THORLABS

Discovery

EDU-QCRY1
EDU-QCRY1/M
Quantenkryptografie - Analogieversuch

Handbuch

Inhaltsverzeichnis

Kapitel 1 Warnsymbole

Die hier aufgeführten Warnsymbole finden sie eventuell in diesem Handbuch oder auf dem Produkt.

Symbol	Beschreibung
	Gleichstrom
	Wechselstrom
	Gleich- und Wechselstrom
	Erdungsanschluss
	Schutzleiteranschluss
	Chassisanschluss
	Potenzialgleichheit
	An (Versorgung)
	Aus (Versorgung)
	Ein-Position
	Aus-Position
	Vorsicht: Risiko eines elektrischen Schlages
	Vorsicht: Heiße Oberfläche
	Vorsicht: Gefahr
	Warnung: Laserstrahlung

Kapitel 2 Sicherheitshinweise

WARNUNG

Das Lasermodul ist ein Klasse 2 Laser, der keine speziellen Schutzbrillen erfordert. Um Verletzungen zu vermeiden, sollte jedoch nicht direkt in den Strahl geblickt werden.

ACHTUNG

Um Verschmutzungen und Schäden zu vermeiden, sollten die $\lambda/2$ Platten nie mit bloßen Fingern berührt werden. Tragen Sie Schutzhandschuhe.

Kapitel 3 Kurzbeschreibung

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 einmalig verwendete, zufällige Folge von Nullen und Einsen 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 sogenannte 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 in 50% der Fälle 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“.

In diesem Versuchspaket wird nachgestellt, wie die Quantenkryptografie 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.

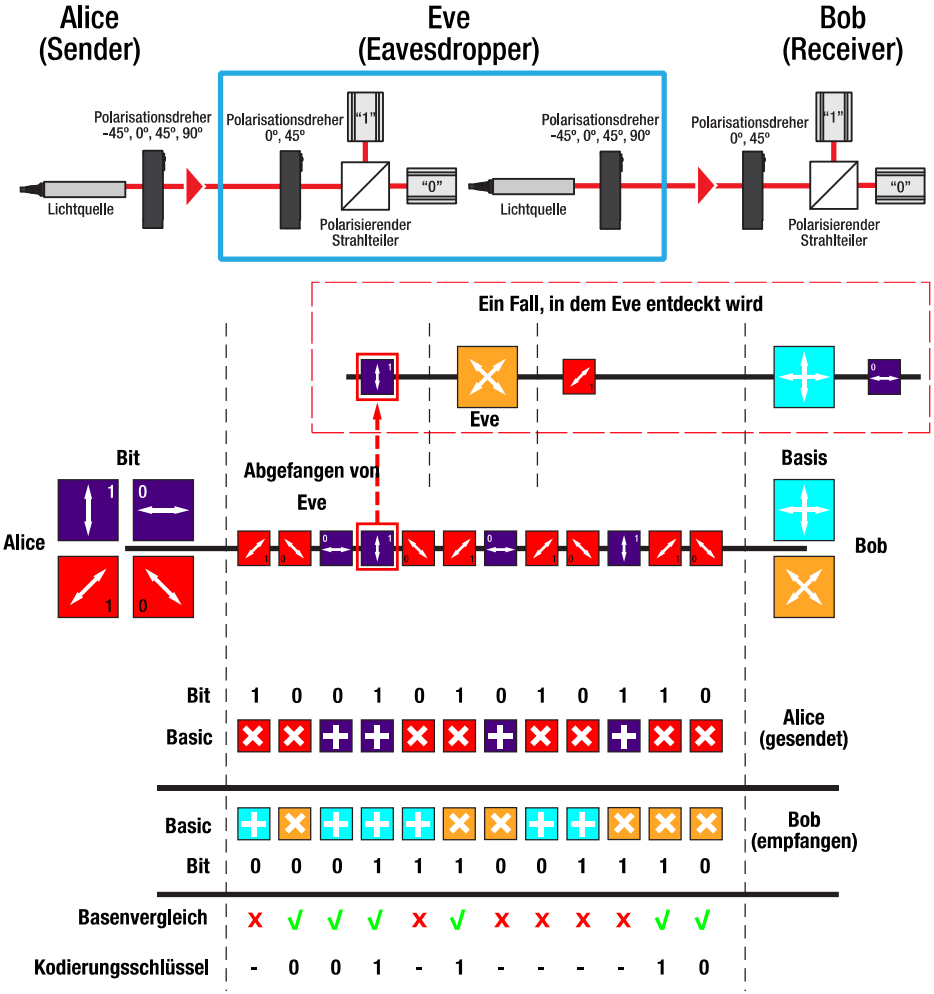


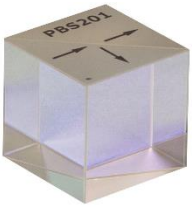
Abbildung 1 Überblick über den Quantenkryptografie-Versuch

Statt einzelner Photonen arbeitet dieser Versuch mit einem Laser, der auf Knopfdruck einen kurzen Laserpuls aussendet. 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.

Kapitel 4 Übersicht über die Einzelkomponenten

Für das metrische Versuchspaket gelten zum Teil andere Artikelnummern als für das zöllige Paket. Wenn die Nummern unterschiedlich sind, dann bezeichnet das „(/M)“ die metrische Komponente. Die Größenangaben in Klammern beziehen sich ebenfalls auf die metrischen Teile.

 1 x **MB8 (MB2020/M)** Aluminium Breadboard, 8" x 8" (20 cm x 20 cm)	 1 x **MB810 (MB2025/M)** Aluminium Breadboard, 8" x 10" (20 cm x 25 cm)	 1 x **MB1218 (MB3045/M)** Aluminium Breadboard, 12" x 18" (30 cm x 45 cm)
 3 x **RDF1** 4 Gummifüße	 10 x **BA1(/M)** Base, 1" x 3" x 3/8" (25 mm x 75 mm x 10 mm)	 5 x **PH2 (PH50/M)** Ø1/2" (Ø12.7 mm) Stiel-Halter, 2" (50 mm) lang
 6 x **PH1.5 (PH40/M)** Ø1/2" (Ø12.7 mm) Stiel-Halter, 1.5" (40 mm) lang	 2 x **UPH2 (UPH50/M)** Ø1/2" (Ø12.7 mm) Universal Stiel-Halter, 2" (50 mm) lang	 Zöllig: 6 x **TR1.5** Metrisch: 4 x **TR30/M,** 2 x **TR40/M** Ø1/2" (Ø12.7 mm) Stiel, 1.5" (30 mm, 40mm) lang

 7 x **TR2 (TR50/M)** Ø1/2" (Ø12.7 mm) Stiel, 2" (50 mm) lang	 2 x **RSP1X225(/M)-ALICE** Ø1" Drehhalter mit 22,5° Sprungmechanismus	 2 x **RSP1X225(/M)-BOB** Ø1" Drehhalter mit 22,5° Sprungmechanismus
 4 x **WPH10E-633** *λ*/2-Platte, Polymer Zero Order	 2 x **Kinematischer Halter** Modifizierter KM100PM(/M)	 2 x **PM3(/M)** Haltearm
 2 x **PBS201** Polarisierender Strahl-teilerwürfel, 20 mm x 20 mm	 2 x **KM100** Kinematischer Halter, Ø1"	 2 x **AD11NT** Ø1" Adapter für Ø11 mm Komponenten

 2 x **CPS635R-C2** Klasse 2 Laser, 635 nm	 1 x **BA1S(/M)** Kleine Base, 1“ x 2.3“ x 3/8“ (25 mm x 58 mm x 10 mm)	 1 x **AT1(/M)** Justierhilfe, Plexiglas 1.18” x 1.18” (30.0 mm x 30.0 mm)
 2 x **CL3/M** **Klemme**	 1 x **BBH1** Breadboard Griffe	 1 x **SPW606** SM1 Schlüssel
 4 x **Sensor**	 2 x **Sensorelektronik**	 2 x **Laserelektronik**

Zölliges Kit: Schrauben, Schraubenzieher, Inbusschlüssel

Typ	Anzahl	Typ	Anzahl
1/4"-20 x 3/8" Schraube	11	1/4" Unterlegscheibe	19
1/4"-20 x 1/2" Schraube	12	 1 x **BD-3/16L** Schraubenzieher für 1/4″-20 Schrauben	
1/4"-20 x 5/8" Schraube	17		
1/4"-20 x 1.25" Schraube	2		
1/4"-20 x 2" Schraube	2		
Inbusschlüssel: 9/64", 5/64" und 1/16"			
4 x AS4M8E: Gewindeadapter (Intern M4 x 0.7, Extern 8-32)			

Metrisches Kit: Schrauben, Schraubenzieher, Inbusschlüssel

Typ	Anzahl	Typ	Anzahl
M6 x 10 mm Schraube	11	M6 Unterlegscheibe	19
M6 x 12 mm Schraube	12	 1 x **BD-5ML** Schraubenzieher für M6 Schrauben	
M6 x 16 mm Schraube	17		
M6 x 30 mm Schraube	2		
M6 x 45 mm Schraube	2		
Inbusschlüssel: 3 mm, 2 mm und 1.5 mm			

Kapitel 5 Grundlagen der Quantenkryptographie

Dieses Kapitel erklärt, wie die Quantenkryptografie funktioniert und welche Prozessschritte für die Durchführung nötig sind. Es startet mit einer kurzen Einführung, erklärt danach das „One-Time Pad“, mit dem aus einer Nachricht und einem Schlüssel eine verschlüsselte Nachricht wird. Im Anschluss erfolgt die Generierung der Schlüssel, welche das wesentliche Element der Quantenkryptografie darstellt.

Der Wert der Quantenkryptografie liegt in der Abhörsicherheit, weshalb in Kapitel 5.4 diskutiert wird, wie und warum ein Lauscher ganz prinzipiell detektiert werden kann. Abschließend wird das ganze Protokoll noch einmal als Übersicht dargestellt.

5.1. Einführung

Kryptografie beschreibt die Verschlüsselung von Daten, also das Unkenntlichmachen einer Nachricht, wodurch sie im Idealfall nur für den Sender und dem Empfänger lesbar ist. Der Besitz der verschlüsselten Nachricht hat also nur dann Sinn, wenn der Schlüssel zum Decodieren bekannt ist. Die Sicherheit des Schlüssels besteht entweder in 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 wurde. Quantenkryptografie-Systeme sind kommerziell erhältlich, beispielsweise bei http://www.idquantique.com/quantum-safe-crypto/ .

5.2. 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 eine komplett zufällige Folge aus „Bits“ (Nullen und Einsen) vor, dem Kodierschlüssel. Hat man nun eine Nachricht, die ebenfalls aus Nullen und Einsen besteht (jede Information kann ja binär kodiert werden), 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 binar auf die verschlüsselte Nachricht, und erhält wieder die ursprüngliche Nachricht.

