Aufbau zweier Michelson-Interferometer zur *Time-Bin*-Kodierung von schmalbandigen Photonen für die Quanteninformation

Diplomarbeit

Nils Neubauer

Universität Leipzig
Fakultät für Physik und Geowissenschaften

angefertigt an der
Humboldt-Universität zu Berlin
AG Nanooptik

Berlin, im Februar 2008

Zusammenfassung

Das Quantenbit ist ein zentraler Begriff der Quanteninformationsverarbeitung. Es lässt sich in einem quantenmechanischen Zwei-Niveau-System als kohärente Superposition der beiden logischen Grundzustände $|0\rangle$ und $|1\rangle$ darstellen. Für Fragen der Quantenkommunikation, speziell der Quantenkryptographie, sind Photonen als Träger von Quanteninformation prädestiniert. Das sogenannte *time-bin*-Schema ist eine Möglichkeit, ein Qubit in der globalen Phase eines Photons zu kodieren. Die Präparation eines *time-bin* Qubits erfolgt mit einem unsymmetrischen Interferometer: Durchquert ein Photon das Interferometer, so kann es am Ausgang als zeitliche Überlagerung zweier möglicher Ankunftszeiten beschrieben werden, wenn die Kohärenzlänge der Photonen kleiner als die optische Wegdifferenz der beiden Interferometerarme ist. Die Zustandsmessung (Dekodierung) erfolgt mit einem Interferometer gleicher Form.
Für die Zukunft wird die Realisierung größerer Quantennetzwerke von großer Relevanz sein. Als Knotenpunkte solcher Netzwerke wurden einzelne oder Ensembles von Atomen oder Ionen vorgeschlagen. Es ist also die Übertragung photonischer Qubits auf atomare Qubits erforderlich. Dementsprechend werden wegen der schmalen Übergangsbreiten in atomaren Systemen auch schmalbandige Photonen benötigt, um eine effiziente Wechselwirkung zu garantieren. Für eine Umwandlung von *flying Qubits* (Photonen) in *stationary Qubits* (Atome) benötigt man also bei der Verwendung von *time-bin-encoding* Interferometer mit großer Wegdifferenz, so dass auch schmalbandige Photonen kodiert werden können.
Im Rahmen dieser Diplomarbeit erfolgte der Aufbau zweier Michelson-Interferometer für die Kodierung bzw. Dekodierung schmalbandiger Photonen nach dem *time-bin*-Schema. Die Interferometer sind in der Lage, Photonen mit einer spektralen Bandbreite in der Größenordnung von 10 MHz zeitlich zu trennen. Für die Demonstration der Funktionalität der Interferometer erfolgte der Betrieb mit Gauß-Pulsen von 100 ns Dauer. Die zeitliche Trennung von Pulsen dieser Länge erfolgte mit einer optischen Faser von 50 m Länge, die zweimal durchlaufen wird und den langen Arm des Michelson-Interferometers repräsentiert. Eine besondere Herausforderung bei der Verwendung der beiden Interferometer insbesondere für die Quantenkryptographie ist die erforderliche relative Phasenstabilität der Interferometerarme. Aus diesem Grund wurde ein kompakter Aufbau mit optischen Komponenten in 20 mm Strahlhöhe gewählt. Die Interferometer befinden sich in abschließbaren Boxen, um thermische Driften der Umgebung zu verhindern. Neben

passiver Temperaturstabilisierung wichtiger Komponenten, wie der 50 m langen Faser, wurde außerdem eine aktive Stabilisierung der Wegdifferenz über ein Piezoelement realisiert. Für die Demonstration von Quantenkryptographie wurde die Grundlage mit einem Steuerungsschema geschaffen, dass die Ein- und Ausgabe aller Steuersignale sowie die Weiterverarbeitung für die Generation eines sicheren Schlüssels ermöglicht.
Der im Rahmen dieser Arbeit erstmalig realisierte Aufbau für die Kodierung/Dekodierung schmalbandiger Photonen ist die Grundlage für ein geplantes Experiment zur Photonenspeicherung mittels elektromagnetisch induzierter Transparenz (EIT). Echte Einzelphotonen mit einer spektralen Bandbreite von 10 MHz werden für dieses Experiment in einem optisch parametrischen Oszillator erzeugt. Mit Hilfe des hier realisierten Aufbaus können diese dann mit dem ersten Interferometer kodiert und nach der Speicherung mit dem zweiten Interferometer dekodiert werden. Der Interferometeraufbau ist somit eine wichtige Komponente innerhalb eines zukünftigen Netzwerks photonischer Quanteninformationsverarbeitung.

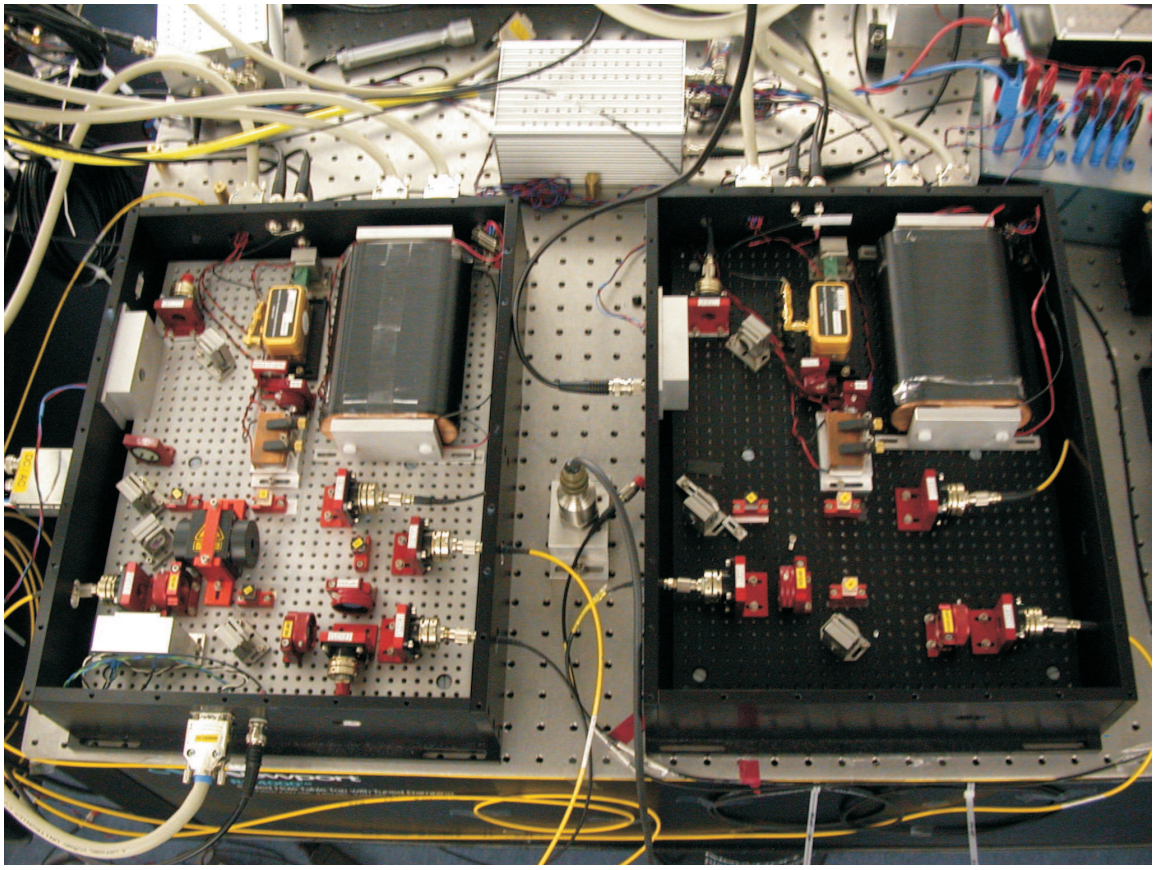

Foto der beiden time-bin-Interferometer. Die Verzögerungsfaser (rechts oben) ist auf einen Kupferblock gewickelt.

Inhaltsverzeichnis

Einleitung

Die Entwicklung der Quantenmechanik zu Beginn des 20. Jahrhunderts markierte einen grundlegenden Wandel im Verständnis der Natur auf atomarer Skala. Die aus diesem Wissen resultierenden Anwendungen, insbesondere der Laser und festkörperbasierte Bauelemente wie der Transistor, bilden die technische Grundlage der Informations- und Kommunikationstechnologie. Die enormen Erfolge dieser Technologie spiegelt auch das Moorsche Gesetz wider, wonach sich die Anzahl der Transistoren auf einem Chip etwa alle zwei Jahre verdoppelt. Information wird in diesen Bauelementen klassisch verarbeitet. Die zunehmende Miniaturisierung stößt in Zukunft allerdings an prinzipielle physikalischen Grenzen. Die quantenmechanische Natur einzelner Atome und Elektronen macht sich dann bemerkbar und induziert Störungen in der Signalverarbeitung.
Anfang der 80er Jahre begann man, grundlegende Gedanken der Quantenmechanik auf die Verarbeitung und Übertragung von Information anzuwenden [Fey82]. Es entstand ein neuer Zweig innerhalb der Quantenphysik, die Quanteninformationsverarbeitung. Zentraler Begriff ist analog zum klassischen Bit das Quanten-Bit (Qubit) als kleinste Informationseinheit. Es kann als quantenmechanisches Zwei-Niveau-System interpretiert werden, das sich als kohärente Überlagerung der beiden Basiszustände $|0\rangle$ und $|1\rangle$ beschreiben lässt. Es konnte gezeigt werden, dass sich einige Probleme der klassischen Informationsverarbeitung mit Algorithmen, basierend auf Operationen an Qubits, effizienter lösen lassen. Ein Beispiel ist der Shor-Algorithmus [Sho97]. Die Sicherheit heute eingesetzter Verschlüsselungsverfahren wie dem RSA-Algorithmus [RSA78] basiert auf der mathematisch komplexen und aufwendigen Faktorisierung großer Zahlen, für die kein effizienter klassischer Algorithmus bekannt ist. Mit dem Shor-Algorithmus steigt die Zeit für die Faktorisierung mit steigender Länge der Zahl nur noch polynomiell, und somit ist die Sicherheit klassischer Verfahren gefährdet.
Die experimentelle Implementierung von Qubits und entsprechender Quantengatter erfolgte inzwischen in den verschiedensten physikalischen Systemen. So nutzt man Energieniveaus in Ionen, die in Paul-Fallen gespeichert werden, um mit Laserpulsen Qubit-Zustände zu präparieren und auszulesen. Auf diese Art konnten Operationen an bis zu acht Qubits experimentell demonstriert werden [SKHR$^+$03]. Des Weiteren nutzt man den Kernspin als Qubit-System, wobei die gezielte Manipulation durch gepulste Magnetfelder erfolgt. Mit diesem NMR-Quantencomputer war es bereits möglich, komplexe Algorithmen, wie den Shor-Algorithmus zu realisieren [VSB$^+$01]. Eine weitere Implementierung

solcher *stationären Qubits* sind SQUIDS, die aus nanostrukturierten supraleitenden Elektroden bestehen, welche über Josephson-Kontakte koppeln [YN05].
Photonen sind der ideale Träger, um Quanteninformation zu übertragen, da sie wenig Wechselwirkung mit ihrer Umgebung zeigen. Bennett und Brassard schlugen 1984 ein Protokoll zum sicheren Schlüsselaustausch (Quantum-Key-Distribution) vor [BB84], dessen Sicherheit auf dem Ein-Teilchen-Charakter von Photonen basiert. Die Messung eines einzelnen Quantenzustandes führt zu einer Projektion in einen Eigenzustand des Messoperators. Außerdem ist es nicht möglich ein einzelnes Qubit zu kopieren (*No-Cloning-Theorem*). Ein Lauschangriff, bei dem unbemerkt der Zustand der übertragenen Qubits bestimmt werden soll, kann somit identifiziert werden. Dies macht die Verfügbarkeit von Quellen einzelner Photonen erforderlich. Die spontane Emission eines einzelnen Atoms oder Ions kann dazu genutzt werden, ist aber mit hohem technischen Aufwand verbunden. Als Alternative dazu nutzt man z.B. Defektzentren in Diamant, wobei zwei benachbarte Gitterplätze im Diamantkristall durch Stickstoff und einer Fehlstelle ersetzt sind [KMZW00] oder die spontane Emission einzelner Moleküle [BLTO99, LM00]. Aus technologischer Sicht zeichnen sich Systeme wie Quantenpunkte durch ihre hohe Stabilität sowie durch die leichte Integrierbarkeit in Mikroresonatoren aus [BGL98, MIM$^+$00, SPS$^+$01]. Neben der Einzelphotonenemission von Quantenpunkten konnte ebenfalls die Erzeugung verschränkter Photonen durch einen Kaskadenübergang gezeigt werden [BSPY00, ALP$^+$06, SYA$^+$06]. Ein weiteres Konzept zur Erzeugung einzelner Photonen basiert auf der spontanen parametrischen Fluoreszenz in einem nichtlinearen Kristall, wobei ein Pumpphoton in zwei Photonen (Signal- und Idlerphoton) geringerer Frequenz konvertiert wird (Abbildung 1). Der Nachweis eines Photons zeigt dann die Präsenz des anderen an. Wird die

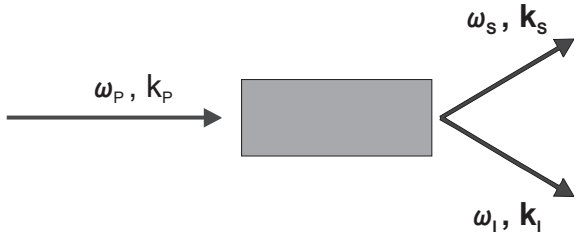

Abbildung 1: *Prinzip der spontanen parametrischen Fluoreszenz.*

parametrische Fluoreszenz innerhalb eines Resonators betrieben, lässt sich die spektrale Bandbreite von Signal- und Idlerphoton von einigen THz auf den MHz-Bereich reduzieren und liegt damit im Bereich atomarer Resonanzen. Eine solche Anordnung nennt man Optisch Parametrischer Oszillator (OPO). Er stellt im Betrieb unterhalb der Schwelle stimulierter Emission bei einer Triggerung auf das Idlerphoton eine Quelle für schmalbandige Photonen dar [LO00, KWS06, NNNT$^+$07, SWHB07].
Zur Darstellung photonischer Qubits kann man die Polarisation der Photonen benutzen. So beruhte die erste experimenelle Demonstration des BB84-Protokolls [BBB$^+$92] auf

diesem Konzept, wobei die Qubits in der $\{|H\rangle\,;|V\rangle\}$-Basis und in der $\{|{+}45°\rangle\,;|{-}45°\rangle\}$-Basis kodiert waren. Aufgrund der Depolarisationseigenschaften von Ein-Moden-Fasern eignet sich dieses Konzept nicht zur langreichweitigen Kommunikation über Glasfasern. Eine Alternative sind *time-bin*-kodierte Qubits. Die Implementierung erfolgt über Interferometer mit unterschiedlich langen Armen (Abbildung 2). Durchläuft ein Photon solch ein Interferometer, so kann der Zustand am Ausgang beschrieben werden als kohärente Überlagerung der zwei möglichen Zeitfenster (*time-bins*) in denen sich das Photon befinden kann, wobei die Zeitdifferenz der beiden Zustände größer als die Kohärenzzeit der Photonen sein muss. Die Messung in der $\{|0\rangle\,;|1\rangle\}$-Basis erfolgt dementsprechend über die Messung der Ankunftszeit. Die Gewichtung der zeitlichen Basiszustände erfolgt über das Teilungsverhältnis des Strahlteilers und die relative Phase ergibt sich durch den optischen Weglängenunterschied der beiden Arme. Die Interferometerarme müssen also stabil in der Größenordnung eines Bruchteils der benutzten Wellenlänge des Lichtes sein. Experimente zur phasenkodierten Quantenkryptographie wurden u.a. in der Arbeitsgruppe von Gisin durchgeführt [MHH+97, RBG+00]. Auch die Erzeugung time-bin verschränkter Photonenpaare ist möglich [BGTZ99, MdRT+02].

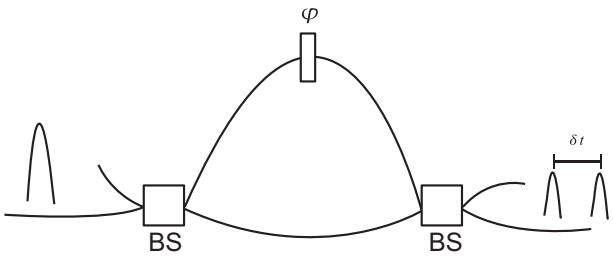

Abbildung 2: *Time-bin-Kodierung mit einem unsymmetrischen Interferometer (BS: Strahlteiler, φ: relative Phasendifferenz)*

Aktuelle Vorschläge zur Implementierung größerer Quanteninformationsnetzwerke basieren auf Atomen oder Ionen als Knotenpunkten, zwischen denen Information mit einzelnen Photonen ausgetauscht wird [CZKM97, BDCZ98, TRBZ04]. Die Schnittstelle zwischen stationären und photonischen Qubits ist also von großer Bedeutung. Die spektrale Bandbreite der Photonen muss dabei in der Größenordnung atomarer Resonanzen liegen, um eine effiziente Wechselwirkung zu garantieren. Ein Schritt in Richtung einer Schnittstelle ist die bereits gezeigte Teleportation von Zuständen zwischen Licht und Materie [SKO+06, CCY+08]. Auch das Konzept der elektromagnetisch induzierten Transparenz (EIT) dient zur Übertragung photonischer Zustände auf Atome. In einem Λ-Energieniveauschema, beispielsweise in Alkaligasen, führt die kohärente Kopplung der beteiligten Niveaus durch Laserfelder auf einen ausgewählten Übergang zur Abbremsung und in dem erweiterten Schema der dynamischen EIT [FL00, BZL03] zur Speicherung des Probelichts [BIH91, Har97, HHDB99, PFM+01]. Das EIT-Konzept gilt auch für die Speicherung von Einzelphotonen und wurde bereits experimentell gezeigt [EAM+05, CMJ+05].

Ziel dieser Arbeit war die Realisierung eines Aufbaus zur *time-bin*-Kodierung schmalbandiger Photonen. Der Aufbau besteht aus zwei Michelson-Interferometern, die zur Kodierung bzw. Dekodierung genutzt werden und ist Teil eines Gesamtexperiments zur Realisierung einer Schnittstelle zwischen stationären und photonischen Qubits. Die Photonen werden dabei in einem OPO erzeugt. Das erste Interferometer präpariert die *time-bin* Qubits, die dann in einer Cäsiumzelle unter Ausnutzung des EIT-Effekts gespeichert und ausgegeben werden sollen. Anschließend kann die Auslesung der Qubits mit dem zweiten Interferometer erfolgen. Die spektrale Bandbreite von Photonen, die mit EIT gespeichert werden können, ist in der Größenordnung von 10 MHz. Daraus resultieren Pulslängen von ungefähr 100 ns. Um separate Pulse garantieren zu können, wurde eine optische Faser von 50 m Länge in den Aufbau integriert. Mit einer relativen Armlängendifferenz von 2*50 m konnte so eine Verzögerung von 500 ns erreicht werden. Aufgrund der hohen Anforderungen an die Stabilität der relativen Weglängendifferenz wurde ein Stabilisierungsschema realisiert, dass neben passiver Temperaturstabilisierung der Hauptkomponenten die aktive Stabilisierung über ein Piezoelement ermöglicht. Zur Demonstration der Funktionsfähigkeit des Aufbaus ist außerdem die Implementierung des phasenkodierten BB84-Protokoll geplant. Hierfür wurden die Grundlagen in Form der Steuerungselektronik gelegt.

Aufbau der Arbeit

Die vorliegende Diplomarbeit wurde als externe Diplomarbeit der Universität Leipzig an der Humboldt-Universität zu Berlin angefertigt.
Zunächst sollen im ersten Kapitel grundlegende Themen der Quanteninformation behandelt werden. Am Anfang steht der Begriff des Qubits und dessen formale Beschreibung und Darstellung. Anschließend wird der sichere Schlüsselaustausch als Anwendung von Qubits beschrieben, wobei insbesondere auf das BB84-Protokoll eingegangen wird.
Das zweite Kapitel beschäftigt sich mit der experimentellen Realisierung. Die für den interferometrischen Aufbau wichtigsten optischen Komponenten werden vorgestellt. Hierzu zählt die Verzögerungsfaser, mit der eine relative Wegdifferenz von 100 m realisiert wird und der elektrooptische Modulator zur Einstellung definierter Phasenwerte. Außerdem wird die Konfiguration für die Umsetzung des BB84-Protokolls beschrieben. Das Kapitel schließt mit der Erläuterung der Pulserzeugung sowie der Einzelphotonendetektion.
In Kapitel 3 werden die Messungen vorgestellt. Dabei soll die Charakterisierung der Interferometer, die Stabilisierung, sowie der Betrieb mit Lichtpulsen gezeigt werden.
Es folgt die Diskussion der Ergebnisse und abschließend im Ausblick die weitere Anwendung im Gesamtexperiment und die Möglichkeiten der Optimierung des Systems.

Kapitel 1

Grundlagen der Quanteninformation

In der Informationstheorie geht man von einem einfachen Kommunikationsmodell aus. Eine Quelle, auch Alice genannt, sendet eine Botschaft der Länge n über einen Kanal an einen Empfänger, der Bob genannt wird [Lyr02]. Die Signalquelle ist durch ein Ensemble $\{x_i, p_i\}$ mit $i = 1, ..., N$ charakterisiert. Alice sendet also n-stellige Botschaften, geschrieben in einem Alphabet mit N Zeichen, wobei jeder Buchstabe x_i mit der Wahrscheinlichkeit p_i vorkommt. Einer solchen Signalquelle ordnet man die sog. Shannon-Entropie [Sha48] zu:

$$H(\tilde{p}) = -\sum_{i=1}^{N} p_i \log_2 p_i. \tag{1.1}$$

Eine praktische Bedeutung erlangt die Shannon-Entropie $H(\tilde{p})$ bei der Übertragung der Nachricht. Alice verwendet dafür nicht das ursprüngliche Zeichenensemble, sondern kodiert die Nachrichten in einem binären Alphabet. Bob empfängt also eine Bit-Sequenz aus den Binärzahlen 0 und 1. Jeder Empfang einer der Binärzahlen entspricht der Antwort auf eine Ja-Nein-Frage und wird der Information 1 Bit zugeordnet. Die Frage ist nun, wie viele Bits Alice im Mittel verschicken muss, damit Bob den Ausgangstext eindeutig aus der Menge N^n aller Botschaften identifizieren kann. Man kann zeigen, dass man genau nH Bits benötigt [Aud05]. Die Anzahl nH ist also der Informationsgehalt des Ausgangstextes und die Shannon-Entropie $H(\tilde{p})$ bekommt die Bedeutung der mittleren Information pro Buchstabe des Ausgangstextes. Information ist somit ein Maß für den Neuigkeitswert eines Zeichens. Besteht beispielsweise das Zeichenensemble nur aus einem Buchstaben ($N = 1$), so ist $H(\tilde{p}) = 0$. Bob kennt den Text bereits und muss keine Fragen stellen.

