Fortgeschrittenen-Praktikum
an der Humboldt-Universität zu Berlin

Quantenkryptographie

Friedemann Gädeke, Ronny Möbius

Inhaltsverzeichnis

1. Einführung

Kryptographie wird heute in vielen Bereichen des Alltagslebens eingesetzt (z. B. Online-Banking, E-Mail). Bei vielen Anwendungen ist es nicht möglich, einen Schlüssel zum Kodieren der Daten persönlich (also auf abhörsicherem Wege) auszuhandeln. Aus diesem Grund muss der Schlüssel genauso wie die Daten über eine unsichere Datenleitung übertragen werden. Dieses Problem wird zur Zeit fast immer mit dem RSA-Verfahren gelöst. Bei diesem wird ein privater und ein öffentlicher Schlüssel erzeugt, wobei der öffentliche Schlüssel zum Verschlüsseln der Daten und der private Schlüssel zum Entschlüsseln verwendet wird. Die beiden Schlüssel müssen eine mathematische Abhängigkeit zueinander besitzen. Dabei muss der öffentliche Schlüssel mit geringem Rechenaufwand aus dem privaten erzeugt werden können, der private darf aber nur mit sehr hohem Aufwand (viele Jahrhunderte Rechenzeit) aus dem öffentlichen berechnet werden können. Beim RSA-Verfahren wird dafür die Tatsache ausgenutzt, dass bisher kein Alghoritmus umsetzbar war, mit dem Primzahlzerlegungen schneller als mit exponentiell anwachsender Rechenleistung bei Vergrößerung der zu zerlegenden Zahl berechnet werden können. Mit der Entwicklung der Quantencomputer wird es in naher Zukunft neue Algorithmen geben, mit denen die Primzahlzerlegungen viel schneller möglich werden. Deswegen braucht man dann eine andere Methode, um den Schlüssel für die sichere Datenverbindung auszuhandeln.

Die Quantenkryptographie erfüllt die Anforderung, einen Schlüssel absolut abhörsicher zwischen zwei Stellen auszuhandeln. Dafür wird die physikalische Tatsache ausgenutzt, dass einzelne Photonen nicht kopierbar sind („No Cloning-Theorem“). In diesem Versuch wird das bekannteste Protokoll BB84 verwendet. Bei diesem sendet der Sender („Alice“) Photonen mit verschiedenen Polarisationen. Es werden vier verschiedene Polarisationen so verwendet, dass zwei Basen mit je zwei Zuständen entstehen. Die Basen müssen orthogonale Basen sein. Außerdem muss die Projektion von Zuständen aus verschiedenen Basen gleich sein, damit beim Abhören aus der Intensität bei falscher Basiswahl keine Rückschlüsse auf den Schlüssel gezogen werden können. Als erste Basis verwendet man z. B. zwei orthogonale lineare Polarisationen und als 2. Basis zwei orthogonale lineare Polarisationen, die gegen die 1. Basis um 45° gedreht sind. Die Basen und Projektionen untereinander sehen dann wie folgt aus:
1. Basis: $0° : |\rightarrow\rangle$, $90° : |\uparrow\rangle$
2. Basis: $45° : |\nwarrow\rangle$, $135° : |\nearrow\rangle$

$$\langle\rightarrow|\rightarrow\rangle = \langle\uparrow|\uparrow\rangle = 1$$
$$\langle\rightarrow|\uparrow\rangle = \langle\uparrow|\rightarrow\rangle = 0$$
$$\langle\nwarrow|\nwarrow\rangle = \langle\nearrow|\nearrow\rangle = 1$$
$$\langle\nwarrow|\nearrow\rangle = \langle\nearrow|\nwarrow\rangle = 0$$
$$|\langle\rightarrow|\nwarrow\rangle|^2 = |\langle\rightarrow|\nwarrow\rangle|^2 = |\langle\uparrow|\nwarrow\rangle|^2 = |\langle\uparrow|\nearrow\rangle|^2 = \frac{1}{2}$$

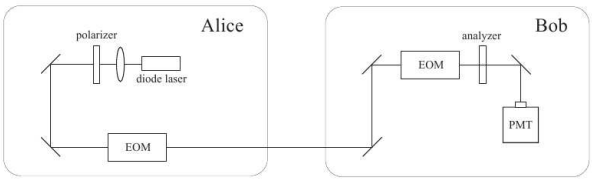

Abbildung 1: Schematische Darstellung des Versuchsaufbaus

In jeder Basis wir nun ein Zustand für eine logische 0 und eine logische 1 definiert. Für die Aushandlung des Schlüssels passiert nun folgendes: Alice erzeugt einen ausreichend langen zufälligen binären Schlüssel. Sie sendet nun Photonen an den Empfänger („Bob“), deren Polarisation durch den Schlüssel und eine zufällige Basiswahl vorgegeben wird. Bob projiziert nun die ankommenden Photonen ebenfalls in einer zufälligen Basis und bestimmt aus der Intensität den logischen Wert. Anschließend wird öffentlich die Basiswahl von Alice und Bob ausgetauscht, und beide Seiten verwerfen alle Bits im Schlüssel, bei denen Alice und Bob verschiedene Basen verwendet hatten. Falls es nun keine Fehler bei der Detektion bei Bob gab und auch kein Abhörer versucht hat, die Photonen zu messen, haben Alice und Bob den gleichen Schlüssel.