Als Beispiel diskutieren wir das Wort „Test“, das mit der Tabelle in der Versuchsdurchführung binär kodiert werden kann (eine Tabelle mit der binären Darstellung des Alphabets findet sich am Ende von Kapitel 9):

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. Dies wird in Kapitel 0 näher diskutiert.

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.

5.3. Schlüsselverteilung

5.3.1. $\lambda/2$-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 Analogieexperiment) 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 Abbildung 2 gezeigt.

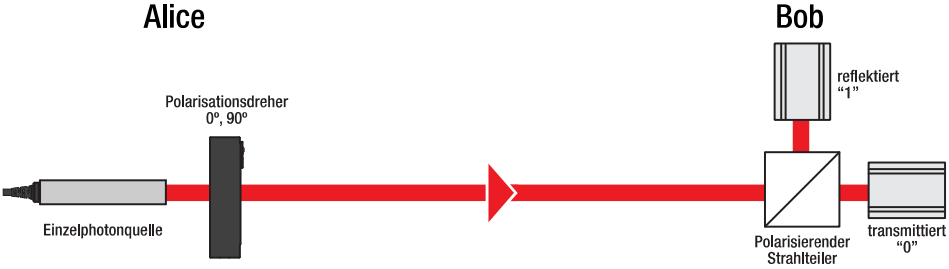


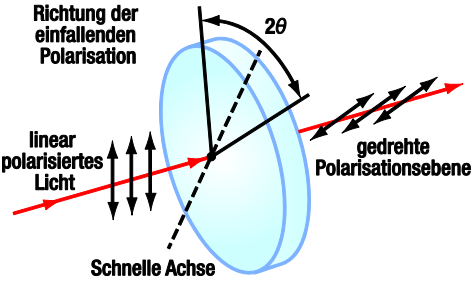
Abbildung 2 Datenübertragung mit einer Polarisations-Basis

Die Sende-Einheit „Alice“ besteht aus einer in horizontaler Richtung linear polarisierten 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 hier auch synonym der Begriff „Polarisationsdreher“ verwendet.

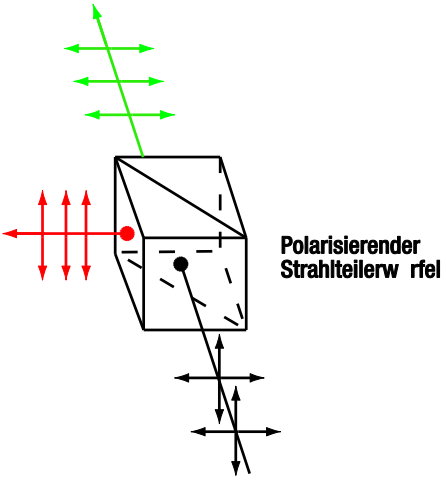
Wenn wir ab jetzt von den Einstellungen „0°“ und „90°“ sprechen (bzw. später von „-45°“ und „45°“), dann ist damit immer der *Drehwinkel der Polarisation* gemeint und nie der Drehwinkel der $\lambda/2$-Platte.

Eine Skizze zur Funktion der $\lambda/2$-Platte sieht man in der Abbildung rechts. Das doppelbrechende Material verlangsamt den Anteil des Lichts, der nicht in Richtung der „schnellen Achse“ polarisiert ist. Für einfallendes linear polarisiertes Licht bedeutet das eine Drehung der Polarisation. 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.



Die Empfänger-Einheit „Bob“ besteht aus einem polarisierenden Strahlteilerwürfel und zwei Detektoren. Der polarisierende Strahlteilerwürfel reflektiert den vertikal polarisierten Anteil, s. rote Pfeile im Bild rechts, und transmittiert den horizontal polarisierten Anteil des einfallenden Lichts.

Sendet Alice also Licht mit einer Einstellung von 0° am Polarisationsdreher (entspricht horizontaler Polarisation), dann tritt das Photon durch den Strahlteiler. Dieses Ereignis nennen wir dann eine binäre „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“.



5.3.2. 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 Abbildung 3. Das ist auch der Aufbau, wie er für die Quantenkryptografie und für dieses Versuchspaket verwendet wird.

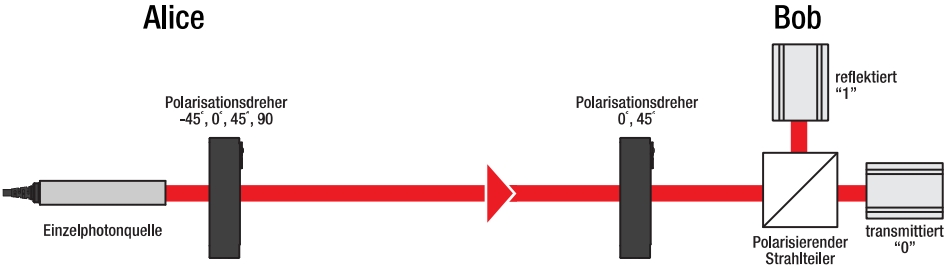


Abbildung 3 Quantenkryptografie-Aufbau, mit den Basen + (= 0° und 90°) und x (= -45° und 45°)

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
Basis	Bit	=> Winkel	Basis	Winkel	Detektor „0“	Detektor „1“	gleich?
+	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

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 ihre BASEN austauschen, denn man beobachtet in den letzten drei Spalten der Tabelle, dass das Ergebnis genau dann eindeutig ist (100%), 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 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 (und das sogar öffentlich!). 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, wodurch er von Alice und Bob nachgewiesen werden kann.

[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.*

5.4. 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 Abbildung 4 dargestellt.

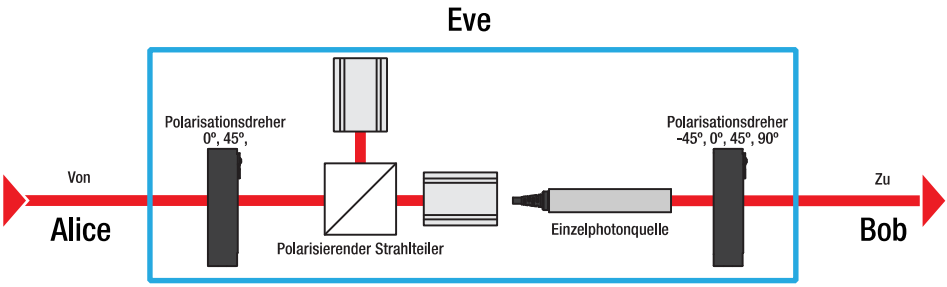


Abbildung 4 Lauscher Eve zwischen Alice und Bob

Eve vermisst also das Licht, das von Alice kommt und versucht die identische Information 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 weiter senden. 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, das 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. der Messung zwei zufällige Detektionen statt: die von Eve (weil ihre

Basis nicht zu Alices 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: Nachdem sie ihre Basen verglichen haben, wählen sie eine gewisse Menge der Bits mit übereinstimmenden Basen 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] 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 Eve 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%.

5.5. Was heißt „zufällig“?

Wie in Kapitel 5.2 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 Quantenphysik gibt es den Zufall aber im Überfluss: Ein Photon, das auf einen nicht-polarisierenden 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, siehe http://www.idquantique.com/random-number-generation/ .

5.6. 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. Damit ist sichergestellt, dass Eve nie das ursprüngliche Photon vermessen oder kopieren kann, ohne seinen Zustand zu verändern.

5.7. Wie läuft nun das Experiment ab?

Die Abfolge der Schritte wurde im sogenannten BB84-Protokoll festgehalten, die Originalpublikation findet sich hier

http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf

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. Dieser Schritt wird zahlreiche Male wiederholt.
2. Löschen falscher Basen	Alice und Bob gehen die Messungen durch und tauschen sich öffentlich über ihre Basen aus. 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 öffentlich 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 Anwesenheit eines Spions werden aus dem eigentlichen Schlüssel gelöscht. Übrig bleibt der Schlüssel, mit dem die Daten codiert werden.
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 ausgetauscht, und zwar nach einem vorher von Alice und Bob festgelegten Schlüssel. Treten hierbei keine Fehler auf, ist sicher, dass nicht schon zu Beginn ein Lauscher in der Leitung ist und auch wirklich Alice und Bob miteinander kommunizieren. Um für jede neue Kommunikation genügend Bits für die Authentifizierung zu haben, werden immer ein paar Bits der aktuellen Kommunikation gespeichert.
- Fehlerkorrektur: Da kein 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.

5.8. 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 nach Kapitel 5.6 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 kann 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.

5.9. Verschränkung

Eine manchmal auftretende Frage bezieht sich auf den Zusammenhang von Quantenkryptographie und Verschränkung. Zur Klärung ist wichtig zu wissen, dass das BB84 an sich zunächst keine polarisations-verschränkten Photonen voraussetzt. Dies lässt sich daran erkennen, dass das erste Paper zur Quantenkryptographie mit verschränkten Photonen erst nach 1984 publiziert wurde, vgl.

- A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991)
- C. H. Bennett, G. Brassard, N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992)

Weiterhin gibt es auf dem Feld der Quantenkryptographie enorme Fortschritte und auch neuere Protokolle, die zwar komplexer sind, aber nicht nur mit einem Photon pro Bit funktionieren. Es handelt sich hier um sogenannte „Decoy States“, vgl.

- W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003)
- H.-K. Lo, X. Ma. K. Chen, Phys. Rev. Lett. **94**, 230504 (2005)

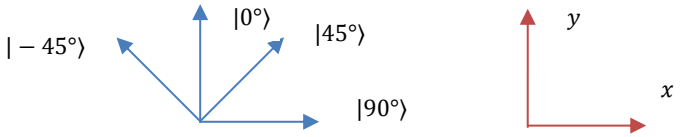
5.10. Mathematische Beschreibung in Dirac-Notation

Bis zu diesem Punkt wurden die hier durchgeführten Experimente qualitativ beschrieben. Die Präparation des Polarisationszustands und die Messung durch Bob (bzw. Eve) sind anschaulich gut verständliche Inhalte. Allerdings bedarf jede physikalische Theorie auch der mathematischen Beschreibung. An dieser Stelle soll nun das Experiment in Formeln gegossen werden.

Am Anfang steht die Wahl einer geeigneten Notation. Für Polarisationszustände bietet sich die Bra-Ket-Notation (nach Dirac) an. Die vier Polarisationszustände, um die es in diesem Experiment geht, werden darin symbolisch als

$$|-45°\rangle,\ |0°\rangle,\ |45°\rangle,\ |90°\rangle \tag{1}$$

bezeichnet, wobei $|0°\rangle$ und $|90°\rangle$ die Basiszustände der + Basis darstellen und $|-45°\rangle$ und $|45°\rangle$ die Basiszustände der x-Basis. Die Eleganz der Dirac-Notation liegt darin, dass man zwar den Zustand beschreiben und mit ihm rechnen kann, sich aber nicht für ein konkretes Koordinatensystem entscheiden muss.



