Quantenkryptographie

Ein Freiraumexperiment zur Schlüsselerzeugung über 23,4 km

Zulassungsarbeit
für die erste Staatsprüfung
für das Lehramt an Gymnasien

eingereicht von
Matthäus Halder
im April 2002

durchgeführt an der
Ludwig-Maximilian-Universität München
am Lehrstuhl Hänsch
in der Arbeitsgruppe von
Prof. Dr. Harald Weinfurter

Inhaltsverzeichnis

1 Einleitung

Ob Geldautomaten, Datenbanken oder Onlineüberweisungen, ob Wirtschaftsgeheimnisse, Rüstungsfragen oder die Organisation von Terroranschlägen - überall dort wo es um Geheimhaltung und sicheren Informationsaustausch geht, spielt die Kryptographie eine wichtige Rolle. Die Sicherheit fast aller verwendeter Verschlüsselungsmethoden basiert auf der Schwierigkeit, mathematische Aufgaben in vernünftiger Zeit mit der heute gegebenen Rechenleistung zu lösen. Bei der augenblicklich verwendeten Verfahren sind allerdings Millionen von Jahren zur Entschlüsselung nötigt. Diese Methoden können also durchaus noch als *sicher* bezeichnet werden. Aber Computer werden immer schneller und leistungsfähiger. Sollte irgendwann einmal der Quantencomputer soweit entwickelt sein, daß man damit komplexere Aufgaben berechnen kann, so wären heute noch als kompliziert geltende mathematische Algorithmen kein großes Problem mehr.

Ein weiterer Schritt also in dem Wettlauf der Kryptologie, den sich Kryptographen und Kryptoanalytiker seit Erfindung ihrer Kunst liefern, wobei die Kryptographen immer wieder neue und sicherere Codierungsverfahren entwickeln, die daraufhin von den Kryptoanalytikern versucht werden zu brechen. Nun scheint es, als hätten die Analytiker mit dem Quantencomputer das Rennen für sich entschieden, doch kommt die Quantenphysik nicht nur ihnen zugute, sondern ebenso den Kryptographen. Auch sie können sich der Gesetze der Physik bedienen, um neue Verschlüsselungsmethoden zu entwickeln,die Quantenkryptographie. Diese gewährleistet uns erstmals eine absolut abhörsichere Methode der Kommunikation, so daß es den Anschein hat, als wären die Kryptographen die endgültigen Sieger dieses Wettlaufs.

Die vorliegende Arbeit soll ein Experiment beschreiben, bei dem eine Möglichkeit dieser abhörsicheren Kommunikation realisiert wurde. Es beginnt mit einem Einblick in die historische Entwicklung der Verschlüsselungstechniken, einigen Methoden der herkömmlichen Kryptographie und anschließend werden ein paar mögliche Verfahren der Quantenkryptographie vorgestellt. Eine Methode der Quantenkryptographie kommt auch in dem Experiment zum Einsatz, welches in seiner technischen Realisierung und Durchführung beschrieben wird. Den Schluß bildet eine Diskussion der erhaltenen Resultate mit einem Ausblick auf mögliche weitere Schritte.

Es sei vorweggenommen, daß es gelang, über 23,4 km einen absolut abhörsicheren kryptographischen Schlüssel auszutauschen, was im Augenblick für die Freiraumübertragung einen Bestwert darstellt.

2 Klassische Kryptographie

Kryptographie (*griechisch:* $\kappa\rho\upsilon\pi\tau o$: ich verberge, $\gamma\rho\alpha\varphi\varepsilon\iota\nu$: schreiben) bezeichnet die Verschlüsselung (Chiffrierung) von Information zur Datensicherung [1]. Sie bildet zusammen mit der Kryptoanalyse, den Techniken der unberechtigten Entschlüsselung (Dechiffrierung) dieser Daten, die Wissenschaft der Kryptologie, und ist etwa 3000 Jahre alt [2]. Betroffen sind in der Regel 3 Parteien: der Absender, der legitime Empfänger und ein Abhörer. Der Absender will dem Empfänger eine Nachricht, den Klartext, zukommen lassen, ohne daß er für einen Abhörer lesbar ist. Er chiffriert ihn daher so, daß man ihn nur wieder mit einem geeigneten Schlüssel decodieren kann. Gelingt es einem Angreifer, ohne den Schlüssel die codierte Nachricht zu entziffern, so gilt das Verfahren als *unsicher*, gelingt dies nicht, nennt man es *sicher* und kann man beweisen, daß es nie gelingen wird, so ist die Verschlüsselung *perfekt*. Dabei ist wichtig, daß ausschließlich Sender und Empfänger über die geeigneten Schlüssel verfügen.

Da das Verfahren, nach dem verschlüsselt wird, meist öffentlich bekannt ist, stellt die Schlüsselvereinbarung das eigentliche Problem dar. Schon im 19. Jahrhundert wurde von A. Kerkhoffs gefordert, daß die Sicherheit eines Verschlüsselungsverfahrens nur von der Geheimhaltung des Schlüssels, nicht jedoch von der Geheimhaltung des Algorithmus abhängen darf (*Kerkhoffs' Prinzip*) [3].

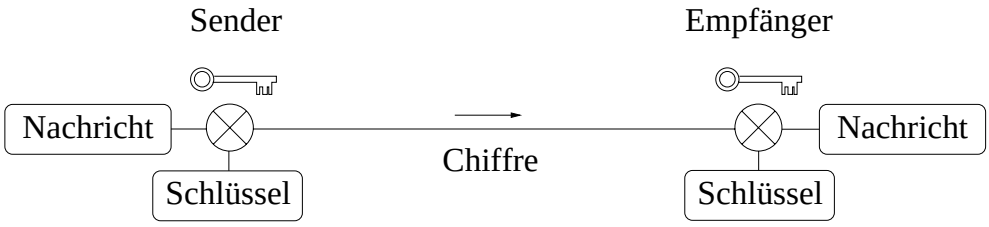


Abbildung 2.1: Um eine Nachricht abhörsicher auszutauschen, muß diese vom Absender verschlüsselt werden. Ebenso wie dieser verfügt auch der Empfänger über einen geeigneten Schlüssel, mit dem er den chiffrierten Text entziffern kann. Beide Parteien müssen entsprechend sichere Verfahren anwenden, um Nachricht und Schlüssel zu verknüpfen.

2.1 Verschiedene Methoden der Chiffrierung

Da die Kryptographie auf mathematischen Fundamenten basiert, bietet sie objektiv überprüfbare Sicherheit. Abgesehen davon, daß eine Nachricht immer erraten werden kann, gibt man als Maß für die Sicherheit meist die Wahrscheinlichkeit an, eine Lösung zu finden. Das sicherste der bekannten Verfahren ist der *Code nach Vernam* (siehe unten). Die meisten der heutzutage verwendeten Codierungen basieren jedoch auf anderen mathematischen Strukturen, deren Sicherheit skalierbar ist, wie etwa durch die Länge eines Schlüssels und der zur Verfügung stehenden Rechenleistung.

Im Folgenden werden einige solcher Methoden in chronologischer Reihenfolge erklärt.

2.1.1 Der Cäsar

Als einer der vielen Väter der Kryptographie gilt der römische Feldherr Gaius Julius Cäsar (100-44 v. Chr.) [1], der für die militärische Kommunikation mit seinen Legionen anstelle des natürlichen Klartextalphabets (KTA) ein Geheimtextalphabet (GTA) benutzte, in dem er die Buchstaben um einen bestimmten Wert verschob. Sei beispielsweise dieser Wert 3, so wird zur Verschlüsselung anstatt eines A ein D, statt eines B ein E, etc. geschrieben. Um den Text wieder zu entschlüsseln, notiert der Empfänger, dem das Geheimtextalphabet bekannt ist, anstelle eines D ein A und anstelle eines E ein B. Dieses Geheimtextalphabet wird durch eine Translation um 3 erhalten und beginnt demnach mit D.

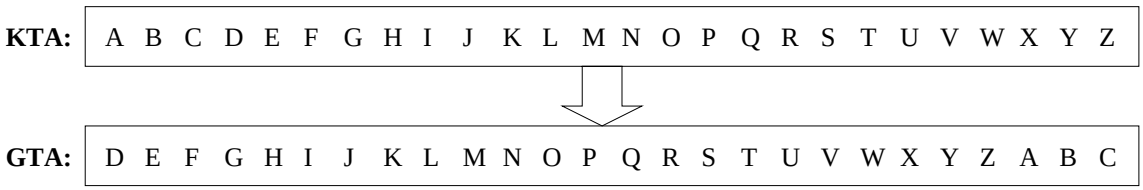


Abbildung 2.2: Cäsars geheimes Alphabet, das einer Translation um den Wert 3 entspricht und mit dem D beginnt.

Diesen Code zu erraten ist nicht schwer, da man höchstens 25 Möglichkeiten durchprobieren muß. Etwas schwieriger wird es, wenn man nicht mehr eine Translation, sondern irgendeine beliebige Permutation der Buchstaben vornimmt. Solche Codes nennt man *monoalphabetische Substitutionsalgorithmen.*

Sie bieten ebenfalls keine besonders große Sicherheit, da sie beispielsweise durch eine Analyse der einzelnen Buchstabenhäufigkeit zu entziffern sind. Bei diesem Werkzeug bedienen sich Kryptoanalytiker der Tatsache, daß die Buchstaben eines (beispielsweise deutschen) Textes nicht gleichverteilt sind. So tritt das “e“ mit 18% vor dem “n“ mit 11% und dem “i“ mit 8% am weitaus häufigsten auf und es lassen sich solche Geheimtexte schnell lösen, sobald sie eine gewisse Länge haben [2].

Schwieriger wird es für die Kryptoanalytiker schon, wenn man zu *polyalphabetischen Codes* wechselt. Die Buchstaben werden hierbei nicht mehr mit einem, sondern mehreren Geheimtextalphabeten im Wechsel verschlüsselt. Als Schlüssel kann ein einziges Wort dienen, wie etwa KOFFER, was bedeutet, daß der erste Buchstabe mit dem bei K startenden Translationsalphabet, der zweite mit dem bei O startenden etc. verschlüsselt wird, was sich beim 7., 14., .. Buchstaben wiederholt. Dieses Verfahren schlug u.a. Blaise de Vignére (1523-1585) vor [4], doch kann man besonders bei kurzen Schlüsselwörtern Muster in der Chiffre erkennen.

Der Verschlüsselungsalgorithmus bei allen solchen Verfahren ist eine Translation oder Permutation, der geheime Schlüssel im ersten Fall die Zahl 3 bzw. im zweiten Fall ein Codewort.

2.1.2 Die Chiffriermaschine Enigma

Nach dem gleichen Muster, jeden Buchstaben des Klartextes mit einem anderen Geheimtextalphabet zu codieren, funktioniert auch die von Arthur Scherbius entwickelte *elektromechanische Chiffriermaschine* Enigma. Diese wurde von den Deutschen im zweiten Weltkrieg zur verschlüsselten militärischen Kommunikation benutzt und dadurch Teil ihres Schicksals. Sie besteht aus drei drehbaren Walzen á 26 Positionen auf einer gemeinsamen Achse, wobei eine Walze nach einer vollständigen Umdrehung die nächste um einen Schritt mitnimmt, ähnlich einem Kilometerzähler. Mit jeder Position schließt sich von Walze zu Walze ein elektrischer Kontakt, der an einer vierten, festen Walze, der Umkehrwalze reflektiert wird und nocheinmal die anderen drei durchläuft. Jede dieser Walzen permutiert die Buchstaben nach einem anderen Muster, jenachdem, wie sie im Inneren verdrahtet ist, und auch ein Steckbrett zwischen Eingabetastatur und Walzen kann diese nochmals beliebig vertauschen . So erhält man eine ständig wechselnde Verschlüsselungsvorschrift [2]. Später wurde die Walzen noch durch austauschbare ergänzt. Nach $26^3 = 17576$ Schritten befinden sich die Walzen wieder in der ursprünglichen Position, welche ebenfalls mit einem Schlüsselwort frei gewählt werden kann. Aufgrund des Permutationsverfahrens, das sich aus der technischen Realisierung ergab, kann niemals ein Klartextbuchstabe in sich selbst überführt werden. Die Identität als Permutation ist also ausgeschlossen. Diesen wichtigen Fakt machten sich die Entzifferer zu Nutzen. Gleichen sich ein vermuteter Klartext und der Geheimtext in nur einem Buchstaben, so kann ausgeschlossen werden, daß es sich um diesen Klartext handelt und die Vermutung muß verworfen werden.

Daß deutsche U-Boot Soldaten sich bei der freien Wahl der Startposition stets für Frauennamen entschieden, hat den alliierten Kryptoanalytikern ihre Arbeit nicht gerade erschwert [5]. So gelang es der Gruppe um den englischen Mathematiker Alan Turing (1912-1954) in Bletchley Park den Enigma-Code zu entschlüsseln. An dieser großen Leistung, die erst 1975 öffentlich bekannt wurde, waren maßgeblich polnische Mathematiker beteiligt, allen voran Marian Rejewski (1905-1980). Zum ersten Mal wurde ein Code mit einer Rechenmaschine gelöst.

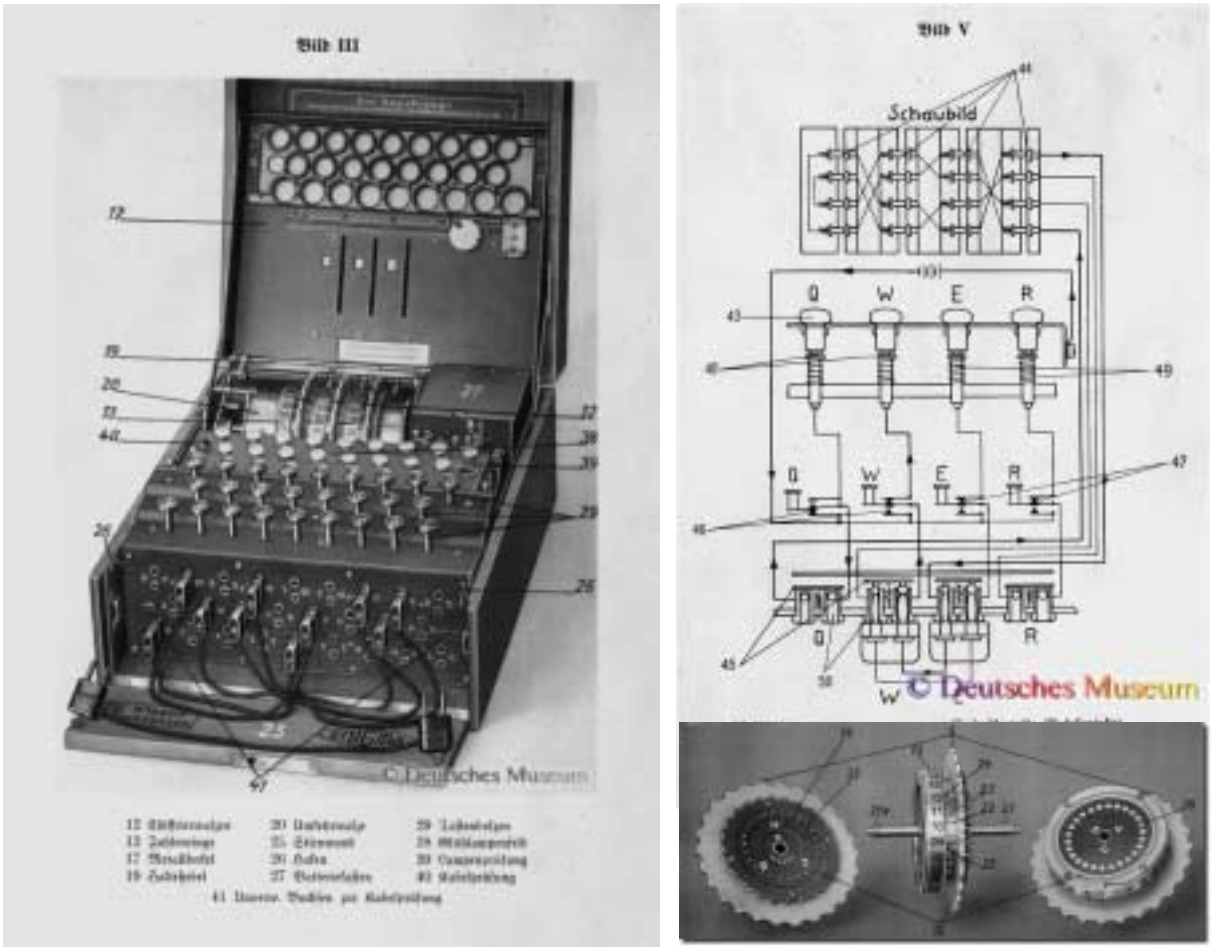


Abbildung 2.3: Die Enigma, Schaltplan und Walzen. 12 Chiffrierwalzen, 13 Zahlenringe, 17 Metalldeckel, 20 Umkehrwalze, 27 Batteriekasten, 38 Glühlampenfeld, 43 Glühlampen, 44 Chiffr. Walzen-Kontakte, 47 Tastkontakte, 48 Lampenkontakte

Zählte bis zu diesem Zeitpunkt die Kryptologie eher zu den linguistischen Wissenschaften, so war sie von nun an Bestandteil der Mathematik. [2] [4]

2.1.3 Der einzig sichere Code: Vernams One-time-pad

Aus den *Polyalphabetischen Substitutionsalgorithmen* läßt sich der bis heute einzige absolut sichere Code entwickeln, der *Vernam-Code* (1917), benannt nach dem Ingenieur G.S. Vernam [6]. Dabei wird anstelle des Schlüsselwortes eine zufällige Folge von Buchstaben verwendet, deren Länge der des Klartextes entspricht. Daraus ergibt sich aber schon der gravierendste Nachteil: Der Schlüssel. Jeder Buchstabe oder Bit des Nachrich-

tentextes wird mit einem anderen Buchstaben, bzw. Bit des Schlüssels codiert, wobei jeder Schlüsselbuchstabe/-bit nur ein einziges mal verwendet wird. Da der Schlüssel ausschließlich Sender und Empfänger bekannt sein darf, muß man, um eine Nachricht der Länge n geheim übertragen zu können, zuvor einen Schlüssel der Länge n geheim übertragen. Ist dies allerdings geschehen, so enthält die chiffrierte Nachricht keine Information mehr über den Klartext und ist somit für eine Analyse unbrauchbar. Die einzige Möglichkeit besteht im Erraten des Textes, wie es auch ohne Chiffre möglich ist.

Den Beweis zur Sicherheit dieses Verfahrens liefert Shannon mit einem Theorem [7], wonach für die Länge l des Schlüssels $l \geq n$ gelten muß.

Klartext:	u	m	8	i	m	k	i	n	o
ASCII−Text:	1110101	1101101	0111000	1101001	1101101	1101011	1101001	1101110	1101111
					⊕				
Schlüssel:	1001100	0011100	1101000	0101110	1001011	0010000	0011000	1111100	1010011
					=				
Chiffre:	0111001	1100001	0001100	1111110	1001000	0100011	1100101	1010001	1111100

Abbildung 2.4: Ein nach dem *Vernam-Code* mit einer XOR-Operation ($\oplus$) verschlüsselter ASCII-Text liefert eine Chiffre, die keinerlei für eine Kryptoanalyse nützliche Muster enthält. Eine Lösung kann nur erraten werden.

Dieses Verfahren wird nicht nur für Buchstaben, sondern auch für bits, wie beispielsweise in ASCII-Dateien, verwendet. Die Chiffre erhält man, indem auf den Klartext aus 0 und 1 eine XOR Operation mit dem ebenfalls aus bits bestehenden Schlüssel angewendet wird. Hier gilt: 1+1=0; 1+0=1; 0+1=1; 0+0=0. (Abb. 2.4)

Der Vernam-Code trägt auch den Namen *One-Time-Pad*, da wie bei einem Abreißblock, jedes Schlüsselbit nur einmal verwendet werden darf. Es ist der einzig bekannte Code, der beweisbare Sicherheit liefert und wir werden ihn später nocheinmal aufgreifen.

