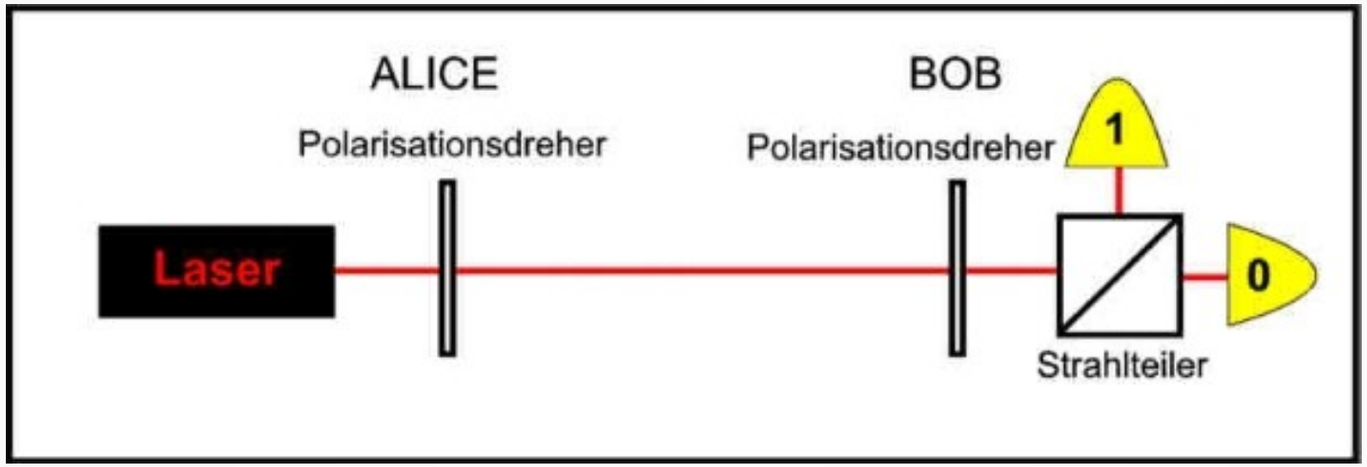
Quantenkryptographie



Ein Modellversuch und seine Erweiterungen auf Grundlage des BB84-Protokolls

von OStR Jörn Schneider
Leibniz-Gymnasium Dormagen

Quantenkryptographie

- Kryptographie: Die Wissenschaft von der Verschlüsselung von Daten und Texten
- Cäsar-Code
- Im Zeitalter des Computers ein ständiges Hase/Igel Problem

Gibt es einen absolut sicheren Schlüssel?

Quantenkryptographie

- **RSA – sicher, solange der Schlüssel lang ist**

  Doch was ist mit dem Quantencomputer?

32 bit	64 bit	128 bit
4,29s	585 Jahre	$1{,}1\ 10^{22}$ Jahre

- **One-Time-Pad (Einweg-Schlüssel)**

  Doch wie bekommt man den Schlüssel ausgetauscht?

Quantenkryptographie

- Der Schlüssel muss genauso lang sein, wie die Daten
- Bei der Übertragung kann ein Lauscher den Schlüssel abhören

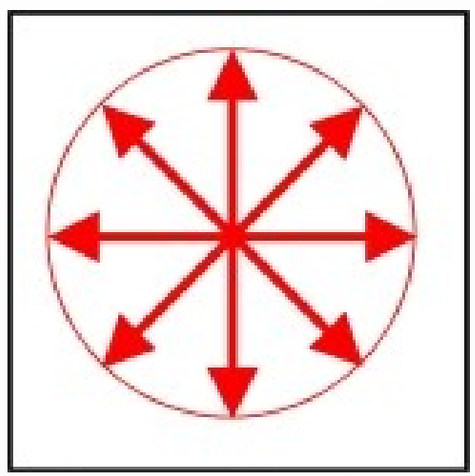
Quantenkryptographie

Das BB84-Protokoll Charles H. Bennett und Gilles Brassard

- Verwendet polarisiertes Licht (Laser)
- Zwei Basensätze (H/V und X)
- ALICE (Sender) und BOB (Empfänger) wählen unabhängig voneinander eine zufällige Base
- Nach der Schlüsselübertragung werden die Basen verglichen und alle Werte mit unterschiedlichen Basen gestrichen
- Ein Lauscher wird durch Fehler in dem Schlüssel entdeckt

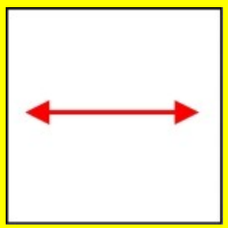
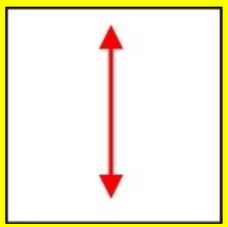
Quantenkryptographie