Gibt man ein konkretes Koordinatensystem vor (rechts, xy), dann kann man die Zustände als Vektoren schreiben, also

$$|0°\rangle = \begin{pmatrix}0\\1\end{pmatrix}, \qquad |90°\rangle = \begin{pmatrix}1\\0\end{pmatrix} \tag{2}$$

Ein wichtiges mathematisches Werkzeug ist das Skalarprodukt, das folgendermaßen gebildet wird[4]

$$\langle 90°|0°\rangle = \begin{pmatrix}1 & 0\end{pmatrix} \cdot \begin{pmatrix}0\\1\end{pmatrix} = 0 \tag{3}$$

Das Betragsquadrat des Skalarprodukts entspricht einer anschaulichen Größe: $|\langle 90°|0°\rangle|^2$ stellt die Wahrscheinlichkeit dar, dass ein Photon, dass in 0° polarisiert ist, durch einen Polarisator der Orientierung 90° hindurchtritt. Bekanntermaßen ist diese Wahrscheinlichkeit 0, was mit Gleichung (3) konsistent ist.

Natürlich kann man nun die einzelnen Zustände als Linearkombinationen ausdrücken, z.B.

$$|45\rangle = \alpha \cdot |0°\rangle + \beta \cdot |90°\rangle \tag{4}$$

Da das Skalarprodukt aber normiert sein muss, muss gelten

[4] *Genauer müsste man festhalten* $|\langle a|b\rangle|^2 = \langle a|b\rangle \cdot \langle a|b\rangle^* = \langle a|b\rangle\langle b|a\rangle$, *wobei* a^* *das komplex Konjugierte von* a *ist.*

$$1 \overset{!}{=} |\langle 45°|45°\rangle|^2 = \alpha^*\alpha \underbrace{\langle 0°|0°\rangle}_{=1} + \alpha^*\beta \underbrace{\langle 0°|90°\rangle}_{=0} + \alpha\beta^* \underbrace{\langle 90°|0°\rangle}_{=0} + \beta\beta^* \underbrace{\langle 90°|90°\rangle}_{=1} = |\alpha|^2 + |\beta|^2 \tag{5}$$

Aus Symmetriegründen folgt dann $\alpha = \beta = 1/\sqrt{2}$. Somit lassen sich die vier Zustände folgendermaßen ineinander umschreiben

$$\begin{aligned} |45°\rangle &= \frac{1}{\sqrt{2}}|0°\rangle + \frac{1}{\sqrt{2}}|90°\rangle \\ |-45°\rangle &= \frac{1}{\sqrt{2}}|0°\rangle - \frac{1}{\sqrt{2}}|90°\rangle \\ |0°\rangle &= \frac{1}{\sqrt{2}}|45°\rangle + \frac{1}{\sqrt{2}}|-45°\rangle \\ |90°\rangle &= \frac{1}{\sqrt{2}}|45°\rangle - \frac{1}{\sqrt{2}}|-45°\rangle \end{aligned} \tag{6}$$

wobei man natürlich auch wieder die Vektordarstellung wählen könnte, z.B. $|\pm 45°\rangle = \left(\pm 1/\sqrt{2} \quad , \quad 1/\sqrt{2}\right)^T$. Damit können wir dann z.B. auch die Wahrscheinlichkeit berechnen, dass ein 0° polarisiertes Photon einen 45°-Polarisator passiert:

$$|\langle 45°|0°\rangle|^2 = \left|\frac{1}{\sqrt{2}} \underbrace{\langle 45°|45°\rangle}_{=1} + \frac{1}{\sqrt{2}} \underbrace{\langle 45°|-45°\rangle}_{=0}\right|^2 = \frac{1}{2} \tag{7}$$

Die Wahrscheinlichkeit ist also 50%, dass ein Photon mit 0° Polarisation durch einen 45° Polarisator transmittiert wird.

Im Experiment legen wir ja allerdings nur die Basis fest (also + oder x) und schauen, welcher Detektor anspringt. Jetzt stellt sich also die Frage, wie man die Messung beschreibt. Hierfür führen wir die Operatoren $\hat{M}_+$ und $\hat{M}_\times$ ein, die jeweils die Messung in der einen oder anderen Basis beschreiben.

$$\begin{aligned} \hat{M}_+ &= |0°\rangle\langle 0°| - |90°\rangle\langle 90°| \\ \hat{M}_\times &= |45°\rangle\langle 45°| - |-45°\rangle\langle -45°| \end{aligned} \tag{8}$$

Wenden wir zunächst den Operator für die gerade Basis auf die vertikal und horizontal polarisierten Zustände an:

$$\begin{aligned} \hat{M}_+|0°\rangle &= |0°\rangle\langle 0°|0°\rangle - |90°\rangle\langle 90°|0°\rangle = |0°\rangle - |90°\rangle \cdot 0 = |0°\rangle \\ \hat{M}_+|90°\rangle &= |0°\rangle\langle 0°|90°\rangle - |90°\rangle\langle 90°|90°\rangle = |0°\rangle \cdot 0 - |90°\rangle = -|90°\rangle \end{aligned} \tag{9}$$

Das Ergebnis ist wenig überraschend – vermisst man einen vertikalen oder horizontalen Zustand in der geraden Basis, so erhält man wieder den Zustand selbst. Hier sei noch einmal daran erinnert, dass die Observable $\hat{M}_+$ die Messgröße darstellt, deren Eigenvektoren (also $|0°\rangle, |90°\rangle$) die möglichen Zustände des Systems beschreiben. Der

Eigenwert (also ± 1) entspricht dem Ausgang der Messung.[5] Hierbei entspricht $+1$ der Transmission des Photons und -1 der Reflexion (was wiederum als Phasensprung bei der Reflexion interpretiert werden kann)

Entsprechend verhalten sich die schräg polarisierten Zustände bei Messung in der schrägen Basis:

$$\begin{aligned} \widehat{M}_\times\,|45°\rangle &= |45°\rangle\langle 45°|45°\rangle - |-45°\rangle\langle -45°|45°\rangle = |45°\rangle \\ \widehat{M}_\times\,|-45°\rangle &= |45°\rangle\langle 45°|-45°\rangle - |-45°\rangle\langle -45°|-45°\rangle = -|-45°\rangle \end{aligned} \tag{10}$$

Hier entspricht der Eigenwert -1 allerdings nicht der Reflexion in unserem Aufbau (denn der Zustand $|-45°\rangle$ entspricht der Transmission und damit dem Bit 0). Dies lässt sich dadurch erklären, dass wir für eine Messung in der schrägen Basis nicht den Strahlteiler rotieren, sondern die Polarisation mittels des $\lambda/2$-Plättchens beim Empfänger.

Was ist allerdings, wenn man ein 45° polarisiertes Photon in der geraden Basis vermisst? In Gleichung (7) haben wir bereits bezeigt, dass sich die Transmissionswahrscheinlichkeit durch einen entsprechenden geraden Polarisator als 50% errechnen lässt. Berechnet man nun den Zustand, so stellt man fest, dass er eine Überlagerung aus den beiden Zuständen $|0°\rangle$ und $|90°\rangle$ ist:

$$\begin{aligned} \widehat{M}_+\,|45°\rangle &= |0°\rangle\langle 0°|\left(\frac{1}{\sqrt{2}}\,|0°\rangle + \frac{1}{\sqrt{2}}\,|90°\rangle\right) - |90°\rangle\langle 90°|\left(\frac{1}{\sqrt{2}}\,|0°\rangle + \frac{1}{\sqrt{2}}\,|90°\rangle\right) \\ &= \frac{1}{\sqrt{2}}|0°\rangle\langle 0°|0°\rangle + \frac{1}{\sqrt{2}}|0°\rangle\langle 0°|90°\rangle - \frac{1}{\sqrt{2}}|90°\rangle\langle 90°|0°\rangle \\ &\quad - \frac{1}{\sqrt{2}}|90°\rangle\langle 90°|90°\rangle = \frac{1}{\sqrt{2}}|0°\rangle - \frac{1}{\sqrt{2}}|90°\rangle \\ \widehat{M}_+\,|-45°\rangle &= \frac{1}{\sqrt{2}}|0°\rangle + \frac{1}{\sqrt{2}}|90°\rangle \end{aligned} \tag{11}$$

Genauso verhält es sich bei der Vermessung eines vertikalen oder horizontalen Zustands mit der schrägen Basis:

$$\begin{aligned} \widehat{M}_\times\,|0°\rangle &= \frac{1}{\sqrt{2}}|45°\rangle - \frac{1}{\sqrt{2}}|-45°\rangle \\ \widehat{M}_\times\,|90°\rangle &= \frac{1}{\sqrt{2}}|45°\rangle + \frac{1}{\sqrt{2}}|-45°\rangle \end{aligned} \tag{12}$$

Nun wissen wir, wie sich der Zustand des Photons ändert. Im Folgenden können wir die in den vorigen Unterkapiteln beschriebenen Messungen und Zustände für Alice, Bob und

[5] *Erinnerung: gilt für einen Zustand $|x\rangle$ und einen Operator $\widehat{M}$ die Gleichung $\widehat{M}|x\rangle = \chi\,|x\rangle$, dann nennen wir $|x\rangle$ einen Eigenvektor des Operators $\widehat{M}$ mit dem Eigenwert χ.*

Eve mit den eben erarbeiteten mathematischen Hilfsmitteln formulieren.[6] Zunächst ist eine Tabelle ohne Eve gezeigt, dann mit ihr.

Alice		***Bob***		
Zustand	Basis, Bit	Basiswahl	Zustand	gemessenes Bit
$\|0°\rangle$	$+, 0$	$+$	$\hat{M}_+ \|0°\rangle = \|0°\rangle$	0
		$\times$	$\hat{M}_\times \|0°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle - \frac{1}{\sqrt{2}}\|-45°\rangle$	0 oder 1
$\|90°\rangle$	$+, 1$	$+$	$\hat{M}_+ \|90°\rangle = -\|90°\rangle$	1
		$\times$	$\hat{M}_\times \|90°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle + \frac{1}{\sqrt{2}}\|-45°\rangle$	0 oder 1
$\|45°\rangle$	$\times, 1$	$+$	$\hat{M}_+ \|45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle - \frac{1}{\sqrt{2}}\|90°\rangle$	0 oder 1
		$\times$	$\hat{M}_\times \|45°\rangle = \|45°\rangle$	1
$\|-45°\rangle$	$\times, 0$	$+$	$\hat{M}_+ \|-45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle + \frac{1}{\sqrt{2}}\|90°\rangle$	0 oder 1
		$\times$	$\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$	0

Basen von Alice & Bob identisch => Bit kann als Schlüsselbit verwendet werden
Basen von Alice & Bob unterschiedlich => Messung wird verworfen