Ein Abhörer („Eve“) kann keine vollständige Kenntnis über den Schlüssel erlangen. Eve kann nämlich auch nur in zufälligen Basen messen und erfährt erst im Nachhinein, welche der Messungen verwendet werden. Überall dort, wo sie zufällig in der falschen Basis gemessen hat, ist aus der Intensität der logische Wert nicht mehr erkennbar. Die Sicherheit wird erhöht, indem die verworfenen Bits öffentlich ausgetauscht und verglichen werden. Falls sie nicht übereinstimmen, kann der Schlüssel verworfen werden und Eve wird aufgedeckt. (s. [Lohse]).

Weitere Informationen zum Versuch finden sich in der [Versuchsanleitung].

2. Versuchsaufbau

Der Aufbau besteht aus dem Sender (Alice) und dem Empfänger (Bob). Beide benutzen ein EOM (Electro-Optic-Modulator) und einen Polarisationsfilter. Mit dem EOM kann durch Anlegen von verschiedenen Spannungen eine $\lambda/4$- oder $\lambda/2$-Platte erzeugt werden. Zusammen mit dem linearen Polarisationsfilter kann Alice das Licht aus ihrem Laser linear und zirkular jeweils in zwei orthogonalen Zuständen senden. Bob kann mit dem umgekehrten Aufbau, aber mit Photodiode (APD) statt Laser, das zirkular und linear polarisierte Licht durch Intensitätsmessung an der Photodiode bestimmen. Die Photodiode war eine Avalache Photo Diode (APD), die bereits bei einzelnen Photonen einen Signalpuls auslöst. Es wurde ein roter Laser mit $\lambda = 633\,\mathrm{nm}$ und einer Leistung von $5\,\mathrm{mW}$ eingesetzt. Der Laser hatte einen stark divergenten Strahl, so dass nicht die ganze Intensität durch den Aufbau kam. Der Laser konnte kontinuierlich abstrahlen oder über einen Signalgenerator (Rechteck) zu Pulsen mit $10\,\mathrm{ns}$ Länge angeregt werden. Hinter dem Laser gab es die Möglichkeit, Filter zum Abschwächen einzubauen. Es wurde keine echte Einzelphotonenquelle verwendet, da die Entwicklung dieser noch nicht weit genug vorangeschritten ist. Um

doch Einzelphotonen zu verwenden, wurde die Intensität des Lasers so weit abgeschwächt, dass nur in etwa 1/1000 der Pulse mehr als ein Photon existierte. Die nötige Abschwächung bestimmen wir im folgenden Kapitel.

3. Bestimmung der Laserintensität

Um mit dem einfachen roten Laser ($\lambda = 633$ nm, $P = 5$ mW), der mit $t_{Puls} = 10$ ns langen Pulsen betrieben wird, Einzelphotonen zu erhalten, wird der Einfachheit halber eine solche Dämpfung vorgenommen, dass sich in einem Puls nach Poisson-Statistik nur noch mit einer Wahrscheinlichkeit von 0.1 % mehr als ein Photon befindet. Zunächst bestimmen wir mit der Poisson-Verteilung den Erwartungswert x für die mittlere Anzahl der Photonen in einem Puls. Die Wahrscheinlichkeit für eine bestimmte Anzahl N Photonen pro Puls ist nach der Poisson-Verteilung

$$P_x(N) = \frac{x^N}{N!}\, e^{-x} \ , \qquad x > 0.$$

Die zu lösende Gleichung ist nun

$$\begin{aligned} P_x(N=0) + P_x(N=1) &= 1 - 0.001 \\ \Rightarrow e^{-x} + x\ e^{-x} &= 0.999 = (1+x)\ e^{-x} \end{aligned}$$

Das verwendete x muss dann kleiner oder gleich sein als das aus dieser Gleichung folgende. Die Gleichung lässt sich algebraisch nicht lösen. Numerisch ergeben sich zwei Lösungen, wobei die positive Lösung

$$x = 0.0454$$

ergibt. Das bedeutet, dass etwa in jedem 20. Puls ein Photon anzutreffen ist. Mit einer echten Einzelphotonenquelle wäre hier ein deutlicher Intensitätszuwachs möglich.

