

Kapitel 7

BB84 - Quantenkryptographie

Quantenkryptographie ist eine der vielen faszinierenden Anwendungen der Quanteninformation. Die Möglichkeit, Nachrichten austauschen zu können, ohne dass diese Nachrichten von dritter Seite abgehört oder entschlüsselt werden können, bietet viele Anwendungen, die - wie immer in solchen Fällen - natürlich auch missbraucht werden können.

Bei den meisten Protokollen zur Quantenkryptographie, unter anderem auch bei dem Protokoll BB84 (benannt nach Charles Bennett und Gilles Brassard, die es 1984 entwickelten [1]), geht es allerdings nur darum, einen idealen Schlüssel - also eine Zufallsfolge von Bits - auszutauschen, der später für die Verschlüsselung der Nachricht verwendet werden kann. Die verschlüsselte Nachricht wird in klassischer Form verschickt. Wichtig ist, dass man überprüfen kann, ob der Schlüssel außer den beiden Teilnehmern (Sender und Empfänger der Nachricht) tatsächlich niemandem bekannt ist. Genau das leistet das BB84 Protokoll.

Für die ideale Übertragungssituation fordert man meist gewisse Bedingungen, die erfüllt sein sollten. So haben beide Teilnehmer - hier verwendet man meist die Bezeichnung Alice für die Senderin der Nachricht und Bob für den Empfänger der Nachricht - einen abgeschlossenen Bereich, in den kein externer Lauscher - hierfür verwendet man die Bezeichnung Eve, nach dem englischen Begriff 'evesdropper - Lauscher' - eindringen kann. Ein Eingreifen von Eve ist nur in Bezug auf die Übertragung von Daten möglich, solange sich diese Daten in einem freien Bereich befinden. Außerdem wird vorausgesetzt, dass Alice und Bob sich über einen klassischen Kanal (z.B. Telefon oder Videokanal) austauschen und dabei verifizieren können, dass sie tatsächlich mit dem/der jeweiligen Partner/Partnerin sprechen. Bei einem klassischen Übertragungskanal wird also angenommen, dass sich Eve nicht als Alice oder Bob ausgeben kann. Allerdings kann Eve natürlich einem solchen Gespräch lauschen.

Wir beginnen mit einer kurzen Beschreibung der klassischen Kryptographie mithilfe eines sogenannten binären One-Time-Pads, also eines binären Schlüssels, der eine Zufallsfolge von Bits darstellt und auch nur einmal verwendet wird. Anschließend wird beschrieben, wie man mit Verfahren der Quantentheorie einen solchen Schlüssel abhörsicher austauschen kann.

7.1 One-Time-Pad - klassische Kryptographie

Ein One-Time-Pad ist eine Folge von Bits, die zur Verschlüsselung einer Nachricht verwendet werden kann. Es gibt auch One-Time-Pads als dezimale Zahlenfolgen oder Buchstabenfolgen, doch diese sind nicht sicherer als eine binäre Bitfolge. Man benötigt allerdings mehr Zeichen bei einer binären Nachrichtenübertragung. Außerdem muss die zu verschlüsselnde Nachricht ebenfalls als Bitfolge vorliegen.

Das One-Time-Pad sollte folgende vier Bedingungen genügen:

- Die Bitfolge muss mindestens so lang sein wie der zu verschlüsselnde Text.
- Es soll sich um eine Zufallsfolge von Bits handeln.
- Die Bitfolge oder Teile von ihr werden kein zweites Mal (weder in der vorliegenden Nachricht noch in anderen Nachrichten) verwendet.
- Die Bitfolge darf nur dem Sender und Empfänger bekannt sein.

Unter diesen Bedingungen kann man beweisen, dass eine entsprechend verschlüsselte Nachricht ~~auch durch einen beliebig hohen Rechenaufwand~~ nicht entschlüsselt werden kann.

