Praktikum Moderne Physik für Lehramtsstudierende

Quantenkryptographie im Analogieversuch

Karlsruher Institut für Technologie
Fakultät für Physik

Inhaltsverzeichnis

1 Quantenkryptographie **3**

1.1 Einführung 4

1.2 Schlüsselverteilung: $\lambda/2$ - Plättchen und Datenübertragung mit einer Basis 6

1.3 Schlüsselverteilung – jetzt aber richtig 8

1.4 Detektion eines Lauschers 10

1.5 Was heißt „zufällig“? 11

1.6 Warum kann man die Information nicht kopieren? 12

1.7 Wie läuft das Experiment ab? 12

1.8 Klassisches Licht vs. einzelne Photonen 14

Vorbemerkung:

Der folgende Versuch zur Quantenkryptographie ist ein Analogieversuch, da er nicht mit einzelnen Photonen durchgeführt wird, sondern mit "klassischem Licht"(d.h. mit Laserlicht). Um echte Quanteneffekte zu zeigen, müssten die Experimente mit einer Einzelphotonquelle durchgeführt werden, was sehr aufwendig und teuer ist. Die Analogie-Experimente eignen sich aufgrund des einfachen und transparenten Aufbaus und des günstigeren Preises zudem sehr gut für den Schulunterricht in der gymnasialen Oberstufe.

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 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“ (Quantenschlüsselaustausch).

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 ergeben sich nun - bei großer Statistik - bis zu 25% falsche Test-Bits, wodurch Eve 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 vollständig identisch. Dadurch ist dieser Aufbau sehr gut als Analogieversuch verwendbar.

1.1 Einführung

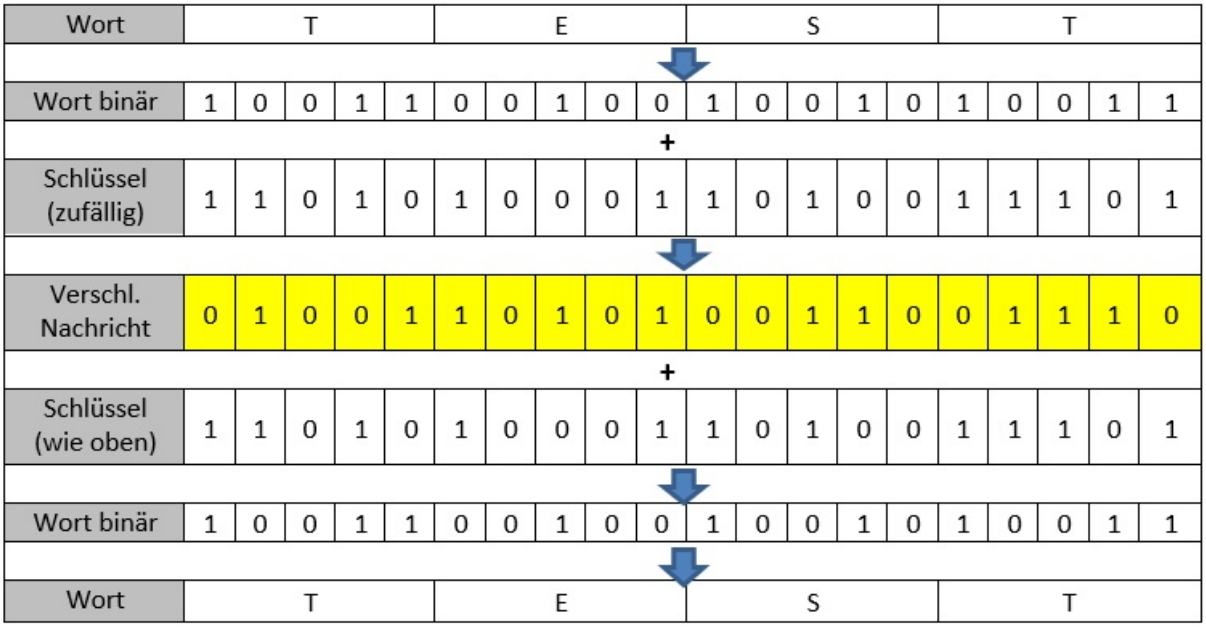
Kryptografie beschreibt die Verschlüsselung von Daten, also das Unkenntlichmachen einer Nachricht, wodurch sie im Idealfall nur für den Sender und den Empfänger lesbar ist. Der Besitz der verschlüsselten Nachricht hat also nur dann Sinn, wenn der Schlüssel zum Decodieren bekannt ist. Die Sicherheit des 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 100lediglich bei der Erfüllung der Voraussetzungen, das Verfahren selbst ist klassisch. Man stelle sich vor, dass man eine vollständig 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 vollständig zufällig ist. Das ist die verschlüsselte Nachricht.