Die Energie eines Photons ist

$$E = h\nu = h\frac{c}{\lambda} = 3.13 \cdot 10^{-19}\,\mathrm{J}.$$

Die Energie in einem Puls ist dann

$$E_{Puls} = x \cdot E = 1.425 \cdot 10^{-20}\,\mathrm{J}.$$

Die Leistung, mit der Alice senden muss, ergibt sich dann zu

$$P_{Alice} = \frac{E_{Puls}}{t_{Puls}} = 1.425 \cdot 10^{-10}\,\mathrm{W}.$$

Um diese Leistung einstellen zu können, benutzen wir die bekannte Leistung des Lasers von $P_{Laser} = 5$ mW und messen sie mit dem Power-Meter, das uns eine zur Leistung proportionale Spannung anzeigt. Dann messen wir die Leistung hinter Alice, ohne einen Filter einzubauen. Diese ist wesentlich kleiner als die

des Lasers, da im Aufbau von Alice bereits starke Verluste auftreten. Wir haben gemessen:

$$U_{Laser} = 748\,\mathrm{mV} \text{ bei } 10\mathrm{V}/100\ \mu\mathrm{A}$$
$$U_{Alice} = 1.63\,\mathrm{V} \text{ bei } 10\mathrm{V}/100\ \mathrm{nA}.$$

Daraus ergibt sich die Leistung von Alice ohne Abschwächung zu

$$P_{Alice,OD0} = 11\,\mu\mathrm{W}.$$

Die Abschwächung (Optical Density: OD), die für die Einzelphotonen gebraucht wird, ist dann

$$\log_{10} \frac{P_{Alice,OD0}}{P_{Alice}} = 4.895.$$

Es muss also mindestens der OD5-Filter verwendet werden.

4. Auswahl der Basiszustände

Im BB84-Protokoll werden für die beiden verwendeten Basen zwei um 45° gegeneinander verdrehte, linear polarisierte Basen für die Übermittlung der Photonen gewählt. Um die entsprechenden Zustände herzustellen, bräuchten wir zwei weitere EOMs, weshalb im folgenden gezeigt werden soll, dass die vier Zustände $|\rightarrow\rangle$, $|\uparrow\rangle$ sowie deren Superpositionen

$$\begin{aligned} |\circlearrowright\rangle &= \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle + i|\uparrow\rangle\right) \text{ sowie} \\ |\circlearrowleft\rangle &= \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle - i|\uparrow\rangle\right) \end{aligned}$$

denselben Anforderungen genügen:

$$\begin{aligned} \langle\circlearrowright\,|\,\circlearrowright\rangle &= \frac{1}{2}\left[(\langle\rightarrow| - i\langle\uparrow|)(|\rightarrow\rangle + i|\uparrow\rangle)\right] \\ &= \frac{1}{2}[1 + 0 + 0 - i^2] = 1 \end{aligned}$$

und völlig analog: $\langle\circlearrowleft\,|\,\circlearrowleft\rangle = 1$, sowie

$$\begin{aligned} \langle\circlearrowright\,|\,\circlearrowleft\rangle &= \frac{1}{2}\left[(\langle\rightarrow| - i\langle\uparrow|)(|\rightarrow\rangle - i|\uparrow\rangle)\right] \\ &= \frac{1}{2}[1 + 0 + 0 + i^2] = 0 \end{aligned}$$

Damit ist die Orthonormalität der zweiten Basis gezeigt. Weiterhin haben die Zustände untereinander gleichlange Projektionen:

$$\begin{aligned} \langle\rightarrow\,|\,\circlearrowright\rangle &= \frac{1}{\sqrt{2}} \Leftrightarrow |\langle\rightarrow\,|\,\circlearrowright\rangle|^2 = \frac{1}{2} \\ \langle\leftarrow\,|\,\circlearrowright\rangle &= i\frac{1}{\sqrt{2}} \Leftrightarrow |\langle\leftarrow\,|\,\circlearrowright\rangle|^2 = \frac{1}{2} \end{aligned}$$

und so weiter. Diese 4 Basiszustände können also genauso gut verwendet werden.

5. Einstellung der Basiszustände

Die EOMs bestehen hauptsächlich aus einem Kristall ("Verzögerungsplatte"), der abhängig von einer angelegten Spannung die Polarisation elektromagnetischer Strahlung verdreht. Zusammen mit einem (festen) Polarisationsfilter kann also ein Photon auf einen gewünschten Zustand projiziert werden.

Damit Alice und Bob in den gleichen Basen messen können, müssen die anzulegenden Spannungen bei Alice und Bob ermittelt werden. Hierfür verwenden wir noch konstantes, unabgeschwächtes Laserlicht. Zunächst haben wir nur das EOM von Alice eingestellt. Als Erstes haben wir einen vertikalen Polarisationsfilter vor und einen hinter das EOM gesetzt. Mit dem Filter vor dem EOM wird das Laserlicht in vertikale Richtung projiziert, im EOM gedreht und mit dem Filter dahinter wird der Anteil vertikal polarisierenden Lichtes herausgefiltert. Mithilfe der diskreten Spannungseinstellungen (im folgenden K) in LabView können wir nun die Intensität hinter dem zweiten Filter in Abhängigkeit der Verschiebung im EOM ermitteln, wobei wir die Intensität mit einer Photodiode messen, deren Signal wir mit einem Digitaloszilloskop beobachten.

