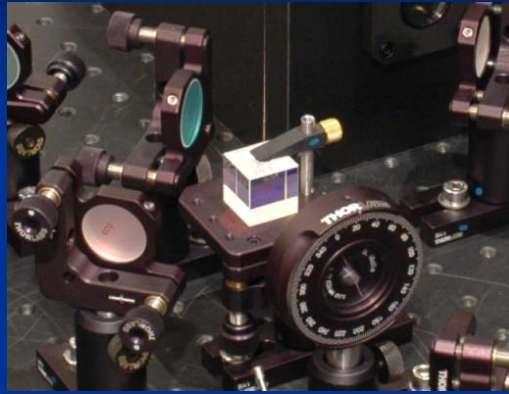


# Quantenkryptographie und Verschränkung für den Schulunterricht



P. Bronner \*, A. Strunz \*, C. Silberhorn †, J.-P. Meyn \*

\* Didaktik der Physik, Universität Erlangen-Nürnberg

† Max-Planck Institut für die Physik des Lichts, Erlangen

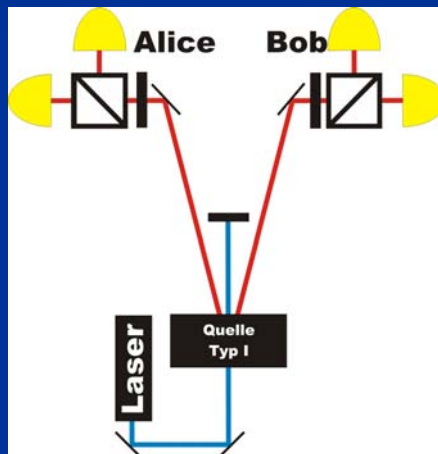


## Inhalt des Vortrags

1. Verschränkung
2. Quantenkryptographie
3. Unterrichtskonzept und Schülerlabor

# 1. Verschränkung

- Einführung über Quantenzufall
- Einzelne Photon am Strahlteiler



# 1. Verschränkung

- 50 % Strahlteiler (45°): gleiches Zufallsverhalten
- Variation Messwinkel (0-90°): [Klick](#)
- Einstein: "Aber dass er würfelt und sich telepathischer Mittel bedient, kann ich keinen Augenblick glauben" [1]
- 1935: Veröffentlichung von Einstein, Podolsky und Rosen [2]
- 1966 Bell-Ungleichung: theoretische Unterscheidung [3]

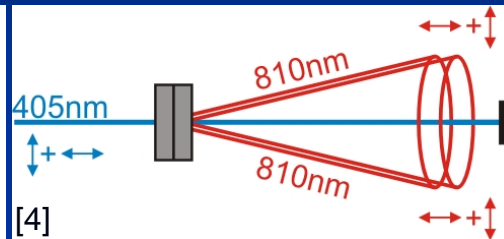
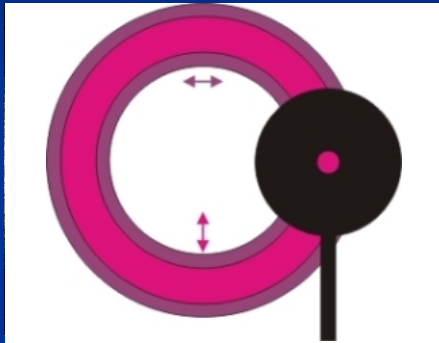
[1] The Born-Einstein Letters (1916-1955).

[2] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. 47, 777 (1935).

[3] J. Bell, Physics 1, 195 (1964).

# 1. Verschränkung

Quelle für verschränkte Photonen:



[4]

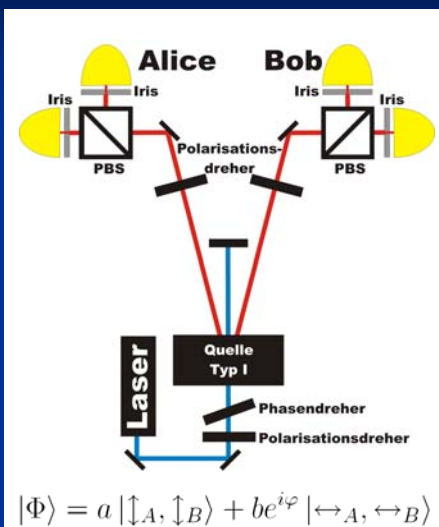
$$|\Phi\rangle = a |\downarrow_A, \downarrow_B\rangle + be^{i\varphi} |\leftrightarrow_A, \leftrightarrow_B\rangle$$

Anteil verschränkte Photonen: 75%

Anteil verschränkte Photonen mit Iris: 98%

[4] P. Kwiat et al., Physical Review A 60, R773 (1999).