Nachdem der Revolutionär Ernesto Ché Guevara von Soldaten der bolivianischen Armee gefangengenommen und am 9.Oktober 1967 getötet wurde, fand man bei ihm ein Blatt Papier, auf dem er eine Nachricht an den kubanischen Präsidenten Fidel Castro chiffriert hatte. Er verwendete dabei das oben beschriebene Verfahren nach Vernam. Diese Nachricht konnte dann öffentlich, etwa mit einem Funkgerät, nach Kuba übertragen werden, da nur Castros Nachrichtendienst über den Schlüssel zur Dechiffrierung verfügte. [2]

Das beschriebene Verfahren gehört zur Klasse der sog. *Wurmchiffren*. Ähnliche wie diese funktionieren auch die *Stromchiffren*, nur daß letztere mit Pseudozufallszahlen anstelle von echten arbeiten, die mit einem mathematischen Algorithmus erzeugt werden. Das reduziert die Länge des Schlüssels, der zuvor auszutauschen ist, auf einen Bruchteil. Die kryptographische Sicherheit hängt hierbei von der Qualität des Pseudozufallszahlengenerators und der Länge der Pseudozufallszahlen ab.

2.2 Chiffren, wie man sie heute verwendet

2.2.1 Blockchiffren

1977 wurde bei IBM eine Methode entwickelt, deren Grundidee noch heute verwendet wird, der Data Encryption Standard (DES) [8]. Sie ist eine der bekanntesten *Blockchiffren*, die ihren Namen deshalb tragen, weil der Klartext in Blöcke einer bestimmten Länge aufgeteilt wird, die alle mit dem selben Schlüssel chiffriert werden. Jeder Block wird dabei in einen Block von gleicher Länge überführt. Die ursprüngliche Schlüssellänge von 128 bit wurde beim DES jedoch von der amerikanischen Geheimdienst-Behörde National Security Agency (NSA) auf 56 bit reduziert. Aufgrund der Codierungsvorschrift ist es nicht mehr möglich, den Klartext durch eine Häufigkeitsanalyse der Buchstaben zu rekonstruieren. So bleibt einem Abhörer die einzige Chance, den Schlüssel durch Probieren zu erraten, wobei der Aufwand exponentiell mit der Länge des Schlüssels zunimmt.

Dies gelang am 19. April 1999 innerhalb von 22 Stunden und 15 Minuten, indem 100.000 weltweit vernetzte PC alle möglichen Schlüssel durchprobierten, was allerdings keine Schwäche dieses Codes ist [9]. Ein solcher Angriff hätte bei allen Codierungsverfahren mit einem maximal 56-bit-Schlüssel funktioniert. Abhilfe wird hier durch einen längeren Schlüssel geschaffen oder durch mehrmaliges Anwenden des Verfahrens hintereinander. Daraus entwickelten sich der *Triple-DES*, der *Advanced Encryption Standard (AES)* [10] oder der *International Data Encryption Algorithm (IDEA)* [11], ebenfalls alles Blockchiffren, wie sie immer noch in Gebrauch sind.

Sämtliche bisher beschriebenen Chiffrierungen nennt man *symmetrische Algorithmen*, da die Entschlüsselungsfunktion die Inverse der Verschlüsselungsfunktion f ist und beide mit dem gleichen Schlüssel arbeiten. Oder, mathematisch notiert, mit Klartext k und Schlüssel s:

$$f^{-1}(f(k,s);s) = k$$

Sowohl Sender wie auch Empfänger benötigen dabei den Schlüssel, so daß dieser zuvor sicher übermittelt werden muß, ohne daß ihn ein Dritter erfährt.

Dieser Schlüsselaustausch ist allen bisher erwähnten Verfahren gemeinsam. In Fällen von höchster Sicherheit wird er beispielsweise von einem vertrauenswürdigen Kurier überbracht. Das macht diese Codes nicht besonders praktikabel und für die Kommunikation zwischen mehreren Personen wie in einem Netzwerk oft unbrauchbar. Hier müssen etwa n Parteien zuvor $\frac{n(n-1)}{2}$ Schlüssel abhörsicher untereinander austauschen.

Eine Lösung dieses organisatorisch aufwendigen Problems wird im folgenden Kapitel vorgestellt. Trotzalledem sind diese Codes sehr effizient und werden heute am meisten verwendeten.

2.2.2 Ohne geheimen Schlüsselaustausch: Public-Key Verfahren

Im Jahre 1976 wurde die Kryptographie erneut revolutioniert. Hatte man sich bis dahin damit abgefunden, daß verschlüsselte Kommunikation nur dann funktioniert, wenn zuvor schon einmal ein vertraulicher Kontakt stattgefunden hat, in dem ein gemeinsames Geheimnis, wie etwa ein Schlüssel vereinbart wird, so liefern W.Diffie und M.Hellman nun ein Gegenbeispiel [12]. Das war der Beginn der *asymmetrischen Chriffierverfahren*, bei denen nicht mehr mit ein und demselben Schlüssel ver- und entschlüsselt wird, sondern mit zwei verschiedenen.

Bei symmetrischen Verfahren ist die Operationen zur Ver- und Entschlüsselung etwa gleich aufwendig, wohingegen asymmetrische Verfahren sich in diesem Punkt unterscheiden. Sie benutzen zur Chiffrierung Operationen, die um einiges einfacher sind als ihre Inversen, die man zur Dechiffrierung benötigt. Beispielsweise ist die Faktorisierung einer Zahl viel aufwendiger als die Multiplikation ihrer Primfaktoren, was bei dem bekanntesten asymmetrischen Code, dem RSA-Code zur Anwendung kommt [13]. Zur Verschlüsselung einer Nachricht benutzt man den *öffentlichen Schlüssel*, die Multiplikation mit einer großen Zahl, ohne daß dabei der Absender oder irgendjemand anderes außer dem Empfänger deren Primfaktorenzerlegung kennt. Die Entschlüsselung kann aber nur gelingen, wenn man die Primfaktoren dieser Zahl weiß, also den *privaten Schlüssel* besitzt. Ein Empfänger stellt also seinen öffentlichen Schlüssel zur allgemeinen Verfügung, so daß jeder ihm eine codierte Nachricht schicken kann, die dann nur mit seinem geheimen privaten Schlüssel zu entziffern ist. Der interessierte Leser findet ein Beschreibung dieses Verfahrens im Glossar.

Nun ist es also möglich, daß fremde Personen eine geheime Botschaft abhörsicher austauschen können. Die Sicherheit dieses Verfahrens beruht darauf, daß ausreichend große Zahlen nicht mehr in einer sinnvollen Zeit faktorisiert werden können [14]. Zumindest gilt das für den augenblicklichen Stand der Technik. Verfolgt man den Zuwachs an Rechenleistung von Computern über die letzten Jahre oder Jahrzehnte, so stellt sich die Frage nach dem Zeitpunkt, an dem augenblickliche Chiffren nicht mehr in der Lage sind, ihre Geheimnisse zu schützen. Zwar läßt sich mit zunehmender Kapazität der Rechner einfach die Länge des Schlüssels erhöhen, doch stößt man noch auf ein anderes Problem, nämlich die Lebensdauer von Geheimnissen. So kann möglicherweise in einigen Jahrzehnten eine Chiffre aus heutiger Zeit von jederman gelesen werden. Dabei kann es sich aber durchaus noch um Informationen handeln, die auch dann noch als geheim gelten sollten.

Abgesehen von dem Faktor Zeit gibt es auch noch keinen Beweis, daß kein einfacherer Algorithmus zur Faktorisierung einer Zahl existiert. Somit können auch die Public-Key-Verfahren nicht als dauerhafte Lösung für kryptographische Kommunikation gelten.

3 Quantenkryptographie

Bis auf den *Vernam-Code* basieren sämtliche Codes auf algebraischen Algorithmen, die abhängig von der aufgewandten Rechenleistung und Zeit mehr oder minder schwer zu brechen sind. Nimmt man als Operation beispielsweise die Faktorisierung einer 400-stelligen Zahl, so bedeutet *schwer zu brechen*, daß die besten Hochleistungsrechner heute schätzungsweise 10 Milliarden Jahre bräuchten [2]. Mit der Entwicklung immer schnellerer Rechner ist das Faktorisieren von großen Zahlen immer einfacher. Der Rekord wurde vor kurzem erst mit Hilfe von 144 PCs (400 MHz-PentiumII) auf eine 158-stellige Dezimalzahl (525 bit) erhöht [15], und auf der anderen Seite ist auch schon mit einem Quantencomputer die Faktorisierung der Zahl $15 = 3 \cdot 5$ gelungen [16]. Für Quantencomputer existiert ein Algorithmus, dessen Anzahl an Rechenoperationen nur noch polynomial mit der Länge der Zahl und nicht mehr exponentiell zunimmt.

Die gängigen Codes sind damit aber im Augenblick noch nicht in Gefahr, doch müssen auch die Entwickler von Verschlüsselungstechniken über neue Verfahren nachdenken. Einen alternativen Ansatz bietet die Quantenkryptographie. Sie bedient sich physikalischer Gesetzmäßigkeiten, wie etwa der Heisenberg'schen Unschärferelation, um Sicherheit gewährleisten und sogar beweisen zu können. (Auf die dazu nötige Quantentheorie wird im Glossar näher eingegangen.)

Da bereits absolut sichere Codes, wie beispielsweise der nach Vernam, bekannt sind, ist das zentrale Problem der geheime und sichere Schlüsselaustausch. Für diesen Austausch bietet Quantenkryptographie eine Lösung, indem sie den vertrauenswürdigen Boten durch physikalische Gesetze ersetzt. Es handelt sich also nicht um eine Verschlüsselungstechnik, sondern um eine Methode der Schlüsselvereinbarung. Korrekterweise müßte man also von Quanten-Schlüsselaustausch sprechen, doch bleiben wir bei dem gebräuchlichen und hierfür eingebürgerten Begriff der Quantenkryptographie.

3.1 Mögliche Protokolle

Es gibt eine Vielzahl von Möglichkeiten, Quantenkryptographie praktisch zu implementieren. Die mögliche Kommunikation über einen sog. *Quantenkanal* wird erstmals von S. Wiesner [17] erwähnt. Im Folgenden werden drei wichtige Protokolle für einen Schlüsselaustausch vorgestellt, die sich allesamt des quantenoptischen Aspekts von Licht bedienen. Da in dem beschriebenen Experiment das sogenannte Protokoll BB84 verwendet

wird, sei dieses am ausführlichsten erklärt. Anschließend wird noch auf zwei weitere Verfahren eingegangen, wie sie teilweise von anderen Gruppen realisiert wurden.

Nach der allgemeinen Konvention in der Kryptographie, den Sender einer Botschaft Alice und den Empfänger Bob zu nennen, werden auch wir diese Namen hier benutzen.

3.1.1 Das BB84-Protokoll

Das nach seinen Entwicklern Charles H. Bennet und Gilles Brassard (1984) benannte Protokoll [18] überträgt die Quanten-Information mit Hilfe einzelner Photonen unterschiedlicher Polarisationsrichtungen. Der Sender, auch Alice genannt, schickt dem Empfänger Bob einzelne Photonen, um daraus in einer anschließenden Diskussion einen Schlüssel zu gewinnen. Die Verbindung, über die man Photonen sendet, wird *Quantenkanal* genannt und kann eine Glasfaser oder wie in unserem Fall eine Freiraumstrecke sein. Dieser Kanal wird in nur einer Richtung durchlaufen, wohingegen die anschließende Diskussion zwischen Alice und Bob in beide Richtungen über den *klassischen Kanal* stattfindet. Dazu kann man eine Telefonleitung, das Internet oder eine Funkstrecke benutzen, die öffentlich mitgehört, aber nicht manipuliert werden darf.

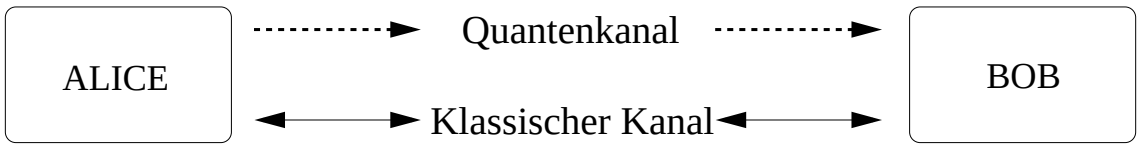


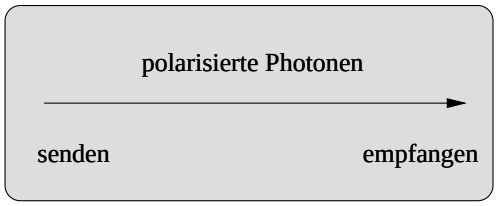
Abbildung 3.1: Nachdem Alice die Photonen über den Quantenkanal zu Bob geschickt hat kommunizieren sie über den klassischen Kanal in beiden Richtungen

Das Verfahren besteht aus mehreren Schritten. Zuerst übermittelt Alice einzelne Photonen zufällig in einer von 4 Polarisationsrichtungen an Bob, wobei zwei der Richtungen jeweils orthogonal zueinander sind. Idealerweise wählt man die Richtungen 0°, 45°, 90° und 135° (Kap. 5.1.3.) und nennt sie H für horizontal, +45°, V für vertikal bzw. -45°. H und V bilden eine Orthogonalbasis, *gerade* Basis genannt und +45° und -45° bilden eine zweite Basis, *schräge* Basis genannt. Alice notiert sich Zeitpunkt und Polarisationsrichtung der losgesandten Photonen. Beim Empfangen eines Photons entscheidet sich Bob wiederum zufällig, ob er dessen gerade oder schräge Polarisation messen will, also in welcher Basis er die Messung vornimmt. Er notiert sich ebenfalls Zeitpunkt und Ergebnis der Messung. So entsteht auf beiden Seiten eine Liste (Abb.3.2), die nun öffentlich verglichen wird.

In einem zweiten Schritt teilt Bob mit, wann er ein Photon empfangen und in welcher Basis er es gemessen hat, nicht aber, zu welchem Ergebnis er gekommen ist. Alice und Bob streichen daraufhin sämtliche Einträge aus ihren Listen, bei denen Bob kein Photon empfangen oder in der anderen Basis als Alice gemessen hat (Abb. 3.3).

ALICE

Nr.	Basis	Pol.	Bit
1	+/−	−45°	0
2	+/−	+45°	1
3	H/V	H	1
4	+/−	+45°	1
5	H/V	V	0
6	+/−	−45°	0
7	H/V	V	0
8	H/V	H	1
9	+/−	+45°	1
10	+/−	−45°	0
11	H/V	V	0
12	+/−	+45°	1
13	H/V	H	1
14	+/−	−45°	0
15	H/V	V	0
16	H/V	H	1
17	H/V	V	0
18	+/−	+45°	1
19	+/−	−45°	0
20	H/V	H	1
21	+/−	+45°	1
22	H/V	V	0
23	H/V	H	1
24	+/−	−45°	0
25	+/−	+45°	1
26	+/−	−45°	0
27	H/V	V	0
28	H/V	H	1
29	+/−	+45°	1
30	H/V	H	1
31	+/−	−45°	0
32	H/V	V	0



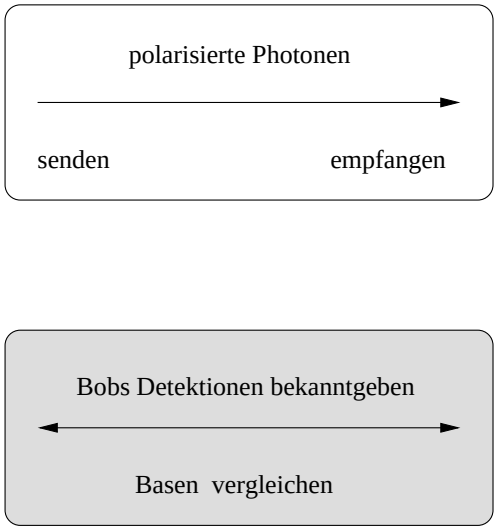
BOB

Nr.	Basis	Pol	Bit
1	+/−	−45°	0
2	+/−	x	x
3	H/V	H	1
4	+/−	+45°	1
5	H/V	x	x
6	H/V	V	0
7	+/−	+45°	1
8	H/V	V	0
9	H/V	V	0
10	+/−	x	x
11	H/V	V	0
12	H/V	x	x
13	+/−	+45°	1
14	H/V	x	x
15	+/−	x	x
16	H/V	H	1
17	H/V	x	x
18	+/−	+45°	1
19	H/V	H	1
20	+/−	x	x
21	H/V	x	x
22	+/−	x	x
23	+/−	−45°	0
24	+/−	x	x
25	H/V	H	1
26	H/V	x	x
27	+/−	−45°	0
28	H/V	x	x
29	+/−	−45°	0
30	+/−	x	x
31	+/−	−45°	0
32	H/V	V	0

Abbildung 3.2: 1. Schritt im BB84-Protokoll: Photonenaustausch. Alice sendet einzelne Photonen in zufällig einer der 4 Polarisationsrichtungen H, V, +45°, -45°. Bob analysiert diese zufällig in einer der beiden Basen H/V bzw. +/-45°. So entsteht auf beiden Seiten eine Liste mit Einträgen zur Uhrzeit, Basis und emittierter bzw. gemessener Polarisation. Ein x bedeutet, daß Bob kein Photon detektieren konnte.

ALICE

Nr.	Basis	Pol.	Bit
1	+/−	−45°	0
2	+/−	+45°	1
3	H/V	H	1
4	+/−	+45°	1
5	H/V	V	0
6	+/−	−45°	0
7	H/V	V	0
8	H/V	H	1
9	+/−	+45°	1
10	+/−	−45°	0
11	H/V	V	0
12	+/−	+45°	1
13	H/V	H	1
14	+/−	−45°	0
15	H/V	V	0
16	H/V	H	1
17	H/V	V	0
18	+/−	+45°	1
19	+/−	−45°	0
20	H/V	H	1
21	+/−	+45°	1
22	H/V	V	0
23	H/V	H	1
24	+/−	−45°	0
25	+/−	+45°	1
26	+/−	−45°	0
27	H/V	V	0
28	H/V	H	1
29	+/−	+45°	1
30	H/V	H	1
31	+/−	−45°	0
32	H/V	V	0



BOB

Nr.	Basis	Pol	Bit
1	+/−	−45°	0
2	+/−	x	x
3	H/V	H	1
4	+/−	+45°	1
5	H/V	x	x
6	H/V	V	0
7	+/−	+45°	0
8	H/V	V	0
9	H/V	V	1
10	+/−	x	x
11	H/V	V	0
12	H/V	x	x
13	+/−	+45°	1
14	H/V	x	x
15	+/−	x	x
16	H/V	H	1
17	H/V	x	x
18	+/−	+45°	1
19	H/V	H	0
20	+/−	x	x
21	H/V	x	x
22	+/−	x	x
23	+/−	−45°	1
24	+/−	x	x
25	H/V	H	1
26	H/V	x	x
27	+/−	−45°	0
28	H/V	x	x
29	+/−	−45°	9
30	+/−	x	x
31	+/−	−45°	0
32	H/V	V	0

Abbildung 3.3: 2. Schritt des BB84-Protokolls: Basenabgleich. Über den öffentlichen klassischen Kanal vergleichen Alice und Bob nun die Sende- und Empfangsbasis der Einträge und verwerfen diejenigen ohne Detektionen oder mit unterschiedlichen Basen. Die Resultate dieses sog. *Rohschlüssel* bleiben geheim und werden in bits übersetzt, wobei H und +45° einer logischen 1, V und -45° einer 0 entsprechen.