1.1 Das Qubit als Einheit der Quanteninformation

Bei klassischen Informationsträgern wird angenommen, dass sie sich bereits vor der Messung in einem der beiden Zustände 0 und 1 befinden.

Im Unterschied dazu können Quantensysteme in einer unbestimmten Überlagerung beider Zustände o und 1 vorliegen, so dass die Information über den Zustand erst nach einer vollständigen Messung sicher bestimmt ist.
Formal werden Quantensysteme, die nicht mehr als zwei linear unabhängige Zustände besitzen, in einem zweidimensionalen Hilbertraum $\mathcal{H}_2$ beschrieben. Hinsichtlich ihrer Bedeutung in der Quanteninformationsverarbeitung heißen die Zustandsvektoren im $\mathcal{H}_2$ *quantum bits* oder kurz *Qubits*. Sie sind von der Form

$$|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle , \qquad \left(|c_0|^2 + |c_1|^2 = 1 \; ; \; c_0, c_1 \in \mathbb{C}\right) \tag{1.2}$$

oder in der Dichtematrixdarstellung

$$\rho = |c_0|^2 |0\rangle \langle 1| + c_0 c_1^* |0\rangle \langle 1| + c_1 c_0^* |1\rangle \langle 0| + |c_1|^2 |1\rangle \langle 1| , \tag{1.3}$$

wobei $\{|0\rangle , |1\rangle\}$ die orthonormalen Elemente der Messbasis (B_z) (auch *Rechenbasis* genannt) sind, in denen sie sich erst nach der Messung mit den Wahrscheinlichkeiten $|c_0|^2$ und $|c_1|^2$ befinden. Für die Rechenbasis gilt die Notation

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle , \qquad \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle , \tag{1.4}$$

die somit gleichzeitig die Darstellung der Pauli-Matrizen $\sigma_j, (j = x, y, z)$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1.5}$$

festlegt. Zusammen mit der Einheitsmatrix $\mathbb{1}$ bilden die Pauli-Matrizen eine Operatorbasis in $\mathcal{H}_2$. Ist $x \in \{0, 1\}$ und rechnet man modulo 2, so gilt

$$\sigma_1 |x\rangle = |x + 1\rangle \tag{1.6}$$

$$\sigma_2 |x\rangle = (-1)^x i |x + 1\rangle \tag{1.7}$$

$$\sigma_3 |x\rangle = (-1)^x |x\rangle \tag{1.8}$$

Eine anschauliche Darstellung der Qubit-Zustände ist die Bloch-Kugel. Dazu zerlegt man den Dichteoperator gemäß der Operatorbasis in

$$\rho = \frac{1}{2}(\mathbb{1} + \boldsymbol{r}\boldsymbol{\sigma}) \tag{1.9}$$

mit Vektor $\boldsymbol{r} \in \mathbb{R}^3$

$$\boldsymbol{r} := tr[\rho\boldsymbol{\sigma}] \tag{1.10}$$

Aus den Eigenschaften der Pauli-Matrizen gewinnt man daraus

$$tr[\rho^2] = \frac{1}{2}(1 + |\boldsymbol{r}|^2) \tag{1.11}$$

Betrachtet man als Spezialfall den Dichteoperator $\rho := |\psi\rangle\langle\psi|$ eines beliebigen normierten Vektors $|\psi\rangle$, so folgt für einen reinen Zustand ($\rho^2 = \rho$) mit $tr[\rho^2] = tr[\rho] = 1$ und (1.11)

$$|\boldsymbol{r}|^2 = 1 \tag{1.12}$$

Weiterhin erhält man als Interpretation von $\boldsymbol{r}$ den Erwartungswert

$$\boldsymbol{r} = \langle\psi|\,\boldsymbol{\sigma}\,|\psi\rangle\,. \tag{1.13}$$

Jedem Qubit $|\psi\rangle$ ist so gemäß (1.13) ein Vektor im $\mathbb{R}^3$ zugeordnet, der *Bloch-Vektor* genannt wird. Seine Spitze liegt für reine Zustände auf der Oberfläche der Einheitskugel (*Bloch-Kugel*).

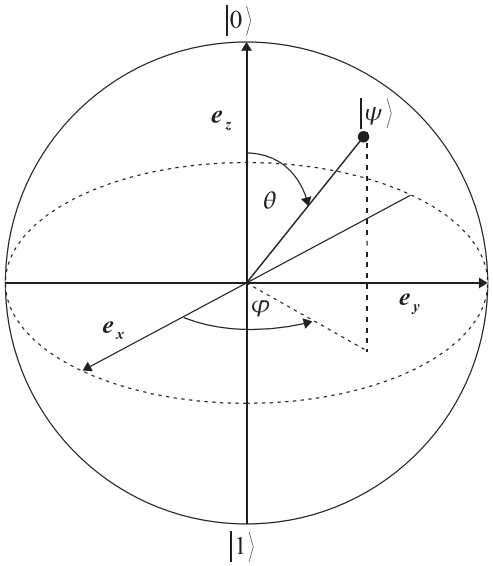

Abbildung 1.1: *Bloch-Kugel mit Bloch-Vektoren.*

Zu zwei orthogonalen Qubits gehören am Ursprung gespiegelte Blochvektoren. Die Bloch-Punkte können mit Hilfe von Polarkoordinaten parametrisiert werden. Ein beliebiges Qubit $|\psi\rangle$ ist dann von der Form

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{1.14}$$

mit $0 \leq \varphi \leq 2\pi, 0 \leq \theta \leq \pi$. Der zu $|\psi\rangle$ gehörende Bloch-Vektor ist also

$$\boldsymbol{r} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta). \tag{1.15}$$

Ein gegebener Zustand $|\psi\rangle$ wird über $\boldsymbol{r}$ eindeutig definiert. So wird die Referenzbasis $\{|0\rangle, |1\rangle\}$ durch die Einheitsvektoren $\{\mathbf{e}_z, -\mathbf{e}_z\}$ dargestellt. Zustände vom Typ

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle) \tag{1.16}$$

liegen entlang des Äquators ($\theta = \pi/2$, φ als Winkel in der $\mathbf{e}_x, \mathbf{e}_y$-Ebene).

Das No-Cloning-Theorem

Zwei beliebige (im Allgemeinen nicht orthogonale) quantenmechanische Zustände können mit einer einzelnen Messung nicht unterschieden werden [NC00]. Es existiert stets eine Komponente des einen Zustandsvektors in Richtung des anderen, so dass man sich bei einer Messung in der jeweiligen Basis nie sicher sein kann, welcher Zustand gerade vorlag. Eine äquivalente Aussage macht das *no-cloning* Theorem, wonach es nicht möglich ist, einen beliebigen unbekannten Quantenzustand zu kopieren. Ein Quantensystem S^A sei im Zustand $\left|\psi^A\right\rangle$. Dieser Zustand soll kopiert werden. Dazu soll ein Quantensystem S^B, welches sich zu Beginn im Zustand $\left|i^B\right\rangle$ befindet, in den Zustand $\left|\psi^B\right\rangle$ überführt werden. Der Kopiervorgang soll universell sein, so dass alle Zustände von S^A mit einer unitären Transformation $\hat{U}$ kopiert werden können. Mit einem zweiten zu kopierenden Zustand $\left|\varphi^A\right\rangle$ heißt das:

$$\left|\psi^A, i^B\right\rangle \rightarrow \left|\psi^A, \psi^B\right\rangle = \hat{U}\left|\psi^A, i^B\right\rangle \tag{1.17}$$

$$\left|\varphi^A, i^B\right\rangle \rightarrow \left|\varphi^A, \varphi^B\right\rangle = \hat{U}\left|\varphi^A, i^B\right\rangle. \tag{1.18}$$

Das Skalarprodukt der Transformation ergibt sich zu

$$\left\langle \varphi^A, \varphi^B \right| \left. \psi^A, \psi^B \right\rangle = \left\langle \varphi^A, i^B \right| \hat{U}\hat{U}^\dagger \left| \psi^A, i^B \right\rangle = \left\langle \varphi^A, i^B \right| \left. \psi^A, i^B \right\rangle. \tag{1.19}$$

Mit der Forderung an die Kopien $\left|\psi^A\right\rangle = \left|\psi^B\right\rangle, \left|\varphi^A\right\rangle = \left|\varphi^B\right\rangle$ erhält man

$$\left\langle \varphi^A \right| \left. \psi^A \right\rangle^2 = \left\langle \varphi^A \right| \left. \psi^A \right\rangle \left\langle i^B \right| \left. i^B \right\rangle \tag{1.20}$$

Wenn $\left|\psi^A\right\rangle$ und $\left|\varphi^A\right\rangle$ nicht orthogonal sind, d.h. $\left\langle \varphi^A \right| \left. \psi^A \right\rangle \neq 0$, folgt

$$\left\langle \varphi^A \right| \left. \psi^A \right\rangle = \left\langle i^B \right| \left. i^B \right\rangle \qquad \text{d.h.} \quad \left|\psi^A\right\rangle = \left|\varphi^A\right\rangle \tag{1.21}$$

Das widerspricht der Annahme, dass $\left|\psi^A\right\rangle$ und $\left|\varphi^A\right\rangle$ beliebige Zustände sein können. Es existiert also keine universelle Kopiermaschine für beliebige unbekannte Quantenzustände. Die volle Information über den Zustand eines Qubits zu erhalten ist also nicht möglich. Jede Messung ist zwangsläufig mit einer Änderung des Zustands des Qubits verbunden. Auf dieser Eigenschaft beruht die Möglichkeit der Identifizierung von Lauschangriffen der im nächsten Abschnitt beschriebenen Protokolle zum sicheren Schlüsselaustausch.

1.2 Sichere Schlüsselübertragung mit Qubits: Quantenkryptographie

1.2.1 Die Vernam-Verschlüsselung

Kryptographie ist die Wissenschaft von der Verschlüsselung einer Nachricht zwischen zwei Parteien, so dass diese für Dritte nicht lesbar ist. Dazu wird ein bestimmter Algorithmus

angewandt, der die ursprüngliche Nachricht mit einem Schlüssel kombiniert und so ein Kryptogramm erzeugt wird. Die verschlüsselte Nachricht kann dann über einen äquivalenten Algorithmus wieder entschlüsselt werden. Man unterscheidet zwei Arten von Kryptosystemen. Benötigen Alice und Bob unterschiedliche Schlüssel, so spricht man von einem asymmetrischen bzw. *public-key* Kryptosystem. Der RSA-Algorithmus ist hierfür ein Beispiel [RSA78]. Bei symmetrischen Kryptosystemen nutzen Alice und Bob den gleichen Schlüssel zur Kodierung bzw. Dekodierung.
Der sog. *one-time pad*, ein von Gilbert Vernam im Jahr 1926 vorgeschlagenes Verfahren [Ver26], ist solch ein symmetrisches Kryptosystem. Die Nachricht m liegt als Bitfolge vor und wird mit einem Schlüssel k verschlüsselt. Dieser besteht aus einer binären Zufallsfolge der gleichen Länge n. Das Kryptogramm c erhält man nun über gliedweise Addition modulo 2 der Elemente der Nachricht und des Schlüssels ($c = m \oplus k$). Hier ein Beispiel:

Nachricht	0110110010
Schlüssel	1010011101
Kryptogramm	1100101111

Das Kryptogramm kann nun an Bob geschickt werden, welcher mit dem gleichen Schlüssel durch abermalige Addition modulo 2 die Originalnachricht erhält ($c \oplus k = m \oplus k \oplus k = m$).

Kryptogramm	1100101111
Schlüssel	1010011101
Nachricht	0110110010

Entscheidend bei Vernams Verfahren ist, dass jede statistische Analyse des Kryptogramms verhindert wird. Da jeder Schlüssel zufällig generiert wird, sind die Nachricht und das Kryptogramm völlig entkoppelt. Um eine Analyse von Korrelationen verschiedener Nachrichten auszuschließen, darf jeder Schlüssel nur einmal verwendet werden. Zusammenfassend muss man für einen sicheren Schlüssel fordern, dass er

- eine echte Zufallsfolge ist,
- die Länge der Nachricht hat,
- nur Alice und Bob bekannt ist,
- und nur einmal verwendet wird (one-time pad).

Erfüllt ein Schlüssel diese Voraussetzungen, ist es für einen Lauscher (Eve) nicht möglich das Kryptogramm zu entschlüsseln [Sha49]. Die Schwierigkeiten einer experimentellen Umsetzung bestehen nun darin, dass für jede neue Nachricht ein neuer Schlüssel zwischen Alice und Bob ausgetauscht werden muss, der außerdem keinem Lauscher zugänglich sein

darf. Die Sicherheit der Verschlüsselung basiert also allein auf der Geheimhaltung des Schlüssels.
Eine diese Anforderung genügende Art der Schlüsselübermittlung ist mit Hilfe von Quantensystemen möglich und soll im nächsten Abschnitt erläutert werden.

1.2.2 Quantenkryptographie

Die Idee der Quantenkryptographie besteht darin, einzelne Qubits als Informationsträger zu verwenden, um so einen sicheren, gemeinsamen Schlüssel für Alice und Bob verfügbar zu machen. Bei klassischen Signalen sind im Allgemeinen sehr viele Träger, wie z.B. Elektronen oder Photonen daran beteiligt, ein und dieselbe Information zu übertragen. So ist es für einen Lauscher ohne Probleme möglich, einen Teil dieser Träger zu benutzen, um die Information auszulesen, ohne dass dies von Alice und Bob bemerkt wird. Ein Lauschangriff ändert den Zustand eines klassischen Signals nicht. Im Gegensatz dazu nutzt man bei der Übertragung einzelner Qubits folgende Eigenschaften [NC00, Aud05]:

- Keine Messung kann nicht-orthogonale Zustände unterscheiden.
- Eine Messung ändert den Zustand eines einzelnen Qubits, wenn sie nicht zufällig in der richtigen Basis erfolgt.
- Qubits können nicht kopiert werden, so dass eine unbemerkte Zustandsbestimmung mittels kopierter Qubits ausgeschlossen werden kann.

Sämtliche Quantenkryptographieprotokolle bestehen daher aus zwei Teilen. Nach der Übertragung der Qubits und der Generierung eines Schlüssels folgt stets ein Kontrollmodus. Wenn die Präparationen von Alice und die jeweiligen Messungen von Bob mit den erwarteten Ergebnissen übereinstimmen, so hat kein Lauschangriff stattgefunden. Dazu wird ein Teil der Ergebnisse öffentlich ausgetauscht. Stimmen diese nicht überein, konnte ein Lauschangriff identifiziert werden und der Schlüssel wird verworfen.
Bei der praktischen Umsetzung der Protokolle muss man allerdings immer mit Störungen beim Transport der Qubits rechnen. Eine bestimmte Fehlerrate ist so unvermeidlich, wobei nie sicher ist, ob diese durch die Anwesenheit eines Lauschers oder durch Rauschen im Quantenkanal begründet ist. Daher werden zusätzlich klassische Fehlerkorrekturalgorithmen angewandt, um Übertragungsfehler zu reduzieren.

Das BB84-Protokoll

Das von Charles Bennett und Gilles Bassard im Jahr 1984 vorgestellte Protokoll [BB84] (BB84-Protokoll) war das erste, welches Qubits als Informationsträger benutzte. Neben der Etablierung eines gemeinsamen, geheimen und zufälligen Schlüssels zwischen Alice und Bob ermöglicht es Lauschangriffe zu erkennen. Zunächst soll der allgemeine Ablauf

des Protokolls erläutert und anschließend die experimentelle Implementierung diskutiert werden.
Alice beginnt mit der Zustandspräparation. Sie benötigt dafür zwei binäre Zufallsfolgen a und b, jeweils mit der Länge $4n$. Die beiden Zufallsfolgen werden nun auf $4n$ Qubits kodiert,

$$|\psi\rangle = \bigotimes_{k=1}^{4n} |\psi_{a_k b_k}\rangle \,, \tag{1.22}$$

wobei a_k und b_k den k-ten Bitwert der Folgen a bzw. b kennzeichnet. Die Qubits werden dabei z.B. den folgenden Zuständen zugeordnet:

$$|\psi_{00}\rangle = |0\rangle \tag{1.23}$$
$$|\psi_{10}\rangle = |1\rangle \tag{1.24}$$
$$|\psi_{01}\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right) = |0_x\rangle \tag{1.25}$$
$$|\psi_{11}\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right) = |1_x\rangle \tag{1.26}$$

Die vier Zustände bilden zwei Basen. Die Bitfolge a ist also gemäß b entweder in der Basis von σ_z oder σ_x kodiert. Alice sendet die so präparierten Qubits an Bob. Zu diesem Zeitpunkt kennt Bob b nicht, er weiß also nicht, in welcher Basis die einzelnen Qubits kodiert sind. Er fährt fort, indem er eine eigene Zufallsfolge b' erzeugt und gemäß dieser jeweils in der Basis σ_x oder σ_z die einzelnen Qubits misst. Die Messergebnisse ergeben eine Folge a'. Wenn Bob seine Messergebnisse a' vorliegen hat und den Empfang aller Qubits öffentlich an Alice bekannt gibt, kann Alice ihrerseits die Basiswahl b bekanntgeben. In einer öffentlichen Diskussion werden alle Fälle gleicher Basiswahl ($b'_k = b_k$) benannt. Durch die öffentliche Bekanntgabe von b und b' wird keine Information über a und a' preisgegeben, doch es ist wichtig, dass Alice erst nach dem Empfang aller Qubits durch Bob die Basisfolge b bekanntgibt. Andernfalls ist klar, dass dann Eve wüsste, in welcher Basis sie messen müsste. Durch die zufällige Basiswahl verbleiben Alice und Bob im Mittel $2n$ Bits.
Während der Übertragung kann Eve versucht haben, die Zustände der Qubits zu bestimmen und ein ihrerseits präpariertes Qubit an Bob zu senden, um aus der anschließenden öffentlichen Kommunikation Kenntnis über den Schlüssel zu erhalten. Durch die zwangsläufige Zustandsänderung einiger Qubits, ist solch ein Lauschangriff identifizierbar. Alice wählt dafür zufällig n Bits aus. Diese Kontrollbits werden öffentlich verglichen. Besteht keine Korrelation zwischen den Ergebnissen von Bob und den nach Alice Präparation erwarteten Werten, so ist der Lauschangriff identifiziert und der Schlüssel wird verworfen. Ist der Test erfolgreich, so schließt sich ein Verfahren zur Reduktion von Übertragungsfehlern (error-correction) an, sowie ein Algorithmus um Eves Information auf ein Minimum zu reduzieren (privacy amplification). Auf diese Weise erhält man m sichere Schlüsselbits aus den verbleibenden n Bits.

Die erste experimentelle Demonstration des BB84-Protokolls erfolgte 1992 durch Bennett [BBB$^+$92]. Die Qubits wurden in der Polarisation der Photonen kodiert. Die Polarisationszustände $|H\rangle, |V\rangle, |+45°\rangle, |-45°\rangle$ sind dabei die vier Zustände, die für das BB84-Protokoll notwendig sind. Zur Veranschaulichung des Protokolls am Beispiel der Polarisationskodierung folgende Tabelle:

Alice			Bob			
Zufallsfolge	Basisfolge	Polarisation	Basisfolge	Messung	gleiche Basis	**Schlüssel**
1	+	$\|H\rangle$	×	$\|+45°\rangle$	nein	
1	×	$\|+45°\rangle$	+	$\|H\rangle$	nein	
0	×	$\|-45°\rangle$	×	$\|-45°\rangle$	ja	0
1	+	$\|H\rangle$	+	$\|H\rangle$	ja	1
0	+	$\|V\rangle$	×	$\|+45°\rangle$	nein	
1	×	$\|+45°\rangle$	×	$\|+45°\rangle$	ja	1
0	+	$\|V\rangle$	+	$\|V\rangle$	ja	0
0	×	$\|-45°\rangle$	+	$\|H\rangle$	nein	
1	+	$\|H\rangle$	+	$\|H\rangle$	ja	1
1	+	$\|H\rangle$	×	$\|+45°\rangle$	nein	

Tabelle 1.1: *Implementierung des BB84-Protokolls mit Polarisationskodierung*

1.3 *Time-Bin*-Kodierung mit Michelson-Interferometern

Als Alternative zur Polarisationskodierung besteht die Möglichkeit den Wert eines Qubits in der Phase der Photonen zu kodieren. Phasenkodierte Qubits sind resistenter gegen

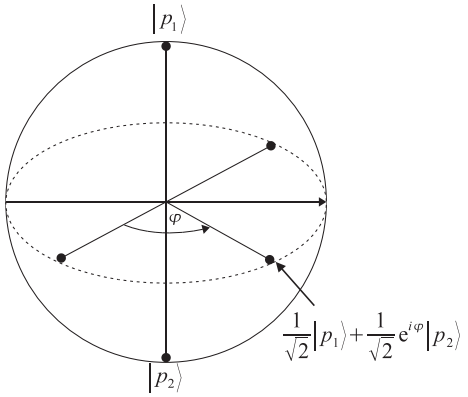

Abbildung 1.2: *Bloch-Kugel mit den Qubit-Zuständen eines Zwei-Wege-Interferometers mit 50:50 Strahlteiler.*

Dekohärenz in optischen Fasern, welche die langreichweitige Übertragung von Polarisationszuständen störend beeinflusst. Für die Präparation und zum Auslesen des Zustands benutzt man Interferometer. Alle Systeme zur phasenkodierten Quantenkryptographie beruhen auf der Tatsache, dass eine Kodierung mittels eines Zwei-Wege-Interferometers formal identisch zur Polarisationskodierung ist [GRTZ02]. Die zwei Wege bilden eine natürliche Basis. Die Gewichtung jedes Qubit-Zustands $|\psi\rangle = (c_1, c_2 e^{i\varphi})$ wird durch das Teilungsverhältnis $(|c_1|^2/|c_2|^2)$ des Strahlteilers bestimmt, während sich die Phase durch den Weglängenunterschied der beiden Interferometerarme ergibt. Die phasenkodierten Zustände lassen sich also ebenfalls mit der Bloch-Kugel darstellen (Abbildung 1.2). Für einen symmetrischen Strahlteiler liegen die Zustände auf dem Äquator. Der Azimuthwinkel φ repräsentiert die relative Phase zwischen den beiden Lichtwegen des Interferometers. Die Darstellung macht deutlich, dass alle polarisationskodierten Protokolle ebenfalls mit einem phasenkodierten System realisiert werden können.
Für die Präparation von *time-bin* Qubits verwendet man ein Interferometer nach dem Schema von Abbildung 1.3. Das kann ein Mach-Zehnder- oder ein Michelson-Interfero-

