Quantenkryptographie

Ein Experiment im Vergleich

Diplomarbeit
zur Erlangung des Grades eines Magisters
an der
Naturwissenschaftlichen Fakultät
der Universität Innsbruck

eingereicht von
Patrick Zarda
im September 1999

durchgeführt am Institut für Experimentalphysik
der Universität Innsbruck
bei
Prof. Dr. Harald Weinfurter

Inhaltsverzeichnis

1. Einleitung

> **Quantenkryptographie** *ist eine neue kryptographische Methode, basierend auf den Grundgesetzen der Quantenmechanik, mit der zwei Personen über eine direkte Verbindung 100% abhörsicher einen Schlüssel vereinbaren können, welcher dann zur geheimen Kommunikation verwendet werden kann.*

Das erste 1989 realisierte Quantenkryptographie-Experiment konnte in eindrucksvoller Weise das prinzipielle Funktionieren der Quantenkryptographie zeigen. Seit dieser Zeit wurden einige weitere Quantenkryptographie-Experimente aufgebaut, um neue Schemas zu testen und bestehende Aufbauten zu verbessern. In der Quantenkryptographie ist jetzt aber sicher die Zeit reif, um funktionierende und ausreichend getestete Schemas so zu modifizieren und zu verbessern, dass sie in naher Zukunft als Prototypen für eine baldige Anwendung verwendet werden können. Die Anforderungen an eine derartige Apparatur sind klar: Neben einer hohen Übertragungsrate und einer verschwindenden Fehlerrate sollte ein derartiges Gerät möglichst kompakt und handlich sein. Die Anwenderfreundlichkeit bedingt weiters Kriterien wie minimaler bzw. wegfallender Justieraufwand vor und während der Übertragung und natürlich eine benutzerfreundliche Schnittstelle zum Anwender (PC mit einfacher Software). Weiters sollte die Länge der Übertragungsstrecke möglichst groß sein.

Nachdem wir uns für ein bestimmtes Quantenkryptographie-Schema entschlossen hatten, konnten wir uns, unter Berücksichtigung der oben angeführten Anforderungen, an die Wahl der für das Experiment notwendige Komponenten machen. Wesentliche Elemente dabei sind der PC, die Elektronik, die optischen Komponenten und alle Schnittstellen zwischen diesen Komponenten.

Das gesamte Projekt läuft dann in mehreren Schritten ab, wobei die erste Stufe im Testen und Ausmessen der einzelnen später im Experiment verwendeten Komponenten besteht. Gleichzeitig werden auch die ausgewählten Schnittstellen zwischen den Komponenten getestet. Nach Auswertung der Daten wird entschieden, ob diese Komponenten den Anforderungen entsprechen und falls nötig wird dann eine andere Auswahl getroffen oder anderweitig optimiert.

Im zweiten Schritt wird mit den ausgewählten Komponenten ein erstes funktionierendes Experiment aufgebaut. Dabei muss darauf geachtet werden, dass die einzelnen Komponenten jederzeit austauschbar bzw. variierbar sind, um so das optimale Zusammenspiel eruieren zu können.

Alle aus den ersten beiden Schritten des Projekts gewonnenen Erkenntnisse können dann in der dritten Stufe des Experiments verwendet werden. Dabei wird der Aufbau des Experiments vor allem in Bezug auf die Kompaktheit verbessert. Alle optimalen Einstellungen des vorangegangenen Experiments werden in diesen Aufbau fix implementiert.

Im letzten Schritt kann dann ein Layout für einen Prototypen eines „Quantenkryptographie-Modems“ entworfen werden.

Im Rahmen meiner Diplomarbeit sollten die ersten zwei Schritte des Projektes realisiert werden. In dieser Niederschrift meiner Arbeit folgt einem einführenden Teil über Kryptographie und deren Geschichte ein Kapitel, welches die grundlegenden Voraussetzungen zum Verstehen der Quantenkryptographie beinhaltet. Anschließend wird das Experiment in allen seinen Details beschrieben und die Messergebnisse präsentiert. Vor der Zusammenfassung der Arbeit ist noch ein Kapitel, welches einen Vergleich mit anderen zur Zeit laufenden oder kürzlich abgeschlossenen Quantenkryptographie-Experimenten anstellt. Das Literaturverzeichnis, eine Plänesammlung und das Nachwort bilden den Abschluss der Diplomarbeit.

2. Klassische Kryptographie

In diesem Kapitel werden zuerst die Grundbegriffe der Kryptographie sowie die Methoden und Algorithmen der verschiedenen Ver- und Entschlüsselungstechniken erklärt. Der anschließende historische Abriß zeigt die geschichtliche Entwicklung der klassischen Kryptographie auf und im letzten Abschnitt dieses Kapitels werden die momentan verwendeten Methoden angeführt.

2.1. Grundbegriffe

Alle für die geheime Übertragung von Nachrichten verwendeten Verschlüsselungstechniken werden in dem Begriff *Kryptographie* (griechisch: $\kappa\rho\upsilon\pi\tau\circ\sigma$ = geheim; $\gamma\rho\alpha\phi\epsilon\iota\nu$ = schreiben) zusammengefaßt. Unter Verwendung bestimmter Algorithmen übersetzen diese Techniken eine Nachricht aus einer allgemein lesbaren Form in eine verschlüsselte Zeichenfolge, welche nur vom Empfänger gelesen werden kann und für Dritte möglichst nicht entschlüsselbar sein soll.

Alle Techniken, welche ein Abhörer anwendet, um eine geheime Botschaft zu entschlüsseln, werden in dem Begriff *Kryptoanalyse* vereinigt.

Der Überbegriff für alle Methoden der Kryptographie und Kryptoanalyse ist *Kryptologie* (griechisch: $\lambda\circ\gamma\circ\sigma$ = Sinn).

Die ursprüngliche Form einer geheim zu sendenden Nachricht wird als *Klartext* m *(message)* bezeichnet, welcher nach Anwendung einer *Chiffrierung* oder *Verschlüsselung* zu einem *Geheimtext* oder *Chiffre* c wird. Ein bei bestimmten Algorithmen notwendiger *Schlüssel* wird mit k *(key)* bezeichnet.

Die Algorithmen der Verschlüsselung lassen sich in zwei Gruppen einteilen:

2.1.1. Transpositionsalgorithmen

Bei einem *Transpositionsalgorithmus* bleiben die Klartextzeichen erhalten und werden nach einer bestimmten, geheimen Regel umgeordnet. Eine solche Regel kann zum Beispiel vorschreiben, jeweils zwei aufeinander folgende Zeichen zu vertauschen. Aus dem Klartext „CODEWORT ROTE AMEISE“ würde dabei der Geheimtext „OCEDOWTR ORET MAIEES“ entstehen. Der Empfänger, welcher die Vertauschungsvorschrift kennt,

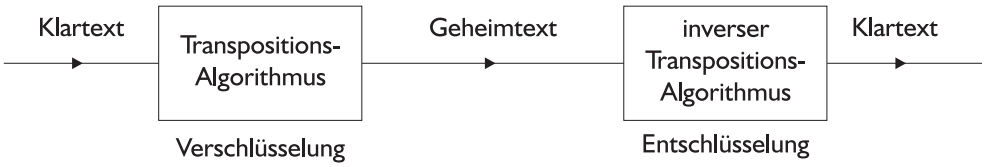


Abbildung 2.1.: Kryptographie mit Transpositionsalgorithmus

kann daraus sehr einfach den Klartext wiedergewinnen. Das Schema dieses Transpositionsalgorithmus ist in Abbildung 2.1 graphisch dargestellt.

Eine derartig verschlüsselte Nachricht ist jedoch relativ einfach zu knacken. Die Entschlüsselung wird unwesentlich schwieriger, wenn die Vertauschungsvorschrift komplizierter wird. Als Beispiel sei hier die *Skytale* (siehe Abbildung 2.2) erwähnt, welche bereits 500 vor Christus (siehe auch Kapitel 2.2 auf Seite 10) von den Griechen verwendet wurde. Bei dieser Verschlüsselungsmethode wurde ein Lederband spiralförmig um einen runden

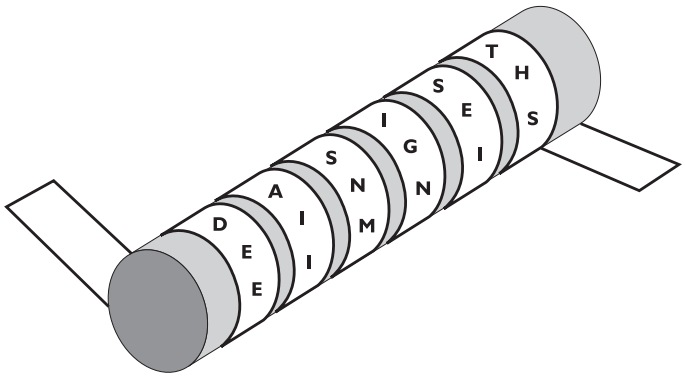


Abbildung 2.2.: Skytale - Transpositionsalgorithmus

Holzstab definierten Durchmessers gewickelt und die Nachricht dann mehrzeilig entlang der Längsachse des Holzstückes notiert. Aus dem Klartext „DASISTEINGEHEIMNIS“ entstand somit auf dem abgewickelten Leder der Geheimtext „EEDIIAMNSNGIIESSHT“. Das Band wurde dann als Gürtel getarnt zu seinem Bestimmungsort gebracht, an dem der Empfänger mit einem Stab gleichen Durchmessers die Nachricht wieder lesen konnte.

2.1.2. Substitutionsalgorithmen

Bei einem *Substitutionsalgorithmus* wird jedes Klartextzeichen an der gleichen Stelle durch ein anderes ersetzt. Dieses Chiffrezeichen wird mit einem Schlüssel und unter Verwendung einer meist einfachen mathematischen Funktion aus dem Klartextzeichen

generiert. Ein wesentlicher Unterschied zu den Transpositionsalgorithmen besteht darin, dass zur Verschlüsselung des Klartextes und zur Entschlüsselung des Geheimtextes bei den Substitutionsalgorithmen ein Schlüssel vorhanden sein muss (siehe Abbildung 2.3). Im Allgemeinen muss bei Transpositionsalgorithmen der Algorithmus selbst geheim bleiben, wobei bei Substitutionsalgorithmen die Methode allgemein bekannt sein kann und eben nur der Schlüssel geheim gehalten werden muss. Bei den Substitutionsalgorithmen

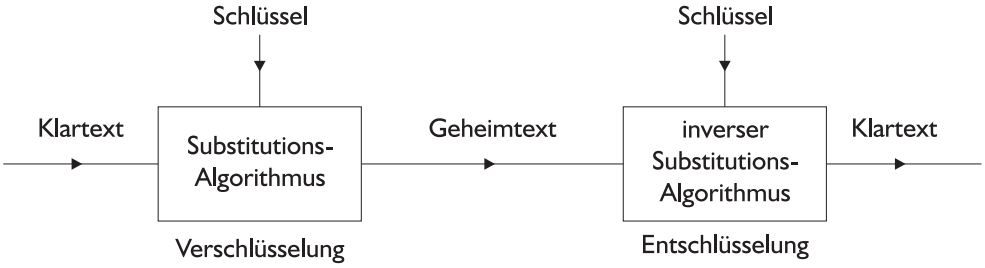


Abbildung 2.3.: Beim Substitutionsalgorithmus ist ein gemeinsamer Schlüssel notwendig.

wird je nach Schlüssel zwischen den folgenden beiden Methoden unterscheiden.

Monoalphabetischer Substitutionsalgorithmus

Beim *monoalphabetischen Substitutionsalgorithmus* (auch *Cäsar Code* genannt; vergl. Kapitel 2.2 auf Seite 10) besteht der Schlüssel aus einem einzigen Zeichen. Dieses Schlüsselzeichen wird mit jedem Klartextzeichen verknüpft und ergibt somit ein Geheimtextzeichen. Ersetzt man zum Beispiel jeden Buchstaben des Klartextes m durch eine Zahl die seine Position im Alphabet bezeichnet (also A≡1, B≡2, C≡3,...usw.) und wählt ein Schlüsselzeichen k aus dem Alphabet, dann kann der monoalphabetische Substitutionsalgorithmus als

$$c_i = (m_i + k) \bmod N \tag{2.1}$$

geschrieben werden, wobei in diesem Fall $N = 26$ ist, entsprechend der Anzahl der Buchstaben im Alphabet. Der Index i geht dabei von 1 bis L (Anzahl Klartextzeichen). Die so berechneten Zahlen werden wieder entsprechend durch Buchstaben ersetzt. Die somit gewonnene Zeichenkette ist der Geheimtext c. In Abbildung 2.4 ist ein Beispiel für einen monoalphabetischen Substitutionsalgorithmus angeführt. Die Kryptoanalyse eines derartig verschlüsselten Textes ist wiederum relativ einfach. Wenn der Abhörer weiß, dass es sich um einen deutschen Text handelt, kann dieser mit einer einfachen Untersuchung der Buchstabenhäufigkeit im Chiffre den am häufigsten auftretenden Buchstaben ermitteln. Ist der Text lange genug, kann mit großer Wahrscheinlichkeit geschlossen werden, dass es sich dabei um die Buchstaben „e“ bzw. „n“ handelt, da beide Buchstaben mit einer Häufigkeit von $\geq 9,7\%$ in der deutschen Sprache vorkommen. Die Differenz zwischen

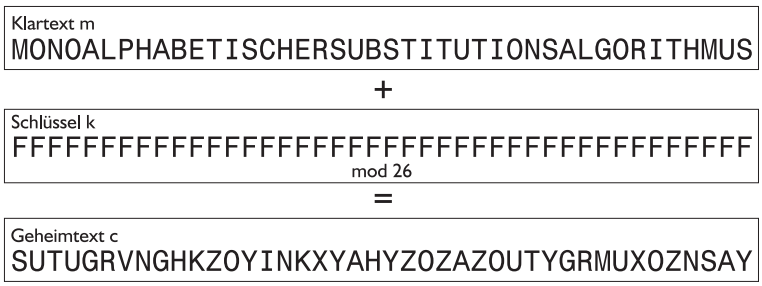


Abbildung 2.4.: Monoalphabetischer Substitutionsalgorithmus mit Schlüssel „F“

Klartextzeichen und Geheimtextzeichen ist dann das Schlüsselzeichen. In Abbildung 2.4 ist auch sehr gut zu sehen, wie alle drei Buchstaben „T“ bei „...TITUT...“ Klartextes in das Geheimtextzeichen „Z“ verwandelt werden. Eine noch einfachere Variante der Kryptoanalyse besteht im Ausprobieren aller möglichen 26 Schlüsselzeichen.

Etwas schwieriger zu entschlüsseln ist die Methode, bei der jedem Klartextbuchstaben ein eindeutiger Geheimtextbuchstabe zugeordnet wird, jeder Buchstabe somit ein eigenes Schlüsselzeichen erhält. Die oben angeführten Attacken werden dann wirkungslos.

Polyalphabetischer Substitutionsalgorithmus

Beim *polyalphabetischen Substitutionsalgorithmus* wird anstelle von nur einem Schlüsselzeichen ein ganzes *Schlüsselwort* verwendet. Dieser Schlüssel wird dann so oft hintereinander gereiht, bis er die gleiche Länge wie der zu verschlüsselnde Klartext hat (Vignére-Chiffre; siehe auch Kapitel 2.2 auf Seite 10). Dadurch werden Entschlüsselungsmethoden wie die der Untersuchung der Buchstabenhäufigkeit zwecklos. Wie in Abbildung 2.5 zu erkennen ist, wird die Stelle „...TITUT...“ des Klartextes zu „...LCAZB...“, wobei der Klartextbuchstabe „T“ im Geheimtext ein jeweils anderer ist. Allerdings kann

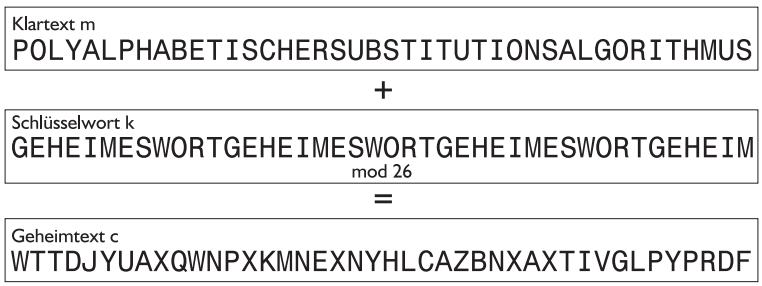


Abbildung 2.5.: Polyalphabetischer Substitutionsalgorithmus mit Schlüsselwort „GEHEIMESWORT“

ein Abhörer den Text auf aufeinander folgende Buchstabenkombinationen untersuchen.

Wird nämlich mit einem relativ zum Klartext kurzem Schlüsselwort verschlüsselt, so ist möglich, dass Zeichenfolgen wie „ST“ und „SCH“ im Deutschen oder „TH“ und „HE“ im Englischen mit dem gleichen Teil des Schlüsselwortes chiffriert werden und so dem Abhörer eine Hilfe geben.

Daraus wird ersichtlich, dass mit zunehmender Länge des Schlüsselwortes diese Methode sicherer wird.

2.1.3. Code nach Vernam

Eine Verallgemeinerung des vorhin erwähnten Vignére-Chiffre stellt ein nach dem Amerikaner G. S. Vernam [1](siehe auch Kapitel 2.2 auf Seite 11) benanntes System dar. Der *Code nach Vernam* schreibt einen Schlüssel vor, welcher

- zufällig erzeugt wird,
- die gleiche Länge wie der Klartext hat
- und nur einmal zum Verschlüsseln einer Nachricht verwendet wird.

Der Code nach Vernam ist in der Abbildung 2.6 schematisch dargestellt. Ist die absolute Geheimhaltung des Schlüssels gewährleistet, so kann dieses System als 100%ig abhörsicher bezeichnet werden. Der in Gleichung 2.2 dargestellte Verschlüsselungsvor-

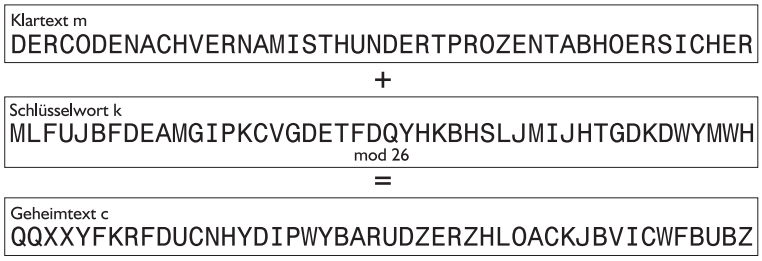


Abbildung 2.6.: Code nach Vernam mit zufällig erzeugtem Schlüsselwort

gang gleicht dem des monoalphabetischen Substitutionsalgorithmus (Gleichung 2.1) bis auf den wesentlichen Unterschied, dass hier jedem Klartextzeichen m_i ein eigenes, zufällig erzeugtes Schlüsselzeichen k_i zugeordnet ist.

$$c_i = (m_i + k_i) \bmod N \tag{2.2}$$

Für die Kryptoanalyse kann ein Abhörer nur alle 26^L möglichen Schlüssel ausprobieren, was selbst bei einer relativ kurzen Nachricht von 70 Zeichen dem Testen mit 10^{99} Schlüsseln gleichkommt. Das Resultat dabei ist aber auch nur wieder jede mögliche und sinnvolle Nachricht bestehend aus 70 Zeichen. Das wiederum ist gleichzusetzen mit dem einfachen Erraten der Botschaft.

In der Praxis wird diese Methode fast nie verwendet, weil die Erzeugung und vor allem die sichere Verteilung eines geheimen und sehr langen Schlüssels aufwendig ist. Die Quantenkryptographie erlaubt jedoch eine Schlüsselvereinbarung zwischen Sender und Empfänger über einen direkten Verbindungskanal, deren Sicherheit und Vertraulichkeit basierend auf physikalischen Gesetzen überprüft werden kann. Sie bildet daher die ideale Ergänzung zum Code nach Vernam und ermöglicht beweisbar abhörsichere Kommunikation.

2.1.4. Asymmetrische Algorithmen

Alle bisher vorgestellten Algorithmen gehören zur Gruppe der *symmetrischen Algorithmen*. Das bedeutet vereinfacht, dass beim Ver- und Entschlüsseln jeweils zueinander inverse Funktionen (siehe Gleichung 2.3; f ist hierbei die Funktion, welche m verschlüsselt und die inverse Funktion f^{-1} entschlüsselt das Chiffre wieder zu m) verwendet werden. Wird dabei ein Schlüssel k verwendet, so ist dieser beim Ver- und Entschlüsseln der Gleiche.

$$f^{-1}(f(m;k);k) = m \tag{2.3}$$

Beim Transpositionsalgorithmus muss der Empfänger aller Permutationen, die der Sender vorgenommen hat, wieder rückgängig machen, also die inversen Permutationen durchführen. Beim mono- und polyalphabetischen Substitutionsalgorithmus sowie beim Code nach Vernam wird zum Verschlüsseln Klartext und Schlüssel beispielsweise addiert und beim Entschlüsseln Geheimtext und Schlüssel voneinander subtrahiert.

Der Nachteil symmetrischer Methoden liegt darin, dass für eine geheime Kommunikation zwischen n Teilnehmern zuerst $\frac{n(n-1)}{2}$ geheime Schlüssel vereinbart werden müssen. Dies macht eine derartiges geheimes Kommunikationsnetz absolut unpraktikabel.

Asymmetrische Algorithmen hingegen verwenden einen *öffentlichen Schlüssel* $(e,\ N)$, welcher allgemein zugänglich ist und der Verschlüsselung dient, und einen *privaten Schlüssel* $(d,\ N)$, der nur dem jeweiligen Besitzer bekannt ist und der Entschlüsselung dient. Die Wahl der zwei Schlüssel sowie die Ver- und Entschlüsselung läuft wie folgt ab:

- Jeder Teilnehmer wählt zwei Zahlen p und q und bestimmt daraus $N = pq$ und e teilerfremd zu $(p-1)$ und $(q-1)$. N und e bilden den öffentlichen Schlüssel.
- Die Verschlüsselungsvorschrift für jeden, der einem Teilnehmer eine Botschaft senden will, lautet $c = m^e \bmod N$, wobei die Werte e und N des jeweiligen Empfängers verwendet werden. Die zu verschlüsselnde Nachricht muss zu diesem Zeitpunkt in Form von natürlichen Zahlen $\leq N$ vorliegen (z.Bsp. jeder Buchstabe wird durch seine Ordnungszahl im Alphabet ersetzt).
- Der Empfänger bestimmt sich aus seinen gewählten Zahlen p und q weiters seine geheime Dekodierzahl d, welche die Bedingung $ed \bmod ((p-1)(q-1)) = 1$ erfüllen muss.

- Die Entschlüsselungsvorschrift für den Empfänger lautet dann $m = c^d \bmod N$. Diese Entschlüsselung kann nur vom rechtmäßigen Empfänger durchgeführt werden, weil nur dieser im Besitz der Dekodierzahl d ist.

Die Sicherheit dieses Systems beruht auf dem enormen Rechenaufwand, um die geheime Dekodierzahl d aus den Zahlen N und e, jedoch ohne Kenntnis der jeweiligen Zahlen p und q zu bestimmen. Dieser Aufwand steigt exponentiell mit der Länge des Schlüssels ($l_k = {}_2\log N$). Könnte man bei diesen Berechnungen einen Quantencomputer verwenden, würde sich der Aufwand drastisch reduzieren (nur mehr quadratische Abhängigkeit des Aufwands von l_k). Der Vorteil dieser Methode besteht nun darin, dass der Aufwand zum Chiffrieren und Dechiffrieren polynomial, der Aufwand für die Kryptoanalyse jedoch exponential mit der Zahl l_k steigt. Das Prinzip dieser RSA-Methode [2](siehe auch

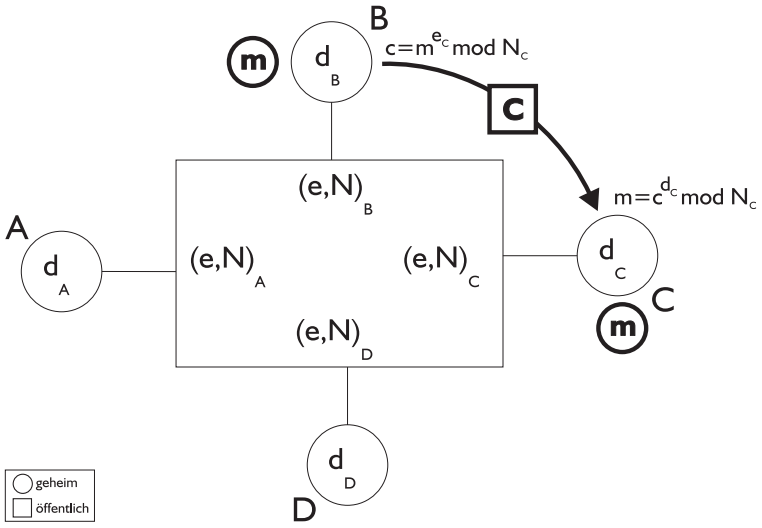


Abbildung 2.7.: RSA-Methode: geheime Kommunikation mehrerer Teilnehmer unter Verwendung öffentlicher Schlüssel

Kapitel 2.2 auf Seite 12) ist in Abbildung 2.7 noch einmal graphisch dargestellt.