Für die binäre Addition gelten die „Rechenregeln“

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

- $1 + 1 = 0$ (mit Übertrag 1)

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 im Dokument ”Justieranleitungen und Messprotokolle”binär kodiert werden kann:



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 **vollständig** zufällig war, hat er auch keinen Anhaltspunkt zum „Knacken“ des Schlüssels. Damit ist die Nachricht **vollständig** abhörsicher.

Nötige Voraussetzungen:

1. Der Schlüssel muss mindestens so lang sein wie die Nachricht.
2. Der Schlüssel darf nur einmal verwendet werden.
3. Der Schlüssel muss vollständig 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 Abschnitt 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.

1.2 Schlüsselverteilung: $\lambda/2$ - Plättchen 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 nachfolgender Abbildung gezeigt:

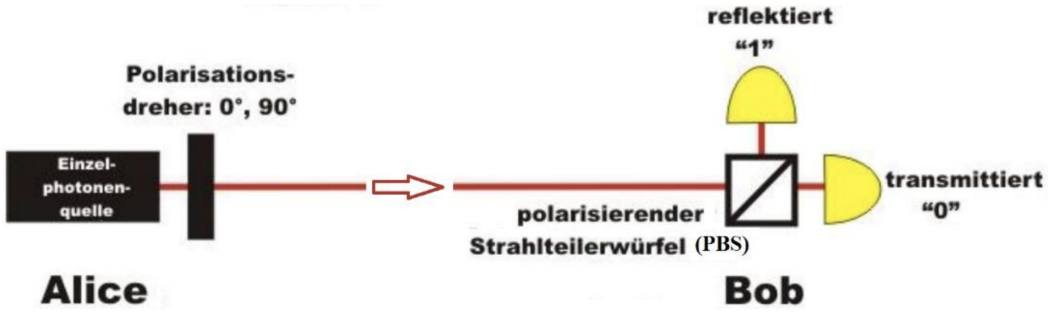


Abbildung 1: Datenübertragung mit einer Polarisations-Basis

Die Sende-Einheit „Alice“ besteht aus der Einzelphotonquelle und einem $\lambda/2$ - Plättchen.

Drehwinkel: Das $\lambda/2$ - Plättchen 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 des $\lambda/2$ - Plättchens.

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

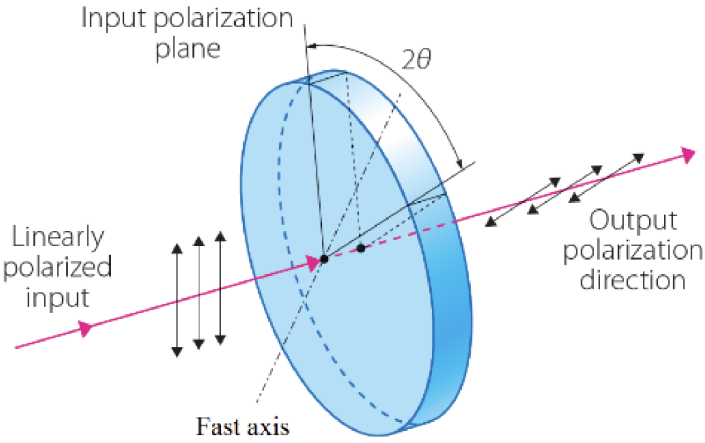


Abbildung 2: Polarisationsdrehung durch ein $\lambda/2$ - Plättchen

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. Abb. 3. 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“.

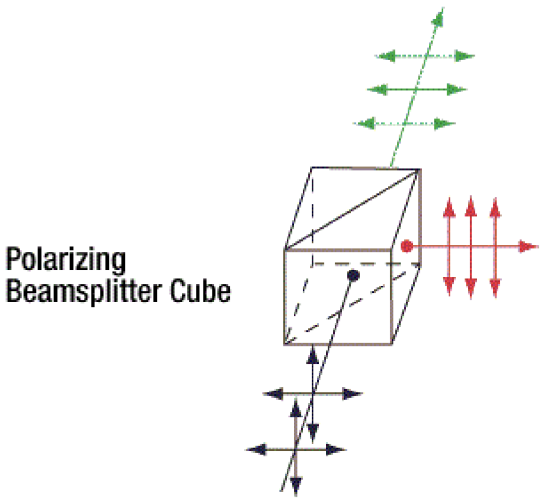


Abbildung 3: Polarizing Beamsplitter Cube

1.3 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. 4. Das ist auch der Aufbau, wie er für die Quantenkryptografie und für dieses Versuchspaket verwendet wird.