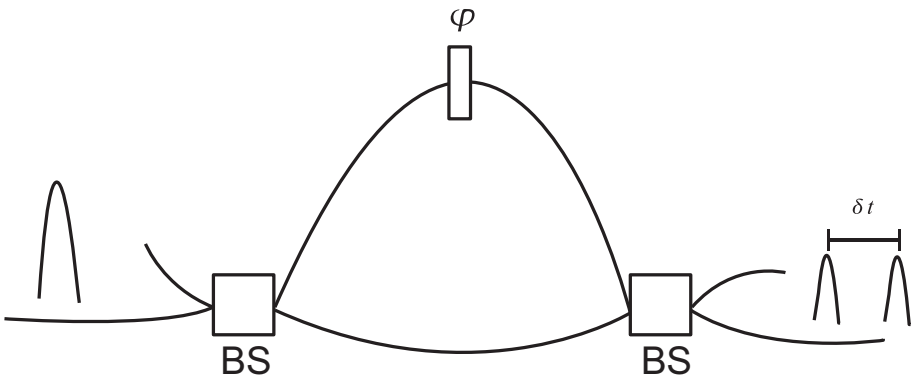

Abbildung 1.3: *Schematische Übersicht eines Interferometers zu Präparation von time-bin Qubits. Durch die Wahl des Teilungsverhältnisses des Strahlteilers (BS) und Einstellung der Phase φ lässt sich ein beliebiger Qubitzustand darstellen*

meter sein, dessen Arme unterschiedliche Längen haben [BGTZ99, EPT03]. Passiert ein Photon solch ein Interferometer, so erhält man am Ausgang des Interferometers eine Superposition aus den beiden möglichen Zeitfenstern (*time-bins*), in denen sich das Photon befinden kann. Die Zeitdifferenz zwischen den beiden Zeitfenstern ergibt sich dabei durch den optischen Weglängenunterschied der beiden Arme. Um eine eindeutige Trennung der beiden Zeitfenster zu ermöglichen, muss die Zeitdifferenz größer als die Kohärenzzeit der Photonen sein. Für den Fall symmetrischer Strahlteiler lässt sich der Ausgangszustand schreiben als [MdRT+02]

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|1,0\rangle + e^{i\varphi_A} |0,1\rangle \right). \tag{1.27}$$

Der Zustand $|1,0\rangle$ entspricht dem Fall, dass sich ein Photon im ersten Zeitfenster befindet, d.h. den kurzen Arm (S_A) des Interferometers durchlaufen hat. Dementsprechend ist im Zustand $|0,1\rangle$ das Photon im zweiten Zeitfenster und hat den längeren Arm (L_A) passiert. Für das Auslesen der Zustände benötigt Bob ein Interferometer mit der gleichen Weglängendifferenz (Abbildung 1.4). Erreicht der Zustand $|\psi\rangle$ (1.27) das Interferometer auf Bobs

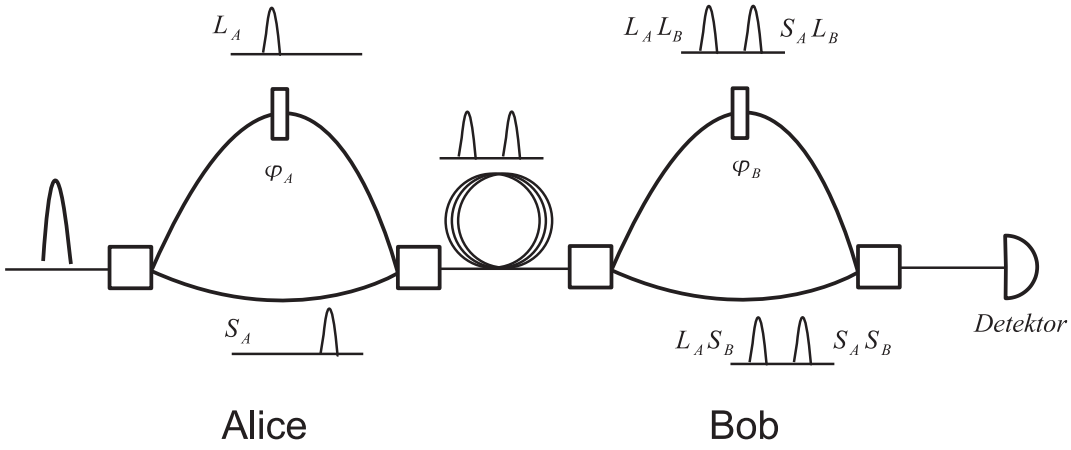

Abbildung 1.4: *Darstellung der zeitlichen Zustände beim Passieren von Alice und Bobs Interferometer*

Seite, so stehen erneut zwei unterschiedlich lange Wege zu Verfügung, und das Photon geht wieder in eine kohärente Überlagerung der beiden möglichen Zeitfenster über. Der Zustand am Ausgang von Bobs Interferometer lässt sich schreiben als:

$$|\psi'\rangle = \frac{1}{2}\left(|1,0,0\rangle + e^{i\varphi_A}|0,1,0\rangle + e^{i\varphi_B}|0,1,0\rangle + e^{i(\varphi_B+\varphi_A)}|0,0,1\rangle\right). \tag{1.28}$$

Detektiert Bob zeitabhängig, so erhält er drei Maxima (Abbildung 1.5). Das erste Maxi-

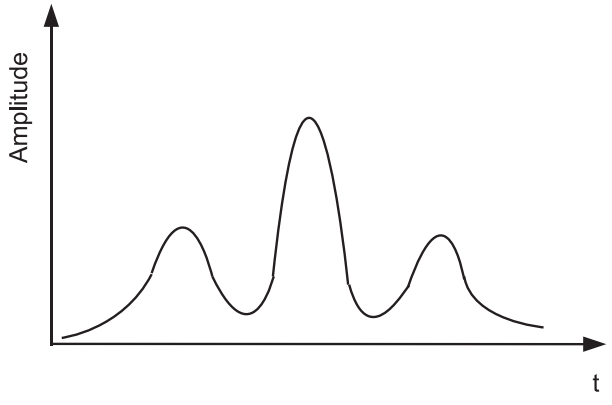

Abbildung 1.5: *Detektionsereignisse am Ausgang von Bobs Interferometer*

mum gehört zu Photonen, die in beiden Interferometern jeweils den kurzen Weg durchlaufen haben ($|1,0,0\rangle$), während im dritten Maximum Photonen detektiert werden, die jeweils durch die langen Arme gelaufen sind ($|0,0,1\rangle$). Der mittlere Peak schließlich gehört zu zwei unterschiedlichen Pfaden. Photonen, die entweder den kurzen Arm auf Alice und dann den langen Arm auf Bobs Seite oder zuerst den langen Arm von Alice Interferometer und anschließend Bobs kurzen Interferometerarm genommen haben, werden gleichzeitig detektiert ($|0,1,0\rangle$). Bei Ununterscheidbarkeit der beiden Pfade interferieren diese miteinander. Die Wahrscheinlichkeit P ein Photon im mittleren Peak zu detektieren ist

$$P = |\langle 0,1,0|\,\psi'\rangle|^2 . \tag{1.29}$$

Setzt man $|\psi'\rangle$ aus Gleichung (1.28) ein, so erhält man

$$P = \frac{1}{4}\left(e^{i\varphi_A} + e^{i\varphi_B}\right)^2 = \frac{1}{2}\left[1 + \cos(\varphi_B - \varphi_A)\right]. \tag{1.30}$$

Die Detektionsereignisse variieren also mit der relativen Phase $(\varphi_B - \varphi_A)$. Für eine hohe Visibilität der beiden interferierenden Pfade ist es notwendig, dass der Weglängenunterschied der beiden Interferometerarme nicht um mehr als einen Bruchteil der benutzten Wellenlänge variiert. Dies erfordert Stabilisierungskonzepte, die Fluktuationen und Drifften in der Phase beider Interferometer ausgleicht, um so korrekte Phasenrelationen zu garantieren.

BB84-Protokoll mit Phasenkodierung

Die Interferenz der beiden ununterscheidbaren Pfade $L_A S_B$ und $S_A L_B$ (Zustand $|0,1,0\rangle$) ist die Grundlage für die phasenkodierte Implementierung des BB84-Protokolls mit den eben beschriebenen Interferometern. Um die Bitwerte 0 und 1 zu senden, muss die relative Phase $\varphi_B - \varphi_A$ variiert werden.
Alice benötigt zur Kodierung der Werte 0 und 1 zwei unterschiedliche Basen. Dazu stellt sie den Wert 0 entweder als Phasenverschiebung 0 (Basis 0) oder mit $\pi/2$ (Basis 1) dar. Der Bitwert 1 wird mit den Phasenverschiebungen π (Basis 0) und $3\pi/2$ kodiert. Alice wendet also vier verschiedene Phasenverschiebungen an $(0, \pi/2, \pi, 3\pi/2)$, um so jeweils die Basis und den Bitwert zu kodieren. Bob hingegen wählt zufällig zwischen den beiden Phasenverschiebungen 0 und $\pi/2$. Wenn ihr Phasenunterschied gleich 0 oder π ist, nutzen Alice und Bob die gleiche Basis. In diesen Fällen registrieren sie beide den gleichen Bitwert. Stimmen ihre Basiszustände nicht überein, d.h. ist der Phasenunterschied gleich $\pi/2$ oder $3\pi/2$, so erhält Bob ein zufälliges Messergebnis. Eine Zusammenfassung gibt das Beispiel in Tabelle (1.2).
Zusammenfassend erkennt man also, dass das BB84-Protokoll die Möglichkeit eröffnet, bei Benutzung einzelner Photonen als Informationsträger, einen sicheren Schlüssel zwischen Alice und Bob zu etablieren. Die Nutzung von *time-bin* Qubits und die Implementierung

Alice	Bob			
Zufallsfolge	φ_A	φ_B	$\varphi_A - \varphi_B$	**Schlüssel**
1	π	$\pi/2$	$\pi/2$	
1	$3\pi/2$	0	$3\pi/2$	
0	$\pi/2$	$\pi/2$	0	0
1	π	0	π	1
0	0	$\pi/2$	$3\pi/2$	
1	$3\pi/2$	$\pi/2$	π	1
0	0	0	0	0
0	$\pi/2$	0	$\pi/2$	
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$	

Tabelle 1.2: *Implementierung des BB84-Protokolls mit Phasenkodierung*

phasenkodierter Quantenkryptographieprotokolle stellt eine Alternative zur Polarisationskodierung dar und ist dafür geeignet auch über längere Strecken einen sicheren Schlüssel zwischen Alice und Bob zu etablieren.

Kapitel 2

Experimenteller Aufbau

Dieses Kapitel beschreibt den Gesamtaufbau des Experiments zur *time-bin*-Kodierung sowie die Funktion und die Eigenschaften der Komponenten, die zu dessen Realisierung notwendig sind. Einen schematischen Überblick gibt Abbildung 2.1. Das zentrale Element bilden die beiden mit Alice und Bob bezeichneten Michelson-Interferometer. Sie dienen der Kodierung bzw. Dekodierung nach dem *time-bin*-Schema. Der Aufbau zur Pulserzeugung erlaubt es, Gauß-Pulse mit einer Dauer von weniger als 100 ns zu generieren. Die Detektion erfolgt im Limit einzelner Photonen pro Puls mit einer APD, im Betrieb mit klassischen Pulsen mit einem schnellen Detektor. Die Interferometer sollen Teil eines Experiments zur Photonenspeicherung in Cäsiumgas unter Ausnutzung des EIT-Effekts sein. Dies legt die Rahmenbedingungen und die Anforderungen fest, denen der Aufbau genügen muss. Im EIT-Experiment wird die D1-Linie des Cäsiums genutzt. Die D1-Linie bezeichnet den Übergang zwischen den Feinstrukturniveaus $6^2S_{1/2}$ und $6^2P_{1/2}$, die jeweils in zwei Hyperfeinniveaus aufgespalten sind. Das für den EIT-Effekt genutzte Drei-Niveau-System in Λ-Anordnung (Abbildung 2.2) wird dabei durch die beiden Hyperfeinniveaus (F=3, F=4) des Feinstrukturniveaus $6^2S_{1/2}$ und durch ein Hyperfeinniveau (F=4) des Feinstrukturniveaus $6^2P_{1/2}$ gebildet. Das Probefeld koppelt dabei an den

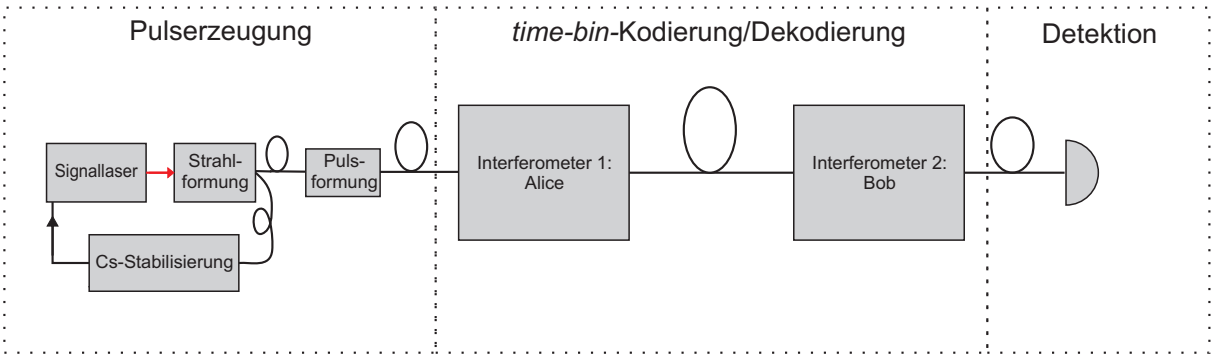

Abbildung 2.1: *schematischer Aufbau des Experiments*

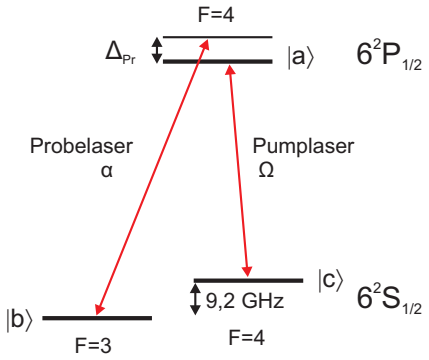

Abbildung 2.2: *Drei-Niveau-System in Λ-Anordnung der Cäsium D1-Linie*

Übergang $6^2S_{1/2}(F = 3) \rightarrow 6^2P_{1/2}(F = 4)$ mit einer Vakuumwellenlänge $\lambda = 894,578$ nm. Die im OPO erzeugten Einzelphotonen haben eine geringe spektrale Bandbreite in der Größenordnung von 10 MHz, um eine effektive Wechselwirkung mit den atomaren Resonanzen zu garantieren. Eine spektrale Bandbreite in der Größenordnung von 10 MHz entspricht dabei einer Pulsdauer von ca. 100 ns. Die Einstellung spezieller Qubit-Werte erfolgt für *time-bin*-Qubits über die Einstellung der relativen Phase zwischen beiden Interferometerarmen. Daher muss die Einstellung spezieller Phasenwerte möglich sein. Dies erfordert des Weiteren die Stabilität der Interferometer in der Größenordnung der benutzten Wellenlänge, um stabile Phasenbeziehungen zu garantieren. Zusammenfassend ist die Implementierung der *time-bin*-Kodierung also an die folgenden Bedingungen geknüpft:

- Wellenlänge der Signalphotonen: $\lambda \cong 894$ nm
- spektrale Bandbreite des Signals: $\Delta\nu \cong 10$ MHz mit entsprechender Pulslänge $T \cong 100$ ns
- Möglichkeit definierter Phaseneinstellung
- Stabilität in der Größenordnung der Wellenlänge

Hierfür werden mit dem Aufbau zur Pulserzeugung Pulse mit 100 ns Dauer erzeugt. Zur Realisierung eines unsymmetrischen Interferometers mit großem optischen Weglängenunterschied für die *time-bin*-Kodierung eignet sich ein Michelson-Interferometer. Es bietet den Vorteil, dass die Interferometerarme zweifach durchlaufen werden und der optische Weglängenunterschied damit verdoppelt wird. Mit einer optischen Faser von 50 m Länge ergibt sich so eine Weglängendifferenz von 100 m bzw. eine Zeitdifferenz von ≈ 500 ns, was deutlich größer als die Puldsdauer von 100 ns ist. Für die Einstellung definierter Phasenverschiebungen wird ein elektrooptischer Modulator (EOM) verwendet. Die Stabilität der Interferometer wird gewährleistet durch passive Temperaturstabilisierung sowie aktive Stabilisierung der Interferometerarmlänge mithilfe eines Piezoelements. Im folgenden soll nun auf die einzelnen Komponenten des Experiments eingegangen werden.

2.1 Die Interferometer

Die beiden Interferometer zur Kodierung bzw. Dekodierung sind in der Form von Michelson-Interferometern realisiert. Nach einer kurzen Einführung in die grundlegende Funktionsweise eines Michelson-Interferometers wird die konkrete Umsetzung gemäß der eingangs dargestellten Anforderungen beschrieben.

2.1.1 Grundlagen des Michelson-Interferometers

Abbildung (2.3) zeigt die schematische Darstellung eines Michelson-Interferometers. Der einfallende Strahl wird am Strahlteiler (BS) in zwei Strahlen aufgeteilt. An den Spiegeln werden die Teilstrahlen zurückreflektiert und treffen wieder auf den Strahlteiler. Dort werden die Teilstrahlen überlagert, interferieren und verlassen das Interferometer zum Eingang und Ausgang. Der Eingang ist also gleichzeitig ein zweiter Ausgang. Für die Berechnung der Transferfunktion betrachtet man das folgende Lichtfeld am Eingang

$$E_{in} = E_0 e^{-(i\omega t - \boldsymbol{kr})}, \tag{2.1}$$

wobei ω die angenommene feste Kreisfrequenz des Lichtfeldes ist. Durch den Strahlteiler (BS) mit der Reflektivität r_{BS} und der Transmittivität t_{BS} ergeben sich zwei Felder:

$$E_1 = -E_{in} r_{BS} e^{i\omega l_1/c} \tag{2.2}$$

$$E_2 = E_{in} t_{BS} e^{i\omega l_2/c} \tag{2.3}$$

Das Feld im Arm 1 ist aufgrund der Reflektion am Strahlteiler um 180° phasenverschoben. Der Phasenfaktor ist außerdem abhängig vom jeweils zurückgelegten Weg l_1 bzw. l_2. Nach

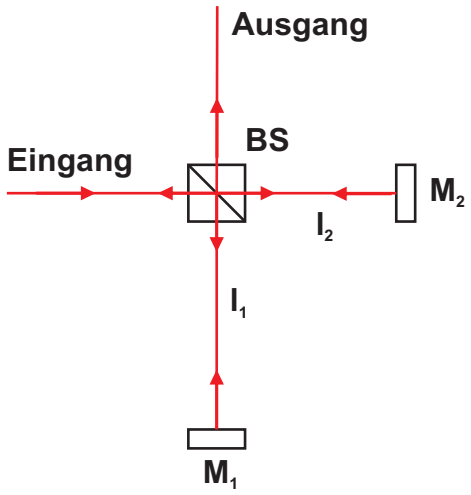

Abbildung 2.3: *Michelson-Interferometer mit Strahlteiler (BS) und den Spiegeln M_1 und M_2. Im Ausgang entsteht ein vom Wegunterschied $(l_1 - l_2)$ abhängiges Interferenzsignal.*

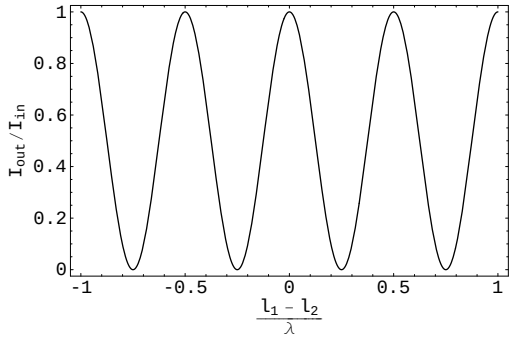

Abbildung 2.4: *Intensität in Abhängigkeit von Armlängenunterschied*

der Reflektion an den Spiegeln M_1 und M_2 mit den Reflektionskoeffizienten r_1 und r_2, wobei beide Strahlen einen Phasensprung von 180° erfahren, ergibt sich am Strahlteiler nun

$$E_1 = E_{in} r_{BS} r_1 e^{i2\omega l_1/c} \tag{2.4}$$

$$E_2 = -E_{in} t_{BS} r_2 e^{i2\omega l_2/c} \tag{2.5}$$

Als Folge der Überlagerung der beiden Teilstrahlen erhält man im Ausgang

$$E_{out} = E_{in} t_{BS} r_{BS} \left(e^{i2\omega l_1/c} + e^{i2\omega l_2/c} \right) \tag{2.6}$$

und damit die Transferfunktion für das in den Ausgang reflektierte Feld

$$T_{MI} = \frac{E_{out}}{E_{in}} = t_{BS} r_{BS} \left(r_1 e^{i2\omega l_1/c} + r_2 e^{i2\omega l_2/c} \right). \tag{2.7}$$

Für die qualitative Diskussion seien ideale Bedingungen ($r_1 = r_2 = 1$) und ein verlustfreier 50:50 Strahlteiler angenommen. Damit erhält man

$$T_{MI} = \frac{1}{2} \left(e^{i2\omega l_1/c} + e^{i2\omega l_2/c} \right) = \cos\left(\frac{\omega}{c} (l_1 - l_2) \right) e^{i\omega(l_1 + l_2)}. \tag{2.8}$$

Für die Intensität am Ausgang ergibt sich eine Abhängigkeit vom Armlängenunterschied $(l_1 - l_2)$

$$I_{out} = I_{in} \cos^2\left(\frac{\omega}{c} (l_1 - l_2) \right). \tag{2.9}$$

Der Verlauf der Intensität ist in Abbildung 2.4 dargestellt.
Die **Visibilität V** der Streifen in einem Interferenzexperiment ist definiert als:

$$V = \frac{I_{max} - I_{min}}{I_{max} + I_{min}} \tag{2.10}$$

Die obige Diskussion der Interferenz in einem Michelson-Interferometer verlief unter der Annahme, dass die Phasendifferenz zwischen den beiden interferierenden Strahlen nur von der Wegdifferenz $2(l_1 - l_2)$ abhängt. Dies gilt nur für monochromatische Wellen. Realistische Lichtquellen haben immer eine Frequenzbandbreite $\Delta\omega$, was zur Verschlechterung der Visibilität führt und so praktische Grenzen der maximalen Wegdifferenz setzt, bei der man einen guten Streifenkontrast beobachtet. Die zeitliche Kohärenz einer Lichtquelle ist also entscheidend für die Beobachtbarkeit von Interferenz in einem Michelson-Interferometer und wird quantifiziert durch die *Kohärenzzeit* τ_c, wobei gilt

$$\tau_c \approx \frac{1}{\Delta\omega}. \tag{2.11}$$

Eine äquivalente Größe ist die *Kohärenzlänge* L_c,

$$L_c = c\,\tau_c. \tag{2.12}$$

Zur genaueren Beschreibung zeitlicher Kohärenz führt man die *Korrelationsfunktion 1. Ordnung* $g^{(1)}(\tau)$ ein, welche definiert ist als

$$g^{(1)}(\tau) = \frac{\langle E^*(t)E(t+\tau)\rangle}{\langle |E(t)|^2\rangle}. \tag{2.13}$$

Nimmt man eine Lichtquelle konstanter mittlerer Intensität an, so dass die Interferenz nur noch von der Zeitdifferenz $\tau = 2\Delta l/c$ abhängt, kann man das Feld am Ausgang des Michelson-Interferometers schreiben als:

$$E_{out}(t) = \frac{1}{\sqrt{2}}\left(E(t) + E(t+\tau)\right) \tag{2.14}$$

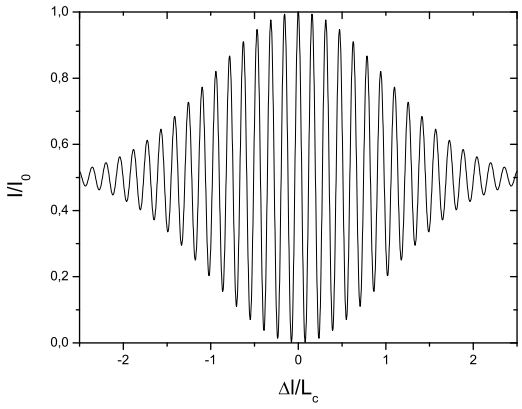

Abbildung 2.5: *Interferogramm für eine Lichtquelle mit spektraler Gauß-Verteilung*

Für die mittlere Intensität am Ausgang erhält man damit:

$$\begin{aligned} I(\tau) &\propto \langle E^*_{out}(t) E_{out}(t) \rangle \\ &\propto \langle E^*(t) E(t) \rangle + Re\left[\langle E^*(t) E(t+\tau) \right]\rangle . \end{aligned} \tag{2.15}$$

Einsetzen von Gleichung (2.13) ergibt

$$\begin{aligned} I(\tau) &\propto \left\langle E^*(t) E_(t) \right\rangle \left(1 + Re\left[g^{(1)}(\tau)\right]\right) \\ &= I_0 \left(1 + Re\left[g^{(1)}(\tau)\right]\right) . \end{aligned} \tag{2.16}$$

Für die Visibilität bedeutet das mit $I_{max/min} = I_0(1 \pm \left|g^{(1)}(\tau)\right|)$:

$$V = \left|g^{(1)}(\tau)\right| . \tag{2.17}$$

Der Interferenzkontrast misst also den Betrag der Autokorrelationsfunktion $g^{(1)}(\tau)$. Über das Wiener-Kintchin-Theorem ist diese mit der spektralen Leistungsdichte $S_E(\omega)$ verknüpft:

$$S_E(\omega) = I_0 \int_0^\infty g^{(1)}(\tau) e^{i\omega\tau} d\tau \tag{2.18}$$

Bei endlicher Linienbreite der Lichtquelle erhält man also ein Interferogramm ähnlich Abbildung 2.5.

