Analogieversuche zur Quantenphysik –

Quantenradierer und Quantenkryptographie

Theorie und Aufgaben zur Vorbereitung

Physikalisches Fortgeschrittenenpraktikum für Lehramtskandidaten

Karlsruher Institut für Technologie

Vorbemerkung:
In den folgenden Versuchen werden Sie zwei quantenphysikalische Experimente kennenlernen, die experimentell in Analogieversuchen behandelt werden (d.h. mit Laserlicht und nicht mit Einzelphotonen, die man für „echte“ quantenphysikalische Effekte bräuchte). Die Experimente sind außerdem schulrelevant und für den Unterricht in der gymnasialen Oberstufe geeignet.
In diesen Versuchen sollen Sie sowohl Erfahrung mit dem Aufbau und der Justierung optischer Strahlengänge sammeln als auch wesentliche quantenmechanische Prinzipien vertiefen, indem Sie sie auf ein Experiment anwenden.

1. Der Quantenradierer mit Mach-Zehnder-Interferometer

In einem Mach-Zehnder Interferometer wird ein Lichtstrahl zunächst durch einen Strahlteiler in zwei Komponenten aufgeteilt und an einem zweiten Strahlteiler wieder vereint (s. Abb.1 der Durchführungsanleitung). Verursacht durch den optischen Gangunterschied der beiden Teilstrahlen können an zwei Schirmen hinter dem zweiten Strahlteiler zwei komplementäre Interferenzmuster beobachtet werden.

Ein Mach-Zehnder Interferometer ist sehr nützlich, um quantenmechanische „Welcher-Weg“-Probleme zu veranschaulichen. Setzt man in jeden Arm des Interferometers einen Polarisator und sind deren Polarisationsebenen um 90° gegeneinander verdreht, so verschwindet das Interferenzmuster. Natürlich kann man diese Beobachtung in diesem Aufbau vollständig durch klassische Elektrodynamik erklären – man kann aber eine quantenmechanische Beschreibung wählen, wenn man sich den Lichtstrahl im Interferometer nun auf einzelne Photonen (bzw. nur ein einziges Photon) reduziert denkt. Durch das Einfügen der gekreuzten Polarisatoren in den Aufbau werden die beiden möglichen Lichtwege unterscheidbar gemacht – wir erhalten eine „Welcher-Weg“ Information. Daher verschwindet das Interferenzmuster.

Fügt man zwischen dem zweiten Strahlteiler und dem Schirm einen dritten Polarisator hinzu, den sogenannten „Radierer”, der gegenüber den anderen beiden nun um 45° orientiert ist, so besitzen alle Photonen, die den Schirm erreichen, wieder dieselbe Polarisation. Da nun die Weginformation wieder verloren ist, also „ausradiert“ wurde, ist wieder ein Interferenzmuster auf dem Schirm zu sehen.

Statt wie der ideale Quantenradierer einzelne Photonen zu verwenden, wird in diesem Aufbau ein kontinuierlicher Laser eingesetzt, der für das Auge sichtbar ist. Obwohl das Experiment vollständig durch klassische Physik beschreibbar ist, bietet es eine sehr gute Analogie zum Einzelphoton-Quantenradierer.

Der Quantenradierer ist ein Standardthema in der gymnasialen Oberstufe und abiturrelevant!

1.1 Klassische Interpretation

Das Mach-Zehnder-Interferometer (s. Abb. 1) ist vom Prinzip her mit dem bekannten Doppelspaltexperiment vergleichbar: Man schickt Photonen in einen Aufbau, in dem es an einem Punkt zwei mögliche Wege für ein Photon gibt. Beim Doppelspalt sind es die beiden Spalte, im Interferometer zwei Wege nach einem Strahlteiler. Zur Behandlung des Quantenradierers ist es jedoch praktikabler, ein Interferometer zu verwenden, da die Wege großräumig aufgespalten werden und man bequem Komponenten in den Strahlengang einbringen kann. Theoretisch kann man die Vorgänge aber durchaus ausgehend vom bekannten Doppelspaltversuch betrachten.

1.2 Quantenmechanische Interpretation

Beschreiben wir das Licht nun mit dem Photonenbild.
Jedem Photon wird eine Wellenfunktion zugeordnet, deren Betragsquadrat der Aufenthaltswahrscheinlichkeit des Photons an einem Ort entspricht.
Für das Doppelspaltexperiment bedeutet dies nun, dass einem Photon, das durch Spalt 1 beziehungsweise durch Spalt 2 tritt, die Wellenfunktion (1) bzw. (2) zugeordnet wird.

(2) $$\Psi_{1,2} = \Psi'_{1,2} \cdot e^{i\vec{k}_{1,2} \cdot \vec{r}_{1,2}}$$

Die Gesamtwahrscheinlichkeit, ein Photon am Ort $\vec{r}$ auf dem Schirm zu finden beträgt dann (Abhängigkeiten weggelassen):

(3) $$I = |\Psi|^2 = |\Psi_1 + \Psi_2|^2 = |\Psi'_1|^2 + |\Psi'_2|^2 + Interferenzterm$$

Welcher-Weg-Information:

Fall 1: In jedem Interferometerarm steht nun ein Polarisator – beide sind gleich ausgerichtet, d.h., parallel zueinander orientiert.

Man stelle sich nun vor, dass jeweils nur ein einziges Photon durch den Aufbau läuft. Man drückt das oft so aus, dass das Photon „mit sich selbst“ interferiert. Quantenmechanisch gesehen bedeutet das, dass der Zustand des Photons eine Überlagerung der beiden Zustände „Photon befindet sich in Pfad 1“ und „Photon befindet sich in Pfad 2“ ist – jeder Zustand wird durch eine Wellenfunktion beschrieben (s. oben). Die Wahrscheinlichkeit für beide Möglichkeiten ist jeweils 50%. Das Intensitätsmuster, das man also am Schirm beobachten kann, nachdem viele einzelne Photonen den Aufbau durchlaufen haben, d.h. die Wahrscheinlichkeitsverteilung dieser Photonen, stellt sich als Interferenzmuster heraus. Wir wissen nicht, „welchen Weg es genommen hat“, da beide Wege ununterscheidbar sind.