[6] *An dieser Stelle sei noch angemerkt, dass all diese Rechnungen auch in Matrixdarstellung hätten ausgeführt werden können. Die Darstellungen der Zustände in Vektorschreibweise wurde schon diskutiert, die Darstellung der Operatoren lautet* $\hat{M}_+ = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ *und* $\hat{M}_\times = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Alice		**Eve**			**Bob**		
Basis, Bit	Zustand	Basis	Zustand	Gesendet wird:	Basis	Zustand	Bit-Messung
+, 0	$\|0°\rangle$	+	$\hat{M}_+ \|0°\rangle = \|0°\rangle$	$\|0°\rangle$	+	$\hat{M}_+ \|0°\rangle = \|0°\rangle$	0
					×	$\hat{M}_\times \|0°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle - \frac{1}{\sqrt{2}}\|-45°\rangle$	0 oder 1
		×	$\hat{M}_\times \|0°\rangle = \frac{\|45°\rangle}{\sqrt{2}} - \frac{\|-45°\rangle}{\sqrt{2}}$	$\|45°\rangle$ oder $\|-45°\rangle$	+	$\hat{M}_+ \|45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle - \frac{1}{\sqrt{2}}\|90°\rangle$ oder $\hat{M}_+ \|-45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle + \frac{1}{\sqrt{2}}\|90°\rangle$	0 oder 1 0 oder 1
					×	$\hat{M}_\times \|45°\rangle = \|45°\rangle$ oder $\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$	1 0
+, 1	$\|90°\rangle$	+	$\hat{M}_+ \|90°\rangle = -\|90°\rangle$	$\|90°\rangle$	+	$\hat{M}_+ \|90°\rangle = -\|90°\rangle$	1
					×	$\hat{M}_\times \|90°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle + \frac{1}{\sqrt{2}}\|-45°\rangle$	0 oder 1
		×	$\hat{M}_\times \|90°\rangle = \frac{\|45°\rangle}{\sqrt{2}} + \frac{\|-45°\rangle}{\sqrt{2}}$	$\|45°\rangle$ oder $\|-45°\rangle$	+	$\hat{M}_+ \|45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle - \frac{1}{\sqrt{2}}\|90°\rangle$ oder $\hat{M}_+ \|-45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle + \frac{1}{\sqrt{2}}\|90°\rangle$	0 oder 1 0 oder 1
					×	$\hat{M}_\times \|45°\rangle = \|45°\rangle$ oder $\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$	1 0
×, 1	$\|45°\rangle$	+	$\hat{M}_+ \|45°\rangle = \frac{\|0°\rangle}{\sqrt{2}} - \frac{\|90°\rangle}{\sqrt{2}}$	$\|0°\rangle$ oder $\|90°\rangle$	+	$\hat{M}_+ \|0°\rangle = \|0°\rangle$ oder $\hat{M}_+ \|90°\rangle = -\|90°\rangle$	0 1
					×	$\hat{M}_\times \|0°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle - \frac{1}{\sqrt{2}}\|-45°\rangle$ oder $\hat{M}_\times \|90°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle + \frac{1}{\sqrt{2}}\|-45°\rangle$	0 oder 1 0 oder 1
		×	$\hat{M}_\times \|45°\rangle = \|45°\rangle$	$\|45°\rangle$	+	$\hat{M}_+ \|45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle - \frac{1}{\sqrt{2}}\|90°\rangle$	0 oder 1
					×	$\hat{M}_\times \|45°\rangle = \|45°\rangle$	1
×, 0	$\|-45°\rangle$	+	$\hat{M}_+ \|-45°\rangle = \frac{\|0°\rangle}{\sqrt{2}} + \frac{\|90°\rangle}{\sqrt{2}}$	$\|0°\rangle$ oder $\|90°\rangle$	+	$\hat{M}_+ \|0°\rangle = \|0°\rangle$ oder $\hat{M}_+ \|90°\rangle = -\|90°\rangle$	0 1
					×	$\hat{M}_\times \|0°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle - \frac{1}{\sqrt{2}}\|-45°\rangle$ oder $\hat{M}_\times \|90°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle + \frac{1}{\sqrt{2}}\|-45°\rangle$	0 oder 1 0 oder 1
		×	$\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$	$\|-45°\rangle$	+	$\hat{M}_+ \|-45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle + \frac{1}{\sqrt{2}}\|90°\rangle$	0 oder 1
					×	$\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$	0

Basen von Alice & Bob & Eve identisch => Eve fällt nicht auf
Basen von Alice & Bob unterschiedlich => Messung wird ohnehin verworfen
0/1 Basen von Alice & Bob identisch; Bits zufällig gleich, Eve fällt nicht auf
0/1 Basen von Alice & Bob identisch; Bits zufällig unterschiedlich => *Eve entdeckt*

Kapitel 6 Beispiele

6.1. Beispiel des Ablaufs ohne Eve mit zwei Buchstaben

Schritt 1: Alice und Bob wählen zufällig ihre Basen und Alice außerdem ihre Bits

Alice

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	x	x	+	x	+	+	+	x	x	+	x	x	x	+	+	x	+	x
Bit	1	0	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0	1

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
Bit																		

Schritt 2: Alice sendet die Bits in der jeweils gewählten Basis und Bob nimmt auf, welche Bits er gemessen hat. Dabei stellt er die Basis ein, wie er es vorher auf den Zettel geschrieben hat. Bei den Messungen, bei denen die Basen nicht übereinstimmen, fällt die Entscheidung, ob 0 oder 1 gemessen wird, zufällig. Dies ist auch im Beispiel so – so ist z.B. beim ersten Bit die Basis unterschiedlich und es wurde eine 1 „gewürfelt“. Bobs Übersicht sieht dann z.B. so aus:

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
Bit	1	0	1	1	1	0	0	1	1	1	0	1	0	1	0	0	0	1

Schritt 3: Alice und Bob tauschen sich über ihre Basen aus („ich habe +“ oder „ich habe x“). Sie markieren jetzt die Messungen, bei denen die Basen übereinstimmen. Bobs gemessene Bits dürfen nicht ausgetauscht werden.

Alice

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	x	x	+	x	+	+	+	x	x	+	x	x	x	+	+	x	+	x
Bit	1	0	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0	1

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
Bit	1	0	1	1	1	0	0	1	1	1	0	1	0	1	0	0	0	1

Damit lautet der von beiden erzeugte Schlüssel: „0 1 1 0 0 1 0 0 0 1“. Beide kennen den Schlüssel, obwohl sie sich nur über ihre Basen ausgetauscht haben.

Schritt 4: Alice verschlüsselt zwei Buchstaben mit dem eben generierten Schlüssel (Binäre Darstellung von Q und M aus der Alphabettabelle in Kapitel 9 ablesen, dann erste und zweite Zeile binär addieren)

Buchstabe	**Q**					**M**				
Datenbit	1	0	0	0	0	0	1	1	0	0
Schlüsselbit	0	1	1	0	0	1	0	0	0	1
Verschlüsseltes Bit	1	1	1	0	0	1	1	1	0	1

Schritt 5a: Alice versendet die Nachricht in der + Basis (also 0° für die Null und 90° für die 1). Sie wählt also nacheinander die folgenden Winkeleinstellungen an ihrem Polarisationsdreher:

90°, 90°, 90°, 0°, 0°, 90°, 90°, 90°, 0°, 90°

Schritt 5b: Bob empfängt parallel Alices Daten in der + Basis (reflektiert = 1, transmittiert = 0). Er misst und notiert

Empfangenes Bit	1	1	1	0	0	1	1	1	0	1

Schritt 6: Bob setzt den Schlüssel ein, um die Nachricht zu entschlüsseln (erste und zweite Zeile binär addieren)

Empfangenes Bit	1	1	1	0	0	1	1	1	0	1
Schlüsselbit	0	1	1	0	0	1	0	0	0	1
Datenbit	1	0	0	0	0	0	1	1	0	0
Buchstabe	**Q**					**M**				

6.2. Beispiel des Ablaufs mit Eve

Es wird hier wieder diskutiert, wie der Schlüssel erzeugt wird, diesmal aber mit Eve, die lauscht. Durch das Vergleichen von Test-Bits wird ihre Anwesenheit entdeckt.

Schritt 1: Alice, Bob und Eve wählen zufällig ihre Basen und Alice außerdem ihre Bits.

Alice

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	x	x	+	x	+	+	+	x	x	+	x	x	x	+	+	x	+	x
Bit	1	0	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0	1

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
Bit																		

Eve

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	x	x	+	+	x	+	+	+	x	x	x	x	+	x	+	x	+	+

Schritt 2: Alice sendet die Bits in der jeweils gewählten Basis und Bob nimmt auf, welche Bits er gemessen hat. Dazwischen ist allerdings Eve, die zufällig ihre Basis wählt (zwischen 0° und 45°). Hat sie die dieselbe Basis wie Alice (was sie natürlich nicht weiß), kann sie das Bit richtig weiterleiten. Hat sie die andere Basis gewählt, misst sie zufällig eine 0 oder eine 1 und sendet diese dann weiter (Eves Sendebasis ist immer gleich ihrer Empfangsbasis). Bob stellt bei seiner Messung die Basis ein, wie er es vorher auf den Zettel geschrieben hat. Die Messungen sehen dann z.B. so aus (Eves Bits müssen im Experiment nicht mitgeschrieben werden, sie können aber)[7]:

Eve

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	x	x	+	+	x	+	+	+	x	x	x	x	+	x	+	x	+	+
Bit	1	0	0	0	1	0	0	1	1	0	0	1	1	1	0	1	0	1

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
Bit	1	0	1	1	0	0	0	0	1	0	0	0	1	1	0	0	0	0

[7] *Ähnlich zum Beispiel ohne Eve sind auch hier wieder die Bits bei den Messungen zufällig gewählt, bei denen die Basen nicht übereinstimmen.*

Zum besseren Verständnis schreiben wir die letzten beiden Tabellen noch einmal und markieren alle Ereignisse grün, die zufällig sind. Man vergleiche für die erste Tabelle die Basen von Alice und Eve und für die zweite Tabelle die Basen von Eve und Bob.
Klar ist, dass weder Eve noch Bob wissen, ob das Ereignis zufällig war.

Eve

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	x	x	+	+	x	+	+	+	x	x	x	x	+	x	+	x	+	+
Bit	1	0	0	0	1	0	0	1	1	0	0	1	1	1	0	1	0	1

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
Bit	1	0	1	1	0	0	0	0	1	0	0	0	1	1	0	0	0	0

Schritt 3: Alice und Bob tauschen sich über ihre Basen aus („ich habe +“ oder „ich habe x“). Sie markieren jetzt die Messungen, bei denen die Basen übereinstimmen.

Alice

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	x	x	+	x	+	+	+	x	x	+	x	x	x	+	+	x	+	x
Bit	1	0	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0	1

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
Bit	1	0	1	1	0	0	0	0	1	0	0	0	1	1	0	0	0	0

Schritt 4: Für den Lauschtest vergleichen Alice und Bob die Bits, bei denen ihre Basen übereinstimmten (also die in den roten Kringeln)

Alice:	0	1	1	0	0	1	0	0	0	1
Bob:	0	1	0	0	0	0	0	0	0	0

Es zeigt sich, dass beide Bitfolgen nicht übereinstimmen – die Fehler sind mit blauen Kringeln markiert. Es sind drei von 10, also in etwa die erwarteten 25%.[8] Ab hier würden Alice und Bob mit dem Protokoll nicht mehr fortfahren, da sie sich bewusst sind, dass sie abgehört werden.