2.1.2 Aufbau der Michelson-Interferometer

Nach der Einführung in die grundlegende Funktionsweise eines Michelson-Interferometers folgt nun die konkrete experimentelle Umsetzung gemäß den Anforderungen für die *time-bin*-Kodierung schmalbandiger Photonen. Es passieren zwei Strahlen unterschiedlicher Wellenlänge die Interferometer. Mit dem Referenzlaser der Wellenlänge $\lambda = 852$ nm wird der Forderung nach Stabilität der Interferometerarme nachgekommen. Er dient zur Realisierung eines aktiven Stabilisierungsschemas (siehe Abschnitt 2.1.5). Der zweite Strahl besteht aus den eigentlichen Signalphotonen, die nach dem *time-bin*-Schema kodiert werden sollen. Der Signalstrahl gelangt über einen Faserkoppler in das Interferometer. Er passiert einen polarisierenden Strahlteilerwürfel (PBS) und trifft anschließend auf den Strahlteiler (BS). Der hier reflektierte Strahl wird in eine Faser eingekoppelt, die eine Länge von 50 m hat und den langen Arm des unsymmetrischen Michelson-Interferometers bildet. Nach Reflektion an der verspiegelten Endfacette (M) der Faser (siehe Abschnitt 2.1.3) tritt der Strahl wieder aus der Faser aus. Der am Strahlteiler transmittierte Teil des Eingangsstrahls durchläuft den kurzen Arm des Interferometers. Nach der Rückreflektion am Endspiegel (PZT-Spiegel) kommt es zur Überlagerung der Teilwellen aus kurzem und langem Arm. Die Weglängendifferenz der beiden Arme beträgt 100 m. Für Pulse mit einer Dauer von 100 ns ist nun keine Interferenz möglich. Die beiden alternativen Wege des Interferometers sind so zeitlich getrennt, und eine Kodierung nach dem *time-bin*

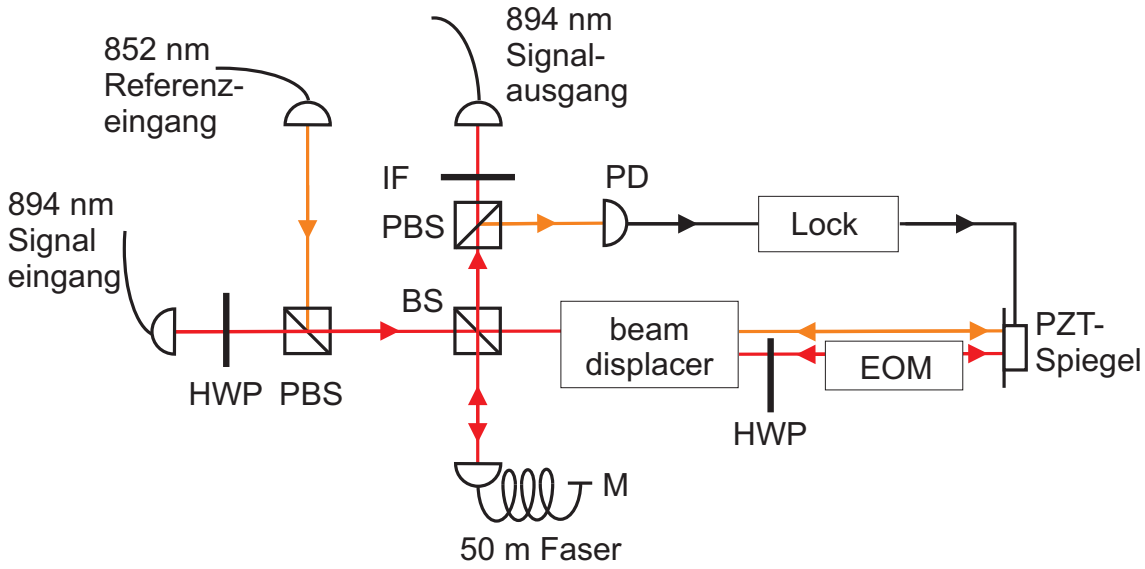

Abbildung 2.6: *Schematischer Aufbau der Interferometer*

Schema ist möglich. Die für die Phasenkodierung notwendige Aufprägung einer globalen Phase geschieht für die Signalphotonen mit einem elektrooptischen Modulator (EOM) im kurzen Arm des Interferometers (siehe Abschnitt 2.1.4). Über eine davor postierte Halbwellenplatte (HWP) wird die Polarisation parallel zur optischen Achse dieses EOM eingestellt.
Der Referenzlaser ist vertikal polarisiert und wird nach Reflektion am ersten PBS in das Interferometer eingekoppelt. Er durchläuft ebenfalls die 50 m-Faser und den kurzen Arm des Interferometers. Der doppelbrechende Calcit-Kristall (*beam displacer*) allerdings trennt Referenz- und Signalstrahl im kurzen Arm, um eine Phasenänderung des Referenzstrahls durch den EOM zu verhindern.
Am Ausgang des Interferometers wird der Referenzstrahl an einem weiteren PBS abgebeugt und trifft auf den Detektor. Der Signalstrahl wird am PBS transmittiert und anschließend ausgekoppelt. Der Interferenzfilter (IF) dient der weiteren Trennung von Referenz- und Signalstrahl. Die Signalphotonen werden dann über die Faser zum Dekodierungsinterferometer geführt. Der Verlauf der Strahlen dort ist identisch zum Kodierungsinterferometer.

2.1.3 Verzögerungsfaser

Die Realisierung einer optischen Weglängendifferenz zur zeitliche Trennung einlaufender Pulse gemäß dem *time-bin*-Schema (Abschnitt 1.3) erfolgt mit einer optischen Faser. Es handelt sich um eine polarisationserhaltende Ein-Moden-Faser mit APC-Steckern, so dass parasitäre Etalons zwischen den Faserendflächen minimiert werden. Die Pulse haben eine

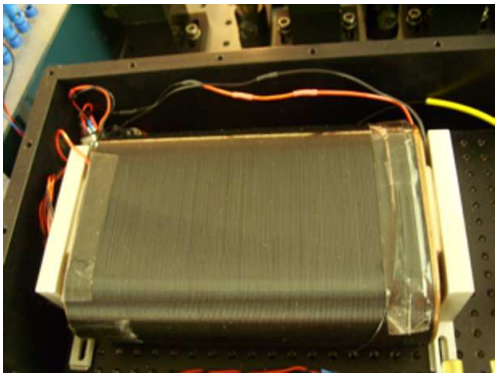

Abbildung 2.7: *Verzögerungsfaser montiert auf einem Kupferblock.*

zeitliche Länge von 100 ns. Dementsprechend wurde eine optische Faser mit 50 m Länge gewählt. Die Endfacette der Faser ist mit einer hochreflektiven Schicht verspiegelt, so dass ein Auskoppeln und anschließendes Einkopplen in die Faser nicht nötig ist. Nach zweimaligem Durchlaufen der Faser ergibt sich so ein Wegunterschied von 100 m. Das entspricht dann einer zeitlichen Differenz von ungefähr 500 ns.
Um interferometrische Stabilität zu gewährleisten, ist es nötig, dass sich die Faser weniger als der Stellweg des Piezoelements für die Interferometerstabilisierung ändert. Daher ist eine passive Stabilisierung der Faser notwendig. Die Faser wurde auf einen thermisch stabilisierten Kupferblock gewickelt, um bereits eine passive Stabilisierung zu gewährleisten. Dies reduziert sowohl die thermische Ausdehnung der Faser als auch Polarisationsänderungen aufgrund der Faserbiegung. Der verwendete Temperaturregler erlaubt eine Stabilisierung auf 25 mK, was bei einem thermischen Ausdehnungskoeffizienten von Quarz ($\alpha = 6 \times 10^{-7}$ K^{-1}) einer absoluten Längenänderung von 0,75 μm entspricht. Aufgrund der richtig gewählten orthogonalen Eingangspolarisation von Signal- und Referenzstrahl parallel zur schnellen bzw. langsamen Achse der Faser konnte so jede störende Änderung der Polarisation vermieden werden.

2.1.4 Elektrooptischer Modulator zur definierten Phaseneinstellung

Die Einstellung spezieller Qubitwerte erfolgt bei *time-bin*-Qubits über die Einstellung definierter globaler Phasenverschiebungen (Abschnitt 1.3). Für die Realisierung phasenkodierter Quantenkryptographie mit *time-bin*-Qubits nach dem BB84-Protokoll sind das z.B. die Werte $0, \frac{\pi}{2}, \pi, \frac{3}{2}\pi$.
Wichtig ist, dass nur der Signalstrahl eine Phasenänderung erfährt, während der Referenzstrahl unverändert bleibt. Ansonsten wäre eine Stabilisierung nicht möglich. Aus diesem Grund durchlaufen Signal- und Referenzstrahl zunächst einen doppelbrechenden Kristall (*beam displacer*). Es handelt sich dabei um einen Calcit-Kristall mit 45 mm Länge. Der

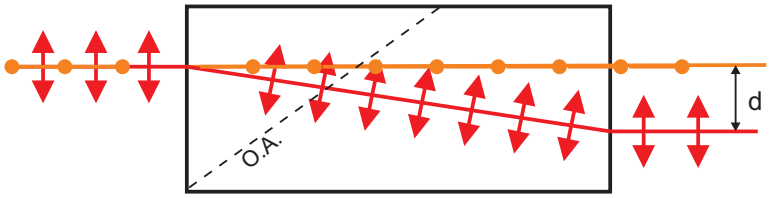

Abbildung 2.8: *Calcit-Kristall zur Trennung von Signal- und Referenzstrahl.*

Referenzstrahl durchläuft den Kristall als ordentlicher Strahl, während der Signalstrahl den Kristall als außerordentlicher Strahl passiert (Abbildung 2.8). Aufgund der Länge ergibt sich ein horizontaler Abstand der beiden Strahlen von 5 mm. Die Phasenänderung erfolgt nun mit einem elektrooptischen Modulator (EOM). Es handelt sich dabei um eine Sonderanfertigung des Modells 4102 der Firma New Focus. Mit einer zusätzlichen Apertur im Gehäuse des Geräts ist es möglich, dass der Referenzstrahl unverändert den EOM passiert, während der Signalstrahl den eigentlichen Weg durch den EOM nimmt (Abbildung 2.9). Der EOM besteht aus zwei MgO:$LiNbO_3$-Kristallen. An zwei gegenüberliegenden Seiten der Kristalle sind Elektroden aufgedampft. Durch Anlegen einer Spannung erreicht man aufgrund des elektooptischen Effekts eine Brechungsindexänderung Δn zwischen zwei senkrechten Achsen des Kristalls. Die beiden Kristalle sind dabei um 90° gegeneinander gedreht, um durch Temperaturdrift verursachte Doppelbrechung zu minimieren. Die Halbwellenspannung für 895 nm beträgt 276 V. Der EOM wird allerdings zweifach durchlaufen (*double-pass*), so dass sich die Halbwellenspannung auf 138 V reduziert. Mit Hilfe einer Halbwellenplatte vor der Eingangsapertur wird die Polarisation des Signalstrahls auf die optische Achse des Kristalls eingestellt, um so eine globale Phasenänderung zu gewährleisten und eine Polarisationsdrehung zu vermeiden.
Die Ansteuerung erfolgt mit einem in der Arbeitsgruppe entwickelten Treiber. Er liefert Ausgangsspannungen im Bereich ±200 V mit einer Bandbreite von > 500 kHz. Damit ist es möglich, eine Phasenverschiebung innerhalb von 2π einzustellen und insbesondere die

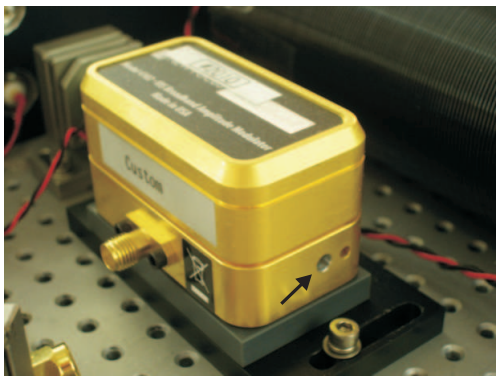

Abbildung 2.9: *EOM 4102 mit zusätzlicher Apertur (schwarzer Pfeil).*

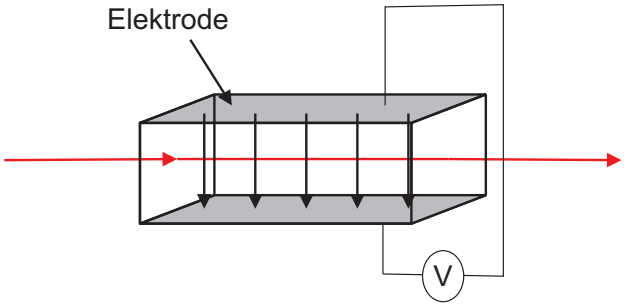

Abbildung 2.10: *Schematischer Aufbau eines EOM.*

für die phasenkodierte Quantenkryptographie notwendigen Basiszustände.

2.1.5 Interferometerstabilisierung

Das Einstellen spezifischer Phasenwerte erfordert die Stabilität der Interferometer in der Größenordnung der Signalwellenlänge. Nur wenn eine stabile Phasenlage der Arme garantiert ist, ist die Phasenkodierung mit dem EOM möglich. Hierfür wurden zwei Stabilisierungsschemata realisiert. Zum einen wird eine passive Temperaturstabilisierung gewährleistet. Die Grundplatte liegt auf vier Peltierelementen. So ist es möglich, eine für den gesamten Aufbau konstante Temperatur zu realisieren. Der kompakte Aufbau in 20 mm Strahlhöhe und die Integration des Interferometers in eine verschließbare Box minimieren außerdem Temperaturdriften durch die Umgebung. Um thermisch induzierte Phasenänderungen des Kristalls zur Trennung von Referenz- und Signalstrahl zu vermeiden, wird auch dieser passiv stabilisiert. Der Kristall liegt in einem thermisch stabilisierten Kupferblock. Auch hier hat der verwendete Temperaturcontroller eine Genauigkeit von 25 mK. Somit erreicht man mit dem Ausdehnungskoeffizienten von Calcit ($\alpha \approx 6 \times 10^{-6}\,\mathrm{K}^{-1}$) eine maximale Längenausdehnung von ungefähr 7 nm. Wie in Abschnitt (2.1.3) beschrieben, ist auch die Verzögerungsfaser thermisch stabilisiert.
Über die passive thermische Stabilisierung hinaus ist außerdem eine aktive Stabilisierung möglich. Dazu wird über einen zusätzlichen Eingang ein Referenzlaser in das Interferometer gebracht. Er ist orthogonal zum Signalstrahl polarisiert und kann so vor dem EOM mit dem Calcit-Kristall vom Signal getrennt werden. Das Fehlersignal ist somit unabhängig von den Phasenänderungen, die durch den EOM induziert werden. Im folgenden soll nun auf den Referenzlaser und auf den Regelkreis zur aktiven Stabilisierung näher eingegangen werden.

Referenzlaser

Die Laserdiode (#LD-0852-0150-DFB-1 der Firma Toptica) ist eine DFB- (*distributed feedback*) Laserdiode. In den Halbleiterchip ist ein Bragg-Gitter integriert. Das Gitter se-

lektiert eine bestimmte longitudinale Lasermode und bestimmt so die Wellenlänge. Bei einer DFB-Diode ist das Gitter dabei direkt in die aktive Region der Diode integriert. Durch Ändern des Gitterabstands mittels Temperatur und Strom, kann so die Emissionswellenlänge geändert werden.
Die hier benutzte Diode hat einen Schwellenstrom von $I_{th} = 30$ mA. Die Emissionswellenlänge liegt in einem Bereich von $\lambda = 851.2$ nm bis $\lambda = 853.7$ nm.
Die Nutzung der Diode als Referenzlaser für die Stabilisierung erfordert eine schmale Linienbreite. Sie ist mit $\Delta\nu \approx 0,5$ MHz angegeben. Damit ergibt sich eine Kohärenzlänge L_c von

$$L_c = \frac{c}{\Delta\nu} \approx 600\ m.$$

Das ist größer als der Wegunterschied von $\Delta l = 100$ m in den Interferometern, und es ist somit möglich, ein Interferenzsignal zu erzeugen.
Der Referenzlaser befindet sich im Kodierungsinterferometer. Zur Verminderung von Rückreflexionen in die Laserdiode ist vor der Laserdiode ein Faraday-Isolator postiert (Die durch den Kristall im Magnetfeld hervorgerufene Polarisationsdrehung ist richtungsabhängig (Faraday-Effekt) und hat zur Folge, dass rückreflektiertes Licht abgebeugt wird). Der Referenzstrahl wird anschließend in optische Fasern zur Strahlformung eingekoppelt und zu den beiden Interferometern geführt.

Regelkreise

Ganz allgemein folgt die Regelung einer physikalischen Größe, wie z.B. die Temperatur, die Frequenz eines Lasers oder die Weglänge eines Interferometers, immer dem gleichen Schema (Abbildung 2.11).
Die Regelgröße soll auf einem bestimmten Sollwert (Führungsgröße) gehalten werden. Der zu regelnde Parameter u wird als Regelgröße (Istwert) bezeichnet. Aus der Differenz zwischen Regelgröße und Führungsgröße (Sollwert) $w-u(t)$ ergibt sich eine Regelabweichung als Eingangssignal für einen Regler. Die Übertragungsfunktion F_R des Reglers bestimmt dann den Stellwert $s(t) = F_R(w-u(t))$. Dazu wird die Störgröße $e(t)$ addiert. Beide wirken

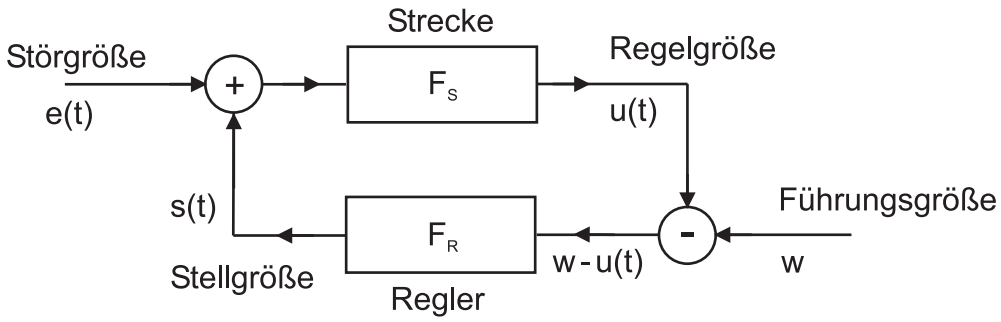

Abbildung 2.11: *Blockschaltbild eines Regelkreises [TS93].*

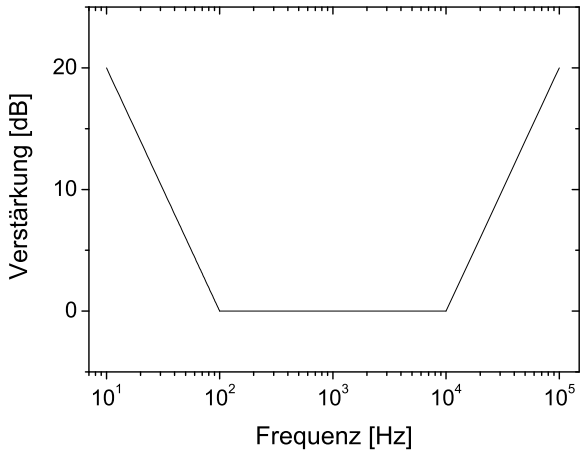

Abbildung 2.12: *Übertragungsfunktion eines PID-Reglers. Der I-Anteil fällt mit 20dB/Dekade ab (links), der P-Anteil ist nicht frequenzabhängig (Mitte), der D-Anteil steigt mit 20dB/Dekade an (rechts)*

über die Übertragungsfunktion der Regelstrecke F_S wieder auf die Regelgröße $u(t)$. Die Größe $F_0 = F_R F_S$ bezeichnet man als Schleifenverstärkung. Je nach Regelaufgabe wird der Proportionalregler (*P-Regler*) mit einem integrierenden Anteil zum *PI-Regler*, bzw. mit einem integrierenden und differenzierenden Anteil zum *PID-Regler* kombiniert. In der Praxis werden häufig PID-Regler eingesetzt, da sie die Regelgröße schnell in die Nähe des Sollwerts bringen und die verbleibende Abweichung ebenfalls ausregeln. Für den Fall der Interferometerstabilisierung sieht die Regelung wie folgt aus: Der Referenzlaser erzeugt

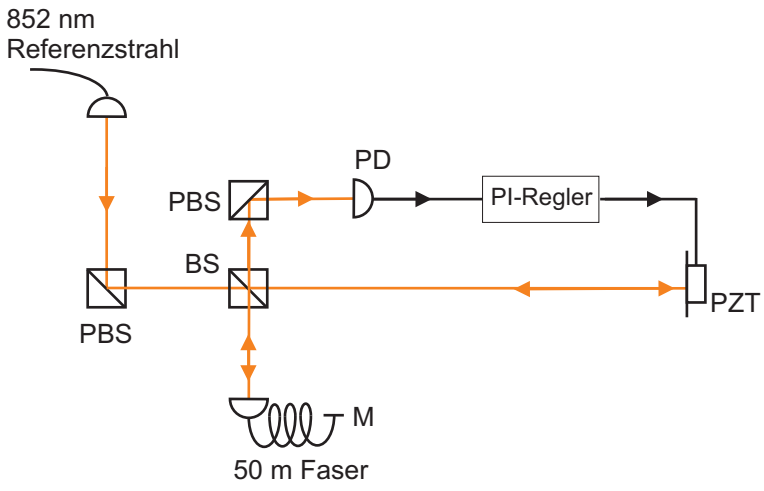

Abbildung 2.13: *Schema der aktiven Interferometerstabilisierung*

für den Fall einer Änderung von $(l_1 - l_2)$ am Detektor ein Signal gemäß Gleichung (2.9),

$$I_{out} = I_{in} \cos^2 \left(\frac{\omega}{c}(l_1 - l_2) \right).$$

Das Interferenzsignal dient nun als Fehlersignal für den Regler. Der Regler ist in diesem Fall ein PI-Regler mit einer Zeitkonstante von 2 ms. Entsprechend dem allgemeinen Regelungsschema gibt der Regler ein Stellsignal aus. Das Stellelement ist in diesem Fall ein Piezoelement, befestigt am Spiegel im kurzen Interferometerarm (Abbildung 2.13). Auf diese Weise ist es möglich, aktiv nachzuregeln und so die Stabilität der Interferometer zu gewährleisten.