2.2. Historischer Abriß

1900 v. Chr. **Hieroglyphen**
Ein ägyptischer Schreiber verwendet keine Standard-Hieroglyphen. Dies wird als erstes Dokument für niedergeschriebene Kryptographie geführt. [3] S.71

1500 v. Chr. **Geheimrezept**
Eine mesopotamische Tafel beinhaltet eine verschlüsselte Formel zur Herstellung einer Glasur für Töpfe. [3] S.75

600-500 v. Chr. **Bibel**
Teile der Originalschriften des Buches *Jeremia* wird mit einem einfachen Substitutionscode (ATBASH) verschlüsselt. Zu dieser Zeit gibt es im hebräischen einige einfache Verschlüsselungstechniken. [3] S.77

487 v. Chr. **Skytale**
Die Griechen verwenden ein einfaches „Chiffriergerät“, genannt Skytale (siehe auch Kapitel 2.1.1 auf Seite 4), dem ein Transpositionsalgorithmus zu Grunde liegt. [3] S.82

60-50 v. Chr. **Cäsar-Code**
Julius Cäsar (100-44 v. Chr.) verwendet einen einfachen Substitutionsalgorithmus (siehe auch Kapitel 2.1.2 auf Seite 5) für die Kommunikation mit seinen Legionen. [3] S.83

0-400? **Kama Sutra**
Im Kama Sutra wird Kryptographie als die 44. von 64 Künsten gelistet. Diese Kunst wird wie folgt beschrieben: *Die Kunst des Verstehens von verschlüsselten Schriften und des Schreibens von Wörtern in eigentümlicher Art.* [4]

1518 **Erstes Kryptographie Buch**
Johannes Trithemius schreibt das erste Buch über Kryptographie mit hoher Auflagenzahl. Er erfindet einen Code, bei dem jeder Buchstabe durch ein Wort ersetzt wird, wobei der entstehende Text wieder Sinn macht und so der Eindruck entsteht, dass es sich dabei nicht um ein Chiffre handelt. [3] S.130

1553 **Der Ursprung des Vignére-Codes**
Giovan Batista Belaso schlägt die mehrmalige Verwendung eines Schlüsselwortes zur Chiffrierung vor (polyalphabetischer Substitionsalgorithmus; siehe auch Kapitel 2.1.2 auf Seite 6). Dieser erste Vorschlag gerät aber in Vergessenheit und wird 22 Jahre später von Blaise de Vignére wieder aufgegriffen (siehe übernächsten Eintrag in der Zeittafel). [3] S.137

1563 **Klassifizierung der Kryptographie**
Die Einteilung in Transpositions- und Substitutionsalgorithmen sowie in Symbolsubstitutionsalgorithmen (Klartextzeichen werden durch Symbole ersetzt) macht *Giovanni Battista Porta*. Er schlägt auch die Verwendung von Synonymen, Phrasen und Rechdschraibfelern vor, um die Kryptoanalysten zu verwirren. [3] S.138

1585 **Der Vignére-Code von Giovan Batista Belaso**
Blaise de Vignére schreibt ein Buch über Geheimtexte und stellt darin eine Methode der regenerativen Schlüsselerzeugung vor. Dabei werden Klartexte oder Geheimtexte von früheren Botschaften als Schlüssel weiterverwendet. Er greift die Idee von *Giovan Batista Belaso* auf und prägt deren Namen. [3] S.146

1917 **Code nach Vernam**
Der AT&T Ingenieur *Gilbert S. Vernam* erfindet den bis heute einzig bekannten 100% sicheren Code, den *Vernam-Code*, auch *one-time-pad* genannt (siehe auch Kapitel 2.1.3 auf Seite 7). Er konstruiert auch ein Maschine, welche diesen Code verwendet. Dieses Chiffriergerät wird 1920 kommerziell vermarktet. [3] S.401

1919 **Rotorkryptographiemaschine**
Hugo Alexander Koch reicht in den Niederlanden ein Patent für eine Kryptographiemaschine mit einer rotierenden Walze ein. Auf dieser Walze sind die Verschlüsselungsvorschriften eingearbeitet. Die Patentrechte gehen später auf *Arthur Scherbius* über. [3] S.420

1923 **Enigma**
Arthur Scherbius gründet die *Chiffriermaschinen Aktiengesellschaft* um die Enigma-Maschine zu produzieren und zu vermarkten. [3] S.421

1933-1945 **Enigma und der zweite Weltkrieg**
Die Enigma wird kein kommerzieller Erfolg, wird aber überholt und verbessert und dient der deutschen Wehrmacht im zweiten Weltkrieg als Chiffriergerät. Die Tatsache, dass der Code von den Alliierten geknackt wird, ist wesentlich für den Ausgang des Krieges. [3]

1976 **Kryptographie mit öffentlichem Schlüssel**
Whitefield Diffie und *Martin Hellman* veröffentlichen einen Artikel, in dem sie die Idee eines Kryptographiesystems mit öffentlichen und geheimen Schlüsseln präsentieren (siehe auch Kapitel 2.1.4 auf Seite 8). [5]

1977 **RSA-Methode**
Inspiriert von den Ideen der Herren *Diffie* und *Hellman* und als absolute Neulinge auf dem Gebiet der Kryptographie, erarbeiten *Ronald L. Rivest*, *Adi Shamir* und *Leonard M. Adleman* ein praktikables *public key system* (siehe auch Kapitel 2.1.4 auf Seite 9). Die RSA-Methode ist ein auch noch heute gebräuchliches System. [2]

2.3. Was ist momentan in Verwendung ?

Die Entscheidung, welches System für eine bestimmte geheime Kommunikation verwendet werden soll, hängt in erster Linie davon ab, wie sicher die Kommunikation gegen eine Abhörattacke sein soll. Um beispielsweise ein geheimes Treffen in drei Tagen zu arrangieren, ist es ausreichend, eine Methode zu verwenden, die von einem etwaigen Abhörer erst in vier Tagen geknackt werden kann. Sollen jedoch Daten übertragen werden, die dauerhaft geheim bleiben sollen, muss eine 100% abhörsichere Kommunikation verwendet werden - der Code nach Vernam also.

Die Firma *Mils Elektronik* bei Innsbruck hat genau diese Überlegungen in ihr *System 700* integriert. Um vollständig sichere Kommunikation zu führen, wurde eine PC-Einschubkarte entwickelt, die mit Hilfe einer Rauschquelle einen zufälligen Schlüssel erzeugt, welcher auf zwei Datenträgern zu Sender und Empfänger gebracht werden muss. Zu übetragende Texte oder Bilder werden mit dem Code nach Vernam unter Zuhilfenahme des verteilten, geheimen Schlüssels ver- und entschlüsselt. In einem Netzwerk von mehreren Benutzern werden standardmässig für jeweils zwei Teilnehmer Schlüssel vereinbart, wobei die Möglichkeit offengehalten wird, auch für mehr als zwei Teilnehmer den gleichen Schlüssel zu verwenden. Für weniger brisante Nachrichten kann man alternativ zum *one-time-pad* auch einen geheimen Kryptographiealgorithmus verwenden, welcher sich ebenfalls auf einer PC-Karte in einem zugriffgeschützen Speicher befindet. Diese Methode kann jederzeit und zwischen jedem Teilnehmer innerhalb des Netzes verwendet werden. Das System erlaubt eine weltweite Vernetzung von prinzipiell beliebig vielen Teilnehmern, wobei es eine (oder mehrere) Station(en) zu Erzeugung der geheimen Schlüssel gibt. Der wohl einzige Schwachpunkt in diesem System ist jedoch die komplizierte und unsichere Verteilung der Schlüssel. Hier kann jedoch die Quantenkryptographie Abhilfe verschaffen.

Eine weitere zur Zeit verwendete Methode ist die RSA-Methode. Dieses System hat

den großen Vorteil, dass sich sehr einfach beliebig viele Benutzer daran beteiligen können. Es muss nur an einem für jeden Teilnehmer zugänglichen Ort eine Datenbank mit allen offentlichen Schlüsseln liegen und schon kann jeder Benutzer jedem anderen Teilnehmer sichere (im Rahmen der RSA-Methode) Kommunikation betreiben. Diese RSA-Methode findet vor allem im Gebiet der privaten Kommunikation häufigen Einsatz.

Für die Übertragung der großen Mengen an Daten im Bereich des Finanzwesens und der Wirtschaft wird auf die Substitutions-Methode mit langen Schlüsseln zurückgegriffen. Die Kommunikation für das Netbanking über das Internet wird beispielsweise mit Hilfe eines 128bit Schlüssel „sicher“ gemacht.

3. Quantenkryptographie

Im vorigen Kapitel wurde der Code nach Vernam als die einzige 100%ig abhörsichere Methode vorgestellt und der Quantenkryptographie die Fähigkeit zuerkannt, einen geheimen Schlüssel über einen direkten Verbindungskanal zu erzeugen. Warum die Quantenmechanik derartige Möglichkeiten eröffnet und wie die Protokolle der Quantenkryptographie ablaufen, soll in diesem Kapitel erklärt werden.

3.1. Abhören = Messen

Der Code nach Vernam bezieht seine Sicherheit aus der Geheimhaltung des Schlüssels. Bei allen klassischen Methoden muss der Schlüssel generiert und anschließend zu Sender und Empfänger gebracht werden. Diese Übertragung, wie immer sie auch geschehen mag, kann ein Abhörer ausnutzen, um sich diesen Schlüssel möglichst unbemerkt anzueignen. Jeder dieser Versuche des Abhörens ist mit einer Messung an dem klassischen Objekt „Schlüssel“ gleichzusetzen. Wird der Schlüssel beispielsweise über eine elektrische Leitung in Form von TTL-Pulsen übermittelt, kann ein Abhörer mit einer elektronischen Messschaltung dieses Signal in einer Weise abgreifen, dass Sender und Empfänger dies nicht von einem Verlust entlang der Übertragungsstrecke unterscheiden können. Genausogut könnte der Schlüssel über ein Glasfaserkabel übertragen werden. Der Abhörer leitet von den Lichtpulsen einige Promille ab und kann somit den gesamten Schlüssel abhören, wiederum ohne von Empfänger oder Sender bemerkt zu werden. Wird der Schlüssel auf einem Datenträger (vergleiche one-time-pad bei Mils Elektronik; Kapitel 2.3 auf Seite 12) übermittelt, so besteht immer noch die Möglichkeit, dass entweder der Kurier nicht verlässlich ist oder die Daten auf dem Datenträger von einem Abhörer vom Kurier unbemerkt gelesen werden.

Billigt man dem Abhörer nun beliebige technische Möglichkeiten zu, so kann er immer ein Meßsystem bauen, welches das klassische Übertragungssystem in geringerem Ausmaß beeinflusst, als Sender und Empfänger je feststellen können. Innerhalb der klassischen Physik ist somit prinzipiell jede Übertragung des Schlüssels in gewissem Maße unsicher.

Betrachtet man jedoch Quantensysteme und die Messungen von Quantenzuständen, so erkennt man, dass Messungen nur mit einer bestimmten Erfolgsquote (Wahrscheinlichkeit) und nur mit einer signifikanten Veränderung bzw. Zerstörung des Quantenzustandes durchgeführt werden können. Dies ist Thema des nächsten Abschnittes.

3.2. Ein wenig Quantentheorie

3.2.1. Zustand und Messung

Für ein quantenmechanisches System wird ein beliebiger Zustand zur Zeit $t = t_0$ durch einen Zustandsvektor $|\Psi(t_0)\rangle$ beschrieben, welcher ein Element des Hilbertraumes $\boldsymbol{\mathcal{H}}$ ist. Jede messbare physikalische Größe α kann durch einen Operator $\mathbf{A}$ beschrieben werden, wobei die Eigenwerte a_n von $\mathbf{A}$ die einzig möglichen Messresultate sind. Bei einem derartigen Messprozeß wird der Hilbertraum $\boldsymbol{\mathcal{H}}$ in die Eigenvektoren $|u_n\rangle$ aufgespaltet. Sind die Eigenwerte a_n des Operators $\mathbf{A}$ nicht entartet, so kann jedem Eigenwert a_n ein separater Eigenvektor $|u_n\rangle$ zugeordnet werden:

$$\mathbf{A}|u_n\rangle = a_n|u_n\rangle \tag{3.1}$$

Bilden die Eigenvektoren $|u_n\rangle$ eine Eigenbasis im Hilbertraum $\boldsymbol{\mathcal{H}}$, so bezeichnet man den Operator $\mathbf{A}$ als Observable $\tilde{\mathbf{A}}$. Der normierte Zustand des Quantensystems kann dann als

$$|\Psi\rangle = \sum_n c_n|u_n\rangle \tag{3.2}$$

geschrieben werden. Die Dimension n der Eigenbasis ist dabei durch die Anzahl aller möglichen, unterscheidbaren Messergebnisse a_n gegeben. Die Wahrscheinlichkeit, bei einer Messung der Observablen $\tilde{\mathbf{A}}$ den Eigenwert a_n zu messen, ist

$$P(a_n) = |\langle u_n|\Psi\rangle|^2. \tag{3.3}$$

Wird die Messung der Observablen $\tilde{\mathbf{A}}$ oft wiederholt, so ergibt sich eine Wahrscheinlichkeitsverteilung der Eigenwerte a_n. Daraus läßt sich der Mittelwert $\langle\tilde{\mathbf{A}}\rangle$ der Messergebnisse der Observablen $\tilde{\mathbf{A}}$

$$\langle\tilde{\mathbf{A}}\rangle = \sum_n a_n|c_n|^2 \tag{3.4}$$

und die Standardabweichung $\Delta\tilde{\mathbf{A}}$ der Messergebnisse dieser Wahrscheinlichkeitsverteilung

$$\Delta\tilde{\mathbf{A}} = \sqrt{\tilde{\mathbf{A}}^2 - \langle\tilde{\mathbf{A}}\rangle^2} \tag{3.5}$$

bestimmen, welche ein Maß für die Verteilung der Messergebnisse um den Mittelwert $\langle\tilde{\mathbf{A}}\rangle$ ist.

Für zwei Operatoren $\mathbf{A}$ und $\mathbf{B}$ ist der Ausdruck $(\mathbf{AB} - \mathbf{BA})$ als der Kommutator $[\mathbf{A},\mathbf{B}]$ definiert. Kommutieren die beiden Operatoren ($[\mathbf{A},\mathbf{B}] = 0$ bzw. $\mathbf{AB} = \mathbf{BA}$), so haben beide Operatoren dieselben Eigenvektoren. Die mit den Operatoren $\mathbf{A}$ und $\mathbf{B}$ verbunden Observablen $\tilde{\mathbf{A}}$ und $\tilde{\mathbf{B}}$ können somit gleichzeitig scharf gemessen werden. Das Produkt der Standardabweichungen zweier kommutierender Operatoren verschwindet.

$$\Delta\mathbf{A}\Delta\mathbf{B} = 0 \tag{3.6}$$

Kommutieren die beiden Operatoren **A** und **B** jedoch nicht

$$[\mathbf{A},\mathbf{B}] = i\,\mathbf{C}, \tag{3.7}$$

so kann man zeigen, dass das Produkt der Unschärfen der beiden Operatoren ein bestimmte Grenze nicht unterschreiten darf:

$$\Delta\mathbf{A}\Delta\mathbf{B} \geq \frac{|\langle\mathbf{C}\rangle|}{2} \tag{3.8}$$

Der Wert $|\langle\mathbf{C}\rangle|$ läßt sich aus Gleichung 3.7 bestimmen. Ersetzt man nun den Operator **A** durch den Ortsoperator **Q** und den Operator **B** durch den Impulsoperator **P**, deren Kommutatorrelation

$$[\mathbf{Q},\mathbf{P}] = i\hbar \tag{3.9}$$

lautet, so erhält man die Heisenberg'sche Unschärferelation:

$$\Delta\mathbf{Q}\Delta\mathbf{P} \geq \frac{\hbar}{2} \tag{3.10}$$

Diese bedeutet: Je genauer man den Ort eines Teilchens misst, desto ungenauer ist der dazugehörige Impuls bestimmbar. Bestimmt man den Ort eines Teilchens exakt, so wird die Wahrscheinlichkeitsverteilung der Resultate von Impulsmessungen völlig zufällig sein.

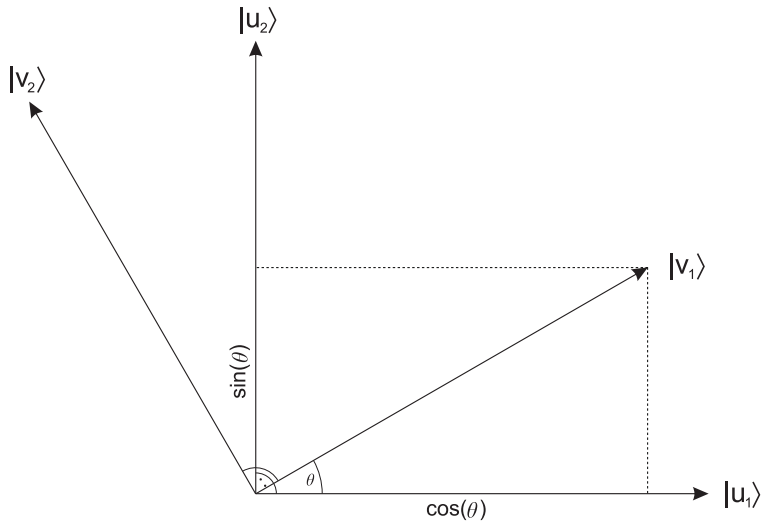


Abbildung 3.1.: Messung des Vektors $|v_1\rangle$ in der **U**-Basis

Betrachtet man nun ein 2-Zustands-System mit zwei miteinander nicht kommutierenden Operatoren **U** und **V** mit je zwei orthogonalen Eigenvektoren $|u_1\rangle$ und $|u_2\rangle$ bzw.

$|v_1\rangle$ und $|v_2\rangle$, dann werden die Eigenvektoren von $\mathbf{U}$ und $\mathbf{V}$ im Hilbertraum $\boldsymbol{\mathcal{H}}$ nicht in die gleich Richtung zeigen, sondern einen bestimmten Winkel θ zueinander einnehmen (siehe Abbildung 3.1). Versucht man nun $|v_1\rangle$ oder $|v_2\rangle$ in der $\mathbf{U}$-Basis zu messen, so wird das Ergebnis nur von der Projektion des zu messenden Vektors auf den entsprechenden Eigenvektor der $\mathbf{U}$-Basis abhängen. Misst man beispielsweise $|v_1\rangle$ in der Basis $|u_1\rangle$, so ist die Meßwahrscheinlichkeit nach Gleichung 3.3 die Projektion des Vektors $|v_1\rangle$ auf $|u_1\rangle$ (siehe Abbildung 3.1).

$$P_1 = P(|v_1\rangle/|u_1\rangle) = |\langle u_1|v_1\rangle|^2 = |\cos(\theta)|^2 = \cos^2(\theta) \tag{3.11}$$

Analog verhält es sich bei der Messung von $|v_1\rangle$ in der Basis $|u_2\rangle$.

$$P_2 = P(|v_1\rangle/|u_2\rangle) = |\langle u_2|v_1\rangle|^2 = |\sin(\theta)|^2 = sin^2(\theta) \tag{3.12}$$

Wählt man den Winkel $\theta = \frac{\pi}{4}$ so ist der Wert der beiden Messwahrscheinlichkeiten P_1 und P_2 gleich $\frac{1}{2}$, was bedeutet, dass sich die Messergebnisse völlig zufällig verhalten und keine Information über den ursprünglichen Zustand zu erhalten ist.

3.2.2. Polarisationszustandsmessung an einem Photon

Drückt man folglich einen beliebigen, linearen Polarisationszustand eines Photons unter dem Winkel α in der $\mathbf{U}$-Basis nach Gleichung 3.2 aus

$$|\Psi_\alpha\rangle = \cos(\alpha)|u_1\rangle + \sin(\alpha)|u_2\rangle \tag{3.13}$$

und beschreibt die Messung (Operator $\mathbf{M}$) dieses Polarisationszustandes mit einem Polarisator unter dem Winkel δ gefolgt von einem Einzelphotonendetektor wie folgt (graphische Darstellung siehe Abbildung 3.2)

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

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

$$\text{wobei} \quad |v_{1\delta}\rangle = \begin{pmatrix}\cos(\delta)\\ \sin(\delta)\end{pmatrix},\ |v_{2\delta}\rangle = \begin{pmatrix}-\sin(\delta)\\ \cos(\delta)\end{pmatrix} \tag{3.14}$$

$$\text{d.h.} \quad \mathbf{M}_\delta = \begin{pmatrix}\cos(2\delta) & \sin(2\delta)\\ \sin(2\delta) & -\cos(2\delta)\end{pmatrix},$$

dann ergibt sich für die Detektionswahrscheinlichkeit eines linear im Winkel α polarisierten Photons bei Messung unter einem Winkel δ

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

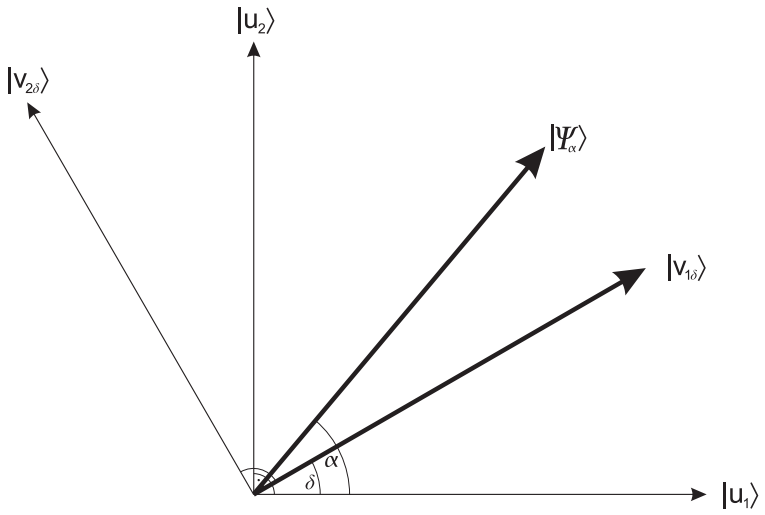


Abbildung 3.2.: Messung eines im Winkel α polarisierten Photons mit einem Polarisator beim Winkel δ

$$
\begin{aligned}
&= \left| \begin{pmatrix} \cos(\delta) \\ \sin(\delta) \end{pmatrix} (\cos(\alpha), \sin(\alpha)) \right|^2 = \\
&= |\cos(\delta)\cos(\alpha) + \sin(\delta)\sin(\alpha)|^2 = \\
&= |\cos(\alpha - \delta)|^2 = \\
&= \cos^2(\alpha - \delta) \ .
\end{aligned} \tag{3.15}
$$

Sind also α und δ gleich groß (die Polarisationsrichtung des Photons stimmt mit der optischen Achse des Polarisators überein), so ist die Detektionswahrscheinlichkeit gleich 1 (unter der Voraussetzung der Verwendung von Detektoren mit 100% Effizienz). Stehen Polarisation und optische Achse im rechten Winkel zueinander, ist die Detektionswahrscheinlichkeit gleich 0. Schließen die beiden Achsen jedoch einen Winkel von 45° ein, so ist die Wahrscheinlichkeit einer Detektion gleich $\frac{1}{2}$, also zufällig. Die Detektionswahrscheinlichkeit für ein unter $\alpha = 25°$ polarisierten Photons in Abhängigkeit des Polarisatorwinkel δ ist in Abbildung 3.3 graphisch dargestellt. Die Bestimmung der Polarisation eines Photons ist somit nicht möglich, da die Detektion oder Nicht-Detektion bei einer bestimmten Polarisatoreinstellung lediglich Auskunft über eine Polarisation parallel oder senkrecht zu der gewählten Quantisierungsrichtung geben und somit keiner eindeutigen Polarisation zugeordnet werden kann. Die Wahrscheinlichkeitsverteilung geht in eine Häufigkeitsversteilung über, wenn man die oben beschriebene Messung oftmals mit unterschiedlichen Polarisatoreinstellung wiederholt. Mit dieser Methode bestimmt man

auch experimentell die Polarisation in einem bestimmten Polarisationszustand präparierter Photonen (siehe Kapitel 4.2.4 auf Seite 41).

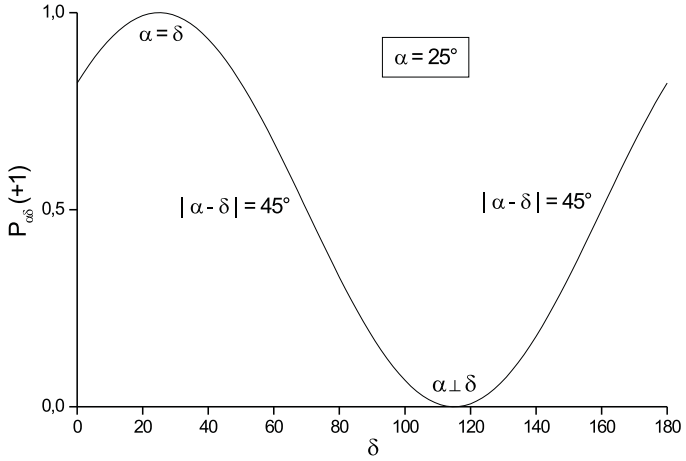


Abbildung 3.3.: Detektionswahrscheinlichkeit eines polarisierten Photons ($\alpha = 25°$) und rotierendem Polarisator ($\delta = 0°..180°$)

Das Verhalten von polarisierten Photonen bei Messungen in der Quantentheorie reicht jedoch noch nicht aus, um abhörsichere Kommunikation zu führen. Es bedarf auch bestimmter Vorschriften (Protokolle), wie eine Schlüsselvereinbarung abzulaufen hat. Diese Protokolle sind Gegenstand des nächsten Abschnitts.

3.3. Quantenkryptographieprotokolle

Die ursprüngliche Idee, über einen Quantenkanal geheime Kommunikation zu führen, stammt von *S. Wiesner* [6]. Der Physiker der Columbia University (New York) schlägt dabei das gleichzeitige Senden zweier Nachrichten vor, wobei zufällig Bits aus den beiden Nachrichten gewählt werden. Eine Nachricht wird mit horizontal und vertikal polarisierten Photonen kodiert und die zweite Nachricht mit rechts- bzw. linkszirkular polarisierten Photonen. Der Empfänger kann schließlich nur eine der beiden Nachrichten detektieren - die Zweite ist unwiederbringlich verloren.

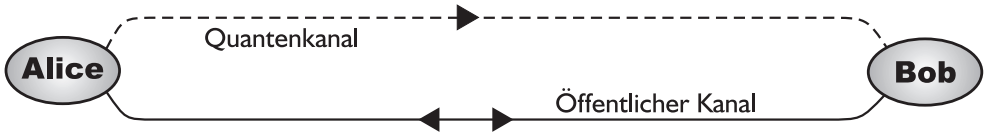
Unter Quantenkryptographie versteht man heute jedoch lediglich das Vereinbaren eines geheimen und sicheren Schlüssels, welchen man anschließend mit klassischen Methoden zur Nachrichtenübermittlung verwendet. In der Quantenkryptographie werden die miteinander kommunizierenden Partner mit Alice und Bob bezeichnet, wobei Alice meist die sendende und Bob die empfangende Einheit ist. Wie diese Schlüsselvereinba-

rung abläuft, soll anhand der folgenden drei Beispielen erklärt werden, wobei das erste Protokoll (BB84) sehr ausführlich behandelt wird, da dies die Methode unsere Wahl ist.

3.3.1. BB84

Dieses Protokoll wurde von *Charles H. Bennett* und *Gilles Brassad* [7] 1984 vorgeschlagen und stellt die Geburtsstunde der Quantenkryptographie dar:

Im **ersten Schritt** (siehe Abbildung 3.4) sendet Alice über den Quantenkanal (Glasfaser oder Luft) Photonen, welche zufällig in einer der vier Richtungen H, V, +45° oder −45° polarisiert sind. Bob hingegen versucht diese Photonen ebenfalls zufällig in einer der vier Polarisationsrichtungen zu messen. Beide notieren sich die Nummer des jeweiligen Photons, die Polarisationsrichtung in der sie gesendet bzw. gemessen haben und die dazugehörige Basis. Gleichzeitig übersetzen sie ihre Einträge in Schlüsselbits ($H \equiv 1$, $V \equiv 0$, $+45° \equiv 1$ und $-45° \equiv 0$).

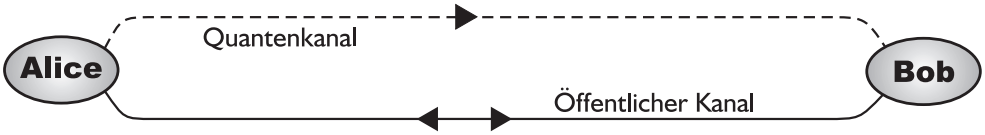


Nr.	Basis	Pol.	Bit
1	+/-	-45°	0
2	+/-	+45°	1
3	H/V	H	1
4	+/-	+45°	1
5	H/V	V	0
6	+/-	-45°	0
7	H/V	V	0
8	H/V	H	1
9	+/-	+45°	1
10	+/-	-45°	0
11	H/V	V	0
12	+/-	+45°	1
13	H/V	H	1
14	+/-	-45°	0
15	H/V	V	0
16	H/V	H	1
17	H/V	V	0
18	+/-	+45°	1
19	+/-	-45°	0
20	H/V	H	1
21	+/-	+45°	1
22	H/V	V	0
23	H/V	H	1
24	+/-	-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

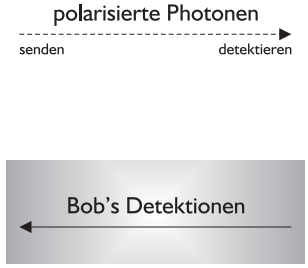
Nr.	Basis	Pol.	Det.	Bit
1	+/-	-45°	■	0
2	+/-	-45°	□	x
3	H/V	H	■	1
4	+/-	+45°	■	1
5	H/V	H	□	x
6	H/V	V	■	0
7	+/-	+45°	■	1
8	H/V	V	■	0
9	H/V	V	■	0
10	+/-	+45°	□	x
11	H/V	V	■	0
12	H/V	H	□	x
13	+/-	+45°	■	1
14	H/V	V	□	x
15	+/-	+45°	□	x
16	H/V	H	■	1
17	H/V	H	□	x
18	+/-	+45°	■	1
19	H/V	H	■	1
20	+/-	-45°	□	x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

Abbildung 3.4.: 1. Schritt BB84: Alice und Bob senden bzw. detektieren zufällig polarisierte Photonen und notieren die Ergebnisse in Listen.

Der **zweite Schritt** des Protokolls schreibt vor, alle Einträge in den beiden Listen zu streichen, bei denen Bob keine Detektion hatte. In Abbildung 3.5 sind diese Einträge in Bob's Liste mit offenen Quadraten (□) gekennzeichnet. Die Nummern dieser Einträge teilt Bob Alice über den öffentlichen Kanal mit. Dieser Kanal kann jedes abhörbare Kommunikationsmittel (Telefon, Funk, e-mail...) sein.