[8] *Die hier gewählten Zahlen beinhalten keine Systematik. Es ist also Zufall, dass bei Bob so viele Nullen stehen. Ebenso, dass die falschen Paare hier drei Mal die Kombination „Alice=1, Bob=0“ haben. Wenn man die grün markierten, zufälligen Ereignisse anders wählt, dann ändern sich entsprechend auch die Bits, die Alice und Bob vergleichen.*

Kapitel 7 Aufbau und Justierung

7.1. Zusammenbau der Komponenten

Schrauben Sie an alle Breadboards die RDF1-Füße, indem Sie sie von unten mit einer M6*12 mm Schraube an der Lochrasterplatte festschrauben.

Nehmen Sie eine BA1/M-Base und schrauben Sie sie mit einer M6 x 10 mm Schraube an einen der PH40/M Stiel-Halter. Setzen Sie einen TR40/M-Stiel ein und schrauben Sie darauf den KM100 (s. Bilder unten). Setzen Sie den CPS635R-C2 Laser in den AD11NT Adapterring, der im KM100 fixiert wird.	Nehmen Sie eine BA1S/M-Base und schrauben Sie darauf einen der PH50/M Stiel-Halter. Setzen Sie einen TR50/M-Stiel ein und schrauben Sie darauf die AT1/M-Justierhilfe.	Nehmen Sie eine BA1/M-Base und schrauben Sie darauf einen der PH50/M Stiel-Halter. Setzen Sie einen TR50/M-Stiel ein. Entfernen Sie die Gewindeschraube des TR50/M Stiels mit einem Inbus-Schlüssel. Schrauben Sie dann die Sensoreinheit auf den Stiel. Führen Sie diese Schritte für alle 4 Sensoren aus.
		

Abbildung 5 Befestigen des KM100-Halters an einem Ø1/2" Stiel

Bauen Sie nun die beiden Strahlteiler auf: verwenden Sie den UPH50/M Universal-Halter und setzen Sie einen TR50/M Stiel hinein. Entfernen Sie am Stiel wieder die Gewindeschraube mit einem Inbus. Schrauben Sie nun den modifizierten KM100PM/M auf, dem eine passende Schraube beiliegt. Befestigen Sie den PM3/M Haltearm wie im Bild gezeigt. Nehmen Sie dann den PBS201 *mit Schutzhandschuhen* und setzen ihn in der Orientierung wie im rechten Bild gezeigt ein. Fixiert wird er durch die Schraube im Haltearm. Achten Sie auf die richtige Orientierung (Schrift unten, Kante richtig).

Abbildung 6 Orientierung des PBS201 Strahlteilers im kinematischen Halter

ACHTUNG

WICHTIG: Die λ/2 Platten sollten nicht mit bloßen Händen berührt werden. Es empfiehlt sich dringend beim Zusammenbau Handschuhe zu tragen und nur die Ränder anzufassen, damit nicht mit blanken Fingern auf das optische Element gefasst wird.

Nun werden die $\lambda/2$-Platten eingebaut. Schrauben Sie zunächst einen PH40/M Stiel-Halter mit einer M6 x 10 mm Schraube auf eine BA1/M Base. Schrauben Sie einen TR30/M Stiel in einen RSP1X225/M-ALICE Rotationshalter. Drehen Sie mit Hilfe des SPW606 Schlüssels den Haltering aus dem Rotationshalter, setzen Sie die $\lambda/2$-Platte ein und fixieren Sie sie mit dem Haltering. Wiederholen Sie die Schritte für alle 4 Halter (je zwei mit der Skala „0, 45“ und „-45, 0, 45, 90“). Die Skalenjustierung wird in Kapitel 7.3 beschrieben.

7.2. Elektronik

7.2.1. Netzteile

Die im Kit enthaltenen Netzteile sind stabilisiert und liefern 5 V. Wählen Sie den passenden Stecker für ihr Land aus und setzen Sie ihn in die Halterung am Netzteil.

7.2.2. Laserelektronik

Die Elektronikbox des Lasers hat neben dem Anschluss für das Netzteil[9] nur einen Eingang für den Laser. Für die Verbindung von Laserelektronik zum CPS635R-C2 Lasermodul liegt ein Adapterkabel bei.

Der Laserelektronik besitzt einen roten „Feuerknopf“, der auch zur Umschaltung zwischen dem Pulsmodus und dem Dauerstrichmodus dient, s. Bild rechts. Hält man den Feuerknopf 2 Sekunden lang gedrückt, geht der Laser in den Dauerstrichmodus über. Ein kurzer Druck beendet ihn wieder, wodurch wieder kurze Pulse gesendet werden. Diese sind auch sichtbar, wenn man ein Stück Papier vor den Laser hält. Eine grüne LED an der Seite signalisiert die Betriebsbereitschaft.

[9] *Verwenden sie für den Betrieb das mitgelieferte Netzteil. Wenn sie ein anderes Netzteil verwenden möchten, dann achten sie darauf, dass dieses ein stabilisiertes Netzteil mit 5V und minimal 0,5A (2,5W) mit einer Hohlbuchse 5,5/2,1mm (Pluspol innen) ist.*

7.2.3. Sensorelektronik

Die Sensorelektronik hat neben dem Anschluss für das Netzteil noch zwei Sensoreingänge. Sie sind völlig identisch – es ist daher egal, welchen Sensor man an welche Buchse anschließt.
Stellen Sie sicher, dass Sie erst die Sensoren mit der Elektronikbox verbinden, bevor Sie das Netzteil einstecken.

Die Sensorelektronik hat weiterhin einen grünen Knopf, mit dem zwischen dem „Justiermodus“ und dem „Messmodus“ umgestellt wird. Beim **Justiermodus** leuchtet die seitliche LED **gelb**. Ist dieser Modus aktiviert, dann leuchten BEIDE blauen LEDs an den Sensoren, wenn ein Laserpuls mit gleicher Intensität bei Ihnen eintrifft – das entspricht den Fällen, bei denen die Basen von Alice und Bob nicht übereinstimmen.
Der **Messmodus**, bei dem die LED **grün** leuchtet, verhält sich im Fall unterschiedlicher Basen anders: Er wählt zufällig eine der beiden blauen LEDs aus und lässt diese aufleuchten. Dies simuliert die „Entscheidung“ eines einzelnen Photons, das am Strahlteiler mit 50% Wahrscheinlichkeit transmittiert oder reflektiert wird.

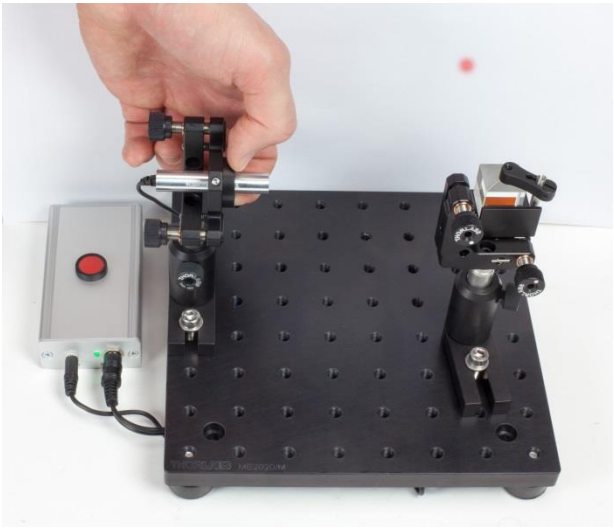
7.3. Einstellen des Lasers und der $\lambda/2$-Platten

Bevor das eigentliche Experiment beginnen kann, muss noch die Polarisationsebene des Lasers und die Orientierung der $\lambda/2$-Platten richtig eingestellt werden.

- Stellen Sie zunächst einen Laser und einen Strahlteiler auf eine der Lochrasterplatten.
    - Drücken Sie den roten Knopf an der Laserelektronik, bis der Laser in den Dauerstrichmodus übergeht. Das erleichtert alle Justierarbeiten deutlich.

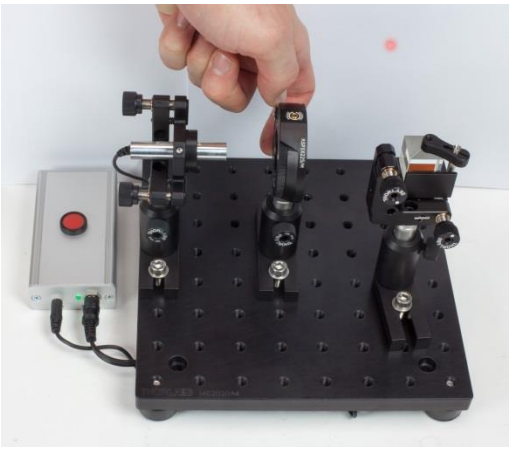
WARNUNG

Das Lasermodul ist ein Klasse 2 Laser, der keine speziellen Schutzbrillen erfordert. Um Verletzungen zu vermeiden, sollte jedoch nicht direkt in den Strahl geblickt werden.



- Nehmen Sie nun die AT1/M-Höhenjustierhilfe und stellen Sie sicher, dass der Laser parallel zum Tisch verläuft, indem Sie den Laserhalter verkippen. Setzen Sie dafür die Justierhilfe abwechselnd nah vor den Laser und weit entfernt.
- Stellen Sie sicher, dass der reflektierte Anteil des Laserlichts am Strahlteiler im 90°-Winkel zum einfallenden Strahl reflektiert wird.
- Jetzt wird der Laser in seinem Halter gedreht und damit die Polarisation des Lasers. Der Laser ist zwar nicht vollständig linear polarisiert, hat aber eine Vorzugsrichtung. Lösen Sie die Schraube ein wenig, mit der der Adapterring im kinematischen Halter festgeklemmt ist. Drehen Sie den Laser samt Adapterring; damit er nicht wegrutscht, sollte man mit zwei Fingern von vorn auf den Adapterring drücken. Beobachten Sie jetzt mit einem Blatt Papier die Laserintensität des am Strahlteilerwürfel **reflektierten** Lichts. Sie sollte während der Drehung deutlich abnehmen und wieder ansteigen. Gesucht ist die Einstellung mit der **geringsten** Intensität.
- Drehen Sie also den Laser so lange, bis die Intensität des reflektierten Strahls **minimal** ist und fixieren Sie den Adapterring in dieser Position.
- Nehmen Sie die gesamte Laserkomponente (=Laser samt Halterung) aus dem Aufbau und **wiederholen** Sie die bisherigen Schritte **mit dem anderen Laser.** Nun sind beide Laser horizontal, also parallel zum Breadboard, polarisiert.

- Setzen Sie einen der Rotationshalter (RSP1X225/M-ALICE) mit der eingebauten $\lambda/2$-Platte zwischen den Laser und den Strahlteiler, wobei die Skala zum Laser zeigt.
    - Stellen Sie sicher, dass die Schraube auf der Oberseite des Halters gelöst ist, wodurch sich der Halter kontinuierlich drehen lässt.