2.2 Laserquelle

Die für die *time-bin*-Kodierung notwendigen Signalpulse werden mit einem Lasersystem erzeugt, dessen Details in diesem Abschnitt beschrieben werden. Speziell soll auf den verwendeten Laser, dessen Stabilisierung auf einen Cäaiumübergang sowie die Erzeugung der Pulse eingegangen werden.

Der Laser

Bei dem verwendeten Laser handelt es sich um einen gitterstabilisierten Diodenlaser. Üblicherweise dient der Halbleiterkristall selber als Laserresonator und ermöglicht Linienbreiten von einigen 10 MHz. Die Integration der Laserdiode in einen externen Resonator ermöglicht die Verringerung der Linienbreite und eine Verbreiterung des spektralen Bereichs modensprungfreier Verstimmung der Emissionswellenlänge. Damit sind Linienbreiten im Bereich von 1 kHz technisch möglich [Wya85, WD83].
Der Laser ist in einer Littman/Metcalf-Konfiguration aufgebaut [HM91, Las05]. Das kollimierte Licht der Diode trifft auf ein Beugungsgitter. Mit dem Spiegel wird das in erster Ordnung gebeugte Licht zurück in die Laserdiode gekoppelt. In unsererm Aufbau wird

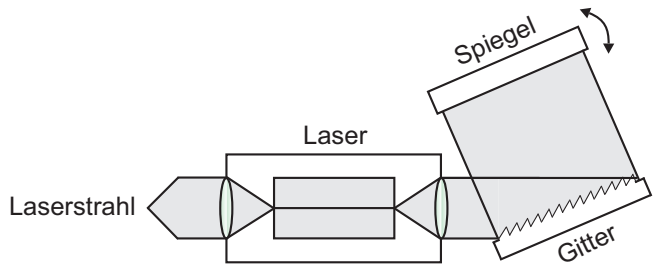

Abbildung 2.14: *Aufbau des Diodenlasers in Littman/Metcalf-Konfiguration. Der drehbare Spiegel bildet zusammen mit dem Gitter einen verstimmbaren Resonator.*

Modulations-pfad	Wirkungsweise	Verursachte Wellenlängen-änderung	Bandbreite des Pfades
Temperatur	Änderung der Temperatur und damit der Geometrie der Laserdiode durch einen Strom im Peltier-Element	> 0.1 nm/K	< 10 mHz
Piezo (PZT)	Anlegen einer Spannung an den Laserpiezo und damit Modifikation des externen Resonators	~ 2 GHz/V	0 - 1000 Hz
Diodenstrom (PS)	Anlegen einer Spannung an den Modulationseingang des Stromtreibers, dadurch Änderung des Laserdiodenstroms	~ 100 MHz/V	0 Hz - 200 kHz

Tabelle 2.1: Möglichkeiten zur Modulation der Laserwellenlänge

das rückwärtig emittierte Licht als Laserstrahl genutzt. Der Spiegel und das Beugungsgitter bilden den externen Resonator. Über ein Piezo-Element ist der Resonatorspiegel drehbar und eine Verstimmung der Wellenlänge möglich. Die thermische Stabilisierung erfolgt über ein in den Aufbau integriertes Peltier-Element. Im Experiment wird das Modell TEC-520 der Firma Sacher genutzt. Der Laser liefert eine Ausgangsleistung von etwa 30 mW bei einer Wellenlänge $\lambda \approx 894$ nm.
Tabelle 2.1 gibt einen Überblick über die verschiedenen Pfade zur Verstimmung der Wellenlänge des Lasers. Der Laser wird von einem in der Arbeitsgruppe entwickelten Konstantstromtreiber angesteuert. Er verfügt über einen Modulationseingang mit dem der Ausgangsstrom und damit die Laserwellenlänge direkt variiert werden können (PS-Pfad). Das Piezoelement im Laser wird mit einem Treiber, der ebenfalls in der Arbeitsgruppe entwickelt wurde, in einem Bereich von 0-80 V angesteuert (PZT-Pfad).

2.2.1 Frequenzmodulationsspektroskopie

Die Wellenlänge des Lasers wird auf die D1-Linie von Cäsium stabilisiert. Die Laserstabilisierung ist als Frequenzmodulationsspektroskopie (FMS) realisiert. Der Laser wird dabei in einen starken *Pumpstrahl* und und einen schwächeren *Probestrahl* aufgespalten. Die Spektroskopie folgt dabei dem Schema der Doppler-freien Sättigungsspektroskopie. Durchquert ein Laserstrahl in z-Richtung ein Gas, so ist die Laserfrequenz ω_L im bewegten System der Teilchen Doppler-verschoben $\omega'_L = \omega_L - v_z k$. Zur Absorption tragen deshalb nur Moleküle aus dem Geschwindigkeitsbereich um $v_z = (\omega_L - \omega_0)/k$ bei. Wird

der starke Pumpstrahl in z-Richtung eingestrahlt, bewirkt er eine Verringerung der Besetzungsdichte $N_g(v_z)$ des absorbierenden Niveaus für die Geschwindigkeitsklasse Δv_z. Dementsprechend verringert sich der Absorptionskoeffizient $\alpha(\omega_L)$ für den Übergang. Je stärker die Sättigung des angeregten Niveaus, desto kleiner der Absorptionskoeffizient. Es gilt [Dem07]

$$\alpha(\omega_L) = \frac{\alpha_0(\omega_L)}{\sqrt{1+S_0}} \tag{2.19}$$

mit dem Absorptionskoeffizienten ohne Lichtwelle $\alpha_0(\omega_L)$ und dem Sättigungsparameter S_0. In der Besetzungsdichte $N_g(v_z)$ entsteht so bei v_z ein lokales Minimum, was auch als Bennett-Loch bezeichnet wird [Ben62]. Mit dem Probestrahl lässt sich dieses Minimum nun abfragen. Der Probestrahl durchquert das Medium antiparallel zum Pumpstrahl und wird daher von Molekülen aus dem Bereich um $v_z = -(\omega_L - \omega_0)/k$ absorbiert. Gilt $\omega_L = \omega_o$, so ist $v_z = 0$, und beide Strahlen wechselwirken mit denselben Molekülen. Die Sättigung des Besetzungsniveaus durch den Pumpstrahl führt so zu einem Einbruch der Absorption des Probestrahls an der Stelle $\omega_L = \omega_o$. Aufgrund der Wechselwirkung mit nur einer Geschwindigkeitsklasse, ist eine Auflösung unterhalb der Doppler-Breite möglich.
Die FMS ist eine Weiterentwicklung der Sättigungsspektroskopie und erhöht die Nachweisempfindlichkeit wie bei der Lock-In-Technik durch Modulation des Probestrahls mit der Frequenz ω_m und phasenempfindliche Detektion bei ω_m. Die Phasenmodulation erfolgt extern durch einen EOM, um eine Amplitudenmodulation durch direkte Modulation des Diodenstroms zu verhindern. Es gilt für die Feldstärke des modulierten Probestrahls:

$$E(t) = E_0 \cdot e^{i\omega_L t + i\beta \sin \omega_m t} + c.c.\,. \tag{2.20}$$

Die Stärke der Modulation wird bestimmt durch den Modulationsindex β. Diesen Ausdruck kann man mit Hilfe von Bessel-Funktionen entwickeln und erhält

$$E(t) = E_0 e^{i(\omega_L t)} \sum_{-\infty}^{\infty} J_l(\beta) e^{il\omega_m t} + c.c. \tag{2.21}$$

Für kleine Modulationsindizes ($\beta \ll 1$) kann man die Terme mit $|l| > 1$ vernachlässigen:

$$E(t) \approx \frac{E_0}{2}\left(e^{i\omega_L t} - \frac{\beta}{2} e^{i(\omega_L - \omega_m)t} + \frac{\beta}{2} e^{i(\omega_L + \omega_m)t}\right) + c.c.\,. \tag{2.22}$$

Damit erhält man drei verschiedene Strahlen, einen Träger mit der Frequenz ω_L und zwei Seitenbänder mit den Frequenzen $\omega_L \pm \omega_m$. Nach der Durchquerung einer Gaszelle der Länge L, mit Absorptionskoeffizient α und Brechungsindex n ergibt sich für das elektrische Feld

$$E_{Det}(t) = \frac{E_0}{2}\left(-T_{-1}\frac{\beta}{2} e^{-i\phi_{-1}} e^{i(\omega_L - \omega_m)t} + T_0 e^{-i\phi_0} e^{i\omega_L t} + T_{+1}\frac{\beta}{2} e^{-i\phi_{+1}} e^{i(\omega_L + \omega_m)t}\right) + c.c.\,. \tag{2.23}$$

Die Transmissionskoeffizienten für den Träger und die Seitenbänder sind $T_0 = e^{\delta_0}$ bzw. $T_{\pm 1} = e^{\delta_{\pm 1}}$ mit der frequenzabhängigen Dämpfung $\delta_j = \alpha_j(\omega_L + j\,\omega_m)L/2$ und der frequenzabhängigen Phasenverschiebung $\phi_j = n_j L(\omega_L + j\,\omega_m)/c$.
Die Intensität am Detektor ist $\langle I(t)\rangle \propto \langle |E(t)|^2\rangle$. Terme der Ordnung β^2 können für $\beta \ll 1$ vernachlässigt werden. Dämpfung und Phasenverschiebung für Träger und Seitenbänder unterscheiden sich kaum, so dass $|\delta_0 - \delta_1|$, $|\delta_0 - \delta_{-1}|$, $|\phi_0 - \phi_1|$, $|\phi_0 - \phi_{-1}|$ alle $\ll 1$. Der Detektor kann der Frequenz ω_L nicht folgen, d.h. alle Terme mit $e^{i\omega_L}$ verschwinden ebenfalls. Für die Intensität ergibt sich

$$\begin{aligned}\langle I(t)\rangle \propto T_0^2 - \frac{\beta}{2}T_0T_{-1}(&e^{i(\phi_{-1}-\phi_0)}e^{i\omega_m t} + e^{-i(\phi_{-1}-\phi_0)}e^{-i\omega_m t}\\ &+\frac{\beta}{2}T_0T_{+1}e^{i(\phi_0-\phi_{+1})}e^{i\omega_m t} + e^{-i(\phi_0-\phi_{+1})}e^{-i\omega_m t})\,.\end{aligned}$$

Entwickelt man $e^{i(\phi_0-\phi_{\pm 1})}$, vereinfacht sich der Ausdruck zu

$$\langle I(t)\rangle \propto T_0^2\beta T_0\Delta T\cos\omega_m t + \beta T_0^2\Delta\phi\sin\omega_m t \tag{2.24}$$

wobei $\Delta T = T_{+1} - T_{-1}$ und $\Delta\phi = (\phi_{+1} - \phi_0) + (\phi_{-1} - \phi_0)$. Das Signal $U_{PD}(t) \propto I(t)$ wird jetzt mit dem Modulationssignal $U_{Mod}(t) \propto \omega_m(t)$ elektronisch gemischt. Dies entspricht einer Multiplikation der Signale, und der Mischerausgang ist daher

$$\begin{aligned}U(t) &\propto U_{PD}(t)\cdot U_{Mod}(t)\\ &\propto [-\Delta T\beta\cos(\omega_m t) + \Delta\phi\beta\sin(\omega_m t)]\cdot\cos(\omega_m t+\varphi)\\ &= \beta\left[-\frac{1}{2}\Delta T(\cos\varphi + \cos(2\omega_m t+\varphi)) + \frac{1}{2}\Delta\phi(\sin\varphi - \sin(2\omega_m t+\varphi))\right],\end{aligned}$$

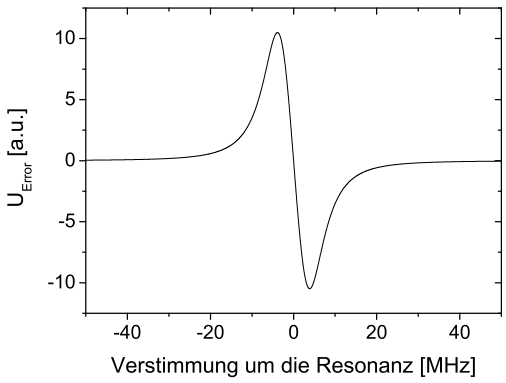

Abbildung 2.15: *Simulation des Fehlersignals der FMS.*

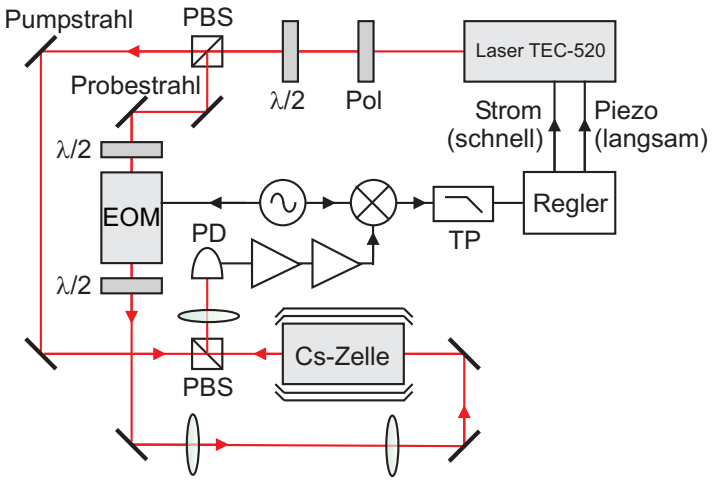

Abbildung 2.16: *Stabilisierung des Lasers mittels FMS auf den Cäsium-D1-Übergang. Die Cäsiumzelle befindet sich in einem zweilagigen magnetischen Schild und wird von Pump- und Probestrahl gegenläufig durchlaufen. Der Probestrahl wird mittels eines EOM phasenmoduliert und hinter der Zelle detektiert. Das Signal wird verstärkt, heruntergemischt, Tiefpass-gefiltert und dient anschließend zur Regelung der emittierten Wellenlänge über den Piezo- (PZT) und Strompfad (PS).*

mit einer Phasenverschiebung φ des Modulationssignals. Es folgt ein Tiefpass zur Filterung der hochfrequenten Anteile und als Fehlersignal $U_{Error}(t)$ ergibt sich:

$$U_{Error}(t) \propto \beta \left[-\frac{1}{2}\Delta T \cos\varphi + \frac{1}{2}\Delta\phi \sin\varphi \right] . \tag{2.25}$$

Das Fehlersignal ist nicht mehr zeitabhängig und für $\varphi = 90°$ bleibt der erste Term übrig, welcher der Absorption der beiden Seitenbänder direkt proportional ist (Abbildung 2.15). Der experimentelle Aufbau der FMS zur Stabilisierung des Lasers ist in Abbildung 2.16 gezeigt. Zunächst wird der Laser mit einer Halbwellenplatte (HWP) und einem Polarisationsstrahlteiler (PBS) in Pump- und Probestrahl aufgespalten, wobei durch die Stellung der Halbwellenplatte die Aufteilung der Leistung bestimmt wird. Die Phasenmodulation des Probestrahls erfolgt anschließend mittels eines EOM bei einer Modulationsfrequenz $f_{Mod} = \omega_m/2\pi \approx 7,3$ MHz. Die Frequenz wird mit einem Frequenzgenerator erzeugt und mit mehreren Verstärkern auf die notwendige Spannung von 300 V_{pp} verstärkt.
Innerhalb einer Cäsiumzelle werden Pump- und Probestrahl nun gegenläufig überlagert. Die beiden Strahlen sind orthogonal zueinander polarisiert, und der Probestrahl kann daher nach der Zelle mit einem weiteren PBS vom Pumpstrahl getrennt und detektiert werden. Die Cäsiumzelle ist eine für 894 nm AR-beschichtete evakuierte Glaszelle und enthält 99,99% isotopenreines ^{133}Cs. Sie ist 7,5 cm lang und zur magnetischen Abschirmung

von einem zweilagigen μ-Metall-Schild umgeben.
Das elektronische Ausgangssignal des Detektors wird über zwei Verstärker (Mini-Circuits ZFL-500LN) um 40 dB verstärkt und mit einem Mischer (Mini-Circuits ZAD-6) mit dem phasenverschobenen Modulationssignal der Frequenz f_{Mod} gemischt. Anschließend wird das gemischte Signal mit einem 1,9 MHz Tiefpass (Mini-Circuits BLP-1.9) gefiltert. Mit dem so gewonnenen Fehlersignal erfolgt die Regelung der Laserwellenlänge über einen schnellen Strompfad (PS) und einen langsamen Pfad (PZT), der den Laserresonator modifiziert.

2.2.2 Erzeugung kurzer Pulse

Die Amplitudenmodulation zur Erzeugung kurzer Pulse für die Quantenkryptographie erfolgt gemäß Abbildung 2.17. Zur Modulation der Amplitude wird ein EOM der Firma New Focus (#4102-VIS) eingesetzt. Der EOM hat eine Kapazität von 10 pF. Er besteht aus zwei MgO:$LiNbO_3$-Kristallen, die so angeordnet sind, dass thermisch induzierte Doppelbrechung kompensiert wird. Die Kristalle sind um $\pm 45°$ gedreht, so dass beim Anlegen einer Spannung die Polarisation von horizontal oder vertikal polarisiertem Licht gedreht wird. Zwischen zwei gekreuzten Polarisatoren erhält man für die Intensität am Ausgang

$$I_{out} = I_{in} \sin^2 \left(\frac{V_{in}}{V_\pi} \cdot \frac{\pi}{2} + \varphi_0 \right) , \tag{2.26}$$

wobei I_{in} die Eingangsintensität, φ_0 ein Phasenoffset, V_{in} die angelegte Spannung und V_π die Halbwellenspannung ist. Bei der Halbwellenspannung erfolgt eine relative Phasenverschiebung um π, also z.B. von horizontal nach vertikal. Bei 894 nm beträgt sie für den verwendeten EOM ≈ 280 V. Der EOM wird allerdings zweifach durchlaufen, so dass nur eine Halbwellenspannung von $V_\pi \approx 138$ V notwendig ist. Der PBS vor dem EOM dient also zugleich als Eingangs- wie Ausgangspolarisator und die Amplitude kann entsprechend moduliert werden. Mit diesem Aufbau wurde eine Amplitudenmodulation von 1:50 erreicht. Der EOM-Treiber wurde in der Arbeitsgruppe entwickelt und ist für einen Bereich ± 80 V ausgelegt, entsprechend einer maximalen Differenz von 160 V. Er hat im Bereich DC–4 MHz eine konstante Transferfunktion. Die Steuerspannung V_{in} wird von einem Stanford Research System DS345 geliefert. Für die Erzeugung von Pulsen nutzt man die Programmierbarkeit der DS345 Funktionsgeneratoren. Wellenformen aus bis zu 16.300 Punkten können in den Funktionsgenerator geladen werden. Die maximale Abtastrate beträgt 40 MHz. Über ein LabVIEW Programm können so beliebige Funktionen als Wellenform und damit als Amplitudenmodulation ausgegeben werden. Dies wurde genutzt, um den Signallaser mit einem Gauß-förmigen Puls zu modulieren. Das Teleskop hinter dem EOM dient der Strahlformung vor der Einkopplung in eine optische Faser, mit der die erzeugten Pulse zu den Interferometern geleitet werden.

