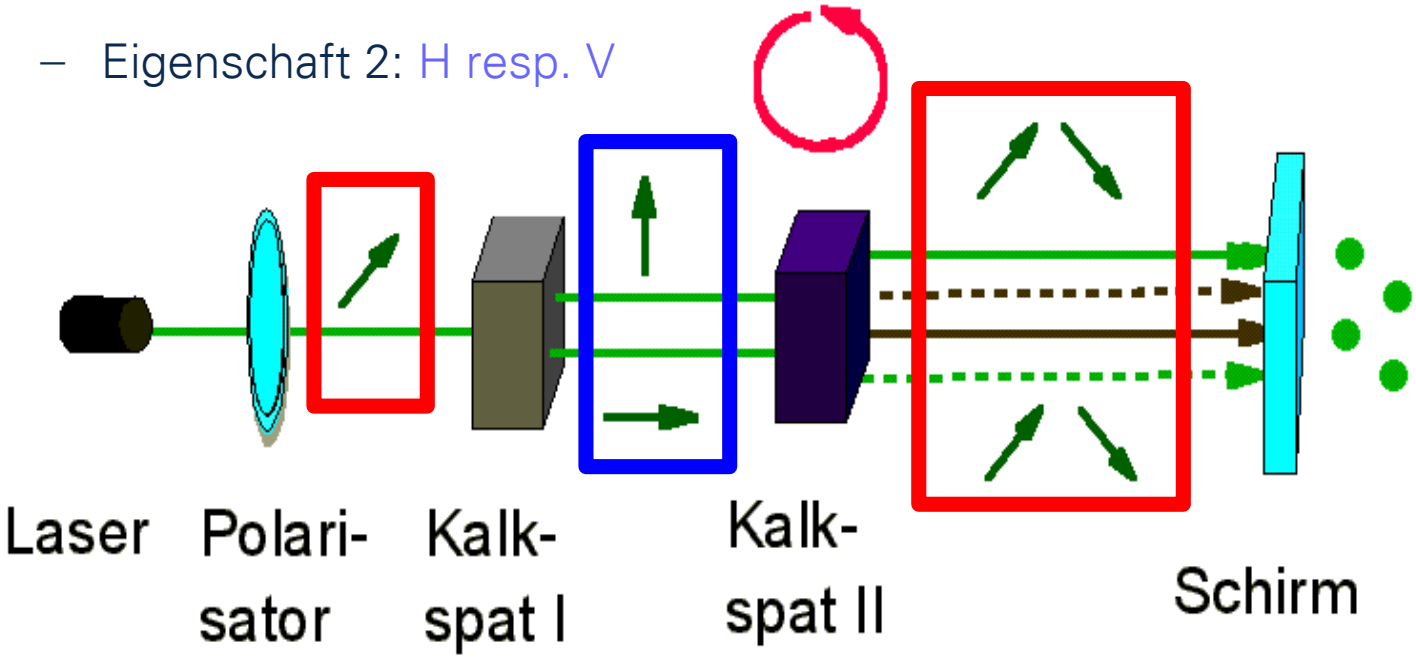
Eigenschaft1 Eigenschaft 2

Wichtig: Wir stellen uns einzelne Photonen vor.

Was bedeutet Unbestimmtheit – ein Modell-experiment

Man stelle sich einzelne Photonen mit einer jeweils festen Polarisationsrichtung vor.

- Eigenschaft 1: D+ resp. D-
- Eigenschaft 2: H resp. V



Quintessenz für Schüler: Unbestimmtheit

- **Quantenobjekte haben nicht feste Werte für alle ihre Eigenschaften.**
  - Beispiele: Ort und Impuls, Spin-Komponenten
  - Hierfür gibt es eine eindeutige mathematische Regel. (Kommutator verschwindet nicht)
  - **Vorstellung**: Es gibt nur dann feste Werte für zwei Eigenschaften zugleich, wenn diese in einem **gemeinsamen** Messgerät gemessen werden können.
- **Ein fester Wert für eine Eigenschaft *entsteht* erst in einem Messprozess.**

Die Unbestimmtheit

Mathematische Beschreibung:
Zwei Operatoren vertauschen nicht.