Bedingung 1 und 3 lassen sich sehr leicht erfüllen, Bedingung 2 ist etwas schwieriger, da die meisten sogenannten Zufallszahlengeneratoren auf einem deterministischen Algorithmus beruhen und damit für jemanden, der diesen Algorithmus sowie den Anfangszustand kennt, auch reproduzierbar sind. Die eigentliche Problematik ist aber die Bedingung 4: Wie kann man sicher sein, dass niemand außer den Teilnehmern die Bitfolge kennt, insbesondere, wenn diese Bitfolge über einen öffentlichen bzw. abhörbaren Kanal ausgetauscht wurde? Wir werden sehen, dass sowohl Bedingung 2 als auch Bedingung 4 im Rahmen der Quantenkryptographie erfüllt werden können.

Ist eine Zufallsbitfolge gegeben, erfolgt die Verschlüsselung ~~meist~~ durch eine ~~einfache~~ XOR-Operation mit der zu verschlüsselnden Nachricht. Die daraus entstandene Bitfolge ist unabhängig von der darin enthaltenen Nachricht nach allen detektierbaren Kriterien ebenfalls wieder eine Zufallsfolge und kann über einen öffentlichen Kanal verschickt werden. Der Empfänger kann diese verschlüsselte Nachricht entziffern, indem er mit demselben Schlüssel nochmals eine XOR-Operation durchführt. Da sowohl $0+0$ als auch $1+1$ bezüglich XOR die 0 ergeben, wird durch die insgesamt zweifache XOR-Addition des Schlüssels die ursprüngliche Nachricht wieder hergestellt. Dies zeigt folgendes Beispiel, bei dem ein Klartext mit einer Zufallsfolge (dem One-Time-Pad) zu einer verschlüsselten Nachricht umgewandelt und anschließend mit demselben One-Time-Pad wieder entschlüsselt wird:

Klartext	1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0 1 1 1	
Zufallsfolge (One-Time-Pad)	0 1 1 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 0 0 1	
XOR-kodierte Nachricht	1 0 0 0 1 0 1 1 0 0 1 1 0 1 0 1 0 1 1 1 0	(7.1)
Zufallsfolge (One-Time-Pad)	0 1 1 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 0 0 1	
XOR-Dekodierung=Klartext	1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0 1 1 1	


7.2 Das BB84-Protokoll

Wie schon erwähnt geht es bei dem BB84-Protokoll nur um den sicheren Austausch eines Schlüssels, also eines One-Time-Pads. Für das BB84-Protokoll werden auch keine verschränkten Photonen benötigt. Es gibt allerdings andere Protokolle, die von verschränkten Zuständen Gebrauch machen.


Wichtig für das Verständnis der Quantenkryptographie sind folgende Tatsachen: (1) ein unbekannter Polarisationszustand eines Einzelphotons kann nicht gemessen werden. Man kann lediglich eine Orientierungsbasis für die Polarisation wählen und erhält bei einer Messung eine der beiden möglichen Orientierungen als Ergebnis. Ob diese Orientierung auch vorher vorlag, ist dabei nicht bekannt. (2) Quantenzustände kann man nicht klonen, d.h., man kann keine Kopien eines Quantenzustands herstellen und dabei das Original behalten. Die Quantenteleportation erlaubt zwar die Erstellung einer Kopie, aber dabei geht das Original verloren, d.h., es gibt immer nur einen Zustand mit den ursprünglichen Eigenschaften. (3) Ist die Orientierungsbasis bekannt, d.h., ist bekannt, bezüglich

welcher Orientierung eine Polarisation präpariert wurde, kann diese natürlich auch ausgelesen und kopiert werden.

