Kompakte Quelle verschränkter Photonen

und

Anwendungen in der Quantenkommunikation

Diplomarbeit an der Fakultät für Physik
der
Ludwig-Maximilians-Universität München
Arbeitsgruppe Prof. Dr. Harald Weinfurter

Christian I. T. Schmid

12. Januar 2004

Erstgutachter: Prof. Dr. Harald Weinfurter
Zweitgutachter: Prof. Dr. Axel Schenzle

Inhaltsverzeichnis

Einleitung

Betrachtet man die Einführung des Wirkungsquantums im Jahre 1900 durch Max Planck als den Beginn der Quantenmechanik, so nahm vor gut 100 Jahren eine wissenschaftliche Theorie ihren Anfang, die heute zwar mathematisch gut verstanden ist, sich aber dennoch einer endgültig schlüssigen und allgemein akzeptierten Interpretation verschließt. Die Probleme bei der Deutung dieser Theorie sind jedoch möglicherweise nicht allzu verwunderlich. Bereits die Semantik des Wortes „be-greifen" macht deutlich, dass unser Verständnis für die Dinge, die uns umgeben, auf ihrem Befühlen, d.h. im weiteren Sinne der Wahrnehmbarkeit durch uns selbst beruht. Die Quantenmechanik, die ihre Relevanz hauptsächlich im Mikrokosmos entfaltet, beschreibt dagegen Eigenschaften von Objekten wie Elektronen und Photonen, die sich vollends der durch unsere körpereigenen Sinne erfahrbaren Welt entziehen. Der Leser möge sich an dieser Stelle bewusst machen, welches vage Bild er beim Lesen des Wortes „Photon" vor Augen hat, im Vergleich zum Begriff der „Kugel" beispielsweise. Im Gegensatz zu klassischen Objekten wie einer Kugel, scheinen für Quanten allerdings Fragestellungen berechtigt und Effekte von Bedeutung zu sein, die, übertragen auf unsere makroskopische Alltagswelt absurd oder nicht relevant erscheinen. Niemand hat je seine Katze in einer Superposition aus tot und lebendig vorgefunden [3] und nur wenige werden sich fragen, ob der Mond auch existiert, wenn sie ihn nicht ansehen [4] (siehe auch Kapitel 1.1 und 1.2).

Trotz dieser scheinbaren Kuriositäten, die unser Verständnis für Realität bisweilen herausfordern, sind die 100 Jahre Quantenmechanik auch, oder sogar vielmehr, eine Erfolgsgeschichte. Die Erklärung zahlreicher experimenteller Beobachtungen sowie moderne technische Errungenschaften basieren auf der Quantenmechanik und eben gerade die „kontraintuitiven" Besonderheiten dieser Theorie wurden gegen Ende des letzten Jahrhunderts zur elementaren Resource eines völlig neuen Bereichs der Physik, der Quanteninformationstheorie. Sie bildet die Synthese von Informatik, Kryptographie, Informationstheorie und Quantenmechanik und versucht, meist von einem pragmatischen Standpunkt, sich typisch nicht-klassische Effekte zur Bewältigung informationstheoretischer Probleme nutzbar zu machen.

Die vorliegende Arbeit befasst sich mit unterschiedlichen Fragestellungen der Quantkommunikation, einem Teilbereich der Quanteninformationstheorie, und gliedert sich

in vier Teile.

Nach einem Überblick über die Grundlagen, die für weiteres notwendig sind, wird die Entwicklung einer kompakten Quelle zur Erzeugung polarisationsverschränkter Photonepaare, basierend auf dem Prozess der spontanen parametrischen Fluoreszenz, beschrieben. Neu ist dabei nicht die Idee für die Art der Erzeugung, sondern die Bauweise. Die Verwendung einer blauen Laserdiode, anstelle von herkömmlichen Ionenlasern zum „pumpen“ des Prozesses ermöglicht einen experimentellen Aufbau auf kleinem Raum bei dennoch hoher Effizienz. Die Eignung der Quelle wird dann im weiteren Verlauf der Arbeit in verschiedenen Experimenten demonstriert, in denen nicht nur die Polarisationsverschränkung der Photonen eines Paares, sondern auch deren zeitliche Korrelation ausgenutzt wird. So dient sie zunächst der Untersuchung quantenmechanischer Statistik, insbesondere der systematischen Rekonstruktion der Schranken des CHSH-Operators. Später stellt sie als Quasi-Einzelphotonquelle den Ausgangspunkt für weitere Versuche dar.

Gegenstand eines dieser Versuche ist die Quantenkommunikationskomplexität. Sie beschäftigt sich mit der Fragestellung, wie bestimmte Berechnungen durch mehrere Parteien unter der Bedingung minimaler Kommunikation gemeinschaftlich gelöst werden können. In dem vorgestellten Experiment bestimmen fünf Personen den korrekten Wert einer boolschen Funktion mit höchstmöglicher Erfolgsrate durch das sequenzielle Versenden eines einzelnen (Qu)bits, wobei die Funktion von zwei-Bit Zufallszahlen abhängig ist, die zuvor an jede Partei verteilt werden. Die erfolgreiche Durchführung des Versuchs ermöglicht erstmals die Demonstration der Überlegenheit einer breiten Klasse quantenmechanischer Komplexitätsprotokolle gegenüber ihren klassischen Entsprechungen, da ein Qubit zwei Bit an klassischer Kommunikation ersetzt.

Ausgehend von dem Versuchsaufbau des Kommunikationskomplexitätsprotokolls wird im letzten Abschnitt der Arbeit ein „Secret-Sharing“-Protokoll mit sechs Parteien implementiert. Es behandelt die Aufteilung eines Geheimnises an fünf Personen in einer Weise, dass zu dessen Rekonstruktion die Kooperation aller fünf erforderlich ist. Das Protokoll, das hierfür verwendet wird, ist neu. Ähnlich wie beim vorher erwähnten Experiment übermitteln die Parteien lediglich ein einzelnes Qubit. Die Korrelationen, die sie durch dessen Messung erhalten sind äquivalent zu verschränkungsbasierten „Secret-Sharing“-Protokollen, die Mehrteilchen GHZ-Zustände nutzen. Diese Äquivalenz zwischen dem Einsatz einzelner Qubits und verschränkter Systeme ist insofern interessant, als sie bereits in anderen Szenarien gezeigt werden konnte. Beispielsweise wurde sie für die von Bennett und Brassard 1984 vorgeschlagene Einzelphotonenkryptographie [5] und das von Bennett, Brassard und Mermin 1992 eingeführte verschränkungsbasierte Verfahren bewiesen [6]. Auch das in dieser Arbeit vorgestellte Kommunikationskomplexitätsprotokoll wurde zunächst für verschränkte Zustände formuliert und erst später für Einzelphotonen modifiziert. Inwieweit all diesen Protokollen eine fundamentale Gemeinsamkeit zu Grunde liegt, die zu diesen Analogien führt, wäre sicherlich einer weiterführenden Untersuchung wert.

Kapitel 1

Allgemeine Grundlagen

Dieses Kapitel führt in die allgemeinen theoretischen Grundlagen ein, die für das weitere Verständnis der vorliegenden Arbeit benötigt werden. Es zeigt die Unterschiede zwischen klassischer und quantaler Mechanik auf und erklärt den Begriff der Verschränkung als logische Konsequenz aus dem Superpositionsprinzip beim Übergang von Ein- zu Mehrteilchensystemen. Die besonderen Eigenschaften verschränkter Systeme werden anhand von EPR's Paradoxon verdeutlicht. Die Bellsche Ungleichung soll auf einfache Weise hergeleitet und der Widerspruch zwischen lokalem Realismus und Quantenmechanik aufgezeigt werden. Inwieweit Bell-Ungleichungen in verschränkungsbasierten Kryptographieprotokollen von Nutzen sind, wird gegen Ende dieses Abschnitts diskutiert.

1.1 Superpositionsprinzip und Verschränkung

Ausgehend von Newtons Axiomen wird in der klassischen Mechanik der physikalische Zustand eines Teilchens durch seinen Ort $\vec{x}(t)$ und seinen Impuls $\vec{p}(t)$ zu jedem Zeitpunkt t beschrieben. Die Kenntnis dieser beiden Größen erlaubt die eindeutige Vorhersage der Dynamik eines Systems. Im Phasenraum stellt sich ein Zustand zur Zeit t als Punkt $(\vec{x}(t), \vec{p}(t))$ dar und seine zeitliche Entwicklung ergibt sich als Trajektorie, also Abfolge von Punkten in diesem Raum.

Fast ebenso axiomatisch, aber dennoch grundlegend anders offenbart sich die Situation in der Quantenmechanik. Die vollständige Information über einen Zustand liegt hier in einem Vektor $|\chi\rangle$,[1] der Element eines Hilbertraumes ist. Die zeitliche Entwicklung ergibt sich durch eine unitäre Transformation dieses Vektors im Hilbertraum, beschrieben

[1] Hilbertraum-Vektoren werden in Dirac-Notation geschrieben, im Gegensatz zu Vektoren des Koordinatenraums, die durch einen Pfeil gekennzeichnet sind.

durch die Schrödinger-Gleichung [7].

Dieser Unterschied in der Zustandsbeschreibung zwischen einem Punkt im Phasenraum und einem Vektor in einem Hilbertraum hat weitreichende Konsequenzen. Während Vektoren per Definitionem die Eigenschaft haben, dass zwischen Ihnen eine additive Verknüpfung existiert, deren Ergebnis wiederum einen Vektor ergibt, macht eine Überlagerung von Punkten keinen Sinn. Wie sich dieser mathematische Sachverhalt physikalisch darstellt soll folgendes einfaches Beispiel verdeutlichen. Zur Beschreibung des Prinzips werden dabei anstelle der zuvor angesprochenen kontinuierlichen Variablen Ort und Impuls der Einfachheit halber diskrete innere Freiheitsgrade verwendet. Der Leser möge sich davon nicht verwirren lassen.

Man betrachte ein Zweizustandssystem; dessen mögliche Zustände seien 0 und 1, repräsentiert durch die Punkte $p0$ und $p1$ im Phasenraum bzw. die Vektoren $|\,0\,\rangle$ und $|\,1\,\rangle$ im Hilbertraum. (Man denke dabei klassisch an eine Münze in den Zuständen „Kopf oben“ und „Zahl oben“ oder quantal an ein Photon das entweder horizontal oder vertikal polarisiert ist). Während klassisch nur *entweder* der Zustand 0 *oder* 1 existiert (entweder „Kopf oben“ oder „Zahl oben“), stellt im quantalen Fall die Superposition aus beiden Zuständen $|\,\chi\,\rangle = \frac{1}{\sqrt{2}}(|\,0\,\rangle + |\,1\,\rangle)$ ebenfalls einen physikalisch realisierten Zustand dar (Photon mit 45 ° Polarisation).

Diese Tatsache, das sogenannte Superpositionsprinzip, führt beim Übergang von einem Einteilchen- zu einem Mehrteilchensystem unmittelbar zu Verschränkung [3]. Was damit gemeint ist und wie es dazu kommt, soll wieder an einem Beispiel verdeutlicht werden:

Es seien $\mathfrak{S}_1$ und $\mathfrak{S}_2$ zwei Zweizustandssysteme (man möge wieder Münzen bzw. Photonen vor Augen haben), die jeweils in den Zuständen 0 oder 1 vorliegen können. Klassisch kann sich das aus $\mathfrak{S}_1$ und $\mathfrak{S}_2$ zusammengesetzte System $\mathfrak{S}_{12}$ nur in einem der vier Zustände 00, 01, 10, 11 befinden[2]. Quantenmechanisch ist jedoch auch jede Superposition der vier Grundzustände möglich, wie beispielsweise $|\,\phi^+\,\rangle = \frac{1}{\sqrt{2}}(|\,00\,\rangle + |\,11\,\rangle)$[3] Dieser Zustand hat die bemerkenswerte Eigenschaft, dass über jedes einzelne Subsystem keine Aussage, seinen Zustand betreffend, gemacht werden kann. Weder System $\mathfrak{S}_1$ noch $\mathfrak{S}_2$ befindet sich im Zustand 0 oder 1. Es ist lediglich eine Aussage über das Gesamtsystem $\mathfrak{S}_{12}$ möglich. Dies wird unmittelbar ersichtlich betrachtet man die von Neumann Entropie E als die Menge an Unkenntnis und somit indirektes Maß für den

[2]Die erste Ziffer bezieht sich immer auf den Zustand von $\mathfrak{S}_1$ während die zweite den Zustand von $\mathfrak{S}_2$ darstellt

[3]Der Vektor $|\,00\,\rangle = |\,0\,\rangle \otimes |\,0\,\rangle$ entspricht dem Zustand 00, d.h. System $\mathfrak{S}_1$ befindet sich im Zustand 0 und System $\mathfrak{S}_2$ im Zustand 0.

Informationsgehalt. Sie ist für das Gesamtsystem gegeben durch

$$\begin{aligned} E_{\mathfrak{S}_{12}} &= -\mathrm{Tr}\left[|\,\phi^+\,\rangle\langle\,\phi^+\,|\,\log_2\left(|\,\phi^+\,\rangle\langle\,\phi^+\,|\right)\right] \\ &= -\sum_i \lambda_i \log_2(\lambda_i) \end{aligned} \tag{1.1}$$

wobei λ_i die Eigenwerte von $|\,\phi^+\,\rangle\langle\,\phi^+\,|$ sind und es gilt $E_{\mathfrak{S}_{12}} = 0$. Das bedeutet die Unkenntnis ist gleich null und damit die Information maximal. Für ein Subsystem ergibt sich hingegen

$$E_{\mathfrak{S}_1,\mathfrak{S}_2} = -\mathrm{Tr}[\rho_{1,2}\,\log_2(\rho_{1,2})] \tag{1.2}$$

mit $\rho_{1,2} = \mathrm{Tr}_{\mathfrak{S}_1,\mathfrak{S}_2}[|\,\phi^+\,\rangle\langle\,\phi^+\,|] = \frac{1}{2}\,|\,0\,\rangle\langle\,0\,| + \frac{1}{2}\,|\,1\,\rangle\langle\,1\,|$ und $E_{\mathfrak{S}_1,\mathfrak{S}_2} = 1$, also maximal. Die Information ist daher minimal.

Obwohl man bei einer Messung der beiden Teilchen perfekt korrelierte Ergebnisse erhält, z.B. findet man beide im gleichen Zustand, d.h. beide im Zustand 0 oder beide in 1, ist dennoch für ein einzelnes Teilchen keine Information den Zustand betreffend vorhanden. Diese besondere Eigenschaft bestimmter quantaler Zustände wurde von Erwin Schrödinger als Verschränkung bezeichnet [3]. Mathematisch ist dies eine Konsequenz der Tatsache, daß der Zustand $|\,\phi^+\,\rangle$ nicht faktorisierbar ist:

Definition 1 (Verschränkung eines Zweiteilchenzustands) *Es seien* $\mathbb{H}_1$ *und* $\mathbb{H}_2$ *zwei Hilberträume und* $\mathbb{H}_{12} = \mathbb{H}_1 \otimes \mathbb{H}_2$.
Ein Zustand $|\,\xi\,\rangle \in \mathbb{H}_{12}$ *heißt verschränkt* $\Longleftrightarrow \nexists\, |\,a\,\rangle \in \mathbb{H}_1 \wedge |\,b\,\rangle \in \mathbb{H}_2 : |\,\xi\,\rangle = |\,a\,\rangle \otimes |\,b\,\rangle$.

Diese Definition erscheint auch im Bezug auf obige Betrachtungen sinnvoll. Läßt sich ein Zustand als Produkt schreiben, ist die Information über ein Subsystem von der Kenntnis des anderen völlig unabhängig. Sie ist in Form der Zustandsvektoren, welche die Faktoren bilden, separabel zugänglich.

1.2 EPR's Paradoxon und Bells Theorem

Die Beobachtung, dass keinem der beiden Teilchen eines verschränkten Zustands zu jeder Zeit bestimmte Eigenschaften zugeschrieben werden können, führte Einstein, Podolsky und Rosen (EPR) im Jahr 1935 zu einer philosophisch anmutenden Diskussion über Realität und einem vermeintlichem Paradoxon [8]. Diese Betrachtungen kulminierten in dem Schluß die Quantenmechanik sei keine vollständige Beschreibung der Wirklichkeit. Fast 30 Jahre später konnte Bell im Jahr 1964 zeigen, daß die Quantenmechanik, solange sie nicht im Experiment als ungültig widerlegt wird, in der Tat die Aufgabe von Lokalität oder Realismus fordert. Die Argumentationskette, die Bell

ausgehend von EPRs Definitionen von Vollständigkeit und Realismus einer Theorie zu seinen Ergebnissen geführt haben, soll hier kurz skizziert werden.

Nach EPR ist ein notwendiges Kriterium für die Vollständigkeit einer Theorie, dass jedes Element der physikalischen Realität („*element of physical reality*“) eine Entsprechung in der physikalischen Theorie aufweist. Realismus wird nach EPR wie folgt definiert:

Wenn sich der Wert einer physikalischen Größe mit Sicherheit, d.h. Wahrscheinlichkeit gleich eins, vorhersagen läßt, ohne dabei in irgendeiner Weise das System selbst zu stören, dann existiert ein Element unserer physikalischen Realität, das dieser physikalischen Größe entspricht.

Was bedeutet dies im Fall des Beispiels aus Abschnitt 1.1? Man nehme den Zustand $|\phi^+\rangle$ und entferne die Systeme $\mathfrak{S}_1$ und $\mathfrak{S}_2$ voneinander. Ist ihre Distanz raumartig kann eine Messung an System $\mathfrak{S}_1$ das System $\mathfrak{S}_2$ unter der Annahme von Kausalität nicht stören. Ferner erlaubt aber eine Messung am System $\mathfrak{S}_1$ die Vorhersage über das Resultat einer möglichen Messung am System $\mathfrak{S}_2$, da bekannt ist dass sich beide Systeme immer im gleichen Zustand befinden. Gemäß der Realitätsdefinition von EPR muß also der Zustand von $\mathfrak{S}_2$ bereits vor der Messung existent gewesen sein, d.h. ein Objekt der Realität sein. Dies steht im Widerspruch zu obiger quantenmechanischer Behauptung, eine Aussage über den Zustand eines der beiden Subsysteme sei nicht zu jeder Zeit (insbesondere bereits vor der Messung eines Teilchens) möglich. Wenn also kein definierter Zustand eines Einzelsystems $\mathfrak{S}_1$ oder $\mathfrak{S}_2$ vorliegt, das heißt wenn er also nicht „*element of physical reality*“ ist, genügt die Quantenmechanik nicht der Anforderung einer vollständigen Theorie im Sinne von EPR. Vermöge der Bellschen Ungleichung läßt sich jedoch zeigen, dass keine lokal-realistische, d.h. die Kausalität erhaltende und der obigen Definition von Realismus genügende Theorie[4] existieren kann, die zugleich Messergebnisse reproduziert, die gemäß einer quantenmechanischen Statistik verteilt sind. Bells Idee ist die folgende [9]:

Eine Quelle Q emittiert einen Zweiteilchenzustand, wovon je ein Teil an eine Partei Alice bzw. Bob verteilt wird. Sowohl Alice als auch Bob besitzen einen Apparat der zwei Observable mißt, abhängig von zwei lokalen Einstellungen (1) und (2). Die Messung kann dabei für jede Observable das Resultat $A_1 = \pm 1, A_2 = \pm 1$ bzw. $B_1 = \pm 1, B_2 = \pm 1$ ergeben. Die lokalen Einstellungen einer Partei können *nicht* das Meßergebnis der anderen Partei beeinflussen (Kausalität). Es gibt folgende Möglichkeiten:

[4]Solche Theorien werden häufig auch als „Local-hidden-variables-“-Theorien (LHV-Theorien) bezeichnet, da den Teilchen ein „verborgener“ Parameter zugeordnet wird, der alle möglichen Messergebnisse in Abhängigkeit lokaler Einstellungen beinhaltet.

$$\begin{array}{ccc} A_1 & \stackrel{?}{=} & B_1 \\ \text{||?} & & \text{||?} \\ B_2 & \stackrel{?}{=} & A_2 \end{array}$$

Ohne einen Widerspruch kann nur eine gerade Anzahl von Gleichungen Bestand haben, daher folgt

$$P(A_1 = B_1) - P(A_2 = B_1) - P(A_1 = B_2) - P(A_2 = B_2) \leq 0 \tag{1.3}$$

wobei $P(X)$ die Wahrscheinlichkeit für X ist. Wegen der Kausalität gilt ferner für die Verbundwahrscheinlichkeit

$$P(X \wedge Y) = P(X) \cdot P(Y) \tag{1.4}$$

Somit folgt mit der Definition für bedingte Wahrscheinlichkeit $P(X|Y) = \frac{P(X \wedge Y)}{P(Y)}$ wiederum $P(X|Y) = P(X)$ und Gleichung 1.3 läßt sich in äquivalenter Weise schreiben als

$$P(R_A = R_B|1,1) - P(R_A = R_B|1,2) - P(R_A = R_B|2,1) - P(R_A = R_B|2,2) \leq 0. \tag{1.5}$$

R_A bzw. R_B bezeichnen die Resultate von Alice oder Bob und die Ziffern 1 und 2 beziehen sich auf die jeweiligen lokalen Einstellungen. Sendet die Quelle Q einen verschränkten Zustand aus beträgt die obere Schranke S von Gleichung 1.5 für die quantenmechanischen Erwartungswerte $S_{qm} = \sqrt{2} - 1$.

1969 präsentierten Clauser, Horne, Shimony und Holt [10] (CHSH) eine Verallgemeinerung des Bellschen Theorems, die besonders für eine experimentelle Anwendung geeignet ist. Dieser Ansatz findet auch in dieser Arbeit für den Test von Polarisationsverschränkung Anwendung. Die Observablen bilden die Spinfreiheitsgrade von Teilchen, repräsentiert durch folgende vier Operatoren [11]:

$$\hat{A}(\theta) = \cos(2\theta)\sigma_z + \sin(2\theta)\sigma_x, \tag{1.6}$$

$$\hat{B}(\theta) = \cos(\theta)\sigma_z + \sin(\theta)\sigma_x, \tag{1.7}$$

$$\hat{a} = \sigma_z, \tag{1.8}$$

$$\hat{b}(\theta) = \cos(3\theta)\sigma_z + \sin(3\theta)\sigma_x \tag{1.9}$$

mit $0 \leq \theta \leq \pi$ einem Parameter und σ_x, σ_z den üblichen Pauli-Matrizen (siehe Anhang A.1.2). Die Schranke für quantenmechanische bzw. klassische Korrelationen bildet der Erwartungswert $S_{qm,LHV} = \langle \mathbf{CHSH} \rangle$ des Zweiteilchen-Operators **CHSH**

$$\mathbf{CHSH} := \hat{A} \otimes \hat{B} + \hat{A} \otimes \hat{b} + \hat{a} \otimes \hat{B} - \hat{a} \otimes \hat{b} \tag{1.10}$$

Es gilt [12]

$$| S_{LHV} | \quad \leq 2 \tag{1.11a}$$

$$| S_{qm} | \ \leq 2\sqrt{2}. \tag{1.11b}$$

Der maximale Wert $| S_{qm} | = 2\sqrt{2}$ wird jedoch nicht für alle Werte von θ und alle maximal verschränkten Zweiteilchenzustände erreicht. Das Maximum von S_{qm} folgt der Funktion [11]

$$F(\theta) = \pm 2 \left(\frac{1}{\sqrt{1 + \sin^2(2\theta)}} + g(\theta) \sin(2\theta) \sqrt{1 + \frac{2}{\cos(4\theta) - 3}} \right), \tag{1.12}$$

mit

$$g(\theta) = \begin{cases} +1 & \text{if } 0 \leq \theta < \pi/2 \\ -1 & \text{if } \pi/2 \leq \theta \leq \pi \end{cases} \tag{1.13}$$

Dies wird in 2.3.3 experimentell bestätigt.