Wenn das EOM die Polarisation gar nicht dreht, erwarten wir an der Photodiode ein maximales Signal, weil dann (im Idealfall) das Licht ungefiltert durch das EOM gelangt. Ist das EOM auf eine Verschiebung um $\lambda/2$ eingestellt (d.h. es dreht die Polarisation um π, so dass horizontal polarisiertes Licht entsteht), sollte im Idealfall keine Intensität mehr an der Photodiode zu messen sein, da der zweite Polarisationsfilter nur vertikal polarisiertes Licht hindurch lässt (im Realfall wird natürlich dennoch etwas gemessen, da Umgebungs- und Streulicht vorhanden ist). Dazwischen wirkt der Kristall im EOM als $\lambda/4$-Plättchen, erzeugt also oben definierte, zirkular polarisierte Zustände. Wie wir bereits gezeigt haben, ist dann die Intensität der Projektion auf einen Zustand vertikaler Polarisation gerade $1/2$ der maximalen Intensität, so dass wir noch zwei Spannungseinstellungen finden können, mit denen am Oszillotor gerade ein Signal zwischen den oben gemessenen Extrema zu beobachten ist. Wann das Licht nun rechts und wann links zirkular polarisiert ist, kann man an dieser Stelle nicht sagen. Wichtig jedoch ist nur, die hier verwendete Festlegung den ganzen Versuch über zu verwenden.

Um die Zustände für Bobs EOM einzustellen, sind wir analog vorgegangen, haben allerdings Alices EOM auf oben ermittelte Zustände eingestellt und nur noch mittels der Minimal- und Maximal-Projektionen am Oszilloskop die Bob-Zustände gefunden. So kann sichergestellt werden, dass die links- und rechtszirkular polarisierten Zustände auf jeden Fall zueinander passen.

Eine Übersicht über die ermittelten Zustände sind in den Tab. 1 und 2 zu finden.

Signal [mV]	K	Zustand
548	230	$\lvert \rightarrow \rangle$
1630	105	$\lvert \uparrow \rangle$
1089	53	$\lvert \circlearrowright \rangle$
1089	159	$\lvert \circlearrowleft \rangle$

Tabelle 1: EOM-Zustände für Alice

Zustand Alice	Signal [mV]	K	Zustand Bob
$\langle \uparrow \rvert$	199	140	$\lvert \uparrow \rangle$
$\langle \uparrow \rvert$	74.5	41	$\lvert \rightarrow \rangle$
$\langle \circlearrowleft \rvert$	183	94	$\lvert \circlearrowleft \rangle$
$\langle \circlearrowleft \rvert$	64.5	193	$\lvert \circlearrowright \rangle$
$\langle \circlearrowright \rvert$	199	193	$\lvert \circlearrowright \rangle$
$\langle \circlearrowright \rvert$	80.3	94	$\lvert \circlearrowleft \rangle$

Tabelle 2: EOM-Zustände für Bob, die letzten beiden Zeilen sind sozusagen eine Probe

6. Untersuchung der Similarity

Bedeutung der Similarity LabView gibt nach jeder Schlüsselübertragung die Similarity aus, welche berechnet wird nach

$$\frac{\text{richtig detektierte Photonen}}{\text{gesendete Photonen}},$$

wobei hier nur Photonen gemeint sind, deren Zustand von Bob zufällig zur richtigen Basis gemessen wurden. Eine Liste von benutzten Basen kann Alice ja gefahrlos nach Schlüsselübertragung an Bob übermitteln.

Sofern durch Eve keine Zustände auf eine andere Basis projiziert werden, sollte diese bei idealem Messaufbau bei 100% liegen. Sobald jedoch durch die APD auch Untergrundereignisse detektiert werden, sinkt die Similarity, da Bob nicht mehr die von Alice verschickten Zustände misst. Ein zweiter wichtiger Faktor ist die Ungenauigkeit bei der Einstellung der Eigenzustände, auf die die EOMs projizieren sollen. Die Genauigkeit der statischen Polarisationsfilter, insbesondere ihre Einstellung zueinander kann auch dazu führen, dass Bob nicht die von Alice gesendeten Zustände misst.

Sobald Eve spioniert, sinkt die Similarity schlagartig um mind. 25%, da Eve statistisch gesehen in mind. 50% der Fälle in der falschen Basis misst, wenn sie weiß, in welchen Basen sie zu messen hat. Da in die Similarity nur die Bits eingehen, die Alice und Bob zufällig auf die gleiche Basis projiziert haben, geht Eves Neugier nur zu 25% in die Similarity ein.