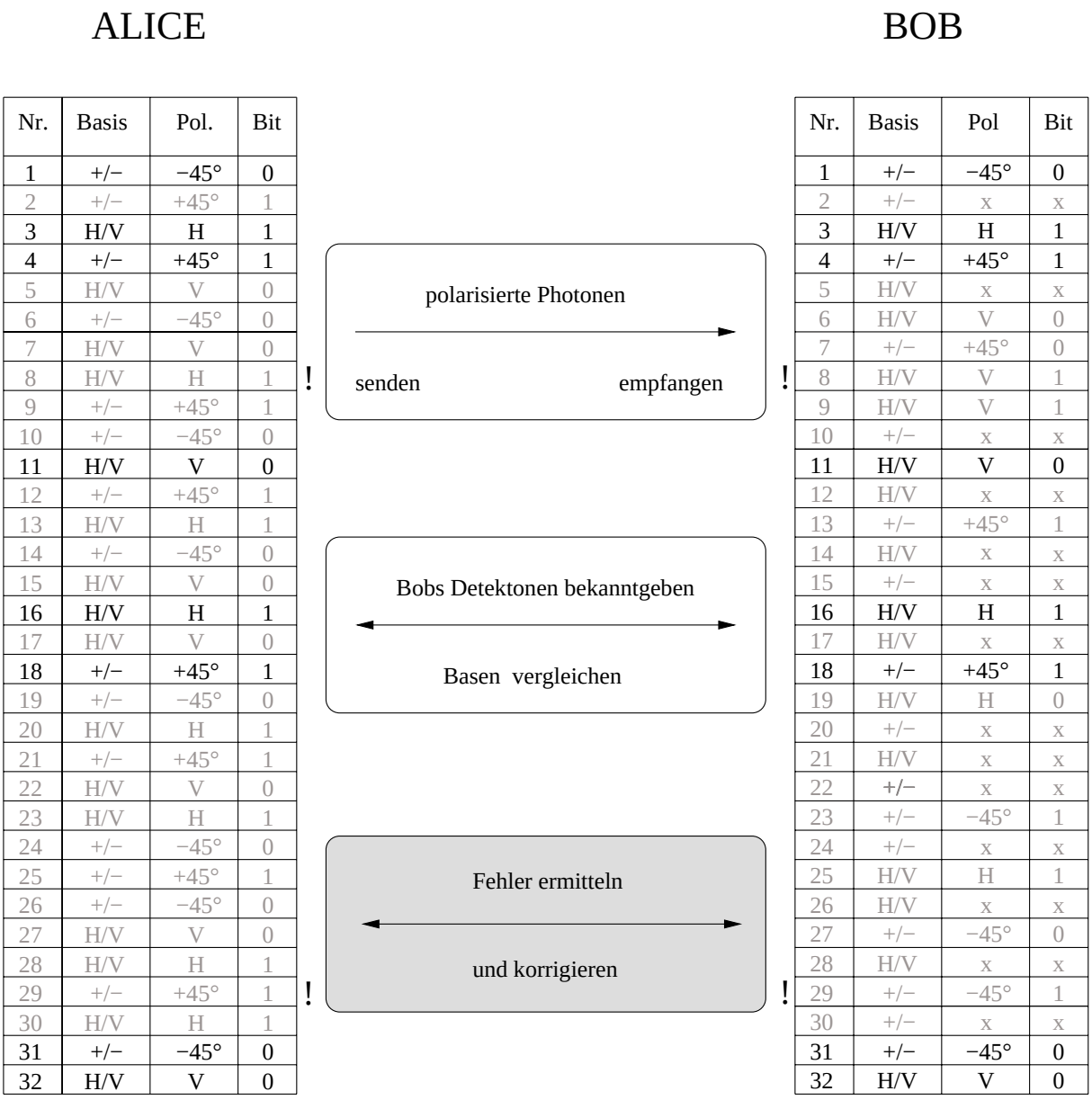


Abbildung 3.4: 3. Schritt des BB84-Protokolls: Fehlerkorrektur. Ein bestimmter Teil dieses Rohschlüssels wird veröffentlicht, um den enthaltenen Fehler feststellen und korrigieren zu können. Es bleibt der fertige und auf beiden Seiten identische Schlüssel. Mit diesem kann nun eine Nachricht chiffriert werden.

So wird die Hälfte der gemeinsamen Einträge verworfen, da sich Alice und Bob für unterschiedliche Sende- und Empfangsbasen entschieden haben. Die Polarisationen der

noch verbleibenden Einträge werden nun in bits übersetzt, wobei H und +45° einer logischen 1 und dementsprechend V und -45° einer logischen 0 entsprechen. Es liegt nun auf beiden Seiten die gleiche Bitfolge vor, die man den *Rohschlüssel* nennt. Diese Bitfolge kann jedoch Fehler enthalten, die es noch zu korrigieren gilt. Fehler in der Polarisation werden beispielsweise durch optische Komponenten, Justageungenauigkeiten oder einen Abhörer verursacht.

Eve, die Abhörerin

Einem potentiellen Abhörer kann, wie in der klassischen Kryptographie, zugestanden werden, den gesamten Aufbau und seine Funktionsweise zu kennen. Die Stärke der Quantenkryptographie ist aber, daß ein Abhörer auch über *alle* physikalisch möglichen Verfahren zur Manipulation des informationtragenden Photons verfügen darf.

Wird ein Photon in einem der Ausgänge eines Polarisators gefunden, so ist es in einem Zustand, der durch die Orientierung des Polarisators gegeben ist. Eine erneute Messung gibt keine zusätzliche Information mehr über den Zustand vor dem Polarisator.

Versucht eine dritte Person, Eve genannt (von *engl.: eavesdropping=heimlich zuhören*), die Schlüsselerzeugung abzuhören, so muß sie sich in den Quantenkanal einschalten und an den Photonen eine Messung vornehmen.

Eine der möglichen Abhörmethoden ist die folgende. Eve hat die gleichen Chancen wie Bob, für ein ankommendes Photon die zugehörige Eigenbasis korrekt zu wählen und somit die Polarisation richtig bestimmen zu können. Entscheidet sie sich für die falsche Basis, so erhält sie ein Ergebnis, das von der ursprünglichen Polarisation abweicht. Die Polarisation der weitergeschickten Photonen entspricht der von Eve analysierten.

In den Fällen, in denen sie die falsche Basis gewählt hat, wird sie auch eine falsche Polarisation weitergeben, und kann somit einen Fehler in der Bitfolge von Alice und Bob verursachen. Dieser Fehler wird von Alice und Bob in der anschließenden öffentlichen Diskussion entdeckt (Abb.3.4).

Sendet Alice beispielsweise ein V-polarisiertes Photon und entscheidet sich Eve aber, es in der +/-45° Basis zu messen, so erhält sie entweder das Ergebnis +45° oder -45°. (vergl. dazu Kap. 5.1.3.). Sie wird also entsprechend ihres Ergebnisses entweder ein +45° oder ein -45° polarisiertes Photon weitersenden. Mißt nun Bob wieder in der H/V-Basis, so detektiert er mit 50% Wahrscheinlichkeit eine H-Polarisation und somit ein von Alice' bit unterschiedliches Resultat. Dies ist bei 25% der Photonen der Fall.

Aufgrund dieses notwendigerweise verursachten Fehlers können Alice und Bob Rückschlüsse auf einen eventuellen Abhörer ziehen und den Schlüsselblock nicht verwenden, sondern einen erneuten Schlüsselaustausch versuchen.

Die Ungenauigkeit bei der Bestimmung der Polarisation, auch Ergebnisunschärfe genannt, ermöglicht es, die absolute Abhörsicherheit zu beweisen. Aufgrund der *Heisenberg'schen Unschärferelation* ist es unmöglich, zwei voneinander abhängige Größen eines Systems gleichzeitig exakt zu bestimmen. (Eine ausführliche Beschreibung folgt im Glossar.) In unserem System sind solche Größen die Polarisationsrichtungen in den un-

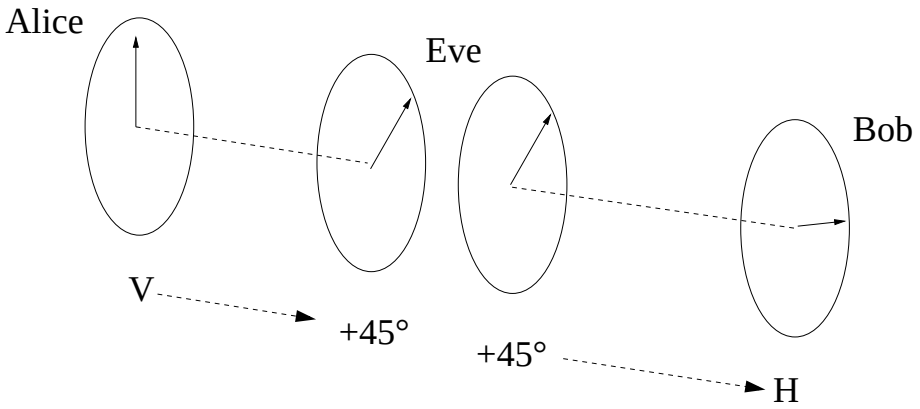


Abbildung 3.5: Eine Abhörerin wird in 25% aller Fälle einen Fehler erzeugen. Da sie in der falschen Basis mißt, dreht sie die Polarisationsrichtung um 45°, und Bob in der wiederum richtigen ebenso. Aus V (0) wird H (1).

terschiedlichen Basen H/V und +/-45°. Das heißt, die Polarisation eines Photons kann nicht gleichzeitig in beiden Basen exakt gemessen werden.

Ein abgehörtes Photon muß weitergegeben werden, wodurch eine Fehler von mindestens 25% erzeugt wird.

Eine andere Möglichkeit des Mithörens sind die sogenannten *decoherent attacks*, wie beispielsweise das Klonen eines Photons, wie etwa von Bužek und Hillery vorgeschlagen [19] [20]. Dabei wird das Photon "kopiert", eines behalten und das zweite weitergeschickt. Da eine Quanten-Klon-Maschine mit einer theoretischen Zuverlässigkeit von bestenfalls $\frac{5}{6}$ funktioniert, beträgt der dadurch erzeugt Fehler noch mindestens 16,6%. Auch durch *coherent attacks*, bei denen die Photonen nicht mehr einzeln, sondern als ganzes Ensemble abgefangen werden, wird noch ein Fehler von mindestens 11% verursacht [21]. Da für den zweiten Fall ein Quantencomputer benötigt wird, können coherent attacks zur Zeit noch außer Betracht gelassen werden. Es kann hier nicht näher auf die beiden letzten Methoden eingegangen werden, und der interessierte Leser sei auf die angegebenen Referenzen verwiesen. Zusammenfassend kann man feststellen, daß ein Abhörer stets einen Fehler von mindestens 11% verursacht, wenn er den gesamten Schlüssel mithört. Wird also ein Schlüssel mit einer geringeren QBER erzeugt, so ist sicher, daß keine dritte Person diesen vollständig kennt. Es gibt zwar noch andere Abhörmethoden, wie beispielsweise die Analyse der Software, der Sendeelektronik oder der Empfangsdioden (Kap.4.2.3.), doch betrachten wir hier Sender und Empfänger als nach außen abgeschlossene Einheiten.

Die Sicherheit ist allerdings nur gewährleistet, solange Alice einzelne Photonen emittiert. Sendet Alice mehr als ein Photon, so könnte Eve eines davon zur Analyse abgefangen und die restlichen unverändert passieren lassen, womit sie unbemerkt bliebe. Das abgefangene Photon wird aufbewahrt und erst dann gemessen, wenn Bob seine Meßbasis öffentlich bekannt gibt. Eve würde dadurch den gesamten Schlüssel erhalten.

3.1.2 Kryptographie nach dem Bell'schen Theorem

Ein anderes Verfahren zum Schlüsselaustausch basiert auf einem Gedankenexperiment von Einstein, Podolsky und Rosen (EPR) [22]. Das von A. Ekert 1991 vorgeschlagene Schema [23] nutzt dabei die Korrelation eines EPR-Paares [24] aus, bei deren Erzeugung aus einem System mit Spin 0 zwei Teilchen mit entgegengesetztem Spin $\frac{1}{2}$ entstehen, in diesem Fall Photonen. Resultate von Polarisationsmessungen daran sind dabei korreliert. Der Zustand eines solchen Systems kann unter Umständen nicht mehr durch ein Produkt von Zuständen der einzelnen Teilchen beschrieben werden. Diese Eigenschaft des Zustandes wird seit Schrödinger als *Verschränkung* bezeichnet und von den Erhaltungssätzen für den Gesamtspin bei der Erzeugung von Photonenpaaren gefordert. Man betrachtet ihn als eine Superposition von Basiszuständen, wie etwa $|H\rangle$ und $|V\rangle$ und notiert ihn wie folgt.

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle - |V\rangle|H\rangle) \tag{3.1}$$

Die beiden Photonen werden emittiert und je eines von Alice bzw. Bob empfangen. Diese nehmen daran unabhängig von einander jeweils eine Polarisationsmessung vor. (Abb.3.6)

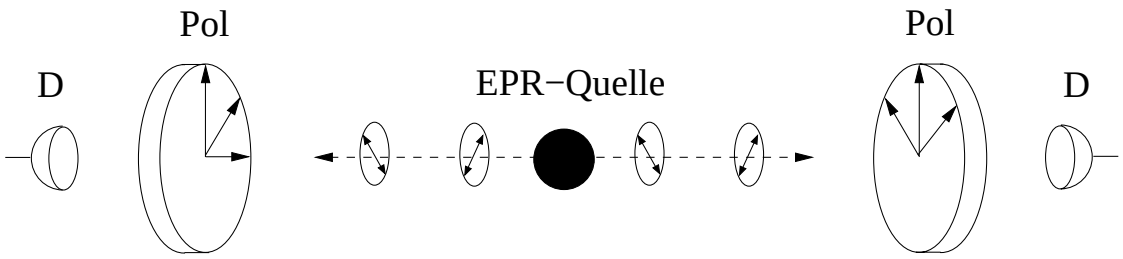


Abbildung 3.6: Möglicher Schlüsselaustausch nach dem Bell'schen Theorem durch Verwendung von verschränkten Photonenpaaren

Dabei entscheidet sich Alice zufällig für eine Polarisationsmessung im Winkel 0, $\frac{\pi}{4}$ oder $\frac{\pi}{2}$ und Bob ebenfalls zufällig zwischen den Winkeln 0, $+\frac{\pi}{4}$ und $-\frac{\pi}{4}$. Hinter einem so orientierten Polarisator wird jedes der Photonen in jeweils einem der Analysatorausgänge gemessen, ergibt also als Ergebnis "0" oder "1". Alice und Bob tragen dieses in je eine Liste ein. Anschließend tauschen sie öffentlich die jeweiligen Meßbasen aus, verwerfen

die Einträge, bei denen nur einer oder keiner von ihnen ein Photon detektieren konnte und teilen die restlichen in zwei Gruppen ein.

In der ersten Gruppe sind die Fälle mit unterschiedlicher Analysatorstellung und in der zweiten diejenigen mit gleicher. Durch Veröffentlichung der ersten Gruppe kann nun die Verletzung der Bell'schen Ungleichung [25] getestet und ein potentieller Abhörer entdeckt werden. Ist dies nicht der Fall, so kann man aufgrund der Spin-Erhaltung sicher von einer Antikorrelation der Einträge in der zweiten Gruppe ausgehen. Werden diese in Bits übersetzt, so erhält man den Rohschlüssel, der noch Fehler enthalten kann, ähnlich dem BB84-Protokoll.

Zur realistischen Anwendung des Verfahrens sei gesagt, daß es wegen des hohen technischen Aufwands für die Erzeugung von verschränkten Photonenpaaren zur Zeit noch nicht praktikabel ist, eine Schlüsselerzeugung nach diesem Konzept durchzuführen, jedoch laufen in einigen Gruppen Experimente dazu, wie etwa in Wien (Zeilinger) oder Genf (Gisin).

3.1.3 Durch Interferometrie zum Schlüssel: B92

Ein Schema, das sich nicht der Polarisationscodierung sondern der Phasencodierung bedient, schlug Bennett im Jahre 1992 vor [26]. Der Aufbau ist eine Variation des Mach-Zehnder Interferometers wie in Abb.(3.7) skizziert, wobei Alice und Bob jeweils über ein Halbinterferometer verfügen.

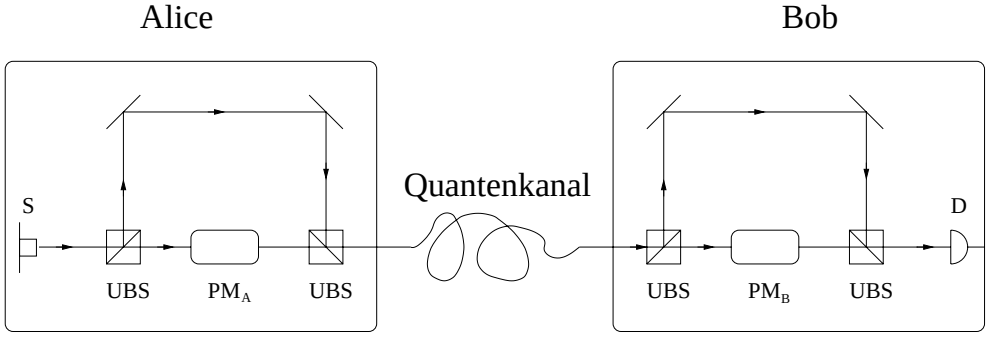


Abbildung 3.7: Alice wie Bob verfügen über jeweils ein Halbinterferometer aus unsymmetrischen Strahlteilern (UBS), je einem Phasenmodulator (PM), einer Pulsquelle (S) und einem Detektor (D), verbunden über eine Faser als Quantenkanal. Die Informationskodierung geschieht durch Phasenmodulation.

Alice emittiert einen Lichtpuls (S) und teilt ihn an einem unsymmetrischen Strahlteiler (UBS) kohärent auf. Der schwache Signalpuls mit einer mittleren Photonenzahl $\mu < 1$ erfährt einen Phasenschub (PS_A) von entweder 0° oder 180°, der starke mit $\mu > 1$ eine Zeitverzögerung von Δt. Mit dem Phasenschub werden die Bits 0 (0°) und 1 (180°)

kodiert. Die Pfade der beiden Pulse werden an einem zweiten unsymmetrischen Strahlteiler wieder zusammengeführt und über den Quantenkanal, etwa eine Glasfaser, an Bob übermittelt. Dieser kann ebenso mit einem baugleichen Halbinterferometer einen eintreffenden Puls kohärent aufspalten, den schwachen um 0° oder 180° phasenverschieben (PS_B) und den starken zeitlich um Δt verzögern.

An Bobs Ausgang erhält man somit drei Pulse im Abstand Δt. Der erste, von beiden Parteien abgeschwächte und somit sehr schwache Puls wird vernachlässigt. Der zweite Puls, auch Signalpuls genannt, ist Träger der Information und der dritte wird als Referenzpuls verwendet. Der Signalpuls stellt eine Superposition des von Alice phasenmodulierten und von Bob zeitverzögerten, sowie des von Alice zeitverzögerten und von Bob phasenmodulierten Pulses dar. Abhängig von den Phaseneinstellungen, die Bob und Alice gewählt haben, interferieren die beiden Teilpulse miteinander: konstruktiv bei gleichem Phasenschub und destruktiv bei unterschiedlichem. Dieses Signal wird von einem Detektor (D) erfaßt.

