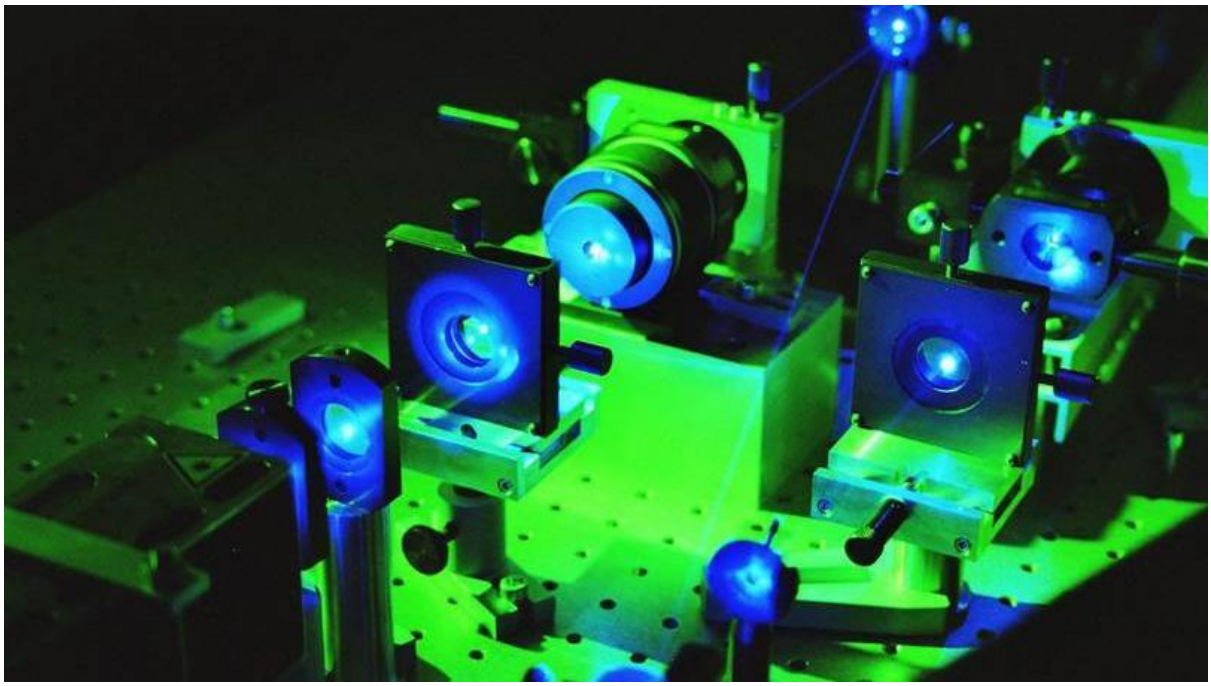
Sven Jodocy
Jan Huberty
Max Zuidberg
Marc Feller

Quantenkryptografie

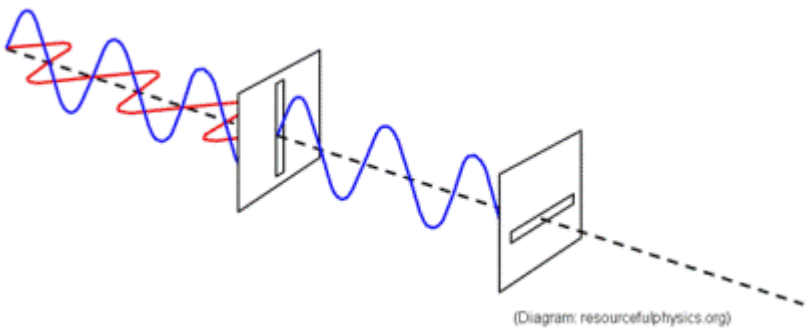


Einleitung:

In diesem Praktikum geht es um das Verschlüsseln von Informationen durch Quantenkryptografie. Diese benutzt das Prinzip, dass einzelne Photonen, welche miteinander verschränkt sind (also miteinander verbunden), sich polarisieren lassen (Erklärung siehe unten). Dadurch können Informationen verschlüsselt verschickt werden, da die Antwort durch die zufällige Polarisation nicht von Fremdpersonen ausgewertet werden können. Weitere Vorteile sind die hohe Geschwindigkeit mit der die verschränkten Photonen verschickt werden können, da wenn eines dieser Photonen polarisiert wird, das andere gleichzeitig den gleichen Wert annimmt, also theoretisch schneller als Licht. Jedoch ist das zweite Photon ohne weitere Information (nämlich die der Art der Polarisation) nicht entschlüsselbar, weswegen über traditionellere Wege (zum Beispiel Brief, Telefon, E-Mail, …) Zusatzinformationen übermittelt werden müssen, welche langsamer als Lichtgeschwindigkeit sind. Die Aufgabe des Praktikums ist es die Art wie die Informationen verschlüsselt werden und weshalb Quantenkryptografie als abhörsicher zählt zu verstehen.

