BB84 - Quantenkryptographie

Physikdidaktik, Albert-Ludwigs-Universität Freiburg

27.03.2024

Professor Dr. Thomas Filk

Weitere Kurztexte hier: https://physikdidaktik.uni-freiburg.de/kurztexte/

universität freiburg

Inhaltsverzeichnis

Kapitel 1

BB84 - Quantenkryptographie

Autor: Thomas Filk, Version vom: 27.03.2024

Kurzzusammenfassung

Eine gesicherte Nachrichtenübertragung ist mit einem Schlüssel möglich, der aus einer Zufallsfolge von Bits (0 und 1) besteht, der dieselbe Länge wie die zu übertragende Nachricht hat und der nur ein einziges Mal verwendet wird. Dieses Protokoll bezeichnet man als One-Time Pad. Die meisten Verfahren der Quantenkryptographie, insbesondere auch das sogenannte BB84-Protokoll, verwenden die Quantentheorie lediglich zur sicheren Erzeugung eines solchen Schlüssels (also einer Zufallsfolge aus 0 und 1), von dem überprüft werden kann, dass nur der Sender und der Empfänger diesen Schlüssel kennen.

Eine wesentliche Eigenschaft der Quantentheorie, die dieses Verfahren ermöglicht, ist das sogenannte „No-Cloning“-Theorem bzw. die Unmöglichkeit, einen unbekannten Quantenzustand eines Systems durch die Messung an einem Einzelsystem bestimmen zu können.

Alice erzeugt dazu eine Serie von Photonen, die sie in einer Zufallsfolge von horizontaler, vertikaler, $+45°$-diagonaler und $-45°$-diagonaler Polarisation präpariert und an Bob versendet. Bob analysiert den Polarsationszustand dieser Photonen mit Polarisationsstrahlteilern, deren Orientierung ebenfalls zufällig auf h/v (horizontal/vertikal) oder $+/-$ ($+45°$- und $-45°$-diagonal) gestellt wird. Anschließend tauschen Alice und Bob über einen klassischen Kanal die Folge der Basissysteme (h/v oder $+/-$) aus und wählen nur die Ergebnisse, bei denen sie zufällig dieselbe Basis gewählt haben. Die dabei gemessenen Polarisationen definieren ihren Schlüssel.

Eve kann die Photonen von Alice abfangen, ähnlich wie Bob die Polarisationszustände bezüglich zufällig gewählter Basen untersuchen, und dann gezielt diese Polarisationszustände an Bob weiterleiten. In rund der Hälfte der Fälle wird ihre Polarisation mit der von Alice übereinstimmen und die Photonen wurden nicht verändert. In der Hälfte der Fälle wählt sie jedoch die falsche Polarisation, sodass Bob in diesen Fällen wiederum in der Hälfte der Fälle ein anderes Ergebnis erhält als Alice (in der anderen Hälfte der Fälle sind die Ergebnisse zufällig gleich). Durch einen Vergleich eines Teils ihres Schlüssels lässt sich diese Diskrepanz nachweisen und somit feststellen, ob der Schlüsselaustausch „abgelauscht“ wurde.

Einführung

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 – in diesem Fall eine Zufallsfolge von Bits – auszutauschen, der später sowohl für die Verschlüsselung als auch für die Entschlüsselung der Nachricht verwendet werden kann. 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. Die eigentliche Nachricht wird nach klassischen Verfahren ver- und entschlüsselt und auch in klassischer Form verschickt.

Um nicht immer von einer Senderin oder einem Sender A und einer Empfängerin oder einem Empfänger B zu sprechen, haben sich in der Informationstheorie die Bezeichnungen „Alice“ für die Senderin der Nachricht und „Bob“ für den Empfänger der Nachricht etabliert. Den Lauscher bzw. die Lauscherin bezeichnet man meist als „Eve“, abgeleitet von der englischen Bezeichnung „evesdropper“ für Lauscher.