    - Drehen Sie die $\lambda/2$-Platte und beobachten Sie die Intensität des reflektierten Strahls. Wie beim Laser wird sich die Intensität mit dem Drehwinkel verändern. Gesucht ist der Drehwinkel mit der **geringsten reflektieren Intensität**.
    - Wenn Sie die Einstellung mit der geringsten Intensität im reflektierten Strahl gefunden haben, schrauben Sie die Schraube am Kopf des Halters ein.
    - Nehmen Sie nun den Rotationshalter aus dem Aufbau, um die Skala richtig einzustellen. Lösen Sie dafür die beiden Schrauben an der Frontplatte des Rotationshalters . Dadurch können Sie das Blatt mit der Skala drehen – tun Sie dies, bis die „0“-Markierung mit der mittigen Markierung am oberen Rand des Halters übereinstimmt. Stellen Sie sicher, dass Sie nur das Skalenblatt drehen und nicht die $\lambda/2$-Platte. Schrauben Sie dann die beiden Schrauben wieder fest.

- Wiederholen Sie diese Schritte für alle Rotationshalter / $\lambda/2$-Platten.

7.4. Justierung für Alice und Bob

Alice und Bob sollen sich in etwa 60 cm Abstand gegenüber stehen. Es ist sinnvoll, die beiden Breadboards möglichst parallel aufzustellen.

- Bauen Sie den Laser am Rand und die $\lambda/2$-Platte von Alice mittig auf dem kleinsten Breadboard auf. Der Halter hat die Einstellungen „-45, 0, 45, 90“ und zeigt mit der Skala zum Laser. Stellen Sie Alice’ Laser auf Dauerbetrieb ein (drücken sie dafür 2 Sekunden lang den roten Knopf).
- Bauen Sie die $\lambda/2$ −Platte von Bob auf, direkt am Rand des Breadboards. Der Halter hat nur die Einstellungen „0, 45“. Die Skala zeigt von Alice weg.
- Stellen Sie einen der Sensoren so ans andere Ende von Bobs Breadboard, dass er möglichst gerade im Strahl steht und der Laserstrahl in die Öffnung fällt.
- Stellen sie den Strahlteiler zwischen Bobs Polarisationsdreher und den Detektor. Er soll möglichst senkrecht zum Strahl stehen.
- Stellen Sie den zweiten Sensor so in den Aufbau, dass er das Loch trifft und
  - senkrecht zum Strahl steht, der vom Strahlteiler reflektiert wird.
  - sein Abstand zum Strahlteiler gleich dem Abstand des ersten Sensors zum Strahlteiler ist.

Der Aufbau sollte jetzt so aussehen:

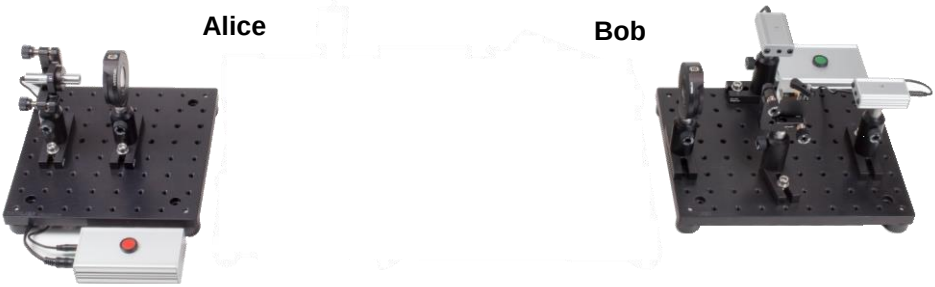


Abbildung 7: Alice und Bob

Nun kommt die Feinjustierung.

- Stellen Sie die Sensorelektronik in den Justiermodus (= seitliche LED leuchtet gelb).
- Stellen Sie beide Polarisationsdreher auf 0° ein und drücken den Feuerknopf kurz. Es sollte die blaue LED auf dem Sensor aufleuchten, der im gerade durchlaufenden Strahl sitzt. Wenn das nicht der Fall ist, prüfen Sie:
  - Ob der Sensor wirklich senkrecht zum Strahl steht.
  - Ob der Laserstrahl sauber in das Loch vor der Photodiode fällt, also
    - ob Sie die Höhe richtig eingestellt haben
    - ob der Laserstrahl mittig in das Loch fällt

Falls man etwas Schwierigkeiten hat, dann empfiehlt es sich, dass ein Anwender mit dem Laser immer weiter „schießt“, während der andere die Feinstellung vornimmt.

Wenn dieser Sensor richtig eingestellt ist und die LED nach einem Schuss angeht, dann wird der zweite Sensor, auf den der reflektierte Strahl trifft, justiert:

- Stellen Sie die $\lambda/2$-Platte bei Alice auf die Skalenanzeige 90° ein (Bob bleibt bei 0°). Nun sollte die LED am zweiten Sensor leuchten, wenn man einen Schuss macht**.**
- Zur Vereinfachung der Einjustierung des zweiten Sensors kann der Strahlteilerwürfel mit dem kinematischen Halter verkippt und gedreht werden.

Nun müssen die anderen Fälle getestet werden:
Bei den Einstellungen „45°“ und „-45°“ von Alice sollten BEIDE LEDs leuchten, denn beide Photodioden sollten die gleiche Intensität messen. Es kann sein, dass die beiden vorigen Fälle klappen, aber z.B. der 45°-Fall nicht. Dann war die Feinjustierung noch nicht gut genug. Verändern Sie leicht die Ausrichtung der Sensoren. Prüfen Sie alternativ, dass Sie im Justiermodus sind, also die seitliche LED an der Sensorelektronik gelb leuchtet.

Insgesamt muss man **8 Fälle** ausprobieren, die **alle** funktionieren müssen, bevor man den Versuch starten kann:[10]

Alice	Bob	Welche LED leuchtet	Bit
-45°	0°	Beide	Zufall
0°	0°	Geradeaus	0
45°	0°	Beide	Zufall
90°	0°	Reflektiert	1

Alice	Bob	Welche LED leuchtet	Bit
-45°	45°	Geradeaus	0
0°	45°	Beide	Zufall
45°	45°	Reflektiert	1
90°	45°	Beide	Zufall

Wenn alle Fälle funktionieren, können Sie die Sensorelektronik in den Messmodus umschalten (LED springt von gelb auf grün).
Sollten z.B. nur 7 von 8 Fällen funktionieren, muss trotzdem die Justierung so lange verfeinert werden, bis alle 8 Fälle funktionieren, da sonst das Experiment nicht sinnvoll durchgeführt werden kann. In Kapitel 11 findet sich ein Troubleshooting, das die wichtigsten Punkte noch einmal zusammenfasst und zusätzliche Hilfe bietet.

Wichtig: Der Aufbau sollte während des ganzen Experiments nicht bewegt werden. Auch sollte man sich nicht auf den Tisch aufstützen! Dies kann den Aufbau dejustieren, wenn sich der Tisch durchdrückt!

7.5. Einbau von Eve

Stellen Sie für den Einbau von Eve das große Breadboard zwischen die Breadboards von Alice und Bob. Didaktisch sollte vermieden werden an Alice und Bob Veränderungen vorzunehmen, da Eve ja nur „unbemerkt“ abhören soll. Justieren Sie dementsprechend Eve ohne Veränderungen an Alice oder Bob.

- Schrauben Sie die BBH1 Griffe an das Breadboard von Eve. Das ermöglicht den schnellen Ein- und Ausbau von Eve.
- Bauen Sie den Empfangsteil von Eve auf. Das erfolgt völlig analog zum in Kapitel 7.4 beschriebenen Aufbau von Bob (Sensorelektronik auf Justiermodus schalten, LED leuchtet gelb!). Testen Sie, dass alle 8 Fälle zwischen Alice und dem Empfangsteil von Eve funktionieren. Stellen Sie danach die Sensorelektronik wieder vom Justier- in den Messmodus.
- Bauen Sie den Sender von Eve auf. Dazu müssen Sie den Laser so einstellen, dass beide Sensoren von Bob gut getroffen werden. Dies erfordert etwas Fingerspitzengefühl (und auch wieder die Sensorelektronik im Justiermodus und den Laser im Dauerstrichmodus). Stellen Sie auch hier wieder sicher, dass alle 8 Fälle zwischen der Sendeeinheit von Eve und Bob funktionieren und am Ende in den Messmodus umgestellt wird.

[10] *In die Tabelle ist zur Hilfe noch der Bit-Wert aufgenommen. Ist die Sensorelektronik im Justiermodus, dann leuchten beide LEDs. Ist die Sensorelektronik im Messmodus, dann leuchtet nur eine LED; welche ist zufällig.*

- Die Laser- und die Sensorelektronikbox können mit CL3/M-Klemmen am Breadboard befestigt werden. Das erleichtert die Herausnahme von Eve. Verwenden Sie für jede Klemme eine 1/4"-20 x 1,25" (M6 x 30 mm) und eine 1/4"-20 x 2" (M6 x 45 mm) Schraube.

Der fertige Aufbau von Eve sieht folgendermaßen aus:

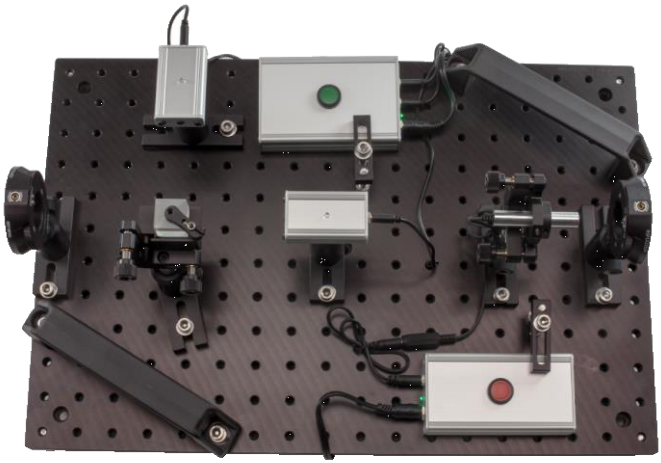


Abbildung 8: Eve

Kapitel 8 Versuchsdurchführung

Der Versuchsablauf gliedert sich in drei Teile:

- **Abschnitt 8.1:** Generierung eines mindestens 20bit langen Schlüssels
- **Abschnitt 8.2:** Verschlüsseln und Übertragen eines 4-Buchstaben Wortes
- **Abschnitt 8.3:** Einbau von Eve und Lauscher identifizieren

Um die Aufgaben durchführen zu können, sollten die Grundlagen aus Kapitel 5 bekannt sein. Weiterhin ist ein ausführliches Beispiel in Kapitel 6 dargestellt, welches den kompletten Ablauf mit und ohne Eve zeigt. Die Messprotokolle finden sich als Vorlage in Kapitel 9.