Fall 2: Einer der Polarisatoren wird nun gegenüber dem anderen um 90° verdreht.

Da die Welcher-Weg Information aber in der Polarisationsrichtung enthalten ist, gewinnen wir die Information über den Weg, den das Photon genommen hat. Dies resultiert im Verschwinden des Interferenzmusters, da die beiden Wege nun unterscheidbar sind. Auf dem Schirm erscheint eine Intensitätsverteilung ohne Interferenzmuster.

Quantenradierer:

In diesem Experiment sollten die beiden Polarisatoren im Aufbau zunächst um 90° gegeneinander verdreht sein, sodass - aufgrund der Weginformation – keine Interferenz beobachtbar ist. Dann wird der dritte Polarisator zwischen den letzten Strahlteiler und einen Schirm mit eingebaut, der sog. „Radierer“. Der Radierer ist um 45° gegenüber den beiden anderen Polarisatoren orientiert.

Sind die beiden Polarisatoren im Aufbau zunächst um 90° gegeneinander verdreht, so ist - aufgrund der Weginformation – keine Interferenz beobachtbar. Dann wird der dritte Polarisator zwischen den letzten Strahlteiler und einen Schirm eingesetzt, der sog. „Radierer“. Der Radierer ist um 45° gegenüber den beiden anderen Polarisatoren orientiert. Hinter dem Radierer erscheint nun wieder ein Interferenzmuster auf dem Schirm, während auf dem anderen Schirm (ohne Radierer davor) keine Interferenz zu beobachten ist.

Diese Beobachtungen können folgendermaßen erklärt werden: Der Radierer stellt die Interferenz wieder her, da die Weginformation der Photonen nun nicht mehr vorhanden ist. Alle Photonen, die auf den Schirm treffen, weisen eine 45° Polarisation auf. Die Photonen, die am anderen Schirm ohne „Radierer“ ankommen, tragen diese Weginformation noch – es kann bestimmt werden, ob sie über Pfad 1 (0° Polarisator) oder Pfad 2 (90° Polarisator) gekommen sind. Somit ergibt sich am Schirm ohne Radierer keine Interferenz.

Achtung: Es soll hier nochmals darauf hingewiesen werden, dass das Experiment in dieser Form rein klassisch per Elektrodynamik erklärt werden kann. Würde man das Experiment mit Einzelphotonen durchführen (was teuer und aufwändig ist), könnte man aber dieselben Beobachtungen machen, die dann nur noch quantenmechanisch erklärt werden könnten. Gerade für den Unterricht ist aber ein klassischer Analogieaufbau wie dieser gut geeignet, um quantenmechanische Prinzipien zu veranschaulichen.

2. Quantenkryptographie

Kryptografie, die Verschlüsselung von Botschaften und Daten, ist seit jeher ein fundamentales Thema der Kommunikation. Über die Jahrhunderte wurde eine mannigfaltige Anzahl von Methoden entwickelt, um der Entschlüsselung durch Dritte entgegenzutreten. Sie alle weisen aber Angriffspunkte auf, sodass keine Methode als vollkommen sicher gilt. Dies änderte sich erst durch die geschickte Einführung der Quantenphysik, welche eine prinzipielle Abhörsicherheit garantieren kann. Die hierfür wesentlichen Methoden sind das *One-Time-Pad* und die quantenphysikalische Schlüsselerzeugung nach dem *BB84 Protokoll*.

Das One-Time-Pad beschreibt lediglich, dass eine zufällige Anzahl von 0 und 1 einen perfekten Schlüssel für Datenübertragung darstellt. Addiert man diesen Schlüssel binär auf die Nachricht, ist die verschlüsselte Nachricht ebenso eine zufällige Folge von 0 und 1. Eine weitere binäre Addition des Schlüssels ergibt wieder die ursprüngliche Nachricht. Wenn nur der Sender („Alice“) und der Empfänger („Bob“) den Schlüssel kennen, dann kann die verschlüsselte Nachricht sogar öffentlich übertragen werden – das Abhören ist wegen des fehlenden Schlüssels sinnlos, da dem Schlüssel selbst keine Methodik oder Muster zugrunde liegt.

Die fundamentale Frage ist nun, wie es möglich ist, dass der Schlüssel auch wirklich nur Alice und Bob zur Verfügung steht. Hierfür wurde das sog. BB84-Protkoll entwickelt. Es beschreibt, wie ein Schlüssel generiert werden kann, den nur Alice und Bob kennen. Darüber hinaus, und das ist der riesige Vorteil, kann auch ein Lauschangriff von „Eve“ (engl. für „eavesdropping“ = abhören) ganz prinzipiell detektiert werden. Das Protokoll basiert auf der Wahl von zwei Basen (0° und 90°, bzw. -45° und 45°) für die Polarisation des Lichts. In jeder Basis kann man eine 0 (0° bzw. -45°) und eine 1 (90°, bzw. 45°) darstellen. Alice schickt in einer zufälligen Basis ein zufälliges Bit, Bob misst in einer zufälligen Basis. Sie tauschen sich dann über die Basis aus – ist sie unterschiedlich, wird die Messung verworfen; ist die Basis gleich, dann haben beide nun ein Schlüsselbit generiert. Da der öffentliche Austausch nur die Basis beinhaltete, ist das Bit anderen unbekannt. Versucht Eve sich zwischen Alice und Bob zu klinken, kann auch sie bei jedem Bit nur die Basis raten. Damit rät sie auch immer wieder die falsche Basis, wodurch sich automatisch Fehler ergeben, die Alice und Bob durch den Austausch einiger Testbits nachweisen können.