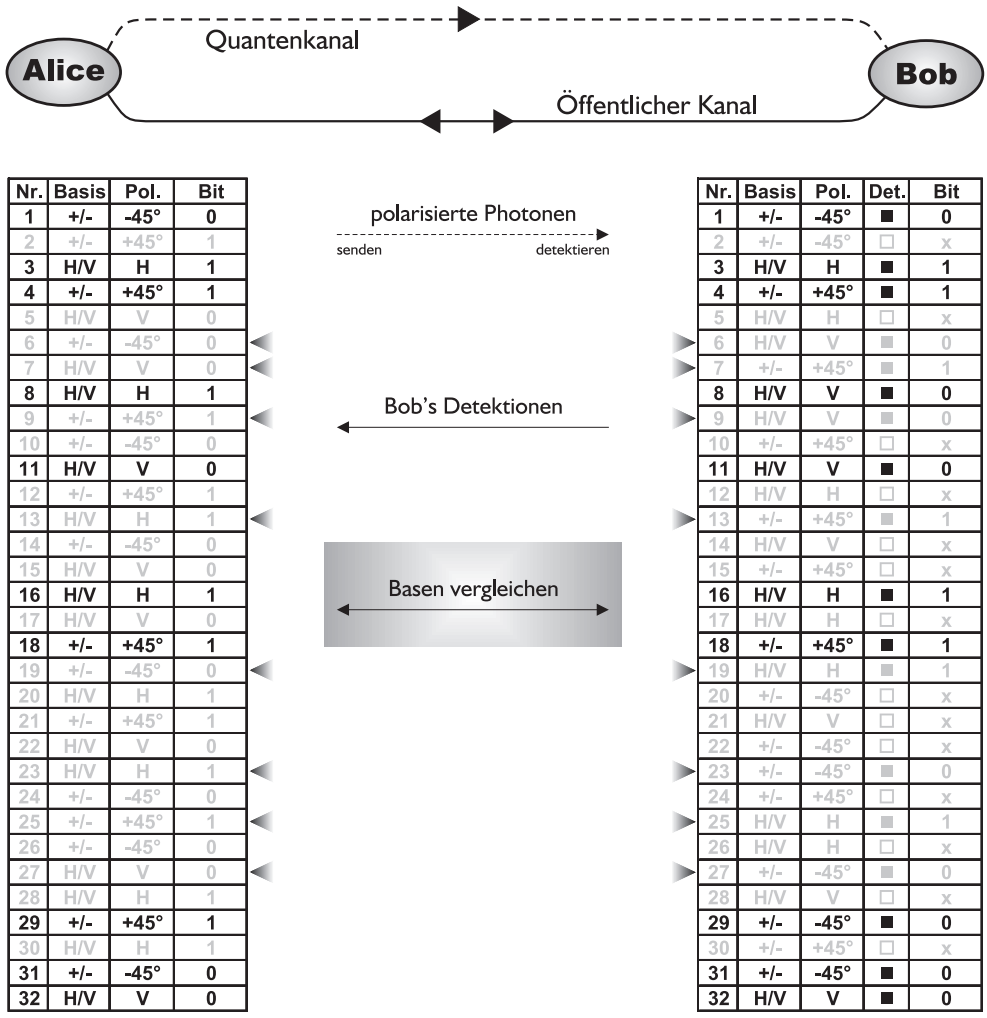
Nr.	Basis	Pol.	Bit
1	+/-	-45°	0
2	+/-	+45°	1
3	H/V	H	1
4	+/-	+45°	1
5	H/V	V	0
6	+/-	-45°	0
7	H/V	V	0
8	H/V	H	1
9	+/-	+45°	1
10	+/-	-45°	0
11	H/V	V	0
12	+/-	+45°	1
13	H/V	H	1
14	+/-	-45°	0
15	H/V	V	0
16	H/V	H	1
17	H/V	V	0
18	+/-	+45°	1
19	+/-	-45°	0
20	H/V	H	1
21	+/-	+45°	1
22	H/V	V	0
23	H/V	H	1
24	+/-	-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



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

Abbildung 3.5.: 2. Schritt BB84: Alice und Bob streichen alle Einträge, bei denen Bob kein Photon detektierte.

Im **dritten Schritt** werden die Basen der verbleibenden Einträge verglichen und all jene Positionen ausgeklammert, an denen Alice und Bob unterschiedliche Basiseinstellung verwendeten (siehe Abbildung 3.6). Wichtig bei diesem Schritt ist, dass wirklich nur Position und Basis, nicht aber die Polarisationsrichtung selbst über den öffentlichen Kanal ausgetauscht werden. Nur so bleibt gewährleistet, dass ein sich im öffentlichen Kanal befindlicher Abhörer keine Information aus dieser öffentlichen Diskussion gewinnen kann. Die nun vorliegende Folge von Schlüsselbits wird Rohschlüssel genannt und beinhaltet noch Fehler, die einerseits von Sender, Übertragungsstrecke und Empfänger und andererseits von einem etwaigen Abhörer herrühren.

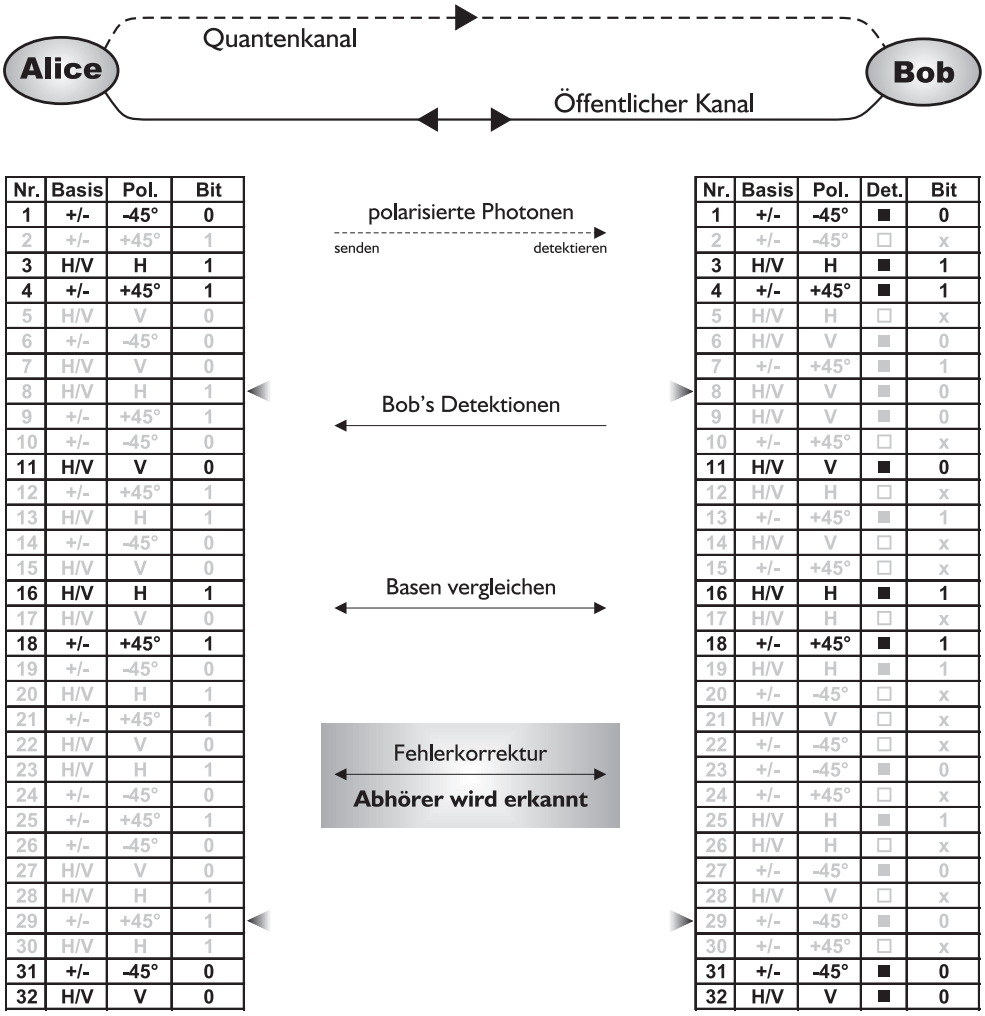


Nr.	Basis	Pol.	Bit
1	+/-	-45°	0
2	+/-	+45°	1
3	H/V	H	1
4	+/-	+45°	1
5	H/V	V	0
6	+/-	-45°	0
7	H/V	V	0
8	H/V	H	1
9	+/-	+45°	1
10	+/-	-45°	0
11	H/V	V	0
12	+/-	+45°	1
13	H/V	H	1
14	+/-	-45°	0
15	H/V	V	0
16	H/V	H	1
17	H/V	V	0
18	+/-	+45°	1
19	+/-	-45°	0
20	H/V	H	1
21	+/-	+45°	1
22	H/V	V	0
23	H/V	H	1
24	+/-	-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

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

Abbildung 3.6.: 3. Schritt BB84: Aus beiden Listen werden jene Einträge gestrichen, bei denen Alice und Bob unterschiedliche Basen verwendeten.

Ein entscheidender Punkt ist der **vierte Schritt** des Protokolls: Hier wird unter Zuhilfenahme verschiedener Fehlerkorrekturalgorithmen (siehe Kapitel 3.4 auf Seite 28) die Fehlerrate bestimmt, welche Aufschluß darüber gibt, ob ein Abhörer im Quantenkanal war oder nicht. Im letzteren Fall werden die vorhandenen Fehler korrigiert und der Schlüssel verwendet.

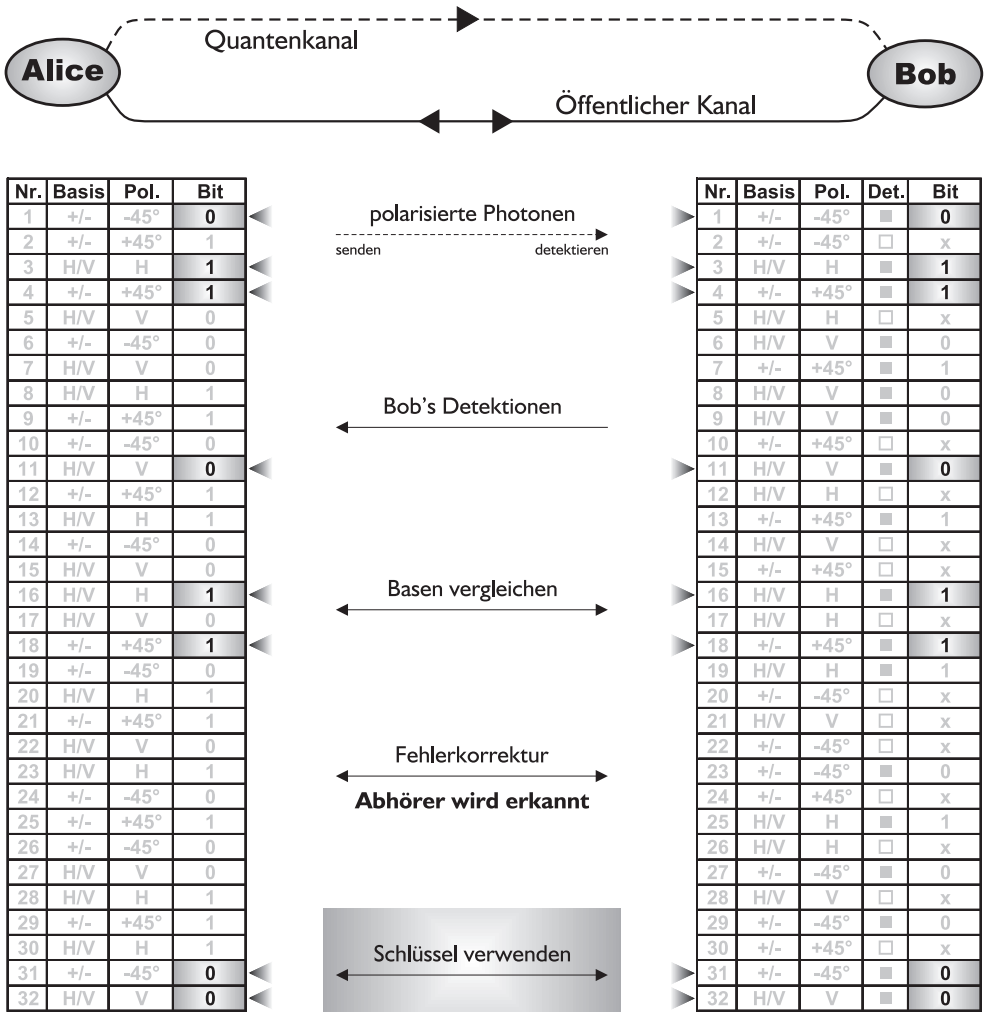


Nr.	Basis	Pol.	Bit
1	+/-	-45°	0
2	+/-	+45°	1
3	H/V	H	1
4	+/-	+45°	1
5	H/V	V	0
6	+/-	-45°	0
7	H/V	V	0
8	H/V	H	1
9	+/-	+45°	1
10	+/-	-45°	0
11	H/V	V	0
12	+/-	+45°	1
13	H/V	H	1
14	+/-	-45°	0
15	H/V	V	0
16	H/V	H	1
17	H/V	V	0
18	+/-	+45°	1
19	+/-	-45°	0
20	H/V	H	1
21	+/-	+45°	1
22	H/V	V	0
23	H/V	H	1
24	+/-	-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

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

Abbildung 3.7.: 4. Schritt BB84: Bei der Fehlerkorrektur werden falsche Einträge und vor allem ein etwaiger Abhörer identifiziert.

Der **fünfte Schritt** ist eigentlich nicht mehr dem BB84-Protokoll zugehörig, soll hier aber der Vollständigkeit halber erwähnt sein. Der durch die Fehlerkorrektur aus dem Rohschlüssel gewonnene endgültige, sichere Schlüssel kann jetzt in Verbindung mit nicht dechiffrierbaren Algorithmen (one-time-pad, siehe Kapitel 2.1.3 auf Seite 7) zur 100% sicheren Kommunikation verwendet werden.



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

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

Abbildung 3.8.: 5. Schritt BB84: Der somit gewonnene Schlüssel kann von Alice und Bob unter Zuhilfenahme klassischer Algorithmen (one-time-pad) zur sicheren Kommunikation verwendet werden.

3.3.2. Quantenkryptographie auf Basis des Bell'schen Theorems

Das von A. Ekert [8] 1991 vorgeschlagene Schema macht sich ein Gedankenexperiment von Einstein, Podolsky und Rosen [9] in der von Bohm modifizierten Form zur Grundlage. Dabei wird die Korrelation der beiden Teilchen eines EPR-Paares [10] ausgenützt, bei deren Erzeugung aufgrund der Erhaltungssätze aus einem Spin-0 Teilchen zwei Teilchen mit entgegengesetztem Spin-$\frac{1}{2}$ entstehen. Die Wellenfunktion dieses Zweiteilchenzustandes hat eine besondere Form und wurde von Schrödinger als verschränkter Zustand bezeichnet. Der Aufbau für eine experimentelle Realisierung ist in Abbildung 3.9 zu sehen. Eine zentrale Quelle (S) erzeugt EPR-Paare bestehend aus Spin-$\frac{1}{2}$ -Teilchen und sendet diese über einen Quantelkanal entlang entgegengesetzter Richtungen der z-Achse zu Alice bzw. Bob. Beide machen folglich zufällig Messung der Spinkomponenten in der Ebene senkrecht zur z-Achse. Wird der Winkel φ der Messung in Bezug auf die x-Achse angegeben, so mißt Alice zufällig unter einem der Winkel 0°, 45° bzw. 90° und Bob wählt ebenfalls zufällig einen der Winkel 45°, 90° bzw. 135° (siehe Abbildung 3.9). Hinter beiden Analysatoren (A_A bzw. A_B) werden dann die Teilchen detektiert (D).

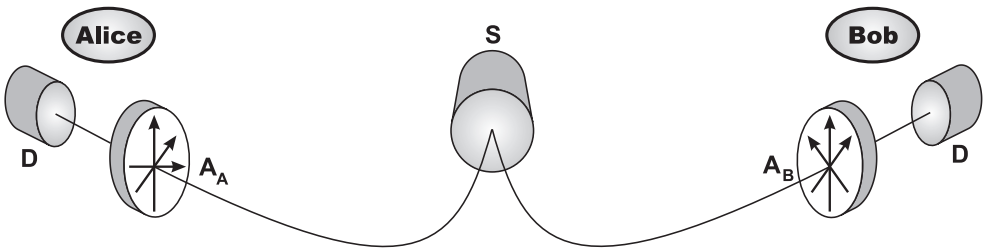


Abbildung 3.9.: Quantenkryptographie nach Bell'schem Theorem

Anschließend werden die Meßergebnisse über einen öffentlichen Kanal verglichen, wobei im ersten Schritt alle jene Einträge gestrichen werden, bei denen entweder Alice oder Bob oder beide keine Detektion hatten. Die restlichen Einträge werde in zwei Gruppen geteilt, wobei eine Gruppe aus allen Positionen besteht, an denen Alice und Bob unterschiedliche Meßeinstellungen verwendeten. Im einfachsten Fall werden auch diese Einträge verworfen und mit den restlichen verfahren wir im BB84-Protokoll (Fehlerkorrektur; Abhörer erkennen). Eine andere Methode ist, mit den Einträgen unterschiedlicher Winkel die Verletzung der Bell'sche Ungleichung zu testen und damit festzustellen, ob ein Abhörer im Quantenkanal war [8].

Als Nebenprodukt eines Bell-Experiments mit unabhängigen Beobachtern [11] konnte dieses Protokoll getestet werden. Hierbei wurden die polarisationsverschränkten Photonenpaare durch parametrische Fluoreszenz erzeugt. Die Rohschlüsselrate lag bei 850 Hz und die Fehlerrate bei ca. 2,5%. Nach einer Fehlerkorrektur sank die effektive Schlüsselrate auf 500Hz und die Fehlerrate auf 0,4%. Diese Werte sind zwar verglichen mit anderen Quantenkryptographie-Experimenten recht gut, der technische Aufwand für diese Vari-

ante ist jedoch enorm größer und somit als Realisierung für eine praktische Anwendung indiskutabel.

3.3.3. Interferometrische Quantenkryptographie

Bennet schlug 1992 ein Schema für die Quantenkryptographie vor, in dem zwei beliebige nichtorthogonale Zustände verwendet werden [12]. Der experimentelle Aufbau ist in Abbildung 3.10 zu sehen: Alice verwendet eine Kombination von unsymmetrischen Strahlteilern (UBS) und Spiegeln (M), um den ursprünglichen Puls der Quelle (S) kohärent in zwei zeitseparierte Pulse aufzuteilen: einen schwachen Signalpuls mit mittlerer Photonenzahl $\mu < 1$ gefolgt von einem hellen Puls ($\mu > 1$). Der Signalpuls erfährt einen Phasenschub von 0° oder 180°, womit die Bits 0 und 1 kodiert werden. Anschließend erfolgt die Übertragung über den Quantenkanal. Der Empfänger, Bob, benützt

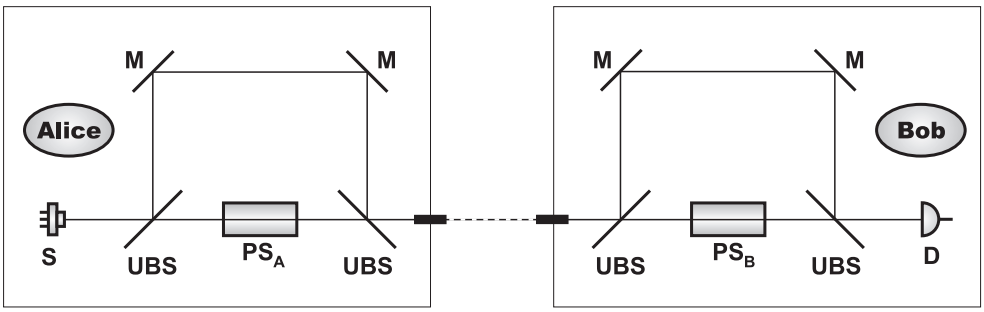


Abbildung 3.10.: Interferometrische Quantenkryptographie

ein analoges Halbinterferometer um den ankommenden Puls wieder entweder zeitlich zu verzögern oder die Phase zu verändern. Der schwache Puls wird wieder zufällig und unabhängig von den Einstellungen des Phasenschiebers von Alice mit einem Phasenschub von 0° oder 180° und der helle Puls mit einer Zeitverzögerung von Δt versehen. Das Resultat sind nun drei mit Δt separierte Pulse: Der erste Puls (ein sehr schwacher Puls, da von Alice und Bob abgeschwächt) wird vernachlässigt. Der zweite Puls, der die wichtige Schlüsselinformation enthält, ist eine Superposition von dem Puls, der von Alice abgeschwächt und von Bob zeitverzögert wurde und jenem Puls, der von Alice zeitverzögert und von Bob abgeschwächt wurde. Hatten beide zufällig den gleichen Phasenschub eingestellt, so ergibt sich am letzten Strahlteiler konstruktive Interferenz und eine Detektionswahrscheinlichkeit von $\approx 4\mu Tq$, wobei T der Transmissionskoeffizient des Quantenkanals und q die Quanteneffizienz des Detektors ist. Waren die Phasenschiebereinstellungen unterschiedlich, so ist die Pulsintensität idealerweise gleich 0. Schließlich, wiederum nach Δt, kommt der Puls, welcher von beiden zeitverzögert wurde, bei Bob an. Dieser dient als Referenzpuls.

Bennet zeigt weiters in seiner Veröffentlichung, dass die Abhörstrategie des Detektierens und Weitersendens von Signal-Referenzpulspaaren wieder zu Fehlern führen muss, was von Alice und Bob erkannt werden kann.

Diese Methode der Quantenkryptographie wurde unter anderem von den Arbeitsgruppen in Genf, Los Alamos und bei der BT (British Telecom) realisiert. Die Ergebnisse werden in Kapitel 5 diskutiert und verglichen.

3.4. Fehlerkorrekturen und Abhörstrategien

Diese beiden für die Quantenkryptographie sicher sehr wichtigen Themen können im Rahmen dieser Arbeit nicht ausführlich beschrieben werden, sollen jedoch auch nicht ganz unerwähnt bleiben.

Bei der Fehlerkorrektur gibt es sehr einfache und effiziente Methoden, die allerdings meist mit einem erheblichen Verlust an Schlüsselbits verbunden sind. Um prinzipiell die Größe der im Schlüssel vorhandenen Fehlerrate festzustellen, muss ein direkter Vergleich eines Teiles des Schlüssels bei Alice und Bob erfolgen. Der erste Hinweis auf das Vorhandensein eines Abhörers ist dann gegeben, wenn die Fehlerrate trotz erfolgreicher Justage vor der Übertragung einen Wert erreicht, der wesentlich über den für die Übertragung Typischen liegt. In diesem Fall muss die Übertragung wiederholt werden. Liegt die Fehlerrate im normalen Bereich, kann mit der Methode des Paritätbitvergleichs die Fehlerrate reduziert werden. Dabei wird aus einem Block, dessen Größe aus der vorhandene Fehlerrate abzuleiten ist (umso größer die Fehlerrate, desto kleiner die Blöcke), ein Paritätsbit erzeugt, welches 0 ist, wenn sich eine gerade Anzahl von 1en im gewählten Schlüsselblock befinden (und 1 bei einer ungeraden Anzahl). Der Block wird verworfen, wenn Alice und Bob eine unterschiedliche Parität erhalten. Bei gleicher Parität wird beispielsweise das erste Bit des Blocks gestrichen und die restlichen als Schlüssel verwendet. Das Streichen eines Bits aus dem untersuchten Block ist notwendig, um die Paritätsinformation für einen etwaigen Abhörer zu verwischen. Auf komplizierte Verfahren (zum Beispiel *privacy amplification* [13] oder *quantum key growing* [14]) soll hier nicht eingegangen werden.

Auch bei den Abhörattacken gibt es sehr einfache und anschauliche Methoden. Die sogenannte Strahlteilerattacke beruht auf der Tatsache, dass im Experiment anstelle von wirklichen Einzelphotonenquellen abgeschächte Pulse verwendet werden, in denen sich mit einer bestimmten Wahrscheinlichkeit auch zwei oder mehr Photonen befinden können. Eine Messung, welche den Zustand nicht zerstört aber Auskunft über die Photonenzahl gibt, veranlasst den Abhörer, bei Pulsen mit mehr als nur einem Photon mit einem Strahlteiler den Quantenkanal abzuhören. Eine Abschätzung in einem der ersten Experimente der Quantenkryptographie [15] zeigte, dass bei einer mittleren Photonenzahl von $\mu = 0.17$ bei 85000 von Alice gesendeten und 640 von Bob in der richtigen Basis gemessenen Pulsen, ein Abhörer immerhin 54 Bits lernen konnte. Im gleichen Experiment wurde auch eine zweite Abhörmethode versucht, jene des Messens und Weitersendens.

Dabei konnten im gleichen Durchlauf 56 Bits gewonnen werden, allerdings erhöht sich bei dieser Methode die Fehlerrate um 25% der Übertragungsrate. Weiters könnte man sich durch das einfache Kopieren des vorbeifliegenden Photons einen effektiven Abhörvorgang vorstellen. Der Artikel „*A single quantum cannot be cloned*“ [16] beweist jedoch, dass der Zustand eines beliebigen Quantenzustandes nicht kopiert werden kann. Eine weitere Methode sind *coherent attacks* [17]. Dabei wird ein ganzer Satz von Quantenbits mit Hilfe eines Quantencomputers verarbeitet. Allerdings kommt es auch hierdurch zu unvermeidlichen Fehlern. Eine etwas umstrittene Methode names „*indirect coping attack*“ ist in [18] nachzulesen.

4. Das Experiment

Das im folgenden Kapitel beschriebene Quantenkryptographie-Experiment wurde unter Bedacht auf eine künftige Anwendung nach den Gesichtspunkten der Schnelligkeit, Kompaktheit und Anwenderfreundlichkeit realisiert. Das Experiment wird hier nun zuerst als ganzes mit seinen wesentlichen Teilen vorgestellt. Anschließend werden alle Komponenten von Alice und Bob im Detail beschrieben und Resultate ausgewertet.

4.1. Experimenteller Aufbau

Der schematische Aufbau des Experiments ist in Abbildung 4.1 zu sehen. Alice (Sender) und Bob (Empfänger) sind zum einen durch den abhörsicheren Quantenkanal, über welchen Alice Bob zufällig polarisierte Photonen schickt , und zum anderen durch den öffentlichen Kanal, über welchen die Schritte 2 bis 5 des BB84-Protokolls (siehe Kapitel 3.3.1 auf Seite 21) durchgeführt werden, miteinander verbunden. Die optischen Ein-

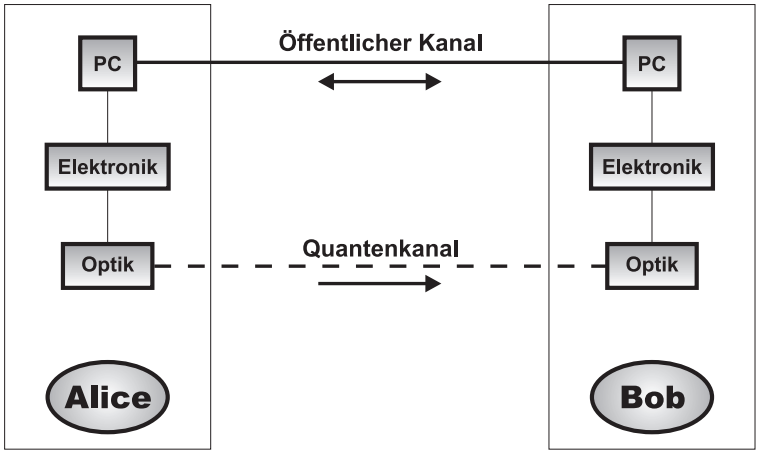


Abbildung 4.1.: Schematischer Aufbau des Quantenkryptographie-Experiments

heiten von Alice und Bob, welche die polarisierten Photonen senden bzw. empfangen, werden jeweils von einem PC und einer Elektronik angesteuert. Der öffentliche Kanal ist in der ersten Stufe des Experiments eine direkte Parallelverbindung der beiden Rechner

und wird später durch eine Internetverbindung ersetzt werden. Der Quantenkanal kann entweder eine Verbindung über eine Single-Mode-Faser oder eine Übertragungsstrecke über Luft sein, wobei im ersteren Fall eine Polarisationskontrolle vor oder nach dem Quantenkanal notwendig ist.