Das Protokoll für den Schlüsselaustausch besteht aus drei Schritten, ein weiterer Schritt kann verwendet werden, um ~~zum~~ zu überprüfen, ob der Schlüssel abgehört wurde. Auf diesen letzten Schritt gehen wir in Abschnitt 7.2.5 ein, die ersten drei Schritte sind:

1. Alice präpariert  Polarisationszustände von Photonen bezüglich zweier Basissysteme und verschickt diese an Bob.
2. Bob nimmt Polarisationsmessungen an den Photonen vor, wobei er zwischen den beiden vorab gewählten Basissystemen zufällig auswählt.
3. Alice und Bob vergleichen über einen klassischen Kanal, welche Basis sie bei den einzelnen Photonen gewählt haben. Die Bitfolge in den übereinstimmenden Fällen ist ihre Zufallsfolge.

7.2.1 Alice präpariert die Photonen für Bob

Alice (die Senderin) möchte sich mit Bob (dem Empfänger) einen **One-Time-Pad** teilen, den nur die beiden kennen. Dazu benötigt Alice zunächst eine **Quelle** von Einzelphotonen, deren Polarisationszustand sie gezielt bezüglich einer von ihr gewählten  Orientierung präparieren kann. Dabei werden nur zwei mögliche Orientierungen zugelassen: Die Orientierung bezüglich horizontaler-vertikaler Polarisation und die Orientierung bezüglich einer $+45^\circ$ - -45° diagonalen Polarisation (siehe Abb. 7.1).

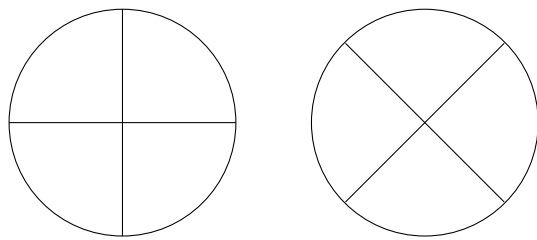






Abbildung 7.1: Die beiden Basissysteme für die Präparations- bzw. Messanordnungen beim BB84-Protokoll. (links) horizontal-vertikal (h/v -Basis), (rechts) $+45^\circ$ - -45° ($+/-$ -Basis).

Alice erzeugt nun eine Folge von Einzelphotonen, die jeweils eine zufällige Polarisation bezüglich einer der beiden Polarisationsorientierungen haben, d.h. die zufällig eine der vier Polarisationen  h , v , $+$ oder $-$ haben. Das kann z.B. folgendermaßen geschehen (es geht hier nur um ein Prinzip, nicht um die in der Praxis verwendete Realisierung): Es gibt nicht  lineare Kristalle (z.B. Bariumborat, ~~BBO~~), bei denen ein einfallendes Photon einer bestimmten Energie in zwei Photonen von jeweils der halben Energie (doppelte Wellenlänge) umgewandelt wird. Eines dieser Photonen dient als Signalphoton - es zeigt an, dass ein zweites Photon (das sogenannte Idler-Photon) in diesem Moment in eine bestimmte Richtung emittiert wird. Gewöhnlich hat dieses zweite Photon eine wohldefinierte Polarisation, die Alice in eine der vier genannten Polarisationen drehen kann. Sie kennt also den genauen Polarisationszustand des Photons, das sie an Bob schickt. Alice sollte die Orientierungen, bezüglich der sie die Polarisationen präpariert, zufällig wählen, z.B. mithilfe eines **Quantenzufalls-** **zahlgenerators**.

Diese Folge von Einzelphotonen schickt Alice an Bob. Sie hat dabei für jedes einzelne dieser Photonen folgende Information, die sie natürlich geheim hält: Sie kennt die Basis, bezüglich der sie die Polarisation der Photonen präpariert hat, und sie kennt den zugehörigen Polarisationszustand dieses Photons. Hierbei verwendet man eine Konvention, die vorher festgelegt wurde, z.B. 0 für den Zustand h in der h/v -Basis und 1 für den Zustand v in der h/v -Basis, entsprechend 0 für den Zustand $+$ in der $+/-$ -Basis und 1 für den Zustand $-$ in der $+/-$ -Basis. Alice besitzt also eine Tabelle wie in Tab. 7.1.