1.3 Bell'sche Ungleichungen in der Quantenkryptographie

Kryptographie transformiert Information derart, dass sie unzugänglich, somit nutzlos, für nichtlegitimierte Empfänger wird. Um dies zu bewerkstelligen gibt es eine Reihe von Möglichkeiten. Eine, der sogenannte „one time pad“, wurde 1917 vom amerikanischen AT&T Ingenieur Gilbert Vernam erfunden [13] (siehe auch [14]). Darin ist die Transformation selbst öffentlich bekannt, jedoch ist sie abhängig von einem sog. Schlüssel, der geheim, d.h. nur den legitimen potentiellen Empfängern der Nachricht bekannt ist. Die zu übermittelnde Information wird vermöge dieses Schlüssels in eine Chiffre übersetzt, welche öffentlich zugänglich sein kann. Claude Shannon [15] bewies, dass es ohne die Kenntnis des Schlüssels keine Möglichkeit gibt die verschlüsselte Nachricht in Klartext zurückzuführen. Voraussetzung für die perfekte Sicherheit ist allerdings dessen Zufälligkeit und seine lediglich einmalige Verwendung. Liegt die zu versendende Nachricht als Bit-String vor, könnte der Schlüssel beispielsweise ebenfalls ein Bit-String mit einer zufälligen Abfolge von Nullen und Einsen sein. Eine einfache Transformation könnte in der bit-weisen Addition der beiden Strings bestehen, wobei sich die Zufälligkeit des Schlüssels auf die Nachricht überträgt und sie damit chiffriert. Zu klären bleibt hier jedoch die Frage, wie die beteiligten Parteien eines derartigen Kryptographieprotokolls in den Besitz des geheimen Schlüssels kommen. Eine "quantenmechanische Antwort“ lieferte erstmals Wiesner 1983 [16] (siehe auch [5]). Das erste verschränkungsbasierte Quantenkryptographieprotokoll schlug Artur Ekert 1991 vor [17].

1.3.1 Das Prinzip am Beispiel des Ekert Protokolls

In diesem Protokoll ergibt sich die Sicherheit aus dem zunächst *Nicht*-Vorhandensein der in 1.2 angesprochenen „*elements of physical reality*". Durch eine eventuelle Messung würden diese allerdings festgelegt, was dann wiederum die Erfüllung der Bell-Ungleichung zur Folge hätte.

Die zwei kommunizierenden Parteien Alice und Bob sind über einen Quantenkanal verbunden. Dieser besteht aus einer Quelle Q, die ein Paar von Photonen emittiert, welche sich in einem Singulett Zustand $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle - |V\rangle|H\rangle)$ befinden. Die zu übertragende Information wird dabei binär in der Polarisation der Photonen kodiert, wobei immer ein Paar orthogonaler Polarisationen die Bit-Werte 0 bzw. 1 repräsentiert. Je ein Teilchen des Singuletts erhält Alice bzw. Bob. Sie messen unabhängig von einander und zufällig die Observablen $\hat{a}, \hat{B}(\frac{\pi}{4}), \hat{A}(\frac{\pi}{4})$ bzw. $\hat{B}(\frac{\pi}{4}), \hat{A}(\frac{\pi}{4}), \hat{b}(\frac{\pi}{4})$. Nach der Übertragung geben beide bekannt welche Observablen sie wann gemessen haben. In den Fällen, in denen unterschiedliche Messungen gewählt wurden, werden die Meßergebnisse öffentlich verglichen um $S = \langle \mathbf{CHSH} \rangle$ zu berechnen. Bei ungestörter Kommunikation gilt für S Gleichung 1.11b. In den übrigen Fällen bilden die perfekt antikorrelierten Resultate die Grundlage für einen gemeinsamen, geheimen Schlüssel.

1.3.2 Lauschangriffe

Ein potentieller Lauscher kann während der Übertragung den Teilchen keine Information entnehmen weil sie schlichtweg nicht kodiert ist. Sie wird im Moment der Messung und öffentlichen Kommunikation durch die legitimen Empfänger erst existent. Es liegt seitens des Spions nahe, die Quelle auszutauschen und Alice und Bob mit speziell präparierten Daten zu versorgen. Da die zufällige Wahl der verwendeten Messbasen jedoch nicht bekannt ist, führt eine derartige Attacke unweigerlich zum Aufdecken des Abhörers. Sie entspricht der Einführung von "Elementen physikalischer Realität" in die Messung der Spinfreiheitsgrade, die dazu führt, dass der Wert von S die klassische Grenze nicht überschreitet oder zumindest nicht das quantenmechanische Maximum erreicht.

Eine experimentelle Realisierung und Bestätigung des von Ekert vorgeschlagenen Protokolls findet sich in [18]. In [19] wurde die Sicherheit einer Verallgemeinerung des Ekert-Protokolls auf N-Zustandssysteme bezüglich verschiedener Abhörattacken studiert. Im Allgemeinen bedeutet die Verletzung einer Bellschen Ungleichung jedoch nicht zwingend die Abwesenheit eines Lauschers. Dies zeigt folgendes Beispiel einer Variation des Ekert Protokolls, bei dem anstelle der CHSH-Ungleichung, Wigners Version [20] verwendet wird. Der Vorschlag dafür sowie dessen experimentelle Umsetzung stammt

aus dem Jahr 2000 [21]. Entsprechend S wird hier der Parameter

$$W = p(+,+|\alpha_1,\alpha_2) + p(+,+|\alpha_2,\alpha_3) - p(+,+|\alpha_1,\alpha_3) \tag{1.14}$$

bestimmt, mit

$$p(+,+|\alpha_i,\alpha_j) = |\,\langle H|\langle H|\hat{B}(\alpha_i)\otimes\hat{B}(\alpha_j)|\,\psi^-\,\rangle\,|^2 = \sin^2(\alpha_i-\alpha_j)/2 \tag{1.15}$$

und $\alpha_i \in \{-\frac{\pi}{6}, 0\}, \alpha_j \in \{0, \frac{\pi}{6}\}$. Für maximal verschränkte Zustände gilt $W = \frac{1}{8}+\frac{1}{8}-\frac{3}{8} = -\frac{1}{8}$, während für lokal realistische Theorien $W \geq 0$ ist.

Der Wert von W ist nur dann ein Maß für die Sicherheit der Kommunikation, falls ein möglicher Spion Eve lediglich Kontrolle über *ein* Subsystem des Singuletts hat. In diesem Fall gilt $W \geq \frac{1}{16}$. Sobald Eve beide Teilchen kontrollieren kann gibt es keine Schranke und W kann Werte annehmen, die sogar unter dem quantalen Limit liegen [22]. Dies wird in 2.3.3 experimentell gezeigt. (Zeitgleich wurden Experimente hierzu von Bovino, Colla und Castagnoli durchgeführt, siehe [23].) Sowohl die Erklärung als auch die Lösung dieses Problems liegt in der Herleitung der Wignerungleichung selbst, bei der perfekte (Anti-)Korrelationen vorausgesetzt werden, die in der Praxis jedoch aufgrund von Imperfektionen nicht gewährleistet werden können. Verwirft man folglich Wigners Annahme $p(+,+|\alpha_2,\alpha_2) = p(-,-|\alpha_2,\alpha_2) = 0$ mit

$$p(-,-|\alpha_i,\alpha_j) = |\,\langle V|\langle V|\hat{B}(\alpha_i)\otimes\hat{B}(\alpha_j)|\,\psi^-\,\rangle\,|^2 = \sin^2(\alpha_i-\alpha_j)/2, \tag{1.16}$$

analog zu Gleichung 1.15, gelangt man zu einem modifizierten Parameter

$$\begin{aligned}\widetilde{W} &= p(+,+|\alpha_1,\alpha_2) + p(+,+|\alpha_2,\alpha_3) + p(-,-|\alpha_2,\alpha_2) - p(+,+|\alpha_1,\alpha_3)\\ &= W + p(-,-|\alpha_2,\alpha_2).\end{aligned} \tag{1.17}$$

Wie man leicht sieht, gilt für lokal realistische Theorien $\widetilde{W} \geq 0$ und für einen reinen Zustand $|\,\psi^-\,\rangle$ ist $p(-,-|\alpha_2,\alpha_2) = 0$ und folglich $\widetilde{W} = W$. Der minimale Wert von $\widetilde{W}$ bei einem Lauschangriff beträgt $0,04428$ auch unter der Annahme totaler Kontrolle beider Kanäle durch Eve [22].

Die Intention bei der Nutzung von W anstelle von S in [21] war eine Vereinfachung des von Ekert ursprünglich vorgeschlagenen Protokolls dahingehend, dass die beteiligten Parteien nicht zwischen drei sondern lediglich zwei Analysatorstellungen auszuwählen haben. Dem wird aber auch durch die in [22] angeregte Einführung und Verwendung von $\widetilde{W}$ kein Abbruch getan. Alice und Bob müssen allerdings, wollen sie einen Abhörer ausschließen, einen Teil der Schlüsselbits, d.h. der Bits bei denen sie die gleiche Analysatorstellung verwendet haben, opfern. Dies wäre bei einer praktischen Anwendung im Rahmen von Fehlerkorrekturen zur Bestimmung der Quantum-Bit-Error-Rate (QBER), also der Fehlerrate, ohnehin nötig, selbst bei Verletzung einer Bell-Ungleichung. Denn auch bei Fehlern die durch experimentelle Imperfektionen, wie

mangelnde Verschränkung der Quelle, Rauschen des Quantenkanals etc. verursacht sind, muss grundsätzlich zunächst davon ausgegangen werden, dass ihr Ursprung in einem Lauschangriff liegt. Es ist daher naheliegend Fehlerkorrektur und Sicherheitsanalyse simultan zu betreiben und die selben Bits für beide Zwecke zu verwenden, wie es bei Einzelphotonen-Quantenkryptographieprotokollen üblich ist (siehe beispielsweise [5]). Die Anzahl der zum Schlüssel beitragenden Bits richtet sich demgemäß nach den Sicherheitsanforderungen und liegt zwischen 2/9 und 1/3 der insgesamt ausgetauschten Bits. Bei der Verwendung von S beträgt sie zum Vergleich in jedem Fall 2/9. Eine Frage die trotz allem offen bleibt, ist die nach dem Informationsgewinn eines Abhörers bei der Durchführung einer der zuvor beschriebenen Attacken.

Abschließend sei noch erwähnt, dass die Verwendung von Verschränkung in der Quantenkryptographie einen entscheidenden Vorteil gegenüber dem Einsatz von Einzelphotonen bringt. Sie ermöglicht die sichere Verteilung der Schlüßelbits an Alice und Bob durch (möglicherweise nicht vertrauenswürdige) Dritte. Man denke beispielsweise an die in [24] vorgeschlagene Verteilung von verschränkten Photonen über Satellit. Ein unseriöser Satellitenbetreiber würde beim Versuch die Quelle zu manipulieren, der obigen Argumentation analog folgend, unweigerlich erkannt werden.

Kapitel 2

Kompakte Quelle polarisationsverschränkter Photonenpaare

Das Konzept der Verschränkung findet nicht nur in der Kryptographie und anderen Kommunikationsprotokollen Anwendung, sondern stellt eine wichtige Resource in der gesamten Quanteninformationstheorie dar. Die Wahl von Photonen als Informationsträger erweist sich speziell in der Nachrichtenübermittlung als besonders geeignet, da sie das physikalische System mit der schnellstmöglichen Übertragungsgeschwindigkeit darstellen und darüber hinaus mittels Glasfaserleitungen auf einfache Weise zuverlässig versandt werden können. Dieses Kapitel behandelt daher die Entwicklung einer kompakten Quelle zur Erzeugung polarisationsverschränkter Photonenpaare durch spontane parametrische Fluoreszenz. Es beschreibt ausgehend von den zugrundeliegenden theoretischen Konzepten die experimentelle Implementierung und Umsetzung sowie die erzielten Resultate. Zum Abschluß dieses Teils wird die Quelle zur eingehenderen Untersuchung quantenmechanischer Korrelationen verwendet.

2.1 Theorie

2.1.1 Spontane parametrische Fluoreszenz

Tritt ein elektromagnetisches Feld in Wechselwirkung mit einem dielektrischen Medium erzeugt es elektrische Dipolmomente deren makroskopische Summe eine Polarisationsdichte $\vec{P}$ ergibt. In einem anisotropen[1] Kristall ergibt sich folgende Beziehung zwischen

[1] Die Beziehung zwischen $\vec{E}$ und $\vec{P}$ ist abhängig von der Richtung von $\vec{E}$.

der Polarisationsdichte und dem eingestrahlten elektrischen Feld $\vec{E}$ [25]:

$$P_i = \epsilon_0 \sum_j \chi_{ij}^{(1)} E_j + 2 \sum_{jk} \chi_{ijk}^{(2)} E_j E_k + 4 \sum_{jkl} \chi_{ijkl}^{(3)} E_j E_k E_l + ..., \tag{2.1}$$

Mit $i, j, k, l, = 1, 2, 3$ und der Vakuumdielektrizitätskonstante ϵ_0; $\chi_{ij}^{(1)}$ ist der elektrische Suszeptibilitätstensor des Mediums und $\chi_{ijk}^{(2)}, \chi_{ijkl}^{(3)}$ dessen Entsprechungen für nichtlineare Effekte zweiter und dritter Ordnung.

Der Beitrag von $\chi_{ijk}^{(2)}$ zu $\vec{P}$ ist typischer Weise um zehn Größenordnungen geringer als der des linearen Terms. Daher wird er für schwache Felder für gewöhnlich vernachlässigt. Unter der Wechselwirkung eines starken Pumpfeldes der Frequenz ω_p mit dem Kristall führt er jedoch zur Erzeugung zweier neuer Felder der Frequenzen ω_e und ω_o. Im Teilchenbild der zweiten Quantisierung entspricht dies der spontanen Umwandlung eines Pumpphotons der Energie $\hbar\omega_p$ und dem Impuls $\hbar\vec{k}_p$ in zwei Photonen mit den Energien und Impulsen $\hbar\omega_e$, $\hbar\vec{k}_e$ und $\hbar\omega_o$, $\hbar\vec{k}_o$, üblicherweise Signal- und Idlerphoton genannt. Dieser Prozeß ähnelt dem, aus der klassischen Elektrodynamik bekannten Vorgang der Drei-Wellen-Mischung bzw. der parametrischen Verstärkung, bei dem zwei Felder verschwindender Intensität ω_1 und ω_2 in einem nichtlinearen Medium durch die Anwesenheit eines starken Pumpfeldes ω_3 ($\omega_1 + \omega_2 \leq \omega_3$) verstärkt werden. Im Gegensatz dazu kann er aber wegen seines spontanen Auftretens, d.h. ohne die a priori Anwesenheit eines zusätzlichen schwachen Feldes, nur quantenmechanisch verstanden werden. Auf eine detaillierte quantenoptische Herleitung wird in dieser Arbeit verzichtet. Der interessierte Leser sei auf die ausreichend vorhandene Fachliteratur verwiesen (siehe z.B. [26]).

In beiden Prozessen gilt Energie- und Impulserhaltung:

$$\omega_p = \omega_e + \omega_o \tag{2.2a}$$

$$\vec{k}_p = \vec{k}_e + \vec{k}_o \tag{2.2b}$$

Entsprechend der Polarisation der Fluoreszenzphotonen unterscheidet man zwei Arten der spontanen parametrischen Fluoreszenz:

- **Typ I**: Der Pumpstrahl ist bezüglich des einachsigen Kristalls ausserordentlich[2] polarisiert, während die Fluoreszenzphotonen ordentlich polarisiert sind.
- **Typ II**: Der Pumpstrahl ist ebenfalls außerordentlich, die Fluoreszenzphotonen jedoch jeweils ordentlich bzw. außerordentlich, d.h. orthogonal zu einander polarisiert.

[2]Die Begriffe „ausserordentlich“ und „ordentlich“ polarisiert entsprechen hier der allgemein üblichen Nomenklatur für uniaxiale optische Kristalle. Ausserordentlich polarisiert bedeutet, der Polarisationsvektor liegt in der Ebene, die von optischer Achse und Wellenvektor $\vec{k}$ aufgespannt wird, während im ordentlichen Fall der Polarisationsvektor senkrecht zu dieser Ebene steht.

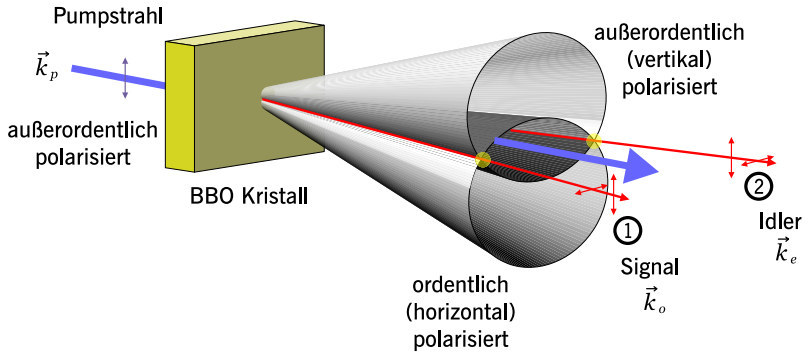


Abbildung 2.1: spontane parametrische Fluoreszenz vom Typ II. Die orthogonal zueinander polarisierten Fluoreszenzphotonen werden entlang zweier Kegel emittiert. Die entlang der Schnittgeraden emittierten Photonen sind nicht eindeutig einem der beiden Kegel zuzuordnen.

Die Art des Erzeugungsprozeßes legt bereits nahe, daß die paarweise generierten Photonen starke Korrelationen bezüglich Entstehungszeitpunkt sowie Energie und Impuls aufweisen. Bei der Fluoreszenz des Typs II kommt darüberhinaus eine Polarisationskorrelation hinzu, was diese Art des Prozesses zur bevorzugten Wahl für die Erzeugung einer Polarisationsverschränkung macht.

Räumlich betrachtet werden Signal- und Idlerphoton entlang zweier Kegel emittiert. Je nach Lage der Kegelachsen zueinander spricht man vom kollinearen bzw. nichtkollinearen Fall. Im ersteren berühren sich die Kegel entlang einer Gerade. Im letzteren hängt der Winkel zwischen den Kegelachsen sowie der Öffnungswinkel der Kegel vom Winkel θ_p ab, den der Pumpwellenvektor $\vec{k}_p$ mit der optischen Achse des Kristalls einschließt. In dieser Arbeit wurde die nichtkollineare entartete Fluoreszenz realisiert, siehe Abbildung 2.1. Die Fluoreszenzphotonen haben dieselbe Wellenlänge und die Emissionskegel schneiden sich entlang zweier Geraden die einen Winkel $2\Phi_{e,o}$ bilden. Die Tangentialebenen an die Kegel entlang der Schnittgeraden kreuzen in diesem Fall einander senkrecht [27]. Die entlang der Schnittgeraden emittierten Moden können nicht eindeutig einem der beiden Kegel zugeordnet werden. Damit ist auch Ihre Polarisation nicht klar zu bestimmen, da die Polarisationsinformation von der Modenzugehörigkeit (Signal s oder Idler i) entkoppelt wird.

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|s,H\rangle|i,V\rangle + e^{i\phi}|s,V\rangle|i,H\rangle\right) = \\ = \frac{1}{\sqrt{2}}\left(|s\rangle|i\rangle\right)\left(|H\rangle|V\rangle + e^{i\phi}|V\rangle|H\rangle\right) \quad (2.3)$$

Es liegt lediglich eine strikte Antikorrelation vor. Ist ein Photon horizontal, so ist das andere vertikal polarisiert und vice versa. Dies resultiert folglich idealerweise in dem

maximal verschränkten Zustand

$$|\,\psi\,\rangle = \frac{1}{\sqrt{2}}\left(|\,H\,\rangle|\,V\,\rangle + e^{i\phi}|\,V\,\rangle|\,H\,\rangle\right). \tag{2.4}$$

Für einen anisotropen Kristall ist jedoch zu beachten, dass aufgrund der Doppelbrechung die ordentlich und außerordentlich polarisierten Fluoreszenzphotonen unterschiedliche Brechungsindizes erfahren und sich deshalb innerhalb des Kristalls mit verschiedenen Geschwindigkeiten in unterschiedliche Richtungen bewegen. Man spricht von einem longitudinalen und einem transversalen „walk-off“. Beides kann im Experiment zu einer Unterscheidbarkeit der beiden Moden und damit zum Verlust der Verschränkung führen. Der transversale „walk-off“ führt zu einer Aufweitung des ordentlich polarisierten Strahls. Ist diese größer als der Pumpstrahldurchmesser kommt es zu einem inkohärenten Überlappen der beiden Konversionsmoden entlang der Schnittgeraden. Der longitudinale „walk-off“ führt zu einer relativen zeitlichen Verzögerung δt der Fluoreszenzmoden zueinander. Sie beträgt maximal für am Kristallanfang erzeugte Photonen bei senkrechtem Einfall des Pumpstrahls:

$$\begin{aligned}\delta t &= \left|\, \tfrac{n_o d}{c} - \tfrac{n(\theta_p) d \cos(\theta_p - \theta_e)}{c} \,\right| \\ &= \frac{d}{c} \cdot \left|\, n_o - n(\theta_p)\cos(\theta_p - \theta_e) \,\right| \end{aligned} \tag{2.5}$$

für eine Kristalldicke d und [25]

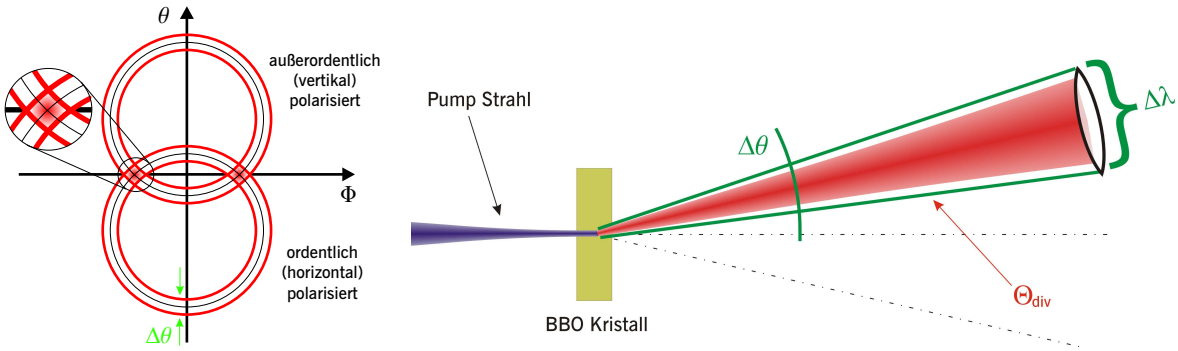
$$\frac{1}{n^2(\theta_p)} = \frac{\cos^2(\theta_p)}{n_o^2} + \frac{\sin^2(\theta_p)}{n_e^2} \tag{2.6}$$

sowie θ_e dem Winkel den der Wellenvektor k_e des außerordentlichen Strahls mit der optischen Achse einschließt. Ist δt größer als die Kohärenzzeit τ_c sind ordentlicher und außerordentlicher Strahl durch den Detektionszeitpunkt zu unterscheiden. Eine Kompensation dieser Effekte durch zusätzliche Kristalle ist allerdings möglich (siehe Abschnitt 2.2.2 sowie [28]).

2.1.2 Modenanpassung

Wie aus vorangegangenem Abschnitt hervorgeht, ist es notwendig die Fluoreszenzphotonen entlang der Kegelschnittgeraden auszuwählen um polarisationsverschränkte Paare zu erhalten. Die in [29] vorgeschlagene Modenanpassung ist eine Technik, die eine möglichst effiziente Kopplung dieser Photonen in single-mode Lichtwellenleiter[3] bei gleichzeitiger spektraler Selektion garantieren soll. Da sie entscheidenden Einfluß

[3]Die Verwendung von single-mode Fasern garantiert eine wohldefinierte räumliche Mode und die folgenden Betrachtungen sind lediglich hierfür sinnvoll.



(a) Die Annahme einer runden Gaußmode ist gerechtfertigt, da sich die Tangentialebenen an die Kegel entlang der Schnittgeraden im entarteten Fall senkrecht schneiden.