In Abbildung 4.2 ist das Gesamtexperiment mit den optischen Details zu sehen. Erwähnenswert ist, dass die optischen Aufbauten von Alice und Bob symmetrisch zueinander sind, d.h. bei Alice gehen dem optischen Aufbau vier Laserdioden als Quellen voraus und bei Bob folgen dem selben, jedoch gespiegelten optischen Aufbau vier SPAD's (Single-Photon-Avalanche-Diode) als Detektoren. Die einzelnen Komponenten

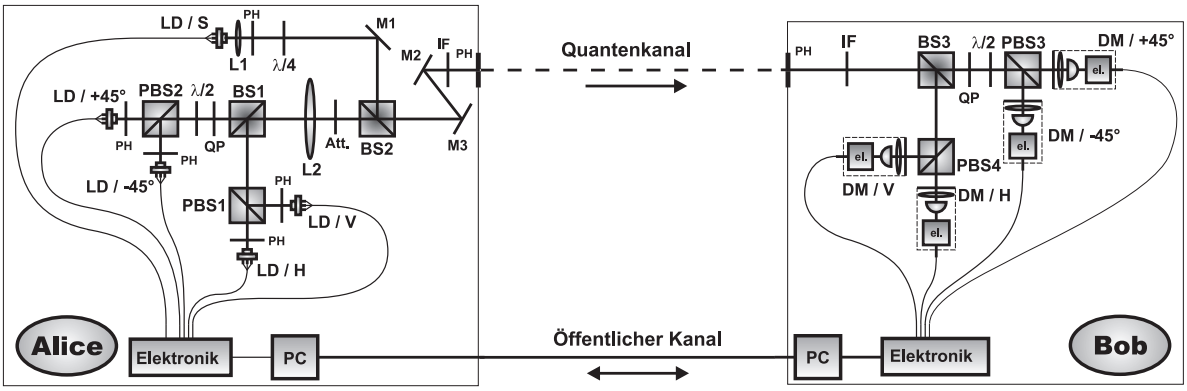


Abbildung 4.2.: Das Gesamtexperiment

der optischen Einheiten werden in den Kapiteln 4.2.3 (Alice) und 4.3.1 (Bob) genauer beschrieben.

Im Rahmen dieser Diplomarbeit konnte eine vollständig funktionierende Sendeeinheit (Alice) realisiert und getestet werden. Für die Empfangseinheit (Bob) wurde hauptsächlich an der Entwicklung und Fertigung einfach bedienbarer Detektormodule gearbeitet. Ein Testaufbau für Bob ließ die zu erwartenden Ergebnisse für das Gesamtexperiment abschätzen. Die Synchronisation zwischen Alice und Bob wurde in [19] getestet.

4.2. Alice

Wie vorhin erwähnt ist Alice beim BB84-Protokoll in Bezug auf den Quantenkanal die sendende Einheit. In Abbildung 4.3 ist im speziellen der optische Aufbau noch einmal größer dargestellt. Auf diese Abbildung wird im Laufe dieses Kapitels immer wieder Bezug genommen.

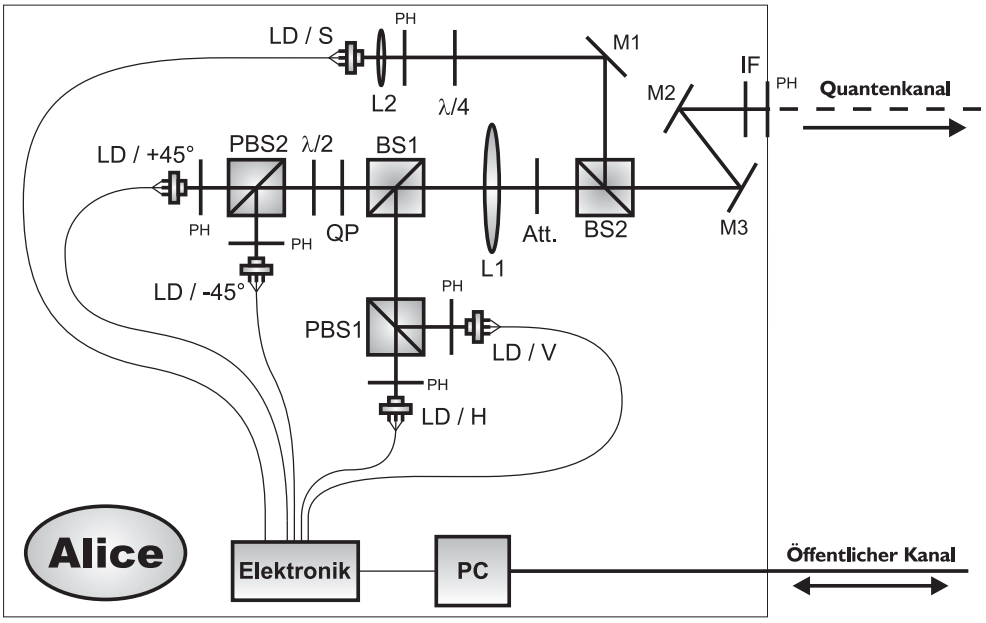


Abbildung 4.3.: Detaillierter optischer Aufbau von Alice

Aus den einleitend erwähnten Gründen wie Schnelligkeit, Kompaktheit und einfache Bedienung wurde bei diesem Experiment auf aktive Einheiten, wie etwa Pockelszellen zum Rotieren der Polarisation, verzichtet. Anstatt dessen werden zur Erzeugung der vier Polarisationsrichtungen (H, V, $+45°$, $-45°$) vier separate Laserdioden (LD/H, LD/V, LD/$+45°$, LD/$-45°$) zum Einsatz gebracht, welche über einen optischen Aufbau (polarisierende und nichtpolarisierende Strahlteiler, $\lambda/2$-Plättchen, Abschwächer, Spiegel, Filter) in einen Ausgang gekoppelt werden. Die Laserdiode LD-S dient zur Synchronisation von Bob und sendet nach 97 schwachen Pulsen einen hellen, zirkular-polarisierten Puls aus. Das Schema dieser Synchronisation, welche einige Vorteile bietet, ist in Kapitel 4.3.3 (Elektronik Bob) ausführlich beschrieben.

Abbildung 4.4 zeigt ein Foto des experimentellen Aufbaus aus der Vogelperspektive. Links ist das Netzgerät zur Versorgung der Elektronik und rechts daneben die Elektronik-Box selbst zu sehen. Dreht man dieses Bild um 90° gegen den Uhrzeigersinn, so entspricht die räumliche Positionierung der optischen Komponenten jener der in Abbildung 4.3 dargestellten. Es sind die elektrischen Verbindungen von der Elektronik zu

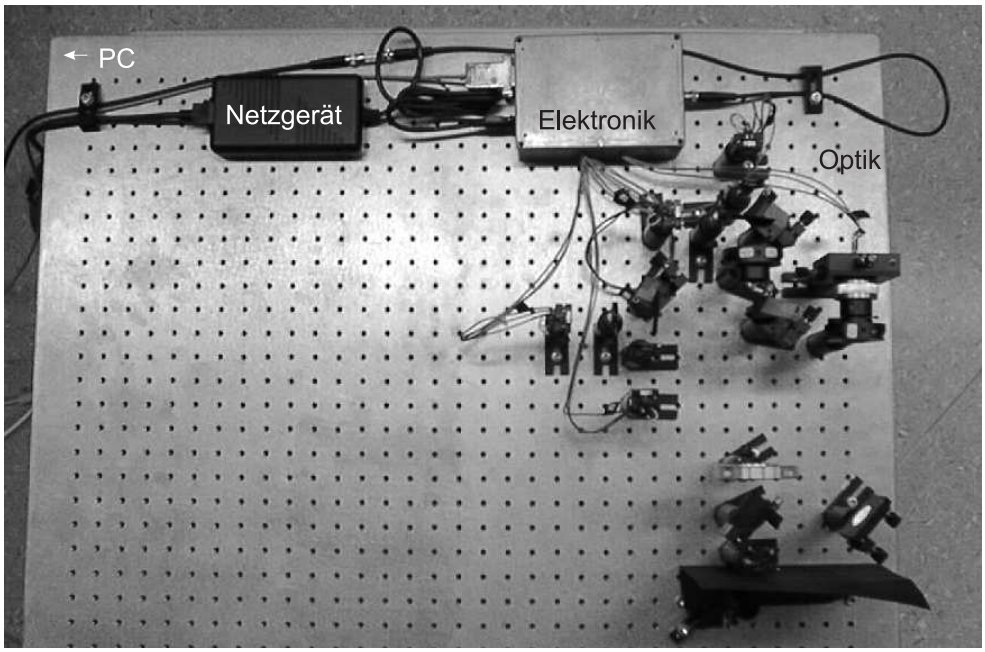


Abbildung 4.4.: Experimenteller Aufbau aus der Vogelperspektive

den fünf Laserdioden und die Halterungen für die optischen Komponenten zu erkennen. Die optischen Komponenten wurden der Kompaktheit wegen sehr klein gewählt und werden in der nächsten Stufe des Experiments auf noch engeren Raum angeordnet. Auch die Elektronik wird im nächsten Schritt miniaturisiert, sodass Elektronik und Optik entweder in der Größe eines herkömmlichen Modems als externe Einheit oder direkt als Einschubkarte für den PC realisiert werden können.

4.2.1. PC & Programm

Der PC hat in diesem Quantenkryptographie-Experiment zwei Funktionen: Erstens stellt der Computer die Schnittstelle zum künftigen Anwender dar und sollte daher über ein einfaches Programm zu bedienen sein. Zweitens steuert der Rechner über eine digitale Ein-/Ausgabekarte die Elektronik, welche ihrerseits die Optik steuert.

Digitale Ein-/Ausgabekarte

Die Anforderungen an die Digitalkarte für das Experiment waren primär eine hohe Datenrate und die Möglichkeit, die Datenausgabe extern zu triggern. Wir wählten daher die PCI7200 D-I/O-Card der Firma AdLib . Diese Karte lässt sich extern bis zu einer Frequenz von 2MHz triggern. Die Karte ließ sich problemlos installieren und funktionierte mit den mitgelieferten Testprogrammen auf Anhieb. An den zwei 37-poligen Ports (CN1

und CN2) der Karte stehen 2x32 digitale Ein- bzw. Ausgänge und diverse Anschlüsse für die Kommunikation (externer und interner Trigger, hand-shake) zur Verfügung. Für das Experiment wurden folgende Anschlüsse der Digitalkarte verwendet:

Port	Ausgang	Pin	Beschreibung
CN1	DOA0	1	H
CN1	DOA1	2	V
CN1	DOA2	3	+45°
CN1	DOA3	4	−45°
CN1	DOA4	5	Start
CN1	DOA5	6	Init
CN1	GND	36	Masse
CN2	O-ACK	3	2MHz
CN2	GND	36	Masse

Die ersten vier Ausgänge steuern über die Elektronik die jeweiligen Laserdioden an, Start bedeutet den Beginn der Übertragung und Init bereitet die Elektronik auf den Start der Übertragung vor. Der Eingang O-ACK ist für die Triggerung der Ausgabe mit einem externen 2MHz-Signal, welches erst nach dem Startimpuls anliegt. Die Ansteuerungssequenz für die Synchronisations-Laserdiode (LD/S, siehe Abb. 4.3) wird in der Elektronik erzeugt. Für die richtige Ansteuerung der Ausgänge ist die folgende Software zuständig.

Programm

Im Lieferumfang der Digitalkarte sind Bibliotheksdateien enthalten, die das Einbinden aller Ansteuerungsbefehle für die Karte in einige Programmiersprachen (Lab View, C++, Visual-Basic) erlauben. Die Oberfläche des ungefähr 500 Zeilen langen Visual-Basic-Programmes, welche nach einem zwei Sekunden langen Initialisierungsvorganges nach Programmstart erscheint, ist in Abbildung 4.5 zu sehen. Im Rahmen „Outputfield“ kann ausgewält werden, wie die zu übertragende Sequenz auszusehen hat: Für richtige Quantenkryptographie ist die Option „random“ zu wählen, wobei in diesem Fall der interne Zufallsgenerator verwendet wird. Die anderen acht Einstellungen sind für Testzwecke gedacht. Eine weitere Option für Testzwecke wäre die Möglichkeit, eine ausgewählte Diode im cw-Betrieb (continuous wave) laufen zu lassen. Dies ist für Justiervorgänge von Vorteil und wird in der nächsten Versionen des Programms und der Elektronik implementiert. Rechts daneben kann das nach Drücken des „generate“-Knopfes erzeugte Feld der Zufallszahlen kontrolliert werden. Bei „Fieldlength“ kann die Länge des Feldes und ob dieses Feld rekursiv ausgegeben werden soll eingestellt werden. „Start“ leitet dann die Übertragung der eingestellten Sequenz ein. Wurde die rekursive Form der Übertragung gewählt, kann der Vorgang mit „Stop“ abgebrochen werden.

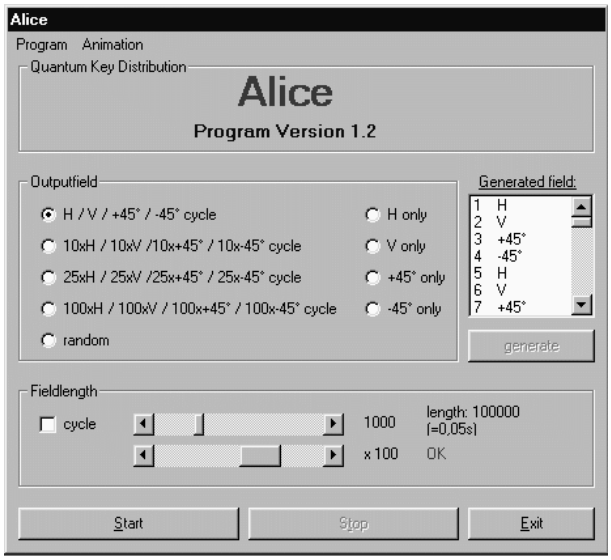


Abbildung 4.5.: Oberfläche des Programmes Alice Version 1.2

„Exit“ beendet das Programm. Zur besseren Erkennbarkeit, ob eine Übertragung momentan läuft, erscheint nach dem Start eine Animation, welche über den Menüpunkt „Animation“ deaktiviert werden kann.

4.2.2. Elektronik

Die Elektronik wurde in [19] entwickelt und enthält zwei wesentliche Einheiten (siehe Abbildung 4.6):

Zum ersten beinhaltet sie den 2MHz-Quarz, welcher als Grundfrequenz für die Übertragung fungiert. Der gleiche Quarz ist auch in der Elektronik von Bob enthalten, wobei über eine spezielle Synchronisation beide „Uhren“ gleich gehen. Der Quarz in Alice's Elektronik wird erst gestartet, wenn der „Start“-Ausgang der digitalen Karte dies zuläßt und die vorangegangene Initialisierung der Elektronik erfolgreich war. Das 2MHz-Signal wird dann einmal der Digitalkarte als Trigger zugeführt und zum anderen der restlichen Elektronik ebenfalls als Trigger zur Verfügung gestellt.

Der zweite Teil der Elektronik bereitet die Pulse so auf, dass damit die Laserdioden angesteuert werden können. Zuerst werden aus dem symmetrischen 2MHz Signal Pulse mit einer Länge von 5ns erzeugt. Diese Pulse werden anschließend einem Laser-Driver zugeführt. Die nun zur Verfügung stehenden Pulse steuern über einen schnellen Schalter die entsprechende Laserdiode an. Dafür werden die an den Ausgängen DOA0 bis DOA3 der Digitalkarte anliegenden Signale verwendet.

Das Synchronisationssignal (20kHz) für die Laserdiode LD/S wurde einfach aus dem 2MHz-Signal generiert. Ein Zähler registriert 100 Pulse des 2MHz-Signals, gibt anschlie-

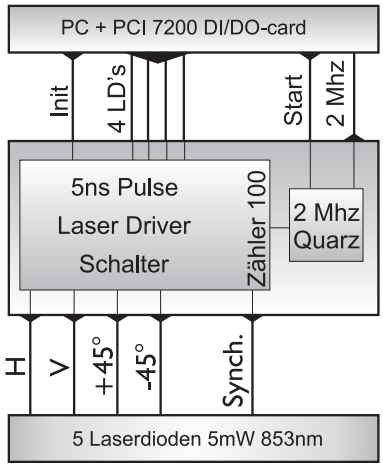


Abbildung 4.6.: Blockschaltbild Elektronik Alice

ßend den 1μs langen Synchronisationspuls aus und setzt sich selber wieder auf null.

Die Elektronik wurde hauptsächlich mit normalen Elektronikbausteinen realisiert und könnte in ihrer bestehenden Form sicher um den Faktor fünf in der Bauweise verkleinert werden. Geht man auf SMD-Bauweise über, wäre auch eine Miniaturisierung auf ein Zehntel der ursprünglichen Größe denkbar. Die Obergrenze von 2MHz rührt von der Totzeit der Detektoren auf Bob's Seite her (vergleiche Kapitel 4.3.2 auf Seite 46). Will man diese Frequenz erhöhen, was vorerst schnellerer Detektoren bedarf, so gehen die Überlegung dahin, dass man den Zufallsgenerator in die Elektronik integriert und die übertragene Sequenz in einem Speicherbaustein zwischenspeichert und während oder nach der Übertragung in den PC einließt. Der Computer hätte dann nur mehr die Aufgabe, die Übertragung zu starten und die gesendete Sequenz einzulesen. Dieses Konzept würde sich recht einfach in Form einer PC-Einschubkarte realisieren lassen. Diese Karte hätte dann nach außen nur mehr eine Schnittstelle zu einer Glasfaser.

4.2.3. Optik

Die Optik hat nun die Aufgabe, die von den Laserdioden (RTL8505G, Sharp) erzeugten Lichtpulse in einen Ausgang derart einzukoppeln, dass erstens die Wahrscheinlichkeit, dass mehr als zwei Photonen in einem Puls enthalten sind verschwindend gering ist und zweitens die Polarisation der Photonen eine hohe Sichtbarkeit aufweisen.

Die Laserdioden selbst emittieren in einen elliptischen Lichtkegel (siehe Abb. 4.7) bei einer Wellenlänge von 853nm und einer Leistung von 5mW sehr stark polarisiertes Licht (96% Sichtbarkeit), was aber für die Quantenkryptographie noch nicht ausreichend ist. Die Laserdioden wurden auf Halterungen montiert, welche senkrecht zur Emissionsrichtung verkippt werden können. In Kombination mit davor montierten Blenden (PH, pinhole) kann die Intensität der Laserdioden auf einfache mechanische Weise justiert

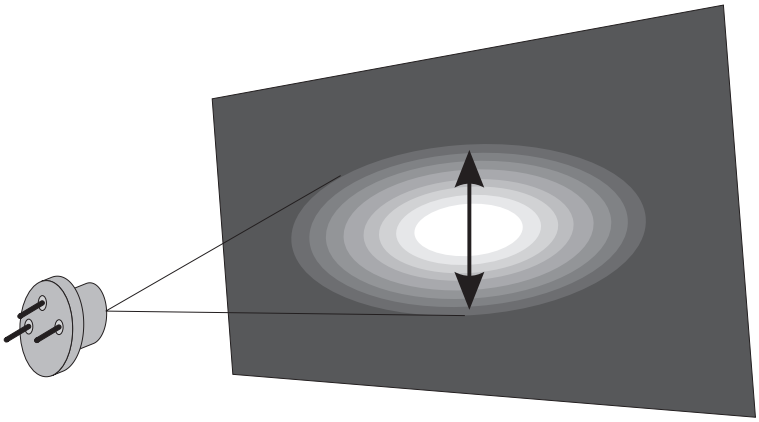


Abbildung 4.7.: Lichtkegelprofil und Polarisation der verwendeten Laserdioden (853nm, 5mW, RLT850G von Sharp)

werden.

Das Licht von je zwei Laserdioden (LD/H und LD/V bzw. LD/+45° und LD/+45°) wird anschließend über einen polarisierenden Strahlteiler (PBS1 und PBS2, polarising beamsplitter) kombiniert. Ein polarisierender Strahlteiler transmittiert die horizontale und reflektiert die vertikale Komponente des Lichtes. Testmessungen an einem derartigen Strahlteiler haben gezeigt, dass die Sichtbarkeit in Transmissions- und Reflexionsrichtung im Falle von horizontal bzw. vertikal polarisiertem Licht größer als $99,6\%$ ist. Schlechter hingegen ist das Ergebnis, wenn Licht unter 45° eingestrahlt wird: im Transmissionszweig sinkt die Sichtbarkeit dabei auf 99% und im Reflexionszweig auf 97%. Dieser Effekt kommt daher, dass die Beschichtung an der Grenzschicht eines polarisierenden Strahlteilers dieser Bauart nur für die vertikale Polarisationskomponente optimal realisiert werden kann. Ein kleiner Teil der horizontalen Komponente wird jedoch immer auch in den Reflexionszweig gelangen, wodurch die schlechteren Sichtbarkeiten von eingestrahltem Licht in diesem Reflexionszweig entstehen. Die Laserdioden wurden so eingestellt, dass ihre Polarisationen richtig, das heißt horizontal für den Transmissionszweig und vertikal für den Reflexionszweig, ausgerichtet sind. Nach den beiden polarisierenden Strahlteilern ist also die Sichtbarkeit des Lichtes aller vier Laserdioden größer als $99,6\%$. Für das BB84-Protokoll sind jedoch vier verschieden Polarisationsrichtungen (H, V, +45° und +45°) notwendig. Die beiden letzteren Polarisationen werden einfach durch Drehen der sauberen H-V-Polarisation um 45° erreicht. Dies wurde mit einem $\lambda/2$-Plättchen (Casix), dessen optische Achse unter $22,5°$ steht, realisiert (siehe Abbildung 4.3 auf Seite 32). Das Ergebnis sind nun zwei Lichtpfade, welche die vier benötigten Polarisationen repräsentieren.

Diese werden schließlich an einem normalen Strahlteiler (BS1, beamsplitter) in einen Pfad zusammengebracht. An normalen Strahlteilern wurden ebenfalls Testmessungen vorgenommen, um deren Verhalten für gewisse Polarisationen zu studieren. Auch hier

ist es so, dass sich in Transmissionsrichtung die Sichtbarkeit für beliebige Polarisationsrichtungen nur unwesentlich verschlechtert, in Reflexionsrichtung die Sichtbarkeit für 45° jedoch auf unter 80% sinkt. Daher wurde der Aufbau so geplant, dass die Polarisationen unter 45° im Transmissionszweig des normalen Strahlteilers liegen. Die Quarzplatte (QP) kompensiert die Doppelbrechung, welche an der Oberflächenbeschichtung und der Klebeschicht des normalen Strahlteilers BS1 entsteht.

Um im Ausgang einen parallelen Lichtstrahlen zu bekommen, müssen alle vier Strahlen mit eine Linse (L1, f=35cm) kollimiert werden. Wichtig dabei ist, dass der Abstand aller vier Laserdioden zur Linse genau der Brennweite der Linse entspricht und die Position der Laserdiode in der Ebene senkrecht zur Emissionsrichtung genau mit dem theoretischen optischen Weg übereinstimmt. Nur so ist gewährleistet, dass das Licht aller vier Quellen am Ausgang in die exakt gleiche Richtung geht. Diese Einstellung wurde mit Hilfe eines HeNe-Justierlaser bewerkstelligt, welcher in den Ausgang eingestrahlt wurde.

Das nächste optische Element im Aufbau der sendenden Einheit Alice ist der Abschwächer (Att., Attenuator). In den ausgesendeten Pulsen darf die Wahrscheinlichkeit, dass sich darin zwei oder mehr Photonen befinden, eine bestimmte Grenze nicht überschreiten. Da es noch keine einfachen Einzelphotonenquellen gibt, bleibt nur die Möglichkeit, die Pulse so weit abzuschächen, bis dieses Kriterium erfüllt ist. Im Falle dieses Experiments reichte eine Abschwächung von 1% aus. Dabei ist darauf zu achten, dass die vorhin genannte Wahrscheinlichkeit für alle vier Polarisationsrichtungen die gleiche ist. Dies wurde durch Einstellungen an den Blenden vor den Laserdioden und durch Verkippen der Laserdioden selbst erreicht.

Über den im Setup nun folgenden Strahlteiler (BS2) wird das Synchronisationssignal eingekoppelt. Für diese neue Art der Synchronisation ist eine heller, zirkular polarisierter Lichtpuls notwendig (genaue Beschreibung der Synchronisation siehe Kapitel 4.3.3). Die Quelle ist wieder eine Laserdiode gleicher Bauart wie oben erwähnt, deren Licht gleich anschließend mit einer Linse (L2, f=2cm) gebündelt wird. Nach einer Blende zur Einstellung des Strahldurchmessers und somit der Intensität, folgt ein $\lambda/4$-Plättchen, welches das linear polarisierte Licht der Laserdiode in zirkular polarisiertes Licht konvertiert. Über einen Spiegel (M1) und den Strahlteiler BS2 wird das Licht eingekoppelt, wobei auch hier auf die richtige Justage des optischen Weges geachtet werden muss.

Die nun folgenden beiden Spiegel (M2 und M3) dienen lediglich der Auskoppelung bei einer Übertragung über Luft, um den gesamten Ausgangsstrahl in eine bestimmte Richtung zu schicken. Die beiden Spiegel stehen im Experiment in einem wesentlich flacheren Winkel von nur einigen Graden zueinander (anders als in der Abbildung dargestellt), um durch die zweifache Reflexion die Güte Polarisationen nicht zu verschlechtern. Im Falle der Auskoppelung über Glasfaser folgt dem Strahlteiler BS2 sofort die Faser.

Der einzige kleine Nachteil dieses Aufbaus kommt von der Verwendung von vier verschiedenen Quellen. Die Aufnahme der Spektren der vier verwendeten Laserdioden hat gezeigt, dass alle in etwa auf einer Breite von 1nm (in halber Höhe) und in einem Bereich von $\pm$1nm um 853nm herum emittieren. Die Linienbreite ist bei allen Laserdioden die

gleiche, das Emissionsmaximum ist jedoch unterschiedlich. Ein etwaiger Abhörer könnte nun aus den Wellenlängen Information über den Polarisationszustand erlangen. Um die Wellenlängenunterschiede zu kompensieren, gibt es mehrere Möglichkeiten. Die vier Laserdioden könnten beispielsweise jede für sich auf 853nm stabilisiert werden. Diese Methode ist jedoch etwas aufwendig, vor allem in Bezug auf das Ziel, ein kompaktes und einfaches System zu entwickeln. Eine andere Möglichkeit ist das sogenannte „seeden“ der vier Dioden. Eine Referenzdiode, die etwa am Strahlteiler BS1 von oben einstrahlt, zwingt die anderen vier Laserdioden, auf dieser Referenzwellenlänge zu emittieren. Die Referenzdiode muss zeitlich nicht stabil sein, da sich ohnehin alle vier anderen Dioden der eventuell schwankenden Wellenlänge anpassen und für einen Abhörer somit jede Information verwischen. In einem Versuchsaufbau werden wir diese dritte Methode in nächster Zeit testen und dann in das bestehende Quantenkryptographie-Experiment integrieren.

Somit sind alle Voraussetzungen (Software, Hardware, Elektronik, Optik) gegeben, um die funktionierende Alice einigen Testmessungen zu unterziehen.

4.2.4. Testmessungen

2MHz-Pulse

Die Signale für die Laserdioden konnten an der Elektronik einfach gemessen werden und entsprachen den Erwartungen. Das Signal wurde aber auch nach den Laserdioden mit einem Powermeter gemessen. Im Software-Programm wurde die Option „H only“, „V only“ usw... und eine zyklische Ausgabe gewählt. Anschließend wurde an allen vier Laserdioden gemessen. In Abbildung 4.8 a.) sind drei aufeinander folgende Pulse dieses Signals zu sehen. Der Abstand von 500ns entspricht genau den 2MHz. Das Untergrundrauschen kommt von der Umgebung.