Photon	1	2	3	4	5	6	7	8	9	10	11	12	13
Basis	$+/-$	$+/-$	h/v	$+/-$	h/v	h/v	h/v	$+/-$	$+/-$	h/v	$+/-$	$+/-$	$+/-$
Wert	1	0	0	1	0	0	0	0	1	0	1	1	0

Tabelle 7.1: Tabelle von Alice der Photonenzustände, die sie an Bob verschickt.



7.2.2 Bob nimmt an den Photonen von Alice Messungen vor


Bob erhält von Alice die Folge der Photonen und weiß nur, dass jedes einzelne Photon entweder bezüglich der Basis h/v oder bezüglich der Basis $+/-$ präpariert wurde. Er nimmt nun an jedem dieser Photonen eine Messung vor, wobei er die Basis dieser Messung ebenfalls zufällig wählt. In ungefähr der Hälfte dieser Messungen wählt Bob eine Basis, die mit der Präparationsbasis von Alice übereinstimmt. In diesen Fällen stimmt sein Ergebnis ~~natürlich~~ mit dem Ergebnis von Alice überein. In der anderen Hälfte der Fälle ist seine Basis von der Präparationsbasis von Alice verschieden und seine Ergebnisse sind zufällig. Bob erhält dadurch eine ähnliche Tabelle wie vorher Alice (siehe Tab. 7.2).


Photon	1	2	3	4	5	6	7	8	9	10	11	12	13
Basis	h/v	$+/-$	h/v	h/v	$+/-$	$+/-$	h/v	h/v	$+/-$	h/v	h/v	h/v	$+/-$
Wert	1	0	0	0	1	0	0	0	1	0	0	1	0



Tabelle 7.2: Tabelle von Bob der Photonenzustände, die er an den Photonen von Alice gemessen hat. Stimmt die Basis mit der von Alice überein, sind die Ergebnisse gleich, andernfalls sind sie zufällig.

7.2.3 Alice und Bob vergleichen ihre Basissysteme



Nachdem Alice ihre Photonen an Bob verschickt hat und Bob an diesen Photonen die genannten Messungen vorgenommen hat, vergleichen Alice und Bob über einen klassischen Kanal, für welche der Photonen sie diese  Basis gewählt haben. Das wird  bei ungefähr der Hälfte der Photonen der Fall sein.

Dieser klassische Kanal kann ~~ruhig~~ abgehört werden, die ausgetauschte Information ist nicht mehr verwendbar, da Bob die Photonen schon vermessen hat (und wegen des No-Cloning  Theorems auch beim Austausch der Photonen keine Kopien angefertigt werden konnten). Alice und Bob müssen nur sicherstellen, dass sie tatsächlich miteinander kommunizieren und die ausgetauschte Information authentisch übertragen wird.

Sie tauschen natürlich nur die jeweils gewählten Basissysteme h/v bzw. $+/-$ aus, keine Informationen über die dabei präparierten  bzw. gemessenen Werte. Falls die Basis, die Alice zur Präparation verwendet hat, und die Basis, in der Bob die Messung vorgenommen hat, dieselbe ist, sollten die Werte übereinstimmen. Alle anderen Fälle werden verworfen, da in diesen Fällen die Bitwerte zufällig gleich oder verschieden sein können.

Bob verschickt über den klassischen Kanal im Wesentlichen die zweite Zeile seines Messprotokolls. Alice vergleicht diese Zeile mit ihrer zweiten Zeile und schickt an Bob die Nummern  der Photonen zurück, für die beide Basen gleich sind. Das sind in obigem Fall die Photonen 2, 3, 7, 9, 10 und 13. Die Bit-Werte zu diesen Photonen sind beiden bekannt und sie sind gleich. Haben Alice und Bob ihre Basen zufällig gewählt, handelt es sich auch um eine Zufallsfolge. Diese Folge können sie  ihren Schlüssel verwenden.