Polarisation von Licht



Laserlicht von Halbleiterlasern ist polarisiert

Quantenkryptographie

			
H/V-Base		X-Base	
0° „0“	90° „1“	-45° „0“	+45° „1“

ALICE hat 4 Winkelpositionen

Quantenkryptographie

BOB benötigt nur zwei Winkelstellungen

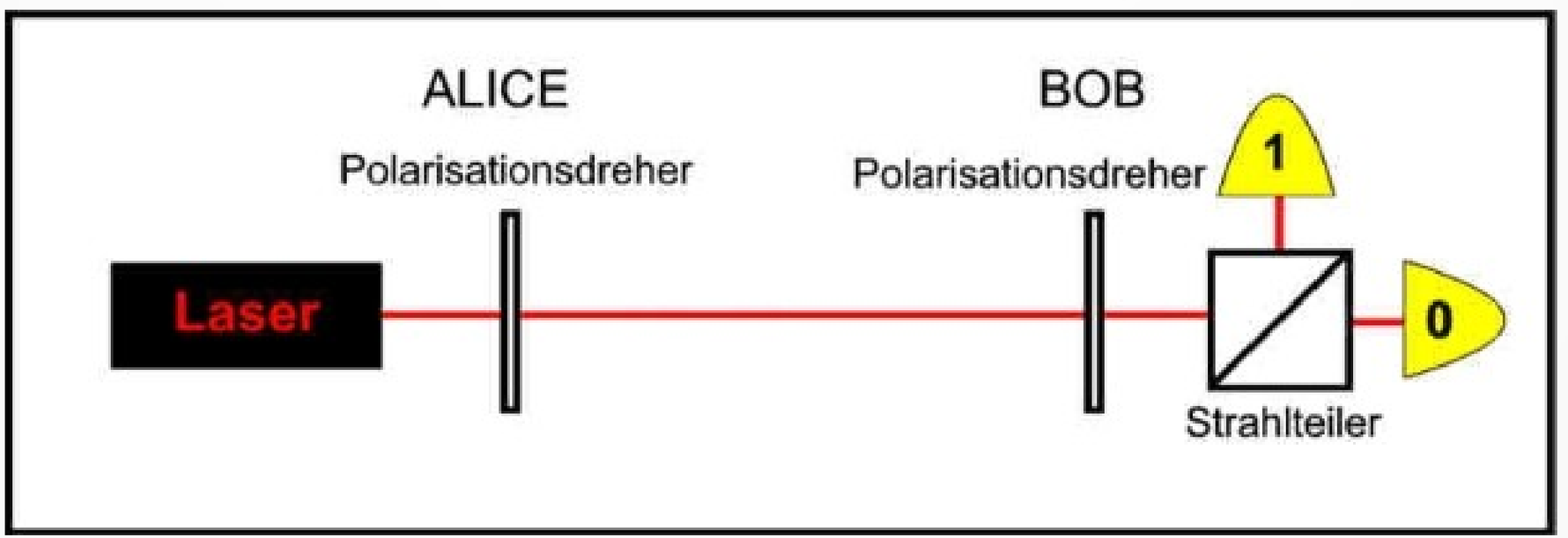
um die H/V und die X-Basis einzustellen

ALICE	0°	90°	0°	90°	-45°	+45°	-45°	+45°
BOB	0° (H/V)		45° (X)		0° (H/V)		45° (X)	
Bit	0	1	X	X	X	X	0	1

Stimmen die Basen nicht überein wird kein sinnvoller Bitwert erzeugt!

Quantenkryptographie

Aufbau des Versuchs



Quantenkryptographie

Versuchsdurchführung Schlüsselerzeugung

- ALICE und BOB wählen 52x eine zufällige Base
- ALICE wählt 52x einen zufälligen Bitwert
- ALICE sendet jedes Bit an BOB
- BOB notiert sich die Sensorwerte
- ALICE und BOB vergleichen die Basen miteinander
- Nicht übereinstimmende Basenwerte werden gestrichen

Quantenkryptographie

Versuchsdurchführung Datenübertragung

- ALICE denkt sich ein Wort mit 4 Buchstaben aus
- Aus der Codetabelle werden 20bit Daten erzeugt
- Diese werden verschlüsselt und an BOB gesendet. Dazu wird nur die H/V-Base benutzt. Dies kann aber auch über jeden anderen öffentlichen Kanal erfolgen.
- BOB entschlüsselt die Daten und mit der Codetabelle kann er das Wort lesbar machen
- ALICE und BOB vergleichen das übertragene Wort

Quantenkryptographie

Ein bisschen Quantenphysik…….