(b) Einer bestimmten spektralen Breite $\Delta\lambda$ entspricht ein Winkelbereich $\Delta\theta$. Für die Einkopplung in eine single-mode Faser folgt der Divergenzwinkel Θ_{div} der Gaußschen Mode aus $\Delta\theta$.

Abbildung 2.2: Modenanpassung

auf verschiedene Designparameter des experimentellen Aufbaus hat, soll sie hier kurz beschrieben werden (siehe [27, 29]).

Im nicht-kollinearen entarteten Fall werden die Fluoreszenzphotonen der Wellenlänge $\lambda \pm \Delta\lambda/2$ (FWHM[4]) ausgehend vom Erzeugungsort im Kristall in einen Winkelbereich $\theta \pm \Delta\theta/2$ emittiert. Der Zusammenhang zwischen spektraler Breite $\Delta\lambda$ und ausgeleuchtetem Winkelbereich $\Delta\theta$ führt somit die spektrale Selektion auf eine Begrenzung des einzukoppelnden Winkelbereichs zurück.

$$\Delta\theta = \frac{d\theta}{d\lambda}\Delta\lambda \tag{2.7}$$

Da sich die Emissionskegel senkrecht schneiden (siehe Abschnitt 2.1.1) kann für die spektrale Verteilung der Fluoreszenzmoden eine Rotationssymmetrie angenommen werden, siehe Abbildung 2.2(a). Berücksichtigt man ferner, daß sich ausschließlich eine TEM_{00} Mode in einem single-mode Wellenleiter ausbreiten kann, läßt sich für die entlang der Schnittgeraden einzukoppelnden Zielmoden annähernd folgende Gaußsche Intensitätsverteilung voraussetzen:

$$I(\theta) \propto \exp(-2(\theta/\Theta_{div})^2), \tag{2.8}$$

[4]FWHM steht für „*Full Width at Half Maximum*“ und ist die Breite, bei der die spektrale Verteilung die Hälfte des Maximalwertes erreicht.

wobei Θ_{div} der Divergenzwinkel des Gaußschen Strahls ist, für den gilt:

$$\begin{aligned}\Theta_{div} &= \frac{\Delta\theta}{\sqrt{2\ln(2)}} \\ &= \frac{1}{\sqrt{2\ln(2)}}\frac{d\theta}{d\lambda}\Delta\lambda \end{aligned} \tag{2.9}$$

Die Strahltaille $w_0 = \lambda/(\pi\Theta_{div})$ ist im Konversionskristall lokalisiert, da der Pumpstrahl näherungsweise als ebene Welle angenommen werden soll (Abbildung 2.2(b)). Bildet man die so festgelegten Moden mittels Linsen in eine single-mode Glasfaser ab, werden lediglich Photonen selektiert, die in der Überlappregion von Pumpstrahl und Zielmode entstehen. Dies legt nahe, die Pumpleistung möglichst in diesem Bereich zu konzentrieren. Daher ist das Ziel der Modenanpassung eine Anpassung der Strahltaille des Pumpstrahls w_p an die der gewünschten Zielmoden w_0.

$$w_p \stackrel{!}{=} w_0 \tag{2.10}$$

2.2 Implementierung

Im Laufe der vergangenen Jahre hat sich die spontane parametrische Fluoreszenz als Standardmethode zur Erzeugung verschränkter Photonenpaare etabliert. Sie stellt ein wichtiges Instrument vieler Anwendungen in verschiedenen Gebieten der experimentellen Quanteninformationstheorie dar. Mit dem Einsatz in diversen Bereichen sind jedoch auch unterschiedliche An- und Herausforderungen an eine Quelle verschränkter Photonen verbunden. Für Kommunikationszwecke via Glasfasern über größere Distanzen beispielsweise, sind die Wellenlängen um $\lambda = 1,31\,\mu m$ und $1,55\,\mu m$ besonders geeignet, da Lichtwellenleiter in diesen spektralen Bereichen sehr geringe Absorption besitzen. Für diese Wellenlängen wurde bereits eine kompakte Quelle entwickelt, die eine rote Laserdiode als Pumpquelle verwendet [30, 31]. Ein Nachweis einzelner Fluoreszenzphotonen erweist sich allerdings in diesem Fall als schwierig, da die einzig nutzbaren Detektoren, Germanium oder InGaAs/InP Halbleiter, niedrige Effizienz und hohe Dunkelzählraten aufweisen. Hingegen existieren im nahen Infrarotbereich zwischen $\lambda = 600\,\text{nm}$ und $\lambda = 900\,\text{nm}$ kommerziell erhältliche Siliziumdetektoren mit hohen Effizienzen von bis zu 70 % und niedrigen Dunkelzählraten. Die Erzeugung von Fluoreszenzphotonen im nahen Infraroten erfordert allerdings eine Pumpwellenlänge im Blauen bis Ultravioletten mit einer Wellenlänge unter $\lambda = 450\,\text{nm}$. Dies führte bisher zur Verwendung unhandlich großer Ionen-Laser mit hohen Anschaffungs- und Betriebskosten, was die Verwendung polarisationsverschränkter Photonen außerhalb einer Laborumgebung unmöglich machte. Jüngste Entwicklungen in der Halbleiterindustrie ermöglichen aber mittlerweile den Einsatz blauer und violetter Gallium-Nitride basierter Laserdioden mit optischen Ausgangsleistungen von bis zu 50 mW. Eine Aufgabenstellung dieser Arbeit

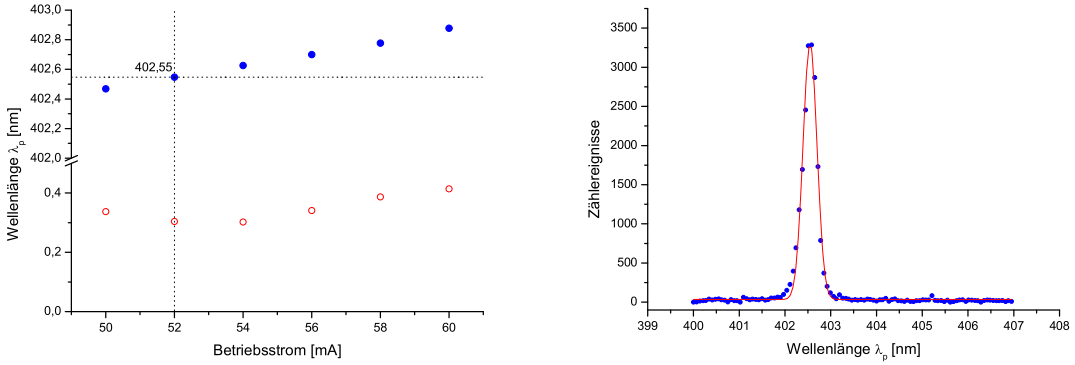
war daher durch die Verwendung einer blauen Laserdiode eine möglichst kompakte und billige Quelle für Fluoreszenzphotonen im Wellenlängenbereich um $\lambda = 800\,\mathrm{nm}$ zu entwickeln, die in ihrer Effizienz mit herkömmlichen Ionen-Laser Systemen vergleichbar ist [32]. Dies stellt den logisch nächsten Schritt dar, nachdem bereits frequenzverdoppelte rote Laserdioden erfolgreich eingesetzt wurden um eine vollständig festkörperbasierte Quelle im Infrarotbereich zu bauen [28].

2.2.1 Der Pumplaser - eine UV Laserdiode

Die im folgenden verwendete blaue Laserdiode vom Typ NDHV310ACA der Firma Nichia mit einer nominalen Wellenlänge von $\lambda = 403\,\mathrm{nm}$ und einer optischen Ausgangsleistung von 30 mW wurde in einem Aluminiumgehäuse zusammen mit einer asphärischen Kollimationslinse einer Brennweite von $f = 8\,\mathrm{mm}$ montiert. Ein elektronischer Regler hält mittels eines Peltierelements die Betriebstemperatur konstant bei $20\,^\circ\,\mathrm{C}$. Die tatsächlich abgestrahlte Wellenlänge und Leistung ist abhängig vom Versorgungsstrom. Deren Abhängigkeit für verschiedene Betriebsströme zwischen 40 und 60 mA zeigt Abbildung 2.3(a). Die einzelnen Datenpunkte wurden durch einen Gaußfit an die mit einem Spektrometer der Firma Ocean Optics (PC2000) aufgenommenen Spektren ermittelt. Bei diesem Gerät wird das zu analysierende Licht in eine Glasfaser eingekoppelt. Am anderen Ende der Faser tritt es durch einen $10\,\mu m \simeq 10\,\mathrm{px}$ breiten Spalt, trifft auf ein selbstfokussierendes Gitter (2400 Linien/mm) für einen Einsatzbereich zwischen 330 und 450 nm und wird auf ein lineares Si-CCD-Array (Sony ILX511) mit 2048 Pixeln abgebildet. Mit diesen Spezifikationen besitzt das Spektrometer eine Auflösung von $\sim 0,2 - 0,3\,\mathrm{nm}$ (FWHM) [33].

Fluktuationen in der Wellenlänge für einen festen Stromwert liegen außerhalb der Meßgenauigkeit und können vernachlässigt werden. Alle im Laufe der vorliegenden Arbeit vorgestellten Experimente wurden bei 52 mA durchgeführt. Das Spektrum für diesen Fall zeigt Abbildung 2.3(b). Die optische Ausgangsleistung steigt linear mit dem Versorgungsstrom an. Das Maximum liegt bei 24 mW (60 mA). Die nominalen 30 mW konnten auch bei 62 mA nicht erreicht werden. Um den Halbleiterchip der Diode nicht zu beschädigen, wurde selbst von einem sehr kurzen Testbetrieb mit über 62 mA abgesehen. Bei einer typischen Stromversorgung von 52 mA beträgt die abgestrahlte optische Leistung 12,23 mW. Den Verlauf für verschiedene Ströme zeigt Abbildung 2.4.

Die Leistung wurde über die durch den Fotostrom an einem Meßwiderstand abgefallene Spannung einer Fotodiode (Fabrikat Thorlabs DET110) gemessen.



(a) Abhängigkeit der zentralen Pumpwellenlänge λ_p (●), sowie der spektralen Breite (○) vom Versorgungsstrom.

(b) Gemessene Wellenlänge (●) $\lambda_p = 402,55\,\text{nm}$ und spektralen Breite $w = 0,3\,\text{nm}$ bei einem Versorgungsstrom von 52 mA. Gaußfit (–): $y(\lambda) = y_0 + A\exp(-\frac{(\lambda-\lambda_p)^2}{2w^2})$.

Abbildung 2.3: Pumplaserspektrum

2.2.2 Designparameter und Experimenteller Aufbau

Aus den Kapiteln 2.1.1 und 2.1.2 geht bereits hervor, in welche Hauptbestandteile sich eine Quelle zur Erzeugung polarisationsverschränkter Photonen mittels spontaner parametrischer Fluoreszenz gliedert. Es bedarf eines Linsensystems, um den Pumpstrahl unter Beachtung der Modenanpassungsbedingung zu fokussieren sowie des Konversionskristalls mit einer Kompensation für den „walk-off“ und einer Optik zum Einkoppeln der Fluoreszenzphotonen. Der hier realisierte Aufbau verwendet einen 2 mm dicken BBO ($\beta - BaB_2O_4$) Konversionskristall, der bereits für die Phasenanpassung des Typ II geschnitten ist. Das bedeutet der k-Vektor des Pumpstrahls $\vec{k}_p$ bildet bei senkrechtem Lasereinfall einen Winkel θ_p von $42,13\,^\circ$ mit der optischen Achse. Die Kompensation des „walk-offs“ erfolgt durch eine $\frac{\lambda}{2}$-Platte unter $45\,^\circ$, die die Rollen von ordentlichem und außerordentlichem Strahl vertauscht, gefolgt von je einem BBO-Kristall der halben Dicke in jedem der beiden optischen Wege. Für eine Pumpwellenlänge $\lambda_p = 402,6\,\text{nm}$ ergibt sich im entarteten Fall für die Fluoreszenzphotonen eine Wellenlänge von $\lambda = 805,2\,\text{nm}$. Daraus folgt mit den Dispersionseigenschaften von BBO der Ausdruck für $\frac{d\theta}{d\lambda} = 0,045\,^\circ/\text{nm}$. Da eine spektrale Breite der Zielmoden $\Delta\lambda = 6\,\text{nm}$ angestrebt wird, erhält man für deren Divergenzwinkel mit Gleichung 2.9 $\Theta_{div} = 0,23\,^\circ$ und damit für die Strahltaille $w_0 = 72\,\mu\text{m}$.

Um den Pumplaser auf diese Größe zu fokussieren (siehe Gleichung 2.10) bildet eine konkav-sphärische Linse mit einer Brennweite von $f = -25\,\text{mm}$ zusammen mit der Kollimationslinse ($f = 8\,\text{mm}$) im Gehäuse der Diode ein Galileo Teleskop. In dieser Konfiguration befindet sich die Strahltaille in einem Abstand von 230 mm hinter dem

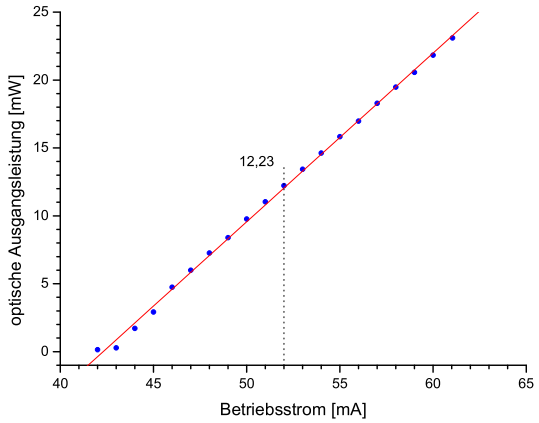


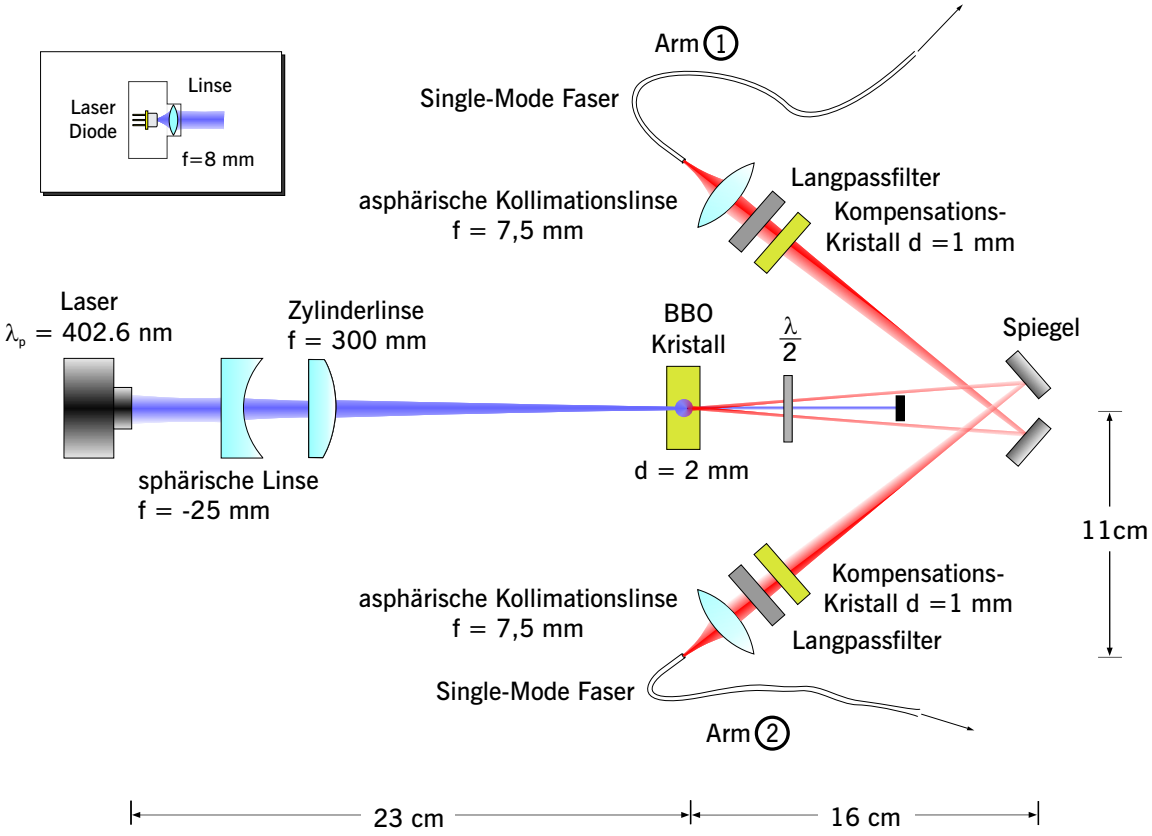
Abbildung 2.4: Optische Ausgangsleistung (•) des Pumplasers in Abhängigkeit des Versorgungsstroms. Die Abhängigkeit ist annähernd linear (–)

Gehäuse. Gemäß den Bedingungen aus Kapitel 2.1.2 wird an dieser Stelle der Kristall positioniert.

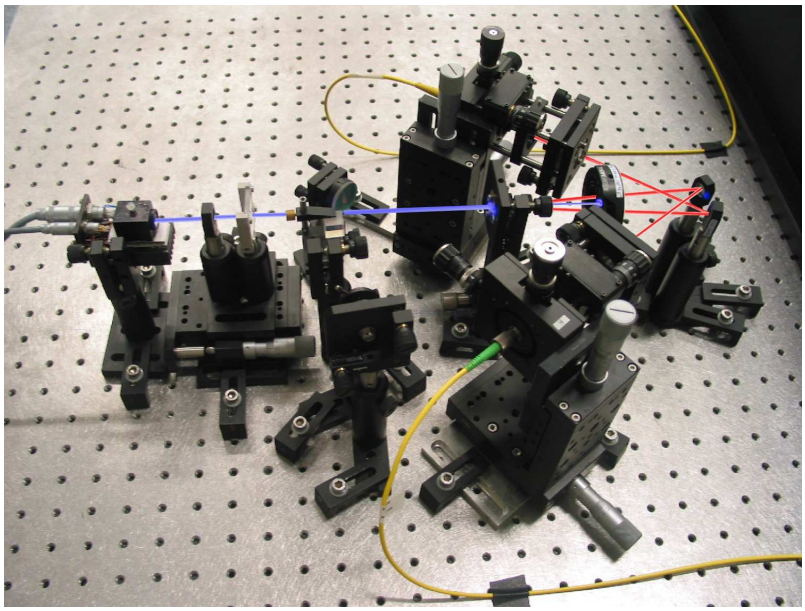
Die Laserdiode ist so ausgerichtet, dass ihre intrinsische Polarisation, wie für die Phasenanpassung des Typ II notwendig, außerordentlich im Bezug auf die Lage der optischen Achse des Konversionskristalls orientiert ist. Da Laserdioden im Gegensatz zu Ionenlasern kein rundes, aber typischerweise elliptisches Strahlprofil besitzen, muß dies durch eine zusätzliche Zylinderlinse ($f = 300\,\mathrm{mm}$) kompensiert werden.

Im entarteten Fall bilden die Schnittgeraden der Emissionskegel einen Winkel von $6\,^\circ$. Um die Photonen, die unter diesem Winkel emittiert werden in Single-Mode Fasern zu koppeln, werden asphärische Linsen der Brennweite $f = 7,5\,\mathrm{mm}$ mit einer numerischen Apertur von $0,30$ verwendet. Der Abstand vom Kristall zu den Kopplungslinsen beträgt 365 mm und ist durch die Größe der bild- und gegestandsseitigen Strahltaille vorgegeben. Diese sind zum einen $w_p = 72\,\mu\mathrm{m}$ des Pumpstrahls und $w_f = 2,6\,\mu\mathrm{m}$, die Größe, die für die Kopplung in den Faserkern der Single-Mode Faser erforderlich ist. Langpassfilter in beiden Armen verhindern, dass ultraviolettes Streulicht ebenfalls in die Glasfasern gelangt.

Die Wegstrecke von 365 mm wird mittels zweier Spiegel gefaltet. Dies ermöglicht eine kompaktere Bauweise. Der gesamte Abstand von der Pumpdiode bis zu den Spiegeln beträgt somit lediglich 390 mm. Würde man den kompletten Aufbau in eine Box integrieren wollen, würde diese in etwa eine Fläche von 400 x 600 mm einnehmen. (siehe Abbildung 2.5(a) und 2.5(b).)



(a) Schematische Darstellung des Aufbaus der Quelle.



(b) Foto des Aufbaus.

Abbildung 2.5: Versuchsaufbau Quelle

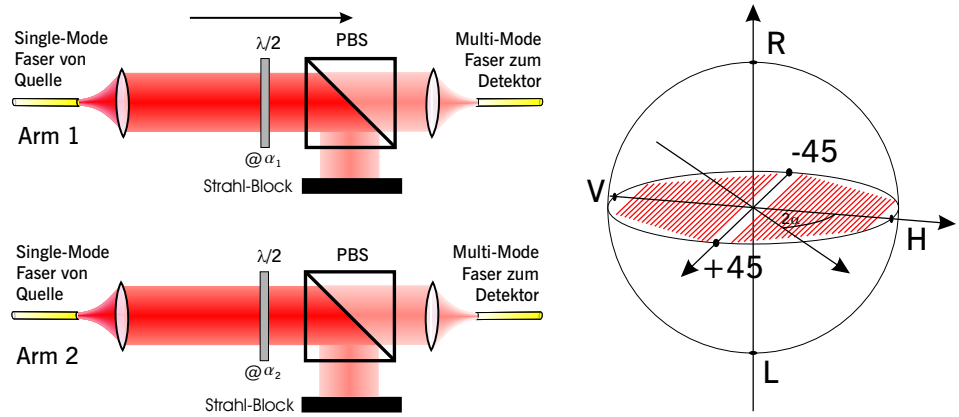
2.2.3 Detektion und Polarisationsanalyse

Die bei der spontanen parametrischen Fluoreszenz paarweise emittierten Photonen müssen nachgewiesen und hinsichtlich ihrer Polarisation untersucht werden. Die Detektion erfolgt mittels passiv gequenchter fasergekoppelter[5] Silizium-Avalanche-Photo-Dioden (Si-APDs) vom Typ C30902S der Firma Perkin-Elmer. Die APDs sind in ein selbstgebautes Modul integriert. Sie befinden sich in einem Aluminiumblock der mit Hilfe eines Peltierelements und einer Regelelektronik auf einer konstanten Temperatur von $-23\,^\circ$C gehalten wird. Dies reduziert die Dunkelzählrate auf ca. 700 Hz und garantiert eine konstante Durchbruchspannung. Bei einer Betriebsspannung die 17 Volt über der Durchbruchspannung liegt beträgt die Detektionseffizienz in etwa 36%. Eine Zusammenstellung verschiedener im Hinblick auf APDs relevanter Parameter und deren Zusammenhänge findet sich im Anhang A.2. Die Signalverarbeitung innerhalb des Moduls wird in ECL-Logik durchgeführt. Der Ausgang liefert allerdings einen NIM-Puls. Um Koinzidenzen von zwei Photonen eines Paares zu registrieren werden die NIM-Pulse beider APDs in einem Und-Gatter[6] zusammengeführt. Das Koinzidenzzeitfenster ist dabei durch die Pulslänge vorgegeben. Diese beträgt 10 ns.