Für die Übertragungssituation des BB84 Protokolls fordert man gewisse Bedingungen, die erfüllt sein sollten, damit das Protokoll sicher ist. So haben sowohl Alice als auch Bob einen abgeschlossenen Bereich, in den kein externer Lauscher eindringen kann. Ein Eingreifen von Eve ist nur während der Übertragung von Daten möglich, solange sich diese Daten in einem offenen Bereich befinden. Außerdem wird vorausgesetzt, dass sich Alice und Bob über einen klassischen Kanal (z.B. Telefon oder Videokanal) austauschen und dabei verifizieren können, dass sie tatsächlich mit der jeweils anderen Person sprechen. Bei einem klassischen Übertragungskanal wird also angenommen, dass sich Eve nicht als Alice oder Bob ausgeben kann. In der Informatik bezeichnet man diese Bedingung als Authentizität. Allerdings kann Eve natürlich einem solchen Gespräch lauschen.

Wir beginnen mit einer kurzen Beschreibung des sogenannten One-Time-Pads, einem Protokoll der klassischen Kryptographie, bei dem einmalig eine Zufallsfolge von Bits sowohl vom Sender zur Verschlüsselung als auch vom Empfänger der Nachricht zur Entschlüsselung verwendet wird. Anschließend wird beschrieben, wie man mit Verfahren der Quantentheorie einen solchen Schlüssel austauschen und gleichzeitig sicherstellen kann, dass außer Alice und Bob niemand den Schlüssel kennt.

1.1 Klassische Kryptographie – das One-Time-Pad

Ein One-Time-Pad ist spezielles Protokoll der klassischen Kryptographie, bei dem eine Nachricht mit Hilfe einer Zufallsfolge von Bits vom Sender verschlüsselt und vom Empfänger entschlüsselt werden kann. Sender und Empfänger müssen diese Zufallsfolge kennen, allerdings sollte niemand sonst Informationen über diese Folge haben. Es gibt auch One-Time-Pads, bei denen dezimale Zahlenfolgen oder Buchstabenfolgen verwendet werden, doch sofern es sich in allen Fällen um wirkliche Zufallsfolgen handelt sind diese nicht sicherer als eine binäre Bitfolge. Man benötigt allerdings bei einer binären Nachrichtenübertragung mehr Zeichen. Außerdem muss die zu verschlüsselnde Nachricht ebenfalls als Bitfolge vorliegen, was sich aber immer erreichen lässt. Der Schlüssel des One-Time-Pads sollte den folgenden vier Bedingungen genügen:

1. Die Bitfolge muss mindestens so lang sein wie der zu verschlüsselnde Text.

2. Es muss sich um eine Zufallsfolge von Bits handeln.

3. Die Bitfolge oder Teile von ihr werden kein zweites Mal (weder in der vorliegenden Nachricht noch in anderen Nachrichten) wiederverwendet.

4. Die Bitfolge darf nur dem Sender und dem Empfänger bekannt sein. Auch keine einschränkenden Informationen über die Bitfolge dürfen potenziellen Lauschern bekannt sein.

Unter diesen Bedingungen kann man beweisen, dass eine entsprechend verschlüsselte Nachricht prinzipiell nicht entschlüsselt werden kann. Der Grund ist sehr einfach: Bei der mit einer Zufallsfolge verschlüsselten Nachricht handelt es sich wieder um eine Zufallsfolge, und wenn man alle möglichen Schlüssel ausprobiert, erhält man jede beliebige Bitfolge und somit auch jeden beliebigen Text derselben Länge. Sofern über den Schlüssel nichts bekannt ist, kann man auch keine Information über die ursprüngliche Nachricht gewinnen.