- Heisenbergsche Unschärferelation

Ort und Impuls lassen sich nicht gleichzeitig völlig exakt messen….

$$\Delta p \cdot \Delta q \sim h$$

Heisenbergsche Unschärferelation

Quantenkryptographie

- Das „Super-Heisenberg-Mikroskop“ SHM
- Wir fertigen eine Kopie des Teilchens an und messen bei einem den Ort und bei dem anderen den Impuls völlig exakt

SHM

Quantenkryptographie

- Das „Super-Heisenberg-Mikroskop“ SHM
- Wir fertigen eine Kopie des Teilchens an und messen bei einem den Ort und bei dem anderen den Impuls völlig exakt

Quantenkryptographie

- Das „Super-Heisenberg-Mikroskop“ SHM
- Wir fertigen eine Kopie des Teilchens an und messen bei einem den Ort und bei dem anderen den Impuls völlig exakt

No-cloning-theorem

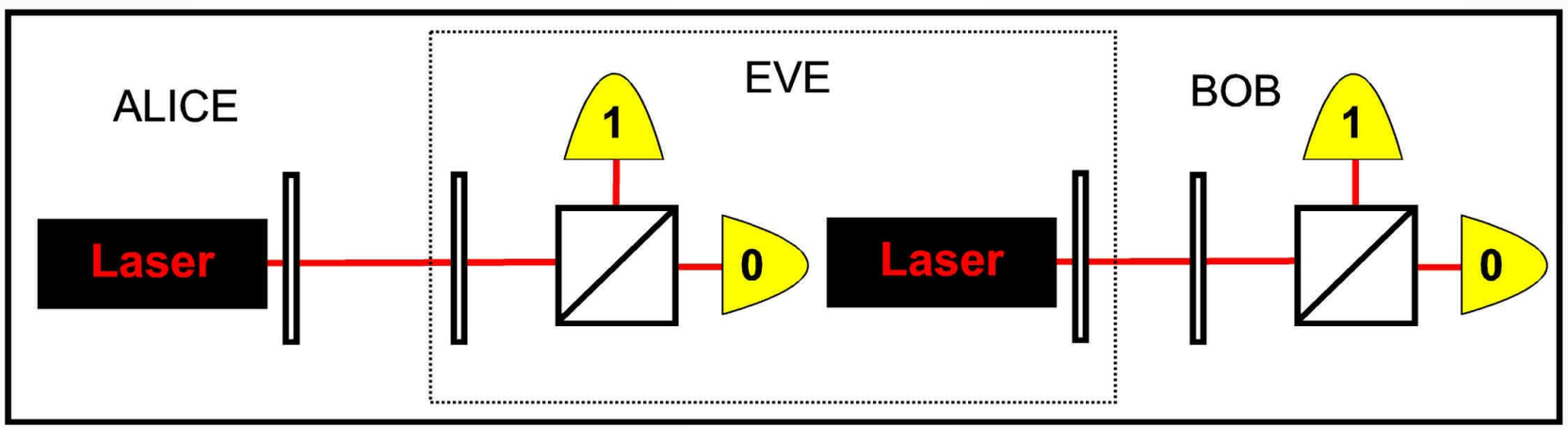
Quantenkryptographie

Modellversuch vs. Quantenexperiment

- Der Modellversuch arbeitet mit vielen Photonen, daher nicht wirklich abhörsicher
- Einzelne Photonen lassen sich nicht kopieren (No-Cloning-Theorem), daher kann der Lauscher den Schlüssel nicht kopieren - er muss raten!
- Dabei entsteht ein Fehler von statisch 25%, der den Lauscher verrät.

Quantenkryptographie

Der Lauscher EVE



Der Lausche EVE besteht aus einer Kombination von BOB und ALICE

Quantenkryptographie

Erweiterungen

- Automatische Version mit elektronischem Basenvergleich
- Automatischer Lauscher EVE
- Trennung von Quantenkanal und Informationskanal. Austausch einer verschlüsselten Nachricht via WLAN und Schlüsselübertragung mit der Quantenkryptographie

Quantenkryptographie

- **ALICE und BOB erzeugen permanent Schlüsseldaten und speichern diese.**
- **Ein Smartphone fordert über BT eine gewisse Anzahl Schlüsselbits an und verschlüsselt damit einen Text.**
- **Der verschlüsselte Text wird via Mail / Internet / WLAN an ein zweites Smartphone gesendet.**
- **Dieses fordert von BOB nun die gleiche Anzahl Schlüsselbits über BT an und entschlüsselt den Text.**

Quantenkryptographie

Ausblicke

- Ersetzen der Rotationsdreher durch Pockelzellen
- Modifikation des BB84-Protokolls mit Quanten-Messungen auf der Grundlage der Heisenbergschen Unschärfe
- Quantenverschränkung zur Schlüsselgenerierung

Vielen Dank für die Aufmerksamkeit!

Besuchen sie meine Webseite

www.physik-am-gymnasium.de