Polarisation:

Die Polarisation beschreibt die Richtung in welche sich eine elektromagnetische Welle sich fortbewegt. Durch Polarisationsfilter oder Polarisationsdreher lassen sich die Wellen herausfiltern, welche sich in eine bestimmte Richtung fortbewegen. Sollte sich keine der Wellen in der gewollten Richtung fortbewegen, dann lässt der Filter keine Welle durch. (siehe Abbildung)

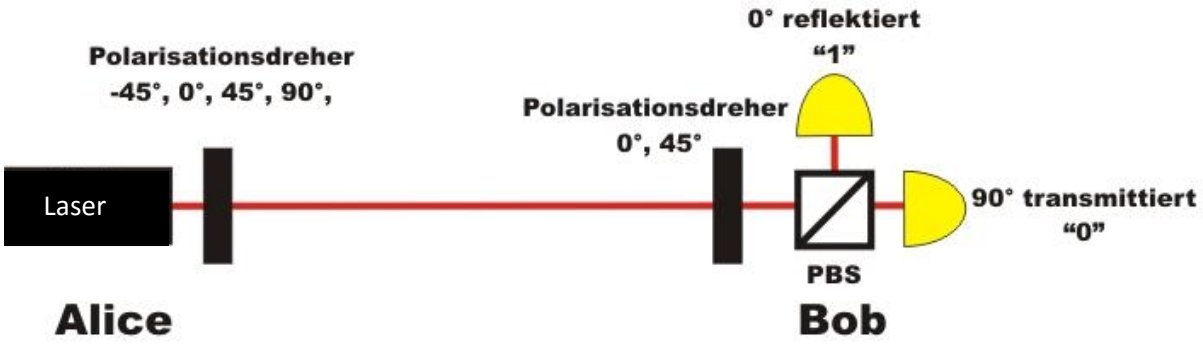


(Diagram: resourcefulphysics.org)

Anmerkung:

Bei diesem Praktikum arbeiten wir mit Lasern statt mit einzelnen verschränkten Photonen. Diese Änderung vereinfacht das Praktikum um ein vielfaches, ohne jedoch die Grundprinzipien zu verändern. Einzig und allein die Quantenteleportation, welche auch normalerweise gleichzeitig genutzt wird, wird nicht in Betracht gezogen.

Aufbau 1: Grundprinzipien der Quantenkryptografie



Der Aufbau kann in 2 Stationen aufgeteilt werden. Eine Sendestation „Alice“ und eine Empfangsstation „Bob“.

Alice besteht aus:

- Einem Laser
- Einem Polarisationsdreher mit den Einstellungsmöglichkeiten -45°, 0°, 45° und 90°

Bob besteht aus:

- Einem Polarisationsdreher mit den Einstellungsmöglichkeiten 0° und 45°
- Einem polarisierenden Strahlenteiler (PBS)
- Zwei Detektoren

Prinzip:

Alice möchte eine Nachricht an Bob versenden. Da der polarisierende Strahlenteiler den Laser nur Strahlen komplett umlenken können, wenn sie entweder gradlinig oder rechtwinklig polarisiert sind. Sie nutzt deswegen einen vereinfachten Binärcode, da nur Buchstaben verwendet werden:

Buchstabe	Binärcode	Buchstabe	Binärcode
A	00000	N	01101
B	00001	O	01110
C	00010	P	01111
D	00011	Q	10000
E	00100	R	10001
F	00101	S	10010
G	00110	T	10011
H	00111	U	10100
I	01000	V	10101
J	01001	W	10110
K	01010	X	10111
L	01011	Y	11000
M	01100	Z	11001

Alice hat 2 Modi zur Auswahl, zwischen welchen sie zufällig wechseln kann:

1. „0°“ und „90°“, wobei „0°“ für eine „1“ und „90°“ für eine „0“ stehen
2. „-45° und 45°“, wobei „45°“ für eine „1“ und „90°“ für eine „0“ stehen

Bob erhält, wenn Alice mit „0° und 90°“ arbeitet nur eine eindeutige Antwort, wenn sein Polarisationsdreher auf „0°“ eingestellt ist. Sonst werden beide Detektoren aktiviert.

Bob erhält, wenn Alice mit „-45° und „45°“ arbeitet nur eine eindeutige Antwort, wenn sein Polarisationsdreher auf „45°“ eingestellt ist. Sonst werden beide Detektoren aktiviert.