Um eine Polarisationsanalyse durchzuführen, werden die Photonen aus den single-mode Fasern ausgekoppelt, durch eine $\frac{\lambda}{2}$-Platte und einen polarisierenden Strahlteilerwürfel (PBS) gesendet und anschließend in die multi-mode Fasern der Detektoren eingekoppelt (siehe Abbildung 2.6(a)). Die Effizienz der Aus- und Einkopplung beträgt in beiden Armen 87 %. Eine Drehung der $\frac{\lambda}{2}$-Platte um den Winkel α ermöglicht in Kombination mit dem PBS eine Untersuchung aller Polarisationen, die in der Äquatorialebene der Poincaré-Sphäre liegen (Abbildung 2.6(b)). Dies ist leicht zu verstehen, verfolgt man den Weg des Photons von der Detektorseite rückwärts. Das Photon kann im PBS nur transmittiert werden, wenn seine Polarisation horizontal ist. Das so polarisierte Photon wird an dem Wellenplättchen in eine andere Polarisation rotiert. Da die Phasenverzögerung jedoch unabhängig vom eingestellten Winkel stets π beträgt, kann die neue Polarisation lediglich linear und nicht zirkular oder elliptisch sein. Dies entspricht einer Lage in der Äquatorialebene der Poincaré-Sphäre. Diese Betrachtungen müssen analog in umgekehrter Reihenfolge gelten. Welche Polarisation man dabei für welchen Rotationswinkel analysiert, läßt sich einfach in der Matrixdarstellung der Wellenplatten und Polarisationsvektoren berechnen (siehe Anhang A.1.1 und A.1.2.3).

[5] Bei den Glasfasern der Detektoren handelt es sich um multi-mode Fasern

[6] Eigentlich wird ein Oder-Gatter verwendet, aber in negativer Logik stellt ein Oder-Gatter das Äquivalent zu einem Und-Gatter in normaler Logik dar.



(a) Schematische Darstellung des Aufbaus zur Polarisationsanalyse.

(b) Äquatorialebene der Poincaré-Sphäre.

Abbildung 2.6: Polarisationsanalysator

2.3 Daten und Ergebnisse

Im vorangegangenen Kapitel wurde der Aufbau der Quelle in seinen Teilen beschrieben. Im folgenden werden nun die damit gewonnen Daten vorgestellt. Anhand der Spektren der Fluoreszenzphotonen wird geprüft, ob in der Tat der entartete Fall vorliegt. Desweiteren werden Zählraten in Abhängigkeit der optischen Ausgangsleistung des Pumplasers überprüft. Einen ersten Test für Verschränkung bildet die Aufnahme der Korrelationsfunktion in zwei Basen. Die Verschränkung wird durch die Verletzung von Bellungleichungen bestätigt und am Ende dieses Abschnitts werden die in [11] berechneten Schranken für quantale Korrelationen experimentell bestätigt.

2.3.1 Spektren und Zählraten

Das in Kapitel 2.2.1 beschriebene Spektrometer besitzt nicht die nötige Empfindlichkeit um Einzelphotonen nachzuweisen. Aus diesem Grund wird für die Aufnahme des Fluoreszenzphotonenspektrums ein selbstgebautes Gitterspektrometer verwendet, das als Eingang eine single-mode Faser[7] besitzt (siehe Abbildung 2.7). Die erste Beugungsordnung wird über einen Spiegel und eine Linse ($f = 10\,\mathrm{mm}$) in eine multi-mode Faser[8] abgebildet. Mit einer Gitterkonstante von 1200 Linien/mm, den verwendeten Fasern und den in Abbildung 2.7 gezeigten Abmessungen wird ein gemessenes Auflösungsvermögen von $0,6\,\mathrm{nm}$ (FWHM) erreicht. Als Referenz und Justierhilfe diente die $633,42\,\mathrm{nm}$ Li-

[7] Mode Field Diameter: $5,5\,\mu\mathrm{m}$
[8] Kerndurchmesser: $50\,\mu\mathrm{m}$

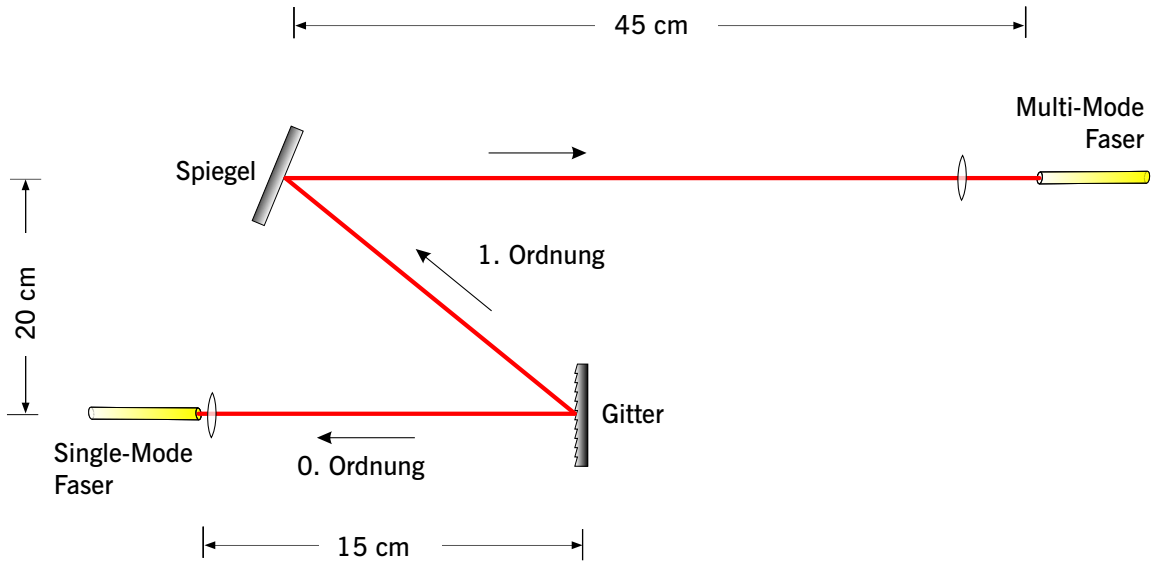


Abbildung 2.7: Gitterspektrometer. Wird an den Ausgang eine Avalanche-Photodiode angeschlossen, lassen sich mit entsprechender Integrationszeit Einzelphotonenspektren aufnehmen.

nie eines Helium-Neon Lasers. Die Effizienz[9] beträgt 18% bei einer Wellenlänge von $\lambda = 805\,\text{nm}$ gemessen mit einem abgeschwächten Justierlaser (siehe Anhang A.3). Schließt man an den multi-mode Faser Ausgang des Spektrometers eine Avalanche-Photo-Diode, läßt sich mit einer genügend großen Integrationszeit das Spektrum der Fluoreszenzphotonen aufnehmen. Durch wiederholtes Messen der Wellenlängen in beiden Armen in Abhängigkeit von der Kopplerposition, war es möglich die Quelle auf den entarteten Fall einzujustieren. Dabei zeigte sich eine starke Abhängigkeit der gemessenen Wellenlänge von der vertikalen Kopplerposition. Das erzielte Endergebnis zeigt Abbildung 2.8. Beide Photonen eines Paares besitzen annähernd die gleiche spektrale Verteilung um die entartete Wellenlänge von $805,2\,\text{nm}$ und sind lediglich um $0,22\,\text{nm}$ voneinander separiert. Ein Gaußfit an die gemessenen Daten ergibt in Arm 1 eine Wellenlänge von $805,47 \pm 0,05\,\text{nm}$ mit einer Breite von $6,03 \pm 0,14\,\text{nm}$ (FWHM) und in Arm 2 eine Wellenlänge von $805,25 \pm 0,21\,\text{nm}$ mit einer Breite von $6,24 \pm 0,56\,\text{nm}$ (FWHM). Die Integrationszeit für diese Messung betrug 60 Sekunden für jeden Datenpunkt. Hierfür stellt sich ein Offset bedingt durch die Detektordunkelzählrate von 44000 Ereignissen ein.

Sowohl für den praktischen Einsatz der Quelle in Experimenten oder Kryptographieanwendungen, als auch für den Vergleich mit herkömmlichen Ionenlasersystemen, sind die erreichbaren Zählraten ein entscheidendes Kriterium. Diese hängen in erster Linie von der optischen Ausgangsleistung des Pumplasers und der Qualität der Kopplung

[9] Anzahl der Zählereignisse im Spitzenwert des Spektrums dividiert durch Anzahl der Zählereignisse vor dem Eintritt in das Spektrometer.

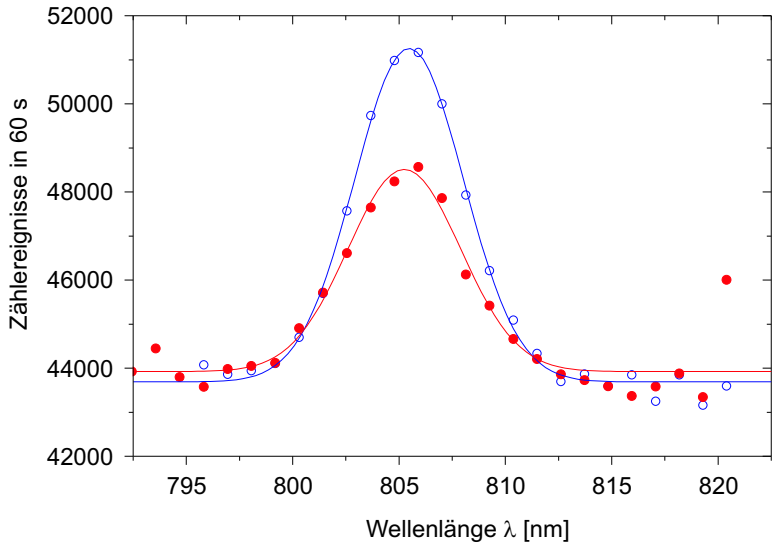


Abbildung 2.8: Spektrale Verteilung der Fluoreszenzphotonen. Beide Photonen eines Paares haben annähernd die gleiche Wellenlänge um 805,2 nm und sind lediglich um 0,22 nm separiert. Ein Gaußfit an die gemessenen Daten zeigt FWHM von $6,03 \pm 0,14$ nm in Arm 1 ($-\circ-$) und $6,24 \pm 0,56$ nm in Arm 2 ($-\bullet-$). Der Offset von 44000 Zählereignissen ist durch die Detektordunkelzählraten bedingt.

ab. Abbildung 2.9 zeigt daher den linearen Zusammenhang zwischen Pumpleistung und Einzelzählereignissen sowie Koinzidenzen im entarteten Fall. Die Steigung beträgt 220 Koinzidenzen pro Sekunde und mW. Ein Maß für die Güte der Kopplung ist das Verhältnis von Einzelzählereignissen zu Koinzidenzen. Es beträgt 0,19 und ist stabil über den gesamten Bereich der Pumpleistung. Zufällige Koinzidenzen sind für das verwendete Koinzidenzzeitfenster von 10 ns vernachlässigbar (siehe Anhang A.2.10). Bei der Aufnahme dieser Daten wurden die Multi-Mode Fasern der Detektoren direkt mit den Single-Mode-Fasern der Koppler verbunden.

2.3.2 Zustandsmessung und Verschränkung

2.3.2.1 Korrelationsfunktion

Als erster Test, ob die gemessenen Koinzidenzen in der Tat von verschränkten Paaren stammen, dient die Messung der Korrelationsfunktion in verschiedenen Basen. Hierbei wird der Aufbau aus Abbildung 2.6(a) verwendet, um die Koinzidenzraten in Abhängigkeit der analysierten Polarisation zu untersuchen.

Ziel ist die Erzeugung des Bell-Zustands $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle - |V\rangle|H\rangle)$. Wie sich leicht zeigen läßt, ist dieser Zustand invariant unter unitären Transformationen, wie

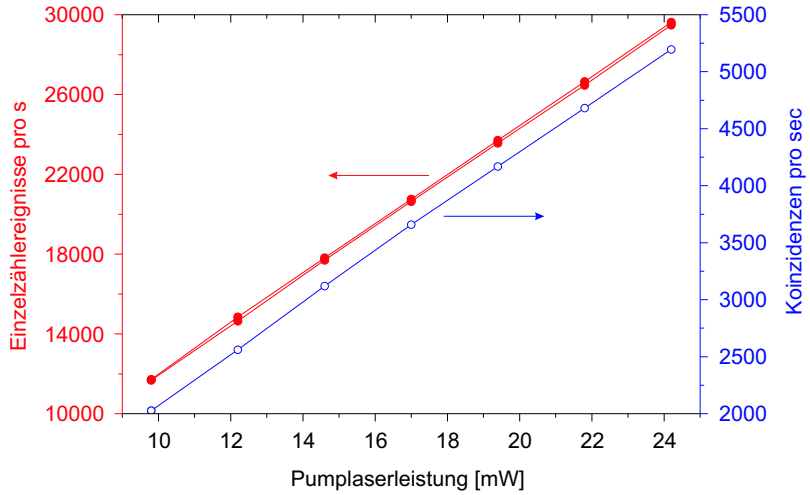


Abbildung 2.9: Einzelzählraten (– • –) und Koinzidenzen (– ∘ –) in Abhängigkeit von der optischen Ausgangsleistung des Pumplasers.

beispielsweise einem Basiswechsel. Es glit:

$$
\begin{aligned}
|\psi^-\rangle &= \frac{1}{\sqrt{2}}\left(|H\rangle|V\rangle - |V\rangle|H\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(|+\rangle|-\rangle - |-\rangle|+\rangle\right)
\end{aligned}
\tag{2.11}
$$

Emittiert die Quelle den Zustand $|\psi^-\rangle$, sollte folglich sowohl in der H/V- als auch in der $\pm 45\,^\circ$-Basis die Koinzidenzzählrate für eine Analyse derselben Polarisation in beiden Armen auf null abfallen bzw. im Falle orthogonaler Polarisation ein Maximum erreichen. Fixiert man die Analysatorstellung in Arm 2 (α_2) bei gleichzeitiger Variation in Arm 1 (α_1) schwankt die Koinzidenzzählrate zwischen diesen Extremen gemäß einer $\sin^2$ Kurve. Abbildung 2.10 zeigt die Koinzidenzzählrate aufgenommen in der H/V-Basis ($\alpha_2 = 0\,^\circ$) und $\pm 45\,^\circ$-Basis ($\alpha_2 = 22,5\,^\circ$). Deutlich zu sehen ist, daß in beiden Basen dasselbe Verhalten vorliegt, was für einen Produktzustand nicht möglich wäre. Die Visibility oder Sichtbarkeit, ein Maß für den Kontrast der Kurven, ist wie folgt definiert

$$
\text{Visibility} = \frac{\text{Zählratenmaximum} - \text{Zählratenminimum}}{\text{Zählratenmaximum} + \text{Zählratenminimum}}
$$

und beträgt $98,3 \pm 0,1\%$ (H/V) bzw. $94,3 \pm 0,2\%$.

2.3.2.2 Verletzung der CHSH-Ungleichung

Einen weiteren Test für Verschränkung stellt die Messung des CHSH-Operators dar. Dessen Erwartungswert ist für den Zustand $|\psi^-\rangle$ bei einem Winkel von $\pi/4$ maximal.

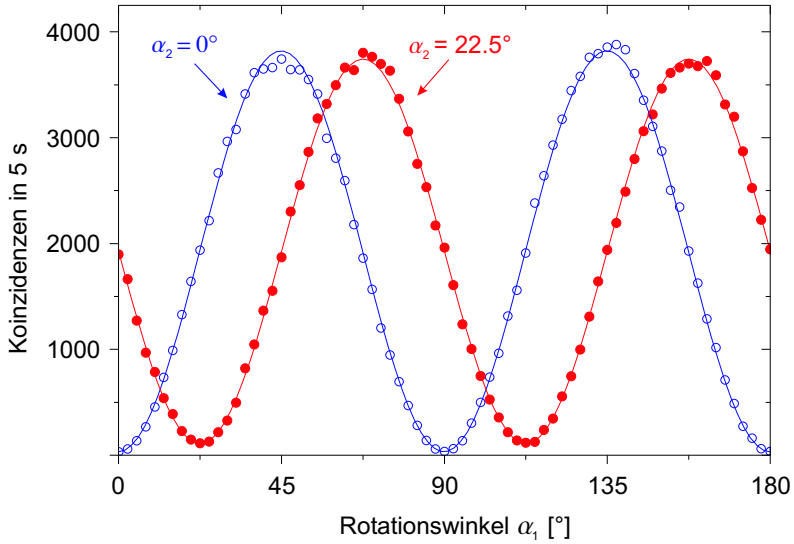


Abbildung 2.10: Polarisationskorrelationen der Photonen eines Paares gemessen in der H/V- (– ○ –) und ±45 °- (– ● –) Basis. Aus einem $\sin^2$-Fit ergibt sich die Visibility zu $98,3 \pm 0,1\%$ bzw. $94,3 \pm 0,2\%$.

Vergleicht man die Basisdarstellung der Operatoren $\hat{A}(\theta)$, $\hat{B}(\theta)$, $\hat{a}$, $\hat{b}(\theta)$ (siehe Anhang A.1.2.2) mit der von linearen Verzögerungsplatten (siehe Anhang A.1.2.3), sieht man, dass jeder der Operatoren durch eine $\frac{\lambda}{2}$-Platte realisiert werden kann. Für die Messung von $S_{qm} = \langle \mathbf{CHSH} \rangle$ wird folglich ebenfalls der Aufbau 2.6(a) verwendet. Hierbei ist jedoch zu beachten, dass nur ein Ausgang des polarisierenden Strahlteilers analysiert wird, entsprechend nur einem Meßresultat, beispielsweise assoziiert mit dem Ergebnis „+1“ für den jeweiligen Operator. Um den Erwartungswert vollständig bestimmen zu können, müssen aber beide möglichen Resultate für jeden Operator, sprich „+1“ *und* „-1“ aufgenommen werden. Dieses Problem kann durch die Verwendung orthogonaler Winkel gelöst werden. Einer Messung unter dem Winkel α im reflektierten, entspricht eine Messung unter dem Winkel $\alpha^{\perp}$ im transmittierten Arm. Dieses Verfahren ist vollständig äquivalent zu einer Analyse beider Ausgänge des PBS, erfordert aber mehr Messungen. Für den Erwartungswert eines Operators $\hat{O} = \hat{O}_1 \otimes \hat{O}_2$ implementiert durch die $\frac{\lambda}{2}$-Platten $\mathbf{lam2}(\alpha_1)$ in Arm 1 und $\mathbf{lam2}(\alpha_2)$ (siehe Anhang A.1.2.3) in Arm 2 ergibt sich der Erwartungswert zu:

$$\langle \hat{O} \rangle = \frac{C(\alpha_1, \alpha_2) + C(\alpha_1^{\perp}, \alpha_2^{\perp}) - C(\alpha_1, \alpha_2^{\perp}) - C(\alpha_1^{\perp}, \alpha_2)}{C(\alpha_1, \alpha_2) + C(\alpha_1^{\perp}, \alpha_2^{\perp}) + C(\alpha_1, \alpha_2^{\perp}) + C(\alpha_1^{\perp}, \alpha_2)}, \tag{2.12}$$

wobei $C(\alpha_1, \alpha_2)$ die Koinzidenzzählrate bei der Winkelstellung α_1 in Arm 1 und α_2 in Arm 2 ist. Unter Berücksichtigung aller vorherigen Betrachtungen ergibt sich für die Quelle der Erwartungswert des CHSH-Operators zu

$$S_{qm} = \langle \mathbf{CHSH} \rangle = -2,732 \pm 0,017 \tag{2.13}$$

bei einer Integrationszeit von 80 Sekunden für jede Winkeleinstellung. Das entspricht einer Verletzung des klassischen Limits $\mid S_{LHV} \mid \leq 2$ um 44 Standardabweichungen.

2.3.2.3 Zustandstomographie

In einem realen Experiment wird man nicht erwarten können, daß die Quelle einen reinen $|\psi^-\rangle$-Zustand emittiert. Vielmehr wird ein gemischter Zustand ρ_{exp} produziert, dessen Tomographie mittels des in [34] beschriebenen Verfahrens durchgeführt wird. Dabei werden 16 Polarisationsmessungen durchgeführt und die so gewonnenen Daten rechnerisch ausgewertet. Da hierfür auch Polarisationen außerhalb der Äquatorialebene der Poincarè-Sphäre analysiert werden müssen, wird in den Aufbau 2.6(a) zusätzlich in jeden Arm je eine $\frac{\lambda}{4}$-Platte hinzugefügt. Auf eine Darstellung der einzelnen Arbeitsschritte wird hier verzichtet. Deren ausführliche Beschreibung findet sich bereits in [34]. Es werden lediglich die Ergebnisse präsentiert, da sie im nächsten Abschnitt für theoretische Vorhersagen von Nutzen sind. (Der Vollständigkeit halber sei allerdings erwähnt, dass der lineare Rekonstruktionsansatz bereits eine physikalische Matrix ergibt, was eine Likelihood-Optimierung unnötig macht). Es gilt $\rho_{exp} = \mathrm{Re}[\rho_{exp}] + i\mathrm{Im}[\rho_{exp}]$ und Real- und Imaginärteil ergeben sich aus den gemessenen Daten zu:

$$\mathrm{Re}[\rho_{exp}] = \begin{pmatrix} 0,0064 & 0,0359 & -0,0302 & 0,0181 \\ 0,0359 & 0,5002 & -0,4906 & 0,0493 \\ -0,0302 & -0,4906 & 0,4842 & -0,0420 \\ 0,0181 & 0,0493 & -0,0420 & 0,0092 \end{pmatrix} \tag{2.14a}$$

$$\mathrm{Im}[\rho_{exp}] = \begin{pmatrix} 0 & -0,0368 & 0,0338 & 0,0058 \\ 0,0368 & 0 & -0,0703 & -0,0177 \\ -0,0338 & 0,0703 & 0 & 0,0467 \\ -0,0058 & 0,0177 & -0,0467 & 0 \end{pmatrix} \tag{2.14b}$$

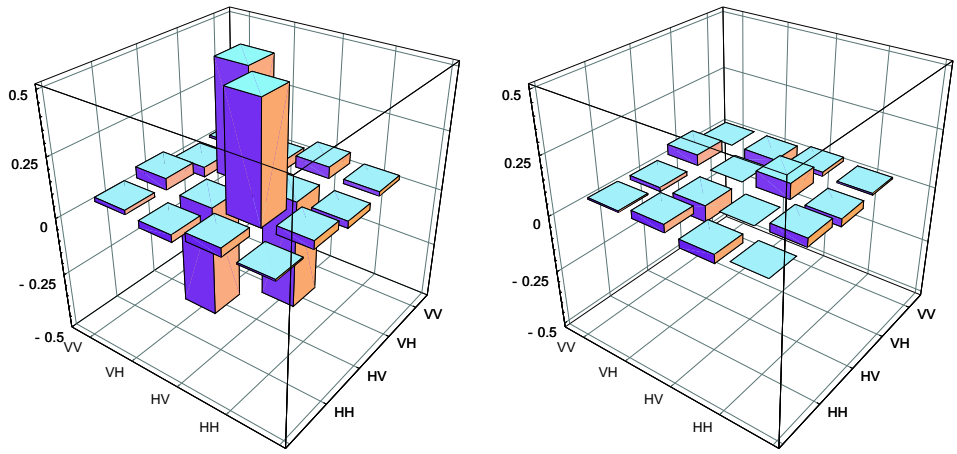
Eine graphische Darstellung zeigt Abbildung 2.11. Ein Maß dafür wie nahe der experimentell erzeugte dem theoretisch erwarteten Zustand $\rho_{theo} = |\psi^-\rangle\langle\psi^-|$ liegt, bildet der Überlapp oder die sogenannte Fidelity $\mathcal{F}$. Sie ist wie folgt definiert

$$\mathcal{F} = \mathrm{Tr}\left[(\sqrt{\rho_{theo}}\,\rho_{exp}\,\sqrt{\rho_{theo}})^{\frac{1}{2}}\right] \tag{2.15}$$

und beträgt für obige Daten $\mathcal{F} = 0,9914$. Dies ist unmittelbar plausibel, schreibt man ρ_{theo} ebenfalls in der Basisdarstellung

$$\rho_{theo} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0,5 & -0,5 & 0 \\ 0 & -0,5 & 0,5 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{2.16}$$

und vergleicht mit Ausdruck 2.14.



(a) Realteil. (b) Imaginärteil.