# 1. Verschränkung



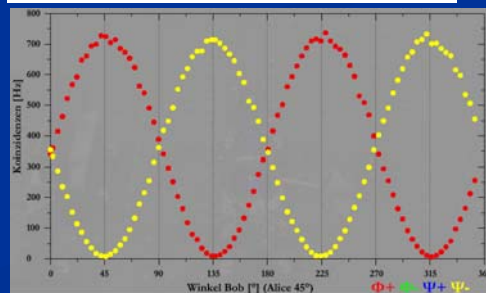
$$|\Phi\rangle = a |\downarrow_A, \downarrow_B\rangle + be^{i\varphi} |\leftrightarrow_A, \leftrightarrow_B\rangle$$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}} (|\downarrow_A, \downarrow_B\rangle + |\leftrightarrow_A, \leftrightarrow_B\rangle) \quad (B1)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}} (|\downarrow_A, \downarrow_B\rangle - |\leftrightarrow_A, \leftrightarrow_B\rangle) \quad (B2)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}} (|\downarrow_A, \leftrightarrow_B\rangle + |\leftrightarrow_A, \downarrow_B\rangle) \quad (B3)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}} (|\downarrow_A, \leftrightarrow_B\rangle - |\leftrightarrow_A, \downarrow_B\rangle) \quad (B4)$$



# 1. Verschränkung

## Beweis der Nichtlokalität für die Schule:

- "Verschränkte Photonen verhalten sich immer gleich"
- "Beide Photonen führen unendlich lange Liste mit"
- "Bedingungen von Anfang an festgelegt"
  
- Bell-Ungleichung:  
CHSH-Ungl. [5], Wigner-Ungl. [6], Hardys-Ansatz [7]
- Machen die Annahme: "von Anfang an festgelegt"
- Führen das Experiment zu einem Widerspruch

[5] J. F. Clauser et al., Physical Review Letters 23, 880 (1969).

[6] E. Wigner, American Journal of Physics 38, 1005 (1970).

[7] L. Hardy, Physical Review Letters 71, 1665 (1993).

# 1. Verschränkung

## Beweis der Nichtlokalität für die Schule:

- Didaktische Beispiele:  
farbige Socken [8], blinkende Lampen [9]  
Quantenkuchen [10], Zwillinge [11]
  
- Unser Beispiel für die Schule:  
Schüler mit Kleidungsstücke  
Beispiel mit Hardys Ansatz

[8] J. Bell, Journal de Physique Tome 42, 41 (1980).

[9] N. D. Mermin, AJP 58, 731 (1990).

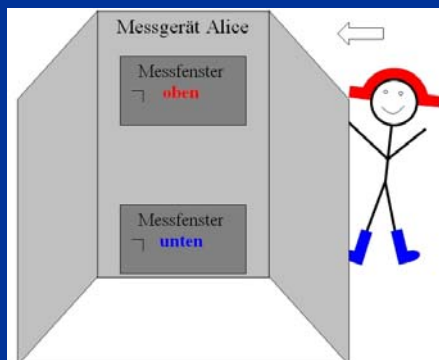
[10] P. Kwiat, and L. Hardy, AJP 68, 33 (2000).

[11] A. Zeilinger, Einsteins Spuk, Bertelsmann Verlag, (2005).

# 1. Verschränkung

## Beweis der Nichtlokalität für die Schule:

- 2 Schüler treffen sich in Umkleide: Hut, Schuhe
- Laufen in 2 getrennte Kleidungsmessgeräte
- Alice bzw. Bob messen die Schüler



Messergebnis Alice

Person	Messung	Eigenschaft	Ja	Nein
1	Unten	Schuhe		X
2	Oben	Hut	X	
3	Oben	Hut		X
4	Unten	Schuhe		X
5	Oben	Hut	X	
6	Unten	Schuhe	X	
7				
8				
9				

# 1. Verschränkung

## Beweis der Nichtlokalität für die Schule:

- Alice und Bob messen 100 Schüler unabhängig
- Alice und Bob vergleichen Listen
- Beide stellen 3 Regeln fest, folgern daraus die vierte Regel
- Überprüfen 4. Regel in den Listen: Keine Bestätigung
- Versuchen Erklärung aus dem Alltag zu finden: Scheitern
- Phänomen ist nicht mit Alltagsvorstellung zu erklären

## 1. Verschränkung

### Beweis der Nichtlokalität für die Schule:

Regel 1: Alice misst oben und Bob misst oben:  
9% aller Personenpaare tragen beide einen **Hut**.