Das Schema bringt aber einige technische Schwierigkeiten mit sich. So muß der Pfadlängenunterschied der beiden Halbinterferometer exakt der gleiche sein und um Bruchteile der Wellenlänge stabil gehalten werden. Da optische Bausteine, wie die Phasenmodulatoren eine bevorzugte Polarisationsrichtung aufweisen, ist außerdem eine aufwendige Polarisationskorrektur der Faser nötig.

Umgangen werden diese Probleme in einer modifizierten Version dieses Aufbaus, bei der Bob den Lichtpuls aussendet. Dieser durchläuft dessen Halbinterferometer, wird bei Alice phasenmoduliert, zurückreflektiert, und gelangt über die selbe Faser wieder zu Bob. Dort passiert er erneut das Halbinterferometer und wird von Bob phasenmoduliert. Polarisationsänderungen können kompensiert werden, da die selbe Faser in Hin- und Rückrichtung durchlaufen wird, wenn man einen sogenannten Faraday-Spiegel verwendet.

Experimente dazu wurden u.a. bereits in Genf [27], Los Alamos [28] und bei der British Telecom [29] erfolgreich durchgeführt. Bei Weiterentwicklungen wurde aber wieder auf das BB84-Protokoll zurückgegriffen, nun mit Phasenkodierung. Solch ein System ist auch kommerziell erhältlich [30].

3.2 Die Bitfehlerrate und deren Korrektur

Der im Rohschlüssel enthaltene Fehler wird durch das Verhältnis von falschen Bits **F** zur Gesamtzahl an übertragenen Bits **G** angegeben. Diesen Quotienten $\frac{\mathbf{F}}{\mathbf{G}}$ bezeichnet man als Quanten-Bitfehlerrate (QBER). Ihr Wert wird bestimmt, indem man einen Teil des Rohschlüssels öffentlich vergleicht und danach verwirft. Die Quanten-Bitfehlerrate ist ein Kriterium für die Güte der Schlüsselübertragung und wird für jeden übertragenen Schlüssel neu ermittelt.

Der somit ermittelte Fehler muß nun korrigiert werden, da ein Schlüssel nur dann einen Wert für das Chiffrieren von Nachrichten hat, wenn er Sender und Empfänger in

identischer Form vorliegt. Eine Möglichkeit der Korrektur ist folgende [31]:

Abhängig von der Quanten-Bitfehlerrate wird nun eine geeignete Blockgröße gewählt, in die man den Rohschlüssel auf beiden Seiten einteilt. Es folgt die Bildung eines Paritätsbits zu jedem Block, was bedeutet, daß jedem Block ein Bit zugeordnet wird. Dieses Bit ist 1 für eine gerade Anzahl an Einsen in dem Block, und 0 für eine ungerade. Ist das Paritätsbit zum gleichen Block bei Alice und Bob identisch, so behalten sie den Block. Sind sie unterschiedlich, enthält also der gleiche Block bei Alice und Bob eine unterschiedliche Anzahl an Einsen, so teilen sie diesen in zwei Unterblöcke, bilden wiederum Paritätsbits, behalten den mit gleichem Bit und unterteilen den anderen erneut.

Der Fehler läßt sich so auf ein einziges Bit zurückverfolgen, ohne den Schlüssel veröffentlicht zu haben. Nach dem Vergleich jedes Blocks muß eines der Bits gestrichen werden, um die Information, die ein Abhörer aus dem Paritätsbit ziehen kann, zu verwischen. Nun besteht noch die Möglichkeit, daß ein Block eine gerade Anzahl an Fehlern enthält. Wiederholt man diesen Vorgang oft genug mit unterschiedlichen Teilmengen als Blocks, deren Größe optimal aus der QBER errechnet werden muß, so kann man am Ende von einem fehlerfreien, identischen Schlüssel auf beiden Seiten ausgehen.(Abb. 3.4).

3.3 Wie Eve wieder Information verliert: Privacy Amplification

Im Allgemeinen muß angenommen werden, daß alle Fehler durch eine Abhörerin Eve verursacht worden sind. So läßt sich ein oberer Wert für die Information abschätzen, die diese maximal über den Schlüssel besitzen kann. Aus diesem Wert läßt sich errechnen, um welchen Betrag w der korrigierte Schlüssel s der Länge n vermindert werden muß, so daß Eves Informationsgehalt unter eine zuvor festgelegte Grenze sinkt. Mit Algorithmen, wie der Privacy Amplification [32], kann nun mittels einer öffentlichen Diskussion zwischen Alice und Bob die Information, über die Eve verfügt, auf einen Bruchteil reduziert werden. Dazu wählt Alice eine zufällige Binärmatrix $\mathbf{M}$ (mit den Einträgen 1 und 0) der Größe $(n - w)$ x n und übermittelt diese öffentlich an Bob. Beide wenden die Matrix $\mathbf{M}$ auf ihren Schlüssel s an und erhalten so den endgültigen Schlüssel s' der Länge $n - w$.

$$s' = \mathbf{M} * s \ (mod 2) \tag{3.2}$$

Diese Verfahren anzuwenden ist relativ einfach verglichen damit, einen Beweis seiner Sicherheit zu führen. Für weitere Informationen sei auf [32] verwiesen.

Der fertige Schlüssel

Liegt die ermittelte Fehlerrate des Rohschlüssel unter einem zuvor festgelegten Wert – wie beispielsweise 10%– so wird dieser als *gültig* erklärt. Das bedeutet, daß Eve weniger

als alle Schlüsselbits besitzen kann. Nach der Korrektur des Rohschlüssels und der anschließenden *Privacy Amplification* reduziert sich die Anzahl an korrekten Bits bei Eve auf ein Minimum, wie im vorherigen Absatz erläutert.

Man kann davon ausgehen, daß ausschließlich Alice und Bob über den Schlüssel verfügen und eine sichere Chiffrierung von Nachrichtentexten damit möglich ist. Welchen Code man nun bei der Verschlüsselung verwendet, ist dem Anwender selbst überlassen. Absolute Sicherheit bietet aber nur der *Vernam-Code*. Ein schon erwähnter Nachteil dabei ist Länge des benötigten Schlüssels, die gleich der Länge des Klartextes ist.

Um mit kürzeren Schlüsseln auszukommen muß man auf andere Verfahren, wie den DES, AES oder ähnliche ausweichen, was eine Reduzierung der Sicherheit mit sich bringt.

4 Das Experiment

Ziel des Experimentes ist die Realisierung eines quantenkryptographischen Schlüsselaustausches zwischen zwei Punkten über eine Freiraumstrecke von mindestens 20 km. Im Vordergrund steht dabei ein kleiner und praktisch anwendbarer Aufbau.

4.1 Alice, der Sender

Die Sendeeinheit (ohne Teleskopoptik) ist in einem Gehäuse von $5 * 5 * 7\ cm^3$ untergebracht. Es wird also nicht mehr im Maßstab, wie er im Labor üblich ist, gearbeitet, sondern ein System entwickelt, daß einer praktikablen Anwendung gerecht wird.

4.1.1 Aufbau von Modul und Optik

Um nach dem BB84 Protokoll vorgehen zu können, benötigt man Photonen der 4 Polarisationsrichtungen H, V, +45° und -45°. Für jede dieser Richtungen wird je eine Laserdiode als Quelle benutzt.

Die Laserdioden sind im Abstand von 45° so auf einer Kreislinie angebracht, daß ihre Emissionsachsen jeweils zum Mittelpunkt zeigen, wo sie auf eine vergoldete Kegelspitze treffen und jeder Strahl auf die gemeinsame Kreisachse reflektiert wird (Abb. 4.1).

Das emittierte Licht der Laserdioden besitzt einen sehr hohen intrinsischen Polarisationsgrad und macht somit keine zusätzlichen polarisierenden Bauteile mehr notwendig. Abbildung (4.2) zeigt das Ergebnis einer Polarisationsmessung der Laserdioden, nachdem das Licht an der Kegelspitze reflektiert wurde. Dabei ist die durch einen Polarisator transmittierte Intensität abhängig von dessen Orientierung angetragen. Die Sichtbarkeit (Kap.5.1.6.) von 99,0% ($\pm$ 0,27%) kann dabei als Maß für den Grad der Polarisation herangezogen werden.

Da die Sicherheit des BB84-Protokolls auf der Ergebnisunschärfe einer Polarisationsmessung aufbaut, sollten die Photonen ansonsten identisch sein. Sind sie anhand einer anderen Eigenschaft, wie etwa Wellenlänge oder Emissionsrichtung zu unterscheiden, können daraus Rückschlüsse auf die Quelldiode und somit auch auf die Polarisation gezogen werden, ohne die Polarisation selbst zu messen. Deshalb wird mit einem Raumfilters aus dem Überlappungsbereich der 4 Lichtkegel nur eine räumliche Mode herausgegriffen,

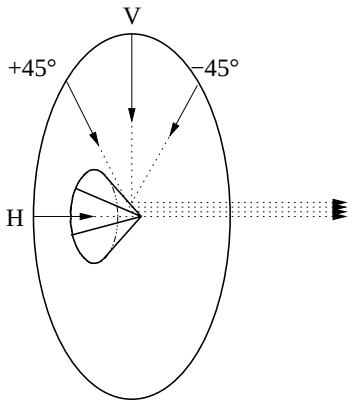


Abbildung 4.1: Anordnung der 4 emittierenden Laserdioden im Winkel von 45° zueinander, deren Licht an einer Kegelspitze in eine gemeinsame Richtung reflektiert wird.

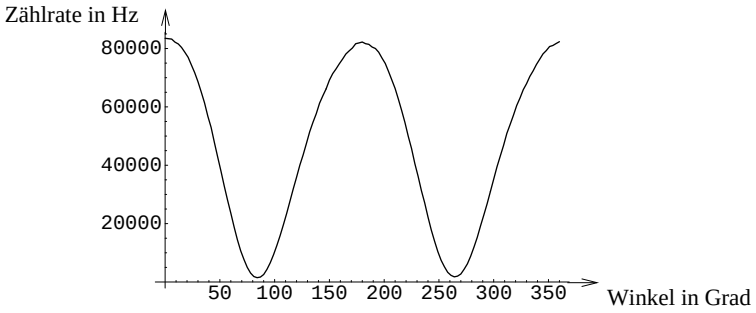


Abbildung 4.2: Die Sichtbarkeit einer Polarisationsmessung mit einem Polfilter (99%± 0,27%) kann als Maß für den Polarisationsgrad betrachtet werden

so daß die Ausbreitungsrichtung eines Photons keine Information mehr über seine Quelle enthält.

Dieser Raumfilter besteht aus zwei Blenden mit je 100 μm Durchmesser im Abstand von 9 mm (Abb. 4.3). Um dadurch nicht allzuviel Licht zu verlieren, wird es mit einer Sammellinse (f=2.75 mm) auf die Mitte des Raumfilter fokussiert.

Das aus dem Raumfilter austretende Licht wird mit einer Kombination aus zwei Sammellinsen (f=4,5 und f=35 mm) zu einem parallelen Strahl mit einer vollen Halbwertsbreite von 2 mm kollimiert.

Bei der anschließenden Teleskopoptik handelt es sich um ein *astronomisches* Teleskop mit 20-facher Vergrößerung, das aus zwei Sammellinsen mit Brennweiten f=25 mm und f=500 mm im Abstand von 52,5 cm besteht (Kap.5.1.7.). Der eintreffende parallele Strahl mit einer vollen Halbwertsbreite von 2 mm verläßt das Teleskop mit einer Breite von

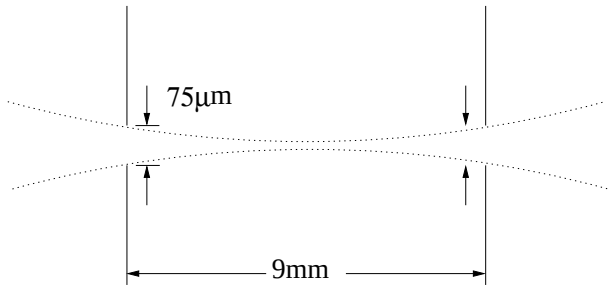


Abbildung 4.3: Der Raumfilter dient zur Selektion einer einzigen räumlichen Mode aus dem Licht aller 4 Quelldioden

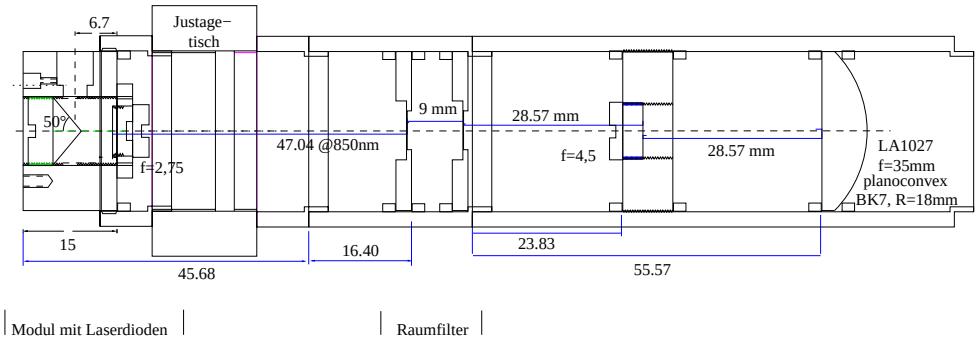


Abbildung 4.4: Maßstabsgetreue Zeichnung des Sendemoduls incl. Raumfilter und Linsen

40 mm. Er wird dazwischen über zwei Goldspiegel (S_1 und S_2) umgelenkt (Abb.4.5). Sämtliche reflektierende Bauteile tragen eine Beschichtung aus Gold, da dieses einen sehr guten Reflexionswert von 96% für Licht der Wellenlänge 850 nm besitzt [33] und keinen großen Phasenschub zwischen H- und V-Polarisation aufweist, was für Licht der 45°-Basis von Bedeutung ist.

Die ursprünglich zur Feinjustage vorgesehenen Spiegel (S_1, S_2) waren im weiteren Verlauf des Experiments nicht mehr nötig, da sich ein Verkippen des gesamten Aufbaus als vorteilhafter erwies, wie noch erläutert wird.

Nach dem Raumfilter gibt es die Möglichkeit, mit Hilfe eines einklappbaren Spiegels den Strahl auf eine Silizium-Avalanche-Photo-Diode (SiAPD, siehe Kap.4.2.3.) zu lenken, womit man in der Lage ist, die Intensität des emittierten Strahls und somit die Anzahl der Photonen eines Pulses zu bestimmen und einzustellen. Zur Ausrichtung des Senders kann noch das Licht einer weiteren Laserdiode über einen Hilfsspiegel in den Strahlengang gelenkt und auf das Raumfilter fokussiert werden. Die dadurch erreichte höhere Intensität ermöglicht eine einfache Justage. (Kap.4.3.4.)

Weitere, einem Abhörer nützliche, Informationen über die jeweils sendende Licht-

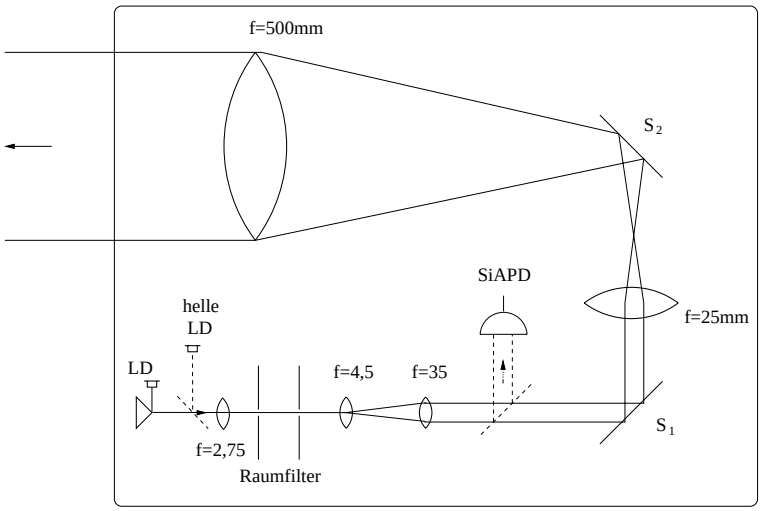


Abbildung 4.5: Die gesamte Sendeoptik ist auf einer $25 * 50\ cm^2$ großen Platte montiert, deren Lagerung eine exakte Ausrichtung erlaubt. Über zusätzliche Spiegel können eine helle Justierdiode (LD) und eine SiAPD zur Kontrolle der Emissionsintensität in den Strahlengang gebracht werden.

quelle geben unterschiedliche Wellenlängen des von den Laserdioden emittierten Lichts. Deshalb wurde versucht, Laserdioden mit möglichst deckungsgleichen Spektren zu verwenden. Hier ist die Entscheidung auf *single-mode* Laserdioden der Firma Roithner [34] mit einer nominalen Wellenlänge von 850 nm gefallen, deren 4 Spektren in Abb.(4.6) dargestellt sind.

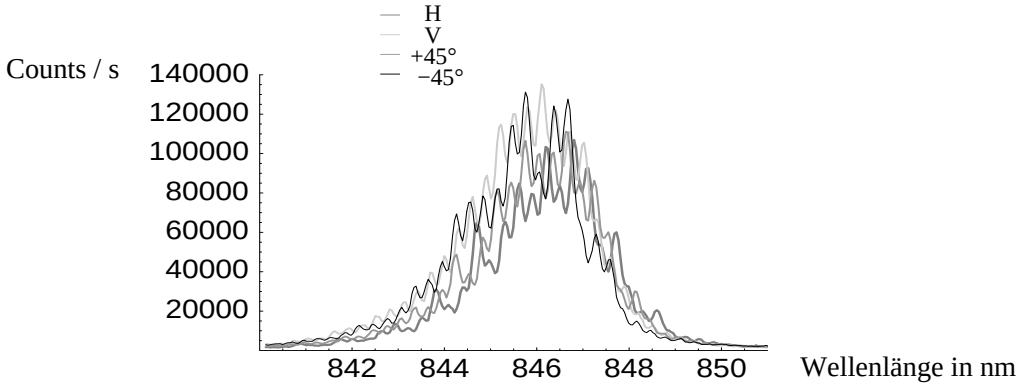


Abbildung 4.6: Frequenzspektren der 4 Laserdioden im gepulsten Betrieb bei 10 MHz und Raumtemperatur. Diese sollten bestmöglich überlappen, damit das Licht spektral ununterscheidbar ist.

Da im Augenblick echte Einzelphotonen-Quellen in einem kleinen Aufbau wie diesem aufgrund ihrer Ausmaße, Effizienz und spektralen Verteilung noch schwierig handzuhaben sind, wird hier auf die Erzeugung quasi-einzelner Photonen ausgewichen. Die Laserdioden werden im Takt von 10 MHz gepulst und so stark abgeschwächt, daß bei einer Pulslänge von etwa 500 ps noch durchschnittlich 0,1 Photonen pro Puls vorhanden sind. Dieser Wert wird als Photonenzahl μ=0,1 bezeichnet und bedeutet, daß unter 10 Pulsen im Schnitt ein Photon enthalten ist. Es ist ein Kompromiß aus den Anforderungen, die Photonenrate so groß und die Wahrscheinlichkeit von zwei Photonen pro Puls so gering wie möglich zu halten. Einerseit steigt mit der Photonenrate auch die Bandbreite der Übertragung, andererseits hat ein Abhörer bei zwei Photonen die Möglichkeit, eines der beiden zur Analyse abzufangen und das andere unverändert passieren zu lassen, womit er völlig unbemerkt bliebe.

Geht man bei der Emission einer Laserdiode von einer Poisson-Verteilung der Photonen aus, so beträgt die Wahrscheinlichkeit, während eines Zeitintervalls $\Delta\ t$ genau k Photonen zu erhalten

$$P(X = k) = \frac{\lambda^k}{k!}\ e^{-\lambda}. \qquad k \in \mathbb{N},\ \lambda \geq 0 \tag{4.1}$$

Der Parameter $\lambda = 0,1 = E(X)$ gibt die mittlere Photonenzahl in einem Zeitintervall $\Delta\ t$.