Messung der Similarity Für eine sinnvolle Fehlerabschätzung haben wir die Similarity für gleiche Frequenz und Dämpfung immer sechsmal ($n = 6$) gemessen. Die Unsicherheit für einen Messpunkt x_i ergibt sich dann aus der Standardabweichung

$$\sigma = \sqrt{\sum_i \frac{(\bar{x_i} - x_i)^2}{n-1}}$$

geteilt durch $\sqrt{n}$ (siehe auch [Müller], S. 36). Diese Rechnungen haben wir mit OpenOffice durchgeführt. Bei der Messung der Similarity für die Dämpfung OD5.0 haben wir leider noch nicht bemerkt, wie stark die Ergebnisse streuen und nur einmal gemessen. Daher haben wir, ausgehend von den Unsicherheiten der anderen beiden Messreihen, hier für die relative Unsicherheit einfach ±4% angenommen.

Interpretation der Messungen In den Abbildungen 2 bis 5 sind einige Abhängigkeiten der Similarity von der Dämpfung und der Frequenz, in der Laserpulse geschickt werden, dargestellt. In allen Fällen lassen sie die Schlussfolgerung zu, dass wir von Eve abgehört worden.

Gehen wir jedoch davon aus, dass es an unserer experimentellen Anordnung liegt, wollen wir zumindest eine optimale Kombination von Dämpfung und Frequenz finden. Die Daten mit Funktionen zu beschreiben erscheint uns aussichtslos, da wir zu wenige Messdaten aufgenommen haben. Günstig wäre es gewesen, die Dämpfung genauer einzustellen.

Nichtsdestotrotz ist an den Diagrammen zu erkennen, dass die Similarity mit steigender Frequenz zunimmt und sich einem dämpfungsabhängigen Wert annähert. Für kleine Frequenzen nähert sie sich 50% an, was bedeutet, dass Bits nur noch zufälligerweise richtig detektiert werden.[1] Dies kann so interpretiert werden, dass es bei wenigen Pulsen relativ gesehen öfter vorkommt, dass die APD statt des Laserphotons ein Umgebungsphoton detektiert, welches keine Information von Alice mitbringt. Bei hohen Frequenzen kann dieser Effekt minimiert werden, das Problem der ungenau eingestellten Basiszustände bleibt aber erhalten.

Die reine Dämpfungsabhängigkeit ist in Abb. 5 dargestellt. Wir wollen nur die beiden Messreihen für 5 kHz und 10 kHz betrachten. Die drei Messpunkte legen nahe, dass eine kleine Dämpfung gut ist. Wir vermuten aber, dass die Similarity für kleinere Frequenzen auch wieder sinkt, da wir dann nur noch sehr selten Pakete mit einzelnen Photonen messen. Außerdem könnte uns dann Eve unbemerkt abhören. Weiterhin wäre die APD überlastet. Für die Dämpfung von $10^{-4.5}$ befand sich der LabView-Kontrollregler für die APD bereits im gelben Bereich. Um nicht eine Zerstörung der APD zu riskieren hätten wir also maximal noch eine Dämpfung von $10^{-0.2}$ herausnehmen können. Wir hatten aber leider nur $10^{-0.5}$-Dämpfungsplatten zur Verfügung. Eine Anpassung der Messungen erscheint uns als nicht sinnvoll, da wir zu wenige Messpunkte haben.

[1] diese Annäherung haben wir nicht wirklich gemessen, da bei diesen kleinen Frequenzen sehr lange Wartezeiten erforderlich sind, damit statistisch relevante Schlüssellängen erzeugt werden können. Allerdings erscheint es uns extrem unplausibel, dass kleinere Frequenzen zu einer Invertierung des Signals führen würden.