Bedingung 1 und 3 lassen sich im Prinzip sehr leicht erfüllen, sind aber in der Praxis oft ein Problem, da Sender und Empfänger für den Bedarfsfall oft sehr lange Schlüssel austauschen oder vorrätig haben müssen. Bedingung 2 ist etwas schwieriger, da die meisten sogenannten Zufallszahlgeneratoren auf einem deterministischen Algorithmus beruhen und damit für jemanden, der diesen Algorithmus sowie den Anfangszustand kennt, auch reproduzierbar sind. Die eigentliche Problematik ist aber 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 durch eine XOR-Operation, also eine Addition modulo 2, mit der zu verschlüsselnden Nachricht. Die Rechenregeln sind:[1]

$$0+0=1+1=0 \qquad 0+1=1+0=1\,. \tag{1.1}$$

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 (abwechselnd dreimal 0 und dreimal 1) mit einer Zufallsfolge zu einer verschlüsselten Nachricht umgewandelt und anschließend mit derselben Zufallsfolge 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 0 0 0
Zufallsfolge	0 1 1 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 0 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 0 0 1
Zufallsfolge	0 1 1 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 0 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 0 0 0

(1.2)

1.2 Das BB84-Protokoll

Wie schon erwähnt geht es bei dem BB84-Protokoll nur um den sicheren Austausch eines Schlüssels, also einer binären Zufallsfolge. Im Prinzip lässt sich das BB84-Protokoll mit jedem QBit, also jedem

[1] Man beachte, dass es sich hier nicht um eine binäre Addition im arithmetischen Sinne handelt. Die Summe $1+1=0$ führt nicht zu einem Übertrag in die nebenstehende Spalte.

quantenmechanischen Zwei-Zustandssystem durchführen, allerdings verwendet man meist die linearen Polarisationszustände von Photonen. Für das BB84-Protokoll werden auch keine verschränkten Photonen benötigt. Es gibt allerdings andere Protokolle, die von verschränkten Zuständen Gebrauch machen.

1.2.1 Messung und Präparation der Polarisation von Einzelphotonen

Wichtig für das Verständnis der Quantenkryptographie im Allgemeinen wie auch speziell für dass BB84-Protokoll sind folgende Tatsachen:

1. Ein unbekannter Polarisationszustand eines Einzelphotons kann nicht durch Messungen bestimmt werden. Ein polarisationsabhängiger Strahlteiler oder auch ein Polarisationsfilter hat immer eine bestimmte Orientierung. Dadurch wird eine Basis aus zwei orthogonalen Polarisationszuständen ausgezeichnet. Eine „Messung“ findet immer in Bezug auf diese Basis statt und man erhält einen der beiden möglichen Basiszustände als Ergebnis. Ob diese Polarisation auch vorher schon vorlag, ist dabei nicht bekannt.

2. Quantenzustände kann man nicht clonen, 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 Polarisationsbasis bekannt, d.h., ist bekannt, bezüglich welcher Orientierung (z.B. eines Polarisationsstrahlteilers) eine Polarisation präpariert wurde, kann diese natürlich auch ausgelesen und kopiert werden.

Das Protokoll für den Schlüsselaustausch besteht aus drei Schritten. In einem weiteren Schritt kann überprüft werden, ob der Schlüssel abgehört wurde. Auf diesen letzten Schritt gehen wir in Abschnitt 1.2.6 ein, die ersten drei Schritte sind:

1. Alice präpariert zufällig ausgewählte Polarisationszustände von Photonen bezüglich zweier vorab festgelegter Orientierungen (Basissysteme) und verschickt diese an Bob. Diese Polarisationszustände kodieren eine Bitfolge.

2. Bob nimmt Polarisationsmessungen an den Photonen vor, wobei er zwischen den beiden vorab festgelegten möglichen Orientierungen (Basissystemen) zufällig auswählt. Er erhält auf diese Weise ebenfalls eine Bitfolge.

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.

Diese Schritte werden im Folgenden eingehender behandelt.