Betrachtet man die Wahrscheinlichkeit, mindestens ein Photon in einem dieser Zeitintervalle vorzufinden, so erhält man für $X \geq 1$

$$P(X \geq 1) = 9,516\ \%. \tag{4.2}$$

In etwa 95 von 1000 Fällen sind also in einem Puls Photonen enthalten. Die Wahrscheinlichkeit, daß sich aber mehr als nur ein einzelnes Lichtteilchen darin befindet wird durch den Fall $X \geq 2$ beschrieben und es gilt

$$P(X \geq 2) = 0,4524\ \%. \tag{4.3}$$

Die bedingte Wahrscheinlichkeit $\mathrm{P}(X \geq 2|X \geq 1)$ gibt die Häufigkeit von mehr als nur einem Photon unter allen Pulsen, bei denen überhaupt Photonen emittiert werden, an.

$$P(X \geq 2|X \geq 1) = \frac{P(X \geq 2)}{P(X \geq 1)} = 4,754\ \% \tag{4.4}$$

Das bedeutet, daß in 4,75% aller Fälle, bei denen ein Photon emittiert wird, noch ein zweites auftritt, das von einem Abhörer für einen unbemerkten Angriff herangezogen werden kann. Dieser Wert kann als gering genug betrachtet werden.

Die Photonen werden nun in zufällig einer der 4 Polarisationsrichtungen emittiert, wobei diese Zufälligkeit aus einer 1 GByte großen Binärdatei mit Zufallszahlen stammt. Die Zufälligkeit, mit der die Polarisation vom Sender gewählt wird, ist dabei einer der

Kernpunkte für die Sicherheit des Gesamtsystems. Hat ein Abhörer Kenntnis über diese Zahlen oder ein Muster in der Reihenfolge, so muß er nur noch den öffentlichen Kanal mithören um den Schlüssel zu gewinnen. Bei dem vorliegenden Experiment wurde allerdings stets die selbe Datei von Zahlen verwendet, weil dieser Aspekt für den aktuellen Stand des Systems noch ohne Bedeutung ist.

4.1.2 Software und Elektronik

Die digitale I/O-Ausgabekarte des Sende-Computers gibt ein 2-bit Signal mit einer Taktfrequenz von 10 MHz aus, das auf eine externe hochstabile Quarzuhr synchronisiert ist. Dieses Signal wird von einer Elektronik so umgewandelt, daß damit ein Treiber für die 4 Laserdioden gesteuert werden kann. Die Dioden werden dabei stets auf einem Offsetstrom knapp unter dem Schwellstrom gehalten, bei dem sie zu lasen beginnen. Nur im Falle eines Signals wird der Strom kurz darüber hinausgehoben. Dadurch ist es möglich, innerhalb einer Nanosekunde einen definierten Lichtpuls zu emittieren und Pulslänge, Stromhub sowie Offsetstrom zu variieren.

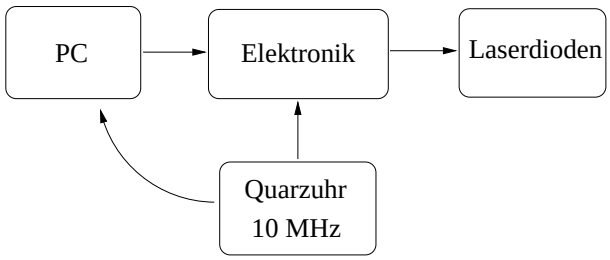


Abbildung 4.7: Schematische Darstellung der Verbindung der einzelnen Hardwarekomponenten von Alice

Die Software zur Steuerung des Systems wurde von Paul Tapster aus der kooperierenden QuinetiQ-Gruppe beigesteuert [35]. Sie ist als LabView-Programm unter Windows geschrieben und läuft auf jeweils einem Rechner auf Sender- und Empfängerseite. Die zwei Computer der Marke Dell arbeiten mit einem 400 MHz getakteten Pentium II Prozessor.

4.2 Bob, der Empfänger

Wie beim Sender konnte auch hier ein etwa handtellergroßer Aufbau realisiert werden ($75 * 68 * 40\ mm^3$). Der limitierende Faktor für die Größe des Gesamtsystems ist durch die Teleskopoptik gegeben, wie es bei einer solchen Übertragungsstrecke nötig ist, so daß eine weitere Miniaturisierung keinen Vorteil mehr brächte.

4.2.1 Die Optik und Polarisationsanalyse

Mit einem kommerziellen 10“-Teleskop (Ø 25 cm, Meade LX200) nach Schmidt-Cassegrain-Bauart und einer computergesteuerten Justiermöglichkeit wird ein Teil des ankommenden Lichts eingesammelt und fokussiert.

Über einen Klappspiegel am Ausgang des Teleskops läßt sich der Strahl auf eine CCD-Kamera lenken, so daß die Senderseite über einen Monitor betrachtet werden kann und sich dadurch die grobe Ausrichtung des Teleskops kontrollieren läßt (Abb. 4.12).

Ist der Spiegel zur Seite geklappt, so trifft der Strahl auf das eigentliche Analysemodul (Abb.4.8), das hinter dem Teleskop montiert ist und zur Polarisationsmessung dient. Dieses besteht aus einem unpolarisierenden 50/50-Strahlteiler, in dessen beiden Ausgängen je ein polarisierender Strahlteiler folgt. Ein polarisierender Strahlteiler läßt horizontal polarisiertes Licht passieren und reflektiert vertikal polarisiertes. Am Ende dieser 4 Pfade ist je eine Silizium-Avalanche-Photo-Diode (SiAPD) angebracht. Damit kann ein Photon in einem der 4 Ausgänge detektiert werden.

Die Ausgänge des unpolarisierenden Strahlteilers entsprechen den Basen H/V bzw. +/-45°. Wird ein Photon in der gleichen Basis detektiert wie emittiert, so läßt sich eine Aussage über dessen Polarisation machen, andernfalls nicht.

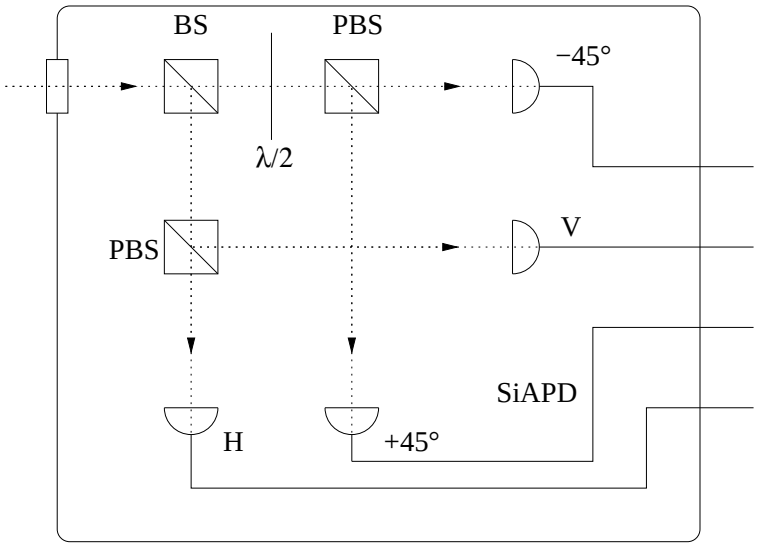


Abbildung 4.8: Strahlengang in Bobs Detektionsmodul mit polarisierenden Strahlteilern (PBS), $\frac{\lambda}{2}$-Plättchen, den 4 Detektoren (SiAPD) und 50/50-Strahlteiler (BS), der über die Zufälligkeit der Meßbasis bestimmt.

Die Zufälligkeit der Basenwahl ist der entscheidende Punkt für die Sicherheit dieses Protokolls. Während der Sender über Zufallszahlen aus einem Generator gesteuert wird, basiert die Zufälligkeit bei der Detektion darauf, in welchem Ausgang des unpolarisie-

renden Strahlteilers ein Photon detektiert wird. Für einen 50/50-Strahlteiler, wie er hier verwendet wird, besteht für beide Ausgänge die gleiche Wahrscheinlichkeit. [36]

Aus Gründen der einfacheren Montage und Justierbarkeit wird der polarisierende Strahlteiler im Pfad der +/-45° Basis ebenfalls im rechten Winkel angebracht, so daß die Polarisation des Strahls um 45° gedreht werden muß, was man mit einem $\frac{\lambda}{2}$- Plättchen im Winkel von $22,5°$ im Strahlengang erreicht.

Die Dioden sind zur Kühlung auf Peltierelementen angebracht und das gesamte Modul ist luftdicht abgeschlossen, um Eisbildung auf den Photodioden zu verhindern.

4.2.2 Die Filterung von Streulicht

Eine der Herausforderungen besteht darin, einzelne vom Sender emittierte Photonen aus dem Hintergrundlicht diverser anderer Lichtquellen herauszusieben. Obwohl sämtliche Versuche bei Dunkelheit stattfinden, ist die Verwendung von spektralen Filtern unumgänglich, um restliches Streulicht, wie etwa Mond- oder Kunstlicht, bestmöglichst zu unterdrücken. So werden stets ein bzw. zwei Kantenfilter des Typs RG780 verwendet, um Wellenlängen von unter 780 nm abzublocken (Abb. 4.9), sowie meistens zusätzlich ein Interferenzfilter mit einem Transmissionsbereichen von 10 nm Breite und einer zentralen Wellenlänge von 853 nm. Der klassische Kanal funktionierte ursprünglich über eine optische Übertragungsstrecke, die mit Licht der Wellenlänge 650 nm arbeitete und war dadurch für einen Großteil des Streulichts verantwortlich.

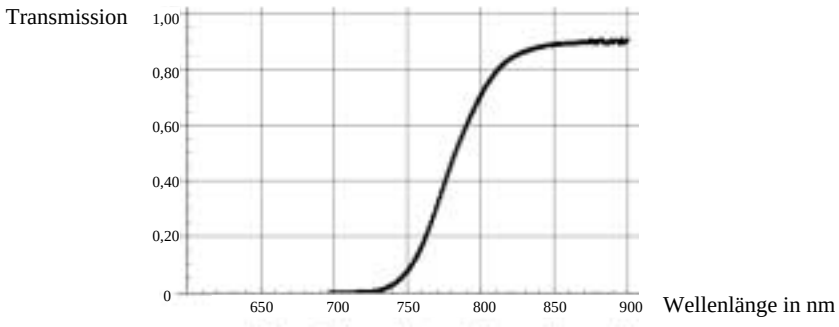


Abbildung 4.9: Transmissionsspektrum eines Kantenfilters vom Typ RG780

Da die Wellenlänge der emittierten Photonen von der Temperatur der Dioden abhängt und mit dieser um etwa 0.26nm/°K abnimmt (siehe Abb. 4.10) , ist es nötig, den Transmissionsbereich der Filter variieren zu können.

Verkippt man einen Interferenzfilter so, daß er nicht mehr senkrecht im Strahlengang steht, sondern in einem einstellbaren Winkel dazu, so verschiebt sich der Transmissionsbereich zu kürzerwelligem Licht (Abb.4.11). Bei einer Diodentemperatur von beispielsweise -15°C, wie sie bei dem Experiment realistischerweise herrscht, beträgt die

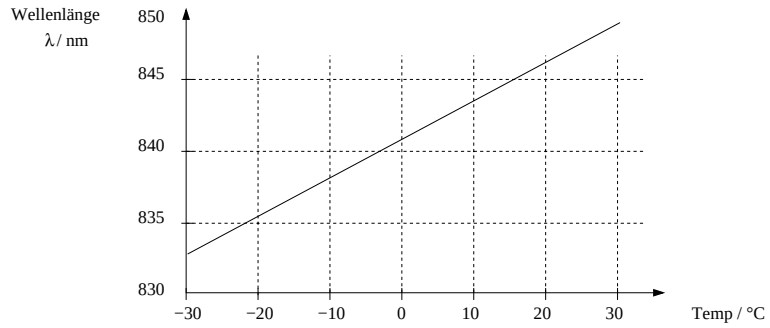


Abbildung 4.10: Die Temperaturabhängigkeit der zentralen Wellenlänge von Laserdioden ist linear und nimmt mit etwa 0,26nm/°K zu.

Wellenlänge des emittierten Lichts 838 nm, was einem Winkel des Interferenzfilters von 17° entspricht. Je nach augenblicklicher Temperatur auf der Senderseite kann damit eine optimale Transmission des Interferenzfilters eingestellt werden.

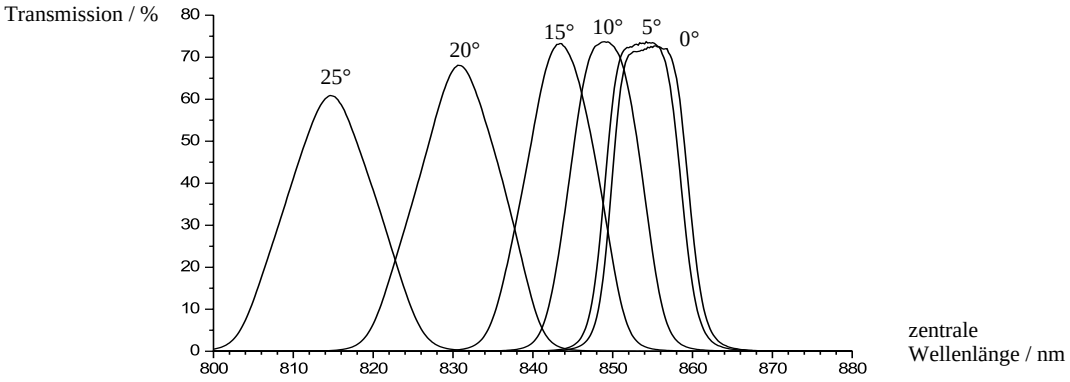


Abbildung 4.11: Die transmittierte Wellenlänge eines Interferenzfilters ist abhängig von seinem Winkel. Die Wellenlängenverteilungen sind für verschiedene Winkel gemessen.

Ein weiterer zu korrigierender Effekt tritt bei der Reflexion an Goldspiegeln auf. Die unterschiedliche Eindringtiefe von S- und P-polarisiertem Licht in eine Metallschicht führt zu einer scheinbar unterschiedlichen Lage der Reflexionsebenen, oder gleichbedeutend damit zu einer Phasendifferenz zwischen den beiden Polarisationsrichtungen. Das ist zwar für diese beiden Richtungen ohne Belang, jedoch nicht für die schrägen Polarisationsrichtungen. Betrachtet man schräge Polarisation als Linearkombination aus H und V, die am Spiegel phasenverschoben reflektiert werden, so ergibt sich nach der

Reflexion eine elliptische Polarisation. Diesen Fehler kompensiert ein doppelbrechendes Quarzplättchen (Kap. 5.1.5.) im Strahl abhängig von seinem Winkel dazu. Auch dabei ist eine präzise Einstellung notwendig.

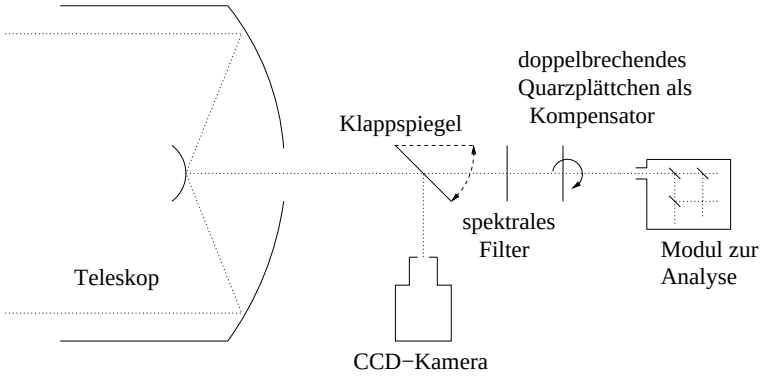


Abbildung 4.12: Aufbau der gesamten Empfängeroptik mit angeschlossener CCD-Kamera, Filter, Kompensator und Analyseblock.

4.2.3 SiAPD zur Detektion einzelner Photonen

Trifft ein Photon auf das Silizium einer SiAPD, so erzeugt es dort ein Elektron-Loch-Paar (*innerer Photoeffekt*). Das Elektron wird von einer an der Diode anliegenden Spannung von etwa 215 V so stark beschleunigt, daß es ein zweites Paar erzeugt, dessen Elektron wiederum beschleunigt wird etc.. Die dadurch ausgelöste Lawine von Elektronen erzeugt einen Strom (*Geiger-Modus*), der als elektrisches Signal verarbeitet werden kann. Dieser fließt über einen hochohmigen Wiederstand ab, so daß die Spannung nun größtenteils dort abfällt und nicht mehr an der Diode anliegt. Die Elektronen werden weniger beschleunigt und die Lawine kommt zum Erliegen (*passives Löschen*). Fließt kein Strom mehr, so liegt nach einer kurzen Ladezeit die gesamte Spannung wieder an der Diode an und es kann beim nächsten eintreffenden Photon erneut eine Lawine ausgelöst werden. Wird aber ein Elektron aufgrund thermischer Bewegung ausgelöst, ohne daß ein Photon detektiert wurde, so führt das ebenfalls zu einem elektrischen Impuls. Diese Pulse sind nicht von den richtigen Photonen-Pulsen zu unterscheiden und verursachen die *Dunkelzählrate (DCR)*. Um die DCR aufgrund thermischer Bewegung zu reduzieren werden die Dioden mit Peltierelementen gekühlt. Da mit der Temperatur auch die Durchbruchspannung abnimmt, muß die angelegte Spannung variiert werden, um optimale Detektionseffizienz bei geringer DCR zu erreichen. Ein typischer Wert ist ungefähr 20 V über Durchbruchspannung.

Im beschriebenen Experiment werden die SiAPD bei etwa −30°C bei einer Außentemperatur von unter 0°C betrieben, wodurch die DCR auf bis zu 50 s^{-1} sinkt. Die SiAPD besitzen in unserem Fall eine Quanteneffizienz von 45 %.

Ein andere Möglichkeit, einzelne Photonen nachzuweisen, ist die Verwendung von Photomultipliern. Diese haben zwar den Vorteil einer geringen Dunkelzählrate, jedoch auch den Nachteil einer geringeren Quanteneffizienz von etwa 5-10 % für den Wellenlängenbereich um 850 nm. [37]

Die Wellenlänge

Avalanche-Photo-Dioden gibt es außer aus Silizium auch noch aus einer Verbindung von Indium-Gallium-Arsenid (InGaAs-APD), aus der die Photoelektronen ausgelöst werden. Diese besitzen eine höhere Dunkelzählrate, eine geringe Effizienz und werden für Wellenlängen im Bereich von 1,3 - 2 μm verwendet. Sie eignen sich daher ideal für die Kombination mit Glasfasern, die bei 1300 nm bzw 1550 nm minimale Absorption zeigen.

In unserem Experiment haben sich Silizium-APD aufgrund Ihrer Dunkelzählrate und hohen Quanteneffizienz für Wellenlängen zwischen 600 - 900 nm als die beste Wahl erwiesen. Vergleicht man das Transmissionsspektrum von Luft (Abb.4.13) mit dem Absorptionsspektrum von SiAPD (Abb.4.14), so ergeben sich als mögliche Wellenlängen 780 und 850 nm, wobei wir uns aufgrund der optischen Komponenten für letztere entschieden haben.