Experimenteller Effekt:
Stern-Gerlach-Experimente
Quantenradierer

Verbale Umschreibung:
Zwei Eigenschaften existieren nicht gemeinsam (mit festen Werten)

Metapher:
s. Beispiel

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.

Nutzen der Unbestimmtheit für die Quantenkryptographie

Wie kann “Unbestimmtheit” dazu dienen, einen Spion zu finden?

- **Unbestimmtheit wird zugleich genutzt und ausgeschaltet.**
- **Entscheidende Phase ist der Quantenschlüsselaustausch mit Quantenkanal und klassischem Kanal**
- **Dieses spezielle Vorgehen wird im BB84 Protokoll beschrieben**

BB84-Protokoll – ohne Spion

- Alice erzeugt einen Quantenschlüssel, d. h. eine Serie von 0 und 1, erzeugt durch Messergebnisse bezüglich der + oder x Basis
- Alice sendet die so präparierten Photonen an Bob (Quantenkanal)
- Bob misst diese in zufälliger Reihenfolge in + oder x Basis
- Beide führen Buch: sie registrieren die Nummer des Photons, die Basis und das Resultat
- Beide kommunizieren (öffentlich): Nummer und Basis, aber keinesfalls das Resultat (klassischer Kanal)
- Die Nummern mit gleicher Basis ergeben den Schlüssel. Warum?

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Alice Basis	+	+	+	x	+	x	x	+	+	x	x	x	+	x	+	x	+	x	x	+
Alice Resultat	1	0	1	1	1	0	1	0	1	0	0	0	1	0	1	1	0	1	0	1
Bob Basis	x	+	+	x	x	+	x	+	+	+	x	+	x	x	x	x	+	+	x	+
Bob Resultat	0	0	1	1	1	1	1	0	1	0	0	1	1	0	1	1	0	1	0	1
Schlüssel	-	0	1	1	-	-	1	0	1	-	0	-	-	0	-	1	0	-	0	1
Eve Basis																				
Eve Resultat																				
Ver-gleich																				

Wie ändert sich das Bild, wenn ein Spion „Eve“ eingreift?

Spion auf der Leitung?

- Eve fängt das von Alice an Bob gesandte Photon ab.
- Sie kennt die von Alice verwendete Basis nicht, muss also raten
- Sie misst das Photon selber und sendet es dann an Bob weiter

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Alice Basis	+	+	+	x	+	x	x	+	+	x	x	x	+	x	+	x	+	x	x	+
Alice Resultat	1	0	1	1	1	0	1	0	1	0	0	0	1	0	1	1	0	1	0	1
Bob Basis	x	+	+	x	x	+	x	+	+	+	x	+	x	x	x	x	+	+	x	+
Bob Resultat	0	0	1	1	1	1	1	0	1	0	0	1	1	0	1	1	0	1	0	1
Schlüssel	-	0	1	1	-	-	1	0	1	-	0	-	-	0	-	1	0	-	0	1
Eve Basis	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Eve Resultat	1	0	1	0	1	1	0	0	1	1	1	0	1	1	1	0	0	0	0	1
Ver-gleich	-	j	j	n	-	-	n	j	j	-	n	-	-	n	-	n	j	-	j	j

Analyse der Ergebnisse

- **Situation**
  - Wenn ein Spion die Photonen abfängt, misst und erst dann weitersendet, wird es einen Anteil unterschiedlicher Resultate zwischen Bob und Alice geben
- **Finden eines Spions**
  - Von den ausgewählten Nummern gleicher Basis wählen Alice und Bob eine zufällige Stichprobe von ca 10% - 25 % aus.
  - Überprüfen (auch öffentlich) ihre Resultate (dieser Teil des Schlüssels wird nicht verwendet.)
  - Stimmen die Resultate überein: wahrscheinlich kein Spion;

    gibt es Abweichungen: es gab einen Spion

TECHNISCHE UNIVERSITÄT DRESDEN

Warum kopiert der Spion nicht einfach den Zustand?

Quantenphysik unterscheidet sich fundamental von klassischer Physik

- **In der Quantentheorie gilt das sog. No-Cloning-Theorem:**

  Beliebige Zustände lassen sich nicht exakt kopieren
- **Formulierung:** Es gibt keinen quantenmechanischen Vorgang, der einen Zustand kopiert, indem er ihn auf einen "leeren" Zustand transferiert.