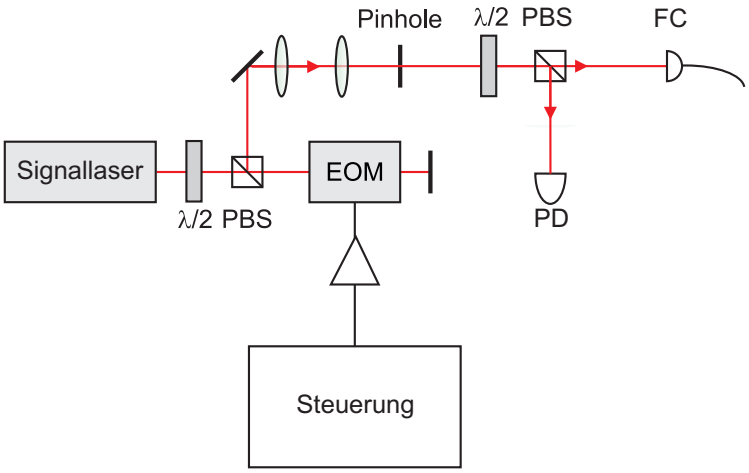

Abbildung 2.17: *Aufbau zur Erzeugung kurzer Pulse. Die Amplitudenmodulation wird mit einem EOM realisiert. Die Pulse werden nach der Einkopplung in eine optische Faser (Faserkoppler FC) zu den Interferometern geführt. Der Photodetektor PD dient der Kontrolle der Pulsform.*

2.3 Detektion

Es stehen unterschiedliche Detektoren zur Verfügung. Zur Demonstration der Funktionalität der Interferometer werden zunächst Gauß-Pulse verwendet, deren Erzeugung im letzten Abschnitt beschrieben wurde. Die Detektion erfolgt mit einem in der Arbeitsgruppe entwickelten Detektor für hochfrequente Signale. Er basiert auf einer FND-100 Si-PIN-Photodiode der Firma Perkin Elmar. Die Diode ist mit einer Vorspannungsquelle versehen und an einen Transimpedanzverstärker (Phillips SA5211D, 180 MHz Bandbreite) angeschlossen. Das Ausgangssignal wird mit einen Intersil EL5175 „Differential Line Receiver“ in ein mit 50 Ω abgeschlossenes Signal umgewandelt. Für die Detektion der Referenzstrahlen in den beiden Interferometern kommen zwei Detektoren zum Einsatz, die ebenfalls eine FND-100 Photodiode enthalten. Hier wird allerdings ein OP27 Operationsverstärker nachgeschaltet, und es steht ein DC-Ausgang zur Verfügung, mit dem absolute Spannungen und langsame Signale < 1 MHz gemessen werden können.
Der spätere Betrieb mit den Einzelphotonen des OPO bzw. die Detektion der Photonen abgeschwächter Pulse erfordert den Einsatz von Lawinenphotodioden (4SPCM-AQR-14, Perkin Elmer). PIN-Photodioden sind zwar aufgrund ihrer dicken I-Schicht insensitiver gegen Temperaturänderungen, aber weniger empfindlich als eine Lawinenphotodiode. Eine solche Diode besteht aus einem Si-pn-Übergang. Sie wird mit einem großen Vorwiderstand in Sperrrichtung betrieben. Wird ein Photon absorbiert, so entsteht ein Elektron-Loch-Paar. Durch die hohe Feldstärke kommt es durch Stoßionisation zu einem Lawinenprozess (Avalancheeffekt), so dass ein messbarer Strom entsteht. Solange der Strom anhält, kann kein weiteres Photon gemessen werden. Das Verringern der Vorspannung unter die Durch-

bruchspannung wird elektronisch geregelt. Ist die Lawine beendet, so wird die Spannung wieder erhöht, und die Diode ist in der Lage ein neues Photon zu detektieren. Diese Totzeit beträgt bei dem verwendeten Modell 50 ns [Gmb]. Während der Detektion eines Photons besteht eine erhöhte Wahrscheinlichkeit, dass ein weiterer Puls ausgelöst wird. Werden einige Lawinenelektronen im Kristall, z.B. an Defekten, gefangen, so können diese später eine weitere Lawine auslösen. Man bezeichnet das als Nachpulswahrscheinlichkeit, die für das vorliegende Modell 0,5 % beträgt. Bei der verwendeten Wellenlänge von 894 nm liegt die Quanteneffizienz bei $\eta \sim 35\%$. Die Dunkelzählrate beträgt ungefähr 100 cps. Der Strahl wird mit einer Linse ($f = 50$ mm) auf die Detektoroberfläche mit einem Durchmesser von 180 μm fokussiert. Die Linse ist auf einem linearen Verschiebetisch montiert und in einem Halter mit Mikrometerschrauben für die Justage in x- und y-Richtung befestigt. Durch ein äußeres Signal ist es möglich, die APD nur für ein bestimmtes Zeitfenster detektionsbereit zu halten (*gating*). Dies ist für den Betrieb der Interferometer wichtig, um so nur das mittlere Maximum interferierender Photonen für die Detektion zu selektieren.

2.4 Aufbau zur Realisierung des BB84-Protokolls

Der Aufbau der beiden Michelson-Interferometer schafft die Voraussetzungen für die Demonstration phasenkodierter Quantenkryptographie. Die Umsetzung des BB84-Protokolls erfordert die genaue Ansteuerung der einzelnen Komponenten und die richtige Verarbeitung der Signale. Wie in Abschnitt 1.2.2 erläutert, werden die Bitwerte 0 und 1 gemäß

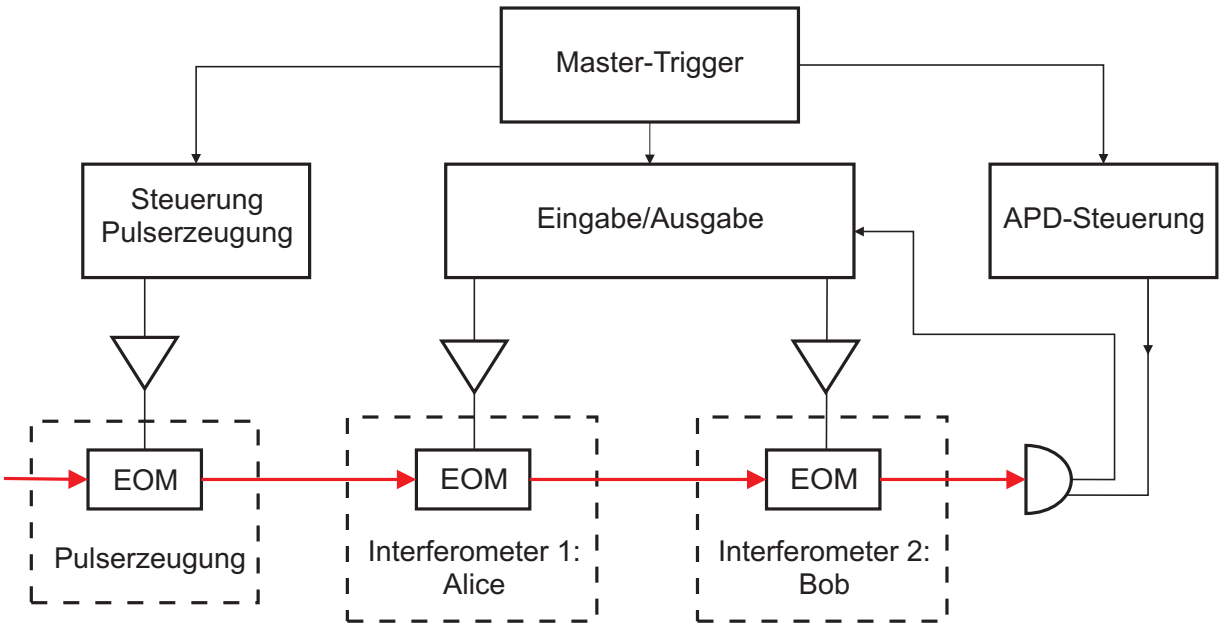

Abbildung 2.18: *Steuerungsschema für die Realisierung des BB84-Protokolls.*

dem phasenkodierten BB84-Protokoll z.B. durch die vier relativen Phasenverschiebungen $0, \frac{\pi}{2}, \pi, \frac{3}{2}\pi$ dargestellt. Realisiert wird dieses Schema durch die EOM in den beiden Interferometern. Die Umsetzung des Protokolls erfordert die Ansteuerung der EOM mit den entsprechenden Spannungswerten. Nach der Detektion müssen die Messwerte so verarbeitet werden, dass nach dem Vergleich der Basen ein gemeinsamer Schlüssel generiert werden kann. Abbildung 2.18 gibt eine Übersicht über das Steuerungsschema. Wichtig ist eine synchronisierte Eingabe und Ausgabe der Signale. Ein Mastertrigger gibt dafür die Zeitbasis für alle Schritte des Protokolls vor. Das Triggersignal initialisiert die Pulserzeugung und die Ausgabe der Spannungswerte an die EOM in den Interferometern. Wird mit der APD detektiert, so ist ein Steuerungssignal (*gating*) notwendig, um die interferierenden Photonen zu selektieren. Dieses Signal wird ebenfalls durch das Triggersignal initialisiert.
Für die Steuerung wurde ein Programm in LabVIEW geschrieben. Der in die Software integrierte Taktgeber wurde als Mastertrigger benutzt. Das Programm steuert sowohl die zufällige Ausgabe der vier Spannungswerte für die jeweiligen relativen Phasenverschiebungen, als auch das Einlesen der entsprechenden Detektionsereignisse und die Weiterverarbeitung für die Schlüsselgeneration. Die Ein- und Ausgabe der entsprechenden Signale erfolgt mit einer PCI-6014-Karte von National Instruments.
Der zeitliche Verlauf der Signale ist in Abbildung 2.19 dargestellt. Jeder Schreib-und Lesevorgang beginnt mit einem Triggerpuls. Anschließend werden die EOM in Interferometer 1 und 2 auf die entsprechenden zufälligen Spannungswerte gesetzt. Dazu werden die EOM-Treiber mit Spannungen aus dem Bereich ± 5 V angesteuert und auf Werte im Bereich ± 200 V verstärkt. Das Triggersignal löst außerdem die Pulserzeugung aus. Nach den beiden Interferometern erhält man dann die drei möglichen Maxima (siehe Abschnitt 1.3). Interferierende Ereignisse treten nur im mittleren Maximum auf. Die APD wird entspre-

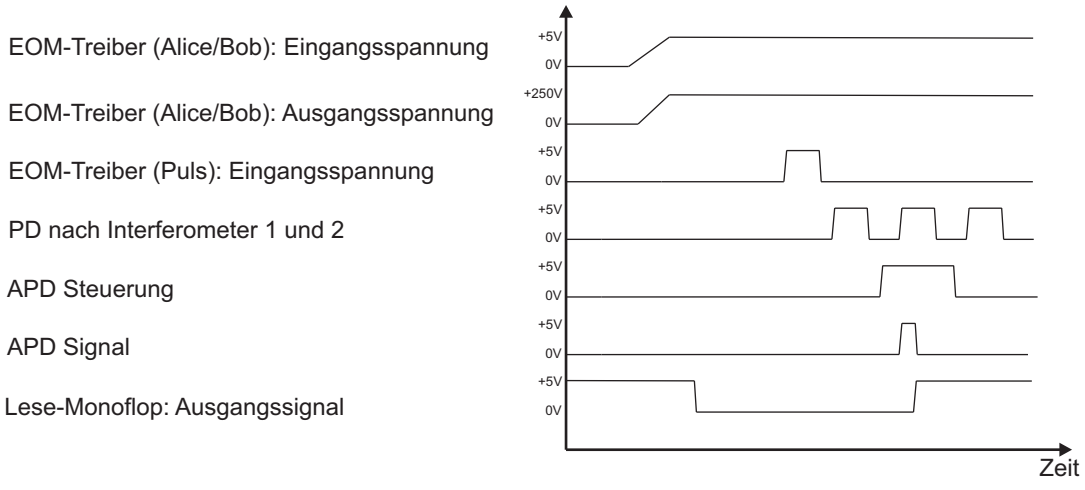

Abbildung 2.19: *Schema des zeitlichen Verlaufs der Steuerungssignale.*

chend in diesem Zeitbereich detektionsbereit gehalten. Der APD-Ausgangspuls ist 35 ns lang und dient als Eingang für einen Monoflop, der daraufhin in den oberen Schaltzustand (+5 V) wechselt. Die Dauer dieses Zustands wird so eingestellt, dass der Wert von der Karte eingelesen werden kann. Nachdem der nächste Triggerpuls des Master-Trigger die Signalfolge von neuem startet, geht der Monoflop wieder in den Grundzustand über und ist bereit für ein erneutes Detektionsereignis.

Kapitel 3

Messungen

In diesem Kapitel werden Messungen zur Charakterisierung und Test der Funktionalität der Interferometer vorgestellt. Zunächst werden die mit dem Aufbau zur Pulserzeugung generierten Pulse dargestellt. Anschließend erfolgt die Charakterisierung der Interferometer. Entscheidend für die Qualität ist eine gute Visibilität sowohl des Signalstrahls als auch des Referenzstrahls. Die Stabilisierung mit Hilfe des Referenzstrahls wird danach erläutert. Im nächsten Abschnitt folgen die Messungen im Betrieb mit klassischen Pulsen, die zeigen, dass die Interferometer in der Tat in der Lage sind, schmalbandige Photonen nach dem *time-bin*-Schema zu kodieren. Mit den Interferometern soll phasenkodierte Quantenkryptographie nach dem BB84-Protokoll demonstriert werden. Dazu wird schließlich das Steuerungsschema für die Ansteuerung der einzelnen Komponenten gezeigt.

3.1 Pulserzeugung

Die Modulationseigenschaften eines EOM hängen stark vom Strahlweg durch den Kristall ab. Läuft der Strahl nicht parallel zur Längsachse des Kristalls, so verringert sich die Modulationstiefe. Da der Strahl in diesem Aufbau den EOM zweimal durchläuft, ist die optimale Strahljustage umso wichtiger. Zunächst wird der Strahlüberlapp von hin- und rücklaufendem Strahl mit einem Spiegel vor dem EOM und dem Spiegel dahinter, der den Strahl zurück in den Kristall reflektiert, optimiert. Die Steuerung des EOM erfolgt mit einem Treiber, an den ein DS345-Funktionsgenerator angeschlossen ist. Der EOM wird so zunächst mit einem Rechtecksignal angesteuert und das modulierte Licht im Detektor (PD, siehe Abbildung 2.17) beobachtet. Mit einem 5-Achsen-Verschiebetisch wird der EOM nachjustiert und das Extinktionsverhältnis anhand des Detektorsignals optimiert.
Der DS345-Funktionsgenerator ist programmierbar mit Wellenformen aus bis zu 16.300 Punkten und einer maximalen Abtastrate von 40 MHz. Über die serielle Schnittstelle des Geräts wird so eine Pulsform geladen (siehe Abbildung 3.1).
Dieses Signal geht an den EOM-Treiber. Das Eingangssignal des Treibers wurde so optimiert, dass im Detektor der entsprechende Gauß-Puls gemessen werden konnte. Zunächst

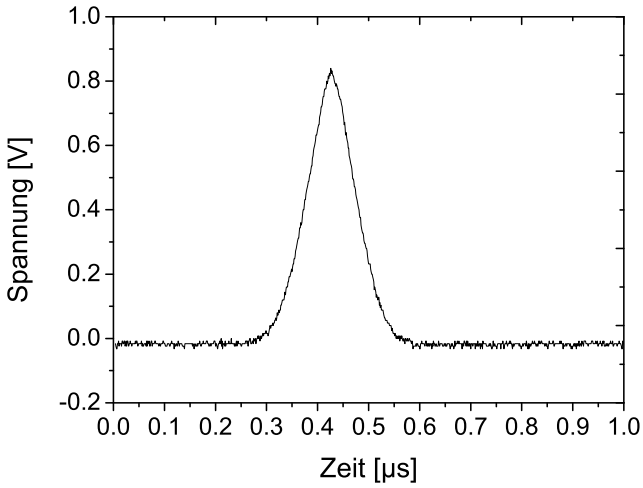

Abbildung 3.1: *Eingangssignal des EOM-Treiber für die Pulserzeugung*

wurde bei der programmierten Wellenform explizit die Transferfunktion des EOM (Gleichung 2.26) beachtet. Das Treibereingangssignal ist also von der Form

$$V_{in} = \arcsin\left(\sqrt{e^{\frac{(t-t_0)^2}{\sigma^2}}}\right).$$

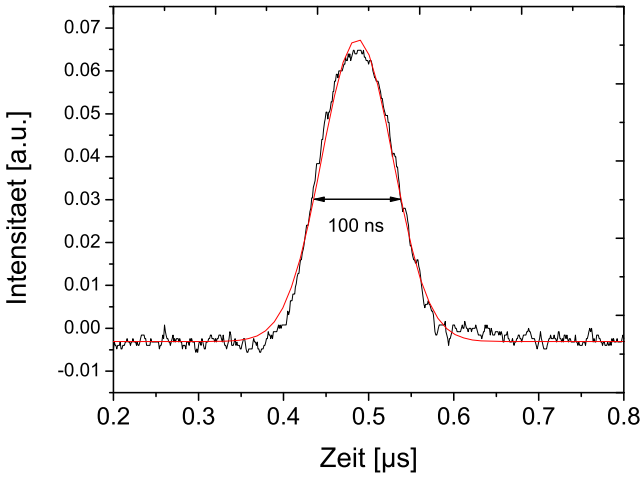

Abbildung 3.2: *Gemessener Intensitätsverlauf nach dem EOM. Ein Gauß-Puls mit einer Halbwertsbreite von ca. 100 ns.*

Eine weitere Optimierung ist dann über das Einstellen von Amplitude und Offset am Funktionsgenerator möglich, so dass man die in Abbildung 3.2 gemessene Pulsform erhält. Es ist ein Gauß-Puls mit einer Halbwertsbreite (FWHM) von ungefähr 100 ns. Die leichte Asymmetrie des Pulses ist durch Nichtlinearitäten des Treibers zu erklären.

3.2 Visibilität der Interferometer

Die Funktionalität der Interferometer wird durch den Kontrast des Interferenzsignals bestimmt. Für die Erzeugung eines Interferenzsignals wird das Piezoelement am Spiegel im kurzen Arm der Interferometer mit einer Dreiecksspannung angesteuert. Diese wird durch die Lock-Box erzeugt, die einen internen Dreiecksgenerator enthält und eine Ausgangsspannung von ±10 V liefert. Das Piezoelement ist das Modell PSt 150/10x10/20 der Firma Piezomechanik und hat einen maximalen Hub von 28 μm im Betrieb von -30 bis 150 V. Bei einer Ansteuerung mit ±10V erhält man damit einen Hub von ungefähr 3 μm. Die Messung des Interferenzsignals des Signalstrahls erfolgt im *cw*-Betrieb des Lasers. Sowohl der Signalstrahl als auch der Referenzstrahl für die Regelung müssen einen guten Kontrast des Interferenzsignals zeigen. Zunächst wird der Referenzstrahl in das Interferometer eingekoppelt (siehe Abbildung 2.6). Der Strahlengang wird so justiert, dass eine gute Einkopplung in die 50 m lange Faser gewährleistet ist. Anschließend wird der Signalstrahl mit dem Referenzstrahl überlagert, um auch hier eine gute Einkopplung in die 50 m lange Faser zu ermöglichen. Im kurzen Arm durchlaufen beide Strahlen den Calcitkristall und danach passiert nur der Signalstrahl den EOM. Die Messung der Interferenz erfolgt

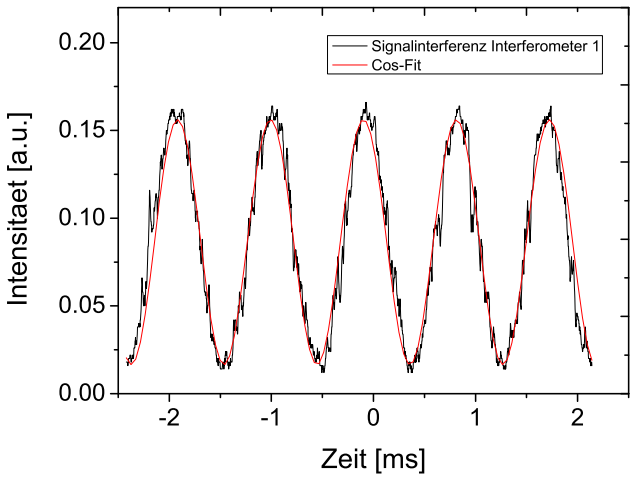

Abbildung 3.3: *Interferenzsignal des Signalstrahls im Interferometer 1. Die Visibilität beträgt 0,81±0,01*

mit zwei getrennten Detektoren. Am zweiten PBS wird der Referenzstrahl abgebeugt und mit einem langsamen Detektor, der an der Gehäusewand der Interferometer-Box befestigt ist, gemessen. Der Signalstrahl wird ausgekoppelt und mit einem separaten Detektor aufgenommen. Das Interferenzsignal beider Strahlen lässt sich nun über den justierbaren Endspiegel des kurzen Arms einstellen. Das Interferenzsignal des Signalstrahls wird anschließend optimiert. Eine Verschlechterung der Interferenz für den Referenzstrahl wird dabei in Kauf genommen, solange es für die Regelung ausreichend ist.
In Abbildung 3.3 ist das Interferenzsignal des Signalstrahls im ersten Interferometer dargestellt. Die Visibilität (Gleichung 2.10) ergibt sich zu 0,81±0,01. Betrachtet man als nächstes das Interferenzsignal des Referenzstrahls, so fällt die deutlich schlechtere Visibilität von 0,180±0,001 auf (Abbildung 3.4). Wie gerade erwähnt, ist eine etwas schlechtere Interferenz im Referenzstrahl kein Problem, solange ein gutes Fehlersignal erzeugt wird. Bei stark ausgeprägtem Interferenzsignal des Referenzstrahls in beiden Interferometern kam es zu starken Rückkopplungen in die Laserdiode. Frequenzschwankungen und starke Driften ließen dann kein sauberes Interferenzsignal zu. Dies ist als Störung in dem Interferenzsignal in Abbildung 3.5 zu erkennen. Durch den Vergleich mit dem Signalstrahl war offensichtlich klar, dass die Störungen nicht durch eines der optischen Elemente induziert wurde. Eine provisorische Lösung des Problems konnte zunächst durch absichtliche Verschlechterung des Interferenzsignals gefunden werden. Bei schwächer ausgeprägter Interferenz stabilisierte sich das Referenzsignal. Langsame Driften konnten jedoch nicht vollständig beseitigt werden. Für die Zukunft ist ein weiterer Faraday-Isolator zur Reduktion von Rückreflektionen geplant sowie ein separater Aufbau zur Stabilisierung des Referenzlasers. Momentan ist deshalb auch im zweiten Interferometer die Visibilität des

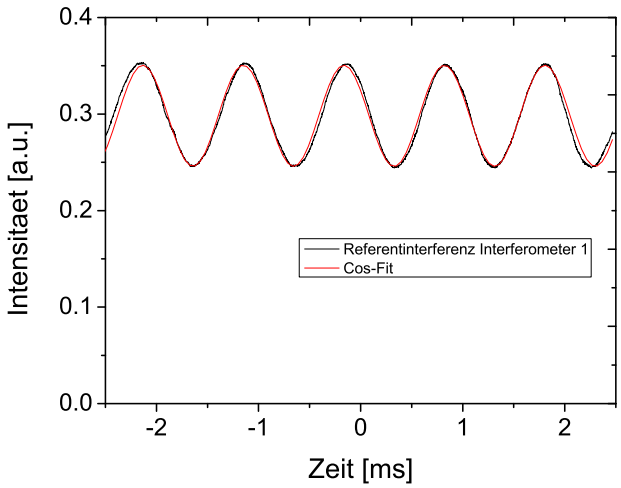

Abbildung 3.4: *Interferenzsignal des Referenzstzrahls im Interferometer 1. Die Visibilität ist 0,180±0,001.*

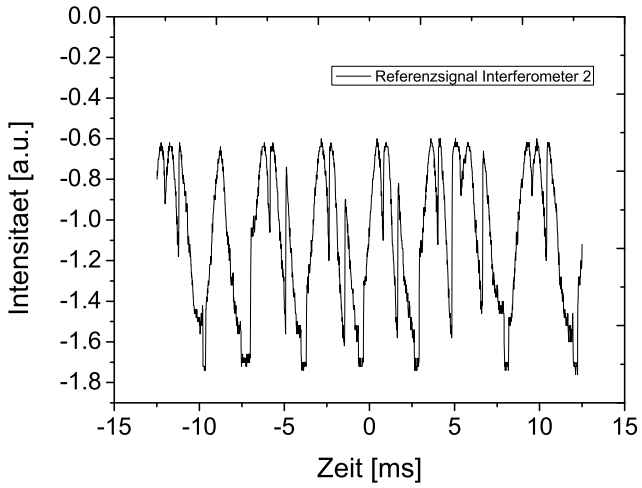

Abbildung 3.5: *Interferenzsignal des Referenzstrahls im zweiten Interferometer. Wegen Rückreflexen zur Laserdiode beobachtet man Sprünge im Interferenzsignal. Durch Verringerung der Visibilität konnte das Interferenzsignal stabilisiert werden.*

Referenzstrahls mit $V = 0,24 \pm 0,01$ beschränkt (Abbildung 3.7). Die Visibilität des Interferenzsignals des Signalstrahls liegt mit 0,84±0,01 im zweiten Interferometer in derselben Größenordnung wie im ersten Interferometer.