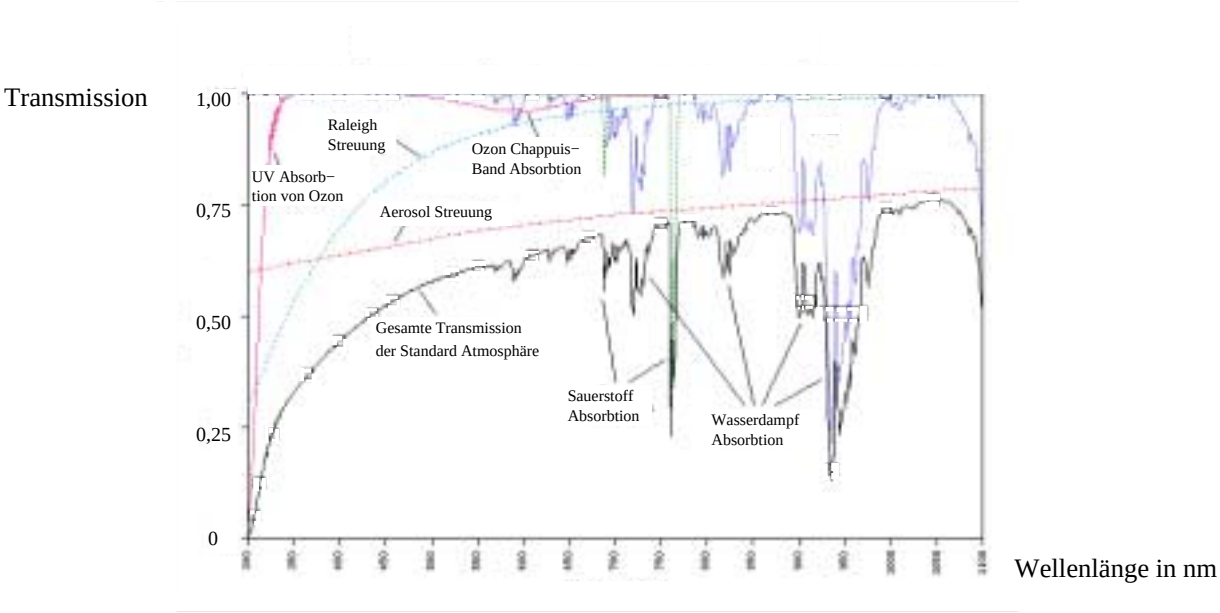


Abbildung 4.13: Transmissionsspektrum der gesamten Atmosphäre in vertikaler Richtung [38]

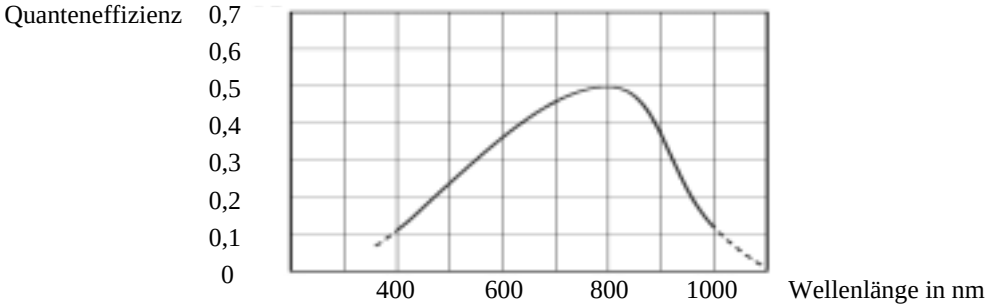


Abbildung 4.14: Absorptionsspektrum einer SiAPD

Noch eine Abhörmethode

Einen möglichen Angriffspunkt für einen Abhörer stellen Effekte in den Photodioden dar. Wird eine Elektronenlawine ausgelöst, so kommt es zur Emission einer Anzahl von Photonen, die von außen beobachtet werden können und Rückschlüsse auf Bobs Detektionen zulassen. Wird zusätzlich der öffentliche Kanal abgehört, so kann dadurch der Rohschlüssel, wie er Alice und Bob vorliegt, rekonstruiert werden. Einem solchen Angriff kann man durch die Verwendung von spektralen und Raumfiltern vorbeugen, da sich die emittierte Wellenlänge von der absorbierten unterscheidet.

4.2.4 Elektronik, Software und Synchronisation

Da die Photonenpulse mit einer Länge von weniger als 1 ns in einem festen Takt von 10 MHz gesendet werden, braucht der Empfänger ebenfalls nur Detektionen betrachten, die im Abstand von 100 ns auftreten. Aufgrund des Jitters (Verwischung des Detektionszeitpunktes) von etwa 0,5 ns und einer Pulsbreite von 0,5 ns wurde ein Detektionszeitintervall von 1,4 ns gewählt.

Somit reduzieren sich die fehlerhaften Detektionen um einen Großteil, da Ereignisse durch die DCR oder gestreute Photonen außerhalb dieser Zeitfenster nicht mehr regestriert werden. Sender und Empfänger müssen nun sicherstellen, daß sie auch wirklich zum gleichen Zeitpunkt senden bzw. detektieren, indem sie sich zuvor synchronisieren. In Abb.(4.15) sind die 4 Pulse der Detektoren in den Zeitfenstern mit einer Breite von 1,4 ns dargestellt, wobei zwei der Detektorsignale durch Kabel um 5 ns verzögert wurden.

Eine Elektronik wandelt die kurzen Strompulse der Detektoren in standardisierte NIM-Pulse um. Zwei der Ausgänge werden dabei um 5 ns verzögert zu den anderen addiert um von einer 2-Kanal-Zeiterfassungskarte (Guide Technology GT654) im Rechner regestriert zu werden. Der Computer protokolliert die Ankunftszeitpunkte der Detektionen und korrigiert digital damit das 10 MHz-Taktsignal seiner externen temperaturstabilisierten Quarzuhr auf den Takt der Sendefrequenz. Dies geschieht mit Hilfe einer Phase-Locked-Loop Software und einer Genauigkeit von unter 1 ns [35]. Nach der

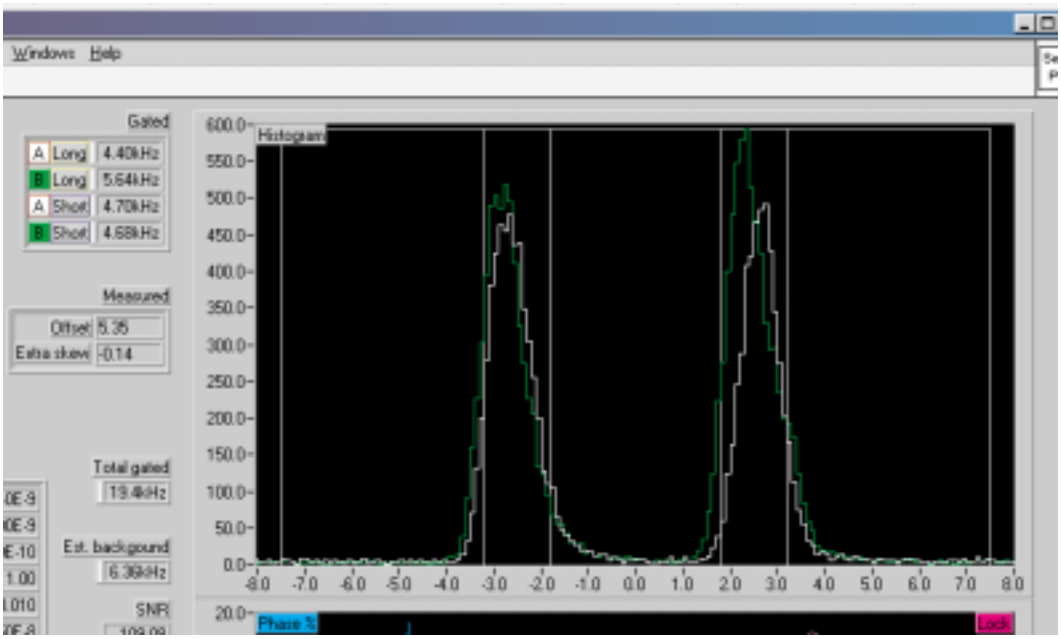


Abbildung 4.15: Der Ausschnitt aus der Bedienoberfläche des Detektionsrechners zeigt die 4 Signale der Detektoren in den 2 zugehörigen Zeitfenstern von 1,4 ns Breite, die alle 100 ns für im Abstand von 5 ns geöffnet werden.

Synchronisation der beiden Computer aufeinander beginnt die Übertragung der zufällig polarisierten Pulse in Blöcken von 700 ms Länge, aus denen später der Rohschlüssel gewonnen wird. Zuvor wird noch für 110 ms jeweils ein Block von vereinbarten Pseudozufallszahlen gesendet, um das Startsignal der Übertragung zu geben. Zum Schluß wird das Signal für etwa 300 ms unterbrochen, um eine erfolgreiche Übertragung bestätigen zu können. Die Dauer eines gesamten Blocks beträgt demnach etwas mehr als 1,1 s. Nachdem eine zuvor festgelegte Anzahl von Schlüsselblocks übermittelt wurden, beginnt das Programm automatisch mit dem Abgleich der Basen sowie der Fehlerkorrektur. Dazu müssen sich Alice und Bob über einen klassischen Kanal unterhalten. Dieser klassische Kanal wird über eine Modemverbindung der beiden Computer untereinander realisiert, wobei der Computer auf der Senderseite mit einem 28.8 Kbaud Modem an das Festnetz angeschlossen ist und beim Empfänger ein Mobiltelefon vom Typ Siemens S35i mit integriertem Modem (9,6 Kbaud) benutzt wird. Somit steht eine Bandbreite von höchstens 9,6 Kbaud zur Verfügung. Für einen Block von 1,1 s Dauer ist zur Fehlerkorrektur ein öffentliche Diskussion von etwa einer Minute notwendig.

4.2.5 Wer sieht was? oder Ausrichtung von Sender und Empfänger gegeneinander

Werden nur Photonen einer bestimmten Polarisation gesendet, so ist zu erkennen, daß jeweils einer der Empfänger idealerweise nichts registriert, da die Photonen orthogonal dazu polarisiert sind.

Wiederholt man die Messung nun für jede der Polarisationsrichtungen und trägt in einer Matrix die Zählrate jedes Detektors gegen jede der Sendedioden an, so erhält man eine Darstellung wie in Abb.(4.16) gezeigt.

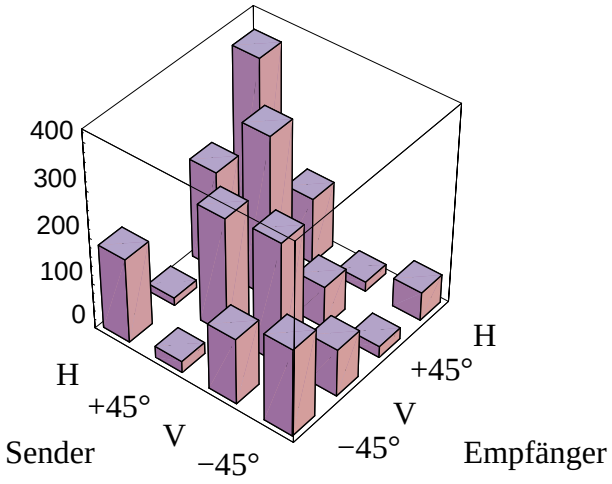


Abbildung 4.16: Trägt man die Signale der 4 Sender gegen die Zählrate der 4 Detektoren an, so erhält man diese Matrix. Jeweils eine Zählrate verschwindet, da Sender und Empfänger orthogonal zueinander polarisiert sind und zwei zeigen Ereignisse in der *falschen* Basis an.

Die geringe vorhandene Zählrate kann durch Dunkelzählrate, Streulicht, Polarisationsfehlern oder einen möglichen Abhörer verursacht werden. Die beiden Detektoren der anderen Basis zählen zusammen die Hälfte der Ereignisse, da sie sich beide im Winkel von 45° zur ausgesandten Polarisation befinden, also jeweils mit einer Wahrscheinlichkeit von 50 % ein Photon in der „falschen“ Meßbasis registrieren. Den höchsten Wert gibt der Zähler für die richtige Polarisation aus, da er die andere Hälfte der Photonen, die in der „richtigen“ Basis detektiert werden aufgrund ihrer gleichen Polarisation vollständig registriert.

Diese Matrix erlaubt eine realistische Beurteilung der Übertragungsverhältnisse und Polarisationsfehler im System, sowie eine Optimierung der Justage.

4.3 Die Strecke

Um mit dem beschriebenen System über eine Distanz von mehr als 20 km noch eine sinnvolle Übertragungsrate zu erhalten, sollten Einflüsse wie Absorption und Streuung gering gehalten werden. Reine klare Luft ohne Turbulenzen bietet dafür die besten Voraussetzungen.

4.3.1 Auswahl der Strecke

Bei der Auswahl der zwei Standpunkte haben wir uns auf Seite des Senders für die Hütte auf der Zugspitze (2950 über NN) entschieden [39], in der das Gipfellabor des Max-Planck-Institutes für extraterrestrische Physik (MPE) untergebracht ist und auf der Empfängerseite für die Bergstation der Karwendelbahn [40] auf der westlichen Karwendelspitze (2244 über NN).

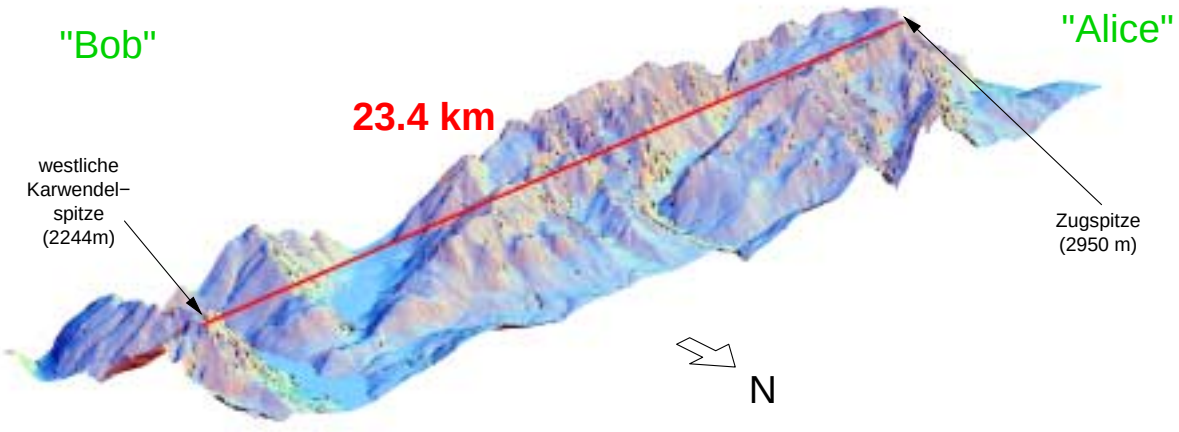


Abbildung 4.17: Zugspitze und westliche Karwendelspitze als Stationen für Alice bzw. Bob.

Argumente dafür waren die gute Transmission in dieser Höhe, geringe Turbulenzen in der Luft und die Hoffnung, dort in der Zeit ab September eine relativ stabile Wetterlage mit klarer Sicht erwarten zu dürfen, womit wir auch teilweise Recht hatten. Beide Stationen sind mit einer Bergbahn zu erreichen, so daß der Transport der Ausrüstung mit einem Gewicht von mehreren hundert Kilogramm kein größeres Problem darstellt. Als infrastrukturelle Voraussetzung benötigen wir prinzipiell nur Anschluß an das Stromnetz, wobei sich aber auch die analoge Festnetz-Telefonleitung auf der Zugspitze als überaus nützlich erwies, unter anderem für den klassischen Kanal. Die Anbindung an das Telefonnetz im Karwendel wird durch eine Mobilfunkverbindung hergestellt. Ein or-

ganisatorisches Problem sollte noch der Schneefall darstellen, so daß man besonders auf der Zugspitze einige Zeit mit Schaufeln beschäftigt ist.

4.3.2 Standort Zugspitze

Eine der Herausforderungen ist es, über solch eine Strecke ausreichend genau justieren zu können. Als *ausreichend* läßt sich hier bezeichnen, wenn man die Orientierung eines Teleskops derart einstellen kann, daß die Position auf der Gegenseite auf weniger als 20 cm definiert ist, also besser als die Teleskopöffnung des Empfängers. Das bedeutet eine Positionierung des Strahls und somit des Senders mit 10 μrad Genauigkeit.

Dazu wird die Platte, auf der sich die Sendeoptik befindet, auf drei Eckpunkten gelagert. Sie kann mit Hilfe einer Mikrometerschraube über einen Hebel von 45 cm mit einer Genauigkeit von 5 μm verkippt werden. Bei vorsichtiger Betätigung der Schraube ist somit ein präzises Justieren möglich. Die Platte ist auf einem massiven dreibeinigen Stativ montiert und steht fest auf einem Fundament aus Beton vor der Hütte, wodurch die nötige Stabilität gewährleistet wird. Der Aufbau besitzt einen Plexiglasdeckel gegen Niederschläge und ist über ein Steuerkabel mit dem Computer im Inneren der Hütte verbunden. So wird der Computer vor Witterungseinflüssen geschützt, denn besonders nachts schaffen die Temperaturen von bis zu -25°C und Windstärken von bis zu 30 m/s hier teilweise recht unkomfortable Bedingungen, die ein längeres Arbeiten im Freien manchmal kaum möglich machen. Das gesamte System erweist sich als äußerst stabil gegen Windböen und Niederschläge.

4.3.3 Das Karwendel

Die Empfangseinheit ist ebenfalls auf einem Stativ montiert, das auf einer überdachten Terrasse vor den Räumen der Bergstation steht und somit keinen Niederschlägen ausgesetzt ist. Der Computer zur Steuerung und Datenanalyse befindet sich, über Kabel verbunden, im Inneren des Raumes.

4.3.4 Die Justage

Verglichen mit anderen klassischen optischen Übertragungstrecken, die mit Sendeleistungen von bis zu einigen hundert Milliwatt arbeiten, muß man hier mit einer Lichtleistung auskommen, die um viele Größenordnungen darunter liegt. Hat man bei größerer Intensität die Möglichkeit, den Lichtstrahl zu sehen und somit nach Augenmaß in Position und Fokussierung zu optimieren, so ist das für den Einzelphotonenstrahl nicht möglich. Dieser besitzt bei 10 MHz Taktfrequenz und 0,1 Photonen pro Puls nur eine Leistung von 0,0023 nW ($2,3 \cdot 10^{-12}$ W), was für das menschliche Auge in diesem Spektralbereich nicht mehr zu erkennen ist. Folglich muß man sich bei der Justage einiger Hilfsmittel bedienen.

Da das System während des Experimentes jeden Tag von Neuem aufgestellt und eingerichtet wird, hat sich im Lauf der Zeit eine effiziente Vorgehensweise beim gegenseitigen Ausrichten von Sender und Empfänger entwickelt, die kurz beschrieben wird. Der tägliche Auf- und Abbau ist nötig, um die Komponenten während der restlichen Zeit zum Schutz im Inneren der Gebäude aufzubewahren.

Begonnen wird mit der groben Positionierung des Empfängerteleskops. Dazu kann über die CCD-Kamera der Bildausschnitt beobachtet und auf den Sender bewegt werden (Abb. S.47 unten) Der parallel zur optischen Achse des Teleskops angebrachte Justierlaser (grün 532 nm, 3 mW) erzeugt auf der Senderseite einen sichtbar schimmernden Lichtfleck von einigen Metern Durchmesser. Von der 80 mm-Austrittslinse (f=500 mm) der Sendeoptik wird nun ein kleiner Teil dieses Lichts aufgesammelt und in der Brennebene fokussiert. Bringt man diesen Fokus durch Verdrehen des Aufbaus in Übereinstimmung mit der optischen Achse des Senders, so ist schon eine Ausrichtung der beiden Teleskope auf weniger als 1 mrad gewährleistet. Nun wird die externe Laserdiode in den Strahlengang des Senders gebracht und so auf das Raumfilter fokussiert, daß ein Strahl von etwa 0,5 mW dieses verläßt. Dieses Licht läßt sich mit einem Sichtgerät für Infrarot von der Empfängerseite aus erkennen, und für den Ort des Empfangsteleskops optimieren. Man beobachtet die Zählrate der 4 Detektoren und optimiert sie auf ein Maximum, wobei mit zunehmender Justiergenauigkeit die Intensität des empfangenen Lichts derart zunimmt, daß die Detektoren sättigen. Dies kann durch eine entsprechende Reduzierung der Emissionsleistung der Justierdiode verhindert werden.