Der quantenphysikalische Aspekt liegt zum einen darin, dass man als Lichtquelle eine Einzelphotonquelle verwendet, damit ein Informations-Bit nur von einem Photon getragen wird und somit nicht kopiert werden kann. Zum anderen werden in Quantenkryptografiesystemen Zufallszahlen mittels quantenoptischer Prozesse generiert. Da die Quantenphysik „nur“ bei der Schlüsselgenerierung eine Rolle spielt, wird im englischsprachigen Raum auch weniger von „quantum cryptography“ geredet, sondern eher von „quantum key distribution“ (Quanten-schlüsselaustausch).

In diesem Praktikumsversuch wird nachgestellt, wie die Quantenkrypografie funktioniert. Insbesondere wird auch ein Lauschangriff durchgeführt und gezeigt, dass dieser detektierbar ist. Zunächst startet der Versuch mit Alice und Bob, die zufällig Basen wählen und dann durch den Basisabgleich einen geheimen Schlüssel erzeugen. Alice codiert und sendet die Nachricht, Bob empfängt und dekodiert sie. Danach setzt man Eve in den Aufbau und wiederholt die Durchführung. Alice sendet ein Bit, Eve versucht abzuhören und weiterzusenden, was sie empfangen hat. Schlussendlich vergleichen Alice und Bob wieder ihre Basen und auch ein paar Test-Bits. Durch Eve sind nun 25% der Test-Bits falsch – wodurch Eve eindeutig enttarnt ist.

Statt einzelner Photonen arbeitet dieser Versuch mit einem gepulsten Laser. Dementsprechend sind alle Ergebnisse rein durch die klassische Physik beschreibbar. Ein quantenphysikalischer Aufbau arbeitet mit einzelnen Photonen, funktioniert allerdings komplett identisch. Dadurch ist dieser Aufbau sehr gut als Analogieversuch verwendbar.

2.1 Einführung

Kryptografie beschreibt die Verschlüsselung von Daten, also das Unkenntlichmachen einer Nachricht, wodurch sie im Idealfall nur für den Sender und den Empfänger lesbar ist. Der Besitz der verschlüsselten Nachricht hat also nur dann Sinn, wenn der Schlüssel zum Decodieren bekannt ist. Die Sicherheit des Schlüssels beruht entweder auf der komplexen zugrunde liegenden Algorithmik oder auf praktischen Hemmnissen, wie der Faktorisierung großer Zahlen.
Allen klassischen Kryptografieverfahren ist allerdings gemein, dass sie nie sicher sein können, dass der Schlüssel nicht doch „geknackt“ wird. Dieses fundamentale Problem kann allerdings durch den Einsatz der Quantenphysik gelöst werden; sie bietet die Möglichkeit, einen zufälligen Schlüssel zu generieren, der nur dem Sender und dem Empfänger bekannt ist, ein Abhörversuch wird ganz prinzipiell erkannt.
Einen Anreiz für die Diskussion der Quantenkryptografie stellt der Fakt dar, dass diese Vision bereits in die Wirklichkeit umgesetzt ist. Quantenkryptografie-Systeme sind bereits kommerziell erhältlich.
Das One-Time Pad

Das „One-Time Pad“, oder Einmalschlüssel-Verfahren, stellt ein Verschlüsselungsverfahren dar, das prinzipiell 100% sicher ist, wenn alle Voraussetzungen vollständig erfüllt werden. Die Quantenphysik hilft lediglich bei der Erfüllung der Voraussetzungen, das Verfahren selbst ist klassisch.

Man stelle sich vor, dass man eine komplett zufällige Folge von 0 und 1 hat, sogenannte „Bits“ (jede Information kann ja binär kodiert werden). Hat man nun eine Nachricht, die ebenfalls aus Nullen und Einsen besteht, kann man beide binär addieren und erhält damit eine Kette von Nullen und Einsen, die auch wieder komplett zufällig ist. Das ist die verschlüsselte Nachricht.

Für die binäre Addition gelten die „Rechenregeln“

- 0 + 0 = 0
- 1 + 0 = 1
- 0 + 1 = 1
- 1 + 1 = 0

Der Empfänger empfängt die verschlüsselte Nachricht, addiert ebenfalls den Schlüssel binär auf die verschlüsselte Nachricht und erhält wieder die ursprüngliche Nachricht.

Als Beispiel diskutieren wir das Wort „Test“, das mit der Tabelle in Anhang C binär kodiert werden kann:

Wort	T	E	S	T

Wort binär	1	0	0	1	1	0	0	1	0	0	1	0	0	1	0	1	0	0	1	1
										+										
Schlüssel (zufällig)	1	1	0	1	0	1	0	0	0	1	1	0	1	0	0	1	1	1	0	1
										⇩										
Verschl. Nachricht	0	1	0	0	1	1	0	1	0	1	0	0	1	1	0	0	1	1	1	0
										+										
Schlüssel (wie oben)	1	1	0	1	0	1	0	0	0	1	1	0	1	0	0	1	1	1	0	1
										⇩										
Wort binär	1	0	0	1	1	0	0	1	0	0	1	0	0	1	0	1	0	0	1	1
										⇩										
Wort	T					E					S					T				

Wird die verschlüsselte Nachricht abgefangen, so kann der Lauscher damit nur etwas anfangen, wenn er den Schlüssel kennt. Da diese Folge von Nullen und Einsen aber komplett zufällig war, hat er auch keinen Anhaltspunkt zum „Knacken“ des Schlüssels. Damit ist die Nachricht komplett abhörsicher.

Fassen wir also die nötigen Voraussetzungen zusammen:

1. Der Schlüssel muss mindestens so lang sein wie die Nachricht.
2. Der Schlüssel darf nur einmal verwendet werden.
3. Der Schlüssel muss komplett zufällig sein.
4. Der Schlüssel darf nur dem Sender und dem Empfänger bekannt sein.

Die Voraussetzung 1 lässt sich leicht durch den Sender erfüllen, der eben nur so viele Bits verschlüsseln kann, wie er Schlüsselbits zur Verfügung hat.

Die Voraussetzung 2 liegt in der Verantwortung von Sender und Empfänger, was also auch leicht realisierbar ist.