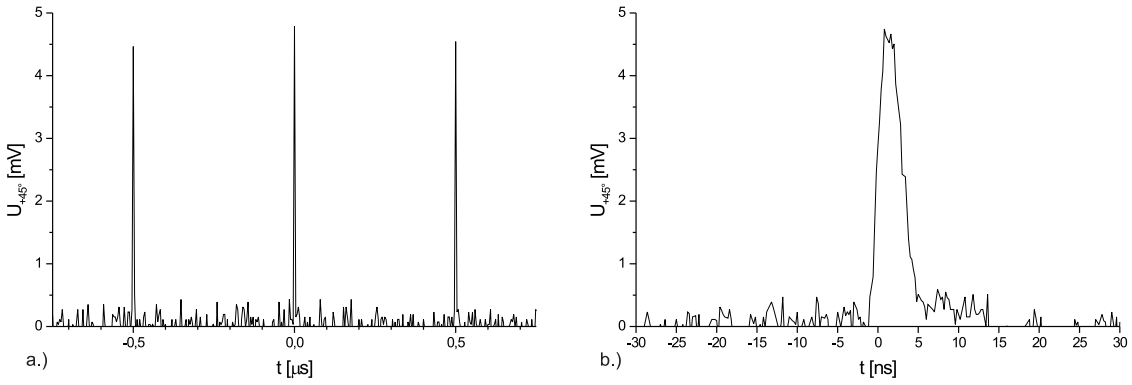


Abbildung 4.8.: 2MHz-Signal an der Laserdiode LD/+45°

Die Pulsdauer kann durch Variieren der Kippstufe (Monoflop) in der Elektronik recht einfach verstellt werden. Die Länge des Pulses hat Einfluß auf die Gesamtenergie des Pulses und somit auf die Photonenzahl in diesem Puls. Weiters hängt die Dauer des Zeitfensters bei Bob's Detektion direkt mit dieser Pulslänge zusammen. In Abbildung 4.8 b.) ist einer dieser 2MHz-Pulse zu sehen. Die eingestellte Pulsbreite von 5ns ist deutlich zu erkennen.

Synchronisationspulse

Die Synchronisationspulse (20kHz) werden in der Elektronik aus dem 2MHz-Signal erzeugt (100-Zähler). Der Abstand zwischen den an der Synchronisationsdiode LD/S gemessenen Pulsen beträgt 50μs was einer Frequenz von 20kHz entspricht. Die Pulsdauer stimmt mit dem eingestellten Wert von 1μs überein (siehe Abb. 4.9 a.) und b.)). An den Spitzen des 20kHz-Signals läßt sich deutlich erkennen, dass das Synchronisationssignal

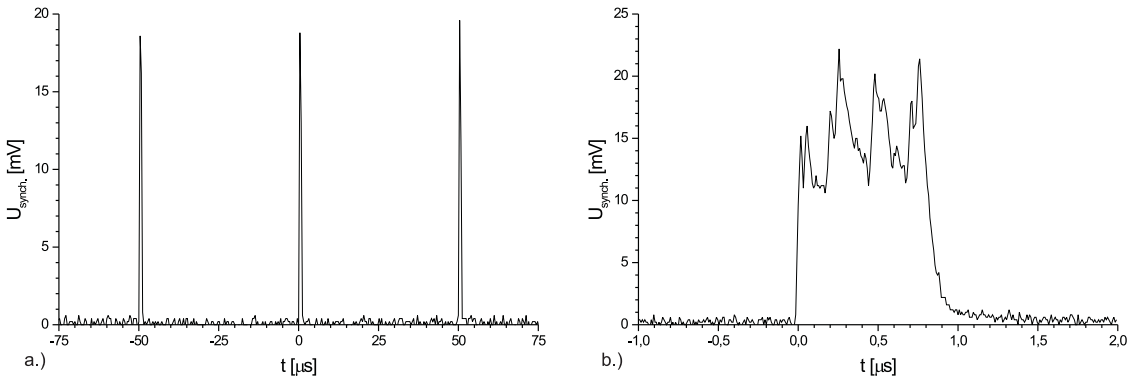


Abbildung 4.9.: 2MHz-Synchronisations-Signal an der Laserdiode LD/S

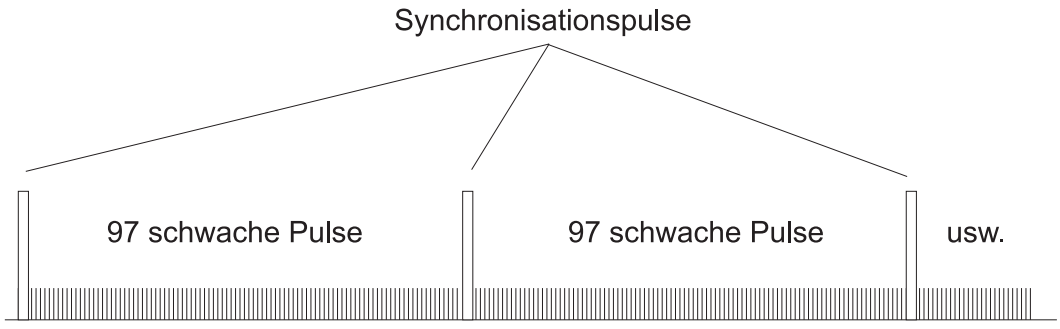


Abbildung 4.10.: Übertragungssequenz

aus dem 2MHz Signal erzeugt wurde. Aufgrund der Länge von 1μs des Synchronisationspulses überblendet dieser drei der schwachen Pulse, wodurch die Übertragungssequenz aus Startsynchronisationspuls, 97 schwachen Pulsen, dem nächsten Synchronisationspuls, 97 schwachen Pulsen usw. besteht (siehe Abbildung 4.10).

Polarisation

Dass die Bestimmung der Polarisation eines einzelnen Photons nicht möglich ist, wurde schon in Kapitel 3.2.2 auf Seite 17 gezeigt. Wohl aber kann man die Polarisation eines Ensembles von Photonen bestimmen. Dabei wird hinter der Quelle, in diesem Fall ist dies Alice, ein rotierbarer Polarisator als Analysator und eine SPAD als Detektor postiert (siehe Abb. 4.11). Im folgenden wird nun der Polarisator in definierten Gradschritten

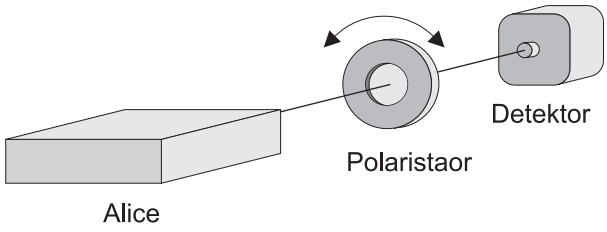


Abbildung 4.11.: Messung der Polarisation mit Polarisator und Detektor

rotiert und bei jeder Einstellung die Zählrate (Detektionen pro Zeiteinheit) notiert. Aus dem Maximum der gegen den Winkel aufgetragenen Zählraten (Sinus-Funktion) kann

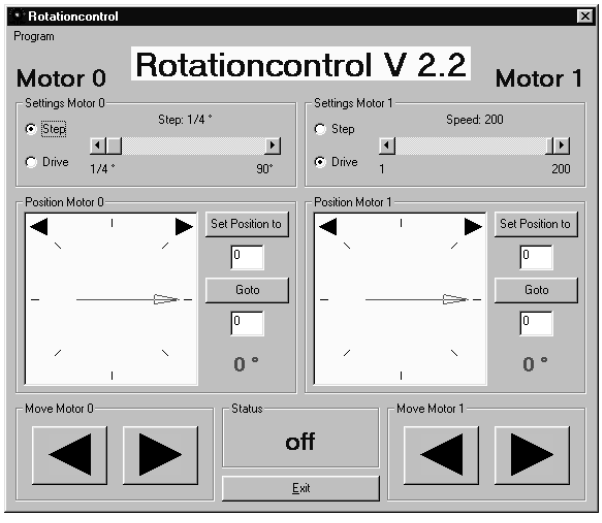


Abbildung 4.12.: Programm-Oberfläche der Schrittmotorsteuerung

die Polarisation bestimmt werden. Eine Aussage über die Qualität der Messung macht die Sichtbarkeit, welche in Prozenten angeben wird. Diese Analyse kann über Fitkurven in Origin gemacht werden.

Da eine derartige Messung ohnehin aufwendig ist und auch im gut abgedunkelten Raum stattfinden muss, wurde der Polarisator in eine Halterung montiert, welche von einem Schrittmotor bewegt werden konnte. Über die PC-Karte (SM30, Owis) kann dieser Schrittmotor angesteuert werden. Zur einfachen und genauen Bedienung wurde ein Programm (Rotationcontrol V2.2) erstellt (siehe Abb. 4.12). Diese Software erlaubt die Ansteuerung des Schrittmotors im schrittweisen (Step) bzw. fahrenden (Drive) Modus, wobei hierbei die Schrittweite ($\frac{1}{4}^\circ$ bis 90°) bzw. das Tempo (1 bis 200) eingestellt werden kann. Weiters besteht die Möglichkeit, die graphische Anzeige auf einen bestimmten Wert zu setzen (z. Bsp. nach einer Eichung auf 0°) und eine bestimmte Position mit dem Motor anzufahren (Zielfahrt). Die Position des Schrittmotors wird numerisch und graphisch angezeigt. Mit den Pfeiltasten am unteren Ende werden die Motoren bedient. Eine neuere Version dieses Programmes startet nach der Einstellung einer Position einen Meßvorgang, dessen Ergebnis in eine Datei eingelesen wird. Somit ist der gesamte Meßvorgang weitgehend automatisiert.

Zu Beginn der Messungen an Alice standen noch keine Detektormodule zur Verfügung. Daher wurden in einer ersten Testmessung die vier Laserdioden (LD/H, LD/V, LD/+45° und LD/+45°) jeweils im cw-Mode betrieben und die Sichtbarkeit der vier Dioden mit einem Powermeter aufgenommen. Das Ergebnis ist in Abbildung 4.13 graphisch dargestellt. Die hier nicht eingezeichneten Sichtbarkeiten betrugen für alle vier Polarisationsrichtungen in etwa 98%.

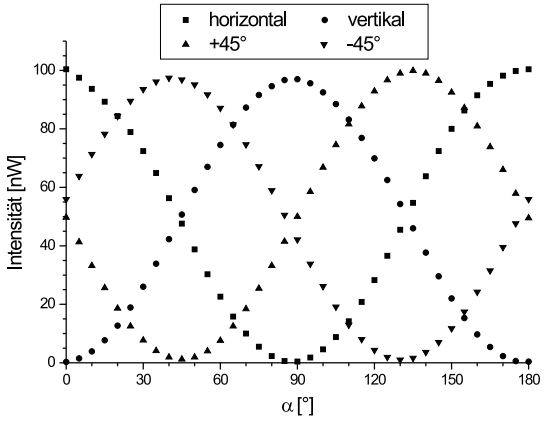


Abbildung 4.13.: Sichtbarkeit der vier Polarisationen bei Alice im cw-Betrieb

Als das erste Detektormodul fertiggestellt war, wurde obige Messung mit abgeschwächten Pulsen wiederholt. Die Schrittweite der Winkeleinstellung betrug dabei 5°

und die maximale Zählrate wurde auf 100.000 Zählungen pro Sekunde eingestellt. Dies wurde durch Suchen des Maximums bei der entsprechenden Diode und dem anschließenden Einstellen der Diodenintensität (Blende und Verkippen) erreicht. In der graphischen Darstellung (Abb. 4.14) wurde die Detektoreffizienz von 50% bereits brücksichtigt. Die

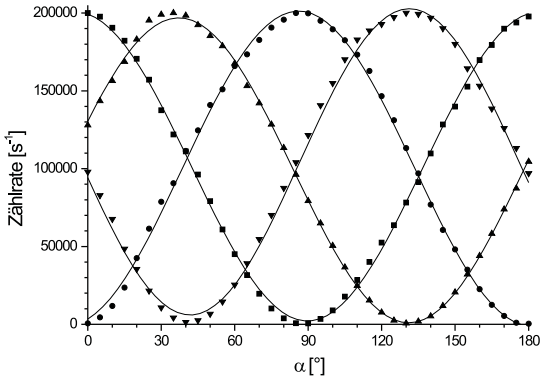


Abbildung 4.14.: Sichtbarkeit der vier Polarisationen bei Alice im gepulsten Betrieb

Zuordnung zwischen Symbol in der Darstellung und Polarisationsrichung entspricht der in Abbildung 4.13. Die hier eingezeichneten Fitkurven ergaben Sichbarkeiten von 99% für H und V bzw. 97% für $+45°$ und $-45°$. Diese Werte liegen im Bereich der Erwartungen. Relevant für eine Aussage über Übertragungsrate und Fehlerrate sind aber die Messungen auf Bob's Seite (siehe Kapitel 4.3.5 auf Seite 59).

Photonen pro Puls

Eine Messung, die jedoch in jedem Fall am Ausgang von Alice gemacht werden muss, ist jene der Bestimmung der Anzahl der Photonen in einem Puls. Diese Messung wurde mit dem in Abbildung 4.15 gezeigten Aufbau durchgeführt, wobei zur Bestimmung von n_1 (siehe Abb. 4.16) nur einer der beiden Detektoren registrierte und zur Bestimmung von n_2 die Koinzidenzen beider Detektoren gezählt wurden. Idealerweise sollte in jedem Puls genau ein Photon sein. In diesem Fall wäre die Strahlteilerattacke eines Abhörers zwecklos und die Übertragungsrate optimal. In diesem Experiment kann diese Bedingung aber nur durch Abschwächen der von den Laserdioden erzeugten Pulse realisiert werden. In Abbildung 4.16 ist die Anzahl der Pulse pro Sekunde mit zwei und mehr Photonen (n_2) gegen die Anzahl der Pulse pro Sekunde, welche überhaupt Photonen (n_1) enthalten. Rechts ist die Wahrscheinlichkeit aufgetragen, in einem der Pulse des 2MHz-Signals zwei oder mehr Photonen zu finden. Wählt man nun für diese Wahrscheinlichkeit 1%, erhält man 300.000 Pulse in der Sekunde (n_1), in welchen sich Photonen befinden. Das reduziert die ursprüngliche Frequenz von 2MHz auf etwa ein Zehntel. Die Bereitstellung von

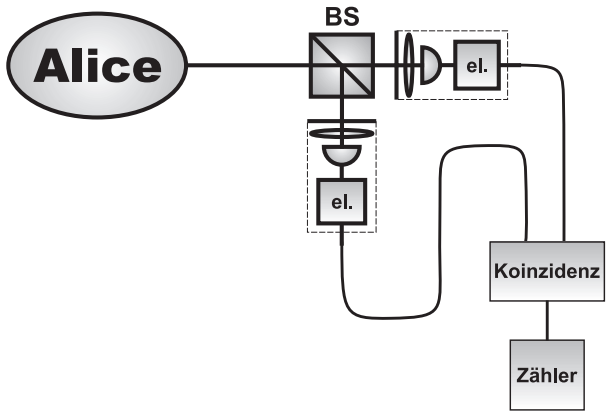


Abbildung 4.15.: Aufbau zur Messung der mittleren Photonenzahl

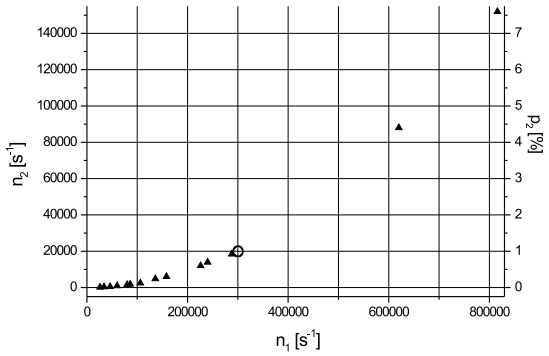


Abbildung 4.16.: Kurve zur Bestimmung der mittleren Photonenzahl

Pulsen mit einem Photon kostet bei einer derartigen Erzeugung somit 90% der Übertragungsrate. Aus diesem Grund ist man auch auf der Suche nach technisch einfachen und effizienten Einzelphotonenquellen.

4.3. Bob

Die Aufgabe von Bob ist es nun, die über den Quantenkanal ankommenden Photonen zufällig in einer der zwei Polarisationsbasen zu messen. Der optische Aufbau dafür ist in Abbildung 4.17 dargestellt und ist der gespiegelte Aufbau von Alice's Optik. Die zwei

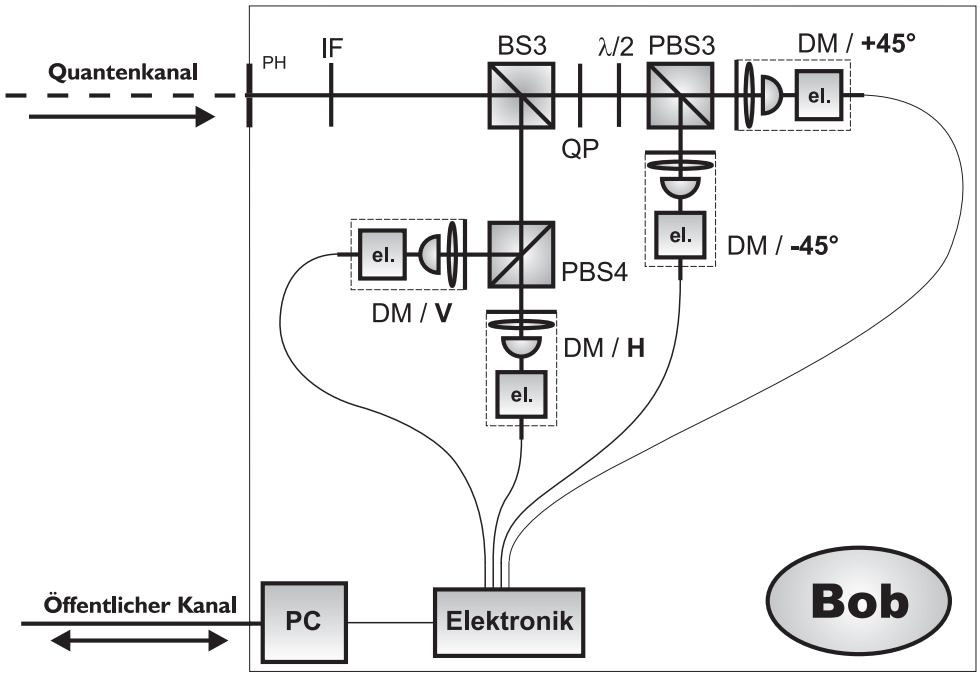


Abbildung 4.17.: Detaillierter optischer Aufbau von Bob

wesentlichen Elemente bei Bob sind die Synchronisationselektronik und die Detektoren. Erst durch eine gute und effiziente Synchronisation ist das zuverlässige Funktionieren des Protokolls gewährleistet. Schnelle, effiziente und kompakte Detektormodule resultieren in einer hohen Schlüsselrate und einer handlichen Bauweise.

4.3.1. Optik

Auch bei Bob's Optik wurde in diesem Experiment auf aktive Einheiten verzichtet und die gleichen optischen Bauteile wie bei Alice verwendet. Diese wurden in Kapitel 4.2.3 ausführlich beschrieben. Hier bleibt somit nur noch die Frage der Zufälligkeit der Polarisationsmessung übrig. Diese Zufälligkeit wird durch die Zufälligkeit der Transmission oder Reflexion eines Photons am normalen Strahlteiler (50%/50%) BS3 gewährleistet. Ein einkommendes Photon wird an diesem Strahlteiler unabhängig von der Polarisation mit gleicher Wahrscheinlichkeit, also zufällig, in den transmittierenden oder den reflektierenden Zweig geleitet. Die Entscheidung, welche Messbasis gewählt wird, fällt somit

zufällig im Strahlteiler BS3. Im transmittierenden Zweig wird dann die ±45°-Basis und im reflektierenden Zweig die H/V-Basis mit den im Folgenden beschriebenen Detektormodulen detektiert.

4.3.2. Detektormodul

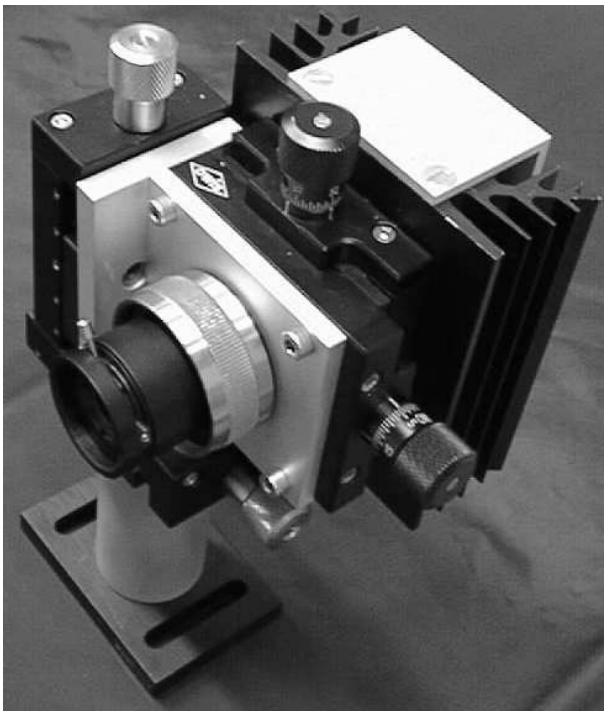


Abbildung 4.18.: Detektormodul

Einer der fünf angefertigten Detektormodule ist in Abbildung 4.18 zu sehen. Das Kernstück dieses Moduls ist eine Si-SPAD (Silicium Single Photon Avalanche Diode), welche mit einem mechanischen Umbau und einer Elektronik derart bestückt wurde, dass dies in einer einfach zu justierenden und kompakten Einheit resultiert. Die einzelnen Teile dieses Moduls werden im folgenden detailliert beschrieben.

Detektoren

Die Siliciumfläche ($25\mu m^2$) des Detektors (C309025-DTC, EG&G) ist in einem bereits evakuiertem Gehäuse auf einem zweistufigen Peltierelement platziert. Form, Abmessung und Pin-Belegung für die Diode mit integriertem Verstärker ist in Abbildung 4.19 zu sehen.

Für die hier beschriebenen Detektormodule wurden allerdings Dioden ohne internen Verstärker verwendet, wobei die Pin-Belegung hierbei wie folgt ist:

Bezeichnung	Pin
NTC1-1	4
NTC1-2	5
Peltier −	7
Peltier +	9
D1 −	2
D1 +	12

In dieser Aufstellung wurden für die Bezeichnung gleich die im Abschnitt Elektronik (ab Seite 48) verwendeten Namen notiert. Der große Vorteil der Bauweise dieser Diode ist die Tatsache, dass die eigentliche Detektorfläche selbst am Peltier-Element im inneren der Diode sitzt und somit nicht die ganze Diode gekühlt werden muss. Es muss daher nur darauf geachtet werden, dass das beim Kühlen sich erwärmende Gehäuse der Diode in Kontakt mit einem genügend großen Kühlkörper steht.

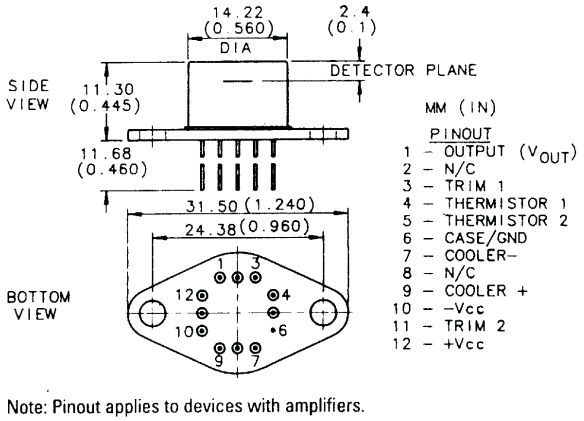


Abbildung 4.19.: Detektor

Mechanischer Aufbau

Ein Ziel war es auch, ein Modul zu bauen, welches schnell und einfach aufgestellt und justiert werden kann (Pläne dazu siehe Anhang A). Nach Fixierung des Detektors am optischen Tisch kann über vier Schlitten und einem Objektiv der Lichtstrahl optimal auf die Detektorfläche fokusiert werden (siehe Abb. 4.20). Mit den Schlitten x_1 und y_1 kann die gesamte Detektoreinheit so eingestellt werden, dass der Lichtstrahl genau durch den Mittelpunkt der im Objektiv eingebauten Linse (f=5cm) geht. Die mittlere Strahlhöhe

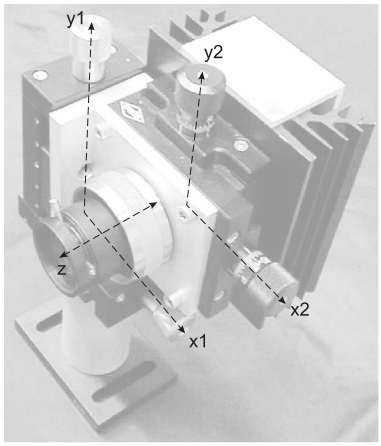


Abbildung 4.20.: Detektormechanik

beträgt 13cm, wobei diese durch den Schlitten y_1 um $\pm$1cm verschoben werden kann. Für größere Änderungen der Strahlhöhe müsste ein Sockel entsprechender Höhe verwendet werden. Anschließend kann die Brennebene mit dem Objektiv in z-Richtung verschoben werden, wobei das Objektiv die Linse dabei nicht dreht. Danach wird mit den Schiebern x_2 und y_2 die Detektorfläche genau in den Brennpunkt gefahren.

Elektronik

Die Beschaltung der sechs Pins der Si-SPAD kann auf unterschiedliche Weise erfolgen. Die einfachste Möglichkeit besteht im Verwenden einer externen Elektronik und Stromversorgung. Dabei müsste der Detektor mit mindesten acht Leitungen (je zwei bei Stromversorgung, Diode, NTC, Peltier) zu Elektronik und Stromversorgung verbunden werden. Auch das Übertragen des direkten Diodensignals über eine längere Strecke ist problematisch. Die wiederum unseren Zielen (Kompaktheit, einfache Bedienung) folgende Lösung bringt alle elektronischen Komponenten direkt im Kühlkörper der Diode unter, so dass von außen nur mehr die Stromversorgung angeschlossen und das aufbereitete Diodensignal (NIM) abgenommen werden muss. Als Netzgerät wurde das Modell SCL25-7608 verwendet, welches die Ausgänge +5V(2A) und $\pm$12V(1A, 0,2A) hat. Die Elektronik teilt sich in drei Teile (Spannungsversorgung, Kühlung und Signalaufbereitung), welche im Folgenden genau beschrieben werden.

Spannungsversorgung Die drei von dem Netzgerät gelieferten Spannungen reichen nicht für die Versorgung aller verwendeten elektronischen Bauteile aus. Benötigt werden neben den +5V noch -5,2V zur Versorgung der ECL-Bausteine und eine steuerbare Hochspannung (150-250V) für die Diode. Die Schaltung für die Erzeugung dieser Spannungen ist in Abbildung 4.21 zu sehen. Die +5V können direkt weiter verwendet werden.