Die nötige Kommunikation zwischen den beiden Stationen findet über handelsübliche Handfunkgeräte statt, die zwar nur für 5 km spezifiziert sind, aber trotzdem über 23,4 km noch funktionieren, wenn auch bei manchmal eingeschränkter Sprachqualität.

Anschließend wird der Hilfsspiegel wieder entfernt und das Sendemodul an die positionierte Teleskopoptik angeschlossen. Zur weiteren Feinausrichtung dient nun eine fünfte Laserdiode ($\lambda = 850$ nm) im Sendemodul, deren Licht wie das der 4 Sendedioden über einen Kegel auf das Raumfilter reflektiert wird und mangels exakter Fokussierung einen viel schwächeren Strahl als die externe Diode erzeugt. Sie wird kontinuierlich betrieben, was die Intensität im Vergleich zum gepulsten Betrieb stark erhöht, und kann ohne eine Veränderung des Aufbaus zur ständigen Nachjustage verwendet werden.

Trotz manchmal starken Windes ist nur etwa jede halbe Stunde eine leichte Korrektur nötig.

4.4 Einige Daten und Ergebnisse

4.4.1 Fokussierung

Das Auflösungsvermögen von optischen Komponenten ist durch Beugung an den Rändern einer Linse begrenzt. Für Licht der Wellenlänge λ sowie einen Durchmesser der Austrittsöffnung d ist der minimale Winkel zwischen zwei Punkten, die noch aufgelöst wer-

den können, durch

$$\alpha = 1,22\,\frac{\lambda}{d}$$

gegeben. Aufgrund der Kleinwinkelnäherung $\sin\alpha \approx \alpha$, wie sie in diesem Fall gilt, läßt sich die Beugungsbegrenzung x für eine Linse mit Durchmesser d und eine Distanz D beschreiben mit:

$$x = 1,22\,\frac{\lambda D}{d}$$

Für eine Wellenlänge $\lambda = 850$ nm, einem Linsendurchmesser $d = 80$ mm und einer Distanz D= 23,4 km erhält man demnach eine mögliche Auflösung von höchstens 30 cm. Es ist es also theoretisch nicht möglich, den Lichtstrahl auf der Empfängerseite kleiner als 30 cm zu fokussieren.

Aufgrund anderer Einflüsse, wie etwa Unterschiede im Brechungsindex durch Luftturbulenzen und Linsenfehler in der Senderoptik konnte dieser Wert nicht erreicht werden. Der erzeugte Lichtfleck hat einen minimal beobachteten Durchmesser von etwa 1,25 m und ist somit noch nicht beugungsbegrenzt.

4.4.2 Fehlerrate

Solange kein Abhörer die Übertragung stört, wird der größte Anteil an fehlerhaften Bits durch die Dunkelzählrate und Streulicht aus anderen Quellen verursacht. Der Anteil an der Quanten-Bitfehlerrate (QBER), der so zustandekommt ergibt sich aus

$$QBER = \frac{F}{G} \quad , \tag{4.5}$$

wobei G die Anzahl an insgesamt übertragenen Bits ist und F die falschen Ereignisse. Letztere lassen sich bei einer Zählrate d aus Umgebungslicht und Dunkelereignissen, einem Detektionsfenster t und einer Pulsfrequenz f durch

$$F = d \cdot t \cdot f \tag{4.6}$$

beschreiben.

Nach (4.5) und (4.6) gilt

$$QBER = \frac{d \cdot t \cdot f}{G} \tag{4.7}$$

Die Zählrate d beträgt bei Einsatz des Interferenzfilters für eine Photodiode etwa 150-250 s^{-1} und ohne diesen zwischen 1000 und 1500 s^{-1}, je nach Umgebungslicht.

Da jeweils zwei der Detektoren um 5 ns verzögert zum Signal der anderen addiert werden, muß die Software zweimal einen Zeitraum von 1,4 ns auf mögliche Ergebnisse untersuchen. Bei einer Frequenz von 10 MHz und einer Übertragungsrate von etwa 1 kbit/s ergibt sich eine theoretische Quanten-Bitfehlerrate von 3,5%, die durch Streulicht verursacht wurde. Man wird sehen, daß dies einen Großteil der gesamten Fehlerrate ausmacht.

4.4.3 Resumée

In Kürze zusammengefaßt sei gesagt, daß es gelungen ist, einen abhörsicheren Schlüssel über eine Distanz von 23,4 km auszutauschen. Als Ergebnisse liegen nun sowohl bei Alice als auch bei Bob eine Reihe von identischen Dateien vor, die den erzeugten Schlüssel enthalten. Einige Ergebnisse sind in Tabelle (4.4.3) zusammengefaßt.

Die Fehlerrate des Rohschlüssels beträgt etwa 4-6% und es wurden Übertragungsraten für den Rohschlüssel um etwa 1 kbit/s erreicht. Dabei sind fehlerhafte Blöcke nicht in die Berechnung mit eingegangen. Bei diesen Blöcken konnte keine Synchronisation von Sender und Empfänger erreicht werden. Dies ist jedoch keine physikalische Barriere, sondern ein Problem der aktuellen Implementierung der Software.

Photonen pro Puls	Roh-schlüssel-rate (bit/s)	Hinter-grund-rate (s^{-1})	Bit-fehler-rate (%)	Fehler-korrektur-effizienz (%)	ausge-tauschter Schlüssel (bit)	Schlüssel-rate (bit/s)
0,37	2242	6268	4,11	51	9395	894
0,27	1253	5504	5,24	56	4341	566
0,18	1326	5578	4,54	51	5448	519
0,096	1314	4516	4,77	56	5399	524
0,096	1136	4510	5,05	60	21284	431
0,081	1064	4474	5,81	49	3799	351
0,081	1113	4360	5,38	60	21896	431

Durch die Korrektur solch eines Fehlers reduziert sich die Größe des Schlüssels auf etwa die Hälfte. Die Schlüsseldateien wurden mit Intensitäten zwischen 0,081 und 0,37 Photonen pro Puls erzeugt.

4.5 Auswertung

Einer der Schwachpunkte ist bestimmt die relativ geringe Übertragungsrate von etwa 1 kbit/s, die in erster Linie durch die Verluste entlang des gesamten Aufbaus entstehen, so daß von den 10^6 losgesandten Photonen nur noch einige 10^3 Photonen pro Sekunde detektiert werden. Davon wird anschließend die Hälfte aufgrund falscher Meßbasis verworfen und dann nocheinmal etwa die Hälfte zur Fehlerkorrektur verwendet. Hier eine kurze Skizze, an welchen Stellen die Verluste auftreten, bzw. wie groß die Transmissionskoeffizienten der einzelnen Abschnitte sind:

1. Transmission durch das Sendeteleskop:	0,85
2. Transmission durch die Atmosphäre:	0,5
3. vom Empfangsteleskop geometrisch aufgesammelter Bruchteil:	0,04
4. Transmission durch das Empfangsteleskop:	0,5

5. Transmission durch die Filter:	0,76
6. Transmission durch die Polarisationsoptik:	0,92
7. Effizienz der APD:	0,45

Es ist zu beachten, daß sowohl die Absorption durch die Atmosphäre starken Schwankungen unterlegen ist und auch die Aufsammeleffizienz des Teleskops von der Größe des Strahls abhängt, so daß Position 2 und 3 nur als grobe Werte verstanden werden dürfen.

Die Transmissionswerte der Teleskope, Filter und Polarisationsoptik (1,4,5,6) wurden unter Laborbedingungen gemessen, wie auch die Quanteneffizienz (7) der SiAPD, wobei nicht die selben, sondern andere baugleiche Dioden verwendet wurden. Der geometrisch vom Empfänger erfaßte Bruchteil des Lichtstrahls (3) läßt sich aus der Appertur des Teleskops und Beobachtung des Strahldurchmessers berechnen.

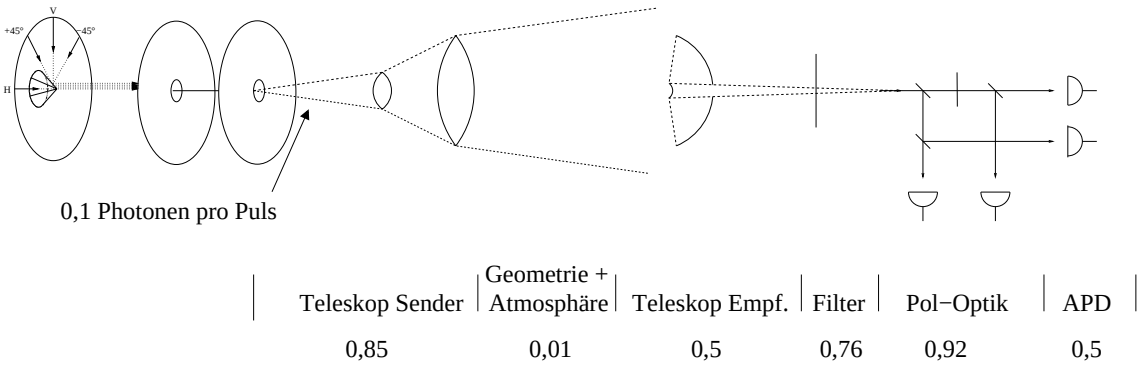
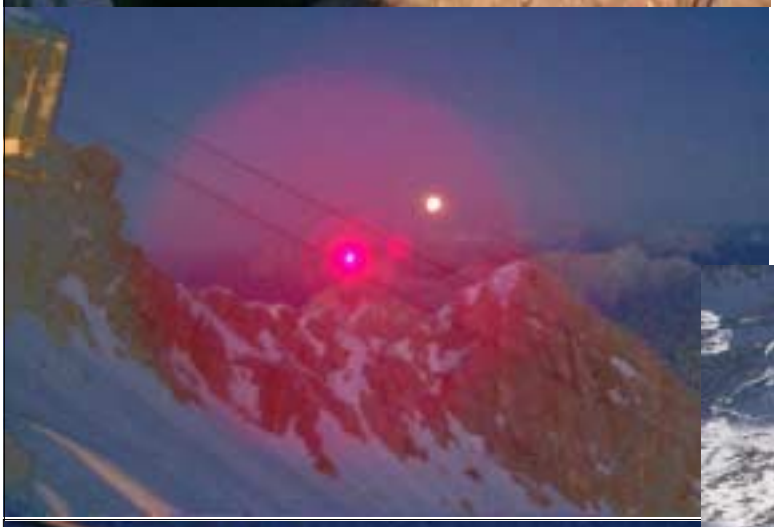


Abbildung 4.18: Transmissionsraten entlang der Übertragungsstrecke

Die relativ schlechte Transmission von 0,5 für das Empfangsteleskop kommt daher, daß es sich um ein kommerzielles Modell handelt, das für sichtbares Licht spezifiziert ist und nicht für den nahen IR-Bereich.

Größenordnungsmäßig ergibt sich über die gesamte Länge dieses Quantenkanals vom Ausgang der Sendeeinheit bis zu den Detektoren der Empfangseinheit eine Abschwächung von etwa 1/500 (27 dB).

oben:
Der Sender ausgerichtet
auf das Karwendel



mitte:
Empfänger und
Mond von der
Zugspitze aus gesehen

unten links:
das Sendemodul

unten rechts:
Sender auf das Stativ
montiert

oben links:
Das Empfangsteleskop

oben rechts:
Die Hütte auf der Zugspitze

mitte:
Das Modul zur Polarisationsanalyse

unten:
Die Zugspitze durch das Empfangsteleskop betrachtet

4.6 Ein kurzer Ausblick

Um nun eine höhere Übertragungsrate zu erreichen, stehen Verbesserungen in einigen Teilen an. So wäre beispielsweise einer der ersten Schritte der Einsatz einer besseren Teleskopoptik auf beiden Seiten, um sowohl den von Alice erzeugten Fleck noch kleiner als die aktuellen 1,25 m zu bekommen, wie auch die von Bob aufgesammelte Lichtmenge zu erhöhen.

Ein weiterer Schritt wird die Verwendung eines Quantenzufallszahlengenerators sein, der die augenblicklich noch verwendete Binärdatei des Senders ablöst. Mit diesem Generator ist es möglich, die benötigten Zufallszahlen in einem Takt von 20 MHz zu erzeugen. Da die Geheimhaltung dieser Zahlen essentiell für die Sicherheit des Verfahrens ist, könnten diese erst kurz vor der Verwendung erzeugt und sofort danach wieder vernichtet werden.

Einer der größten Nachteile sowohl dieses Systems, wie auch aller anderen Freiraum- und Glasfaseranwendungen, ist die räumliche Begrenzung der Übertragungstrecke. So wird es kaum möglich sein, viel mehr als 100 km zu überbrücken.

Quantenkryptographische Kommunikation über längere Distanzen oder gar weltweit ist damit noch nicht möglich. Es gibt aber Vorschläge, Satelliten beim Schlüsselaustausch einzusetzen. Der Absender vereinbart dabei mit dem Satelliten einen Schlüssel, den dieser dann an jedem Ort der Erde erneut mit dem Empfänger austauschen kann. Somit besitzen ihn wiederum ausschließlich diese beiden Parteien. Da der Schlüssel in klassischer Form im Satelliten vorliegt, muß dieser als ebenso sicher gelten wie Alices und Bobs Anlagen, und er darf nicht abgehört werden können. Obwohl die Abschwächung durch die Atmosphäre eher kleiner als in unserem Experiment sein wird, ist vor allem eine effiziente Kopplung wegen der großen Entfernung von 1000 km nur mit aufwendiger Optik möglich.

Eine andere Anwendung für Systeme wie in diesem Experiment stellt die Kommunikation in einem Umkreises von weniger als 100 km dar, wie etwa in Ballungsräumen. Hier ist ein abhörsicherer Informationsaustausch beispielsweise zwischen Bankfilialen oder Geschäftspartnern innerhalb einer Stadt möglich.

5 Glossar

5.1 Quantentheorie

Hier eine kurze Einführung in die Quantenmechanik, wie sie zum besseren Verständnis der Quantenkryptographie hilfreich ist.

5.1.1 Grundzüge der Quantenmechanik

Der quantenmechanische Zustand eines physikalischen Systems zur Zeit t kann durch die Zustandsfunktion $|\Psi(t)\rangle$ beschrieben werden, die das Element eines Hilbertraumes $\boldsymbol{\mathcal{H}}$ darstellt. Jede meßbare physikalische Größe α entspricht einem (linearen hermiteschen) Operator $\mathbf{A}$. Ein Zustand $|\Psi(t)\rangle$ des Systems, in dem die Größe α einen scharfen Wert a_n annimmt, muß durch eine Eigenfunktion $|u_n\rangle$ des entsprechenden Operators beschrieben sein. Die Werte a_n sind die zugehörigen Eigenwerte und die einzig möglichen Resultate dieser Messung bzgl. des Operators $\mathbf{A}$.

$$\mathbf{A}|u_n\rangle = a_n|u_n\rangle \tag{5.1}$$

Bilden diese Eigenvektoren $|u_n\rangle$ eine Eigenbasis im Hilbertraum $\boldsymbol{\mathcal{H}}$ mit den zugehörigen Eigenwerten a_n, so nennt man $\mathbf{A}$ eine Observable $\hat{\mathbf{A}}$.

Jeder Zustand $|\Psi(t)\rangle$ kann nun als additive Superposition von Basisvektoren, also Eigenvektoren $|u_n\rangle$ dargestellt werden,

$$|\Psi\rangle = \sum_n c_n|u_n\rangle \tag{5.2}$$

wobei die Dimension n dieser Eigenbasis die Anzahl der möglichen Meßergebnisse a_n angibt.

Bei der Messung der Observablen $\hat{\mathbf{A}}$ an einem System im Zustand $|\Psi(t)\rangle$ ist die Wahrscheinlichkeit, den Eigenwert a_n zu messen, durch

$$P(a_n) = |\langle u_n|\Psi\rangle|^2 \tag{5.3}$$

gegeben. Bei mehrmaliger Wiederholung dieser Messung erhält man eine Wahrscheinlichkeitsverteilung der Eigenwerte a_n, woraus sich der Mittelwert $\langle\hat{\mathbf{A}}\rangle$ der Meßergebnisse

der Observablen $\hat{\mathbf{A}}$ mit

$$\langle \hat{\mathbf{A}} \rangle = \sum_n a_n |c_n|^2 \tag{5.4}$$

ergibt. Weiter läßt sich die Standardabweichung $\Delta\hat{\mathbf{A}}$ der Meßergebnisse dieser Wahrscheinlichkeitsverteilung durch

$$\Delta\hat{\mathbf{A}} = \sqrt{\hat{\mathbf{A}}^2 - \langle \hat{\mathbf{A}} \rangle^2} \tag{5.5}$$

bestimmen, welche ein Maß für die Verteilung der Meßergebnisse um den Mittelwert $\langle \hat{\mathbf{A}} \rangle$ ist. Für den Fall, daß $|\Psi\rangle = |u_n\rangle$ ein Eigenvektor zu $\mathbf{A}$ ist, stimmen Erwartungswert und Meßergebnis stets überein.

5.1.2 Gleichzeitige Meßbarkeit und Kommutatoren

Was passiert nun, wenn man bei einer zweiten Messung an dem gleichen Zustand eine andere Observable $\hat{\mathbf{B}}$ untersucht?

Für den Fall, daß $\mathbf{A}$ und $\mathbf{B}$ die selben Eigenvektoren $|u_n\rangle$ besitzen, gilt

$$\mathbf{AB}|u_n\rangle = a_n b_n |u_n\rangle = \mathbf{BA}|u_n\rangle \tag{5.6}$$

Für zwei Operatoren $\mathbf{A}$ und $\mathbf{B}$ ist der Ausdruck $(\mathbf{AB} - \mathbf{BA})$ als der Kommutator $[\mathbf{A},\mathbf{B}]$ definiert. Ist dieser Null, so sagt man, sie *kommutieren*, und beide Größen können gleichzeitig exakt gemessen werden. Das Produkt der Standardabweichungen zweier kommutierender Operatoren verschwindet.

$$\Delta\mathbf{A}\Delta\mathbf{B} = 0 \tag{5.7}$$

Haben die beiden Operatoren aber unterschiedliche Eigenvektoren, so kommutieren $\mathbf{A}$ und $\mathbf{B}$ nicht.

$$[\mathbf{A},\mathbf{B}] = i\,\mathbf{C} \neq 0, \tag{5.8}$$

Man kann zeigen, daß das Produkt der Unschärfen der beiden

Operatoren ein bestimmte Grenze nicht unterschreiten darf:

$$\Delta\mathbf{A}\Delta\mathbf{B} \geq \frac{|\langle \mathbf{C} \rangle|}{2} \tag{5.9}$$

Wobei sich der Wert $|\langle \mathbf{C} \rangle|$ aus (5.8) bestimmen läßt. Betrachtet man nun beispielsweise statt $\mathbf{A}$ und $\mathbf{B}$ den Ortsoperator $\mathbf{Q}{=}x$ und den Impulsoperator $\mathbf{P}{=}\ i\hbar\ \delta/\delta x$, so erhält man die *Heisenberg'sche Unschärferelation*:

$$\Delta\mathbf{Q}\Delta\mathbf{P} \geq \frac{\hbar}{2} \tag{5.10}$$

Je genauer man also den Ort eines Teilchens bestimmt, desto unschärfer wird eine gleichzeitig durchgeführte Impulsmessung und umgekehrt.