Regel 2: Alice misst oben und Bob misst unten:  
Immer wenn die Person bei Alice einen **Hut** trägt,  
hat die Person bei Bob **Schuhe** an.

Regel 3: Bob misst oben und Alice misst unten:  
Immer wenn die Person bei Bob einen **Hut** trägt,  
hat die Person bei Alice **Schuhe** an.

## 1. Verschränkung

### Beweis der Nichtlokalität für die Schule:

Aus Regeln 1-3 folgt:

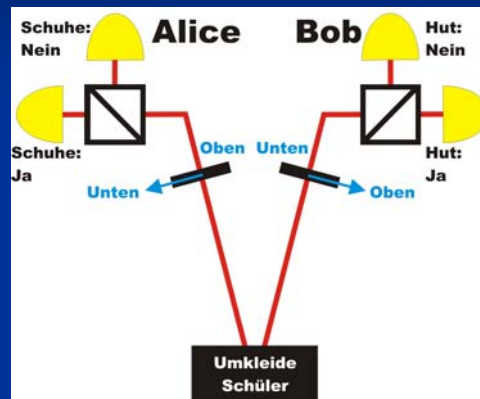
Regel 4:  
Alice misst unten und Bob misst unten:  
mind. 9% aller Personenpaare haben beide **Schuhe** an.

# 1. Verschränkung

## Beweis der Nichtlokalität für die Schule:

Übertragung auf Experiment:

- Schüler = Photonen
- Türe oben = Messung rechts
- Türe unten = Messung links
- Ja = Detektor Transmittiert
- Nein = Detektor Reflektiert



Überprüfung der 4 Regeln: [klick](#)

# 1. Verschränkung

## Beweis der Nichtlokalität für die Schule:

$P(\alpha_{Alice}, \alpha_{Bob}) = 9\%$	$P(18^\circ_{Alice}, 18^\circ_{Bob}) = 9\%$
$P(\beta_{Bob} \alpha_{Alice}) = 100\% \Rightarrow P(\alpha_{Alice}, \overline{\beta_{Bob}}) = 0\%$	$P(18^\circ_{Alice}, -34^\circ_{Bob}) = 0\%$
$P(\beta_{Alice} \alpha_{Bob}) = 100\% \Rightarrow P(\overline{\beta_{Alice}}, \alpha_{Bob}) = 0\%$	$P(-34^\circ_{Alice}, 18^\circ_{Bob}) = 0\%$
$P(\beta_{Alice}, \beta_{Bob}) \geq 9\%$	$P(-34^\circ_{Alice}, -34^\circ_{Bob}) \geq 9\%$

- Nur möglich mit nicht maximal verschränkten Zuständen
- Keine Ungleichung notwendig (Sichtbarkeit: 100%)
- Einfache Variante im Vergleich zu CHSH, Bell-Wigner

# 1. Verschränkung

## Zusammenfassung:

- Qualitativer Zugang über Quantenzufall
- Beweis der Nichtlokalität:  
Hardys-Ansatz: 4 Wahrscheinlichkeiten  
Überprüfung direkt am Experiment
- Philosophische Fragestellungen eröffnen sich ...
- Anwendung:  
Quantenkryptographie  
Quantenteleportation  
Quantencomputer

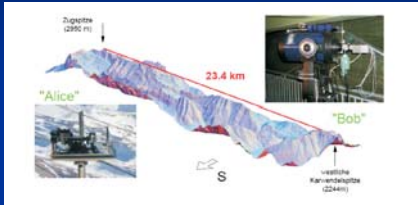
## Inhalt des Vortrags

1. Verschränkung
2. Quantenkryptographie
3. Unterrichtskonzept und Schülerlabor



## 2. Quantenkryptographie

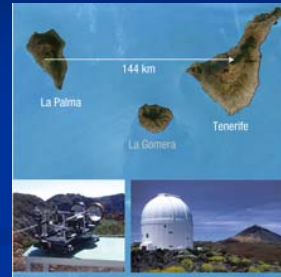
Vom Forschungslabor zur Anwendung:



[Nature, V. 419, P. 3, 2002]



Firma id Quantique, Schweiz, 2008



[Phys. Rev., V. 98, P. 504, 2007]

