

# Quantenkryptographie

## Eine kurze Einführung

---

(c) 2003 Johannes Tränkle

Quelle:

[www.traenkle.org/texte/quanten.shtml](http://www.traenkle.org/texte/quanten.shtml)

# Quantenkryptographie:

- Verschlüsselung: z.B. One-Time-Pad
- Übertragung: hier erklärt

**Exkurs:  
quantenmechanische  
Grundlagen**

# Qubit:

Einheit zur Messung von  
Quanteninformation

**Binär: 0 und 1**

**Qubit: 0 und 1, zusätzlich  
quantenmechanische  
Überlagerung (Superposition) -  
Unsicherheit**

Folge:

- nicht zwei,
- sondern **drei Zustände**  
können gespeichert werden.

# Schrödingers Katze:

- Katze in Kiste
- radioaktives Atom, Zerfall unklar
- Detektor, gekoppelt mit Gift

**Folge:** Katze 'tot' und 'lebendig',  
solange nicht nachgeschaut

# Gängige Umsetzung von Qubits:

Polarisation eines Photons  
(Schwingungsebene des zugehörigen  
elektrischen Feldes)



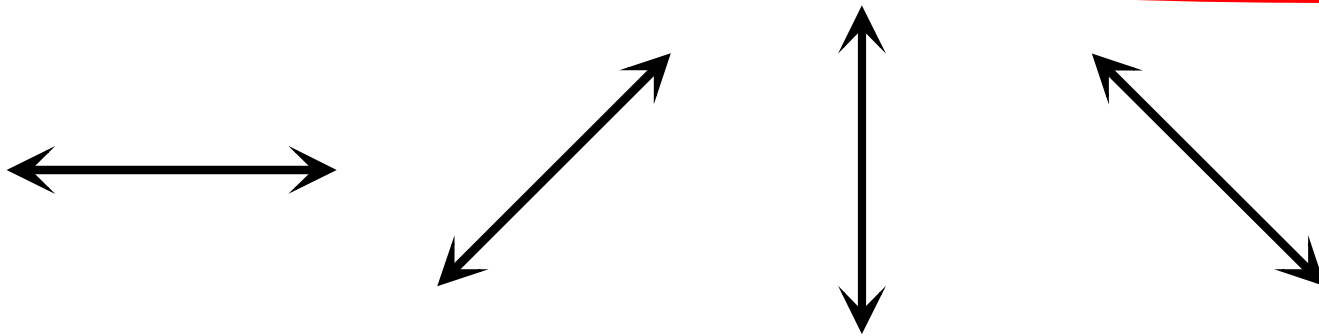
Zusammensetzung: zwei  
Komponenten

gerade ( $0^\circ$ ,  $90^\circ$ ) und ungerade  
( $45^\circ$ ,  $135^\circ$ ) Polarisation

## Zwei Eigenschaften:

- 1.) Gerade Polarisation:  
für Quantenkryptographie 1 oder 0  
(1 bedeutet 100%, oder  
vollständig vorhanden)
- 2.) Ungerade Polarisation:  
auch 1 oder 0

# Vier mögliche Polarisationen



Immer nur eine dieser  
Komponenten messbar (gerade  
oder ungerade).

D.h. Informationsteil der  
anderen Komponente geht bei  
Messung verloren.

Deshalb “Weitersenden” nicht  
möglich!

Grund:  
**Heisenbergsche  
Unschärferelation**

# Heisenbergsche Unschärferelation:

**Je genauer ich die eine  
Komponente bestimme, desto  
ungenauer sind meine  
Aussagemöglichkeiten im  
Hinblick auf die andere  
Komponente.**

# Beispiel:


## Fall A)

0° Photon, Polarisator stimmt  Messung: 0°

## Fall B)

90° Photon, Polarisator stimmt  Messung: 90°

## Fall C)

45° Photon, Polarisator stimmt nicht  Messung:  
entweder 0° oder 90°, da auch in 45° und 135°  
gerade Polarisation vorhanden

# Folgerungen:

Wenn  $0^\circ$  gemessen, dann:

- 1.) Photon hatte tatsächlich  $0^\circ$  (Fall A)
- 2.) Photon hatte  $45^\circ$  (Fall C)
- 3.) Photon hatte  $135^\circ$  (Fall C)