Die Voraussetzung 3 ist bei genauerem Hinsehen schwierig, denn hinter jedem Zufallszahlgenerator steckt letztlich ein Algorithmus. Somit sind vom Computer generierte Zufallszahlen immer nur „Pseudozufallszahlen“. Hier kann allerdings die Quantenphysik Abhilfe schaffen, da sie echten Zufall ermöglicht (siehe 2.5).

Die Voraussetzung 4 ist ebenfalls problematisch, denn die klassische Übermittlung eines Schlüssels lässt ja die Möglichkeit zu, ihn abzufangen. Auch dieses Problem lässt sich wieder quantenphysikalisch beheben. Das Vorgehen zur geheimen Verteilung des Schlüssels wird im nächsten Unterkapitel besprochen.

2.2 Schlüsselverteilung – $\lambda/2$-Platte und Datenübertragung mit einer Basis

Dieses Unterkapitel dient nur dazu, einen leichteren Zugang zum Verständnis des Aufbaus zu ermöglichen, indem kurz durchgespielt wird, wie Daten mit einer Basis übertragen werden. Die richtige Quantenkryptografie (in der realen Welt und diesem Analogie-Experiment) arbeitet mit zwei Basen, was im nächsten Unterkapitel beschrieben ist.

Zur Übertragung einer „0“ bzw. „1“ soll ein Photon verwendet werden. Als Bit wird dabei die Polarisationsrichtung verwendet: Ist das Photon horizontal polarisiert, interpretieren wir das als „0“, ist es vertikal polarisiert als „1“.

Wie sähe nun ein experimenteller Aufbau aus, der damit Daten übertragen kann? Ein Beispiel ist in Abb. 2 gezeigt.

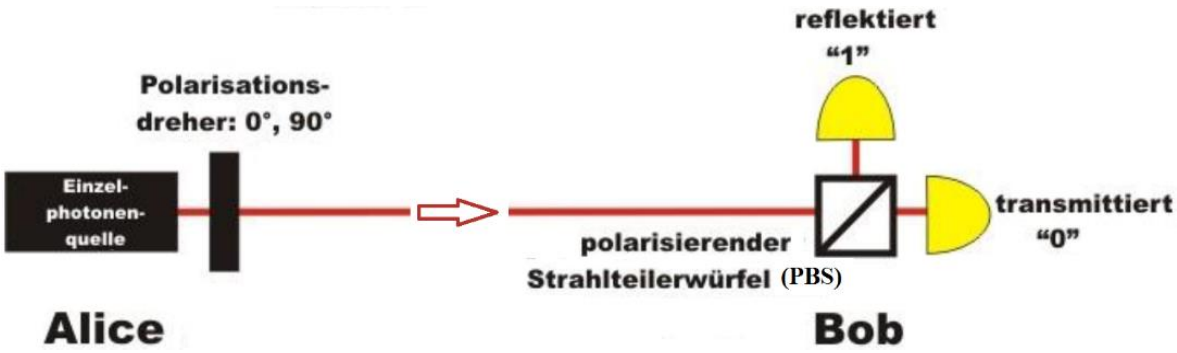
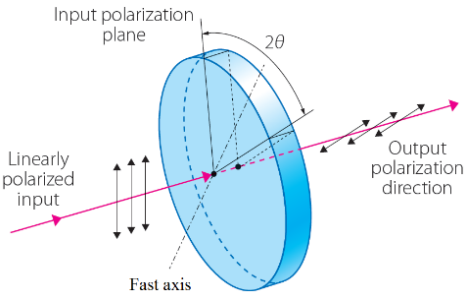


Abb. 2: Datenübertragung mit einer Polarisations-Basis

Die Sende-Einheit „Alice" besteht aus der Einzelphotonquelle und einer **$\lambda/2$-Platte**.

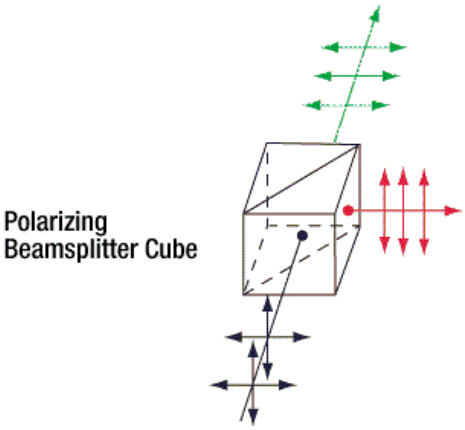
Die $\lambda/2$-Platte dreht die Polarisation um das Doppelte ihres Drehwinkels.
Dreht man sie also um 45°, dann wird die Polarisation des durchtretenden Lichts um 90° gedreht. Deshalb wird wir hier auch synonym den Begriff „Polarisationsdreher" verwendet.
Wenn wir ab jetzt den Einstellungen „0°" und „90°" sprechen (bzw. später von „-45°" und „45°"), dann ist damit immer der *Drehwinkel der Polarisation* gemeint und nie der Drehwinkel der $\lambda/2$-Platte.

Eine Skizze sieht man in der Abbildung rechts. Die einlaufende Polarisation wird an der optischen Achse (= "Fast axis") „gespiegelt", sodass der Drehwinkel der Polarisation zweimal so groß ist wie die Drehung der $\lambda/2$-Platte.



Aus der Lichtquelle treten Photonen aus, die horizontal polarisiert sind.

Die Empfänger-Einheit „Bob" besteht aus einem polarisierenden Strahlteilerwürfel und zwei Detektoren. Der polarisierende Strahlteilerwürfel reflektiert den vertikal polarisierten Anteil, s. rechts.



Bleibt der Polarisationsdreher also auf 0° eingestellt, dann tritt das Photon durch den Strahlteiler. Dieses Ereignis nennen wir dann „0". Stellen wir den Polarisationsdreher so ein, dass er die Polarisation um 90° dreht, dann wird das Photon reflektiert und wir nennen das Ereignis „1".