7.2.4 Eve



Da ein möglicher ischer nur in die Übertragung von Photonen bzw. Information über öffentliche  Kanäle eingreifen kann, bleibt Eve nur eine Möglichkeit: Sie muss die Photonen, die Alice an Bob verschickt, abfangen und ebenfalls Messungen an diesen Photonen vornehmen. Zu diesem Zeitpunkt ist noch nicht bekannt, bezüglich welcher Basis Bob seine Photonen ausmessen wird, da er diese Photonen noch nicht erhalten hat. Also wählt Eve zufällig für jedes Photon eines der beiden Basissysteme. Auch sie erhält so eine Folge von Bits sowie eine Tabelle mit der von ihr gewählten Basis (siehe Tab. 7.3).

Photon	1	2	3	4	5	6	7	8	9	10	11	12	13
Basis	h/v	h/v	$+/-$	$+/-$	h/v	$+/-$	h/v	h/v	h/v	$+/-$	$+/-$	h/v	$+/-$
Wert	1	1	0	1	0	0	0	1	0	0	1	0	0

Tabelle 7.3: Tabelle von Eve der Photonenzustände, die sie an den Photonen von Alice gemessen hat. Stimmt die Basis mit der von Alice überein, sind die Ergebnisse wieder gleich. Sie verschickt ihre Photonen in den von ihr gewählten Basen und den von ihr bestimmten Zuständen. Das ist das Beste, was sie unter diesen Umständen machen kann. In rund der Hälfte der Fälle wird diese Basis mit Alice übereinstimmen. In den anderen Fällen erhält sie Zufallsergebnisse.


In den obigen Tabellen hat Eve für die Photonen 4, 5, 7, 11 und 13 dieselbe Basis gewählt wie Alice. Für die anderen Photonen sind ihre Ergebnisse zufällig. Sie verschickt nun eine Folge von Photonen an Bob, die exakt ihrer Tabelle entspricht, d.h., sowohl die Basissysteme sind für die einzelnen Photonen dieselben als auch die Polarisationen, die sie in der jeweiligen Basis für die Photonen erhalten hat. Sie kann nur hoffen, dass möglichst viele dieser Basissysteme mit den Basen von Alice übereinstimmen.


7.2.5 Überprüfung der Zufallsfolge

 Der letzte Schritt, den Bob und Alice ausführen  sollen, ist die Überprüfung, ob die ausgetauschten Photonen abgefangen und durch Messungen manipuliert wurden.



Photon	1	2	3	4	5	6	7	8	9	10	11	12	13
Alice Basis	$+/-$	$+/-$	h/v	$+/-$	h/v	h/v	h/v	$+/-$	$+/-$	h/v	$+/-$	$+/-$	$+/-$
Wert	1	0	0	1	0	0	0	0	1	0	1	1	0
Bob Basis (oE)	h/v	$+/-$	h/v	h/v	$+/-$	$+/-$	h/v	h/v	$+/-$	h/v	h/v	h/v	$+/-$
Wert	1	0	0	0	1	0	0	0	1	0	0	1	0
Eve Basis	h/v	h/v	$+/-$	$+/-$	h/v	$+/-$	h/v	h/v	h/v	$+/-$	$+/-$	h/v	$+/-$
Wert	1	1	0	1	0	0	0	1	0	0	1	0	0
Bob Basis (mE)	h/v	$+/-$	h/v	h/v	$+/-$	$+/-$	h/v	h/v	$+/-$	h/v	h/v	h/v	$+/-$
Wert	1	1	0	0	1	0	0	1	1	1	0	0	0

Tabelle 7.4: Die gesamte Tabelle des BB84-Protokolls. Die erste Doppelzeile gibt die Basis und die Werte an, in Bezug auf die Alice ihre Photonen präpariert hat. Die nächste Doppelzeile entspricht dem, was Bob für den Fall gemessen hätte, wenn Eve keine Photonen abgefangen hätte. Die dritte Doppelzeile zeigt die Ergebnisse von Eve und die letzte Doppelzeile die Ergebnisse von Bob, die er erhalten hat, nachdem Eve ihre Photonen so weitergeschickt hat, wie sie bei ihr gemessen wurden.