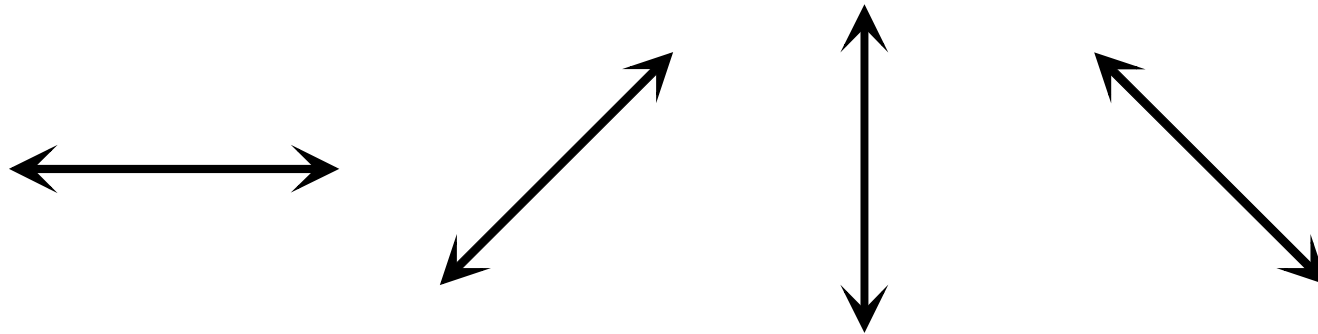
Nur eines ist sicher: Photon hatte keine  $90^\circ$ !



# Die Übertragung

# Photonen mit verschiedener Polarisation

☞ vier Zustände:  $0^\circ$ ,  $45^\circ$ ,  $90^\circ$ ,  $135^\circ$



# Zuweisungen

$0^\circ, 45^\circ$   logisches '0'

$90^\circ, 135^\circ$   logisches '1'

vgl. One-Time-Pad

Alice sendet:

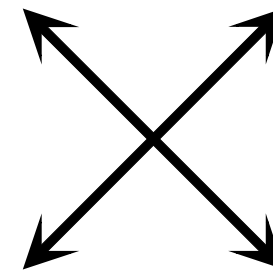
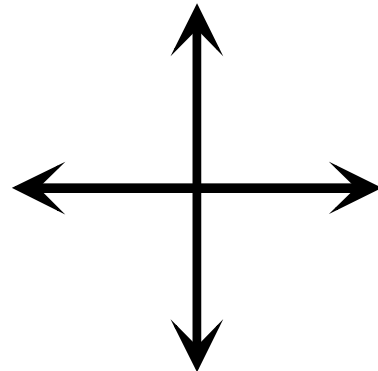
Polarisation **zufällig festgelegt**

Wichtig: **kein Pseudo-Zufall**

Empfang durch Bob:

## Polarisator

$0^\circ$  und  $90^\circ$  bzw.  $45^\circ$  und  $135^\circ$   
(zufällig)



Wenn falsche  
Polarisatoreinstellung:

völlig zufälliges Ergebnis  
entsprechend Polarisator

# Abstimmung:

Möglichst offener Kanal

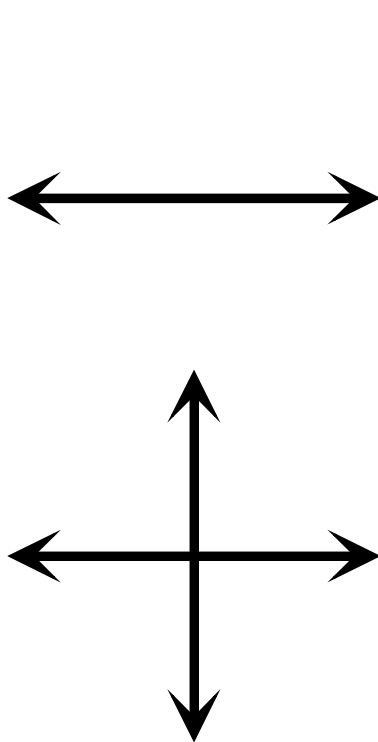
Bob: Übertragung der Einstellung  
des Polaristors

Alice: Stimmen Einstellungen?

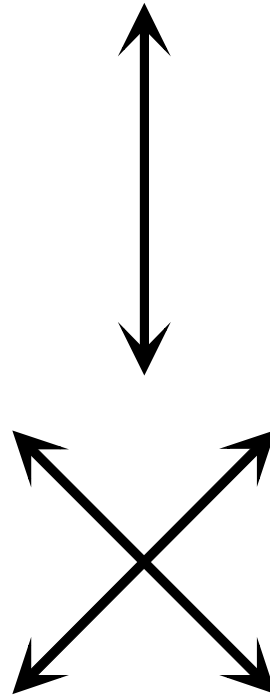
Bob weiß nun, welche  
Messergebnisse zum Schlüssel  
gehören