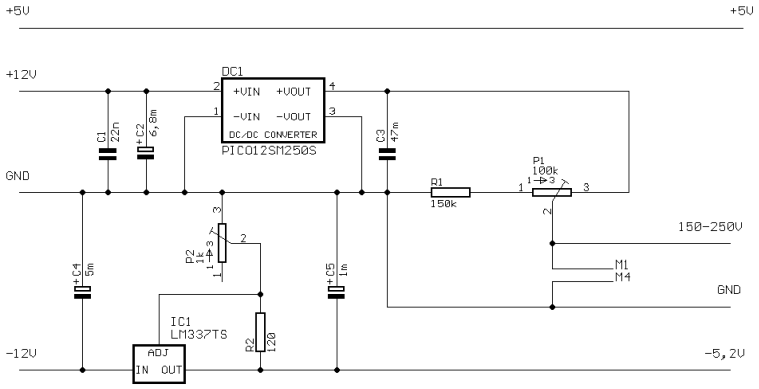


Abbildung 4.21.: Schaltung für die Spannungsversorgung

Zur Erzeugung der Hochspannung wurde ein DC-DC-Wandler (DC1) verwendet, welcher die +12V auf +250V transformiert. Der Wandler wurde primär- und sekundärseitig mit Kondensatoren gestützt, um die Hochspannung während der leitenden Phase der Diode konstant zu halten. Die variable Spannung (150-250V) wurde dann über einen regelbaren Spannungsteiler (R1, P1) realisiert. Dabei ist zu achten, dass durch die Belastung des Spannungsteilers das Teilerverhältnis nicht verfälscht wird. Die eingestellte Hochspannung kann von außerhalb des Moduls eingestellt werden und wird dem Benutzer über die beiden Messkontakte M1 und M4 zugänglich gemacht. Die Spannung von -5,2V wurde mit dem Spannungsregler IC1 realisiert. Dieser Regler wurde standardmäßig beschaltet, wobei zur genaueren Einstellung ein Widerstand durch ein Potentiometer (P2) ersetzt wurde.

Kühlung Die am Datenblatt der Si-SPAD vorgeschlagene Kühlung beruht auf einer

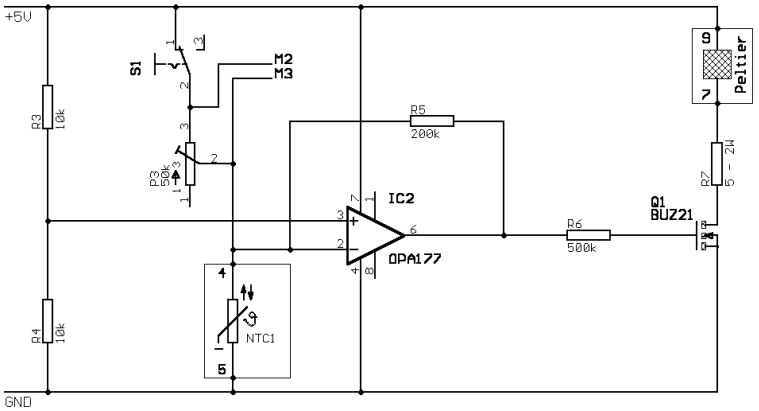


Abbildung 4.22.: Kühlungselektronik

Einpunktregelung. Ist die Temperatur der Diode unter den Regelwert gefallen wird der Kühlstrom über das Peltierelement ausgeschalten, steigt die Temperatur anschließend wieder über den Regelwert wird die Kühlung wieder aktiviert. Dabei werden Ströme von über 1A mit einer Frequenz von etwa 1Hz geschalten. Für ein stärkeres Netzgerät ist dies kein Problem. Die Netzgeräte welche wir verwenden wollten, schaffen diese Stromspitzen zwar, es werden jedoch alle Spannungsquellen des Netzgerätes davon beeinflusst. Daher wurde ein etwas abgewandelte Schaltung auf dem Prinzip eines Differenzverstärkers verwendet. Diese Schaltung (siehe Abb. 4.22) lässt vorerst maximalen Kühlstrom fließen und regelt nach Erreichen der eingestellten Kühltemperatur auf den Strom der nötig ist, um genau diese Temperatur zu halten. Die Kühlung wird sofort nach dem Einschalten der Spannungsversorgung aktiv und kann zuvor von außen über das Potentiometer P3 eingestellt werden. Die Temperatur kann durch Einstellen von P3 (Messung an M2 und M3 bei gedrücktem Taster S1) nach folgender Tabelle justiert werden:

Temperatur [°C]	P3 [kΩ]
+20	6,5
0	13,6
−20	31,6
−30	50,8

Der Kühlstrom fließt über das Peltierelement in der Diode und einem Leistungswiderstand, welcher derart dimensioniert wurde, dass der maximale Kühlstrom knapp oberhalb jenes Stromes liegt, der zum Halten der minimal einstellbaren Kühltemperatur nötig ist. Der Transistor (Q1) wird von dem OPV (IC2) anfangs solange ganz geöffnet, bis die Brückenschaltung (R3-R4 und P3-NTC1) abgeglichen ist. Die beiden Widerstände R5 und R6 wurden durch Ausprobieren so gewählt, dass der Einschwingvorgang auf die entsprechende Temperatur bei allen einstellbaren Werten rasch gedämpft wird. Die fertiggestellte Elektronik mit der Bezeichnung der Bauteile (Spannungsversorgung und Kühlung) ist Abbildung 4.23 zu sehen. Der Leistungswiderstand R7 befindet sich nicht auf dieser Platine sondern wurde aus Gründen der besseren Wärmeabfuhr am Gehäuse auf einen eigenen Kühlkörper montiert (siehe Abb. 4.32 auf Seite 57).

In den Abbildungen 4.24 a.) bis d.) ist der Kühlstrom über die Zeit bei verschiedenen Kühltemperaturen gemessen worden. Deutlich zu erkennen ist, dass die Kühlzeit mit abnehmender Kühltemperatur zunimmt und der Strom, der zum Halten dieser Temperatur nötig ist dabei ebenfalls steigt. Die Werte der Kühlzeit (Zeit, die vom Einschalten bis zum Erreichen der Temperatur verstreicht) und des Kühlstromes zum Halten der Temperatur in Abhängigkeit der Kültemperatur ist in den Abbildungen 4.25 a.) und b.) dargestellt. Daraus ist ersichtlich, dass die Kühlzeit exponentiell mit abnehmender Kühltemperatur zunimmt. Zwischen Kühlstrom und Kühltemperatur ist wiederum ein linearer Zusammenhang, da die Leistung und somit die transportierte Wärmeenergie mit dem Quadrat des Stromes geht.

Der Grund, warum die Diode überhaupt gekühlt wird, liegt an der Tatsache, dass sich Durchbruchspannung und Dunkelzählrate des Detektors mit der Temperatur entschei-

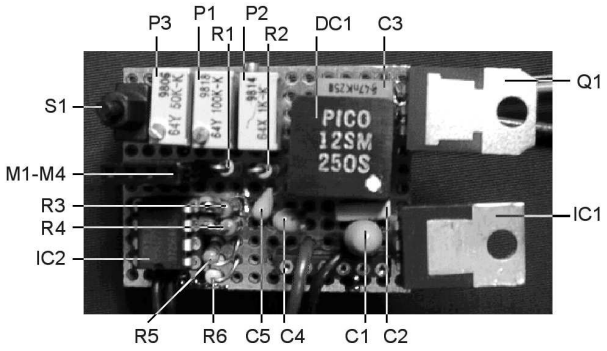


Abbildung 4.23.: Elektronik mit Spannungsversorgung und Kühlschaltung

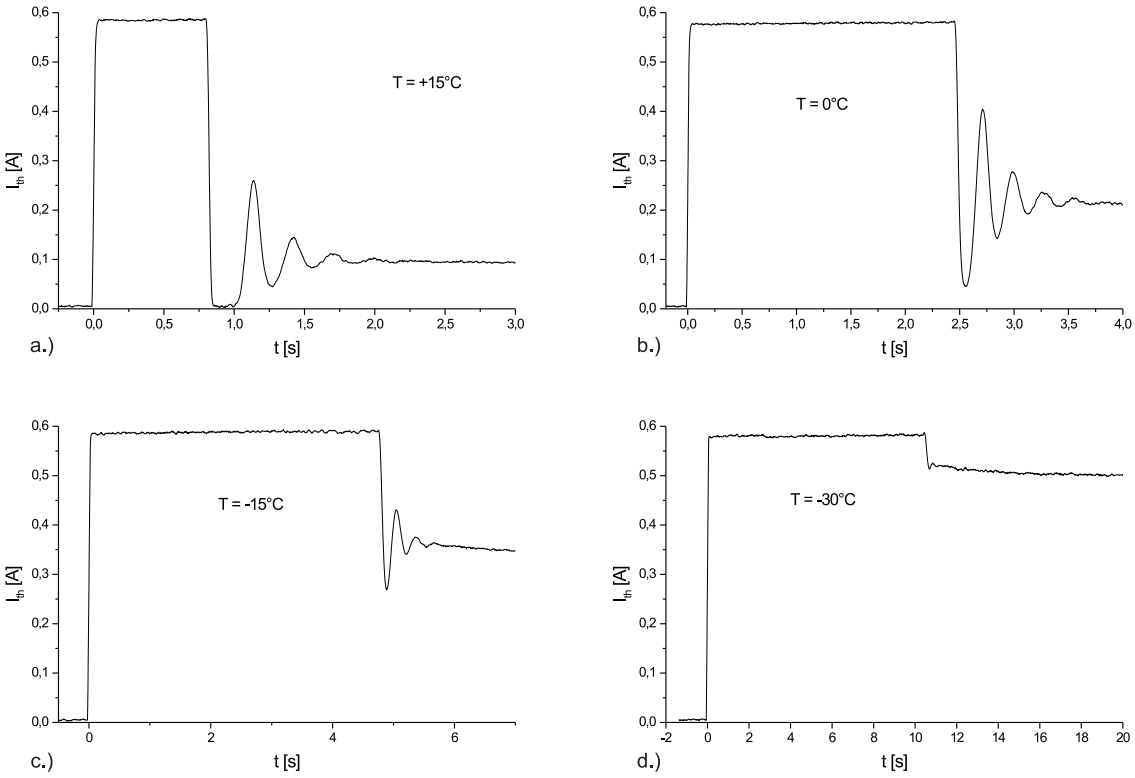


Abbildung 4.24.: Kühlkurven bei verschiedenen Temperaturen

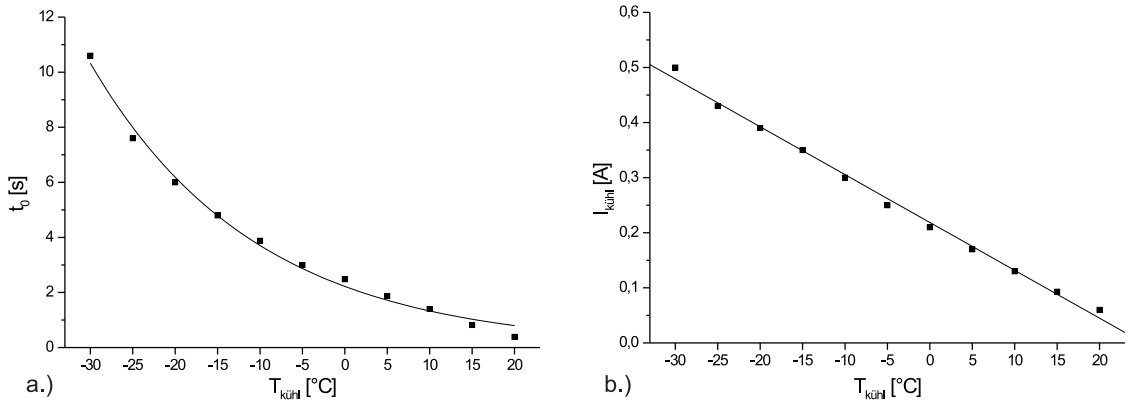


Abbildung 4.25.: Kühlzeit und Kühlstrom in Abhängigkeit von der Kühltemperatur

dend ändern. Die Durchbruchspannung ist jene Spannung, bei der einfallende Photonen es erstmals schaffen, in der Diode eine Elektronenlawine auszulösen. Das Photon erzeugt in der Siliziumschicht ein Elektron-Loch-Paar welches im elektrischen Feld der angelegten Spannung ein Lawine auslöst, welche die Diode zum Durchbruch bringt. Der nun fließende Strom muss durch eine entsprechende Schaltung wieder gelöscht werden

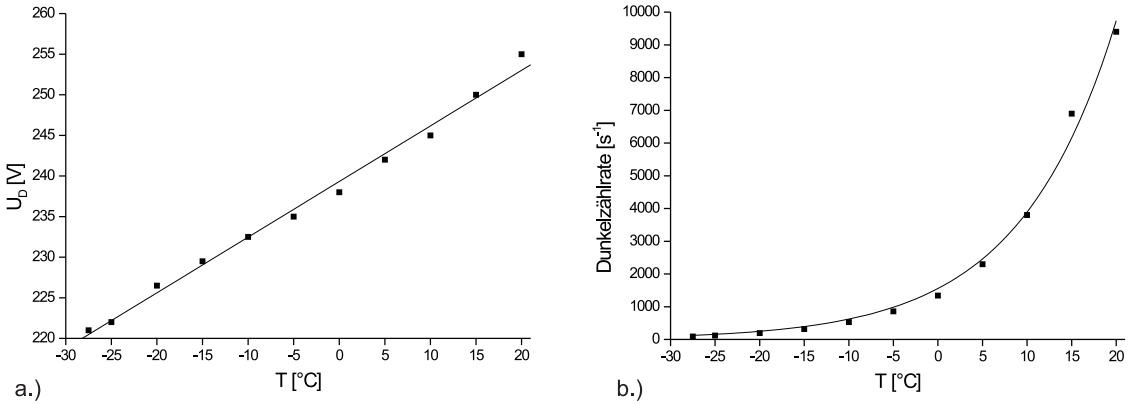


Abbildung 4.26.: Durchbruchspannung und Dunkelzählrate in Abhängigkeit der Kühltemperatur

(siehe Signalverarbeitungsschaltung auf Seite 53). Nun kommt es aber auch vor, dass eine derartige Lawine durch interne thermische Effekte ausgelöst werden kann. Die Anzahl dieser „Fehlzählungen“ pro Sekunde wird als Dunkelzählrate bezeichnet, weil dieser

Effekt auch bei völliger Dunkelheit auftritt. Durch senken der Temperatur kann die Dunkelzählrate gesenkt werden, wobei sich gleichzeitig die Durchbruchspannung verringert. Die Abhängigkeit dieser beiden Größen von der Temperatur ist in Abbildung 4.26 dargestellt. Dabei folgt die Durchbruchspannung einem linearen Verlauf und die Dunkelzählrate einem exponentiellen Zusammenhang. Ein Kühlen unter $-20°C$ bringt keine wesentliche Verbesserung der Dunkelzählrate mehr. Daher wurde die Kühlung auf diesen Wert eingestellt.

Signalverarbeitung Auf der zweiten Platine der Diodenelektronik ist die Beschaltung der Diode selbst und die Diodensignalverarbeitung untergebracht (siehe Abb. 4.27). Die variable Spannung von 150-250V liegt über eine Konstantstromquelle, welche vom Transistor Q2 und dem Potentiometer P4 gebildet wird, an der gesperrten Diode an. Bricht die SPAD aufgrund einer Photonenabsorbtion durch, so beginnt ein dauerhafter Strom über die Diode zu fließen, da diese im Geiger-Mode betrieben wird (angelegte Spannung ist größer als Durchbruchspannung). Dabei werden die Kapazitäten (interne Diodenkapazitat, Anschlusskapazitäten) entladen. Der Strom erzeugt am Widerstand R8 ein Spannungssignal, welches zur Detektion weiterverarbeitet werden kann. Nun muss der fließende Strom wieder gelöscht werden, um die Diode für die nächste Detektion vorzubereiten (quenching). Der Strom wird dabei durch das Potentiometer P4 derart begrenzt, dass sich die Diode selbst löscht. Anschließend kommt es zur Aufladung der vorher entladenen Kapazitäten. Erst wenn diese Aufladung nahezu restlos abgeschlossen ist, kann die Diode wieder detektieren. Wird anstelle des Potentiometers ein fixer Widerstand verwendet und der Transistor weggelassen, so entspricht dies der Standard Passiv-Quenching Methode und der Ladestrom folgt einer gewöhnlichen Ladekurve (exponentiell). Um diesen Vorgang zu beschleunigen, wurde in dieser Schaltung die Methode mit der Konstantstromquelle gewählt, da die Aufladung dabei linear und somit schneller erfolgt (siehe auch Abb. 4.31 auf Seite 56). Für weitere Details über SPAD sei hier auf die Diplomarbeit von Thomas Jennewein verwiesen, der diesem Thema ein ganzes Kapitel widmete ([20] Kapitel 4).

Das somit erzeugte Diodensignal am Widerstand R6 wird nun einer Schaltung zugeführt, welche dieses Signal in ein NIM-Signal wandelt. Zuerst wird das Diodensignal an einem schnellen ECL-Komparator (IC3) mit einem einstellbaren Triggerpegel (P5) verglichen. An den zwei invertierten Ausgängen (11, 12) des Komparators liegt nun ein dem Diodensignal entsprechendes ECL-Rechtecksignal an. Die Widerstände R9-R10 und R11-R12 bilden den für einen ECL-Ausgang nötigen Abschluss mit 100Ω auf $-2V$.

Die weitere Schaltung stellt einen schnellen Konverter des ECL-Signals auf ein NIM-Signal dar. Der Zwischenschritt über ein ECL-Signal wurde gemacht, da die ECL-Logik für schnelle Pulse am besten ist und aus dem ECL-Signal relativ einfach jeder beliebige Logik-Pegel ebenfalls mit einer schnellen Elektronik realisiert werden kann. Um ein NIM-Ausgangssignal (high $\equiv -1V$ bzw. 40mA über zwei parallele 50Ω Widerstände , low $\equiv$ 0V bzw. kein Strom) zu bekommen, muss bei „high“ und einem Pegel von $-1V$ über die

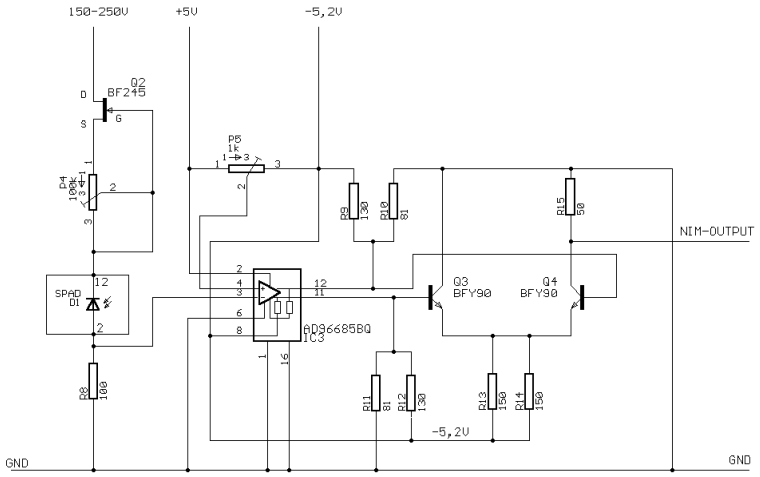


Abbildung 4.27.: Signalverarbeitungsschaltung

Parallelschaltung von R15 und dem Abschlusswiderstand am anderen Ende der Leitung (ebenfalls 50Ω) ein Strom von 40mA fließen. Somit fällt am R15 im leitenden Zustand von Q4 und am Transistor Q4 selbst je 1V ab. Am Punkt, der die Emitter von Q3 und Q4 verbindet soll demnach ein Potential von −2V vorherrschen. Die restlichen 3,2V auf −5,2V ergeben gemeinsam mit einem Strom von 40mA einen Widerstand von 75Ω, welcher durch die Parallelschaltung von R13 und R14 realisiert wurde. Der zweite Teil, der die eben beschriebene Elektronik enthält, ist in Abbildung 4.28 dargestellt.

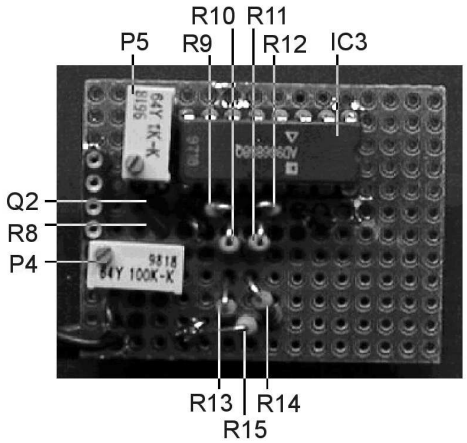


Abbildung 4.28.: Elektronik mit Signalverarbeitung

Im folgenden wurden einige Testmessungen an der Detektorelektronik durchgeführt und diverse Einstellungen (Größe des Konstantstromes, Höhe des Triggerpegels) op-

timiert. In Abbildung 4.29 ist der Zusammenhang zwischen Diodensignal und NIM-Ausgangssignal bei einem Triggerwert von 0,5V (a.)) und 1V (b.)) zu sehen. Das Diodensignal hat etwa ein Höhe von 1,2V und eine mittlere Breite von 5ns. Trotz Verwendung schneller Elektronikbauteile kommt es zu einer Verzögerung von etwa 4ns zwischen Schnittpunkt des Diodensignals mit dem Triggerpegel und der Anstiegsflanke des Ausgangssignals. Ein Nebeneffekt dieser Schaltung ist die Tatsache, dass die Pulsdauer

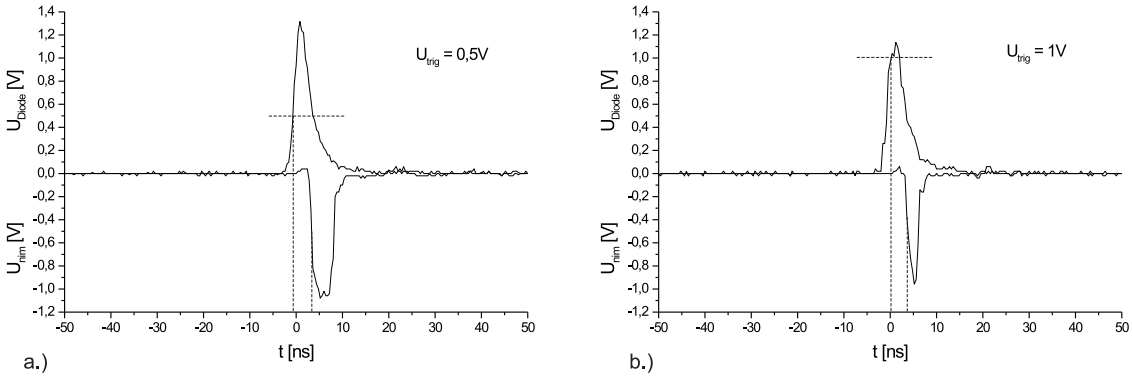


Abbildung 4.29.: Diodensignal - NIM-Signal

des Ausgangssignal indirekt über den Triggerpegel variiert werden kann. Im Falle eines Triggerpegels von 0,5V beträgt die Pulsdauer 5ns, bei 1V etwa 2ns. Der Pegel des NIM-Ausgangssignal liegt mit -1V genau im richtigen Bereich. Für das Experiment wird ein Diodensignal von etwa 5ns benötigt. Daher wurde der Triggerpegel auf 0,5V eingestellt.

Die nächste Abbildung zeigt zwei Messungen, welche bei unterschiedlichen Konstantströmen aufgenommen wurden. In Abbildung 4.30 a.) wurde mit dem Oszilloskop eine sogenannte Envelope-Messung durchgeführt. Dabei wird eine bestimmte Anzahl von Ereignissen in einem bestimmten Zeitausschnitt rund um ein getriggertes Signal aufgenommen. Der zentrale Peak ist das Diodensignal, auf welches getriggert wurde. Rechts daneben sind alle nachfolgenden Pulse aufgenommen. Noch bevor der Ladevorgang ganz abgeschlossen ist, kann die Diode aufgrund einer Photonenabsorbtion wieder durchbrechen. Durch diese Messpunkte können Geraden gelegt werden, welche die Ladekurven repräsentieren. Mit zunehmenden Strom werden die Ladezeiten kürzer. Wird der Strom allerdings zu groß gewählt, kann die Diode nicht mehr selbstständig löschen, was zu einer Zerstörung der Diode führen kann. Der Konstantstrom wurde folglich auf den größten Wert eingestellt, bei dem gerade noch ein sicheres Löschen gewährleistet wird. In diesem Fall beträgt die Totzeit (Zeit, welche nach einer Detektion verstreicht, bis die Diode wieder scharf ist) etwa 2μs. Durch einen höheren Strom und somit einer kleineren Totzeit muss natürlich die Zählrate höher und über einen größeren Bereich linear sein. Die Ergebnisse der Messung dieses Effektes in ist Abbildung 4.30 b.) zu sehen. Dabei wurde hinter

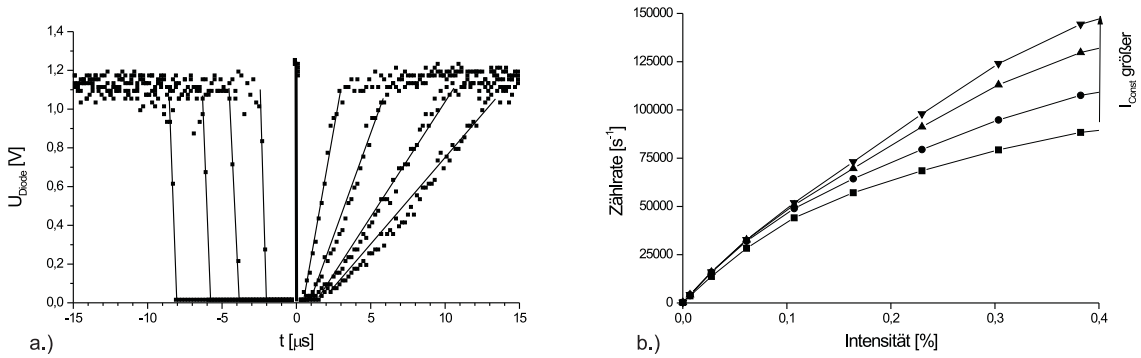


Abbildung 4.30.: Ladevorgang (a.)) und Zählrate (a.)) bei verschieden starken Konstantströmen

einer polarisierten, schwachen Lichtquelle ein Polarisator durchgedreht und von der Polarisatorstellung sinusförmig abhängige Intensitätsverteilung auf eine lineare Prozentskala umgerechnet. Diese Messung wurde bei vier verschiedenen Strömen aufgenommen. Die absoluten Werte der Ströme wurden nicht bestimmt. Bei dem eingestellten, maximal möglichen Strom konnte ein recht guter linearer Verlauf bis etwa 100.000 Zählungen pro Sekunde erreicht werden, was mit der Totzeit von 1μs im Einklang steht.

In Abbildung 4.31 soll der Unterschied zwischen einfachem passiv-quenching mit einem Widerstand und dem Löschen mit einer Konstantstromquelle gezeigt werden. Die Methode mit dem Konstantstrom liegt bei höheren Zählraten deutlich über der Methode, bei der nur ein Widerstand verwendet wird. Auch der lineare Bereich ist bei der hier verwendeten Methode größer.

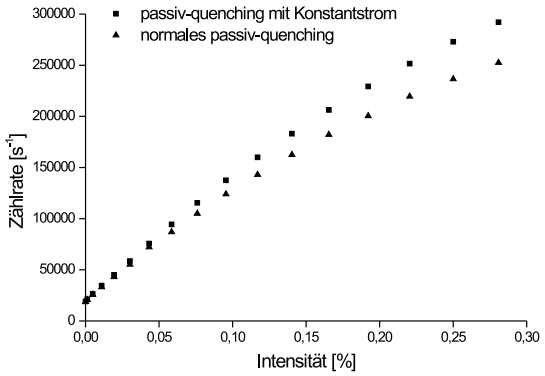


Abbildung 4.31.: Passiv-quenching mit und ohne Konstantstromquelle

Gesamtmodul

Das hier beschriebene Detektormodul besteht aus einer einfach zu bedienenden aber sehr effektiven mechanischen Justiereinheit. Die Inbetriebnahme und Verwendung des Detek-

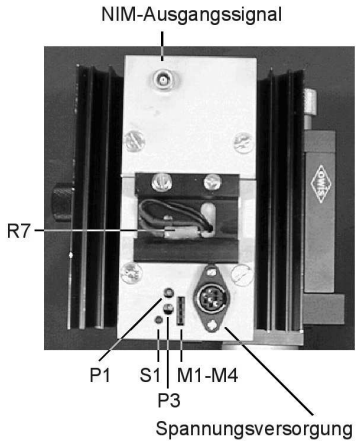


Abbildung 4.32.: Hinterseite des Detektormoduls mit Anschlüssen

tors beschränkt sich auf die Bereitsstellung der Energieversorgung (Anschluß Netzgerät) und der Weiterverwendung des gelieferten NIM-Diodensignals. Weiters können vom Benutzer jederzeit die Kühltemperatur und die Spannung an der Diode eingestellt werden, was für unterschiedliche Einsätze des Detektormoduls sehr von Vorteil ist. Die Rückseite des Detektormoduls mit allen Bedienelementen ist in Abbildung 4.32 dargestellt.