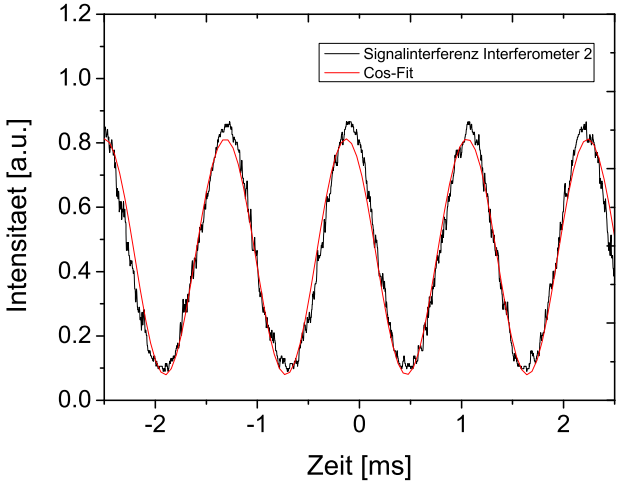

Abbildung 3.6: *Interferenzsignal des Signalstrahls im zweiten Interferometer. Die Visibilität beträgt 0,84±0,01*

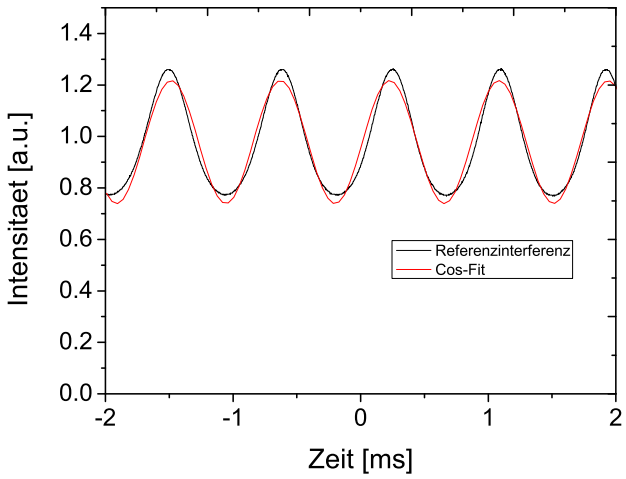

Abbildung 3.7: *Interferenzsignal des Referenzstrahls im zweiten Interferometer nach Reduktion der Visibilität, um Rückreflexe zu vermeiden. Die Visibilität des jetzt stabileren Signals (vergl. Abb. 3.5) beträgt 0,24±0.01.*

3.3 Interferometerstabilisierung

Für die Interferometerstabilisierung wird das Interferenzsignal des Referenzstrahls genutzt (Abbildung 3.8). Es dient als Eingangssignal für einen PI-Regler (Lock-Box) und liefert

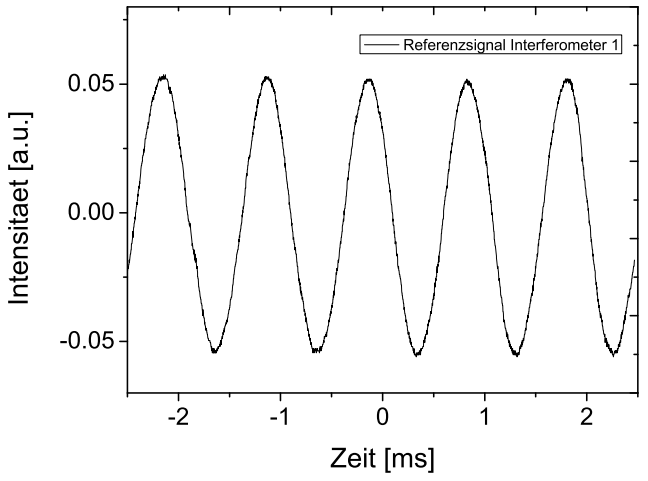

Abbildung 3.8: *Interferenzsignal des Referenzstrahls des ersten Interferometers als Fehlersignal für die Weglängenstabilisierung.*

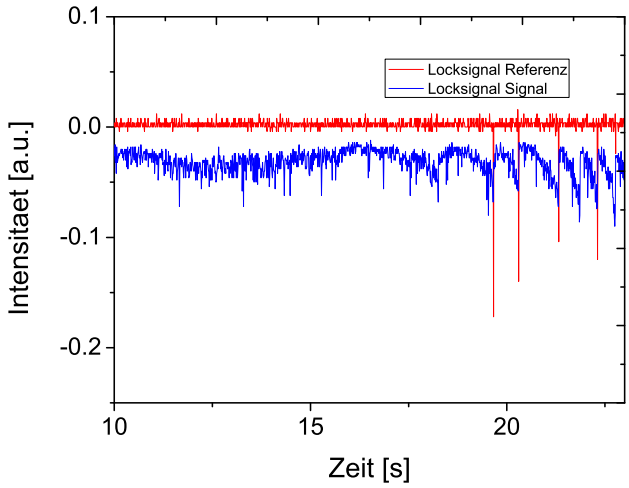

Abbildung 3.9: *Das erste Interferometer im gelockten Zustand.*

ein Fehlersignal. Ein Beispiel für ein Interferometer im gelockten Zustand gibt Abbildung 3.9. Auf kurzen Zeitskalen ist das Locksignal des Signalstrahls durchaus stabil im Vergleich zum Hub für eine $\pi/2$ Phasenverschiebung (siehe Abbildung 3.3). Die kurzzeitigen Störungen und die Driften der Frequenz von Signalstrahl und Referenzstrahl gegeneinander führen dazu, dass der Signalstrahl nach etwa 10s aus dem gelockten Zustand fällt. Trägt man die Schwankungen im Signal mit Hilfe der Transferfunktion des Interferome-

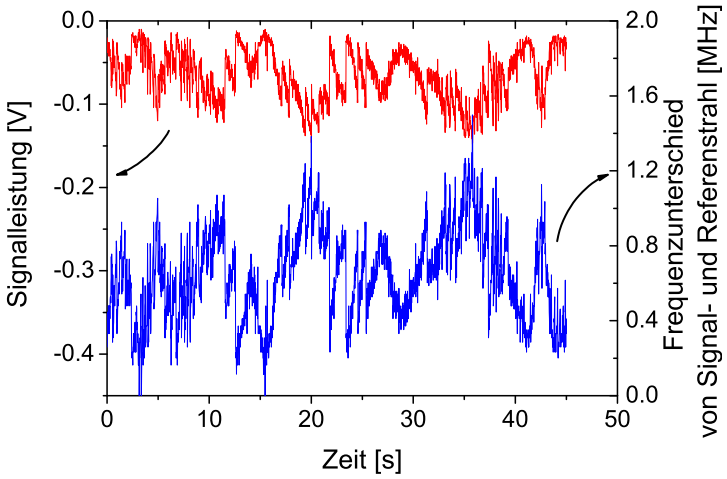

Abbildung 3.10: *Frequenzschwankungen (blau) zwischen Signal- und Referenzstrahl über die Zeit.*

ters als Frequenzschwankung auf, so sieht man direkt den gegenseitigen Drift der Laser in der Frequenz.

3.4 Betrieb der Interferometer mit klassischen Pulsen

Die Messung der Verzögerung der Pulse wurde zunächst für jedes Interferometer separat durchgeführt. Zuerst erfolgt die Einstellung für die Pulserzeugung wie im Abschnitt 3.1 erläutert. Anschließend wird das erste Interferometer stabilisiert und an dessen Ausgang mit einem schnellen Detektor die Pulsform aufgenommen. Abbildung 3.11 zeigt die gemessene Intensität am Ausgang des ersten Interferometers. Durch die Verzögerungsfaser entsteht ein Doppelpuls. Der zeitliche Abstand beträgt 482±2 ns und ist damit deutlich größer als die Dauer von ungefähr 100 ns der Eingangspulse. Die beiden Zeitfenster sind damit soweit getrennt, dass Photonen mit einer Kohärenzzeit in der Größenordnung von 100 ns zeitlich getrennt werden können. Bei einem Brechungsindex von 1,45 für Quarzglas entpricht das dem erwarteten Wert von 483 ns für die Verzögerung. Der zweite Puls hat eine geringere Intensität als der erste Puls. Dies begründet sich mit Verlusten bei der Einkopplung in die Verzögerungsfaser. Bei einer Einkopplungseffizienz von 0,55 entspricht dies den Intensitätsverhältnissen der beiden Pulse.
Die Messung am zweiten Interferometer ist analog zur Messung am ersten Interferometer. Die gemessene Intensität ist in Abbildung 3.12 dargestellt. Die Verzögerung beträgt hier

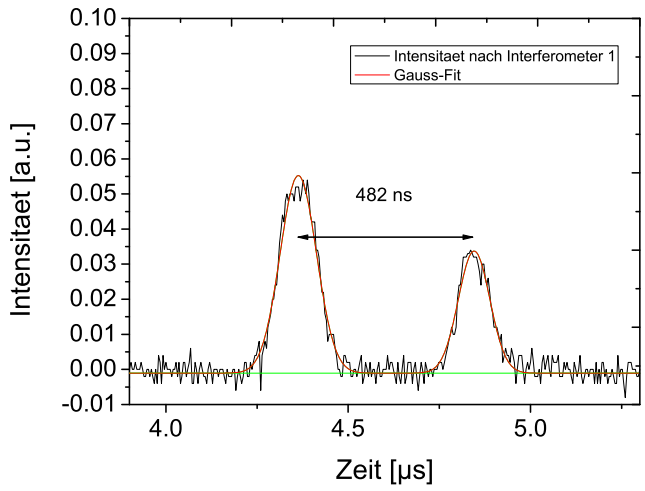

Abbildung 3.11: *Gemessene Intensität am Ausgang des ersten Interferometers bei einem gaußförmigen Eingangspuls. Die durch die Faser induzierte Verzögerung beträgt 485 ns. Die reduzierte Intensität des zweiten Pulses resultiert aus Verlusten bei der Einkopplung in die Verzögerungsfaser.*

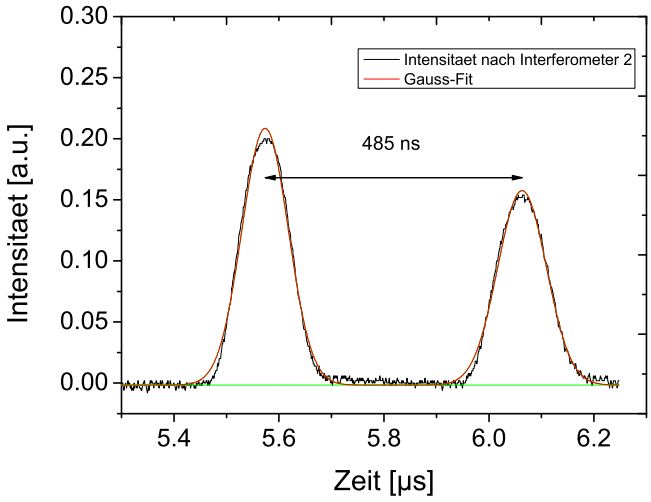

Abbildung 3.12: *Gemessene Intensität am Ausgang des zweiten Interferometers bei einem Gauß-förmigen Eingangspuls. Die Verzögerung beträgt 485 ns. Die reduzierte Intensität des zweiten Pulses resultiert aus Verlusten bei der Einkopplung in die Verzögerungsfaser.*

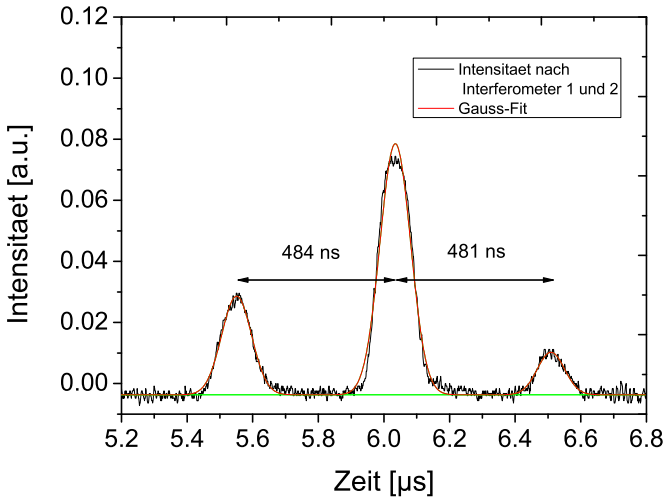

Abbildung 3.13: *Intensitätsverteilung nach der Durchquerung beider Interferometer. Das linke Maximum entspricht Photonen, die in beiden Interferometern den kurzen Arm durchlaufen haben. Das rechte Maximum entspricht Photonen, die beide langen Arme durchlaufen haben. Das mittlere Maximum entsteht durch die beiden interferierenden Wege kurz-lang und lang-kurz.*

485±2 ns. Das Verhältnis der Intensitäten der beiden Pulse beträgt hier 0,7 und entspricht damit der Einkopplung in die 50 m lange Faser.
Nun wird wird der Ausgang des ersten Interferometers mit dem Eingang des zweiten verbunden. Die Pulserzeugung ist wieder am ersten Interferometer angeschlossen. Am Detektor im Ausgang des zweiten Interferometers erhält man das Signal in Abbildung 3.13. Ganz deutlich sind drei Maxima zu erkennen, die zu den verschieden Wegen gehören, auf denen die Photonen die beiden Interferometer passieren. Das erste Maximum gehört zu dem Teil des Pulses, der in beiden Interferometern die kurzen Arme durchläuft, während im dritten Maximum der Puls die beiden Verzögerungsfasern durchquert hat. Die Teile des Pulses, die entweder zuerst den kurzen und dann den langen Arm oder erst den langen und anschließend den kurzen Arm der Interferometer durchquerten, interferieren im mittleren Maxima. Bei eingeschalteter Regelung der Armlängendiffernz der beiden Interferometer bleibt das mittlere Maximum stabil über einige Sekunden (siehe Abschnitt 3.3). Die zeitlichen Abstände betragen 484±2 ns bzw. 481±2 ns . Das dritte Maximum ist im Vergleich zum ersten Maximum reduziert, da hier zweimal Verluste bei der Einkopplung in die Verzögerungsfaser zu berücksichtigen sind. Im Idealfall perfekter Transmission ist das mittlere Maximum doppelt so hoch wie die Summe der beiden Maxima links und rechts. Das liegt daran, dass die nichtinterferierenden Maxima links und rechts zur Hälfte auch in den ungenutzten zweiten Ausgang des Inteferometers gebeugt werden.

3.5 Steuerungsschema für das BB84-Protokoll

Das mittlere Maximum in Abbildung 3.13 entsteht durch die interferierenden Wege *kurz-lang* und *lang-kurz*. Je nach Phasenverschiebung herrscht so konstruktive oder destruktive Interferenz im mittleren Zeitfenster am Ausgang des zweiten Interferometers. Das ist die Voraussetzung für die Implementierung der phasenkodierten Quantenkryptographie (siehe Abschnitt 1.3).
Als ein weiterer Schritt wurde die Ansteuerungselektronik für die Implementierung des BB84-Protokolls geschaffen, sowie das automatisierte Ein-und Auslesen und die Weiterverarbeitung der Daten realisiert. Wichtig ist dabei der exakt synchronisierte Ablauf sämtlicher Steuersignale. In Abbildung 3.14 ist der zeitliche Verlauf der Signale dargestellt. Zum Vergleich ist nochmal das Schema des Zeitverlaufs dargestellt (siehe auch Abbildung 2.19). Der Triggerpuls hat eine Anstiegszeit von 8 ns und initialisiert den Schreib- und Lesevorgang. Nach etwa 2 μs liegen an den EOM in den beiden Interferometern die entsprechenden Spanungswerten. Das LabVIEW-Programm gibt dabei über die PCI-Karte vier Werte im Bereich $\pm 0,5$ V aus. Diese werden vorverstärkt, um die Anstiegszeit zu verkürzen und an die EOM-Treiber gegeben. Diese verstärken die Spannung in einem Bereich ±200 V. Gezeigt ist die Ausgangsspannung des EOM-Treibers im ersten Interferometer, wobei nur der Absolutwert (hier von 0–200 V) gemessen wurde. Der Trigger startet auch die Pulserzeugung. Die Wellenform ist dabei so gewählt, dass die Pulserzeugung erst nach der

Initialisierung der EOM beginnt, um zu garantieren, dass bereits eine Spannung an den EOM anliegt, wenn der Puls die Interferometer passiert. Am Ausgang der Interferometer entsteht die bereits diskutierte Pulsform mit den drei Maxima. Nur das mittlere Maxima ist von Bedeutung, deshalb wird die APD mit einem Rechteckpuls angesteuert, der um das mittlere Maxima konzentriert ist. Der Rechteckpuls hat eine Breite von 300 ns und erfasst so die Detektionszeit. Das Einlesen in die Karte erfolgt nicht direkt, sondern mit einem zusätzlichen Monoflop. Simuliert wurde das Auslösen des Monoflop durch einen simulierten APD-Puls. Dieser hat eine Breite von 35 ns. Der Monoflop bleibt im oberen Zustand, bis nach dem nächsten Triggerpuls der Wert ausgelesen wird. Wie im Graphen zu sehen, geht der Monoflop dann wieder in den Grundzustand über. Die Zeit wird entsprechend der Triggerrate angepasst.
Das Limit der Triggerrate und damit die maximale Übertragungsrate von Qubits ist derzeit 30 kHz. Das ist bedingt durch die PCI-6014-Karte als Ein- und Ausgabemodul des LabVIEW-Programms. Die Software muss die folgenden Aufgaben erfüllen:

- Erzeugung des Zufallsschlüssels für die Ansteuerung der EOM,
- Kalibration der Phase und Ein-/Ausgabe der entsprechenden Spannungswerte,
- Vergleich der Basen und Schlüsselerzeugung.

Ein letztes verbleibendes Problem, bevor mit dem Interferometerpaar das BB84 Protokoll implementiert werden kann ist die Phasenkalibration. Diese Problem lässt sich jedoch mit einem verbesserten Schutz des Stabilisierungslasers vor Rückreflexen lösen wie in Abschnitt 3.2 geschildert.

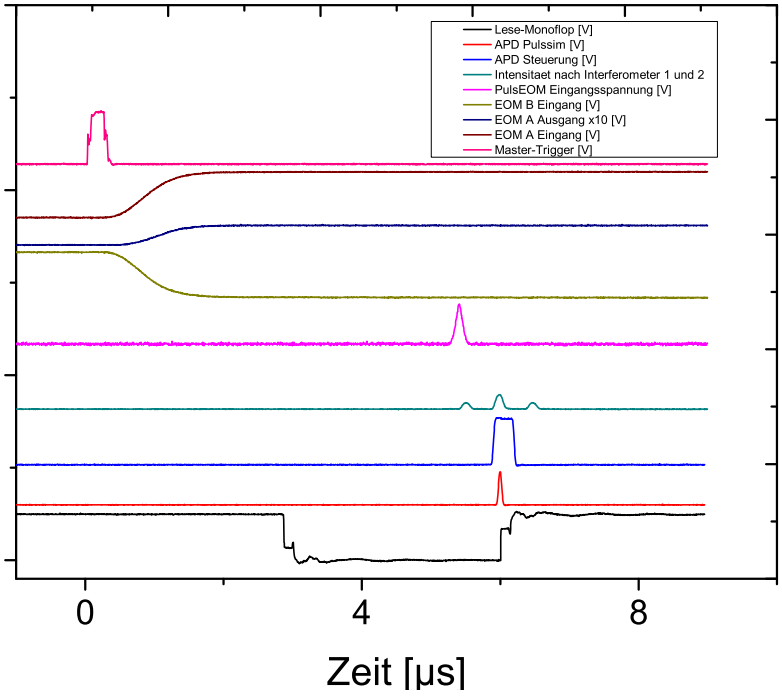

Abbildung 3.14: *Verlauf der Steuersignale für das BB84-Protokoll mit der Pulsverteilung nach den Interferometern.*