☞ falsche Daten streichen

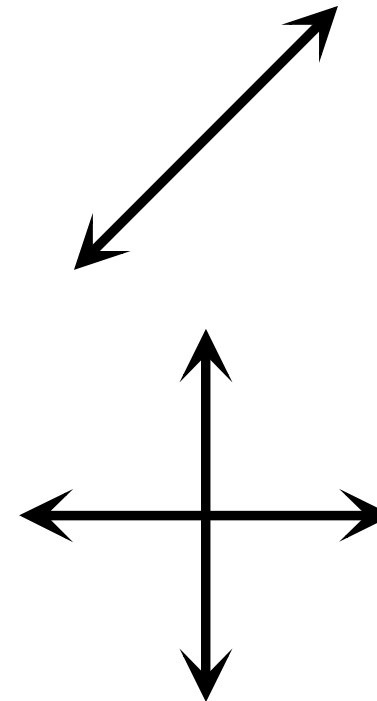




Treffer: '1'



Verwerfen



Verwerfen

Schlüssel ist nunmehr bekannt.

Verschlüsselung kann (prinzipiell)  
vorgenommen werden.

**Wurde abgehört?**

Teil des Schlüssels offen  
übertragen

Stimmen diese Teile überein?

Diesen Teil später löschen,  
Rest = Schlüssel

# Abweichungen bei Schlüssel:

☞ potentiell abgehört

# Abhören durch Eve

- Dazwischenschalten
- “Überzählige” Photonen abfangen

## **Dazwischenschalten:**

**Nach Analyse eine Komponente  
unbekannt,  
Polarisatoreinstellung (noch)  
unbekannt.**

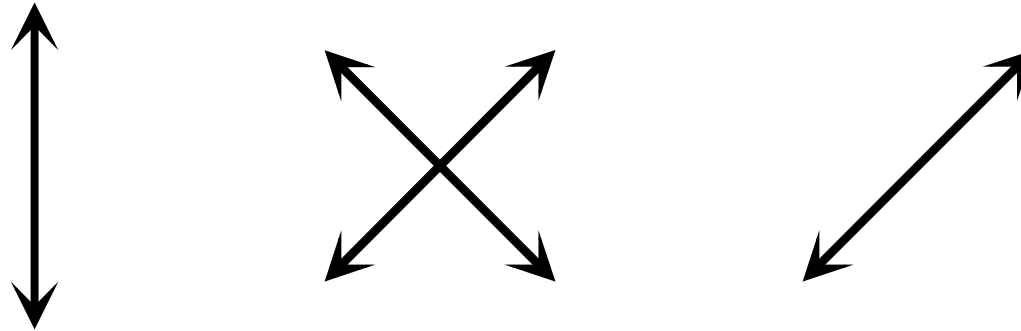
Deshalb (nur) Weitersenden des gemessenen Ergebnisses.

**50%: Richtig, da richtige Polarisatoreinstellung**

**restl. 50%: völlig zufällig, d.h. In 50% der Fälle zufällig richtiges Ergebnis**

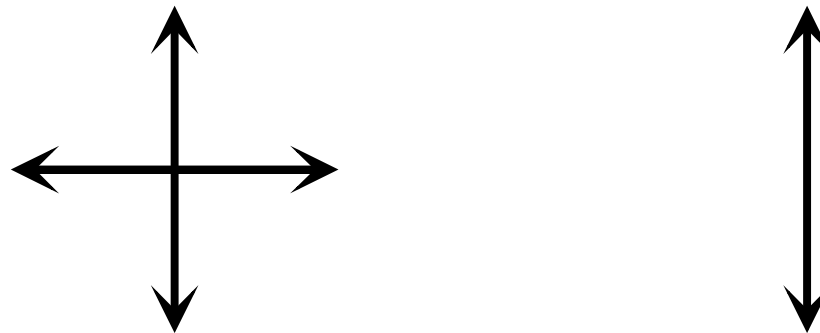


Alice sendet:    Eve analysiert mit:    Eve sendet zufällig



Bob analysiert mit:

50/50-Chance, dass  
doch richtiges Ergebnis:



Fehlerquote von **25 %**

u.U. bei ca. 14 %

“normaler” Informationsverlust  
bei wenigen %

Wird Fehlerquote festgestellt,  
wurde abgehört.

Alles nochmals, Eve hat nichts  
gewonnen.

# Abfangen

Funktioniert nur, wenn keine saubere Datenquelle benutzt wurde.

Dann aber unbemerktes Abhören möglich!

# Praktische Probleme

- Übertragungsfehler, Fehlerkorrekturmaßnahmen
- Unsaubere Datenquelle
- Beschränkte Reichweite (ca. 67 km), keine Verstärkung
- Je länger der Übertragungsweg, desto mehr Photonen gehen verloren.