4.3.3. Elektronik

Die Elektronik von Bob hat die Aufgabe, zuerst einmal mit Hilfe des von Alice gesendeten Synchronisationssignals die eigene Detektion zu synchronisieren und weiters die daraus resultierenden Detektionen einer digitalen Ein-/Ausgabekarte zum Einlesen in den PC zur Verfügung zu stellen. Die Elektronik wurde von Surasak Chiangga entwickelt und ist in seiner Dissertation ausführlich beschrieben [19]. Die Elektronik hat als Eingänge die NIM-Ausgangssignale der vier Detektormodule (H,V,+45° und −45°). Die Synchronisationspulse, welche Alice sendet, sind helle, zirkular polarisierte Lichtpulse (siehe LD/S in Abb. 4.3 auf Seite 32). Dieser Puls löst eine gleichzeitige Detektion in allen vier Detektoren aus. Diese Vierfachkoinzidenz wird von einem schnellen Und-Gatter erkannt und erzeugt somit ein 20kHz-Signal. Dieses Signal wird in einer dreifachen Verstärkerstufe und nach Filterung der hohen Harmonischen von 2Mhz dazu verwendet, um einen 2MHz-Quarz gleicher Bauweise wie bei Alice anzutreiben. Dieses so erzeugte Signal wurde bisher nur auf elektrischem Wege mit dem ursprünglichen 2MHz-Signal bei Alice verglichen. Dabei ergab sich nach 100 Pulsen (dies ist genau der Abstand zwischen

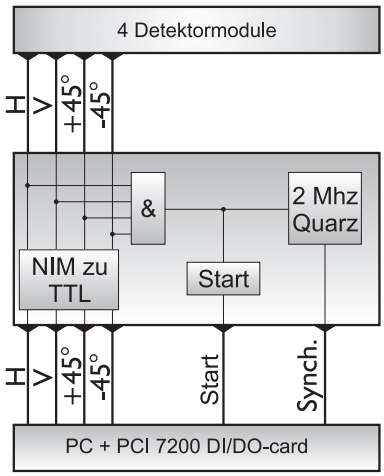


Abbildung 4.33.: Blockschaltbild von Bob's Elektronik

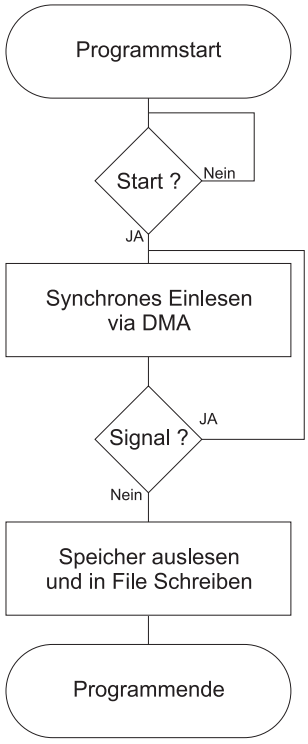


Abbildung 4.34.: Flußdiagramm von Bob's Software

zwei Synchronisationspulsen) ein relativer Unterschied der beiden Signale von nur 3ns. Dies ist für dieses Layout des Experiments ausreichend. Die Wahrscheinlichkeit einer zufälligen vierfachen Koinzidenz der Detektoren, was die Synchronisation stören würde, ist vernachlässigbar gering.

Bevor die Übertragung beginnen kann, muss Bob's Software aktiv sein. Die Digitalkarte wartet dann auf das Startsignal, was dem ersten Synchronisationspuls entspricht. Über die Synchronisation werden die in ein TTL-Signal konvertierten Detektionen getriggert und über die Digitalkarte in den PC eingelesen. Das Einlesen wird fortgeführt, solange die Digitalkarte ein Synchronisationssignal erhält. Die Länge der Übertragung muss Bob also vor dem Start nicht bekannt sein.

4.3.4. PC & Programm

Das Flussdiagramm von Bob's Programm wird die in Abbildung 4.34 gezeigte Form haben. Nach Programmstart wartet die Software auf das Startsignal. Nach erfolgtem Start werden die Daten via DMA erfasst und nach Ende der Übertragung werden diese Werte in einer Datei gespeichert. Anschließend kann über die Schritte 2 bis 4 des BB84-Protokolls (siehe Kapitel 3.3.1 auf Seite 21) der geheime Schlüssel gewonnen werden.

4.3.5. Testmessungen

Um eine vorzeitige Abschätzung der erwarteten Übertragungs- und Fehlerrate zu erhalten, wurde eine Testmessung für Bob mit den Detektoren aufgebaut (siehe Abb.4.35). Die dabei noch nicht implementierte Synchronisation verbessert den Wert der Fehler-

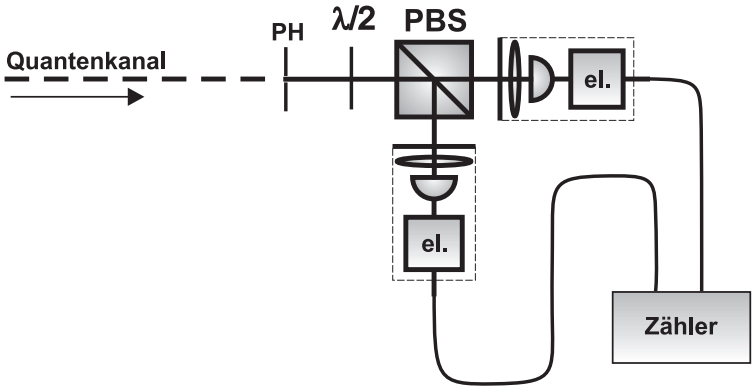


Abbildung 4.35.: Aufbau für Bob's Testmessung

rate, da die Detektoren im endgültigen Experiment nur dann für eine Detektion scharf sind, wenn ein Photon erwartet wird. Diese Faktor wurde hier bereits berücksichtigt. In Abbildung 4.36 sind die aufgenommen Sichtbarkeiten auf Bob's Seite zu sehen. Aus den

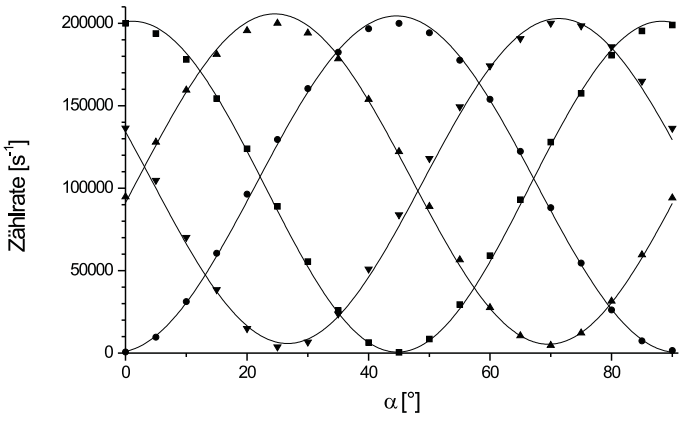


Abbildung 4.36.: Testmessung Bob

Maximum einer Polarisationsrichtung und dem Minimum der senkrecht dazu stehenden Richtung wurden für die vier Polarisationsrichtungen folgende Fehlerraten berechnet.

Polarisation	Fehlerrate
H	0,33%
V	0,22%
+45°	2,68%
−45°	1,61%

Daraus ergibt sich eine mittlere Fehlerrate von 1,21%. Diese Fehlerrate lässt sich durch genaueres Justieren des endgültigen Bob-Setups sicher noch verbessern.

Die Übertragungsrate lässt sich durch Verfolgung des Signals von der Erzeugung bis zur Detektion kalkulieren. Die anfängliche Frequenz von 2MHz reduziert sich am Ausgang von Alice bereits auf 200kHz, da das Signal aufgrund der Einzelphotonenbedingung nur in jedem zehnten Puls ein Photon beinhaltet. Die Verluste entlang der Übertragung sind von Distanz und Art abhängig und können für eine Übertragungsstrecke von etwas mehr als 3km und einer Dämpfung von 3dB/km mit 90% angegeben werden. Bei Bob ist die Wahrscheinlichkeit, in der richtigen Basis zu messen, 50%, was die Übertragungsrate wieder halbiert. Die Detektoreffizienz von ebenfalls 50% reduziert die Rate wiederum auf die Hälfte. Die weitere Verarbeitung der Daten erfolgt verlustlos. Daraus sollte sich eine endgültige Übertragungsrate im Bereich von einigen kHz ergeben.

5. Vergleich mit bestehenden Experimenten

In diesem vorletzten Kapitel werden einige bereits realisierte bzw. momentan in Verwendung stehende Experimente vorgestellt und in einer abschließenden Tabelle die wichtigsten Kenndaten der Experimente direkt verglichen.

5.1. Innsbruck

Zweimal wurden an der Universität Innsbruck Experimente zum Thema Quantenkryptographie aufgebaut. Das erste Experiment [21] basierte auf der interferometrischen Quantenkryptographie. Das Herzstück des Gesamtaufbaues (siehe Abb. 5.1) bildete ein Mach-Zehnder-Doppelinterferometer. Nach langer und genauer Justage des Gesamtex-

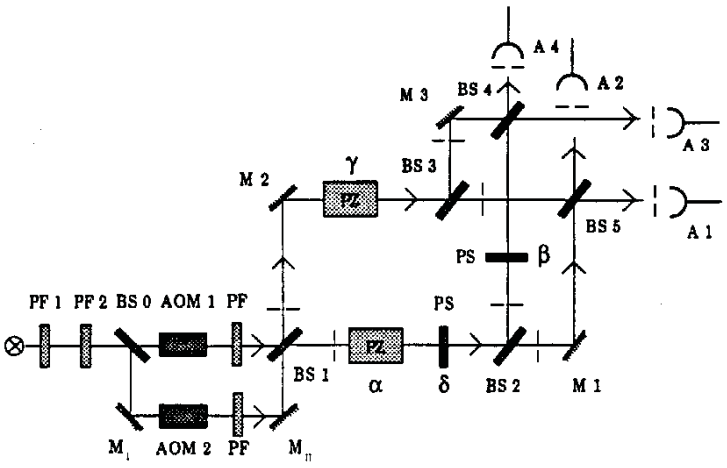


Abbildung 5.1.: Gesamtaufbau des ersten Quantenkryptographie-Experiments an der Universität Innsbruck

periments konnte schließlich über ein Quantenkryptographie-Protokoll eine Schlüsselvereinbarung realisiert werden. Aus einer Sequenz von 100.000 Pulsen innerhalb von

fünf Minuten konnte ein Schlüssel in der Länge von etwa 5.200 Bits gewonnen werden. Dies entspricht einer Übertragungsrate von etwa 17Hz. Aus der Sichtbarkeit (80%) der Messkurven lässt sich eine Fehlerrate von 11% errechnen. Bei einer Abbildung eines Teiles des Gesamtschlüssels ist vermerkt, dass das Verhältnis zwischen 0en und 1er im Schlüssel etwa 42:58 ist (Asymmetrie der Detektoren).

Das zweite Experiment zu Quantenkryptographie [22] an der Universität wurde 1997 durchgeführt. Wie der Abbildung 5.2 zu entnehmen ist, gleicht der Plan dieses Experiments in den wesentlichen Zügen dem in dieser Diplomarbeit Beschriebenen. In dem

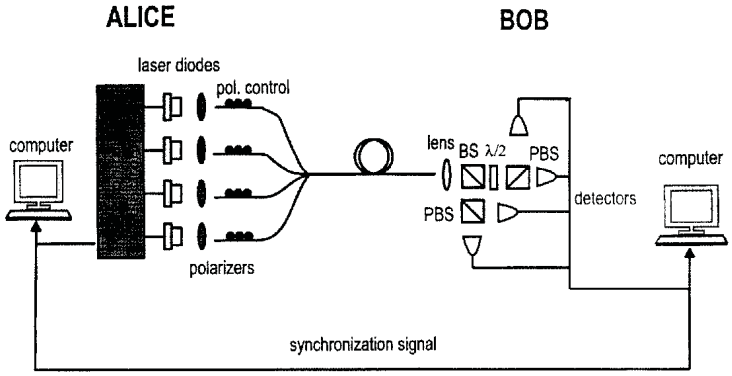


Abbildung 5.2.: Plan des zweiten Quantenkryptographie-Experiments an der Universität Innsbruck

Experiment wurde vor allem der vierfache Faserkoppler und die Reproduzierbarkeit der Polarisation nach einer Übertragung über Glasfaser (2m) untersucht. Unter Verwendung von Single-Mode-Einkopplern und Mikroskopobjektiven konnte eine Sichtbarkeit bei allen vier Polarisationsrichtungen von 98% erreicht werden. Dies ergibt eine Fehlerrate für die Übertragungsstrecke von 2%. Diese Fehlerrate darf allerdings nicht mit der Gesamtfehlerrate verglichen werden, da zu dieser noch die Fehlerrate der gesamten Empfangseinheit hinzukommen. Die Grundfrequenz für die Übertragung ließ sich in acht Stufen zwischen 62,5kHz und 16Mhz einstellen.

5.2. BT

In den BT (British Telecom) Laboratorien wurde 1995 der in Abbildung 5.3 dargestellte Quantenkryptographie-Aufbau getestet [23]. Dabei wurden Schlüsselvereinbarungen mit unterschiedlichen Längen der Übertragungsstrecke und Variieren der Photonenzahl pro Puls (μ) durchgeführt. Ein Halbleiterlaser emittiert Lichtpulse bei einer Wellenlänge von 1,3μm, einer Pulslänge von 80ps und einer Wiederholrate von 1MHz. Der anschließende Abschwächer kann zwischen verschiedenen Werten geschalten werden ($\mu = 2$ für

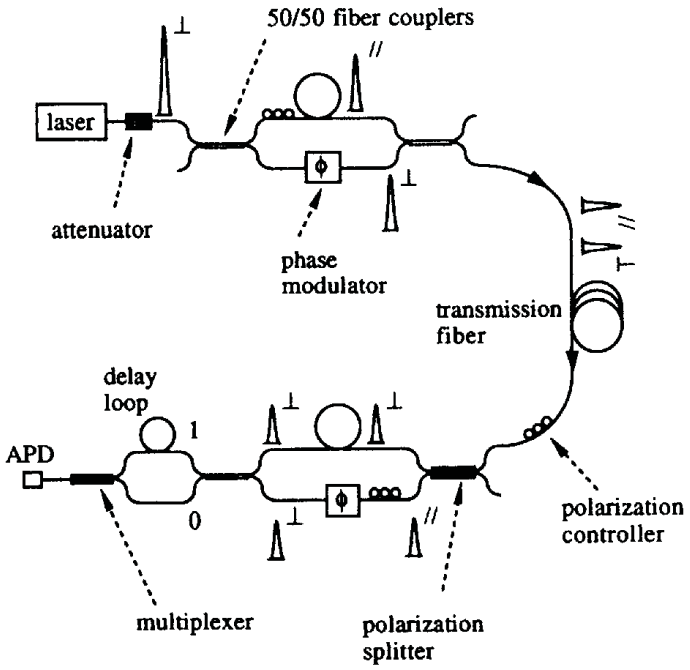


Abbildung 5.3.: Quantenkryptographie-Experiment von BT (British Telecom)

Justierzwecke und $\mu = 0.2$ bzw. $\mu = 0.1$ für unterschiedliche Photonenzahlen bei der Schlüsselvereinbarung). Die Übertragungsstrecke (Faser in Labor auf Rolle) konnte auf eine Länge von 10.5, 21.8 und 30km eingestellt werden. Die Detektion erfolgte mittels Ge-SPAD, welche im Geiger-Mode betrieben und mit flüssigem Stickstoff gekühlt wurden. Die Detektoren wurden über eine Synchronisation (im Artikel nicht näher beschrieben) für eine Zeit von 100ns alle 1μs scharf gemacht, wodurch die Dunkelzählrate der Detektoren auf 10 Zählungen pro Sekunde reduziert wurde.

Im ersten Schritt der Schlüsselvereinbarung sendet Alice helle Lichtpulse ($\mu = 2$), damit Bob sein Interferometer eichen kann. Ist dies erfolgt, sendet Bob Alice den Startpuls und die Übertragung beginnt. Die Eichung erfolgt ca. alle 5s, um thermische Driften zu kompensieren. Folgende experimentelle Ergebnisse werden im Artikel präsentiert:

Länge [km]	μ	Fehlerrate [%]	Übertragungsrate [Hz]
10.8	0.1	1.5	700
10.8	0.2	1.2	1400
21.8	0.1	4	350
21.8	0.2	2.8	700
30	0.2	4	260

Hätte man beim dritten Eintrag in der vorigen Tabelle ideale Bauteile zur Verfügung,

könnte die Übetragungsrate auf fast 40kHz erhöht werden. Zu Verlusten kam es in diesem Experiment vor allem an den Phasenmodulatoren, der Glasfaser und den Detektoren.

5.3. Genf

An der Universität Genf wird an der Realisierung eines interferometrischen „Plug and Play“-Quantenkryptographie-Experiments gearbeitet [24][25]. Der experimentelle Aufbau des bereits getesteten Experiments ist in Abbildung 5.4 zu sehen.

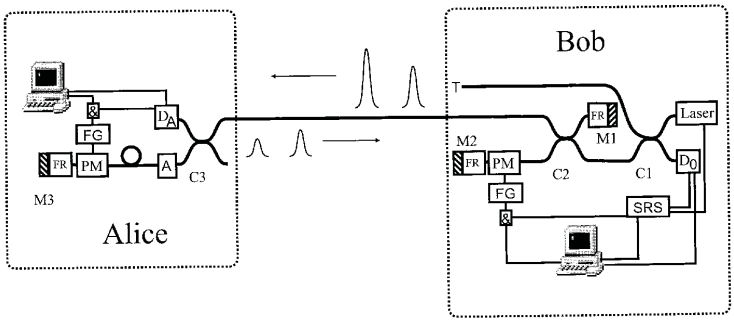


Abbildung 5.4.: Aufbau des „Plug and Play“-Quantenkryptographie-Experiments der Universität Genf

Das Setup besteht aus einem Michelson-Interferometer (Strahlteiler C2), welches im Prinzip zweimal verwendet wird. Bob erzeugt mit seinem Laser Pulse, welche am Strahlteiler C2 aufgespaltet werden. Ein Teil (P1) geht über den kurzen Arm bei Bob durch den Phasenmodulator (PM) und dann über die beiden Faraday-Spiegel (M2, M1) zu Alice (dort ebenfalls durch einen Phasenmodulator) und wieder zurück. Der zweite Teil (P2) läuft zuerst zu Alice und dann durch den kurzen Arm bei Bob. Da beide Pulse exakt den gleichen Weg zurücklegen, interferieren sie maximal am Strahlteiler C2. Alice und Bob wählen nun zufällig Phasenschübe. Ist die Differenz dieser Phasenschübe gleich 0, ergibt dies am Strahlteiler C2 konstruktive Interferenz und Bob wird am Detektor D−0 ein Photon messen. Eine Differenz der Phasenschübe von π ergibt am Strahlteiler C2 destruktive Interferenz und Bob bekommt keine Detektion. Der Abschwächer (A) bei Alice ist so dimensioniert, dass der Puls P1 am Ausgang von Alice eine mittlere Photonenzahl von $\mu = 0.05$ hat. Da beide Pulse (P1 und P2) exakt die gleiche Strecke durchlaufen, justiert sich das Interferometer quasi selbst. Die Sichtbarkeit ist dadurch auch unabhängig von dem Teilungsverhältnis des Strahlteilers C2. Die Sichtbarkeit ist jedoch stark von der Polarisation der Pulse abhängig. Die Pulse unterliegen einer Polarisationsmodulation in den verschiedenen optischen Bauteilen des Setups. Aus diesem Grund wurden vor den drei Spiegeln Faraday-Rotatoren angebracht, welche die ankommende Polarisation um 90° drehen. Jedem Puls wiederfährt diese Transformation drei

mal und die Effekte der Polarisationsmodulation werden kompensiert.

Im Test wurde eine Schlüsselübertragung über 23km Glasfaser durchgeführt, wobei eine bereits (unter dem Genfer See) verlegte Telekom-Faser verwendet wurde und die beiden Einheiten (Alice und Bob) örtlich getrennt angeordnet waren. Bei einer mittleren Photonenzahl pro Puls von $\mu = 0.1$ und einer Sichtbarkeit von 99.8% wurde ein 20kbit langer Schlüssel mit einer Übertragungsrate von 1Hz und einer Fehlerrate von 1.35% generiert. Zur Zeit wird an einem Aufbau mit 2.5MHz Grundfrequenz über 20km gearbeitet. Die endgültige Übertragungsrate soll dann im kHz-Bereich liegen.

5.4. Los Alamos

Ein Quantenkryptographie-Experiment über eine Glasfaserstrecke von 48km wurde in Los Alamos realisiert [26]. In Abbildung 5.5 ist der Aufbau des Experiments zu sehen. Die Übertragungsstrecke führte über das LANL-Gelände und Alice und Bob waren auf einem optischen Tisch nebeneinander untergebracht. Auch dieses Experiment basiert

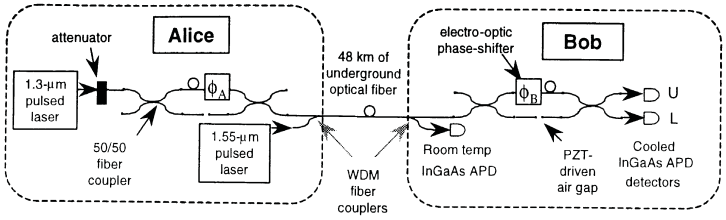


Abbildung 5.5.: Setup des Quantenkryptographie-Experiments in Los Alamos

auf der interferometrischen Quantenkryptographie. Die Einzelphotonen werden dabei mit 300ps langen Pulsen (100kHz Wiederholrate) einer mit einer Glasfaser verbundenen Halbleiterlaserdiode mit anschließendem Abschwächer erzeugt ($\mu = 0.63$). Die Synchronisation erfolgt über einen hellen Puls, welcher sofort nach dem signifikanten Photon geschickt wird und am Eingang von Bob mit einer bei Raumtemperatur betriebenen InGaAs-SPAD detektiert wird. Die Detektoren zur Messung der Einzelphotonen sind ebenfalls InGaAs-APD, welche allerdings gekühlt werden.

Mit diesem Aufbau konnte eine Schlüsselübertragungsrate von etwa 10Hz bei einer Fehlerrate von 9.3% erreicht werden, wobei 90% der Fehlerrate von der Dunkelzählrate der Einzelphotonendetektoren kommt.

In Los Alamos wurde 1997 auch ein Quantenkryptographie-Experiment mit Übertragung über Luft realisiert (xxx.lanl.gov, LA-UR-97-1975). Mit einer Grundfrequenz von 20kHz wurde ein Schlüssel über eine Übertragungsstrecke von 205m mit einer Fehlerrate von 6% und einer effektiven Schlüsselrate von 250Hz erzeugt. Momentan wird in Los

Alamos an einem Experiment gearbeitet, welches Quantenkryptographie über Luft über eine Strecke von 2 bis 7km unter Tageslichtbedingungen erlaubt [27].

5.5. Vergleichstabelle

In der nun folgenden Tabelle sind alle in diesem Kapitel vorgestellten Experimente in ihren wichtigen Daten gegenüberestellt. Die letzte Zeile beinhaltet die erwarteten Daten für das in dieser Diplomarbeit beschriebenen Quantenkryptographie-Experiments. Die Übertragungsrate bezeichnet die Rate der tatsächlich erzeugten Schlüsselbits. Falls nicht anders vermerkt bezieht sich die Länge der Übertragungsstrecke auf Glasfaserverbindungen.

Experiment	Länge [km]	Übertragungsrate [Hz]	Fehlerrate [%]
Innsbruck 1 (Seite 61)	50cm	17	11
Innsbruck 2 (Seite 62)	2m	n.s. [1]	2 [2]
BT (Seite 62)	30	260	4
Genf (Seite 64)	23	1	1.35
Los Alamos (Seite 65)	48	10	9.3
dieses Experiment (Seite60)	1m [3]	einige 1000 [5]	1.21 [6]

[1] nicht spezifiziert, Grundfrequenz 62.5kHz bis 16MHz
[2] nur Übertragungsstrecke
[3] über Luft
[4] zu erwartende Rate, alle Verluste eingerechnet
[5] aus Testmessung für Gesamtaufbau abgeschätzt

6. Zusammenfassung

Ziel der Diplomarbeit war es, alle Komponenten für einen kompakten, schnellen und einfach zu bedienenden Quantenkryptographie-Aufbau zu testen mit denen in einem nächsten Schritt ein funktionierendes Quantenkryptographie-Experiment realisiert werden kann.

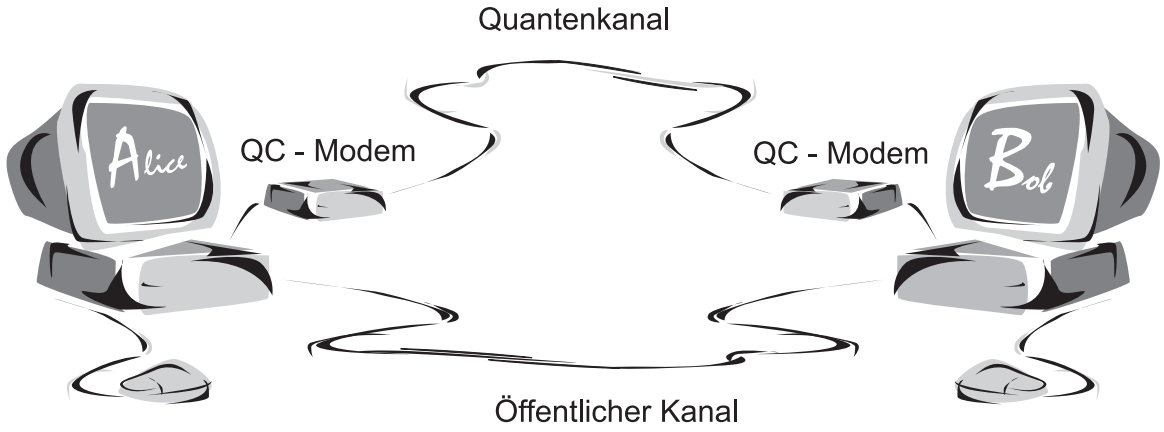
Schon sehr bald konnte eine funktionierende Sendeeinheit (Alice) getestet werden, welche alle Erwartungen erfüllte und sich im Laufe der Zeit als sehr stabile Einheit für weitere Experimente erwies. Mit einer Grundfrequenz von 2MHz sendet Alice 5ns breite Pulse mit einer mittleren Photonenzahl von $\mu = 0.1$, deren Polarisation zufällig in einer der vier Richtung H, V, $+45°$ oder $-45°$ liegt, wobei jeder Puls einer bestimmten Polarisationsrichtung von einer separaten Laserdiode erzeugt wird. Die Sichtbarkeit am Ausgang von Alice beträgt für die H/V-Polarisation 99% und für die $\pm 45°$-Polarisation 97%. Für die neuartige Synchronisation in diesem Experiment sendet eine fünfte Laserdiode jeden 100sten schwachen Puls einen hellen, zirkular polarisierten Puls mit einer Länge von 1μs. Der Ausgang kann mit ein Teleskopsystem über Luft oder mit einem Faserkoppler über Glasfaser ausgekoppelt werden. Für den gesamten Aufbau wurden keine aktiven optischen Komponenten verwendet. Die optischen Elemente wurden über eine Elektronik und einen PC angesteuert. Alle verwendeten Teile wurden so gewählt, dass einer Verkleinerung der sendenden Einheit Alice auf die Größe eines herkömlichen Modems oder einer PC-Steckkarte nichts mehr im Weg steht.