2.3 Schlüsselverteilung – jetzt aber richtig

Die Methode mit einer Basis (also 0° oder 90°) reicht zwar, um Daten von Alice zu Bob zu übertragen, nicht jedoch um die Abhörsicherheit zu gewährleisten. Dafür kommt eine zweite Basis ins Spiel. Neben der Basis mit 0° und 90°, die wir aber jetzt als „+ Basis" bezeichnen, kommt eine zweite Basis mit -45° und 45° dazu. Diese bezeichnen wir ab jetzt als „x Basis".

Der Aufbau sieht dann aus wie in Abb. 3. Das ist auch der Aufbau, wie er für die Quantenkryptografie und für dieses Versuchspaket verwendet wird.

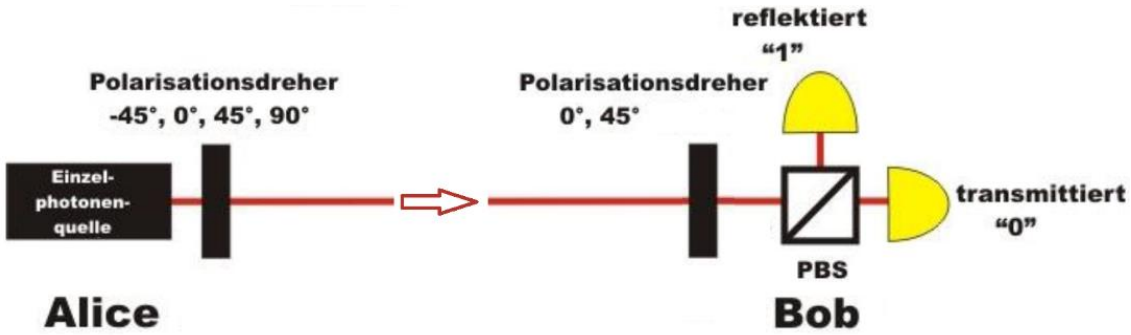


Abb. 3: Quantenkryptografie-Aufbau, mit den Basen + (= 0° und 90°) und x (= -45° und 45°)

Für die Schlüsselgenerierung muss sich Alice nun zweimal *zufällig* entscheiden:

- Alice muss zufällig ihre Basis wählen, also + oder x
- Alice muss zufällig das Bit wählen, also 0 oder 1
    - Die Wahl von 0 bedeutet in der + Basis die Einstellung 0°
    - Die Wahl von 1 bedeutet in der + Basis die Einstellung 90°
    - Die Wahl von 0 bedeutet in der x Basis die Einstellung -45°
    - Die Wahl von 1 bedeutet in der x Basis die Einstellung 45°

Bob entscheidet sich zwischen der + und der x Basis. Entsprechend benötigt er nur die Einstellungen 0° und 45°.

Hat Bob die + Basis gewählt und Alice sendet in der + Basis, dann erhält er ein eindeutiges Ergebnis; genauso, wenn beide die x Basis wählen. Was ist nun aber, wenn Bob eine andere Basis wählt als Alice? Klassisch trifft dann z.B. 45° polarisiertes Licht auf den Strahlteiler. Dieser wird folglich die Hälfte transmittieren und die Hälfte reflektieren. Ist allerdings nur ein Photon im Aufbau, so kann nur einer der Detektoren ansprechen. Welcher von beiden dies tut, ist dann dem Zufall überlassen. Passen also beide Basen nicht zueinander, wird Bob trotzdem ein Signal an einem der beiden Detektoren messen. Die Wahrscheinlichkeit, mit der das Photon an einem der beiden Detektoren detektiert wird, ist dann jeweils 50%.

In der folgenden Tabelle sind die verschiedenen Fälle noch einmal zur Übersicht dargestellt:[1]

Alice			Bob				Basen gleich?
Basis	Bit	=> Winkel	Basis	Winkel	Detektor „0“	Detektor „1“	
+	0	0°	+	0	**100%**	0%	Ja
+	1	90°	+	0	0%	**100%**	Ja
x	1	45°	+	0	50%	50%	Nein
x	0	-45°	+	0	50%	50%	Nein
+	0	0°	x	45°	50%	50%	Nein
+	1	90°	x	45°	50%	50%	Nein
x	1	45°	x	45°	0%	**100%**	Ja
x	0	-45°	x	45°	**100%**	0%	Ja

[1] Falls man in anderen Umsetzungen dieses Versuchs eine leicht variierte Tabelle vorfinden sollte, dann ist dies wahrscheinlich dadurch verursacht, dass die Polarisation des einfallenden Lasers unterschiedlich ist. Ist sie nämlich vertikal, dann wird aus den 0° (Alice) und 0° (Bob) eine digitale 1.

Alice sendet nun also zufällige Bits in zufälligen Basen, Bob analysiert das Signal in einer zufälligen Basis – wie wird nun daraus der Schlüssel für die Datenübertragung?

Die Antwort darauf ist, dass sich beide nach einer gewissen Zeit über einen öffentlichen Kanal über ihre BASEN austauschen, denn man beobachtet in den letzten drei Spalten der Tabelle, dass das Ergebnis genau dann eindeutig ist, wenn die Basen gleich sind.

Alice und Bob gehen also jede einzelne Messung durch und sagen nur „+“ oder „x“. Wenn beide unterschiedlich sind, dann verwerfen beide die Messung. Sind beide Basen aber gleich, dann haben BEIDE Kenntnis, welches BIT übertragen wurde – obwohl sie öffentlich immer nur über die BASEN geredet haben. Die Messungen mit den übereinstimmenden Basen liefern somit die Bits für den Schlüssel.

Sobald Alice und Bob auf diese Art alle Messungen durchgegangen sind, sind beide im Besitz des (zufälligen) Schlüssels. Nun kann Alice die Nachricht verschlüsseln und sie in der + Basis senden. Bob empfängt die Nachricht in der + Basis und kann sie anschließend entschlüsseln.

Im Folgenden wird nun noch das Erstaunliche gezeigt, nämlich dass in diesem Protokoll die Anwesenheit eines Lauschers unweigerlich Fehler erzeugt.