Abbildung 2.11: Dichtematrix des experimentell erzeugten Zustands ρ_{exp}

Der von der Quelle erzeugte Zustand ist folglich fast ein reiner $|\psi^-\rangle$-Zustand. Diese Behauptung wird durch den Wert der Purity $\mathcal{P} = \mathrm{Tr}[\rho_{exp}^2] = 0,9995$ bestätigt. Die Purity hat für reine Zustände den Wert 1 und für vollständig gemischte Zustände den Wert $1/N$, wobei N die Dimension des Zustandes ist; hier $N = 4$ [35]. Die Kenntnis der Dichtematrix erlaubt darüber hinaus eine weitere Überprüfung der Verschränkung mittels des PPT-Kriteriums („Positive Partial Transpose“) [36, 37]. Es sei daher an dieser Stelle ein kurzer Theorie-Einschub gestattet.

Definition 2 (Separierbarkeit und Verschränkung) *Es sei ρ eine Dichtematrix. ρ heißt separabel $\iff$ $\rho = \sum_i p_i \rho_{A,i} \otimes \rho_{B,i}$ mit $\sum_i p_i = 1$. Andernfalls heißt ρ verschränkt.*

Definition und Satz 3 (Peres-Horodecki) *Es sei ρ eine Dichtematrix und $(\rho^{T_A})_{m\mu,n\nu} := (\rho)_{n\mu,m\nu}$ sei die partiell Transponierte von ρ.*

ρ separabel $\Rightarrow \rho^{T_A} = \sum_i p_i \rho_{A,i}^T \otimes \rho_{B,i}$ mit $\sum_i p_i = 1$ und $\rho^{T_A} \geq 0$.

Es seien $\mathbb{H}_A$ und $\mathbb{H}_B$ zwei Hilberträume und $\mathbb{H}_{AB} = \mathbb{H}_A \otimes \mathbb{H}_B$ mit $\dim(\mathbb{H}_{AB}) = 2 \times 2 \vee 2 \times 3$.
$\rho \in \mathbb{H}_{AB} \wedge \rho^{T_A} \geq 0 \Rightarrow \rho$ ist separabel.

Da ρ_{exp} die Dimension $\dim(2 \times 2)$ besitzt, bietet obiges Theorem ein notwendiges und hinreichendes Kriterium für Verschränkung. Ist die partielle Transponierte von ρ_{exp} nicht positiv semi-definit, d.h. besitzt sie mindestens einen negativen Eigenwert, dann ist ρ_{exp} nicht separierbar und daher verschränkt. Die Eigenwerte λ_i von $\rho_{exp}^{T_A}$ sind

$$\lambda_i = \{0,5199; 0,5118; \mathbf{-0,4990}; 0,4673\} \tag{2.17}$$

Daraus läßt sich ferner der Grad der Verschränkung ermitteln, findet man ein Maß dafür wie stark ρ_{exp} das PPT-Kriterium verletzt. Eine solche Größe ist die Negativität $\mathcal{N}$ [38]. Sie ist der doppelte Absolutbetrag der Summe über alle negativen Eigenwerte [35]:

$$\mathcal{N}(\rho^{T_A}) = 2\max(0, -\lambda_{neg}) \tag{2.18}$$

$$\lambda_{neg} = \sum_{j \,|\, \lambda_j < 0} \lambda_j,$$

und ist maximal 1 bzw. minimal 0 für separierbare Zustände.
Für ρ_{exp} ist $\mathcal{N}(\rho_{exp}^{T_A}) = 0,9979$.

2.3.3 quantale Korrelationen: Wigner-Ungleichung und Schranken für CHSH

Im vorangegangenen Abschnitt wurde gezeigt, dass es möglich ist mit der präsentierten Quelle einen polarisationsverschränkten Zwei-Photonen-Zustand zu erzeugen. Im folgenden wird dieser Zustand dazu verwendet die Wignerparameter W und $\widetilde{W}$ mit und ohne die Anwesenheit eines Abhörers im Experiment zu vergleichen. Ferner wird mit Hilfe der Quelle systematisch die Schranke des CHSH-Operators rekonstruiert.

2.3.3.1 Wignerparameter

Um die Wignerparameter zu messen wird in analoger Weise zur Bestimmung von S_{qm} vorgegangen und wiederum Aufbau 2.6(a) verwendet. Es gilt folgende Wahrscheinlichkeiten zu bestimmen:

$$p(+,+|-30\,^\circ, 0\,^\circ)$$
$$p(+,+|0\,^\circ, 30\,^\circ)$$
$$p(-,-|0\,^\circ, 0\,^\circ)$$
$$p(+,+|-30\,^\circ, 30\,^\circ)$$

Die Zeichen „+“ bzw. „−“ stehen dabei für eine Detektion im transmittierten bzw. reflektierten Ausgang des PBS bei den jeweiligen Analysatorstellungen. So ergibt sich für den ersten Term

$$p(+,+|-30\,^\circ, 0\,^\circ) = \frac{C_{++}(-30\,^\circ, 0\,^\circ)}{C_{++}(-30\,^\circ, 0\,^\circ) + C_{+-}(-30\,^\circ, 0\,^\circ) + C_{-+}(-30\,^\circ, 0\,^\circ) + C_{--}(-30\,^\circ, 0\,^\circ)} \tag{2.19}$$

wobei beispielsweise $C_{+,-}(-30\,^\circ, 0\,^\circ)$ die Koinzidenzrate zwischen transmittiertem Ausgang des PBS in Arm 1 bei einer Analysatorstellung von $-30\,^\circ$ und reflektiertem Ausgang des PBS in Arm 2 bei einer Analysatorstellung von $0\,^\circ$ ist. Für die Verwendung von $\frac{\lambda}{2}$-Platten und nur einem Ausgang des PBS unter zu Hilfenahme der orthogonalen Winkelstellungen (siehe Abschnitt 2.3.2) bedeutet dies konkret:

$$p(+,+|-30\,^\circ, 0\,^\circ) = \frac{C_{++}(-15\,^\circ, 0\,^\circ)}{C_{++}(-15\,^\circ, 0\,^\circ) + C_{++}(-15\,^\circ, 45\,^\circ) + C_{++}(30\,^\circ, 0\,^\circ) + C_{++}(30\,^\circ, 45\,^\circ)} \tag{2.20}$$

In analoger Weise lassen sich alle vier Wahrscheinlichkeiten mit Hilfe von Koinzidenzmessungen bestimmen und man erhält die Wignerparameter

$$W = -0,115 \pm 0,010 \tag{2.21a}$$

$$\widetilde{W} = -0,111 \pm 0,011. \tag{2.21b}$$

Es sei nocheinmal daran erinnert, daß quantenmechanisch für eine maximale Verletzung $W = \widetilde{W} = -0,125 = W_{qm}^{max}$ gilt, während für lokal-realistische Theorien $W \geq 0$ und $\widetilde{W} \geq 0$ ist. Damit entspricht Ergebnis 2.21a und 2.21b einer Verletzung der Wignerungleichung um 11 bzw. 10,6 Standardabweichungen. Die Integrationszeit für die Messung betrug 5 Sekunden für jede Koinzidenzzählrate.

Nun soll gezeigt werden, dass ein möglicher Abhörer Eve, sofern er in der Lage ist an beiden Photonen des verschränkten Paares Messungen durchzuführen, einen Wignerparameter W herbeiführen kann, der sogar unterhalb der quantenmechanischen Schranke W_{qm}^{max} liegt, während der Wert von $\widetilde{W}$ positiv bleibt. Dafür wird eine sogenannte „intercept/resend“-Attacke simuliert, bei der Eve beide vom Sender stammenden Photonen in einer Polarisationsbasis mißt, und den gemessenen Zustand zum legitimen Empfänger weitersendet. Experimentell wird das durch jeweils einen Polarisator in jedem Arm des Analysators realisiert. Um in der Tat einen Wert von W zu erhalten, der unterhalb von W_{qm}^{max} liegt, bedarf es z.B. einer Polarisatorstellung von $0,4\pi \mathrel{\widehat{=}} 72\,^\circ$ in Arm 1 bzw. $0,6\pi \mathrel{\widehat{=}} 108\,^\circ$ in Arm 2 [22]. Tabelle 2.1 zeigt die Resultate für W und $\widetilde{W}$ bei verschiedenen Integrationszeiten.

Dies bestätigt innerhalb der Fehler die theoretische Erwartung von $W = -0,1995 < -0,125$ und $\widetilde{W} = 0,6186$. Wie bereits in Kapitel 1.3.2 erwähnt, findet sich eine ausführliche experimentelle Betrachtung von W und $\widetilde{W}$ für verschiedene Polarisatorstellungen in [23].

Integrationszeit [sec]	5	10	15	45
W	$-0,183$ $\pm 0,033$ $(5,6\,\sigma)$	$-0,198$ $\pm 0,025$ $(8\,\sigma)$	$-0,219$ $\pm 0,020$ $(11\,\sigma)$	$-0,201$ $\pm 0,012$ $(17\,\sigma)$
$\widetilde{W}$	$0,578$ $\pm 0,043$ $(13,6\,\sigma)$	$0,575$ $\pm 0,031$ $(18,3\,\sigma)$	$0,592$ $\pm 0,025$ $(24,1\,\sigma)$	$0,603$ $\pm 0,014$ $(41,7\,\sigma)$

Tabelle 2.1: Meßergebnisse für W und $\widetilde{W}$ für verschiedene Integrationszeiten bei Anwesenheit eines Abhörers.

2.3.3.2 Schranken des CHSH-Operator

In Abschnit 2.3.2 wurde für einen bekannten Zustand der Satz von Observablen, d.h. eine bestimmte Winkeleinstellung des Polarisationsanalysators gewählt, der für diesen speziellen Zustand eine maximale Verletzung der CHSH-Ungleichung versprach. Im folgenden Kapitel wird konträr vorgegangen. Für einen bestimmten Satz von Observablen wird der maximal verschränkte Zustand präpariert, der die CHSH-Ungleichung maximal verletzt. Dabei zeigt sich, daß für bestimmte Analysewinkel das quantenmechanische Maximum von $\mid S_{qm} \mid = 2\sqrt{2}$ nicht erreicht wird und darüberhinaus an speziellen Punkten sogar das Limit für lokal-realistische Theorien, $\mid S_{LHV} \mid \leq 2$, nicht überschritten werden kann. Das bedeutet, ist die Quantenmechanik korrekt, treten bestimmte Gruppen von Erwartungswerten dieser Observablen experimentell nicht auf.

Eine geeignete Menge maximal verschränkter Zustände für dieses Experiment ist die folgende Superposition der beiden Bellzustände $|\phi^+\rangle$ und $|\psi^-\rangle$:

$$|\varphi(\xi)\rangle = \cos(\xi)|\phi^+\rangle + \sin(\xi)|\psi^-\rangle. \tag{2.22}$$

Ausgehend von dem Zustand $|\psi^-\rangle$ läßt sich diese Superposition durch eine Unitäre Transformation angewandt auf ein Photon eines Paares erzielen:

$$|\varphi(\xi)\rangle = U(\xi) \otimes \mathbb{1}|\psi^-\rangle \tag{2.23}$$

mit

$$U(\xi) = \begin{pmatrix} \sin(\xi) & -\cos(\xi) \\ \cos(\xi) & \sin(\xi) \end{pmatrix}. \tag{2.24}$$

Ein Vergleich mit Anhang A.1.2.3 zeigt, daß sich $U(\xi)$ experimentell durch zwei $\frac{\lambda}{2}$-Platten in einem der beiden Arme der Quelle bei den Winkelstellungen $\xi/2\,^\circ - 45\,^\circ$ und $0\,^\circ$ implementieren läßt. Um die Schranke des CHSH-Operators systematisch zu

rekonstruieren bedarf es einer Parametrisierung der Variable ξ durch den Parameter θ, der die Observablen bestimmt (siehe [11]).

$$\xi(\theta) = \frac{1}{2}\left\{\theta - g(\theta)\arccos\left(\sqrt{1+\sin^2(2\theta)}\right)\right\}. \tag{2.25}$$

Bei der Messung wird der Winkel θ von $0\,^\circ$ bis $180\,^\circ$ in $5\,^\circ$-Schritten verändert. Für gegebenes θ wird eine der $\frac{\lambda}{2}$-Platten, die die unitäre Transformation repräsentieren auf die Position $\xi(\theta)/2 - 45\,^\circ$ verfahren und daraufhin mit dem Polarisationsanalysator der Erwartungswert von **CHSH** bei θ bestimmt. Abbildung 2.12 zeigt im Wesentlichen vier Kurven, zum einen die theoretische Erwartung (---) sowie die gemessenen Daten (●, ●) für $\langle$**CHSH**$\rangle$ in Abhängigkeit des Parameters θ für die Zustände $|\psi^-\rangle$ und $|\phi^+\rangle$ ohne die Anwendung der unitären Transformation $U(\xi(\theta))$. Zum anderen ist der theoretisch vorhergesagte Verlauf der Schranke des CHSH-Operators zu sehen. Er folgt der Funktion aus Gleichung 1.12 bzw. entspricht $U(\xi(\theta))|\psi^-\rangle$. Zwar emittiert die verwendete Quelle keinen reinen $|\psi^-\rangle$-Zustand, aber die Tomographie aus Kapitel 2.3.2.3 erlaubt dennoch die Berechnung der zu erwartenden Kurve für $U(\xi(\theta))\rho_{exp}U^\dagger(\xi(\theta))$ (—). Die gemessenen Daten (●) folgen exakt dieser Funktion.

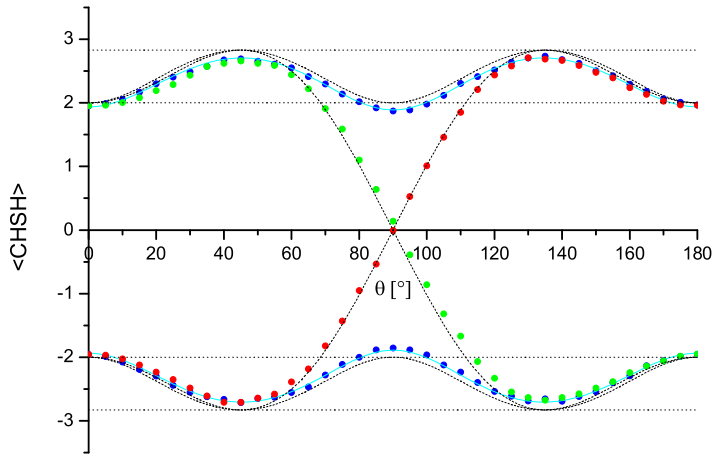


Abbildung 2.12: Der theoretische Erwartungswert des CHSH-Operators in Abhängigkeit des Parameters θ für $|\psi^-\rangle$, $|\phi^+\rangle$, $U(\xi(\theta))|\psi^-\rangle$ in (---) und für $U(\xi(\theta))\rho_{exp}U^\dagger(\xi(\theta))$ in (—). Gemessene Werte von $\langle$**CHSH**$\rangle$ für $|\psi^-\rangle$ (●), $|\phi^+\rangle$ (●) und $U(\xi(\theta))\rho_{exp}U^\dagger(\xi(\theta))$ (●).

Dies ist die experimentelle Bestätigung dafür, daß für bestimmte Observable kein quantenmechanischer Zustand existiert, der die CHSH-Ungleichung maximal verletzt. Für die Werte $\theta = 0\,^\circ$, $\theta = 90\,^\circ$ und $\theta = 180\,^\circ$ kann darüberhinaus die klassische Grenze von $|\, S_{LHV} \leq 2\,|$ nicht überwunden werden. Sollten tatsächlich Experimente zeigen, daß physikalische Zustände existieren, die zu Erwartungswerten jenseits der durch

Gleichung 1.12 vorgegebenen Schranke führen, wäre dies ein Hinweis für "Superquantenkorrelationen“ und die Quantenmechanik könnte nicht länger als vollständige Theorie betrachtet werden. In der zeitgleich entstandenen Arbeit [39] wurde nach solchen Zuständen gesucht. Dabei wurde keine Parametrisierung wie in Gleichung 2.25 durchgeführt, sondern für gegebenen Parameter θ durch eine Änderung von ξ im Bereich von $0\,^\circ$ bis $360\,^\circ$ der Zustand variiert. Das Ergebnis war bis auf experimentell bedingte Imperfektionen eine Bestätigung von Gleichung 1.12.

Kapitel 3

Quantenkommunikationskomplexität

Im vorangegangenen Kapitel wurde die Entwicklung einer kompakten Quelle zur Erzeugung verschränkter Photonenpaare beschrieben. Die Quelle wurde dazu verwendet quantenmechanische Korrelationen im Experiment zu untersuchen. Im folgenden dient ein leicht modifizierter Aufbau als Quasi-Einzelphotonenquelle für die Realisierung des in [40] vorgeschlagenen Mehrparteien Quantenkommunikationskomplexitätsprotokolls. Das Kapitel gliedert sich dabei wie folgt: Zuerst wird der Begriff Quantenkommunikationskomplexität erklärt. Das Protokoll und die experimentellen Voraussetzungen für dessen Umsetzung werden beschrieben. Gegen Ende des Kapitel werden die erzielten Resultate vorgestellt.

3.1 Theoretische Grundlagen

3.1.1 Kommunikationskomplexität - das Problem

In den Kapiteln 1 und 2 wurden Bell-Ungleichungen eingeführt und im Experiment verletzt. Vermöge Bells Theorem bedeutet deren Verletzung, dass entweder tatsächlich keine „*elements of physical reality*“ existieren oder die quantenmechanische Physik nur nicht-lokal verstanden werden kann. Vom Standpunkt der klassischen Physik aus betrachtet, würde letzteres eine „instantane Kommunikation“ zwischen den Teilchen bedeuten, die Information über die Messung des jeweils anderen Teilchens übermittelt. Derartige „*spukhafte Fernwirkungen*“, wie Einstein sie nannte, können, so sie denn in der Tat existieren, jedoch auch in der Quantenmechanik nicht dazu verwendet werden überlichtschnell zu kommunizieren. Selbst wenn zwei raumartig getrennte Personen, Alice und Bob, jeweils einen Teil eines verschränkten Teilchenpaares besitzen, gibt es für Alice keine Möglichkeit ihr Teilchen in irgendeiner Weise zu manipulieren um den

Wert eines beliebigen Bits x zu Bob zu übertragen, wenn dieser Messungen an seinem Teilchen durchführt. Alle Resultate, die Bob bei beliebigen Messungen erhalten könnte, sind durch seine reduzierte Dichtematrix festgelegt und diese kann Alice mittels keiner unitären Transformation verändern.

Verschränkung kann folglich nicht für die direkte Kommunikation verwendet werden, jedoch gibt es einige Kommunikationsszenarien, in denen der Gebrauch von (verschränkten) Qubits einen Vorteil gegenüber der Verwendung von klassischen Bits mit sich bringt, indem er die Menge an benötigter Kommunikation reduziert. Ein einfaches Beispiel ist das sogenannte „Dense coding“, [41] bei dem ein zuvor aufgeteiltes verschränktes Paar einem der Partner erlaubt durch die Übermittlung eines Qubits zwei Bit an klassischer Information an den anderen Partner zu senden. Ein Anderes ist die hier vorgestellte Quantenkommunikationskomplexität. Der Begriff wurde erstmals von Yao [42] eingeführt und befasst sich mit folgender Problematik:
Jede von zwei voneinander getrennten Parteien, Alice und Bob, erhält einen n-Bit String x bzw. y. Ihre Aufgabe ist die gemeinsame Berechnung einer Funktion $f(x, y)$. Die Parteien unterliegen dabei keiner Beschränkung bezüglich der Anzahl der von Ihnen durchgeführten Berechnungen oder der Menge an Speicher, den sie dafür benötigen, jedoch sollte Ihre Kommunikation untereinander minimal sein. Daher ergibt sich der Name Kommunikationskomplexität. Diese Thematik findet bei verteilten Berechnungen in hoch integrierten Prozessoren oder Schaltungen eine praktische Anwendung um die Menge an elektrischen Signalen zwischen den Komponenten und damit die verbrauchte Energie zu minimieren. Das von Yao eingeführte Problem läßt sich auf natürliche Weise von zwei auf k Parteien erweitern [43]. Dabei wird f eine k-variable boolsche Funktion von n-Bit Strings:

$$f : X^k \to \{0, 1\}, \text{ mit } X = \{0, 1\}^n \tag{3.1}$$

Jede der k Parteien $P_1, \ldots, P_k$ ist dabei anfänglich nur im Besitz der Eingabedaten x_i, $i = 1, \ldots, k$. Ziel bleibt die Bestimmung von $f(X^k)$ bei minimaler Kommunikation. Eine andere Betrachtungsweise dieses Problems besteht darin, bei vorgegebener Menge an Kommunikation den Wert von $f(X^k)$ mit möglichst großer Wahrscheinlichkeit korrekt zu ermitteln. Denkt man über eine quantenmechanische Lösung dieser Aufgabe nach, ergeben sich verschiedene Ansätze. In einem davon teilen sich die Parteien einen verschränkten Mehrteilchenquantenzustand und nützen die Verschränkung als Resource für die Kommunikation klassischer Bits. Dabei ergibt sich eine starke Äquivalenz eines derartigen Protokolls zur Verletzung von Bellschen Ungleichungen. Buhrman, Cleve und van Dam fanden ein Zweiparteien Kommunikationskomplexitätsprotokoll [44], das mit einer größeren Erfolgswahrscheinlichkeit als in jedem klassischen Szenario gelöst werden kann, wenn die beteiligten Parteien Verschränkung ausnutzen. Das Protokoll basiert auf der Verletzung der CHSH-Ungleichung durch einen verschränkten Zwei-Teilchen-Zustand. Vor einem Jahr wurde gezeigt [45], dass allgemein für jede Mehr-Teilchen Bell-Ungleichung wenigstens ein Kommunikationskomplexitätsproblem formuliert werden kann, für das gilt: Wenn die verschränkten Teilchen die Bell-Ungleichung verletzen, und *nur* dann, ist die Erfolgswahrscheinlichkeit des Quantenprotokolls höher

als in jedem klassischen Protokoll. Die Verletzung der Bell-Ungleichung bildet folglich ein notwendiges und hinreichendes Kriterium für die Überlegenheit des Quantenprotokolls. Verschränkung ist jedoch nicht die einzige Resource, die der Quanteninformationsverarbeitung zum Nutzen gereicht. Ein anderer Zugang zur Lösung obigen Problems verwendet keine Verschränkung, dafür aber die Kommunikation von Qubits anstelle klassischer Bits. Das in dieser Arbeit realisierte Protokoll ist von letzterem Typ. Das hat im Wesentlichen zwei Gründe. Zum einen wurde ein verschränkungsbasiertes Kommunikationskomplexitätsprotokoll mit zwei Parteien bereits experimentell demonstriert [46]. Dabei handelte es sich um die Umsetzung des in [44] für zwei Parteien eingeführten Protokolls. Zum anderen ist eine Mehr-Photonen Verschränkung im Experiment sehr schwer zu erzeugen, mit mehr als vier Teilchen momentan sogar technisch nicht möglich. Das im nächsten Abschnitt beschriebene Protokoll erlaubt dagegen die Beteiligung von fünf Parteien durch die sequenzielle Kommunikation eines Qubits.

3.1.2 Ein spezielles Protokoll

In dem nachfolgend vorgestellten Protokoll berechnen N Parteien eine Modulo-4 Summe. Der Vorschlag für die experimentelle Realisierung stammt von Galvão [40] und ist die Modifikation des in [44] für drei Parteien vorgeschlagenen und später auf $N \geq 3$ Parteien erweiterten [43] Protokolls.