Der Schwerpunkt beim Aufbau der Empfangseinheit Bob lag in der Entwicklung von kompakten und einfach zu bedienenden Detektormodulen. Das Kernstück eines derartigen Moduls bildet eine Si-SPAD. Diese Diode wurde mit einer Elektronik beschaltet, welche ein einfaches Einstellen der Kühltemperatur (Raumtemperatur bis $-30°$C) und der Spannung über Durchbruch von außen erlaubt. Nach dem richtigen Positionieren mit der ebenfalls sehr kompakt implemtierten Justiereinheit wird dem Anwender nur mehr das Verbinden mit dem Netzgerät und das Abnehmen des NIM-Signals abverlangt. Die Dunkelzählrate der Detektormodule liegt bei etwa 200 Zählereignisse pro Sekunde und die Zählrate hat einen linearen Bereich bis etwa 100.000 Ereignisse pro Sekunde. Mit diesen angefertigten Detektormodulen konnte ein Testaufbau für Bob realisiert werden. Die aus den Ergebnissen der Messung abgeleiteten Werte von einer Übertragungsrate im kHz-Bereich und einer Fehlerrate unter 2% sind bemerkenswert und das erfreuliche Ergebnis meiner Diplomarbeit.

Trotz dieser bereits sehr guten Resultate soll der Blick in die Zukunft gehen und dar-

an gearbeitet werden, diese Werte weiter zu verbessern. Das Konzept von Alice könnte dahingehend verbessert werden, als dass die vier Laserdioden auf einem Halbleiterstück direkt nebeneinander sitzen und somit Platz sparender untergebracht wären. Die weiteren optischen Komponenten (Strahlteiler, $\lambda/2$-Plättchen) könnten direkt berührend angeordnet werden oder in einem Stück gefertigt werden. Der Umstieg auf SMD-Bauweise bei den Elektronikteilen könnte die Größe der Elektronik um mehr als den Faktor zehn verringern. Die Übertragungsrate kann in dem bestehenden Konzept sowohl auf Bob's als auch auf Alice's Seite sehr einfach erhöht werden. Die Detektoren sind sicher jene Einheiten, welche bei Bob den größten Raum beanspruchen. Auch hier geht die Überlegung dahin, alle vier Detektoren auf einem Halbleitermaterial unterzubringen. Für Optik und Elektronik gilt hier das Gleiche wie bei Alice.

Ein großer Teil der hier angeführten Verbesserungsvorschläge wird in der nächsten Stufe dieses Experiments implementiert werden. Vielleicht sieht die Version X dieses Projekts ja wie die nun folgende letzte Abbildung aus...



Literaturverzeichnis

[1] 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.

[2] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

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

[4] Sir R. F. Burton. *The Kama Sutra of Vatsyana.* Arkana/Penguin, 1991.

[5] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT-22:644–654, November 1976.

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

[7] 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.

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

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

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

[11] G. Weihs. *Ein Experiment zum Test der Bell'schen Ungleichung unter Einstein'scher Lokalität.* Dissertaion, Universität Wien, 1999.

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

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

[14] N. Lütkenhaus. Estimates for practical quantum cryptography. *xxx.lanl.gov*, quant-ph/9806008-v2:1–26, 1999.

[15] C.H. Bennet and G. Brassard. The dawn of a new era. *Sigact News*, 30(4):78, 1989.

[16] W.K. Wootters and W.H Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[17] J.I. Cirac and N. Gisin. Coherent eavesdropping strategies for the 4 state quantum cryptography protocol. *xxx.lanl.gov*, quant-ph/9702002:1–6, 1997.

[18] G. Zeng and X. Wang. Attacks of bb84 protocol in quantum cryptography. *xxx.lanl.gov*, quant-ph/9812022:1–9, 1998.

[19] S. Chiangga. *A Prototype Quantum Cryptography System.* Dissertation, Universität Innsbruck, 1999.

[20] T. Jennewein. *Synchrone Erfassung von Photonendetektionen an entfernten Orten.* Diplomarbeit, Universität Innsbruck, 1997.

[21] B. Erckert. *Aufbau eines Quantenkryptographieexperimentes.* Diplomarbeit, Universität Innsbruck, 1994.

[22] R. Haselsberger. *Aufbau eines Quantenkryptographieexperiments.* Diplomarbeit, Universität Innsbruck, 1997.

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

[24] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, and G. Ribordy. Quantum cryptography. *Appl. Phys. B*, 67:743–748, 1998.

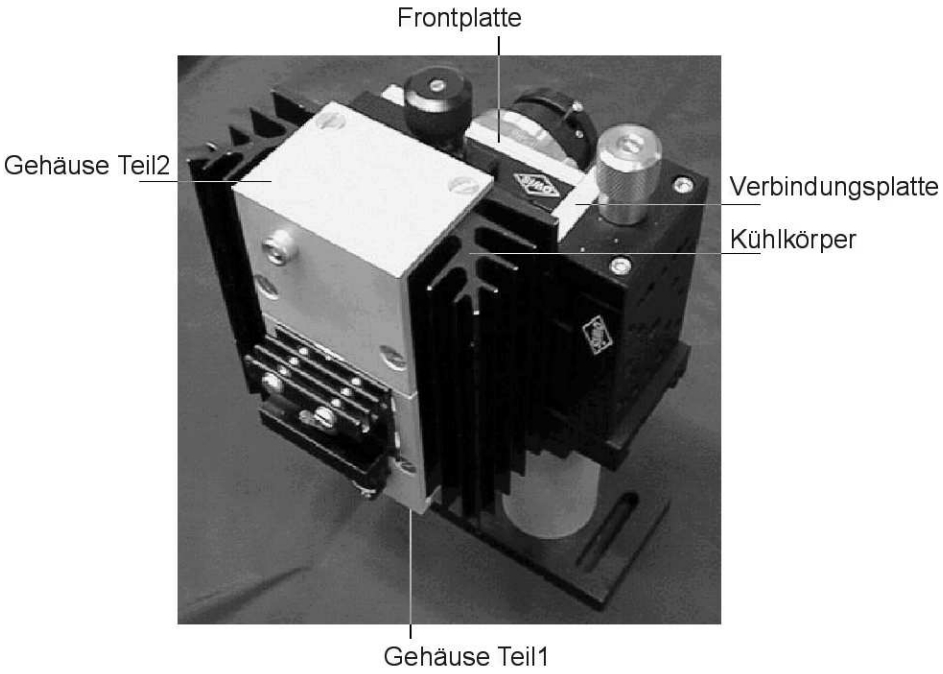
[25] A. Muller, T. Herzog, B. Huttner, W.Tittel, H. Zbinden, and N. Gisin. „plug and play“ systems for quantum cryptography. *Appl. Phys. Lett.*, 70(7):793, 1997.

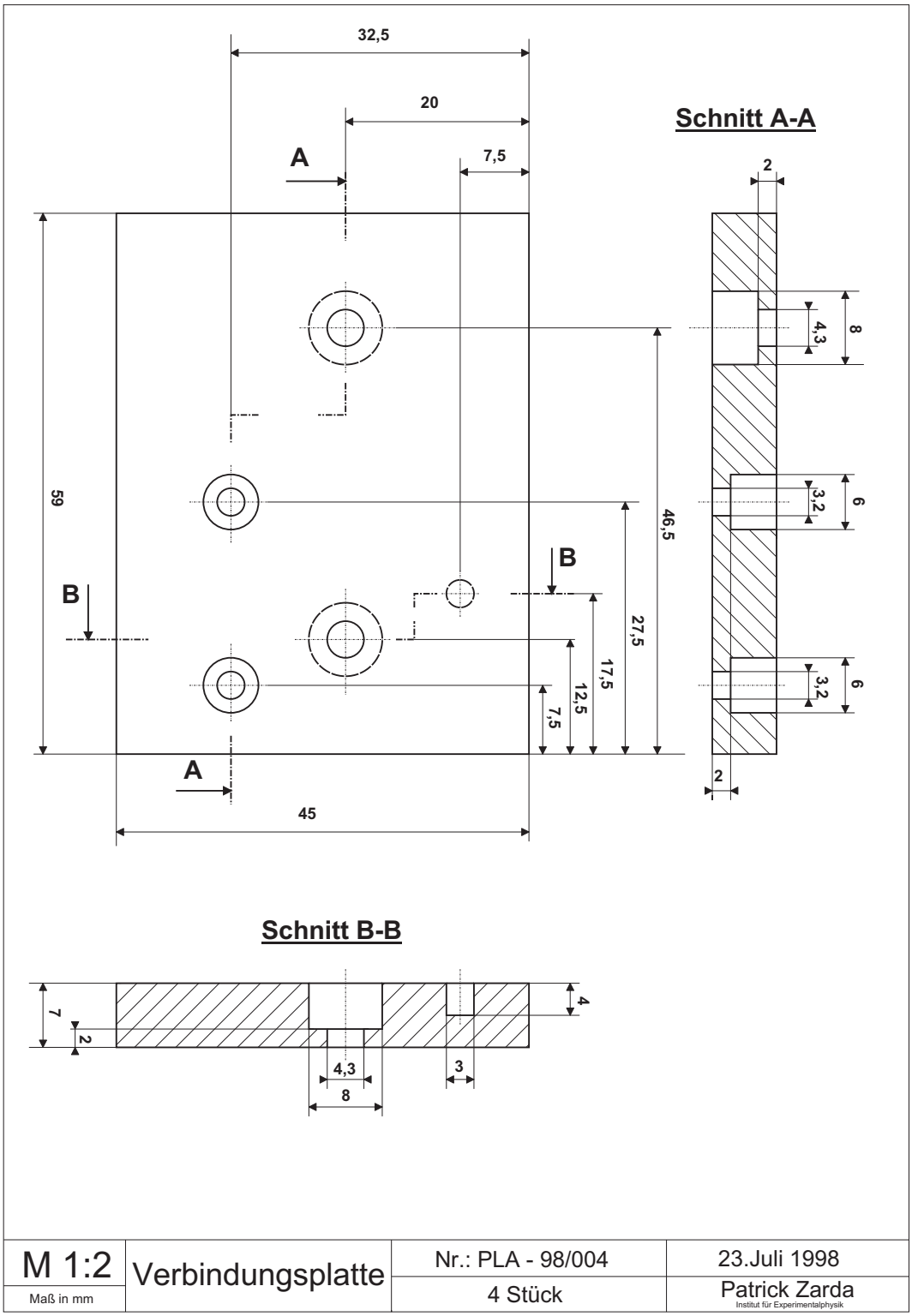
[26] R.J. Hughes, G.G Luther, G.L. Morgan, C.G. Peterson, and C. Simmons. Practical quantum key distribution over a 48-km optical fiber network. *Lecture Notes in Computer Sience*, 1109:329–338, 1996.

[27] R.J Hughes et al. Practical quantum cryptography for secure free-space communication. *xxx.lanl.gov*, quant-ph/9805009:1–12, 1999.

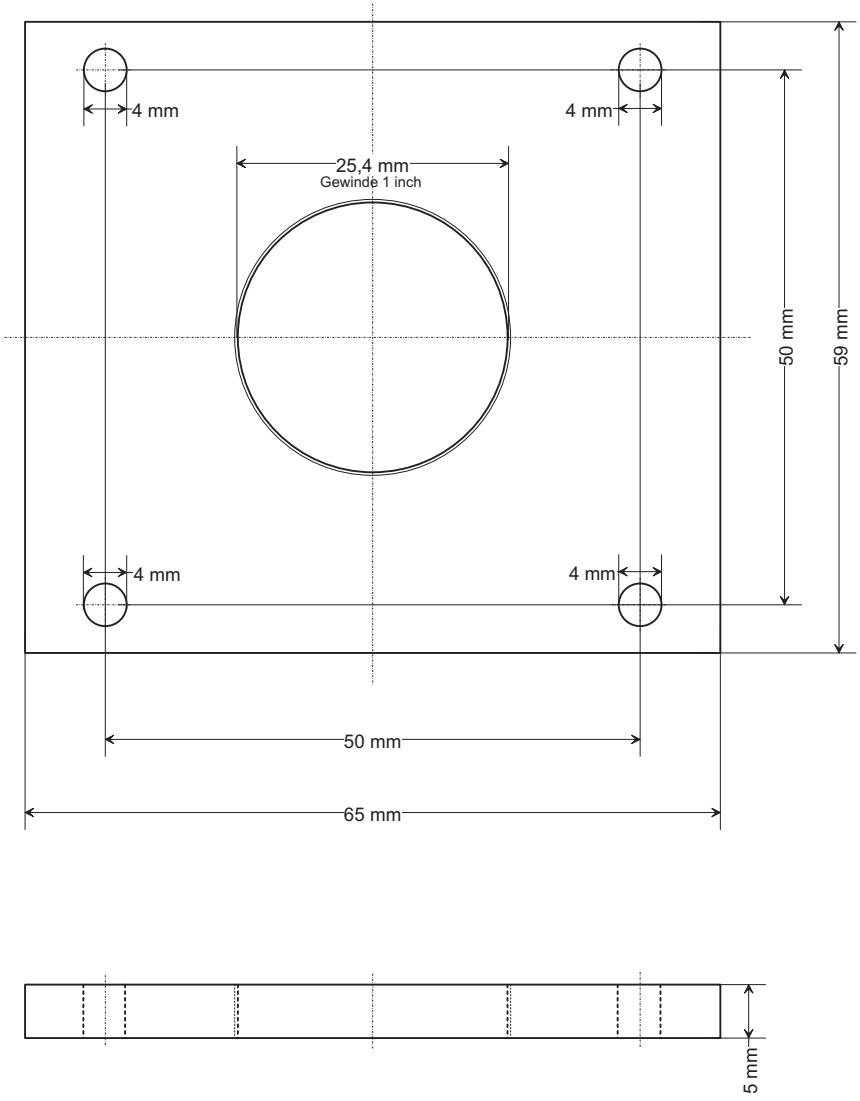
A. Pläne

Die Pläne auf den folgenden fünf Seiten (VI bis X) beziehen sich auf die in der unten abgebildeten Ansicht bezeichneten Teile des Detektormoduls und wurden in der dem Institut für Experimentalphysik zugehörigen mechanischen Werkstätte gefertigt. Der Sockel, auf dem das Detektormodul befestigt ist, besteht aus einem fünf Zentimeter dickem Aluminium Zylinder, welches an Ober- und Unterseite mittels Gewindebohrungen mit dem Schlitten bzw. der Bodenplatte verschraubt ist.

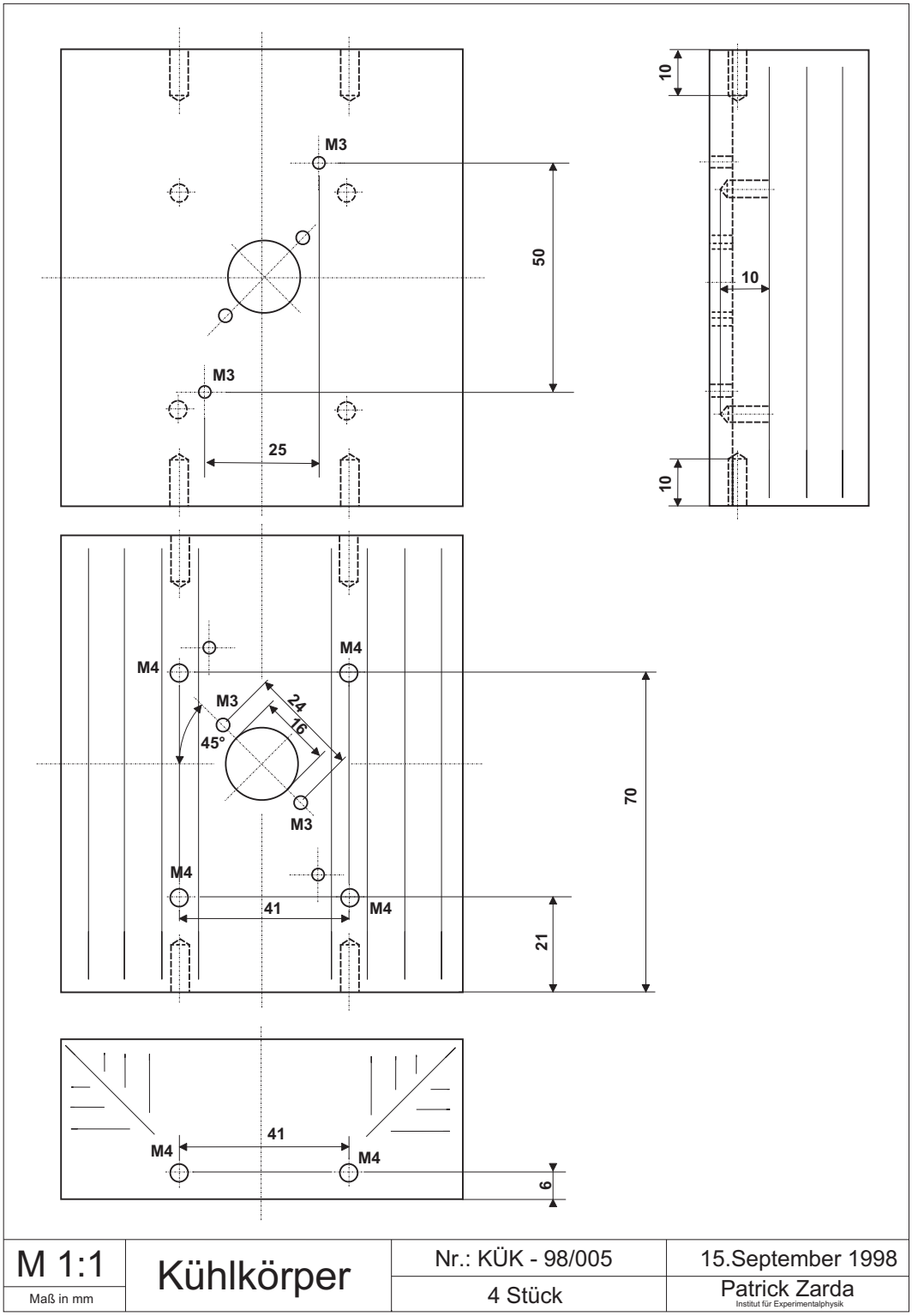




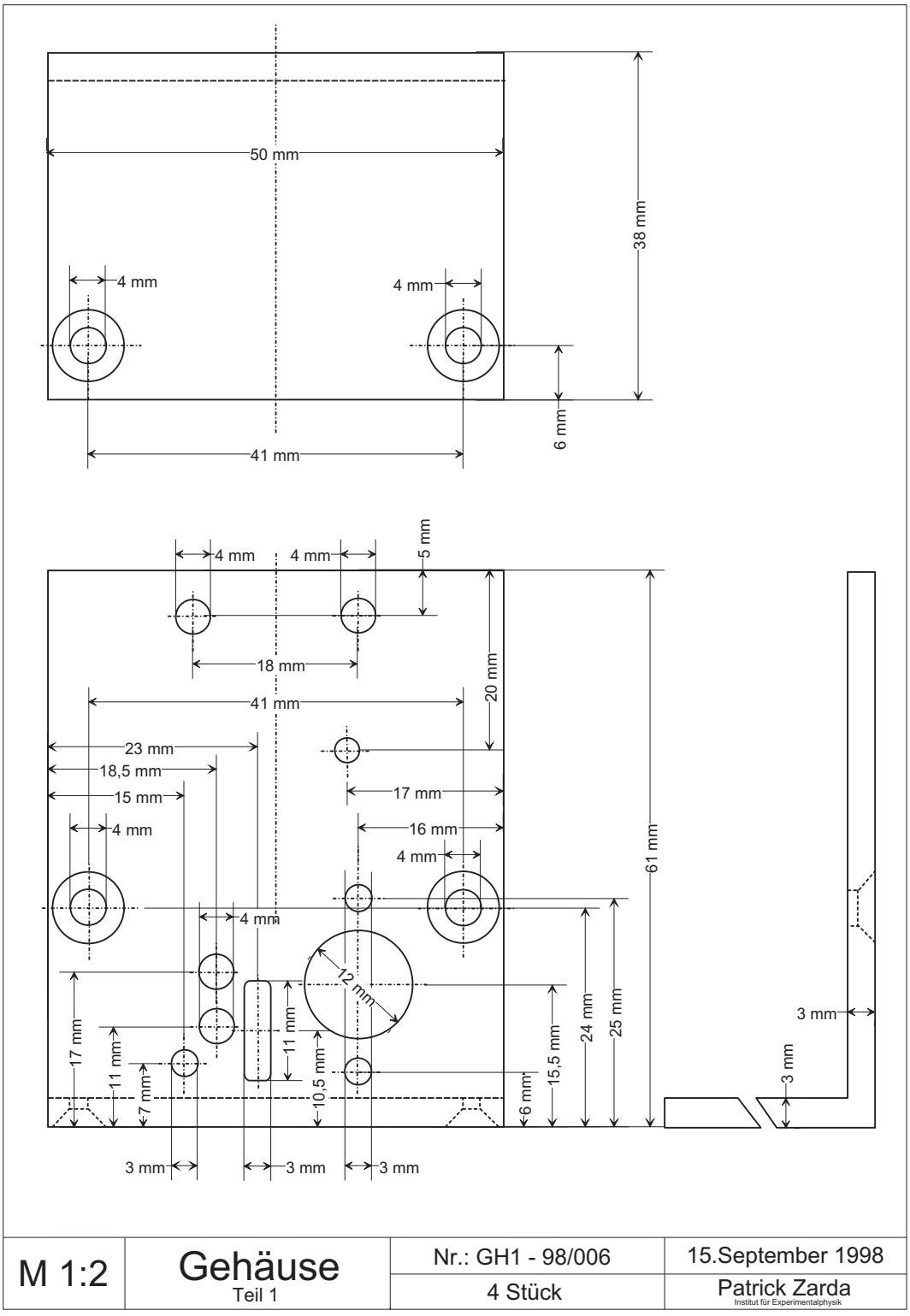
M 1:2 Maß in mm	Verbindungsplatte	Nr.: PLA - 98/004 4 Stück	23.Juli 1998 Patrick Zarda Institut für Experimentalphysik



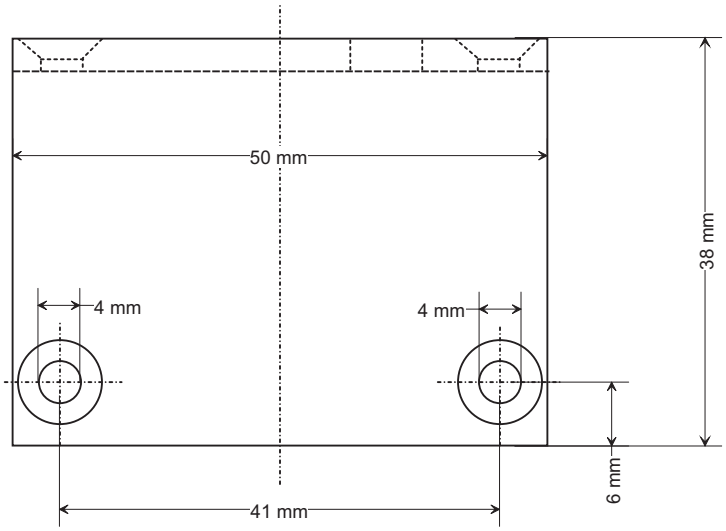
M 1:2	Frontplatte	Nr.: FPL - 98/007	6. August 1998
		4 Stück	Patrick Zarda Institut für Experimentalphysik

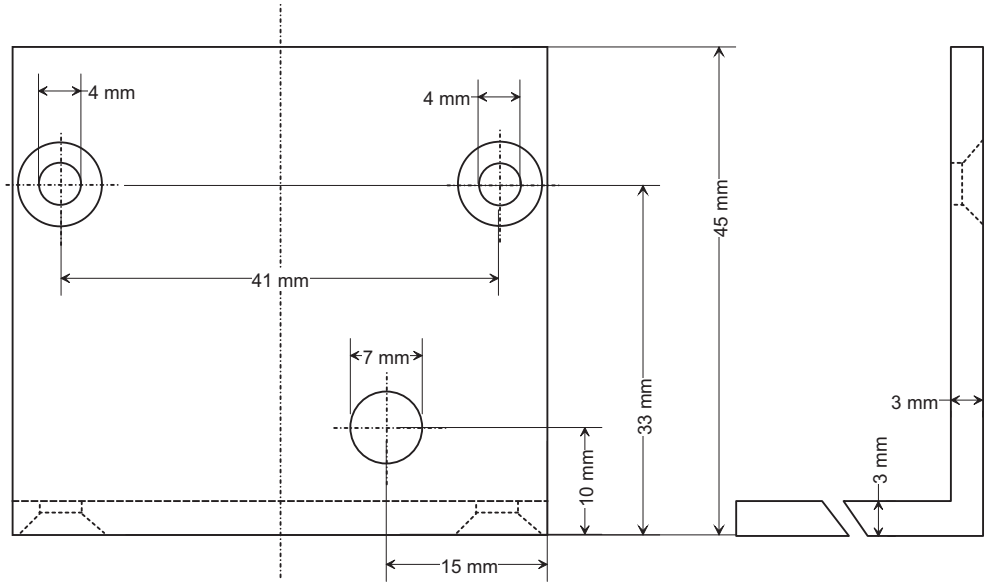


M 1:1	Kühlkörper	Nr.: KÜK - 98/005	15.September 1998
Maß in mm		4 Stück	Patrick Zarda Institut für Experimentalphysik



M 1:2	Gehäuse Teil 1	Nr.: GH1 - 98/006	15.September 1998
		4 Stück	Patrick Zarda Institut für Experimentalphysik





M 1:2	Gehäuse Teil 2	Nr.: GH2 - 98/008	17.Dezember 1998
		5 Stück	Patrick Zarda Institut für Experimentalphysik

B. Nachwort

Das Studium hätte ich nicht ohne Unterstützung einiger Personen so problemlos absolvieren können:

Mein erster Dank gilt meinen Eltern, die mir durch ihre persönliche und finanzielle Unterstützung ein sorgenfreies Studium ermöglichten.

Weiters möchte ich mich bei meinen Studienkollegen *Johannes Aschaber*, *Karlheinz Eder* und *Thomas Zeiger* für die gute und teilweise amüsante Zusammenarbeit während des ganzen Studiums bedanken. Auch wenn die Mannerschnitten nicht immer gerecht aufgeteilt wurden[1]...

Bedanken möchte ich mich vor allem auch bei *Prof. Dr. Harald Weinfurter* für die gute Betreuung während meiner Diplomarbeit. Neben der Möglichkeit des selbstständigen Arbeitens bekam ich jederzeit Unterstützung und konnte auch an zahlreichen Kongressen und Tagungen mit Posterpräsentionen oder Vorträgen teilnehmen. Mein Dank gilt auch allen Kolleginnen und Kollegen der Quantenoptikgruppe, speziell *Markus Oberparleiter, Surasak Chiangga, Thomas Jennewein, Markus Michler* und *Andreas Mitterer* für die Hilfe bei der Arbeit am Experiment. Nicht zu vergessen sind unsere Mechanikgenies *Stefan Haslwanter* und *Anton Schönherr*, die trotz Splitter im Auge auch beim fünften Kühlkörper noch nicht aufgeben.

Danke auch an die beiden Berliner Wahltiroler *Peter Krüger* und *Albrecht Haase*, die damals im Rahmen eines Orientierungspraktikums an der Kühlschaltung der SPAD's mitarbeiteten und auch sehr zum Gelingen der Schiausflüge[2] beim Laserseminar in Mauterndorf beitrugen.

Ein Dank gilt auch den Programmierern des LaTeX 2_ε-KOMA-Script-Packets, welches in einfacher und eleganter Weise ein perfektes Layout der Diplomarbeit ermöglichte.

[1] „*Pfff...*“ läßt grüßen...
[2] „*Dat find ik juud!*“ (Zitat Haase)

Zu guter Letzt möchte ich mich bei den Herren *Goscinny*[3] und *Uderzo*[4] bedanken, die schon früh mein Interesse an der Quantenkryptographie weckten (siehe Abb. B.1).

Abbildung B.1.: Quantenkryptographie in der Antike (aus *Asterix und der Arvernerschild*)

[3] Texter von *Asterix*
[4] Zeichner von *Asterix*