## 2. Quantenkryptographie

Alice   $\xrightarrow{\text{Eve} \text{ }$  Bob



Verfahren G. Vernan (1918): One-Time Pad

## 2. Quantenkryptographie

**One-Time Pad absolut sicher, wenn:**

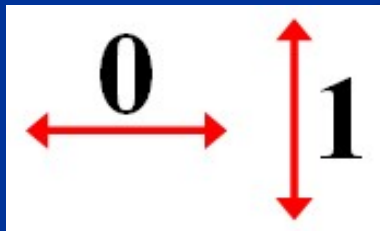
- Schlüssel nur einmal verwendet wird
- Schlüssel mind. genauso lange wie die Nachricht
- Schlüssel absolut zufällig
- Schlüssel nur Alice und Bob bekannt.



## 2. Quantenkryptographie

**Problem Schlüsselerzeugung und Übermittlung:**

- Lösung Quantenphysik [12]
- Übertragung Schlüssel: einzelne Photonen
- Informationskodierung: Polarisation



[12] C. Bennet, and G. Brassard, IEEE, New York, 175 (1984).

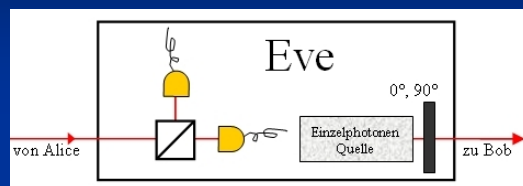
## 2. Quantenkryptographie

### Schlüsselerzeugung und Übermittlung:



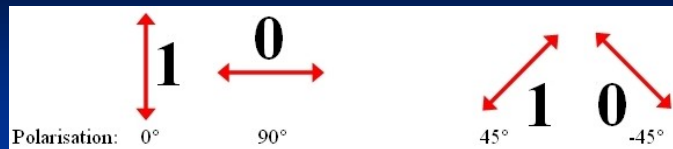
## 2. Quantenkryptographie

### Spion Eve im Experiment:



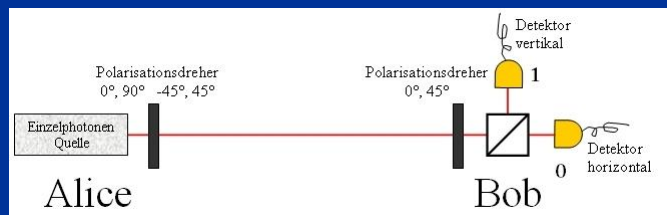
- Alice und Bob können Eve nicht bemerken
- Erweiterung des derzeitigen Systems auf zwei Basen  
Basis 1:  $0^\circ, 90^\circ$   
Basis 2:  $45^\circ, -45^\circ$

## 2. Quantenkryptographie



Messsystem: +

x



- zufällige Wahl der Messsysteme
- Gleiches Messsystem: Ergebnisse eindeutig
- Verschiedenes Messsystem: Ergebnisse zufällig

## 2. Quantenkryptographie

### Verfahren:

- Alice wählt zufällig Basis und Bit
- Bob wählt zufällig Basis
- Experiment ist abgeschlossen
- Alice und Bob kommunizieren und löschen falsche Basen
- Schlüssel ist fertig erzeugt

Liste Alice

Photon	Basis	Bit
1	+	1
2	x	1
3	+	0
4	+	1
5	x	1
6	+	0
7	x	0
8	x	1

Liste Bob

Photon	Basis	Bit
1	+	1
2	+	0
3	+	0
4	x	1
5	x	1
6	+	0
7	x	0
8	+	0

Liste Alice

Photon	Basis	Bit
1	+	1
3	+	0
5	x	1
6	+	0
7	x	0

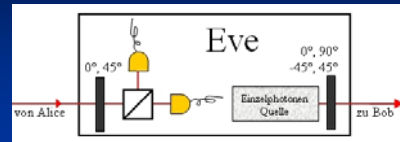
Liste Bob

Photon	Basis	Bit
1	+	1
3	+	0
5	x	1
6	+	0
7	x	0

## 2. Quantenkryptographie

### Spion Eve:

- Eve rüstet auf 2 Messsysteme auf:



- Eve wählt unabhängig und zufällig Messsystem + oder x
- Eve fügt 25% Fehler in eindeutige Messergebnisse ein