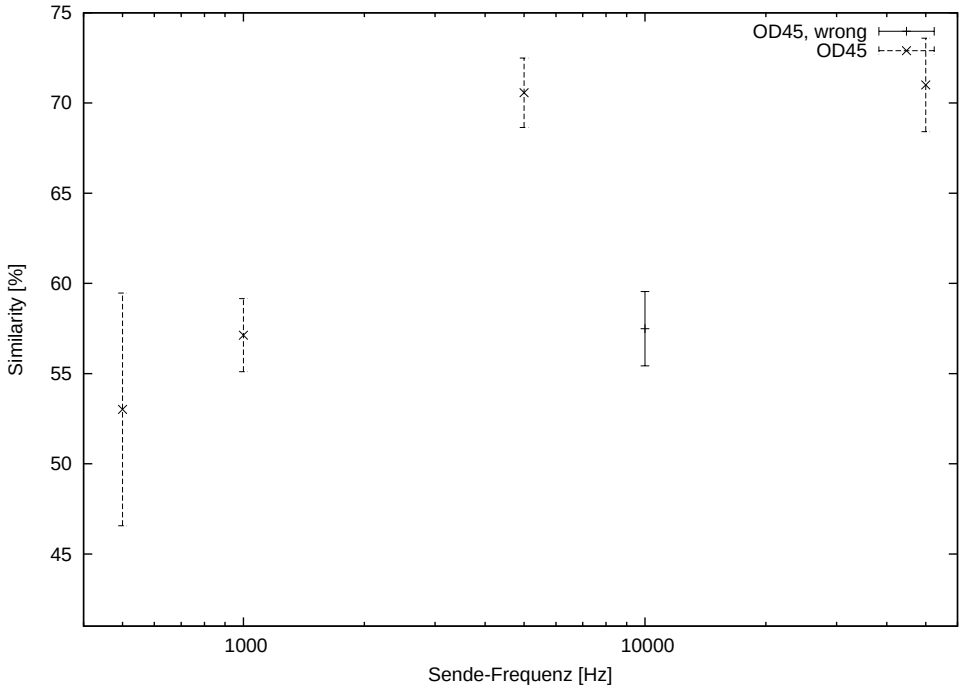

Abbildung 2: Similarity für OD4.5-Dämpfung. Den falschen Messwert haben wir versehentlich mit der falschen Frequenz in LabView gemessen.

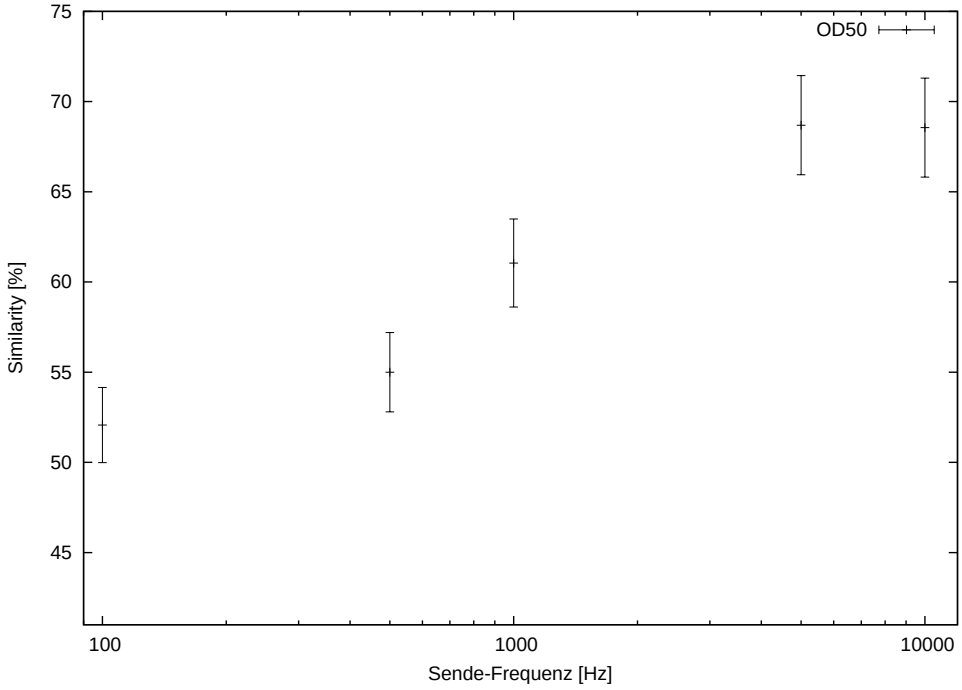

Abbildung 3: Similarity für OD5.0-Dämpfung.