Tabelle 7.4 enthält ~~nochmals~~ alle Resultate, die Alice, Bob und Eve erhalten haben, wobei bei Bob unterschieden wird, ob er direkt die Photonen von Alice erhalten hat (oE - ohne Eve), oder ob Eve die Photonen abgefangen und an ihnen Messungen vorgenommen hat (mE - mit Eve). 


Nachdem Alice und Bob ihre Basissysteme ausgetauscht haben (dieses Gespräch kann Eve abhören, ~~sie kann zu diesem Zeitpunkt nicht mehr eingreifen~~) wissen sie, welche Bitfolge sie für ihren Schlüssel nehmen können. Zur Überprüfung verwenden sie nun eine ausreichende Anzahl dieser Bits und vergleichen diese über einen klassischen (off ) Kanal. In der obigen Liste sind beispielsweise Alice und Bob zu dem Schluss gekommen, dass sie bei den Photonen 2, 3, 7, 9, 10 und 13 dieselben Werte haben sollten. Vergleichen sie nun diese Bits über einen offenen Kanal stellen sie fest, dass nach dem Eingriff von Eve Photon 2 und 10 nicht zu demselben Bit gehören. Daraus können sie schließen, dass ihr Photonen austausch abgefangen und manipuliert wurde. Sie werden nun sämtliche Bits ihrer Folge verwerfen und einen neuen Schlüsselaustausch versuchen.

Alice und Bob sollten also deutlich mehr Bits für ihren Schlüssel erstellen, als sie für die Verschlüsselung ihrer Nachricht benötigen. In der Praxis kann man mehrere Tausend Bits des Schlüssels vergleichen und so ziemlich sicher feststellen, ob der Schlüssel durch Eve manipuliert wurde. Eve hat, bei korrekter Durchführung des Protokolls, keine Möglichkeit, die fehlerhaften Bits zu unterdrücken.

Ganz grob kann man sagen, dass rund die Hälfte der Bits, die Alice und Bob mit dem Verfahren generieren, übereinstimmen und für die Verschlüsselung (bzw. einen Teil davon für den Test) verwendet werden können. Falls Eve die Photonen abgefangen und manipuliert hat, hat sie in rund der Hälfte dieser Fälle eine andere Basis gewählt als Alice und Bob, und davon wird  rund der Hälfte der Fälle das Bit bei Bob ein anderes sein als bei Alice. Ganz grob kann man also sagen, dass ein Viertel der Bits, die Alice und Bob als gemeinsame Folge identifiziert haben, bei einem Eingriff von Alice andere Werte haben sollten. Verwendet man einige Tausend Bits zur Verifikation des Schlüssels, sollte ein solcher Eingriff auffallen. 

7.3 Schulische Teilrealisierung durch Laserlicht

Eine vollständige Realisierung dieses Protokolls scheitert in der Schule ~~schon~~ an dem Problem, dass kaum Experimente mit einzelnen Photonen möglich sein werden . Man kann das Protokoll aber teilweise realisieren, indem man Laserlicht mit Polarisationsfiltern präpariert bzw. misst. Die Zufallselemente, die bei Einzelphotonen bestimmen, welches Bit bei einer bestimmten Basis gemessen wird, kann man durch einen Würfel ersetzen. Im Folgenden werden nochmals die Schritte des Protokolls durchgespielt, wie man sie in der Schule mit einfachen Mitteln (Laserpointer, Polarisationsfilter und geeigneten Würfeln) umsetzen kann. Die folgenden Schritte sollten ausreichend oft wiederholt werden.