Jede der beteiligten Parteien P_i erhält einen zwei-Bit String $x_i \in \{0, 1, 2, 3\}$. Die x_i sind unter den Kombinationen gleichverteilt, die der Bedingung genügen, dass ihre Summe gerade ist:

$$\left(\sum_{i=1}^{N} x_i \right) \mod 2 = 0. \tag{3.2}$$

Eine der Parteien, beispielsweise die letzte P_N soll den Wert der boolschen Funktion

$$f(\vec{x}) = \frac{1}{2} \left[\left(\sum_{i=1}^{N} x_i \right) \mod 4 \right] \tag{3.3}$$

bekanntgeben. Gleichung 3.2 stellt sicher, dass $f(\vec{x})$ in der Tat nur zwei verschiedene Werte annehmen kann. Die Kommunikation unterliegt dabei sowohl im klassischen als auch im quantenmechanischen Fall der Einschränkung, dass sie sequentiell erfolgen muss und die übermittelte Datenmenge nur jeweils ein Bit bzw. Qubit betragen darf. Das bedeutet jede Partei P_i sendet immer nur ein (Qu)bit zur jeweils nächsten Partei P_{i+1}. Die Wahrscheinlichkeit, dass die letzte Partei P_N das Ergebnis von $f(\vec{x})$ unter dieser Prämisse korrekt angibt, gilt es für klassische und quantenmechanische Protokolle zu vergleichen.

3.1.3 Klassisch vs. quantenmechanisch

3.1.3.1 Klassische Protokolle

Für N Parteien werden $(N-1)$ (klassische) Bits sequenziell versendet. Dabei ist es wichtig, dass es zu keiner Unterbrechung in der Kommunikation kommt. Würde die Partei P_i keine Information an P_{i+1} übermitteln, gäbe es für die letzte Partei P_N keine Möglichkeit $f(\vec{x})$ mit einer Wahrscheinlichkeit $p_{kl} > 1/2$ zu bestimmen. Das ist offensichtlich da P_N keine Kenntnis über die Bit Strings $x_1, x_2, \ldots, x_i$ erhält und es unter allen zugelassenen Kombinationen $(x_1, x_2, \ldots, x_i)$ gleich viele i-Tupel gibt, die zum Ergebnis $f(\vec{x}) = 0$ und zu $f(\vec{x}) = 1$ führen. Daher ist es nötig, dass jede Partei ein Bit an die nächste weiterleitet. Hierfür gibt es eine Vielzahl von Möglichkeiten, die zu unterschiedlichen Erfolgswahrscheinlichkeiten führen.

Die erste Partei P_1 hat nur Zugang zu ihren zwei Bits x_1 und kann daher zwischen 2^4 Protokollen auswählen, da sie jeweils nur ein Bit an Information weitersenden darf. Ein Protokoll kann folglich als vier-Bit String $\mathfrak{p}_1$ repräsentiert werden, dessen n-tes $(n = 0, 1, 2, 3)$ Bit die Nachricht $info_1$ repräsentiert, die an P_2 weitergesendet wird. Ein mögliches Beispiel wäre $\mathfrak{p}_1 = 0011$. Das bedeutet P_1 sendet 0 für $x_1 = 0 \mathrel{\widehat{=}} 00$ sowie $x_1 = 1 \mathrel{\widehat{=}} 01$ und für $x_1 = 2 \mathrel{\widehat{=}} 10$ und $x_1 = 3 \mathrel{\widehat{=}} 11$ sendet sie 1. Alle anderen Parteien P_i $(i = 2, \ldots, N-1)$ haben $2^4 \cdot 2^4 = 2^8$ Protokolle zur Auswahl, da sie ihre eigenen Bits x_i und die Nachricht $info_{i-1}$ der jeweiligen Vorgängerpartei in Erwägung ziehen müssen. Die 2^8 Möglichkeiten können durch einen acht-Bit String $\mathfrak{p}_i$ repräsentiert werden dessen n-tes $(n = 0, 1, \ldots, 7)$ Bit für $2x_i + info_{i-1} = n$ die Nachricht $info_i$ kodiert. Die Erfolgswahrscheinlichkeit für ein gegebenes Protokoll kann dann leicht berechnet werden. Für $x_N = 0$ betrachte man alle möglichen Eingabedaten $\{x_1, x_2, \ldots, x_N\}$ und bestimme jeweils $info_{N-1}$. Daraus ergibt sich p^0_{kl} als die Anzahl der Fälle, in denen die wahrscheinlichste Antwort von P_N mit $f(\vec{x})$ übereinstimmt, dividiert durch die Gesamtzahl der Möglichkeiten. Analog wird für $x_N = 1$, $x_N = 2$, $x_N = 3$ verfahren und man erhält p^1_{kl}, p^2_{kl}, p^3_{kl}. Die endgültige Erfolgswahrscheinlichkeit p_{kl} folgt durch Mittelung über p^0_{kl} bis p^3_{kl}. Lässt man einen Computer über alle $2^4(2^8)^{N-2} = 2^{8N-12}$ möglichen Protokolle scannen findet man das optimale klassische Protokoll für das p_{kl} maximal ist.

N	3	4	5	6
p_{kl}	3/4	3/4	5/8	5/8

Tabelle 3.1: Erfolgswahrscheinlichkeiten p_{kl} für klassische Protokolle mit verschiedener Anzahl beteiligter Parteien N

Tabelle 3.1 zeigt die Erfolgswahrscheinlichkeiten für eine verschiedene Anzahl von beteiligten Parteien. Für größer werdendes N stößt man bei der Lösung schnell an die

Leistungsgrenze verfügbarer Computer. Das in [40] vorgeschlagene quantenmechanische Protokoll ist wesentlich einfacher und hat Erfolgswahrscheinlichkeit $p_{qm} = 1$ unabhängig von N.

3.1.3.2 Quantenmechanisches Pendant

Zur quantenmechanischen Lösung des Modulo-4 Summenproblems wird ein Qubit sequentiell von einer Partei zur nächsten gesendet. Ausgehend vom Zustand

$$|\zeta\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right). \tag{3.4}$$

kodiert jede Partei P_j die Information, die sie zur nächsten Partei P_{j+1} sendet durch die Anwendung des Phasenoperators

$$\hat{\phi}(x_j) = \begin{cases} |0\rangle \rightarrow |0\rangle \\ |1\rangle \rightarrow e^{i(\pi/2)x_j}|1\rangle, \quad \text{für } x_j = \{0,1,2,3\}. \end{cases} \tag{3.5}$$

Auf Grund der Bedingung 3.2 resultiert dies nach N Phasenoperationen im Zustand

$$|\zeta\rangle_f = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{f(\vec{x})}|1\rangle\right) \tag{3.6}$$

und die letzte Partei P_N kann durch eine Messung in der Basis $\{\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\}$ den Wert von $f(\vec{x})$ mit Sicherheit, d.h. Wahrscheinlichkeit $p_{qm} = 1$ voraussagen. Dieses Resultat erscheint sehr erstaunlich und auf den ersten Blick Holevos Theorem [47] zu verletzen, das besagt, dass mit einem Qubit lediglich ein Bit an klassischer Information übertragen werden kann. Der scheinbare Widerspruch wird in [48] sogar noch deutlicher, da gezeigt wird, dass in vergleichbaren Problemstellungen ein Qubit nicht nur zwei Bits, sondern sogar eine beliebig große Menge von Bits an klassischer Kommunikation ersetzen kann. Der vermeintliche Widerspruch ist jedoch keiner. Es wird während des Protokolls zu keinem Zeitpunkt verlangt, dass die Information des gesendeten Qubits tatsächlich ausgelesen werden kann. Sie ersetzt lediglich bei der gemeinsamen Berechnung einer Funktion eine entsprechende Menge an klassischer Kommunikation, nicht Information.

3.1.4 Vorschlag zur Realisierung mit Photonen

Das in 3.1.3.2 vorgestellte Protokoll läßt sich mit einzelnen Photonen realisieren. Den Anfangszustand bildet dabei der Polarisationszustand

$$|+\rangle = \frac{1}{2}\left(|H\rangle + |V\rangle\right) \tag{3.7}$$

und der Phasenoperator stellt sich somit in der Form

$$\hat{\phi}(x_j) = \begin{cases} |\,H\,\rangle \rightarrow |\,H\,\rangle \\ |\,V\,\rangle \rightarrow e^{i(\pi/2)x_j}|\,V\,\rangle, \quad \text{für } x_j = \{0,1,2,3\}. \end{cases} \tag{3.8}$$

dar. Die Phase ist eine kontinuierliche Variable und die Verwendung eines klassischen elektromagnetischen Feldes für den Informationsaustausch (z.B. Lichtpulse wie sie in der optischen Telekommunikation verwendet werden) würde in diesem Protokoll ebenfalls zum gewünschten Ergebnis führen. Die Verwendung von einzelnen Photonen ist allerdings am effektivsten und stellt die Kommunikation mit dem kleinstmöglichen physikalischen System dar. Was dem Quantenprotokoll hier zu seiner Überlegenheit verhilft, ist die Tatsache, dass ein Photon zwar im Gegensatz zu einem klassischen Feld nur diskrete unterscheidbare Zustände besitzt, aber trotzdem als einzelnes Quant des Feldes dessen kontinuierliche klassische Beschreibung in Form einer kontinuierlichen Menge reiner, aber nicht unterscheidbarer Zustände bewahrt.

Die Einzelphotonen stammen aus der in Kapitel 2 vorgestellten Quelle. Dabei wird die zeitliche Korrelation zwischen den Photonen eines Paares ausgenutzt. Wann immer man ein Photon in einer Mode registriert, muß in der anderen Mode ebenfalls genau ein Photon emittiert worden sein und man erhält ein Koinzidenzereignis. Ein Teilchen dient daher als Trigger, während das andere für die Durchführung des Protokolls verwendet wird. Die sequenzielle Kommunikation der Parteien besteht dabei darin, dass dieses Signalphoton die optischen Elemente, welche die Parteien repräsentieren nacheinander passiert. Am Ende erfolgt dessen Detektion zusammen mit der Analyse der Polarisation. Dies geschieht jedoch nur mit einer bestimmten Effizienz η, daher ergeben sich im Experiment zusätzliche Bedingungen, will man die klassische Erfolgswahrscheinlichkeit übertreffen. Im Fall der erfolgreichen Detektion kann eine richtige Aussage über den Wert von $f(\vec{x})$ mit der Wahrscheinlichkeit p_{qm} getroffen werden. Strebt man einen fairen Vergleich mit einem klassischen Protokoll an, muss aber auch in den Fällen eine Angabe zu $f(\vec{x})$ gemacht werden, in denen die Detektion des Signalphotons fehlschlägt. Hierbei kann jedoch nur zufällig mit Erfolgswahrscheinlichkeit 1/2 geraten werden. Daraus ergibt sich die Einschränkung

$$\eta + (1-\eta)\frac{1}{2} > p_{kl} \tag{3.9}$$

für eine bessere als klassische Durchführung. Für $N = 5$ folgt daraus bereits $\eta > 0,25$. Die Detektionseffizienz ist nicht die einzige Schwierigkeit, die in einem Experiment überwunden werden muss. Die optischen Komponenten, die für die Zustandspräparation und die Phasenveränderungen verwendet werden, haben eine Transmittivität t kleiner eins. Hinzu kommt ein Beitrag μ zu den Koinzidenzereignissen von den Dunkelzählraten. Darüberhinaus ist selbst bei erfolgreicher Detektion eines Signalphotons auf Grund von Imperfektionen im Setzen der Polarisation oder Phase die Erfolgsrate s nicht perfekt gleich eins, wie man es theoretisch im quantenmechanischen

Protokoll erwarten würde. Gleichung 3.9 erweitert sich somit zu

$$p_{qm}^{eff} = (1-\mu)\eta t s + [1-(1-\mu)\eta t]\frac{1}{2} > p_{kl}. \tag{3.10}$$

Bei der Implementierung im nächsten Kapitel wird sich zeigen, dass μ vernachlässigbaren Einfluss hat. Die Größen η und t können im Experiment in einem Parameter, dem Koinzidenz- zu Einzelzählraten Verhältnis ς zusammengefasst werden. Für s spielt vor allem die Genauigkeit der Phase eine entscheidende Rolle. Die Transmittivität t und s werden sich im Anteil ϱ der richtigen Aussagen bei erfolgreicher Detektion des Signalphotons niederschlagen.

3.2 Implementierung

Dieser Abschnitt beschäftigt sich mit der experimentellen Umsetzung des in 3.1.2 beschriebenen Protokolls. Die beiden zentralen Probleme, die sich ergeben, sind zum einen die Implementierung des Operators $\hat{\phi}$ und damit verbunden die möglichst präzise Anwendung des gewünschten Phasenschubs sowie zum anderen die effiziente Detektion des Signalphotons, was sich in einem hohen Verhältnis von Koinzidenz- zu Einzelphotonzählrate ausdrückt.

3.2.1 Realisierung des Phasenoperators im Experiment

3.2.1.1 Doppelbrechende Kristalle

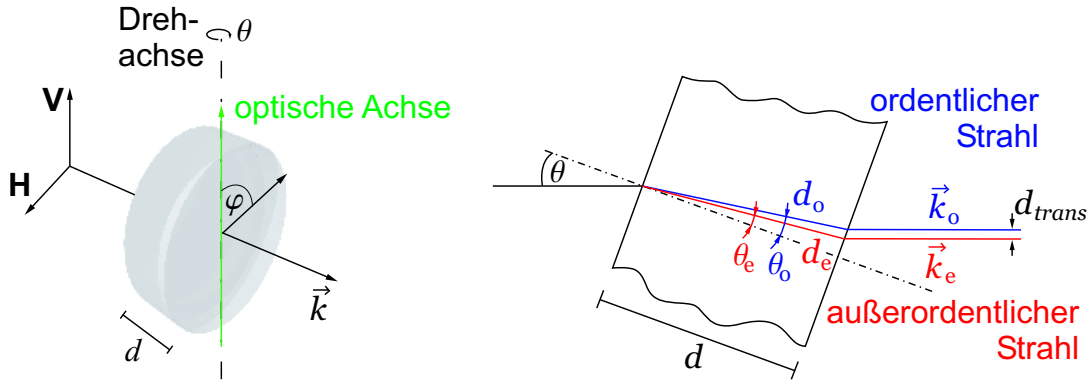
Der Operator $\hat{\phi}$ stellt sich in der Matrixdarstellung wie folgt dar

$$\hat{\phi} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix}, \tag{3.11}$$

wobei δ der Phasenschub ist, den die vertikal polarisierte Komponente erfährt. Ein Vergleich mit Anhang A.14 zeigt, dass $\hat{\phi}$ bis auf eine nicht messbare globale Phase einer linearen Verzögerungsplatte mit variabler Verzögerung δ in der Winkelstellung $\varphi = 90\,^\circ$ entspricht; φ ist der Winkel den die optische Achse mit der horizontalen Polarisationsrichtung einschließt.

$$\mathbf{lam}(\delta, 90\,^\circ) = \begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix} = e^{-i\delta/2} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix} =: \hat{\phi}_{exp} \tag{3.12}$$

Der Betrag der Verzögerung ist bei einer Wellenplatte durch dessen Dicke fest vorgegeben. Bei einer $\frac{\lambda}{2}$-Platte beträgt δ beispielsweise $180\,^\circ$. Dennoch dient eine Wellenplatte



(a) Doppelbrechender Kristall mit optischer Achse in einer Parallelebene zur Oberfläche.

(b) Brechung und Aufspaltung des einfallenden Strahls in ordentlichen und außerordentlichen Strahl.

Abbildung 3.1: Realisierung des Phasenoperators $\hat{\phi}$ mittels eines doppelbrechenden Kristalls.

als Vorlage für den Phasenoperator. Die Idee ist, einen doppelbrechenden Kristall der Dicke d ebenso zu schneiden, dass seine optische Achse in einer Parallelebene zur Oberfläche liegt. Bei senkrechtem Einfall bildet der Wellenvektor $\vec{k}$ eines Photons dann einen rechten Winkel mit der optischen Achse. Durch Rotation des Kristalls um diese Achse kann dessen effektive optische Dicke und somit die Verzögerung δ variiert werden (siehe Abbildung 3.1(a)). Wie sich δ als Funktion des Drehwinkels θ verändert, soll im folgenden hergeleitet werden.

In einem optischen Kristall können die Brechungsindizes, n_1, n_2, n_3, für jede der drei Raumrichtungen unterschiedlich sein. Die Beschreibung der Ausbreitung eines Lichtstrahls mit beliebiger Polarisation innerhalb des Kristalls in eine willkürliche Richtung ist im allgemeinen nicht trivial zu beschreiben, kann jedoch durch die Einführung zweier sog. Normalmoden vereinfacht werden. Der einfallende Strahl wird dabei als Superposition der beiden Normalmoden dargestellt. Deren Ausbreitung ist separat und einfach zu behandeln. Bei einem einachsigen doppelbrechenden Kristall ($n_1 = n_2 = n_o$ und $n_3 = n_e$) sind diese Normalmoden zwei linear-polarisierte ebene Wellen, genannt ordentliche und außerordentliche Mode. Der Polarisationsvektor der ordentlichen Mode steht senkrecht auf der Ebene, die von der optischen Achse des Kristalls und dem Wellenvektor $\vec{k}$ des einfallenden Lichtstrahls aufgespannt wird. Für sie stellt sich der Kristall isotrop dar und sie erfährt daher immer den Brechungsindex n_o. Der Polarisationsvektor der außerordentlichen Mode liegt innerhalb der von $\vec{k}$ und der optischen Achse aufgespannten Ebene. Für sie ist der Kristall anisotrop und der Brechungsindex $n(\vartheta)$ ist abhängig vom Winkel ϑ den $\vec{k}$ mit der optischen Achse einschließt. Es gilt (vgl. Gleichung 2.6 und Abschnitt 2.1.1)

$$\frac{1}{n^2(\vartheta)} = \frac{\cos^2(\vartheta)}{n_o^2} + \frac{\sin^2(\vartheta)}{n_e^2}. \tag{3.13}$$

Dabei variiert $n(\vartheta)$ von n_o für $\vartheta = 0\,^\circ$ bis n_e für $\vartheta = 90\,^\circ$. Für ein bestimmtes Mate-

rial hängen n_o und n_e von der Wellenlänge λ ab. Auf die Verwendung verschiedener Kristalltypen wird später noch eingegangen werden. Liegt die optische Achse in einer Parallelebene zur Einfallsebene, ist für gegebene Wellenlänge und einer Winkelstellung $\varphi = 90\,^\circ$ (siehe Abbildung 3.1(a)) die relative Verzögerung zwischen horizontaler und vertikaler Polarisationskomponente bei senkrechtem Einfall lediglich durch die Differenz zwischen ordentlichem und ausserordentlichem Brechungsindex sowie die Kristalldicke d bestimmt.

$$\delta = \frac{2\pi}{\lambda} |n_e - n_o| \, d \tag{3.14}$$

Vertikale bzw. horizontale Polarisation bilden die beiden Normalmoden, die sich jeweils mit den Geschwindigkeiten c/n_o bzw. c/n_e unabhängig von θ ausbreiten. Denn für $\varphi = 90\,^\circ$ ist ϑ konstant $90\,^\circ$ und ändert sich nicht mit θ. Anders stellt sich die Situation für $\varphi = 0\,^\circ$ dar. In diesem Fall ist $\vartheta = \theta$ und nachfolgende Herleitung wird komplizierter, da n_e durch $n(\vartheta)$ zu ersetzen ist. Das Endresultat ist in beiden Fällen qualitativ ähnlich mit dem einzigen Unterschied, dass sich die effektive Doppelbrechung für $\varphi = 0\,^\circ$ schwächer mit θ ändert. Der Einfachheit halber wird hier daher stets von $\varphi = 90\,^\circ$ ausgegangen. Bei einer Rotation des Kristalls um den Winkel θ erleben ordentlicher und ausserordentlicher Strahl unterschiedliche Brechung und es kommt zur Aufspaltung des einfallenden Strahls. Aufgrund dieser Tatsache erfahren sie unterschiedliche effektive Kristalldicken d_o bzw. d_e. Wie man aus trivialen geometrischen Überlegungen unmittelbar sieht, gilt:

$$\begin{aligned} d_o(\theta_o) &= \frac{d}{\cos(\theta_o)} \\ d_e(\theta_e) &= \frac{d}{\cos(\theta_e)}, \end{aligned} \tag{3.15}$$

wobei θ_o und θ_e die Winkel sind, die der Wellenvektor des ordentlichen ($\vec{k}_o$) und außerordentlichen ($\vec{k}_e$) Strahls mit der optischen Achse einschließen (siehe Abbildung 3.1(b)). Für Gleichung 3.14 folgt somit

$$\delta(\theta_o, \theta_e) = \frac{2\pi}{\lambda} |n_e d_e(\theta_e) - n_o d_o(\theta_o)| = \frac{2\pi}{\lambda} \left| \frac{n_e}{\cos(\theta_e)} - \frac{n_o}{\cos(\theta_o)} \right| d \tag{3.16}$$

Vermöge des Snell'schen Brechungsgesetzes

$$n_l \sin(\theta) = n_{e,o} \sin(\theta_{e,o}), \tag{3.17}$$

mit n_l dem Brechungsindex für Luft, lässt sich Gleichung 3.16 in Abhängigkeit vom Rotationswinkel θ schreiben

$$\delta(\theta) = \frac{2\pi}{\lambda} \left| \frac{n_e}{\cos(\arcsin(n_l/(n_e \sin(\theta))))} - \frac{n_o}{\cos(\arcsin(n_l/(n_o \sin(\theta))))} \right| d. \tag{3.18}$$

Mit Hilfe der Beziehung

$$\cos(\arcsin(x)) = \sqrt{1 - x^2}$$

vereinfacht sich dies zu

$$\delta(\theta) = \frac{2\pi}{\lambda} \left| \frac{n_e}{\sqrt{1 - [n_l/(n_e \sin(\theta))]^2}} - \frac{n_o}{\sqrt{1 - [n_l/(n_e \sin(\theta))]^2}} \right| d. \tag{3.19}$$

Wie bereits zuvor erwähnt, hängt der Wert von n_o und n_e für ein bestimmtes Material von der Wellenlänge ab. Diese Abhängigkeit kann in Form des als Sellmeier-Reihe bekannten Ausdrucks dargestellt werden.

$$n(\lambda) = \sqrt{1 + \sum_{i=1}^{N} \frac{A_i \lambda^2}{\lambda^2 - B_i}} \tag{3.20}$$

Diese Formel kann für die Dispersion im sog. Lorentz-Oszillatormodell weitab der optischen Kristall-Resonanzfrequenzen hergeleitet werden, wobei die Koeffizienten A_i und B_i empirisch zu bestimmende Konstanten sind. Sie sei hier nur der Vollständigkeit halber erwähnt. Auf ihre Herleitung wird in dieser Arbeit verzichtet. Der interessierte Leser sei hierfür auf die Fachliteratur verwiesen (siehe z.B. [49]).

3.2.1.2 Auswahl der Kristallart

Für die Realisierung des Phasenoperators wurden vier verschiedene Kristallarten in Betracht gezogen, Yttrium-Vanadat (YVO_4), Kalzit ($CaCO_3$), Quarz (SiO_2) und β-Barium Borat (BBO). Für diese Kristalle sollen die Sellmeier-Gleichungen in einer Form aufgelistet werden, wie man sie in Datenblättern der kristallverarbeitenden Industrie finden kann (λ in μm):

- YVO_4:

$$n_o(\lambda) = \sqrt{3,77834 + \frac{0,069736}{\lambda^2 - 0,04724} - 0,0108133\lambda^2}$$

$$n_e(\lambda) = \sqrt{4,59905 + \frac{0,110534}{\lambda^2 - 0,04813} - 0,0122676\lambda^2}$$

- $CaCO_3$:

$$n_o(\lambda) = \sqrt{2,69705 + \frac{0,0192064}{\lambda^2 - 0,01820} - 0,0151624\lambda^2}$$

$$n_e(\lambda) = \sqrt{2,18438 + \frac{0,0087309}{\lambda^2 - 0,01018} - 0,0024411\lambda^2}$$

- SiO_2:

$$n_o(\lambda) = \sqrt{2,35736 + \frac{0,010576}{\lambda^2 - 0,01091} - 0,011741\lambda^2}$$

$$n_e(\lambda) = \sqrt{2,38482 + \frac{0,010949}{\lambda^2 - 0,01115} - 0,012595\lambda^2}$$

- BBO:

$$n_o(\lambda) = \sqrt{2,7405 + \frac{0,0184}{\lambda^2 - 0,0179} - 0,0155\lambda^2}$$

$$n_e(\lambda) = \sqrt{2,3730 + \frac{0,0128}{\lambda^2 - 0,0156} - 0,0044\lambda^2}$$

Um abwägen zu können, welches Material für die Durchführung des Experiments am besten geeignet ist, sind in Tabelle 3.2 folgende wichtige Parameter für die Wellenlänge $\lambda = 805,5$ nm dargestellt. Dies sind die Brechungsindizes n_o und n_e, und für eine gegebene Dicke d der Winkel $\theta_{3\pi/2}$ bei dem ein Phasenschub von $3\pi/2$ erreicht wird, der Fehler im Phasenschub ε_δ für $\theta_{3\pi/2}$ bei einer Winkelungenauigkeit von $0,1\,^\circ$, sowie der transversale Strahlversatz d_{trans} beim Winkel $\theta_{3\pi/2}$ zwischen ordentlichem und ausserordentlichem Strahl am Ende des Kristalls, der durch die Beziehung

$$d_{trans} = d \cdot \frac{\sin\left(\theta - \arcsin(\frac{n_l \sin(\theta)}{n_o})\right)}{\cos\left(\arcsin(\frac{n_l \sin(\theta)}{n_o})\right)} \tag{3.21}$$

gegeben ist.