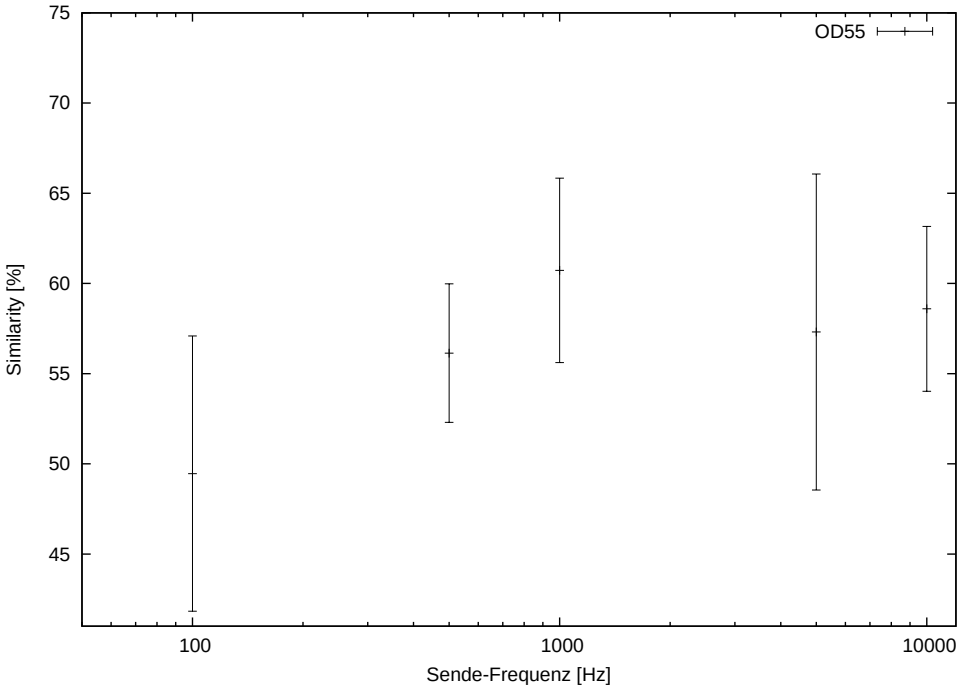

Abbildung 4: Similarity für OD5.5-Dämpfung

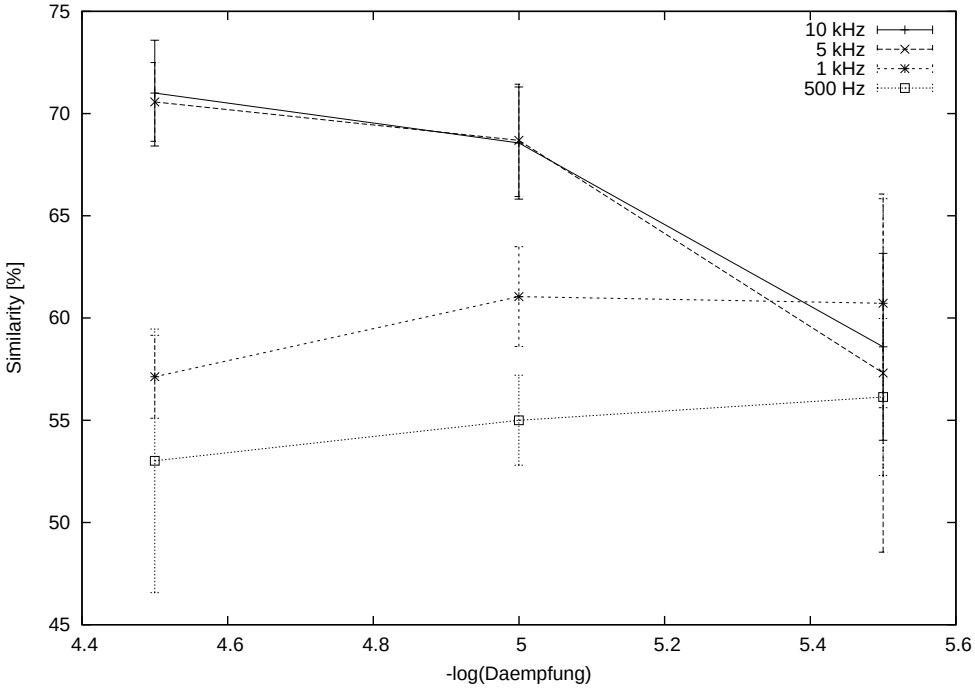

Abbildung 5: Similarity bei gleichen Frequenzen für versch. Dämpfungen

Entsprechend der Überlegungen im vorigen Absatz erwarten wir eine maximale Similarity nach der bei größerer Dämpfung die Similarity wieder abfällt.

7. Diskussion

Einfluss der Basiseinstellungen Nach der Einstellung der Basiszustände haben wir diese nochmal getestet, in dem wir die Intensitäten für alle möglichen "Skalarprodukte" gemessen haben. Schreibt man diese in eine Matrix ($:= A_{\text{exp}}$), ergibt sich folgendes:

$$U_0 \cdot \begin{pmatrix} \langle \circlearrowleft \mid \circlearrowleft \rangle & \langle \circlearrowleft \mid \uparrow \rangle & \langle \circlearrowleft \mid \circlearrowright \rangle & \langle \circlearrowleft \mid \rightarrow \rangle \\ \langle \uparrow \mid \circlearrowleft \rangle & \langle \uparrow \mid \uparrow \rangle & \langle \uparrow \mid \circlearrowright \rangle & \langle \uparrow \mid \rightarrow \rangle \\ \langle \circlearrowright \mid \circlearrowleft \rangle & \langle \circlearrowright \mid \uparrow \rangle & \langle \circlearrowright \mid \circlearrowright \rangle & \langle \circlearrowright \mid \rightarrow \rangle \\ \langle \rightarrow \mid \circlearrowleft \rangle & \langle \rightarrow \mid \uparrow \rangle & \langle \rightarrow \mid \circlearrowright \rangle & \langle \rightarrow \mid \rightarrow \rangle \end{pmatrix} = \begin{pmatrix} 191 & 126 & 70.5 & 126 \\ 163 & 208 & 136 & 80 \\ 84.3 & 148 & 197 & 126 \\ 104 & 58.8 & 128 & 173 \end{pmatrix} \text{ mV}$$