Nehmen wir nun beispielsweise zwei nicht kommutierende Operatoren **U** und **V** in einem 2-Zustands-System mit den zugehörigen orthogonalen Eigenvektoren $|u_n\rangle$ und $|v_n\rangle$, so nehmen diese Vektoren im Hilbertraum $\mathcal{H}$ einen Winkel $\alpha \neq 0$ ein. Eine Messung des Zustandes $|u_n\rangle$ mit dem Operators **V** stellt eine Projektion von $|u_n\rangle$ auf die Eigenbasis $|v_n\rangle$ dar. Die Wahrscheinlichkeit, dabei das Ergebnis $|v_1\rangle$ zu erhalten ist durch

$$P_1 = P(|v_1\rangle||u_1\rangle) = |\langle u_1|v_1\rangle|^2 = |\cos(\alpha)|^2 = \cos^2(\alpha) \tag{5.11}$$

gegeben, und analog dazu ist die Wahrscheinlichkeit, $|v_2\rangle$ zu erhalten

$$P_2 = P(|v_1\rangle||u_2\rangle) = |\langle u_2|v_1\rangle|^2 = |\sin(\alpha)|^2 = sin^2(\alpha). \tag{5.12}$$

Für die Wahl von $\alpha = \frac{\pi}{4}$ ist $P_1 = P_2 = \frac{1}{2}$, der Zustand $|u_n\rangle$ wird also absolut zufällig als $|v_1\rangle$ oder $|v_2\rangle$ detektiert, und es läßt sich keinerlei Aussage über den ursprünglichen Zustand machen.

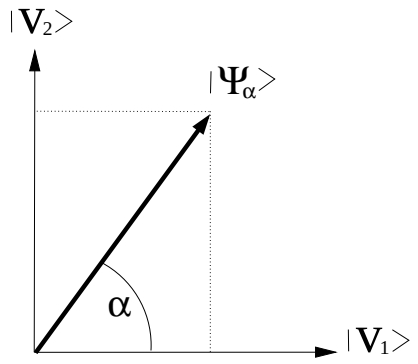


Abbildung 5.1: Messung des Vektors $|\psi_\alpha\rangle$ in der **V**-Basis

5.1.3 Der Polarisationzustand des Lichts

Nehmen wir nun als physikalisches System Photonen, also einzelne Lichtquanten, und als deren Zustand die Polarisation. Die Basis **B** für polarisiertes Licht ist 2-dimensional, wobei die orthogonalen Basisvektoren $|u_1\rangle$ und $|u_2\rangle$ seien. Ein im Winkel α zur Basis **B** linear polarisiertes Photon läßt sich also durch

$$|\Psi_\alpha\rangle = \cos(\alpha)|u_1\rangle + \sin(\alpha)|u_2\rangle \tag{5.13}$$

beschreiben. Nimmt man an solch einem linear polarisierten Photon eine Polarisationsmessung vor, so wird diese durch den Operator **M** beschrieben. Dabei wird in einer Basis im Winkel δ mit einem idealen Detektor der Effizienz 1 gemessen.

Für die Eigenbasis $(|v_{1\delta}\rangle, |v_{2\delta}\rangle)$ mit

$$|v_{1\delta}\rangle = \begin{pmatrix} \cos(\delta) \\ \sin(\delta) \end{pmatrix}, \ |v_{2\delta}\rangle = \begin{pmatrix} -\sin(\delta) \\ \cos(\delta) \end{pmatrix} \tag{5.14}$$

zum Operator $\mathbf{M}_\delta$ mit

$$\mathbf{M}_\delta = \begin{pmatrix} \cos(2\delta) & \sin(2\delta) \\ \sin(2\delta) & -\cos(2\delta) \end{pmatrix} \tag{5.15}$$

gilt dann die Eigenwertgleichung

$$\mathbf{M}_\delta |v_{n\delta}\rangle = m_{n\delta} |v_{n\delta}\rangle$$

wobei die Eigenbasis $(|v_{1\delta}\rangle, |v_{2\delta}\rangle)$ von $\mathbf{M}_\delta$ gegenüber der Basis $\mathbf{B}$ einen Winkel δ einnimmt.

Die zugehörigen Eigenwerte sind

$$m_{1\delta} = +1, \ m_{2\delta} = -1$$

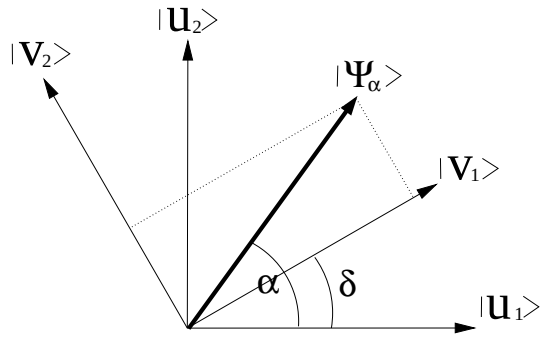


Abbildung 5.2: Messung eines im Winkel α polarisierten Photons $|\psi_\alpha\rangle$ in einer um den Winkel δ rotierten Basis

Für die Analyse eines linear α-polarisierten Photons in der Basis δ ergibt sich eine Detektionswahrscheinlichkeit von

$$P_{\alpha\delta}(+1) = |\langle v_{1\delta}|\Psi_\alpha\rangle|^2 =$$

$$= \left| \begin{pmatrix} \cos(\delta) \\ \sin(\delta) \end{pmatrix} (\cos(\alpha), \sin(\alpha)) \right|^2 =$$

$$= |\cos(\delta)\cos(\alpha) + \sin(\delta)\sin(\alpha)|^2 = \tag{5.16}$$

$$= |\cos(\alpha - \delta)|^2 =$$

$$= \cos^2(\alpha - \delta) \ .$$

Im Fall $\alpha = \delta$ stimmt die Polarisationsachse des Photons mit der des Analysators überein und es ergibt sich eine Detektionswahrscheinlichkeit von 1. Stehen die beiden Achsen senkrecht zueinander ($\delta = \alpha + \frac{\pi}{2}(2k+1)$ mit $k \in \mathbb{N}_\circ$), so ist sie 0. Schließen die Achsen einen Winkel von 45° ein, so ist die Detektion mit einer Wahrscheinlichkeit von $P_{45°}$=0,5 rein zufällig. Die Bestimmung der Polarisation eines Photons ist somit nicht möglich, da eine derartige Messung nur Auskunft über die Polarisation parallel und senkrecht zum Analysator gibt, aber keine eindeutige Beschreibung dieses Zustandes liefert. Eine eindeutige Aussage erhält man, wenn man die Messung unter verschiedenen Winkeln öfter wiederholt. Dann geht die Wahrscheinlichkeitsverteilung in eine Häufigkeitsverteilung über und eine quantitative Aussage wird möglich. Solch eine Messung ist in Abb.(4.2) dargestellt.

5.1.4 Der RSA-Code

Die Sicherheit des RSA-Verschlüsselungssystems (nach Roland Rivest, Adi Shamir und Leonard Adleman) basiert auf dem Problem, eine große Zahl zu faktorisieren, sie also als Produkt aller ihrer Primfaktoren darzustellen. Dieses Verfahren funktioniert wie folgt.

- Jeder Benutzer des RSA-Systems nimmt zufällig zwei große Primzahlen p und q, und eine kleine ungerade natürliche Zahl E, die zu $(p-1)$ und $(q-1)$ relativ prim ist, d.h. $ggT(E,(p-1)(q-1)) = 1$. p und q sind nur dem Empfänger einer Nachricht bekannt, während ihr Produkt $n = p \cdot q$ zusammen mit E öffentlich bekannt gegeben werden.

- Der Absender einer Nachricht stellt diese in Dezimalzahlen dar und unterteilt sie in Blöcke $P_i, i \in \mathbb{N}$, wobei gelten muß $P_i \leq n$. Jeder Block wird in eine chiffrierte Zahl umgewandelt, indem man ihn in die E-te Potenz erhöht und modulo n reduziert, also alle
$$C_i = P_i^E mod\ n$$
bildet.

- Diese Zahlen können nun öffentlich übermittelt werden. Eine Funktion mit Exponent modulo n, läßt sich nur dann mühelos auswerten, wenn man ihren Exponenten modulo $\phi(n)$ berechnet [41], mit
$$\phi(n) = (p-1)(q-1).$$

- Nur der rechtmäßige Empfänger kennt p und q und somit $\phi(n)$ und kann damit den Dechiffrierschlüssel D mit

$$D = E^{-1} mod\ \phi(n)$$

berechnen. Damit erhebt er die C_i in die D-te Potenz und reduziert sie modulo n. Da

$$C_i{}^D mod\ n = (P_i{}^E)^D mod\ n = P_i{}^{ED} mod\ n$$

und

$$ED\ mod\ \phi(n) = 1,$$

führt die Operation $P_i^{ED} mod$ n wieder auf die P_i, also zum Klartext.

Beispiel: Wir wählen p=61 und q=97 und erhalten

$$n = p \cdot q = 5917$$

sowie

$$\phi(n) = (p-1)(q-1) = 60 \cdot 96.$$

Als E wählen wir 47, da teilerfremd zu 5760, und berechnen mit dem erweiterten *Euklidischen Algorithmus*

$$D = E^{-1} mod\ \phi(n) = 47^{-1} mod\ 5760 = 1103$$

$E = 47$ und $n = 5917$ werden als *öffentlicher Schlüssel* bekannt gegeben. Zur Verschlüsselung der Nachricht $P = 348613$ wird diese in Blöcke P_i zerlegt, die jeweils kleiner als n sind. Wir wählen als Blocklänge drei Ziffern und schreiben.

$$P_1 = 348, P_2 = 613$$

Der erste Block P_1 wird verschlüsselt mit

$$C_1 = P_1^E mod\ n = 348^{47} mod\ 5917 = 4479$$

und analog dazu der zweite. Die Chiffre lautet dann

$$C = 4479\ 1333.$$

Das Entschlüsseln des ersten Blocks P_1 ergibt

$$4479^{1103} mod\ 5917 = 348.$$

5.1.5 Doppelbrechung

Das Phänomen der Doppelbrechung tritt in optisch anisotropen Medien auf, also deren optische Eigenschaften richtungsabhängig sind. Das *Doppel-* bezieht sich dabei auf zwei verschiedene Ausbreitungsachsen, die ein Strahl abhängig von seiner Polarisation in solchen Medien nehmen kann. [42]

Entlang dieser sogenannten Hauptachsen breitet sich Licht aufgrund unterschiedlicher Brechungsindizes unterschiedlich schnell aus. Dabei muß die Ausbreitungsrichtung von Licht der jeweiligen Polarisationsrichtung mit den Hauptachsen übereinstimmen.

In unserem Fall handelt es sich um einen Quarz, bei dem die beiden Richtungen auf einer Achse liegen. Für linear polarisiertes Licht dieser Richtungen hat es keine merklichen Auswirkungen. Für eine Linearkombination aus beiden hingegen tritt am Ausgang des Quarz eine Phasendifferenz zwischen diesen auf, so daß die Kombination aus ordentlichem und außerordentlichem Strahl eine elliptische Polarisation ergibt. Dieser Quarz ist bei Bob so angeordnet, daß sich H- und V-Licht entlang den beiden Achsen ausbreitet und unverändert bleibt, Licht der 45°-Basis hingegen verdreht und somit korrigiert werden kann.

5.1.6 Sichtbarkeit

Als Sichtbarkeit S (*engl.:* visibility) einer Messung bezeichnet man das Verhältnis von größtem und kleinstem Meßwert I_{max} und I_{min} zueinander und definiert sie wie folgt:

$$S = \frac{I_{max} - I_{min}}{I_{max} + I_{min}} \tag{5.17}$$

Sie ist ein Ausdruck für die Qualität eines Meßergebnisses und kann beispielsweise zur Beurteilung der Polarisationsgüte in einem Experiment herangezogen werden. Eine Sichtbarkeit von 99% bedeutet etwa nach (5.17), daß der Bruchteil der Lichtintensität in der falschen Polarisation nur 0,5% der Gesamtintensität beträgt.

5.1.7 Astronomisches Teleskop

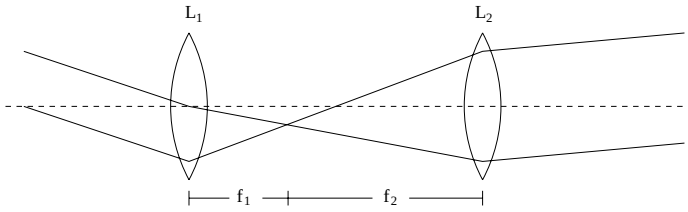


Abbildung 5.3: Teleskop nach *astronomischer* Bauart, mit Linsen L_1 und L_2 der Brennweiten f_1 bzw. f_2.

Diese Bauart für Teleskope besteht aus der Kombination zweier Linsen der Brennweiten f_1 und f_2. Die erste Linse fokussiert parallel einfallendes Licht im Abstand f_1 hinter ihrer Hauptebene. Die zweite Linse, im Abstand f_2 hinter dem Fokus, bildet diesen wiederum ins Unendliche ab, erzeugt also am Ausgang des Teleskops einen parallelen Lichtstrahl.

Literaturverzeichnis

[1] *http://www.brockhaus.de.*

[2] R. Breuer. Kryptographie. *Spektrum der Wissenschaft*, 4, 2001.

[3] D. Kahn. *The Codebreakers.* Macmillian, New York, 1967.

[4] Wolfgang Ertel. *Angewandte Kryptographie.* Fachbuchverlag Leipzig, 2001.

[5] Harald Weinfurter. *Mündliche Bemerkung*, 2002.

[6] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal of the American Institut of Electrical Engineers*, XLV:109–115, 1926.

[7] C. E. Shannon. *Bell System Technical Journal*, 28:656, 1949.

[8] W.F. Ehrsam, C.H.W. Meyer, and W.L. Tuchman. Product block cipher for data security. *U.S. Patent Nr.3,962,539*, 8. Juni 1976.

[9] RSA DES Challenge III. *http://www.rsasecurity.com/rsalabs/des3/*, 1999.

[10] J. Daemen and V. Rijmen. Aes proposal: Rijendael. *http://csrc.nist.gov/encryption/aes/round2/r2algs.htm*, (NIST-AES), 1999.

[11] X. Lai, J. Massey, and I.B. Damgard. *A Proposal for a New Block Encryption Standard, Advances in Cryptology: EUROCRYPT '90, Lecture Notes in Computer Science*, volume 473, 389-404. Springer Verlag, 1990.

[12] W. Diffie and M.E. Hellman. *IEEE Trans. Information Theory*, IT-22:644, 1976.

[13] R.L. Rivest, A. Shamir, and L.M. Adleman. *Communications of the ACM*, 21:120, 1978.

[14] B. Schneier. *Applied Cryptography.* John Willey & Sons Inc., New York, 1996.

[15] J. Franke, T. Kleinjung, and F. Bahr. Neuer weltrekord bei der primfaktorzerlegung. *Mathematisches Institut der Universität Bonn*, www.heise.de/newsticker, 4.2.2002.

[16] IBM Forschungszentrum in Almaden. Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414:883.

[17] S. Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.

[18] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, pages 175–179, 1984.

[19] V. Bužek and M. Hillary. *Phys. Rev. Lett.*, 81:5003, 1998.

[20] H. Bechmann-Pasquinucci and W. Tittel. *Phys. Rev. A*, 61:062308, 2000.

[21] D.J. Meyers. Assoc. comput. math. *Los Alamos e-print archive*, quant-ph/9802025:343, 1996.

[22] N. Rosen A. Einstein, B. Podolsky. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777, 1935.

[23] A. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[24] D. Bohm. *Quantum Theorie.* Prentice-Hall, Englewood Cliffs, NJ, 1951.

[25] J.S. Bell. *On the Einstein-Podolsky-Rosen Paradox*, Physics(1):195, 1964.

[26] C. H. Bennet. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121–3123, 1992.

[27] G. Ribordy, J. Brendel, J.-D. Gaultier, N. Gisin, and H. Zbinden. *Phys. Rev. A*, 63:012309, 2001.

[28] R.J. Hughes, G.G Luther, G.L. Morgan, C.G. Peterson, and C. Simmons. Practical quantum key distribution over a 48-km optical fiber network. *Lecture Notes in Computer Sience*, 1109:329–338, 1996.

[29] Ch. Marand and P.D. Townsend. Quantum key distribution over distances as long as 30 km. *Opt. Lett.*, 20 (16):1695–1697, 1995.

[30] *www.idquantique.com.*

[31] C. E. Shannon. *Bell System Technical Journal*, 27(ibid 623):379, 1948.

[32] C.H. Bennet, G. Brassard, and J.M. Robert. Privacy amplification by public discussion. *Siam J. Comput.*, 17(2):210–229, 1988.

[33] Thorlabs Inc. *Product Catalog*, 14:168.

[34] Roithner Lasertechnik. http://www.roithner-laser.com.

[35] J. G. Rarity, P. Tapster, and P. M. Gorman. Secure key exchange over 1.9 km free-space range using quantum cryptography. *Electronics Letters*, 37(ibid Journal of Modern Optics 48, 1887 (2001)):512–514, 2001.

[36] J.G. Rarity, P.C.M. Owens, and P.R.Tapster. *J. Mod. Optics*, (41):2345, 1994.

[37] *http://www.hamamatsu.com.*

[38] *http://www.soc.soton.ac.uk/RSADU.*

[39] Zugspitze bei Garmisch-Partenkirchen. *http://www.zugspitze.de*, (2964 m ü. NN).

[40] Westliche Karwendelspitze bei Mittenwald. *http://www.karwendelbahn.de*, (2385 m ü. NN).

[41] A. Bartholome, J. Rung, and H. Kern. *Zahlentheorie für Einsteiger.* Vieweg, 1995.

[42] Klein and Furtak. *Optik*, volume 2. Springer-Lehrbuch, 1988.

Dankeswort

Mein Dank zum Gelingen dieser Arbeit sowie meines bisherigen Studiums gilt u.a.:

Prof. Dr. Harald Weinfurter für die Aufnahme in seine Gruppe, die Ermöglichung von einigen interessanten Konferenzbesuchen, sowie den gelungenen Kompromiß aus Unterstützung und selbständigem Arbeitenlassen.

Dr. Christian Kurtsiefer dafür, daß ich an diesem Experiment mitarbeiten durfte, interessante Reisen, viele Wochen auf dem Gipfel der Zugspitze und Unterstützung bei dieser Arbeit.

Patrick Zarda für unterhaltsames Arbeiten in Labor und auf der westlichen Karwendelspitze.

Jürgen Volz für selbstlose Hilfe bei meinem Kampf mit dem Computer.

Meiner Schwester Mechthild, daß sie Jürgen mit Kuchen bei Laune gehalten hat.

Meinen reizenden Mitbewohnerinnen für die Nachsicht in der Haushaltführung während der Anfertigung dieser Arbeit.

Meinen Eltern, die mir das Studium ermöglichen.

Allen übrigen Mitgliedern unserer Gruppe, Karen Sauke, Mohammed Bourenanne, Manfred Eibl, Sascha Gärtner, Nikolai Kiesel, Oliver Schulz und Markus Weber für die lustigen Monate gemeinsamen Arbeitens,

sowie allen übrigen Freunden, Bekannten und Kollegen die noch nicht erwähnt wurden, aber trotzdem zur Fertigstellung dieser Arbeit beitrugen.

Erklärung

Hiermit erkläre ich, die vorliegende Arbeit selbständig verfasst und nur die angegebenen Quellen und Hilfsmittel verwendet zu haben.

München, den 3. April 2002

Matthäus Halder