Der maximale Phasenschub, der im Protokoll aus Abschnitt 3.1.2 auftreten kann ist $\delta = 3\pi/2$ für $x_i = 3 \mathrel{\widehat{=}} 11$. Daher ist $\theta_{3\pi/2}$ eine wichtige Größe. Sie sollte einen vernünftigen Kompromiß zwischen Reflexionsverlusten und dem Fehler in der Phase auf Grund endlicher Winkelpräzision darstellen. Die Reflexionsverluste nehmen mit θ zu und vermindern somit die Detektionseffizienz. Der Winkelfehler nimmt mit kleiner werdendem Winkelbereich $\Delta\theta = \mid \theta_{3\pi/2} - \theta_0 \mid$ (θ_0 sei der Winkel bei dem kein Phasenschub stattfindet) zu und führt zu größerem ε_δ. Sowohl Detektionseffizienz als auch die Genauigkeit des Phasenschubs sind die Erfolgswahrscheinlichkeit p_{qm} entscheidend beeinflussende Größen (siehe Abschnitt 3.1.4). Diese Überlegungen machen daher bereits deutlich, dass Quarz nicht sehr geeignet ist. Er ist im Vergleich zu den restlichen Materialien nur schwach doppelbrechend, was die geringe Differenz zwischen n_o und n_e zeigt. Daher müßte der Kristall, will man in etwa einen Winkel von $\theta_{3\pi/2} \approx 19\,^\circ$ erreichen, um annähernd einen Faktor 10 dicker sein als die anderen Kristalle. Das resultiert wiederum in einem sehr starken Strahlversatz, was ebenfalls nicht erwünscht ist.

Unter diesen Gesichtspunkten scheint Kalzit am vorteilhaftesten, er ist jedoch auf Grund seiner mechanischen Eigenschaften kaum in der erforderlichen Dicke von $d \approx$

	YVO_4	$CaCO_3$	SiO_2	BBO
n_o	1,9716	1,6485	1,5382	1,6612
n_e	2,1852	1,4821	1,5472	1,5461
d [μm]	200	150	2500	230
$\theta_{3\pi/2}$ [°]	19,79	19,08	19,87	19,05
d_{trans} [μm]	34,9	20,3	316,8	31,5
ε_δ [π]	0,015	0,017	0,016	0,017

Tabelle 3.2: Parameter für unterschiedliche Kristallarten.

150 μm herzustellen. Yttrium-Vanadat und Beta-Barium-Borat sind sich in ihren optischen Eigenschaften ähnlich. Auf Empfehlung der kristallverarbeitenden Industrie bezüglich Preis und Verarbeitbarkeit fiel die Entscheidung auf YVO_4 Kristalle der Dicke $d = 200\,\mu$m.

3.2.1.3 Messung relativer Phasen

Da nun feststeht wie der Phasenoperator $\hat{\phi}$ realisiert wird, stellt sich die Frage, wie die relative Phasenverschiebung zwischen horizontaler und vertikaler Polarisationskomponente berechnet und experimentell überprüft werden kann. Eine leicht zu messende Größe ist die Intensität[1] eines Lichtstrahls, oder für einzelne Photonen dem entsprechend die Zählrate. Deswegen ist es wünschenswert die Phasenmessung auf eine Intensitätsmessung zurückzuführen. Dafür wird ein Analysator benötigt, der in zwei Ausgängen T und R die Intensität zweier orthogonaler Polarisationen mißt. Läßt man $\hat{\phi}$ auf eine Überlagerung aus horizontaler und vertikaler Polarisation (z.B. $|+45\rangle$) wirken und wählt dies als Eingang für den Analysator, läßt sich aus dem Intensitätsverhältnis der beiden Ausgänge die Phasenverschiebung zwischen H und V bestimmen (siehe Ab-

[1]Da die Detektionsfläche in keiner Weise berücksichtigt wird, wäre aus physikalischer Sicht die eigentlich gemessene Größe die Leistung. Da andererseits die Detektorfläche eine Konstante ist besteht eine Proportionalität zwischen diesen beiden Größen und sie können in diesem Zusammenhang mehr oder weniger synonym verwendet werden.

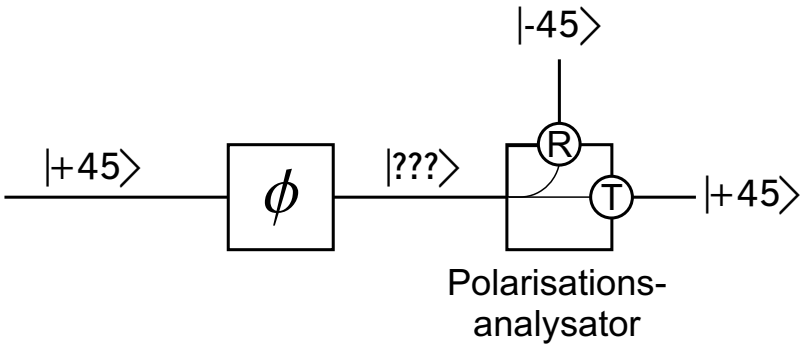


Abbildung 3.2: Messung der relativen Phase zwischen horizontaler und vertikaler Polarisationskomponente.

bildung 3.2). Es gilt:

$$
\begin{aligned}
I(\delta) = \frac{I_T(\delta)}{I_T(\delta) + I_R(\delta)} &= \left| \langle\, +45 \,|\, \hat{\phi}_{exp} \,|\, +45 \,\rangle \right|^2 \\
&= \left| \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & , & 1 \end{pmatrix} \cdot \begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right|^2 \\
&= \left| \cos\left(\frac{\delta}{2}\right) \right|^2 , \qquad (3.22)
\end{aligned}
$$

wobei $I_T(\delta)$ und $I_R(\delta)$ die Intensität im Ausgang T bzw. R in Abhängigkeit der Verzögerung δ ist. Als Polarisationsanalysator kann ein polarisierender Strahlteilerwürfel in Kombination mit einer $\frac{\lambda}{2}$-Platte wie im Aufbau aus Abbildung 2.6(a) dienen. Setzt man Gleichung 3.19 in Gleichung 3.22 ein, erhält man die Intensität in Abhängigkeit des Rotationswinkels $I(\delta(\theta)) = I(\theta)$.

3.2.1.4 Rotation der Kristalle

Die Rotation der Kristalle erfolgt über motorisierte Positioniersysteme der Firma Owis (DRT 40). Diese verwenden Zwei-Phasen Schrittmotoren, die 400 Vollschritte für eine Umdrehung benötigen. Daraus ergibt sich eine Winkelauflösung von $0,9\,^\circ$/Schritt, die durch eine Übersetzung mittels eines Zahnriemens im Verhältnis $1:3$ auf $0,3\,^\circ$/Schritt verbessert wird. Angesteuert werden die Motoren per Computer über eine Motorkarte (Owis, PC-SM 32), die durch Veränderung der angelegten Spannung zwischen jedem Vollschritt 64 Teilschritte interpolieren kann. Dies resultiert in einer theoretisch maximal erreichbaren Winkelgenauigkeit von $0,005\,^\circ$.

3.2.1.5 Charakterisierung der Kristalle

Mit Hilfe dieser drehbaren Montierung kann die für jeden Kristall charakteristische Kurve $I(\theta)$ aufgenommen werden. Die Funktion $I(\theta)$ erlaubt es für jeden Kristall die Winkel zu bestimmen, die dem zu setzenden Phasenschub entsprechen. Ein Beispiel zeigt Abbildung 3.3. Zu sehen ist der theoretische Verlauf (durchgezogene Linie) sowie

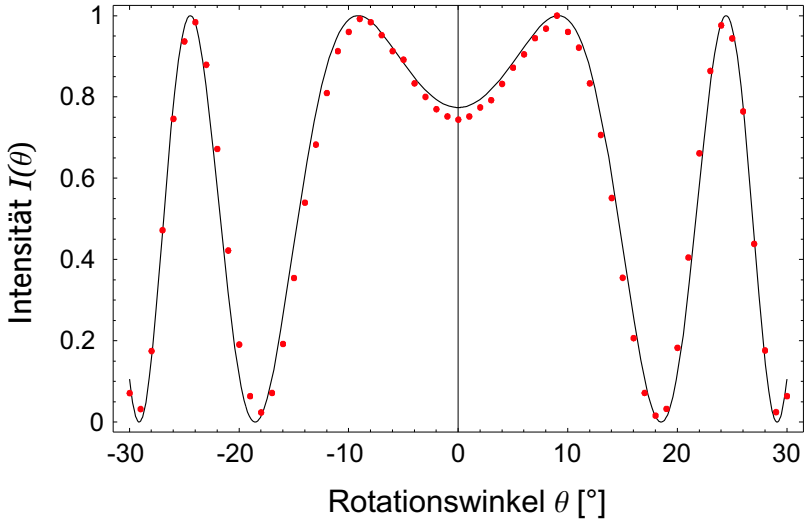
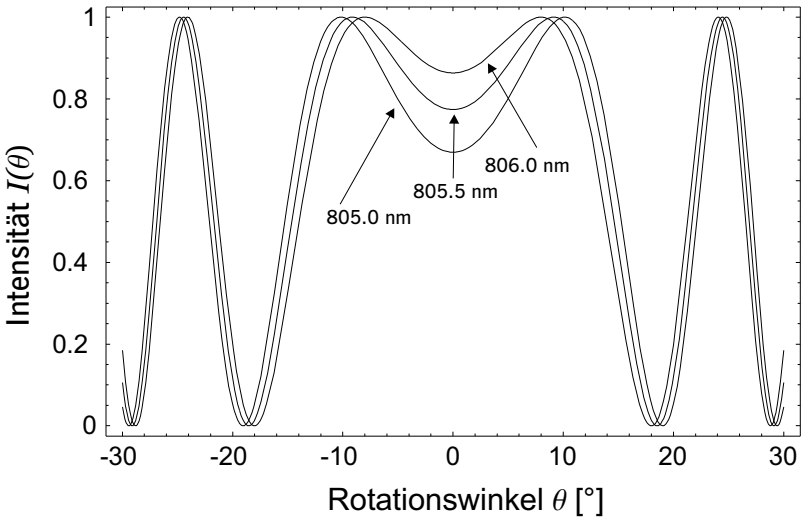


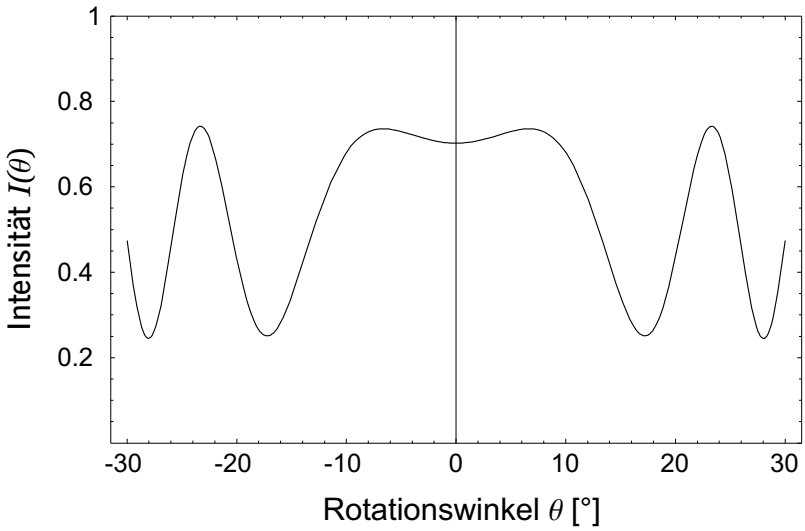
Abbildung 3.3: Intensität in Abhängigkeit des Rotationswinkels. Die Kurve (—) entspricht dem berechneten Verlauf. Sie ist *kein* Fit an die gemessenen Datenpunkte (●)

die gemessenen Datenpunkte von $I(\theta)$. Die Übereinstimmung ist sehr gut, obwohl die Kurve *keinen* Fit darstellt. Es ist allerdings auffällig, daß im Experiment der minimal erreichbare Wert bei $I(\theta) = 0,02$ liegt. Die durch Unzulänglichkeiten der Analysators[2] vorgegebene, gemessene untere Grenze beträgt im Gegensatz dazu $0,001$ und kann daher nicht zur Erklärung für den Offsetwert von $0,02$ herangezogen werden. Für die Messung wurde der Justierlaser aus Anhang A.3 verwendet. Dessen spektrale Breite ist verantwortlich für den Offsetwert. Das erscheint überraschend, bedenkt man, dass dessen Spektrum eine Breite von lediglich $0,3$ nm besitzt. Da die gesamte Phasenverschiebung die horizontale und vertikale Komponente beim Durchgang durch einen YVO_4-Kristall von 200 μm Dicke erfahren in der Größenordnung von 100π liegt ist die effektive relative Phasenverschiebung δ jedoch sehr stark wellenlängenabhängig. Die Darstellung von $I(\theta)$ für drei verschiedene, um ein halbes Nanometer unterschiedliche Wellenlängen in Abbildung 3.4(a) macht dies deutlich. Die resultierende Kurve von $I(\theta, \Delta\lambda)$ für Licht mit einer endlichen spektralen Verteilung der Breite $\Delta\lambda$ um eine zentrale Wellenlänge λ_c, läßt sich als gewichtete Überlagerung von Kurven für

[2]Dies sind beispielsweise nicht perfekte Auslöschung der Polarisationen am PBS, Fehler in der Justierung, etc.



(a) $I(\theta)$ für verschiedene Wellenlängen, 805,0 nm, 805,5 nm, und 806,0 nm bei fester Dicke $d = 200\,\mu$m.



(b) Theoretische Erwartung für $I(\theta)$ für Licht mit einer spektralen Halbwertsbreite (FWHM) von 5 nm.

Abbildung 3.4: Wellenlängenabhängigkeit von $I(\theta)$

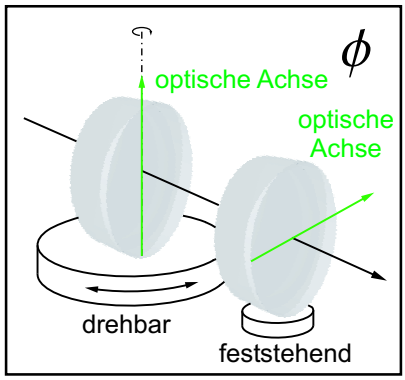


Abbildung 3.5: Der Phasenoperator $\hat{\phi}$ realisiert durch zwei doppelbrechende Kristalle mit gekreuzten optischen Achsen.

Linienspektren $I(\theta, \lambda_i)$ über alle Wellenlängen innerhalb der Verteilung darstellen.

$$I(\theta, \Delta\lambda) = \sum_{\lambda_i \in \{\lambda_c \pm \frac{\Delta\lambda}{2}\}} \mathfrak{w}_i \cdot I(\theta, \lambda_i), \text{ mit} \sum_i \mathfrak{w}_i = 1 \tag{3.23}$$

Dabei kommt es mit zunehmender spektraler Breite zur Reduktion der Sichtbarkeit in der Intensitätsmodulation. Abbildung 3.4(b) zeigt eine Simulation für Licht mit einer Halbwertsbreite (FWHM) von 5 nm. Da für das spätere Experiment Photonen der Quelle aus Kapitel 2 verwendet werden, die eine Halbwertsbreite von 6 nm besitzen (siehe Abschnitt 2.3.1), macht diese Wellenlängenempfindlichkeit die Kristalle zunächst unbrauchbar. Das Problem und dessen Lösung sind für Wellenplatten jedoch bereits bekannt. Die hier verwendeten Kristalle entsprechen im Prinzip sog. „Multi-Order"-Wellenplatten. Sie sind sensitiv bezüglich Wellenlängenänderungen. Im Gegensatz tritt bei sog. „Single-Order"-Wellenplatten dieser Effekt kaum auf. Sie bestehen aus zwei verbundenen „Multi-Order"-Wellenplatten, deren optische Achsen gekreuzt sind. Die zweite Platte kompensiert dabei gerade so viel des Gesamtphasenschubs der ersten, bis die gewünschte Verzögerung δ in nullter Ordnung, anstelle des Modulo eines Vielfachen von 2π bleibt. Die Kombination zweier Kristalle, von denen der erste drehbar und der zweite feststehend montiert wird, bildet daher den Phasenoperator $\hat{\phi}$ und erlaubt somit im Experiment die Einstellung verschiedener Phasenschübe, selbst für breitbandiges Licht (siehe Abbildung 3.5). Die zunächst störende Wellenlängensensitivität eines einzelnen Kristalls, kann bei der Justierung sogar zum Vorteil gereichen. Sie erlaubt es die Achsen aller Kristalle gleich auszurichten. Es ist experimentell einfach die Achsenpositionen $\varphi = 0\,^\circ$ *oder* $\varphi = 90\,^\circ$ zu finden. Dies sind die Stellungen bei denen sich $I(\theta)$ für horizontale und vertikale Polarisation bei Variation von θ nicht ändert. Die beiden Fälle zu unterscheiden ist allerdings etwas schwieriger. Die korrekte Lage der optischen Achse $\varphi = 90\,^\circ$ muss nun aber lediglich für einen Kristall gefunden werden, der dann als Referenz dient. Die richtige Position wird durch Vergleich der experimentellen Kurve mit der theoretischen Erwartung gefunden. Jeder weitere Kristall kann dann relativ zum ersten justiert werden, indem für Licht größerer spektraler Breite

$I(\theta)$ aufgenommen wird. Sind die Achsen gekreuzt, hat $I(\theta)$ eine zu Abbildung 3.3 ähnliche Form. Sind sie parallel ergibt sich eine ungenügende Modulation wie in Abbildung 3.4(b). Abbildung 3.6 zeigt die Intensität in Abhängigkeit des Rotationswinkels für Fluoreszenzphotonen der Quelle, wie sie im Versuch verwendet werden. Die Daten sind mit Kompensationskristall aufgenommen. Die Photonen haben eine Wellenlänge von ca. 11 nm (siehe Abschnitt 3.2.2, Seite 52). Die Kompensation ermöglicht einen Offset von lediglich ca. 2,5 %. Ohne Kompensation wäre bei dieser spektralen Breite ein Offset von über 25 % zu erwarten, vergleiche Abbildung 3.4(b).

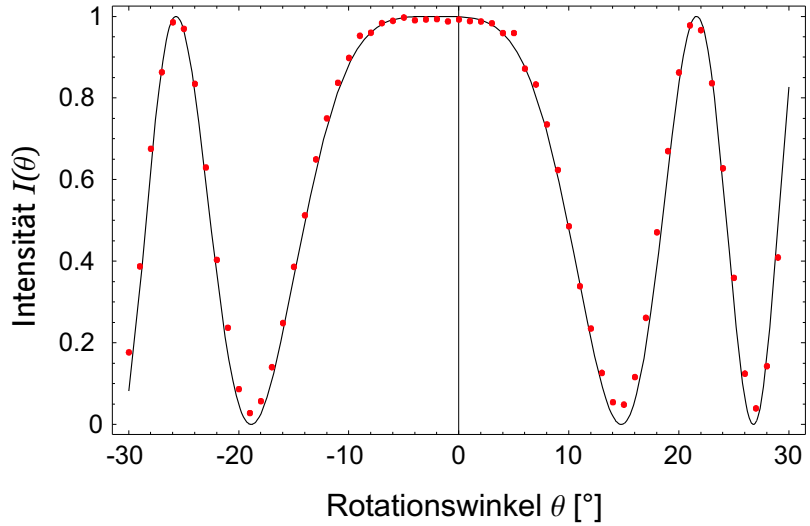


Abbildung 3.6: Intensität in Abhängigkeit des Rotationswinkels für Fluoreszenzphotonen der Quelle. Die Kurve (—) entspricht dem berechneten Verlauf. Sie ist *kein* Fit an die gemessenen Datenpunkte (•).

3.2.2 Detektion

Wie bereits erwähnt ist eine effiziente Detektion der Signalphotonen unabdingbar für das Übertreffen der klassischen Erfolgswahrscheinlichkeit. Ausdruck einer guten Detektionseffizienz ist ein möglichst hohes Verhältnis von Koinzidenz- zu Einzelzählrate. Um dies zu erreichen werden zum einen andere Detektormodule, wie in Abschnitt 2.2.3 verwendet und zum anderen wird die Einkopplung der Signalphotonen verändert. In Kapitel 2.1.2 wurde beschrieben, wie die Verwendung von single-mode Glasfasern zur spektralen Begrenzung der aufzusammelnden Photonen genutzt werden kann. Dieser Effekt ist jedoch bei der experimentellen Implementierung des Kommunikationskomplexitätsprotokolls, zumindest für die Signalphotonen nicht zielführend, da möglichst für jedes Triggerphoton auch das dazugehörige Partner-Photon registriert werden soll. Eine Beschränkung in der Kopplung erhöht allerdings das Risiko das Signalphoton nicht zu detektieren und soll daher vermieden werden. Der Spiegel der den optischen Weg

von Arm 1 in Abbildung 2.5(a) faltet wird entfernt, so daß die Photonen in diesem Arm ungehindert geradeaus propagieren können. Dies schafft Platz für das Einfügen aller später benötigten Komponenten. Der erste Versuch das Verhältnis von Koinzidenzen zu Einzelzählereignissen zu erhöhen, besteht zunächst darin die Signalphotonen über eine Linse (f=100 mm) in die multi-mode Fasern der Detektoren aus Abschnitt 2.2.3 zu fokussieren. So wird ein Wellenlängenbereich von ca. 11 nm erfasst. In dieser Konfiguration liegt das maximal erreichbare Koinzidenz- zu Einzelzählratenverhältnis bei 24%. Dieser Wert ist zwar höher als bei der Verwendung von single-mode Fasern (19%, siehe Abschnitt 2.3.1), aber ein Vergleich mit Gleichung 3.9 zeigt, dass er noch unterhalb der für fünf Parteien erforderlichen 25% liegt, von anderen negativen Einflüssen, die eine noch höhere Rate bedingen würden ganz abgesehen (siehe Gleichung 3.10). Bei der direkten Fokussierung der Photonen auf den Detektorchip einer in der Effizienz vergleichbaren, aber nicht fasergekoppelten APD ist das erzielte Resultat für η nur geringfügig besser. Das legt nahe, dass die Kopplung in multi-mode Fasern nicht der limitierende Faktor ist, sondern die Effizienz der APD. Verbessert man diese künstlich, indem man die Betriebsspannung um weitere 10 Volt über den aktuellen Wert von 17 Volt über Durchbruch erhöht, (siehe Anhang A.2.9), können Werte bis 33% erreicht werden. Eine derartige dauerhafte Erhöhung der Betriebsspannung kann aber zur Beschädigung des Detektorhalbleiterchips führen, weswegen diese Lösung nicht die endgültige sein kann. Für das Experiment werden aus diesem Grund kommerzielle SLiK^{TM} Detektormodule der Firma Perkin Elmer (SPCM-AQR-14) verwendet. Sie besitzen neben einer aktiven Quenching-Schaltung und einer niedrigen Dunkelzählrate von weniger als 100 Hz eine sehr hohe Photon-Detektionseffizienz von bis zu 60% im Wellenlängenbereich um 800 nm. Mit diesen Modulen wird ein Koinzidenz- zu Einzelzählratenverhältnis von 53% erzielt, was eine erfolgreiche Durchführung des Protokolls in Aussicht stellt.