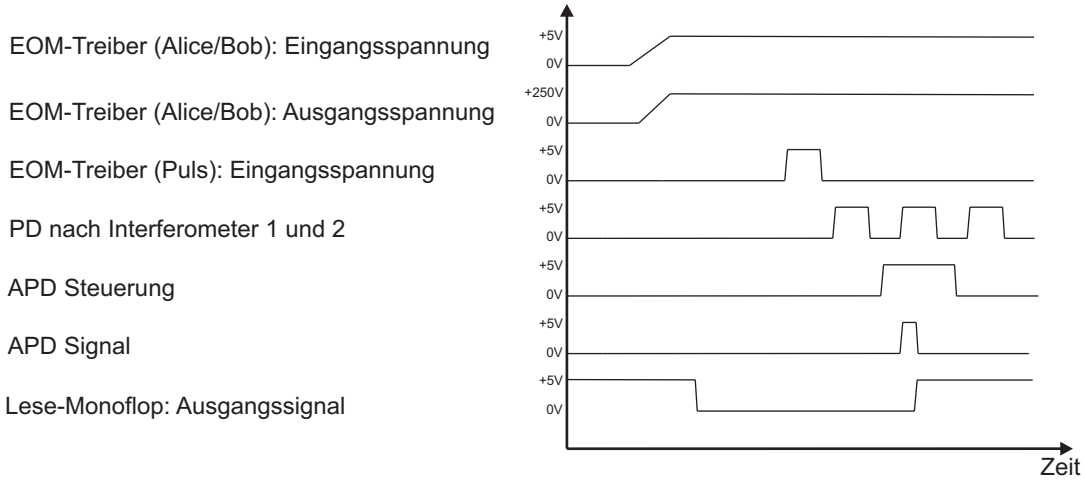

Abbildung 3.15: *Schema des zeitlichen Verlaufs der Steuerungssignale.*

Kapitel 4

Diskussion der Ergebnisse

Gemessen an den Anforderungen für die erfolgreiche Kodierung schmalbandiger Photonen nach dem *time-bin*-Schema ist dies mit dem Aufbau der beiden Michelson-Interferometer gelungen. Eine erfolgreiche *time-bin*-Kodierung ist an die Bedingung geknüpft, dass die Differenz der möglichen Ankunftszeiten (*time-bins*) größer als die Kohärenzzeit der verwendeten Photonen ist. Dementsprechend ist der Wegunterschied der beiden Arme eines unsymmetrischen Interferometers zu wählen. Der realisierte Aufbau ist für Photonen mit einer spektralen Breite in der Größenordnung von 10 MHz ausgelegt. Daraus ergibt sich eine Kohärenzzeit in der Größenordnung von 100 ns. Der Betrieb mit Gauß-Pulsen mit einer Pulsdauer von 100 ns hat gezeigt, dass die beiden Zeitfenster im Bereich des erwarteten Werts von 483 ns voneinander getrennt sind. Das ist deutlich größer als die Pulsdauer des Eingangspulses und damit ist eine Kodierung nach diskreten Ankunftszeiten möglich. Die Realisierung einer solchen Zeitdifferenz erfolgte mit einer optischen Faser von 50 m Länge. Das Signal nach beiden Interferometern zeigt die erwarteten drei Maxima, die jeweils einen Abstand von ungefähr 483 ns haben. Sie stellen die unterschiedlichen Wege dar, die die Photonen bei der Durchquerung der Interferometer nehmen können. Der Teil des Pulses, der beide kurze Arme durchquert, gelangt als erstes zum Detektor. Entsprechend benötigt die Passage der langen Arme die längste Zeit. Das mittlere Maximum entspricht den interferierenden Wegen *kurz-lang* und *lang-kurz*, da sie die gleiche Länge haben. Das dritte Maximum ist in der Intensität reduziert, da hier die Einkopplungsverluste in die Verzögerungsfaser zu berücksichtigen sind. Das Verhältnis der Intensitäten der beiden äußeren Maxima beträgt 0,4 und erklärt sich unter der Annahme einer Einkoppeleffizienz von 0,55 bzw. 0,7.
Die beiden Interferomter dienen als Sende- und Empfangseinheit, wobei das erste Interferomter der Kodierung von *time-bin*-Qubits und das zweite Interferometer zur Dekodierung dient. Die Interferenz im mittleren Maximum wird dabei zur Übertragung phasenkodierter Information genutzt. Mit den in die Interferometer integrierten EOM ist es möglich die relative Phasenverschiebung direkt zu steuern und anhand der destruktiven oder konstruktiven Interferenz im mittleren Zeitfenster die über die Phase kodierte In-

formation auszulesen. Ein wichtiges Protokoll für den sicheren Schlüsselaustausch ist das BB84-Protokoll. Für die Implementierung dieses Protokolls wurden in dieser Arbeit die technischen Vorausetzungen geschaffen und das komplette Steuerungsschema realisiert.
Eine wichtige Bedingung für die Verwendung der Interferometer für die phasenkodierte Quantenkryptographie ist die relative Längenstabilität der Interferometerarme. Für diesen Zweck wurden die Interferometer in kompakter Form realisiert. Dies ermöglicht die Minimierung von Temperatudrifts der Umgebung. Außerdem sind die wichtigsten Elemente temperaturstabilisiert. Dies sind die Grundplatte, der Calcit-Kristall für die Trennung von Signal- und Referenzstrahl und die Verzögerungsfaser. Neben der passiven Stabilisierung über die Temperatur ist die Möglichkeit einer aktiven Weglängenstabilisierung gegeben. Diese wird über ein Piezoelement am Spiegel im kurzen Arm der Interferometer realisiert. Wie gezeigt wird das Interferenzsignal des Referenzstrahls als Fehlersignal genutzt. Allerdings ist die Stabilität des Referenzlasers bisher noch nicht ausreichend. Aufgrund der Drift des Referenzlasers ist die Phasenstabilität der Interferometer über eine längere Zeit noch nicht gewährleistet und setzt im Moment die praktischen Grenzen für deren Gebrauch. Lösungsvorschläge durch eine bessere Stabilisierung des Referenzlasers werden im Ausblick diskutiert.
Vergleicht man die Ergebnisse dieser Arbeit mit Ergebnissen zur Implementierung des BB84 Protokolls mittels *time-bin*-Kodierung aus der Literatur, so sieht man, dass der realisierte Aufbau erstmalig die *time-bin*-Kodierung schmalbandiger Photonen erlaubt. Bisherige Experimente zur *time-bin*-Kodierung waren für Photonen mit einer Bandbreite im GHz-Bereich gedacht [MdRT$^+$02, BGTZ99]. Jetzt ist man in der Lage, Photonen im MHz-Bereich zu kodieren. Dies eröffnet die Möglichkeit für die Verbindung von *time-bin*-Qubits mit Experimenten zur Photonenspeicherung zur Realisierung komplexer Quantennetzwerke.

Kapitel 5

Ausblick

Ziel dieser Arbeit war der Aufbau von zwei Michelson-Interferometern für die *time-bin*-Kodierung und Dekodierung schmalbandiger Photonen. Für die Verbesserung der Phasenstabilität der Interferometer ist die Stabilität des Referenzlasers unerlässlich. Aus diesem Grund ist ein Aufbau geplant, der den Referenzlaser an den Signallaser stabilisiert. Das Ziel ist die Stabilität des Signallasers auf den Referenzlaser zu übertragen, um so das Driften gegeneinander zu minimieren. Dazu wird der Resonator zunächst auf den Signallaser nach dem Pound-Drever-Hall-Verfahren (PDH) stabilisiert [Bla01]. Anschließend wird der Referenzlaser ebenfalls nach dem PDH-Verfahren auf den Resonator stabilisiert. Zunächst werden auf den Signallaser mit einem EOM Seitenbänder moduliert. Die Modulationsfrequenz liefert ein Lokaloszillator. Das so modulierte Licht trifft auf den Resonator. Ein Teil des reflektierten Lichts wird detektiert und das Detektorsignal mit dem Signal des Lokaloszillator gemischt. Nach der Filterung mit einem Tiefpass erhält man so ein Fehlersignal, das als Regelsignal für ein Piezoelement dient, das an einem der Resonatorspiegel befestigt ist.
Der Referenzlaser wird nun ebenfalls phasenmoduliert durch einen EOM und trifft auf den Resonator. Wie beim Signallaser wird auch hier das reflektierte Detektorsignal heruntergemischt und gefiltert. Allerdings wird das Fehlersignal an den Stromtreiber des Referenzlasers gegeben, so dass der Referenzlaser an den Resonator stabilisiert werden kann.
Läuft der Referenzlaser stabiler, ist die Umsetzung des BB84-Protokolls geplant. Nachdem die Voraussetzungen geschaffen worden sind, kann nach der Phasenkalibrierung der Schlüsselaustausch erfolgen.
Langfristig sollen die Interferometer integriert werden in ein Experiment zur Speicherung von echten Einzelphotonen, kodiert nach dem *time-bin*-Schema. Abbildung 5.1 gibt einen schematischen Überblick über den Gesamtaufbau des Experiments zur Implementierung eines Qubit-Relays. Als Quelle echter Einzelphotonen wird ein optisch parametrischer Oszillator (OPO) benutzt, der unterhalb seiner Schwelle betrieben wird. Ein Pumpphoton bei einer Wellenlänge von 447 nm erzeugt in einem BIBO-Kristall bei Phasenanpassung

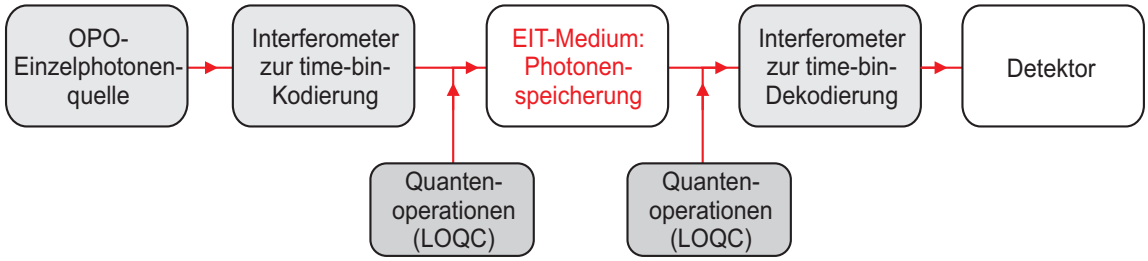

Abbildung 5.1: *Skizze des geplanten Experiments eines Qubit-Relays*

zwei Photonen bei $\lambda = 894$ nm (Signal und Idler). Durch die Detektion des Idler-Photons wird die Präsenz des anderen angekündigt und der Signalstrahl ist eine Einzelphotonenquelle. Der Betrieb innerhalb eines Resonators führt zur Verminderung der Linienbreite von einigen THz in den MHz-Bereich. Eine experimentelle Realisierung wurde bereits fertiggestellt und erreichte eine Bandbreite von $\cong$80 MHz. Dabei ist der Resonator nur für die Signalphotonen resonant (einfachresonant). Die zusätzliche Stabilisierung des OPO-Resonators auf die Pumpphotonen erlaubte zu ersten Mal eine kontinuierliche Erzeugung von Einzelphotonen mit einem solchen Aufbau. Ein im Aufbau befindlicher neuer OPO mit einem PPKTP-Kristall zur Frequenzkonversion und einem KTP-Kristall zur Weglängenkompensation im Resonator soll den doppelresonanten Betrieb erlauben. Dies führt zu einer verbesserten Photonenrate und einer geringeren Bandbreite von ca. 15 MHz.
Die so erzeugten Photonen können dann mit dem ersten Interferometer nach dem *time-bin*-Schema kodiert werden. Die Speicherung erfolgt mittels elektromagnetisch induzierter Transparenz (EIT) in einem Cäsiumgas. Die Kopplung der beteiligten Energieniveaus innerhalb der D1-Linie durch einen starken Pumplaser führen zur Abremsung bzw. Speicherung der Photonen. Die Photonen können dann mit dem zweiten Interferometer dekodiert und anschließend detektiert werden.
Auf diese Weise ist die Realisierung eines Quantennetzwerks möglich, in dem atomare Ensembles die Schnittstellen bilden zwischen denen *time-bin* kodierte Qubits ausgetauscht werden können.

Literaturverzeichnis

[ALP+06] N. Akopian, N. H. Lindner, E. Poem, Y. Berlatzky, J. Avron, D. Gershoni, B. D. Gerardot, and P. M. Petroff. Entangled photon pairs from semiconductor quantum dots. *Physical Review Letters*, 96(13):130501, 2006.

[Aud05] J. Audretsch. *Verschränkte Systeme*. Wiley-VCH, 1 edition, 2005.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Quantum key distribution and coin tossing. In *Proc. IEEE Int. Conference on Computers, Systems and Signal Processing, Bangalore, Indien*, page 175, 1984.

[BBB+92] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *J. Cryptol.*, 5(1):3–28, 1992.

[BDCZ98] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81(26):5932–5935, Dec 1998.

[Ben62] W. R. Bennett. Hole burning effects in a he-ne optical maser. *Physical Review*, 126(2):580–593, April 1962.

[BGL98] D. Bimberg, M. Grundmann, and N. N. Ledentsov. *Quantum Dot Heterostructures*. John Wiley & Sons, Chichester, 1998.

[BGTZ99] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden. Pulsed energy-time entangled twin-photon source for quantum communication. *Physical Review Letters*, 82(12):2594–2597, March 1999.

[BIH91] K. J. Boller, A. Imamoglu, and S. E. Harris. Observation of electromagnetically induced transparency. *Physical Review Letters*, 66(20):2593–2596, May 1991.

[Bla01] E. D. Black. An introduction to pound–drever–hall laser frequency stabilization. *American Journal of Physics*, 69(1):79–87, January 2001.

[BLTO99] C. Brunel, B. Lounis, P. Tamarat, and M. Orrit. Triggered source of single photons based on controlled single molecule fluorescence. *Physical Review Letters*, 83(14):2722–2725, October 1999.

[BSPY00] O. Benson, C. Santori, M. Pelton, and Y. Yamamoto. Regulated and entangled photons from a single quantum dot. *Physical Review Letters*, 84(11):2513–2516, March 2000.

[BZL03] M. Bajcsy, A. S. Zibrov, and M. D. Lukin. Stationary pulses of light in an atomic medium. *Nature*, 426:638, 2003.

[CCY+08] Y.-A. Chen, S. Chen, Z.-S. Yuan, B. Zhao, C.-S. Chuu, J. Schmiedmayer, and J.-W. Pan. Memory-built-in quantum teleportation with photonic and atomic qubits. *Nature Physics*, advanced online, January 2008. 10.1038/nphys832.

[CMJ+05] T. Chanelière, D. N. Matsukevich, S. D. Jenkins, S. Y. Lan, T. A. B. Kennedy, and A. Kuzmich. Storage and retrieval of single photons transmitted between remote quantum memories. *Nature*, 438:833, 2005.

[CZKM97] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi. Quantum state transfer and entanglement distribution among distant nodes in a quantum network. *Phys. Rev. Lett.*, 78(16):3221–3224, Apr 1997.

[Dem07] W. Demtröder. *Laserspektroskopie: Grundlagen und Techniken.* Spinger, Berlin, 5 edition, 2007.

[EAM+05] M. D. Eisaman, A. André, F. Massou, M. Fleischhauer, A. S. Zibrov, and M. D. Lukin. Electromagnetically induced transparency with tunable single-photon pulses. *Nature*, 438:837, 2005.

[EPT03] C. Elliott, D. Pearson, and G. Troxel. Quantum cryptography in practice. In *SIGCOMM '03: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 227–238, New York, NY, USA, 2003. ACM.

[Fey82] R. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6):467–488, June 1982.

[FL00] M. Fleischhauer and M. D. Lukin. Dark-state polaritons in electromagnetically induced transparency. *Physical Review Letters*, 84(22):5094–5097, May 2000.

[Gmb] Laser Components GmbH. Single photon counting module - spcm-aqr series specifications. Technical report.

[GRTZ02] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145–195, March 2002.

[Har97] S. E. Harris. Electromagnetically induced transparency. *Physics Today*, 50:36, 1997.

[HHDB99] L. V. Hau, S. E. Harris, Z. Dutton, and C. H. Behroozi. Light speed reduction to 17 metres per second in an ultracold atomic gas. *Nature*, 397(6720):594–598, February 1999. 10.1038/17561.

[HM91] K. C. Harvey and C. J. Myatt. External-cavity diode laser using a grazing-incidence diffraction grating. *Opt. Lett.*, 16(12):910, 1991.

[KMZW00] C. Kurtsiefer, S. Mayer, P. Zarda, and H. Weinfurter. Stable solid-state source of single photons. *Physical Review Letters*, 85(2):290–293, July 2000.

[KWS06] C. E. Kuklewicz, F. N. C. Wong, and J. H. Shapiro. Time-bin-modulated biphotons from cavity-enhanced down-conversion. *Physical Review Letters*, 97(22):223601, 2006.

[Las05] Sacher Lasertechnik. Spectroscopy with diode lasers. Technical report, Sacher Lasertechnik GmbH, 2005.

[LM00] B. Lounis and W. E. Moerner. Single photons on demand from a single molecule at room temperature. *Nature*, 407(6803):491–493, September 2000. 10.1038/35035032.

[LO00] Y. J. Lu and Z. Y. Ou. Optical parametric oscillator far below threshold: Experiment versus theory. *Physical Review A*, 62(3):033804, August 2000.

[Lyr02] H. Lyre. *Informationstheorie*. UTB, Wilhelm Fink Verlag, München, 1 edition, 2002.

[MdRT+02] I. Marcikic, H. de Riedmatten, W. Tittel, V. Scarani, H. Zbinden, and N. Gisin. Time-bin entangled qubits for quantum communication created by femtosecond pulses. *Physical Review A*, 66(6):062308, December 2002.

[MHH+97] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin. "plug and play" systems for quantum cryptography. *Applied Physics Letters*, 70(7):793–795, 1997.

[MIM+00] P. Michler, A. Imamoglu, M. D. Mason, P. J. Carson, G. F. Strouse, and S. K. Buratto. Quantum correlation among photons from a single quantum dot at room temperature. *Nature*, 406(6799):968–970, August 2000. 10.1038/35023100.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 1 edition, 2000.

[NNNT+07] J. S. Neergaard-Nielsen, B. M. Nielsen, H. Takahashi, A. I. Vistnes, and E. S. Polzik. High purity bright single photon source. *Optics Express*, 15:7940, 2007.

[PFM+01] D. F. Phillips, A. Fleischhauer, A. Mair, R. L. Walsworth, and M. D. Lukin. Storage of light in atomic vapor. *Physical Review Letters*, 86(5):783–786, January 2001.

[RBG+00] G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden. Long-distance entanglement-based quantum key distribution. *Physical Review A*, 63(1):012309, December 2000.

[RSA78] R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM - Association for Computing Machinery*, 21(2):120–126, 1978.

[Sha48] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423 and 623–656, July and October 1948.

[Sha49] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.

[Sho97] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[SKHR+03] F. Schmidt-Kaler, H. Häffner, M. Riebe, S. Gulde, G. P. T. Lancaster, T. Deuschle, C. Becher, C. F. Roos, J. Eschner, and R. Blatt. Realization of the cirac-zoller controlled-not quantum gate. *Nature*, 422(6930):408–411, March 2003. 10.1038/nature01494.

[SKO+06] J. F. Sherson, H. Krauter, R. K. Olsson, B. Julsgaard, J. I. Cirac, K. Hammerer, and E. S. Polzik. Quantum teleportation between light and matter. *Nature*, 443:557, 2006.

[SPS+01] C. Santori, M. Pelton, G. S. Solomon, Y. Dale, and Y. Yamamoto. Triggered single photons from a quantum dot. *Physical Review Letters*, 86(8):1502–1505, February 2001.

[SWHB07] M. Scholz, F. Wolfgramm, U. Herzog, and O. Benson. Narrow-band single photons from a single-resonant optical parametric oscillator far below threshold. *Applied Physics Letters*, 91(19):191104, 2007.

[SYA+06] R. M. Stevenson, R. J. Young, P. Atkinson, K. Cooper, D. A. Ritchie, and A. J. Shields. A semiconductor source of triggered entangled photon pairs. *Nature*, 439:179, 2006.

[TRBZ04] L. Tian, P. Rabl, R. Blatt, and P. Zoller. Interfacing quantum-optical and solid-state qubits. *Physical Review Letters*, 92(24):247902, 2004.

[TS93] U. Tietze and Ch. Schenk. *Halbleiter-Schaltungstechnik*. Springer-Verlag, Berlin, 1993.

[Ver26] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. AIEE*, 45:109–115, 1926.

[VSB+01] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang. Experimental realization of 's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414(6866):883–887, December 2001. 10.1038/414883a.

[WD83] R. Wyatt and W. J. Devlin. 10 khz linewidth 1.5μm ingaasp external cavity laser with 55 nm tuning range. *Electronics Letters*, 19(3):110–112, 1983.

[Wya85] R. Wyatt. Spectral linewidth of external cavity semiconductor lasers with strong, frequency-selective feedback. *Electronics Letters*, 21(15):658–659, 1985.

[YN05] J. Q. You and F. Nori. Superconducting circuits and quantum information. *Physics Today*, 58(11):42–47, 2005.

Publikationen und Konferenzbeiträge

- N. Neubauer, M. Scholz, and O. Benson: *Time-Bin Encoding for Narrow-Band Single Photons, Vortrag, DPG Tagung, 10.-14. März 2008, Darmstadt*
- *M. Scholz, N. Neubauer, and O. Benson: Time-Bin Encoding for Narrow-Band Single Photons, Vortrag, CLEO/QELS, 04.-09. Mai 2008, San Jose*

Danksagung

An dieser Stelle möchte ich mich bei denjenigen bedanken, die für die Durchführung und das Gelingen meiner Diplomarbeit einen entscheidenden Beitrag geleistet haben.

Zunächst gilt der Dank Herrn Professor Oliver Benson, in dessen Arbeitsgruppe ich meine Diplomarbeit anfertigte. Ihm verdanke ich die Möglichkeit an einem interessanten Experiment der Quanteninformation mitzuarbeiten. Die kollegiale Art und das in mich gesetzte Vertrauen habe ich sehr zu schätzen gelernt.

Herrn Professor Marius Grundmann möchte ich sehr herzlich dafür danken, dass er als weiterer Betreuer zur Verfügung stand und mir überhaupt erst die Möglichkeit gab, meine Diplomarbeit extern anzufertigen.

Ganz besonders möchte ich Matthias Scholz danken. Er hat diese Diplomarbeit betreut und gab mir die Möglichkeit in seinem Projekt mitzuarbeiten. Seinem Wissen in experimenteller und theoretischer Hinsicht gilt mein ganzer Respekt, und ohne seine Lösungsvorschläge für die großen und kleinen Probleme im Labor wäre diese Diplomarbeit wohl nicht möglich gewesen. Auch für das Korrekturlesen sei ihm herzlichst gedankt.

Herrn Dipl.-Ing. Klaus Palis möchte ich danken für seine professionelle Unterstützung in Fragen der Elektronik. Ohne seine Sachkenntnis und sein Organisationstalent wären die verschiedensten elektronischen Komponenten und Bauteile nicht realisiert worden. Seine humorvolle Art hat ihr Übriges zur guten Stimmung innerhalb der Gruppe beigetragen.

David Höckel möchte ich danken für seine Anleitung und seinen Rat in Fragen der Laserstabilisierung und Pulserzeugung.

Alexander Walter gilt der Dank für seine Arbeit am Aufbau der Elektronik und diverser Rackkomponenten.

Der Werkstatt des Instituts möchte ich danken für die geduldige Umsetzung unserer Konstruktionen.

Des Weiteren möchte ich mich bei allen Mitgliedern der Arbeitsgruppen NANO, QOM und AMO für die Unterstützung im Labor und die gute Stimmung bedanken, die während der gesamten Zeit die Arbeit erleichtert haben.

Zu guter Letzt danke ich meinen Eltern und meiner Schwester, die mich während des Studiums in jeder Hinsicht unterstützt haben.

Selbständigkeitserklärung

Hiermit erkläre ich, dass ich die Diplomarbeit selbständig verfasst habe und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Stellen der Arbeit, die wörtlich oder sinngemäß aus Veröffentlichungen oder aus anderweitigen fremden Äußerungen entnommen wurden, sind als solche kenntlich gemacht. Ferner erkläre ich, dass die Arbeit noch nicht in einem anderen Studiengang als Prüfungsleistung verwendet wurde.

Ich bin einverstanden, dass die Arbeit nach positiver Begutachtung in der Universitätsbibliothek zur Verfügung steht.