2.4 Detektion eines Lauschers

Betrachten wir also die Situation, dass sich ein Lauscher „Eve“ zwischen Alice und Bob setzt. Eve besteht aus denselben Teilen wie Alice und Bob, nur in umgekehrter Reihenfolge. Dies ist in Abb. 4 dargestellt.

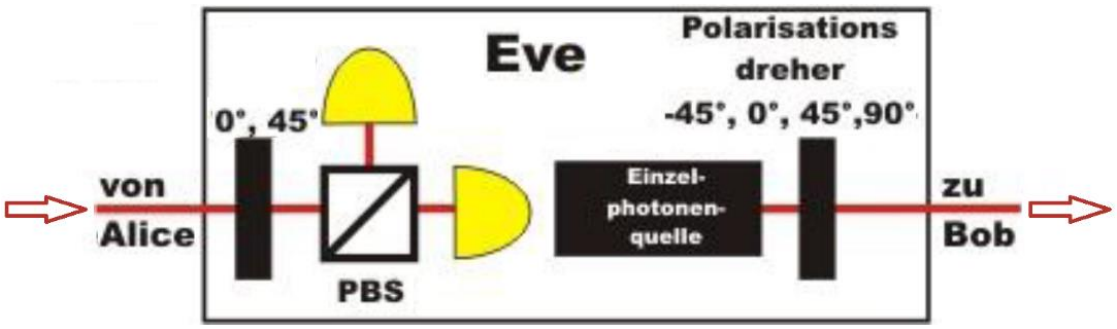


Abb. 4: Lauscher Eve zwischen Alice und Bob

Eve vermisst also das Licht, das von Alice kommt und versucht die Information identisch an Bob weiterzuleiten. Dabei gibt es nun zwei Möglichkeiten:

- Eve wählt die gleiche Basis wie Alice: dann erhält sie das richtige Ergebnis und kann den Polarisationszustand, den Alice losgeschickt hat, auch an Bob weitersenden. Bob wählt nun zufällig seine Basis, auch da gibt es zwei Möglichkeiten:
    - Bob wählt die gleiche Basis wie Alice: Eve hat das Signal in dieser Basis richtig weitergeleitet. Damit erhält Bob genau den von Alice gesendeten Polarisationszustand, ohne die Anwesenheit von Eve zu bemerken.
    - Bob wählt die andere Basis: Dann hat er auch eine andere Basis als das Signal, was Eve weitergeleitet hat. Dementsprechend wird einer seiner Detektoren zufällig anspringen. Wenn nun allerdings Alice und Bob ihre Basen vergleichen (gleiches Vorgehen wie im vorigen Unterkapitel), dann wird diese Messung ohnehin aufgrund der unterschiedlichen Basen verworfen.
- Eve wählt die falsche Basis: Dann wird zufällig einer der beiden Detektoren anspringen. Eve kann natürlich nicht beurteilen, ob die Wahl ihrer Basis richtig war oder nicht und schickt

dementsprechend das Signal in der Basis weiter, mit der sie gemessen hat. Bob wählt nun zufällig seine Basis, auch da gibt es zwei Möglichkeiten:

- Bob wählt eine andere Basis als Alice: Auch diese Messung wird wieder beim Basen-Vergleich von Alice und Bob verworfen.
- Bob wählt die gleiche Basis wie Alice: Dieser Fall ist der, der den Fehler erzeugt, der Eve verrät. Zur Erinnerung: Alice und Bob haben die gleiche Basis, die Messung wird also nicht verworfen. Allerdings hat Eve zwischendurch in einer anderen Basis abgehört! Es fanden also bis inkl. Messung der Messung zwei zufällige Detektionen statt: die von Eve (weil ihre Basis nicht zu Alice' Basis passte) und die von Bob (weil seine Basis nicht zu Eves Basis passte). In der Hälfte der Fälle spricht der richtige Detektor bei Bob an, sodass er das gleiche Bit empfängt, das Alice gesendet hat. In der anderen Hälfte der Fälle detektiert aber der andere Detektor das Photon. Somit erhält Bob ein anderes Bit als das von Alice!

Fassen wir kurz zusammen: es gibt einen Fall, bei dem Alice und Bob trotz *gleicher Basen unterschiedliche Bits* erhalten (was ohne Eve nie passiert). Der Test auf einen Spion ist demnach einfach: Es werden generell deutlich mehr Schlüsselbits generiert, als zur eigentlichen Verschlüsselung der Nachricht benötigt werden. Nachdem Alice und Bob ihre Basen verglichen haben, wählen sie eine gewisse Menge der nicht tatsächlich zur Verschlüsselung der Nachricht benötigten Bits als Test-Bits aus, die sie öffentlich vergleichen. Sind diese Test-Bits identisch, dann war kein Lauscher im System.[2] Haben sich in etwa 25% Fehler eingeschlichen, dann wurde offenbar abgehört!

Nun könnte man einwenden, dass man damit Eve aber erst nach dem Abhören entdeckt – das ist aber nicht der Fall, denn bisher wurde ja nur der Schlüssel generiert. Selbst wenn Eve abgehört hat (und damit eine gewisse Menge von Bits unbemerkt abgehört hat), hat das keine Konsequenz, denn es wurde schließlich noch kein Teil der eigentlichen Nachricht übermittelt.

Zur Übersicht werden hier die einzelnen Fälle noch einmal kurz in einer Tabelle dargestellt. Dabei werden nur die Fälle berücksichtigt, in denen die Basen von Alice und Bob gleich sind – die anderen Messungen werden ja ohnehin beim Basenvergleich gestrichen.[3]

Basis von Alice und Bob	Basis von Eve	Fehler?	Übereinstimmung der Bits von Alice und Bob
+ +	+	Nein	100%
+ +	x	Zum Teil	50%
x x	+	Zum Teil	50%
x x	x	Nein	100%

2.5 Was heißt „zufällig"?

Wie oben beschrieben, basiert das One-Time Pad u.a. darauf, dass der Schlüssel komplett zufällig gewählt wird. Computergenerierte Pseudozufallszahlen sind also keine Lösung für eine 100%ige Sicherheit. In der

[2] Wobei man festhalten muss, dass es statistisch den Fall gibt, dass alle Test-Bits zufällig richtig sind. Dementsprechend darf die Anzahl der Test-Bits nicht zu klein sein, um auch wirklich in etwa 25% zu erhalten.