1.2.2 Alice präpariert die Photonen für Bob

Alice (die Senderin) möchte sich mit Bob (dem Empfänger) eine binäre Zufallsfolge teilen, die nur sie beide kennen. Dazu benögt Alice zunächst eine Quelle von Einzelphotonen, denen sie gezielt bestimmte Polarisationszustände verleihen kann. Sie wählt dabei zwischen vier möglichen Polarisationszuständen aus, die den Basiszuständen von zwei Orientierungen eines Polarisationsstrahlteilers entsprechen: die Basiszustände bezüglich horizontaler-vertikaler Orientierung und die Basiszustände

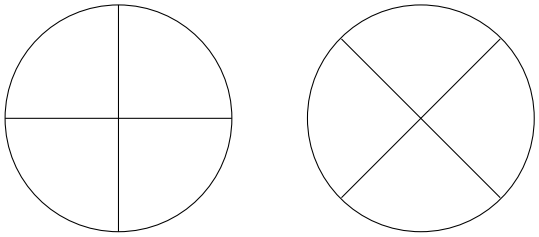

Abbildung 1.1: Die beiden Orientierungen bzw. Basissysteme für die Präparations- bzw. Messanordnungen beim BB84-Protokoll. (links) horizontal-vertikal (h/v-Basis), (rechts) $+45°$-$-45°$ ($+/-$-Basis).

bezüglich einer $+45°$-$-45°$ diagonalen Orientierung (siehe Abb. 1.1). Wenn im Folgenden von Orientierung die Rede ist, bezieht sich dies immer auf die Wahl eines orthogonalen Basissystems. Für jede Orientierung gibt es dann zwei mögliche Basiszustände bzw. Polarisationszustände.

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 Polarisationszustände 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, oft mit BBO abgekürzt), 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.

Diese Folge von Einzelphotonen schickt Alice an Bob. Sie hat dabei für jedes einzelne dieser Photonen folgende Information, die sie zunächst 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. 1.1.

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	$+/-$	$+/-$	$+/-$
Zustand	$+$	$-$	h	$+$	h	h	h	$-$	$+$	h	$+$	$+$	$-$
Bit	1	0	0	1	0	0	0	0	1	0	1	1	0

Tabelle 1.1: Tabelle von Alice. Diese Tabelle enthält die Polarisationszustände der Photonen, die Alice an Bob verschickt.

1.2.3 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, d.h. die Orientierung seines Polarisationsstrahlteilers, 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 mit dem Ergebnis von Alice überein. In allen anderen Fällen 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. 1.2).

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	$+/-$
Zustand	v	$-$	h	h	$+$	$-$	h	h	$+$	h	h	v	$-$
Bit	1	0	0	0	1	0	0	0	1	0	0	1	0

Tabelle 1.2: Tabelle von Bob. Sie enthält die Polarisationszustände, die Bob an den Photonen von Alice gemessen hat. Stimmt die gewählte Basis mit der von Alice überein (die Nummer der zugehörigen Photonen wurde unterstrichen), sind die Ergebnisse gleich, andernfalls sind sie zufällig.

1.2.4 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 (offenen) Kanal die Polarisationsbasen (also die Orientierungen), die sie jeweils für ihre Photonen bewählt haben. In ungefähr der Hälfte der Photonen werden diese Orientierungen gleich 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 gewählen 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 (sie wurden in Tabelle 1.2 unterstrichen). 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 als Schlüssel verwenden.

1.2.5 Eve

Da ein möglicher Lauscher nur in die Übertragung von Photonen oder von 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. 1.3).

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.

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	$+/-$
Zustand	v	v	$-$	$+$	h	$-$	h	v	h	$-$	$+$	h	$-$
Bit	1	1	0	1	0	0	0	1	0	0	1	0	0

Tabelle 1.3: 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 (unterstrichene Photonenzahlen). Sie schickt Photonen in den von ihr bestimmten Zuständen an Bob. Das ist das Beste, was sie unter diesen Umständen machen kann. In rund der Hälfte der Fälle wird diese Basis mit der von Alice übereinstimmen. In den anderen Fällen verschickt sie die Photonen in einem anderen Polarisationszustand.