  W.K. Wootters and W.H. Zurek, Nature 299, 802 (1982)

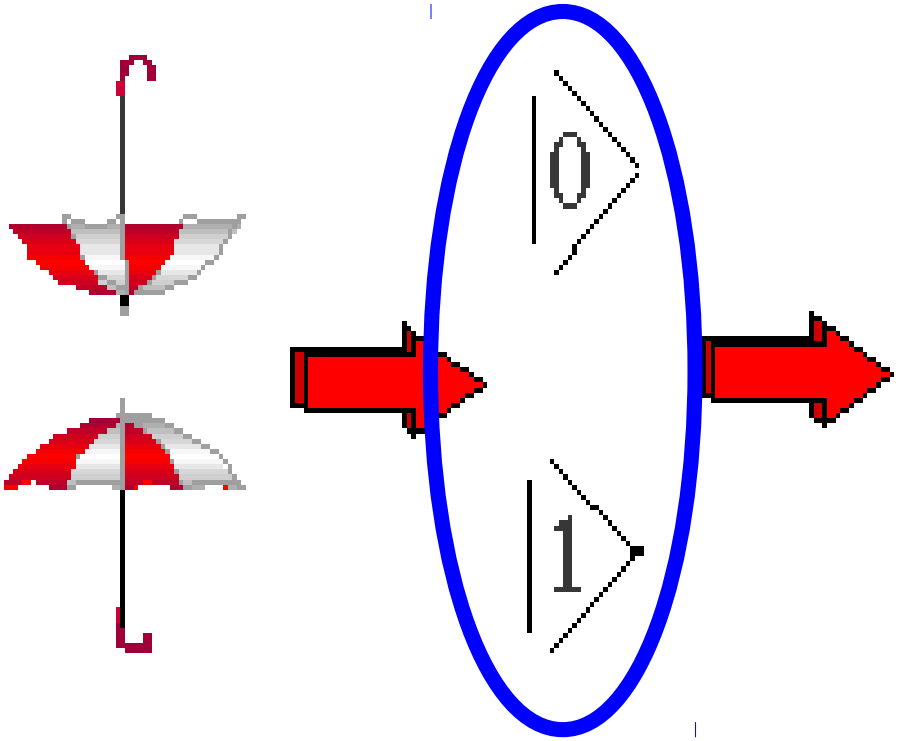
Dies lässt sich nur mit Hilfe von Formalisierung wirklich einsehen.

Darstellung in Dirac-Notation

- **Dirac-Notation als symbolische Schreibweise für Zustände einführen**
  - Verkürzt die Darstellung
  - Vereinfacht die Kommunikation
  - Man kann mit Schreibregeln arbeiten
- **Erlaubt, Systeme aus mehreren Quantenobjekten darzustellen**

Modellierung eines 2-Zustandssystems

Von der Veranschaulichung zur formalen Modellierung



$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

oder:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Beweis des No-cloning Theorems

Grund: Linearität der Quantentheorie

- Aktion des Kopierers: $\mathbf{U}\,|0\rangle\,|i\rangle = |0\rangle\,|0\rangle$, und $\mathbf{U}\,|1\rangle\,|i\rangle = |1\rangle\,|1\rangle$
- Beliebiger Zustand: $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, mit $|\alpha|^2 + |\beta|^2 = 1$
- Wirkung des Kopierers: $\mathbf{U}|\psi\rangle\,|i\rangle = \mathbf{U}\,(\alpha|0\rangle + \beta|1\rangle)\,|i\rangle$

  $= \alpha|0\rangle\,|0\rangle + \beta|1\rangle\,|1\rangle$
- Verschieden von $\neq \quad |\psi\rangle\,|\psi\rangle$

Problembeantwortung

- **Ja, Nachrichten können mit Hilfe von Quantenschlüsseln sicher verschlüsselt werden.**
- **Mit Hilfe der quantenphysikalischen Unbestimmtheit und dem BB84-Protokoll kann man einen Spion entdecken**
- **Also ist im Prinzip die Verschlüsselung auf Basis der Quantenphysik sicher, sicherer als in der klassischen Kryptographie.**