[3] Die 25% lassen sich aus der Tabelle wie folgend ablesen: es reicht zunächst mal eine Basis zu betrachten, die andere verhält sich genauso: Wenn Alice und Bob die + Basis wählen, dann wählt Alice in 50% der Fälle auch die + Basis. Diese Fälle können nicht entdeckt werden. In 50% der Fälle wählt sie aber die x Basis. Zu 50% spricht aber bei Bob der Detektor für das richtige Bit an, obwohl seine Basis mit der von Eve nicht übereinstimmt. In den restlichen 50% spricht der Detektor mit dem falschen Bit an. Der Fehler ist also 50%*50% = 25%.

Quantenphysik gibt es den Zufall aber im Überfluss: Ein Photon, dass auf einen 50:50 Strahlteiler trifft, wird rein zufällig transmittiert oder reflektiert. Im Mittel wird je die Hälfte transmittiert und die andere Hälfte reflektiert, die „Entscheidung" des einzelnen Photons ist aber komplett zufällig. Dies trifft nicht nur auf Photonen zu, auch viele weitere Prozesse wie radioaktiver Zerfall sind quantenphysikalisch komplett zufällig.

Dies macht man sich nun zunutze, indem man z.B. das Ereignis „Photon wird am Strahlteiler reflektiert" als binäre 0 und das Ereignis „Photon wird transmittiert" als binäre 1 interpretiert. Dies kann auch mit klassischem Licht geschehen, das man auf zwei Einzelphotondetektoren hinter einem Strahlteiler leitet. Ist die Intensität an den Detektoren gleich, dann ist auch das Anschlagen der Detektoren komplett zufällig verteilt.

Quantenphysikalische Zufallszahlgeneratoren sind somit ein wesentlicher Bestandteil von quantenkryptografischen Datennetzen. Auch sie sind bereits kommerziell erhältlich.

2.6 Warum kann man die Information nicht kopieren?

Was wäre, wenn Eve das Photon, das die Information trägt, einfach kopieren könnte? Dann wäre die Sicherheit der Quantenkryptografie dahin, denn dann könnte sie das ursprüngliche Photon weiter zu Bob schicken und ihre Messung am kopierten Photon durchführen. Somit könnte sie prinzipiell die Schlüsselbits abhören, ohne dass Alice und Bob davon erfahren würden.

„Praktischerweise" verbietet die Quantenphysik aber das genaue Kopieren eines quantenphysikalischen Zustands. Dieses Prinzip ist unter dem Begriff „No-Cloning-Theorem" bekannt, welches 1982 formuliert und bewiesen wurde[4]. Damit ist sichergestellt, dass Eve nie das ursprüngliche Photon vermessen oder kopieren kann, ohne seinen Zustand zu verändern.

2.7 Wie läuft das Experiment ab?

Die Abfolge der Schritte wurde im sogenannten BB84-Protokoll festgehalten[5].
Der für diesen Versuch wichtige Ablauf ist wie folgend:

1. Schlüsselübertragung	• Alice wählt zufällig eine Basis (also x oder +) und ein Bit (also 0 oder 1). Bob wählt zufällig seine Basis (also x oder +). Beide stellen ihre lambda/2 Platten entsprechend ein. Dann wird das Photon durch den Aufbau geschickt (bei uns der Laserpuls). • Bob schreibt auf, ob er eine 0 oder eine 1 gemessen hat.
2. Löschen falscher Basen	Alice und Bob gehen die Messungen durch und sagen sich gegenseitig, welche Basen Sie gewählt haben. Sie behalten die Ergebnisse, bei denen die Basen gleich waren (den Rest streichen sie durch). Dabei verraten beide nur die Basen und nicht die übertragenen und gemessenen Bits! Der Sinn: Sie wissen jetzt beide, welche Bits übrig bleiben (haben also einen geheimen Schlüssel), haben sich aber nur über die Basen ausgetauscht.
3. Testen auf Spion	Alice und Bob vergleichen einige der übertragenen Bits mit der gleichen Basis. Bei Fehlern war ein Spion in der Leitung und der übertragene Schlüssel wird gelöscht. Die Bits zum Testen der

[4] http://www.nature.com/nature/journal/v299/n5886/pdf/299802a0.pdf
[5] http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf

	Anwesenheit eines Spions werden aus dem eigentlichen Schlüssel gelöscht.
4. Verschlüsseln der Nachricht	Nachdem der Schlüssel generiert wurde und sicher ist, dass nicht abgehört wird, kann Alice die Nachricht verschlüsseln.
5. Übermittlung der Nachricht	Alice schickt die verschlüsselte Nachricht an Bob. Dies geschieht öffentlich.
6. Entschlüsseln der Nachricht	Bob entschlüsselt die Nachricht mit Hilfe des zuvor erzeugten Schlüssels.

Im Protokoll gibt es noch weitere Schritte, die aber für den vorliegenden Versuch nicht umgesetzt werden:

- Authentifizierung: Bereits am Anfang der Kommunikation werden einige Bits ausge-tauscht. Um für jede neue Kommunikation genügend Bits für die Authentifizierung zu haben, werden immer ein paar Bits des aktuellen Schlüssels gespeichert. Diese Schlüsselbits sind nur Alice und Bob bekannt. Wie bei der Schlüsselerzeugung legen Alice und Bob nun wieder zufällige Basen fest, in denen sie Senden bzw. Empfangen werden. Nach der Übertragung tauschen sie sich wieder öffentlich über die verwendeten Basen aus und können einen potentiellen Lauscher sofort erkennen falls die von Bob empfangenen Bits trotz gleicher Basiswahl nicht mit den bekannten Schlüsselbits übereinstimmen.
- Fehlerkorrektur: Da nicht jedes System perfekt ist und immer Messfehler auftreten, gibt es bestimmte Algorithmen, die zur Fehlerkorrektur eingesetzt werden. Auf diese soll hier aber nicht weiter eingegangen werden.