1.2.6 Überprüfung der Zufallsfolge

Der letzte Schritt, den Bob und Alice ausführen sollten, 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	$+/-$	$+/-$	$+/-$
Bit	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	$+/-$
Bit	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	$+/-$
Bit	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	$+/-$
Bit	1	1	0	0	1	0	0	1	1	1	0	0	0

Tabelle 1.4: Die gesamte Tabelle des BB84-Protokolls. Die erste Doppelzeile gibt die Basis und die Bits 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 1.4 enthält nochmals alle Resultate, die Alice, Bob und Eve erhalten haben, wobei bei Bob unterschieden wird, ob er die Photonen direkt 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 (offenen) 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 Photonenaustausch 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 in rund der Hälfte der Fälle das Bit bei Bob ein anderes sein als bei Alice. Ganz grob kann man also sagen, dass ungefähr ein Viertel der Bits, die Alice und Bob als gemeinsame Folge identifiziert haben, bei einem Eingriff von Eve andere Werte haben. Verwendet man einige Tausend Bits zur Verifikation des Schlüssels, sollte ein solcher Eingriff auffallen.

1.3 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, bei 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 lenkt. Bei manchen Aufbauten kann Alice ihr 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 Polarisation, 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 (und etwas abgeschwächt wird). In diesem Fall würfelt er 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, da sich dann herausstellt, dass die Orientierungen verschieden gewählt waren.

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 würfelt 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 würfelt ein Bit. Sie schickt nun Laserlicht mit der Basis und Polarisation an Bob, die sie verwendet bzw. 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. Sie könnte nun die richtige Basis wählen und die Photonen des Laserlichts mit der richtigen Polarisation weiterleiten. Lauscht sie später dem Vergleich der Basissysteme zwischen Alice und Bob kann sie ebenfalls den Schlüssel ermitteln. Mit Einzelphotonen kann Eve die richtige Basis 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 benötigt 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.

1.4 Fragen

Dieser Abschnitt enthält einige Fragen, die man zunächst selbst beantworten sollte. Sie eignen sich auch für die Diskussion in der Schule.

1. Weshalb sollte Bob die Orientierungen bei seinen Messungen zufällig wählen? Welche Gefahr besteht, wenn er für die Orientierungen beispielsweise abwechselnd h/v und $+/-$ wählt?

   Die Gefahr besteht darin, dass Eve diese Vorliebe von Bob kennt. In diesem Fall wählt sie dieselben Orientierungen bei den Messungen wie Bob. Wenn Alice und Bob später ihre gewählten Basissysteme vergleichen, erhalten sie dieselben Übereinstimmungen wie Alice und Eve. Bei den Photonen, bei denen die Orientierungen von Eve und Bob sich von denen von Alice unterscheden, können die Messwerte verschieden sein, doch diese Bits werden verworfen. Bei den Bits, die behalten werden, stimmen Eve, Bob und Alice überein. Alice und Bob werden also nicht bemerken, dass sie belauscht wurden.

2. Hat Eve einen Vorteil, wenn sie ihre Basiseinstellungen zufällig wählt, oder könnte sie auch durchweg immer die Basis h/v verwenden?

   Rein statistisch hat Eve keinen Vorteil, wenn sie die Basis zufällig wählt. Eine Regelmäßigkeit könnte jedoch auffallen: Wenn sie immer nur die Basis h/v wählt, sind die Bits in der h/v-Basis bei Alice und Bob und immer korrekt, wohingegen sie bei den Bits in der $+/-$-Basis Fehler feststellen werden. Getreu dem Grundsatz, dass man überhaupt keine Information über sich preisgeben soll, noch nicht einmal eine Vorliebe für Regelmäßigkeiten, sollte Eve ihre Basis eher zufällig wählen. Ein weiterer Grund ist, dass immer wieder Fehler in der Übertragung auftreten werden. Mit solchen Fehlern müssen Alice und Bob rechnen. Falls also einige wenige Bits nicht übereinstimmen, kann es auch an solchen Fehlern liegen. In einem solchen Fall ist es für Eve günstiger, wenn sie keine Regelmäßigkeiten in ihren Basiseinstellungen gewählt hat, weil Alice und Bob dann eher glauben werden, dass die Unstimmigkeiten auf einer fehlerhaften

Übertragung beruhen. Das gilt aber nur, wenn Alice und Bob nicht ausreichend viele Bits als Test vergleichen.

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).

Index