Alice muss Bob also mitteilen, mit welchen Einstellungen sie arbeitet. Dazu kreiert sie einen Code, welchen sie Bob durch einen traditionellen Weg übermittelt, also z.B.:

durch einen Brief. Es entsteht also ein Code, der die gleiche Länge besitzt wie die zu übermittelnde Nachricht. Wenn sie die Einstellung „-45°“ und „90°“ nutzt, erhält Bob eine „0“, bei „0°“ und „45°“ schickt Alice Bob eine „1“.

Beispiel:

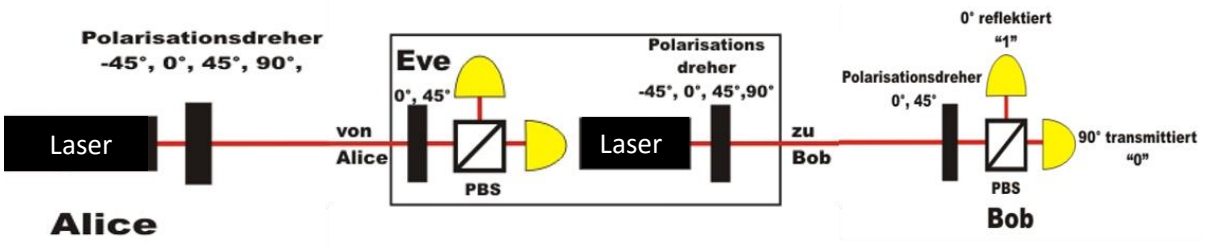
Alice möchte Bob drei Buchstaben schicken. Da bei unserem Binärcode jeder Buchstabe aus fünf Ziffern besteht schickt sie Bob einen zufällig generierten Code aus 15 Ziffern per Post. In diesem Fall: „110000111100010“. Sie möchte ihm die Buchstaben „LCD“ schicken, also „010110001000011“.

Sie dreht also ihren Polarisationsdreher:

Nachricht	Alice	Bob	Nachricht
0	-45°	45°	0
1	45°	45°	1
0	90°	0°	0
1	0°	0°	1
1	0°	0°	1
0	90°	0°	0
0	-45°	45°	0
0	-45°	45°	0
1	45°	45°	1
0	-45°	45°	0
0	90°	0°	0
0	90°	0°	0
0	90°	0°	0
1	45°	45°	1
1	0°	0°	1

Bob kann jetzt dank des Binärcodes die Nachricht entschlüsseln und erhält die Buchstaben „LCD“.

Aufbau 2: Sicherheit durch Quantenkryptografie



Dieser Aufbau besteht aus 2 Sendestationen und 2 Empfangsstationen. Bei diesem Aufbau soll gezeigt werden weshalb die Quantenkryptografie als abhörsicher gilt. „Eve“, der Spion, besteht aus einer Empfangsstation und einer Sendestation.

Eve ist nicht in Besitz des Codes und muss deswegen erraten, in welcher Einstellung Alice sendet. Es besteht also eine Chance von 50% dass Eve richtigliegt. Wenn sie richtig liegt, erhält sie eine eindeutige Antwort und kann diese an Bob weiterleiten. Liegt sie falsch, werden ihre beiden Detektoren aktiviert und sie schickt nur mit einer Chance von 50% die richtige Information an Bob weiter. Die Fehlerquote liegt also bei 25%. Da ja nicht nur einzelne Informationen verschickt werden, sondern große Stränge, fällt ein Lauscher in der Leitung auf, da die Nachricht durch die Fehler keinen Sinn mehr ergibt. Eve kann also nicht mithören ohne Aufzufallen und kann mit den 75% der Informationen die sie erhält nichts anfangen, da diese keinen Sinn ergeben.

Nutzung in der Zukunft:

Dank der Quantenkryptografie wird es in Zukunft zum Beispiel möglich sein:

- Nachrichten komplett anonym und sicher zu versenden
- Im Internet komplett anonym zu surfen, ohne dass Google & co die Daten speichern kann (durch Quanteninternet)
- Online sicher Bankgeschäfte abzuwickeln

Probleme der Quantenkryptografie:

Durch Quantenkryptografie sind zwar die Übermittlungswege sicher, jedoch können Nachrichten immer noch durch am Sendepunkt oder am Empfangspunkt installierte Malware (zum Beispiel Trojaner) die Nachrichten vor dem Chiffrieren beziehungsweise nach dem Dechiffrieren die Informationen erhalten können. Also ist eine Schwachstelle das Sende- beziehungsweise das Empfangsgerät.

Eine andere Schwachstelle ist, wenn der Code, der ja über traditionelle Wege verschickt werden muss, abgehört werden kann. Es muss also auch noch eine Lösung zur Verbesserung der traditionellen Wege gefunden werden um die Quantenkryptografie wirklich 100% abhörsicher zu machen.

Quellen:

Informationen: Zeitschrift „Spektrum“

Schema: http://www.didaktik.physik.uni-erlangen.de/quantumlab/