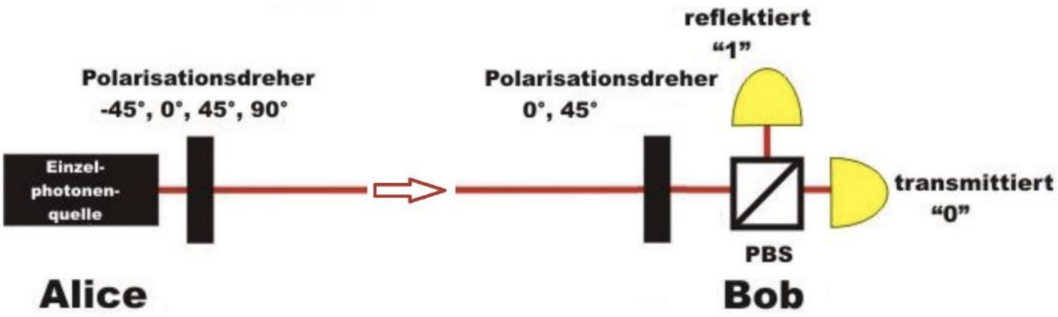


Abbildung 4: Quantenkryptografie-Aufbau, mit den Basen + (= 0° und 90°) und x (= -45° und 45°)

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

Tabelle 1: Messwerte zur Polarisationsmessung bei Alice und Bob. Achtung: Die Werte in der Tabelle beziehen sich rein auf die Einstellungen an den Komponenten. Beachten Sie dabei, dass der Polarisationsdreher bei Bob in die andere Richtung hin aufgebaut ist als bei Alice. Wäre er gleich ausgerichtet, müssten die Winkel anders eingestellt werden, damit die Ergebnisse dieselben blieben (Wie..?).

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

[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.

unweigerlich Fehler erzeugt.

1.4 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. 5 dargestellt.

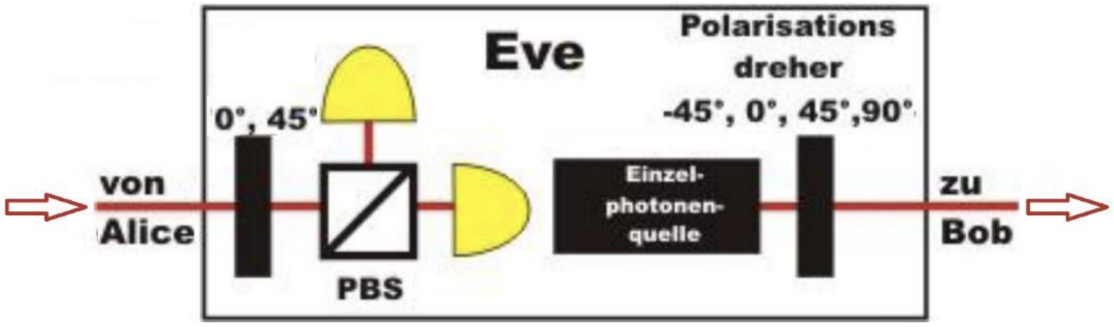


Abbildung 5: Lauscher Eve zwischen Alice und Bob

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 BasenVergleich 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].

1.5 Was heißt „zufällig“?

Wie oben beschrieben, basiert das One-Time Pad u.a. darauf, dass der Schlüssel vollständig 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, dass auf einen 50:50 Strahlteiler trifft, wird rein zufällig transmittiert oder

[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%

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%

Tabelle 2: Übersicht der verschiedenen Fälle

reflektiert. Im Mittel wird je die Hälfte transmittiert und die andere Hälfte reflektiert, die „Entscheidung“ des einzelnen Photons ist aber vollständig zufällig. Dies trifft nicht nur auf Photonen zu, auch viele weitere Prozesse wie radioaktiver Zerfall sind quantenphysikalisch vollständig 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 vollständig zufällig verteilt.

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

1.6 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.

1.7 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:

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

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

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).
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 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.

Tabelle 3: Versuchsablauf

- Authentifizierung: Bereits am Anfang der Kommunikation werden einige Bits ausgetauscht. 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.

1.8 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 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 vollständig identisch zum quantenphysikalischen Fall.