8.1. Schlüsselgenerierung

Aufgabe 1: Bauen Sie Alice und Bob so auf, dass sich beide in größerem Abstand gegenüber stehen (etwa 60cm, sodass also noch Platz für Eve ist). Justieren Sie beide so ein, dass bei allen acht $\lambda/2$ -Kombinationen (zwei Einstellungen bei Bob, vier bei Alice) reproduzierbar die richtigen LEDs leuchten. Stellen Sie dafür sicher, dass die Sensorelektronik im Justiermodus ist (gelbe LED).

> *Durchführung:* Der Aufbau funktioniert so, wie es im Kapitel 7 beschrieben wurde. Skizzenhaft ist dies in Abbildung 3 dargestellt, ein Foto findet sich in Abbildung 7. Die Kombinationen entsprechen denen, die in Kapitel 7.4 beschrieben sind.

Aufgabe 2: Alice und Bob wählen zufällige Basen und Alice weiterhin zufällige Bits. Füllen Sie dafür die Messprotokolle in Kapitel 9 für Alice und Bob aus (für Bob nur die Basen).

> *Durchführung:* Dies entspricht Schritt 1 im Beispielkapitel 6.1. Die Vorlagen für die Protokolle sind in Kapitel 9 zu finden.

Aufgabe 3: Senden Sie die Bits von Alice in den Basen, die in Aufgabe 2 notiert wurden. Bob notiert sich die Bits, die er misst (wobei auch er die Basen aus Aufgabe 2 verwendet). Stellen Sie dafür sicher, dass die Sensorelektronik im Messmodus ist (LED leuchtet grün).

> *Durchführung:* Dies entspricht Schritt 2 in Kapitel 6.1. Alice und Bob sollen einen Schlüssel generieren, der mindestens 20 Schlüsselbits lang ist. Dafür werden 52 Übertragungen durchgeführt. Dies ist ein empirischer Wert, der fast immer dazu führt, dass man 20 übereinstimmende Basen erhält (was dann 20 Schlüsselbits entspricht).
>
> Noch einmal zur Orientierung: Wenn Alice
> - 0° einstellt, dann sendet sie in der „+“ Basis eine 0.
> - 90° einstellt, dann sendet sie in der „+“ Basis eine 1.
> - -45° einstellt, dann sendet sie in der „x“ Basis eine 0
> - 45° einstellt, dann sendet sie in der „x“ Basis eine 1

Alice und Bob übertragen die Bits anhand der in Aufgabe 2 erstellten Tabelle. Dafür sendet Alice ihr Bit und Bob notiert seine Messung (reflektiert = 1, transmittiert = 0).

Aufgabe 4: Alice und Bob tauschen sich nun öffentlich über ihre Basen aus und streichen die Messungen, bei denen die Basen nicht übereinstimmten. Die restlichen Messungen stellen dann den Schlüssel dar.

Durchführung: Dies entspricht Schritt 3 im Beispielkapitel 6.1. Alice und Bob tauschen sich über ihre Basen aus ("Ich habe + gewählt" oder "Ich habe x gewählt") und markieren sich die Messungen, bei denen die Basen übereinstimmten. Die Bits dieser Messungen stellen dann den Schlüssel dar.

Sollten 52 Messungen nicht ausreichen, um 20 Schlüsselbits zu erzeugen, dann müssen weitere Messungen durchgeführt werden (mit zufälliger Basis- und Bitwahl), bis 20 Schlüsselbits erzeugt wurden.

8.2. Verschlüsseln und Übertragen des 4-Buchstaben Worts

Aufgabe 5: Verschlüsseln Sie die Nachricht von Alice (= 4 Buchstaben Ihrer Wahl) mit dem zuvor erzeugten Schlüssel.

Durchführung: Das Vorgehen ist in Schritt 4 in Kapitel 6.1 und außerdem in Kapitel 5.2 beschrieben.

Aufgabe 6: Übertragen Sie die verschlüsselte Nachricht von Alice zu Bob.

Durchführung: Die Übertragung der verschlüsselten Nachricht erfolgt rein mit der + Basis (alternativ auch rein mit der x Basis). Alice sendet ihre verschlüsselten Bits (0° für 0, 90° für 1). Alice und Bob wechseln die Basis beim Übertragen der Daten nicht. Das entspricht den Schritten 5a und 5b in Kapitel 6.1.

Aufgabe 7: Entschlüsseln Sie die Bits, die Bob erhalten hat, um die Nachricht von Alice zu erhalten.

Durchführung: Auch dieser Prozess ist in Kapitel 5.2 beschrieben und ist der Schritt 6 im Beispielkapitel 6.1.

8.3. Einbau von Eve und Detektion des Abhörens

Aufgabe 8: Setzen Sie Eve zwischen Alice und Bob und schalten Sie beide Sensorelektroniken auf den Justiermodus (LED leuchtet gelb). Justieren Sie den Empfangsteil von Eve so ein, dass alle 8 Übertragungs-Fälle mit Alice funktionieren. Justieren Sie nun den Sender von Eve so, dass alle 8 Fälle mit Bob funktionieren. Schalten Sie beide Elektroniken wieder in den Messmodus (LED leuchtet grün).

> *Durchführung*: Die Justierung erfolgt wieder wie im Kapitel 7 beschrieben, s. Abbildung 4 und Abbildung 8. Versuchen Sie Eve ohne das Verändern von Alice und Bob einzujustieren, denn der Lauscher hat ja keinen Einfluss auf Sender und Empfänger. Schalten Sie danach die Sensorelektroniken wieder auf den Messmodus um, sodass die LEDs wieder grün leuchten.

Aufgabe 9: Füllen Sie die Tabelle für Eve aus, in der sie sich für die + oder die x Basis entscheidet. Sie brauchen außerdem wieder zufällige Basen für Alice und Bob, sowie zufällige Bits für Alice.

> *Durchführung:* Man müsste eigentlich für Eve nichts aufschreiben – die Person, die Eve bedient, könnte auch einfach spontan eine Basis wählen und das gemessene Ergebnis weiterleiten. Es hat sich aber herausgestellt, dass sich Eve zu leicht von Alices Wahl beeinflussen lässt (denn entgegen realer Datenübertragung sieht die Person ja, ob Alice ihre Einstellung verändert). Schreibt man vorher eine zufällige Basisfolge für Eve auf, kann man dies verhindern. Die Bits müssen für Eve nicht mitgeschrieben werden.
>
> Die Basen für Alice und Bob können der Einfachheit halber natürlich wie in Aufgabe 2 gewählt werden. Ein Beispiel für diese Aufgabe findet sich in Schritt 1 von Kapitel 6.2.

Aufgabe 10: Übertragen Sie das erste Bit von Alice in der Basis, die in der vorigen Aufgabe festgelegt wurde. Eve stellt ebenfalls die von ihr in der vorigen Aufgabe gewählte Basis ein. Sie misst dann ein Bit, welches sie zu Bob in der gleichen Basis weiter schickt. Bob notiert sich das Bit, wobei auch er die Basis gewählt hat, die in der vorigen Aufgabe für ihn notiert wurde. Dieser Vorgang wird nun für alle 52 Bits/Basen durchgeführt.

> *Durchführung:* Alice und Bob gehen wie in Aufgabe 3 vor. Eve misst das Signal, das Alice geschickt hat, wobei ihre Basis der aus Aufgabe 9 entspricht. Sie schickt dann das gemessene Ergebnis in der gleichen Basis weiter. Bob misst wie zuvor auch. Dieser Aufgabenteil ist in Schritt 2 in Kapitel 6.2 dargestellt.

Aufgabe 11: Alice und Bob tauschen sich wieder öffentlich über die Wahl ihrer Basen aus. Sie markieren die Messungen, bei denen die Basen übereingestimmt haben.

> *Durchführung:* Wie in Aufgabe 4. Alice und Bob vergleichen ihre Basen, markieren die übereinstimmenden Messungen und erhalten so eine Kette von Bits. Dies entspricht Schritt 3 in Kapitel 6.2.

Aufgabe 12: Vergleichen Sie die Ergebnisse von Alice und Bob aus Aufgabe 11.

> *Durchführung:* Wäre Eve nicht im Aufbau gewesen, wäre die Bit-Kette für Alice und Bob identisch und sie könnten Sie als Schlüsselbits verwenden. Aufgrund von Eves Anwesenheit ergibt sich allerdings eine gewisse Menge an nicht übereinstimmenden Bits. Dies verrät eindeutig die Anwesenheit von Eve. Dieser Teil entspricht Schritt 4 in Kapitel 6.2.

Kapitel 9 Messprotokolle

Dieses Kapitel beinhaltet die Messprotokolle für Alice, Bob und Eve.

Damit diese leicht ausdruckbar sind (Das Handbuch findet sich auch frei herunterladbar unter discovery.thorlabs.com), sind sie jeweils auf einer Seite.

Danach finden Sie die Tabelle, in der das Alphabet mit 5 Bit pro Buchstabe codiert ist.

Messprotokoll zur Schlüsselerzeugung – ALICE

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis (+ oder x)																		
Bit (0 oder 1)																		

	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Basis (+ oder x)																		
Bit (0 oder 1)																		

	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
Basis (+ oder x)																
Bit (0 oder 1)																

Erzeugter Schlüssel:

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Winkeleinstellung (Erinnerung)	Basis +	Basis x
Bit 0	0°	-45°
Bit 1	90°	45°

Tabelle zur Verschlüsselung der Nachricht – ALICE

Buchstabe																				
Datenbit																				
Schlüsselbit																				
Verschlüsseltes Bit																				

Datenbit = Buchstabe in binärer Darstellung, 4 x 5 Bit

Messprotokoll zur Schlüsselerzeugung – BOB

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis (+ oder x)																		
Bit (0 oder 1)																		

	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Basis (+ oder x)																		
Bit (0 oder 1)																		

	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
Basis (+ oder x)																
Bit (0 oder 1)																

Erzeugter Schlüssel:

_ _

Erinnerung	transmittiert	reflektiert
Basis + (=0°)	0	1
Basis x (=45°)	0	1

Tabelle zur Entschlüsselung der Nachricht – BOB

Empfangenes Bit																				
Schlüsselbit																				
Datenbit																				
Buchstabe																				

Basiswahl – EVE

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis (+ oder x)																		

	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Basis (+ oder x)																		

	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
Basis (+ oder x)																

Binäre Darstellung des Alphabets

A	0	0	0	0	0
B	0	0	0	0	1
C	0	0	0	1	0
D	0	0	0	1	1
E	0	0	1	0	0
F	0	0	1	0	1
G	0	0	1	1	0
H	0	0	1	1	1
I	0	1	0	0	0
J	0	1	0	0	1
K	0	1	0	1	0
L	0	1	0	1	1
M	0	1	1	0	0
N	0	1	1	0	1
O	0	1	1	1	0
P	0	1	1	1	1
Q	1	0	0	0	0
R	1	0	0	0	1
S	1	0	0	1	0
T	1	0	0	1	1
U	1	0	1	0	0
V	1	0	1	0	1
W	1	0	1	1	0
X	1	0	1	1	1
Y	1	1	0	0	0
Z	1	1	0	0	1

Tabelle für Binäraddition

0	**1**	**0**	**1**
+ **0**	+ **0**	+ **1**	+ **1**
= **0**	= **1**	= **1**	= **0**

Kapitel 10 Didaktische Kommentare

Bei der Quantenkryptografie stellt die Generierung von Zufallszahlen ja ein wesentliches Problem dar. Es bietet sich also an, dies auch im Kontext des Versuchs zu diskutieren. Wenn die Wahl der Basen und Bits im Versuch mit „menschlichen“ Zufallszahlen durchgeführt wird, dann kann es passieren, dass Alice und Bob viele Übereinstimmungen haben, da der Mensch ein schlechter Zufallszahlgenerator ist. Dies kann man sehr einfach auch graphisch darstellen:

- Lassen Sie die Praktikanten eine für sie zufällige Folge von 0 und 1 eintippen
- Schreiben Sie ein Programm, das die 1er-Kettenlängen analysiert: So wäre die Folge 01110 eine 1er-Kette der Länge 3. Das Programm zählt also durch, wie oft eine 1er-Kette der Länge n in der Zahlenfolge der Praktikanten auftritt. Dann trägt man Anzahl über n auf. Bei völligem Zufall müsste die Wahrscheinlichkeit mit $1/2^n$ abnehmen.
- Menschlicher Zufall ist aber durch unsere Intuition geleitet – selten wird ein Praktikant eine 1er-Kette (oder 0er-Kette) mit mehr als 5 Einsen aufschreiben, weil es ihm/ihr nicht zufällig erscheint. In der Realität tauchen sie aber trotzdem auf, nur eben mit kleiner Wahrscheinlichkeit. Die Abweichung zwischen Theorie-Kurve und der menschlichen Kurve ist damit sehr schnell sehr groß.