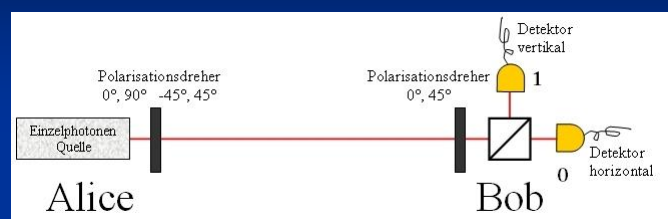
Basis Alice = Basis Bob	Basis Eve	Sender Eve	Empfang Bob	Übereinstimmung der Bits bei Alice und Bob
++	+	<b>1 oder 0 in +</b>	Eindeutig	100%
++	x	<b>1 oder 0 in x</b>	Zufall	50%
xx	+	<b>1 oder 0 in +</b>	Zufall	50%
xx	x	<b>1 oder 0 in x</b>	Eindeutig	100%

- Eve anwesend? Test von einigen Bits gleicher Basen
- Quantenkopierer: No cloning theorem [13]

[13] W. Wootters, and W. Zurek, Nature 299, 802 (1982).

## 2. Quantenkryptographie

### Zusammenfassung:



- Technologie kommerziell verfügbar
- Alice und Bob erzeugen Schlüssel über Polarisation, 2 Basen
- Ausschluss eines Spions: Test auf Eindeutigkeit
- Verwendung des Schlüssel für das One-Time-Pad
- Demonstrationsexperiment: [Klick](#)

## Inhalt des Vortrags

1. Verschränkung
2. Quantenkryptographie
3. Unterrichtskonzept und Schülerlabor

## 3. Unterrichtskonzept

### Konzept besteht aus drei Teilen:

- 1. Teil: Unterrichtseinheit: 10-12 Schulstunden
- 2. Teil: Projektarbeit zur Quantenkryptographie
- 3. Teil: Exkursion zu den Schülerlaboren Uni Erlangen

Erprobt am Albert-Schweitzer Gymnasium Erlangen

10. Klassenstufe, 5 Lehrer, 150 Schüler

Im Unterricht: interaktive Experimente

Schülerorientiert, qualitativ, fächerverbindend (NWT),...

Teile sind unabhängig voneinander durchführbar.

### 3. Unterrichtskonzept

#### 1. Teil: Unterrichtseinheit

1. Stunde: Motivation, Vorstellung Quantenobjekte
- ~~2. Stunde: Grundlagen: Detektoren für einzelne Photonen~~
- ~~3. Stunde: Grundlagen: Quelle für einzelne Photonen~~
4. Stunde: Quanteneigenschaft: Unteilbarkeit
5. Stunde: Quanteneigenschaft: Zufall
6. Stunde: Quanteneigenschaft: Interferenz
7. Stunde: Quanteneigenschaft: Interf., Unteilbarkeit, Zufall
8. Stunde: Quanteneigenschaft: Welcher Weg - Interferenz
9. Stunde: Zusammenfassung und Abschluss

### 3. Unterrichtskonzept

#### 2. Teil: Projektarbeit Quantenkryptographie

- 8 Schulstunden, selbstständige Erarbeitung der QC
- Erstellung einer Zeitschrift für das Schulfest in 7-er Gruppen



Pro Klasse:  
4 Zeitschriften

Beispiel

## 3. Unterrichtskonzept

### 3. Teil: Exkursion zu den Schülerlaboren

- 2 Schülerlabore:  
Grundlagen der modernen Optik (Lernzirkel)  
Quantenoptiklabor
- Voraussetzung: Quantenkryptographie, Quantenradierer
- Zeitbedarf: 4-5 Stunden, max. 15 Schüler
- Möglich: Besuch Max-Planck Institut zur Physik des Lichts

## 3. Unterrichtskonzept

### 3. Teil: Exkursion zum Schülerlabor





### 3. Unterrichtskonzept

#### 3. Teil: Exkursion zum Schülerlabor



### 3. Unterrichtskonzept

#### 3. Teil: Exkursion zum Schülerlabor



### 3. Unterrichtskonzept

Abschlussbericht  
Meine Quantenwelt

Meiner Meinung nach ist das Thema gut geeignet für den Physikunterricht der Klasse, es ist aber sehr schwer zu verstehen, dass man es eigentlich nicht verstehen kann. Um das zu begreifen braucht man, denke ich, viel Zeit. Dennoch war diese Unterrichts einheit ziemlich interessant.

[www.QuantumLab.de](http://www.QuantumLab.de)

**Fortbildung:**  
für Referendare und Fachleiter aus BW  
29. + 30 Juni 2009

**Robert Bosch Stiftung**



**Danke für Ihre Aufmerksamkeit**

P. Bronner et al., European Journal of Physics, 345 (2009).