Im Idealfall sollte diese Matrix folgendermaßen aussehen:

$$U_o \cdot \begin{pmatrix} 1 & 0.5 & 0 & 0.5 \\ 0.5 & 1 & 0.5 & 0 \\ 0 & 0.5 & 1 & 0.5 \\ 0.5 & 0 & 0.5 & 1 \end{pmatrix} := A_{\text{ideal}}$$

Nimmt man vereinfacht ein konstantes Rauschen an, könnte man zunächst von der gesamten Matrix A_{exp} das kleinste Element (58.8 mV) abziehen. Es ergibt sich:

$$A_{\text{exp}} = \begin{pmatrix} 0.89 & 0.45 & 0.08 & 0.45 \\ 0.70 & 1.00 & 0.52 & 0.14 \\ 0.17 & 0.60 & 0.93 & 0.45 \\ 0.30 & 0.00 & 0.46 & 0.77 \end{pmatrix} \cdot 149.2\,\text{mV}$$

Hieran kann man leicht ablesen, welche Einstellungen nicht zueinander passen. Auffällig ist die schlechte Einstellung der vertikalen Polarisation. Die Ergebnisse könnten jedoch auch verfälscht sein durch Schwankungen des Umgebungslichtes und auch durch Schwankungen der Wärmestrahlung aufgrund möglicher Temperaturänderungen. Die eigentliche Übertragung mit sehr schwachen Laserpulsen wurde im Gegensatz zu dieser Messung mit einer einfachen Photodiode mit einer APD durchgeführt. Diese misst nur, wenn der Laser auch einen Puls schickt. Dadurch wird sicher ein Teil der Abweichungen in obiger Matrix vermieden.

weitere Einflüsse Anhand dieser Überprüfung der Zustandseinstellungen fragt sich, welche Grenzen das LabView-Steuerungsprogramm anlegt, um einen Zustand zu erkennen. Es ist davon auszugehen, dass es mitunter Zustände auch falsch erkennt. Dies können wir nicht quantifizieren. Daher wäre es besser, wenn mehr Informationen über die genaue Funktionsweise des LabView-Programms zur Verfügung stehen würden.

Weiterhin ist uns bei der Einstellung der Spannungen für die Verzögerungsplatte aufgefallen, dass im oberen Bereich der Regler (ab ca. 230) keine Veränderungen in der gemessenen Intensität mehr stattgefunden haben. Möglicherweise ist es daher nicht möglich die Platte über ihren vollen Funktionsbereich einzustellen um die optimalen Zustandseinstellungen zu finden.

Der Laserstrahl war nicht sehr gut kollimiert. Bereits nach dem ersten Spiegel war die räumliche Ausbreitung seines Lichtes sehr groß, so dass bereits dadurch einiges an Intensität verloren geht. Dies könnte zum Beispiel unerwünschte Reflexionen zur Folge haben, die Messfehler verursachen.

Schlussfolgerung Bei einer Similarity von 75% fragt sich, inwiefern ein Nutzen besteht. Praktisch alle Informationen, die man verschlüsselt übertragen möchte, sollen identisch beim Empfänger ankommen. Um dieses Problem zu umgehen, könnte man mit unterschiedlichen Schlüsseln dieselbe Information mehrfach übertragen. Auch ein intelligenter Selbstkonsistenzcheck der Daten wäre denkbar. Um so sicher zu sein, dass die Informationen mit einer sehr hohen Wahrscheinlichkeit auch korrekt sind, muss man allerdings sehr lange auf die Übertragung warten. Man darf weiterhin nicht vergessen, das für einen praktischen Nutzen die Entfernung von Alice und Bob deutlich größer sein muss.

Daher würde bei einer praktischen Realisierung sicherlich eine Einzelphotonenquelle eingesetzt. Weiterhin müssten die Basiszustände deutlich genauer eingestellt werden.

Literatur

[Versuchsanleitung] Matthias Scholz. Anleitung zum Versuch "Quantenkryptographie" im Fortgeschrittenen-Praktikum. Berlin 2007
`http://nano.physik.hu-berlin.de/lehre/f-praktikum/crypto.pdf`

[Lohse] Prof. Thomas Lohse. Folien zur experimentellen Quantenmechanik, Kapitel 6. Berlin 2009.
`http://eeh06.physik.hu-berlin.de/~lohse/physik_4/kap6.pdf`

[Müller] Uwe Müller. Einführung in die Messung, Auswertung und Darstellung experimenteller Ergebnisse in der Physik. Berlin 2005.
`http://gpr.physik.hu-berlin.de/Skripten/Einfuehrung/PDF-Datei/Einfuehrung.pdf`