Aufgabe 2 in Kapitel 8 beinhaltet die zufällige Wahl von Basen für Alice und Bob und zusätzlich die zufällige Wahl der Bits von Alice. Wie im ersten Punkt beschrieben, kann der Mensch nur als ungenügender Zufallszahlgenerator dienen. Alternativ bieten sich echte Zufallszahlgeneratoren an. Eine Option wäre ein kommerzielles Gerät wie der Quantis von ID Quantique oder ein Eigenbau mit zwei Einzelphotondetektoren und einem Strahlteiler. Eine sehr einfache Variante besteht darin, eine transparente Box mit mehreren Würfeln zu verwenden. Gerade Zahlen werden dann z.B. als „0“ interpretiert. Andere Optionen sind ein Münzwurf und computergenerierte Pseudozufallszahlen.

Die Aufgaben in Kapitel 8 sind so strukturiert, dass man zunächst Alice und Bob aufbaut, einen Schlüssel generiert und eine Nachricht übermittelt. Erst danach wird Eve eingebaut und bei einer erneuten Schlüsselgenerierung entdeckt. Dieser Ablauf entspricht natürlich nicht dem genauen Ablauf des BB84-Protokolls aus Kapitel 5.7, denn dort wird ja vor dem Übermitteln der Nachricht auf einen Lauscher getestet. Das kann im Praktikum natürlich auch so gemacht werden, allerdings ist es erfahrungsgemäß besser, wenn zunächst die Schlüsselgenerierung und Datenübertragung anhand von Alice und Bob verstanden wird, bevor die Problematik des Abhörens untersucht wird.

Kapitel 11 Troubleshooting

Wenn die 8 Kombinationen der $\lambda/2$-Platten von Alice und Bob (bzw. Alice und Eve, Eve und Bob) durchgespielt werden, dann funktionieren nicht alle 8 Fälle.

- Sind beide Sensor-Elektroniken im Justiermodus? Dies wird durch gelbes Licht an der LED der Sensor-Box angezeigt. Ist die LED grün, dann drücken Sie einmal auf den grünen Knopf, um in den Justiermodus zu schalten. Der Messmodus wird durch grünes Licht aus der LED gekennzeichnet.
- Sind alle $\lambda/2$-Platten richtig im RSP1X225/M-Halter eingebaut? Die „Fast Axis“ muss mit der „0°“ Markierung übereinsimmen. Weiterhin muss der Sprungmechanismus des Halters (Lösen und Fixieren mit der Schraube an der Oberseite des Halters) bei 0° fixiert werden.
- Ist der Laser richtig eingesetzt, sodass seine Polarisationsachse richtig ist? Prüfen Sie erneut, dass die Transmission des Lasers minimal ist, wenn er zunächst durch eine $\lambda/2$-Platte mit 0°, dann durch eine $\lambda/2$-Platte mit 90°-Einstellung („90°“ mit der speziellen Skala! Der Halter selbst wird dafür nur um 45°=2 Sprünge gedreht) und dann durch den Strahlteiler tritt.
- Ist die Orientierung des Strahlteilers richtig? Vergleichen Sie mit den Bildern in Kapitel 7.1.
- Schauen die $\lambda/2$-Platten von Alice und Bob (bzw. Alice und Eve, Eve und Bob) voneinander weg? Zeigt die $\lambda/2$-Platte von Alice zum Laser?
- Ist alles so senkrecht wie möglich aufgebaut? Steht der Sensor senkrecht zum einfallenden Laserstrahl, ist die Linse gerade eingebaut, steht der Sensor für den reflektierten Strahl in 90° zum einfallenden Strahl? Ein Blick von oben auf den Aufbau hilft hier oft.
- Sind beide Sensoren gleich weit vom Strahlteiler entfernt? Manchmal hilft es, wenn man den Abstand der Sensoren/Photodioden zum Strahlteiler variiert. Man kann z.B. beide Sensoren näher an den Strahlteiler stellen.
- Sind Sie sicher, dass die Photodioden gut getroffen werden? Nur weil der Laser in etwa durch die Sensoröffnung tritt, muss die Photodiode noch nicht optimal getroffen worden sein.

Kapitel 12 Danksagung

Dieses Versuchspaket entstand durch die enge Zusammenarbeit mit verschiedenen Lehrenden, die sich der Vermittlung von Quantenphysik verschrieben haben. Wir danken dabei sehr herzlich:

- OStR Jörn Schneider, Leibniz-Gymnasium Dormagen, für die gemeinsame Umsetzung des Experiments, der Elektronik und Sensorik, sowie das Testen im Unterricht und das Teilen seiner Lehrunterlagen.
- Andreas Vetter und Prof. Dr. Jan-Peter Meyn, Universität Erlangen-Nürnberg, die konzeptionelle Vorarbeit geleistet haben. Von beiden wurde ein Aufbau mit einer gepulsten Quelle und entsprechenden Detektoren gebaut und in ihrem Schülerlabor eingesetzt, vgl. A. Vetter, A. Strunz, P. Bronner u. J.-P. Meyn: “Photonik macht Schule - Ein Schülerlabor zur modernen Optik und Quantenoptik.“ Praxis der Naturwissenschaften – Physik in der Schule 59(8) 17-19 (2010).

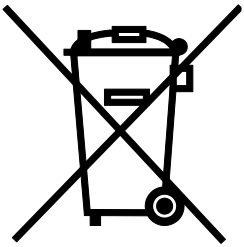
  Zum Thema Quantenphysik ist insbesondere Jan-Peter Meyns Webseite http://www.quantumlab.de zu empfehlen, die auch Inspiration für Teile der vorliegenden Anleitung war.
- Der Heisenberg-Gesellschaft, München, auf deren Workshop „Quantenphysik in der Schule 2014“ der Kontakt zustande kam.
- Jasmin Karim, Karlsruher Institut für Technologie, für den Entwurf zur quantenmechanischen Beschreibung des Versuchs in der Dirac-Notation.

Haben Sie auch Ideen für ein Experiment, das Sie entweder bereits umgesetzt haben oder umsetzen möchten? Melden Sie sich bei uns, wir freuen uns über Kooperationen!

Kapitel 13 Bestimmungen

Thorlabs bietet allen Endnutzern in der EG die Möglichkeit, Produkte am Ende der Nutzung ohne anfallende Entsorgungskosten zurückzugeben, wie durch die WEEE (Waste Electrical and Electronic Equipment Directive) der Europäischen Gemeinschaft und die entsprechenden nationalen Gesetze verlangt.

- Dieses Angebot gilt für elektrische und elektronische Komponenten von Thorlabs, welche:
- nach dem 13. August 13 2005 verkauft wurden
- mit dem nebenstehenden durchgestrichenen Mülltonnen-Logo versehen sind
- an ein Unternehmen oder Institut in der EG verkauft wurden
- momentan von einem Unternehmen oder Institut in der EG besessen werden
- noch intakt sind, also nicht zerlegt und nicht kontaminiert



Da sich die WEEE auf in sich geschlossene, funktionierende elektrische oder elektronische Produkte bezieht, gilt der oben beschriebene Service nicht für folgende Thorlabs Produkte:

- Fremdteile, die durch den Benutzer eingebaut wurden
- Komponenten
- Mechaniken und Optiken
- Teile, die beim Zerlegen von Einheiten übrig geblieben sind (Leiterplatten, Gehäuse usw.).

Wenn Sie ein Thorlabs Produkt zur Entsorgung geben möchten, dann setzen Sie sich bitte mit Thorlabs oder Ihrem Händler in Verbindung.

13.1. Verantwortung für die Müllentsorgung

Wenn Sie ein Produkt nach Ende seines Lebenszyklus nicht an Thorlabs zurückgeben, so übergeben Sie es einem Unternehmen, welches auf Müllentsorgung spezialisiert ist. Entsorgen Sie das Produkt nicht in einem Mülleimer oder auf einer öffentlichen Müllhalde.

13.2. Ökologischer Hintergrund

Es ist bekannt, dass elektrische und elektronische Produkte bei ihrer Zersetzung die Umwelt verschmutzen, indem sie giftige Stoffe abgeben. Das Ziel der europäischen RoHS-Verordnung ist es, die Menge solcher Stoffe in den elektronischen Produkten in Zukunft zu verringern.

Das Ziel der WEEE-Verordnung ist es, das Recycling solcher Produkte durchzusetzen, da ein kontrolliertes Recycling der Produkte am Ende ihres Lebenszyklus negative Folgen für die Umwelt vermeidet.

Kapitel 14 Thorlabs weltweit

Für technischen Support oder Verkaufsanfragen besuchen Sie uns bitte unter www.thorlabs.com/contact, um unsere aktuellen Kontaktinformationen zu erhalten.

.

USA, Canada, and South America
Thorlabs, Inc.
sales@thorlabs.com
techsupport@thorlabs.com

UK and Ireland
Thorlabs Ltd.
sales.uk@thorlabs.com
techsupport.uk@thorlabs.com

Europe
Thorlabs GmbH
europe@thorlabs.com

Scandinavia
Thorlabs Sweden AB
scandinavia@thorlabs.com

France
Thorlabs SAS
sales.fr@thorlabs.com

Brazil
Thorlabs Vendas de Fotônicos Ltda.
brasil@thorlabs.com

Japan
Thorlabs Japan, Inc.
sales@thorlabs.jp

China
Thorlabs China
chinasales@thorlabs.com

THORLABS

www.thorlabs.com