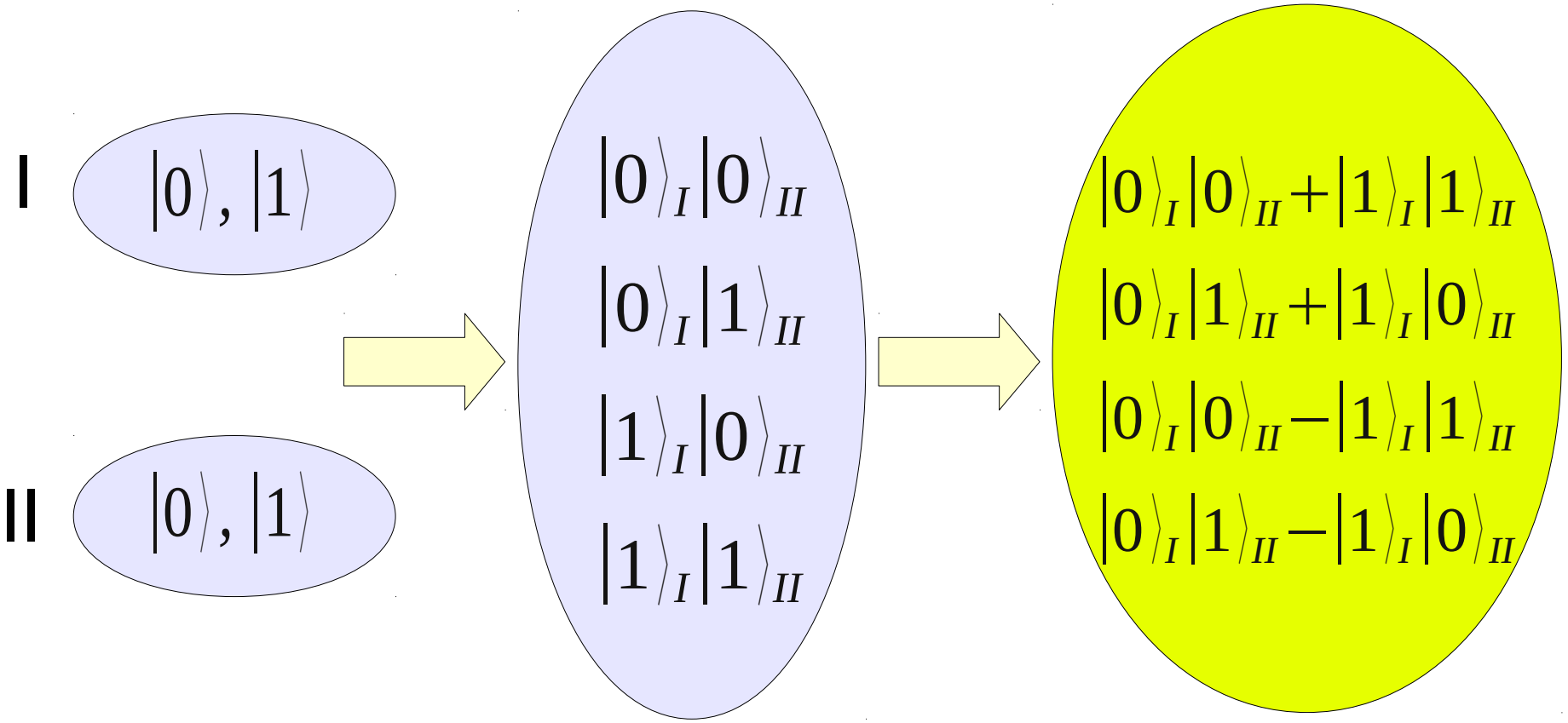
Aber: Die technische Realisierung ermöglicht Schlupflöcher. Diese und Schutzmaßnahmen werden im Moment aktiv erforscht.

Quintessenz

- **Die Linearität der Quantentheorie ist zentral für die mathematische Beschreibung**
- **Aus der Linearität folgen**
  - Superpositionsprinzip
  - Unbestimmtheit
- **Messprozess ergibt zufällige Werte**
- **Bei der Quantenkryptogrpahie greifen diese Eigenschaften ineinander**

Und die Verschränkung?

Element 4: Verschränkung - Zwei Photonen sind noch kein Diphoton



Beschreibung von Verschränkung

- **Charakterisierung: Verschränktes System**
  - Es ist nicht möglich, in einem zusammengesetzten System aus zwei (oder mehr) Quantenobjekten Aussagen nur über ein Teilsystem zu machen.