2.6 Klassisches Licht vs. einzelne Photonen

An dieser Stelle sei noch einmal darauf hingewiesen, dass echte Abhörsicherheit nur bei Verwendung einer Einzelphotonquelle gewährleistet ist. Die Information eines Bits darf also nur von einem einzelnen Photon getragen werden, denn dieses kann nicht kopiert und nicht ohne Veränderung vermessen werden.

Hat man statt einer Einzelphotonquelle allerdings nur klassisches Licht zur Verfügung (und dazu zählen auch abgeschwächte Laser!), dann könnte Eve nicht erkannt werden - schließlich bräuchte sie nur einen winzigen Teil des Lichts zur Detektion/Analyse abzweigen und könnte den Rest unbemerkt an Bob weiterschicken.

Dies macht auch noch einmal deutlich, dass es sich beim vorliegenden Versuchsset um ein **Analogie**-Experiment handelt – der Ablauf des Protokolls ist aber komplett identisch zum quantenphysikalischen Fall.

3. Aufgaben zur Vorbereitung

Die Aufgaben sind vorbereitet zum Praktikumstermin mitzubringen.

Aufgaben zum Quantenradierer

Aufgabe 1a:
Skizzieren Sie (nur ganz prinzipiell) das Doppelspaltexperiment und dessen wesentliches Ergebnis. Begründen Sie, dass für die Intensität am Beobachtungsschirm gilt:

$$(1) \qquad I \sim \left|\vec{E}_1\right|^2 + \left|\vec{E}_2\right|^2 + 2\left|\vec{E}_1\right|\left|\vec{E}_2\right|\cos\delta$$

Welche physikalische Bedeutung hat dabei der Term $2\left|\vec{E}_1\right|\left|\vec{E}_2\right|\cos\delta$ *?*

Erweitert man nun den Versuchsaufbau durch zwei Polarisationsfilter P_1 und P_2, die jeweils hinter einem der Spalte mit den Einstellungen 0° beziehungsweise 90° positioniert werden, so wird am Schirm die Interferenzverteilung verschwinden und eine kontinuierliche Intensitätsverteilung erscheinen.

Aufgabe 1b:
Erklären Sie, wieso! Wie sieht Gleichung (1) nun aus?

Wird nun der Aufbau um einen dritten Polarisationsfilter P_3 mit der Einstellung 45° erweitert, der hinter dem letzten Strahlteiler eingebracht wird, so erhält man wieder ein Interferenzmuster.

Aufgabe 1c:
Erklären Sie, wieso!

Aufgabe 2a:
Welche Bedeutung hat hier der Interferenz-Term, nachdem es sich doch um einzelne Photonen handelt? Paul Dirac prägte einmal den Begriff „Interferenz des Photons mit sich selbst“? Wie ist diese Aussage zu interpretieren?

Nun erweitert man den Aufbau wieder mit den beiden Polarisationsfiltern P_1 und P_2, deren Einstellungen 0° beziehungsweise 90° betragen. Für ein einzelnes Photon bedeutet das, dass man seinen Weg nachvollziehen kann. Man kann also feststellen, welchen Weg das Photon genommen hat und spricht somit von einer **Wegmarkierung**.

Aufgabe 2b:
Wie sieht demnach Gleichung (3) aus? Was beobachtet man am Schirm und wie interpretiert man dies quantenmechanisch?

Aufgabe 2c:
Warum erhält man durch die Einstellung der Polarisationsfilter auf 0° bzw. 90° eine Weginformation?

Aufgabe 2d:
Was passiert, wenn man den dritten Polarisationsfilter vor dem Schirm einbringt?

***Aufgabe 2e*:**
Ein Gedankenexperiment von John Wheeler: Was würde man am Schirm beobachten, wenn man den hinteren Strahlteiler erst in den Aufbau bringen würde, wenn das Photon rein rechnerisch bereits den ersten Strahlteiler und die gekreuzten Polarisatoren passiert hätte (sog. delayed choice Experimente)?

Im Praktikumsversuch verwenden wir nun das Interferometer und stellen die Polarisatoren nicht hinter Spalte, sondern in die beiden Arme des Interferometers – die theoretische Betrachtung bleibt dieselbe.

***Aufgabe 3a*:**
Das Interferenzmuster besteht aus hellen und dunklen konzentrischen Kreisen. Erklären Sie diese Form. Wie verändert sich das Muster, wenn ein Interferometerarm deutlich länger gebaut wird als der andere?

Aufgaben zur Quantenkryptographie

Aufgabe 1:
Erklären Sie kurz in eigenen Worten, was man unter dem „Quantenschlüsselaustausch" versteht. Wo steckt bei der „Quantenkryptografie" die Quantenphysik?

Aufgabe 2:
Worauf kommt es bei der Erstellung des Schlüssels an? Wo liegen Schwachpunkte?

Aufgabe 3:
Worin besteht die Sicherheit der Quantenkryptografie? D.h.

- *Warum kann ein quantenkryptografischer Code nicht geknackt werden, im Gegensatz zu anderen Verfahren?*
- *Warum ist das Verfahren abhörsicher bzw. wie kann der Lauscher Eve erkannt werden?*

Aufgabe 4:
Warum könnte eine Nachricht, die mit dem hier verwendeten Quantenkryptografie-Analogie-Versuchsaufbau übertragen wird, letztlich doch abgehört werden? Wie könnte Eve das in diesem Fall bewerkstelligen?

Aufgabe 5:
Was unterscheidet eine „Pseudozufallszahl" von einer „echten" Zufallszahl? Wie kann man diese Zahlen jeweils erzeugen?