1. Alice würfelt für jedes „Photon“ eine Basis. Bei einem normalen Würfel kann man beispielsweise eine gerade Augenzahl für die Basis h/v wählen und eine ungerade Augenzahl für die Basis $+/-$. **Es gibt aber auch Würfel,  denen h/v und $+/-$ schon auf den Würfelseiten verteilt sind.** Sie würfelt ein zweites Mal und entscheidet damit, auf welche Polarisation der Filter hinter ihrem Laser eingestellt wird (diese Polarisation sollte natürlich mit der vorher gewürfelten Basis verträglich sein). Dann sendet Alice an Bob Laserlicht, das der entsprechenden Polarisation entspricht.
2. Bob entscheidet mit einem Würfel, bezüglich welcher Basis er das Laserlicht von Alice messen möchte. Er wählt nun diese Basis für die Polarisationsfilter, auf die er das Laserlicht von Alice schickt. Bei manchen Aufbauten kann Alice ihre Laserlicht durch einen Strahlteiler aufspalten und dann gleichzeitig auf die beiden orthogonal eingestellten Filter von Bob lenken. Nun gibt es zwei Möglichkeiten: (1) Alice und Bob haben dieselbe Basis gewählt. Dann hat das Laserlicht

von Alice eine Polarisierung, die nur von einem Filter bei Bob durchgelassen wird. Das zugehörige Bit zu diesem Filter (sowie die gewählte Basis) vermerkt Bob in seiner Liste. (2) Falls Bob eine andere Basis als Alice gewählt hat, erkennt er das daran, dass das Laserlicht von Alice durch beide Filter hindurchgeht. In diesem Fall würfeln sie ein beliebiges Bit. Bei Einzelphotonen würde Bob in diesem Fall auch nur ein Ergebnis erhalten, d.h., er kann an diesem Punkt nicht feststellen, dass er die falsche Basis gewählt hat. Das gewürfelte Bit wird später, nachdem die Basisstellungen ausgetauscht wurden, nicht gewertet.

3. Im letzten Schritt tauschen Bob und Alice ihre Basissysteme aus und sollten nun für die Fälle, in denen die Basis gleich war, dieselben Ergebnisse erhalten haben.
4. Falls Eve in den Prozess eingeschaltet wird, macht sie folgende Schritte: Sie würfeln eine Basis und misst bezüglich dieser Basis die Polarisation des einfallenden Laserlichts. Stimmt ihre Basis mit der von Alice überein, misst sie nur hinter einem ihrer Filter Licht und vermerkt das entsprechende Bit. Sind die Basen von Alice und Eve verschieden, beobachtet sie hinter beiden Filtern Laserlicht und würfeln ein Bit. Sie schicken nun Laserlicht mit der Basis und Polarisation an Bob, die sie verwendet w. gemessen oder gewürfelt hat.

Im Wesentlichen an diesem Punkt scheitert das Protokoll in der Realität, wenn man tatsächlich mit Laserlicht statt mit Einzelphotonen arbeiten möchte. Eve kann feststellen, ob sie dieselbe Basis wie Alice gewählt hat oder nicht: Wenn Sie bei einer Basis hinter beiden Filtern Licht beobachtet, ist es die falsche Basis. Mit Einzelphotonen kann Eve dies nicht feststellen.

5. Am Ende vergleichen Alice und Bob ihre Bits, von denen sie glauben, sie seien gleich.

Damit man ein Eingreifen von Eve bemerken kann, sollten insgesamt mindestens 15 bis 20 „Photonen“ ausgetauscht werden. Das kann bei sorgfältiger Durchführung des Experiments eine Weile dauern (insbesondere, wenn man die Schritte von Eve ebenfalls durchführen möchte), sodass leicht eine Doppelstunde mit diesem Protokoll verbraucht wird. Andererseits macht es auch Spaß, wenn man am Ende die Bits vergleicht und feststellt, ob bzw. dass Eve eingegriffen hat. Nach dem Austausch von vier oder fünf „Photonen“ kommt auch eine gewisse Routine hinzu und es geht schneller. Außerdem kann man auf diese Weise den Ablauf des Protokolls wirklich miterleben und begreifen.

Literaturverzeichnis

- [1] Bennett, C.H., Brassard, G., *Quantum cryptography: Public key distribution and coin tossing*; in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Vol. 175 (1984).