    Insbesondere beeinflusst auch eine Messung an einem Teilsystem immer das gesamte System
- **Verdeutlichung:**
  - Klassisch: bei einer in zwei Teile zerplatzenden Kugel kann man Aussagen immer über Ort und Impuls beider Teile machen, auch wenn man nur einen Teil kennt.
  - Quanten: Bei Aussagen über den Impuls sind keine Aussagen über den Ort möglich oder Bei Aussagen über Impuls des einen und Ort des anderen Teils verschwinden Aussagen über die jeweils andere Größe (EPR-Situation)

Die Verschränkung

Mathematische Beschreibung:
Ein zusammengesetztes System lässt sich nicht als Produkt seiner Teilsysteme schreiben.

Experimentelle Effekte:
z.B. EPR-Experiment
Teleportation

Verbale Umschreibung:
Zwei (oder mehr) Quantenobjekte sind miteinander verschränkt, wenn sie nur als ein Ganzes beschrieben werden können.

Metapher:
Schrödingers Katze
Schrödingers Schüler und Lehrer

Was bedeutet Verschränkung für Quantencomputer?

- **Vorteile:**
  - Natürliche Parallelität wegen der Verschränkung
- **Nachteile:**
  - Zufällige Messergebnisse
- **Probleme:**
  - Unbestimmtheit
  - No-Cloning-Theorem
  - Dekohärenz

Grundprinzip eines Quantencomputers

- Reversible Algorithmen
- Q-Bits “kondensieren” Information durch die Superposition (“dense coding”)
- Q-Bits lassen sich verschränken → n Q-Bits können 2^n Bits kodieren
- Beliebig viele verschränkte Q-Bits lassen sich in einem einzigen Schritt manipulieren

Mögliche Realisierung von Quantencomputern

- **Anforderungen**
  - Systeme mit 2 Basiszuständen; Quantenbits
  - Skalierbar zu vielen Bits
  - Fehlertolerant manipulierbar
  - Passende Algorithmen
- **Kandidaten**
  - Josephson-Kontakte → momentan am aktivsten verfolgt
  - Ionen-Fallen
  - Spin-Qbits: Transistorenähnlich, mit Einzelelektronen

Kann ein Quantencomputer helfen, Batterien zu entwickeln?

- **Bekannte Algorithmen**
  - Deutschalgorithmus: “Orakel”, Auswertung einer binären Funktion
  - Deutsch-Josza-Algorithmus: Erweiterung auf n Entscheidungen
  - Grover-Algorithmus: Suche in unstrukturierten Datenbanken
  - Shor-Algorithmus: Quanten-Fourier-Transformation; kann eingesetzt werden, Primfaktoren großer Zahlen zu finden
  - Quantensimulation von Molekülen und Materialien

Vielen Dank für die Aufmerksamkeit!

Dank an meinen Mitarbeiter:
Matthias Schöne

TECHNISCHE UNIVERSITÄT DRESDEN

Literatur

Heusler, S. (2010). Quantendimensionen: Doppelspalt, Verschränkung, Quantencomputer. DVD-ROM für PC und Mac. Klett.

Pospiech, G. (1999a). Quantenkryptographie. Ein elementarer Zugang zur Quantentheorie. Physik in der Schule, 37(3), 201–205.

Pospiech, G. (1999b). Quantenteleportation - nutzbar zur Informationsübertragung. Physik in der Schule, 37(6), 420–424.

Pospiech, G. (1999c). Spukhafte Fernwirkungen der Quantentheorie? Eine Darstellung der Quantentheorie mit Gedankenbildern. Physik in der Schule, 37(1), 56–59.

Pospiech,G. (2000)., *Quantencomputer - Was verbirgt sich dahinter?,* Der Mathematisch-Naturwissenschaftliche Unterricht, 4/2000 (53), S. 196-202

Pospiech, G. (2016). Quantenphysik intuitiv – das GHZ-Spiel. Praxis der Naturwissenschaften - Physik in der Schule, 65(1), 33–36.

Pospiech, G., & Schorn, B. (2016). Der Quantencomputer in der Schule. Praxis der Naturwissenschaften - Physik in der Schule, 65(1), 5–11.

Link: www.quantumlab.debvb