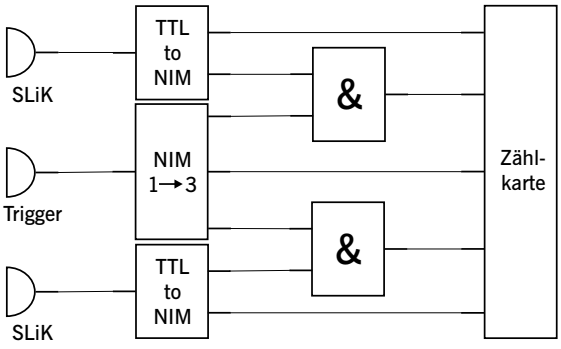


Abbildung 3.7: Signalregistrierung.

Während des Experiments sollen fünf verschiedene Werte aufgenommen werden, die Einzelzählraten eines jeden der drei verwendeten Detektoren, sowie die Koinzidenzen zwischen dem Triggerkanal und jedem der beiden Ausgänge des Polarisationsanalysators. Dafür wird zunächst das Triggersignal verdreifacht. Eines der drei Signale dient zu Registrierung der Einzelzählrate des Triggers, und jeweils eines als Eingang für ein Und-Gatter, wie es in Abschnitt 2.2.3 beschrieben ist. Die SLiK^{TM}Detektoren liefern

TTL Pulse. Diese werden in NIM Signale umgewandelt und gleichzeitig verdoppelt, wovon jeweils eines für die Registrierung der Einzelzählraten dient und das andere den zweiten Eingang der Und-Gatter belegt. Die Signale für die Einzelzählraten sowie die Ausgänge der Und-Gatter werden an die Zählkarte des Meßcomputers übergeben (siehe Abbildung 3.7). Das Koinzidenzzeitfenster beträgt 4 ns.

3.2.3 Experimenteller Aufbau

Der experimentelle Aufbau gliedert sich grob in drei Teile. Am Beginn steht die Quelle zur Erzeugung der Einzelphotonen sowie die Präparation des Anfangszustands. Daran schließt sich ein Bereich an, in dem die fünf Parteien gemäß ihren Zufallszahlen x_i die entsprechenden Phasenschübe mit Hilfe der YVO_4-Kristalle anwenden. Am Ende erfolgt das Auslesen des Polarisationszustands und somit die Bestimmung von $f(\vec{x})$. Eine schematische Darstellung zeigt Abbildung 3.8.

Wie bereits erwähnt wird Arm 1 nicht mehr mit einem Spiegel gefaltet. Ansonsten bleibt die Quelle jedoch unverändert. Arm 2 bildet den Triggerkanal. Die Photonen werden wie in Kapitel 2 dargestellt in Single-Mode Fasern eingekoppelt und über das in Abschnitt 2.2.3 beschriebene Detektormodul registriert. Um im Signalarm den Zustand $|+\rangle$ zu präparieren wird die Polarisationskorrelation der Quelle in der HV-Basis ausgenutzt. Im Triggerarm befindet sich ein Polarisator der horizontale Polarisation transmittiert. Das hat auf Grund der Korrelationen zur Folge, dass nur vertikal polarisierte Photonen aus dem Signalarm zu einer Koinzidenz führen können. Sie werden durch eine $\frac{\lambda}{2}$-Platte auf $-22,5\,^\circ$ in den Zustand $|+\rangle$ transformiert. Diese Methode hat gegenüber der zusätzlichen Positionierung eines Polarisators im Signalarm den Vorteil, dass Absorptionsverluste in Arm 1 vermieden werden.

In den vorangegangenen Ausführungen wurde der Phasenoperator als Kombination aus zwei Kristallen beschrieben. Anstelle hinter jeden drehbaren Kristall der fünf Parteien einen feststehenden zu setzen, kann jedoch auch ein Kristall der fünffachen Dicke am Ende positioniert werden, was ebenfalls die korrekte Kompensation des Gesamtphasenschubs ergibt. Für jede teilnehmende Partei steht folglich je ein Kristall zur Verfügung, der über einen Motor, wie er in Abschnitt 3.2.1.4 beschrieben ist, während der Durchführung des Protokolls auf die Position verfahren wird, welche dem jeweiligen Phasenschub für x_i entspricht. Die fünf zwei-Bit Strings $x_1, \ldots x_5$, die der Bedingung 3.2 genügen, erzeugt ein Zufallsgenerator. Die Winkelpositionen, die jeweils der Phase von x_i entsprechen, sind für jeden Kristall aus der Kurve $I(\theta)$ bekannt und werden vor Beginn des Protokolls einmalig in das Messprogramm eingegeben. Der sechste Kompensatorkristall ist ebenfalls drehbar (aber nicht motorisiert) montiert. Er wird derart justiert, dass in der Nullposition der restlichen Kristalle $\delta = 0$ gilt.

Die Zustandsanalyse erfolgt in der $\pm 45\,^\circ$-Basis, wofür eine $\frac{\lambda}{2}$-Platte bei einem Winkel

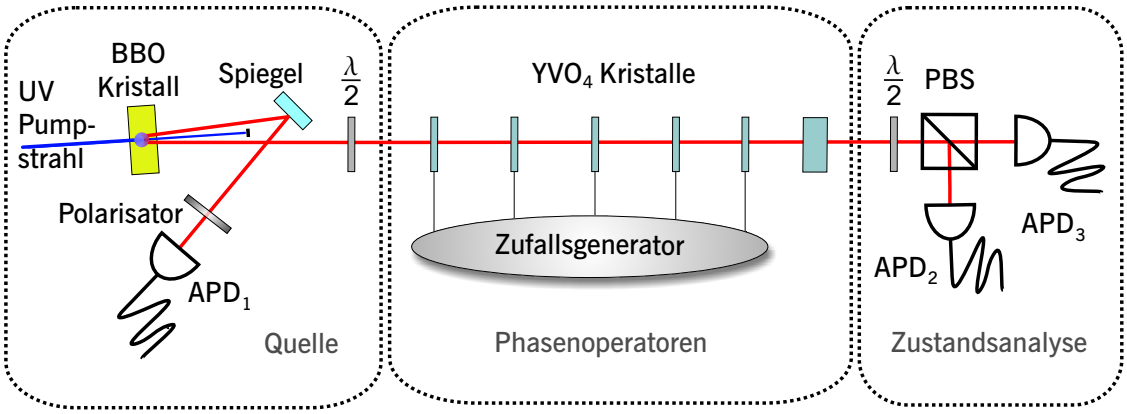


Abbildung 3.8: Schematische Darstellung des experimentellen Aufbaus.

von $22,5\,^\circ$ in Kombination mit einem polarisierenden Strahlteiler verwendet wird. Für die Detektion der Signalphotonen an den beiden Ausgängen des PBS werden die zuvor erwähnten SLiK$^{\text{TM}}$APD-Module verwendet.

3.3 Daten und Ergebnisse

Ziel des Experiments ist es, zu zeigen, dass trotz der experimentellen Beschränkungen, unter realistischen Bedingungen mit der heute zur Verfügung stehenden Technik die quantenmechanische Erfolgswahrscheinlichkeit für das in 3.1.2 vorgeschlagene Protokoll über der des besten klassischen Protokolls liegt. Die folgenden Abschnitte beschreiben die Durchführung des Protokolls und die Erhebung der Daten sowie deren statistische Auswertung zur experimentellen Bestimmung der quantenmechanischen Erfolgswahrscheinlichkeit p_{qm} und deren Fehler.

3.3.1 Durchführung

Da Wahrscheinlichkeit eine statistische Größe ist, impliziert dies bereits, dass es mit der einmaligen Durchführung des Protokolls nicht bewendet sein kann. Das Protokoll wird daher mehrere Male wiederholt. Ein Durchgang besteht dabei immer aus der Erzeugung der Zufallszahlen, der Bewegung der Motoren und schließlich dem senden eines „einzelnen“ Photons durch alle Kristalle sowie dessen Detektion und Zustandsbestimmung. Um wirklich nur ein Photon zu senden, wäre es beispielsweise möglich einen Verschluß vor dem Pumpstrahl anzubringen der sich für ein Zeitintervall öffnet, in dem im Mittel gerade ein Fluoreszenzphotonpaar erzeugt wird. Da dies nicht sehr praktikabel ist, werden stattdessen kontinuierlich Fluoreszenzphotonen erzeugt, aber die Detektoren lediglich für eine Zeitspanne „aktiviert“, in der durchschnittlich ein

Photon am Triggerdetektor ankommt.

3.3.2 Photonenstatistik des Triggerkanals

Die „Aktivierung“ der Detektoren wird indirekt von der Zählkarte des Computers vorgenommen, indem sie die Einzel- bzw. Koinzidenzereignisse nur in bestimmten Zeitintervallen aufnimmt. Die statistische Verteilung der Photonenzahl, die während eines endlichen Zeitintervalls registriert wird, hängt grundsätzlich von der Art des Erzeugungsprozesses des Lichts ab. Für eine Quelle kohärenten Lichts, wie dem Pumplaser der spontanen parametrischen Fluoreszenz, folgt sie einer Poisson-Verteilung. Da die im Triggerkanal detektierten Fluoreszenzphotonen aus dem Umwandlungsprozess der Photonen des Pumplasers stammen (siehe Abschnitt 2.1.1), soll für sie ebenfalls eine Poisson Verteilung angenommen werden. Die Wahrscheinlichkeit n Photonen in einem bestimmten Zeitintervall T zu registrieren, ist somit gegeben durch

$$p(n) = \frac{\bar{n}^n}{n!} \exp(-\bar{n}). \tag{3.24}$$

Der Mittelwert $\bar{n}$ ist abhängig von der optischen Ausgangsleistung P des Pumplasers und der Integrationszeit T der Messung, $\bar{n} \propto \mathrm{P} \cdot T$. Da für das Protokoll die Ereignisse von Interesse sind, bei denen gerade ein Photon im Triggerarm registriert wird, soll dafür die Wahrscheinlichkeit $p(1)$ maximiert werden. Wie aus Gleichung 3.24 trivial folgt, ist $p(1)$ maximal für $\bar{n} = 1$. Die Ausgangsleistung des Pumplasers soll aus verschiedenen Gründen[3] nicht verändert werden, d.h. es muss die Integrationszeit gefunden werden, für die $\bar{n} = 1$ ist. Bei einem Versorgungsstrom der Pumplaserdiode von 52 mA, was einer optischen Ausgangsleistung von $12,23$ mW entspricht, beträgt die optimale Integrationszeit $200\,\mu$s. Abbildung 3.9 zeigt für dieses Zeitintervall ein Histogramm der Anzahl detektierter Photonen im Triggerarm für 18000 Wiederholungen. Der Mittelwert beträgt $\bar{n} = 1,08944 \pm 0,00783$. Dafür ergeben sich Einzelphotonereignisse in $37,18\,\%$ der Fälle. Ebenfalls zu sehen ist in Abbildung 3.9 die zugehörige Poissonverteilung in blau. Die Übereinstimmung ist gut und somit die Annahme einer Poissonverteilung für die Anzahl registrierter Photonen im Triggerarm gerechtfertigt. Vereinzelte Abweichungen ergeben sich aufgrund von experimentellen Effekten wie beispielsweise der Totzeit[4] der Detektoren (siehe hierzu auch [50]).

[3] wie in Kapitel 2 diskutiert, ändert sich die Wellenlänge des Pumplasers mit der Ausgangsleistung, damit ändert sich auch die Wellenlänge der Fluoreszenzphotonen, was sich wiederum auf die Kopplung auswirkt ... usw.

[4] Nach dem Auslösen eines Spannungsdurchbruchs ist eine APD für die Dauer des Quenchens, d.h. des Löschens der Spannungslawine, unsensitiv (siehe Anhang A.2.7).

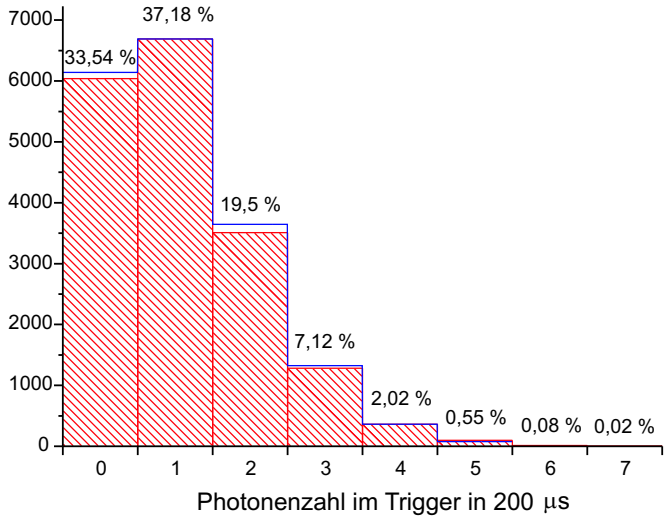


Abbildung 3.9: Histogramm der Photonenzahl im Triggerdetektor bei einer Integrationszeit von 200 μs für 18000 Wiederholungen mit Poissonfit (—).

3.3.3 Datenauswertung und Erfolgsrate

Um die quantenmechanische Erfolgswahrscheinlichkeit p_{qm} zu ermitteln, wurde das Protokoll 18000 mal wiederholt. Eine Durchführung dauert ca. eine Sekunde. Der Großteil der Zeit wird für die Bewegung der Motoren benötigt. Die Erzeugung der Zufallszahlen und die 200 μs Integrationszeit sind dabei vernachlässigbar. Die gesamte Messdauer beträgt folglich in etwa fünf Stunden. Aus den Rohdaten werden bei der Auswertung alle Ereignisse selektiert, in denen ein Photon im Triggerarm detektiert wurde. Dies ist bei $Z_{sift} = 6692$ Durchgängen der Fall, was $37,18\,\%$ entspricht (siehe Abbildung 3.9). Aus diesen gültigen Durchgängen wurde $Z_{koin} = 3025$ Mal das Partnerphoton in einem Ausgang des PBS registriert. Das entspricht einem Koinzidenz- zu Einzelzählratenverhältnis von $\varsigma = 45,20\,\%$. Dessen Abweichung von den in Abschnitt 3.2.2 erwähnten $53\,\%$ ist durch die Transmissionsverluste der optischen Komponenten zu erklären. Nach Einfügen des PBS reduziert sie sich bereits auf $51\,\%$ und wird durch jeden Kristall bzw. Wellenplatte in etwa um weitere $0,7\,\%$ vermindert. Von den $Z_{koin} = 3025$ Koinzidenzen wurde $Z_{wro} = 101$ mal im falschen und $Z_{cor} = 2924$ mal im richtigen Ausgang detektiert. Das Verhältnis $\varrho = Z_{cor}/Z_{koin} = 96,66\,\%$ kann als Maß dafür betrachtet werden, wie gut der Phasenschub mittels der Kristalle gesetzt wird. Bei $Z_{ran} = 3667$ Durchgängen wurde keine Koinzidenz detektiert. In diesen Fällen wurde der Wert von $f(\vec{x})$ erraten, was mit $50\,\%$ Wahrscheinlichkeit zum Erfolg führt. Daraus läßt sich bereits ein Wert für die experimentelle Quantenerfolgswahrscheinlichkeit abschätzen:

$$p_{qm} = 0,4520 \cdot 0,9666 + 0,5480 \cdot 0,5 = 71,09\,\%. \tag{3.25}$$

Allerdings wird nur im Grenzwert für Z_{ran} gegen unendlich exakt in der Hälfte der Fälle richtig geraten. Für eine endliche Zahl wird die Rate möglicherweise etwas darüber oder darunter liegen. Deswegen wurde der Auswertungsprozess für die selben Daten 3000 mal wiederholt. Dabei treten Fälle auf, in denen man etwas mehr Glück beim Raten hat und solche bei denen man weniger Glück hat. Dementsprechend schwankt auch p_{qm} mit einer gewissen Breite um den Wert von $71,09\,\%$. Die unterschiedlichen Werte für p_{qm} aus den 3000 Auswertungen wurden wieder in ein Histogramm gefüllt, das Abbildung 3.10 zeigt. Es ergibt sich eine Normalverteilung um den Wert von Gleichung 3.25, deren

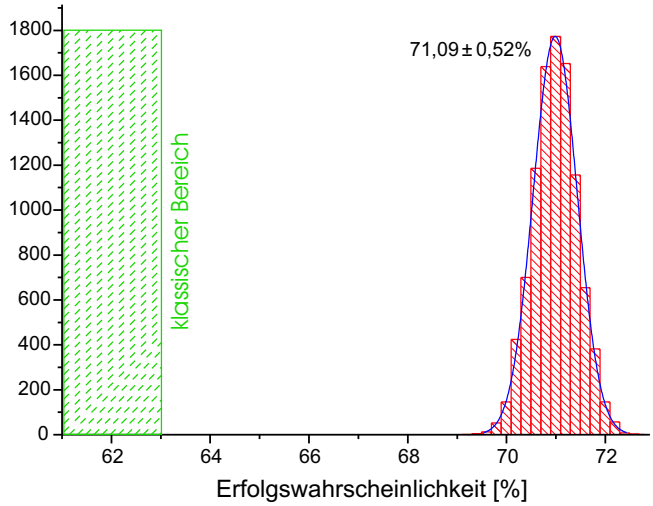


Abbildung 3.10: Histogramm der experimentellen Quantenerfolgsrate mit Gaußfit (—) an die Verteilung.

Breite als Fehler für p_{qm} interpretiert werden kann. Die Breite hängt lediglich von Z_{ran} und somit indirekt von Z_{sift} ab, jedoch nicht von der Anzahl der Wiederholungen bei der Datenauswertung. Die Zahl von 3000 Wiederholungen wurde lediglich gewählt um eine vernünftige Darstellung durch ein Histogramm zu ermöglichen. Ein Gaußfit mit einer Breite von $1,04\,\%$ (FWHM) an die erhaltene Verteilung ergibt schließlich das Endergebnis von

$$p_{qm} = 71,09 \pm 0,52\,\%. \tag{3.26}$$

Das liegt signifikant über dem klassischen Limit von $p_{kl} = 62,5\,\%$. Abbildung 3.11 zeigt den zeitlichen Verlauf dreier Größen während der Messung. Dies sind die Erfolgsrate und das Koinzidenz- zu Einzelzählratenverhältnis ς sowie die Rate korrekter Detektionen ϱ. Man sieht, dass sich ϱ bereits nach knapp 4000 Wiederholungen auf einen konstanten Wert einpendelt. Für ς und p_{qm} dauert dieser Vorgang etwas länger, aber ab ca. 14000 Durchgängen erlangen auch sie einen annähernd konstanten Wert. Aus all den vorangegangen Betrachtungen und Abbildung 3.11 wird ebenfalls deutlich, dass in der Tat ϱ und ς die entscheidenden Parameter des Experiments sind. Der anfängliche Abfall von ς wird durch den Anstieg von ϱ kompensiert, aber sobald ϱ seinen Mittelwert erreicht hat, folgt die Erfolgsrate exakt den Schwankungen von ς. Die verschiedenen,

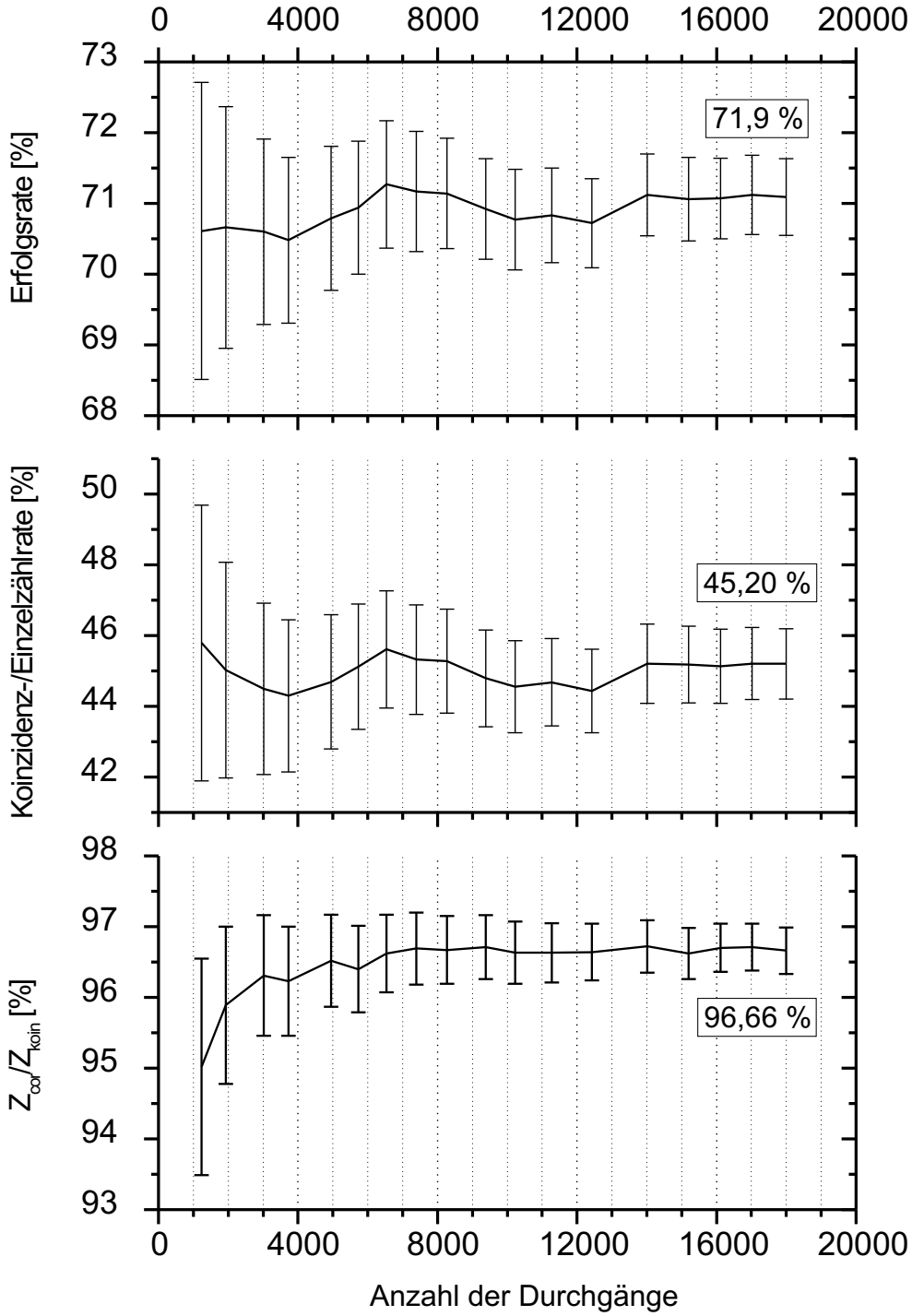


Abbildung 3.11: Zeitlicher Verlauf der Erfolgsrate, des Koinzidenz- zu Einzelzählratenverhältnisses und Z_{cor}/Z_{koin}.

in Gleichung 3.10 vorkommenden, Größen können in ϱ und ς zusammengefasst werden. Die Parameter s und μ spiegeln sich in ϱ wieder und die Transmission der Komponenten t, zusammen mit der Detektionseffizienz η werden in ς berücksichtigt.

Die Verwendung effizienter Detektoren und eine ebenso einfache, wie gute Technik mehrere Phasenschübe mit ausreichender Genauigkeit kumulativ zu setzen, führen in diesem Experiment unter absolut realistischen und fairen Bedingungen zum Beweis der Überlegenheit der Quantenkommunikation gegenüber ihrer klassischen Entsprechung.

Kapitel 4

Quanten-„Secret-Sharing“

Im vorangegangenen Kapitel wurde gezeigt, wie ein zunächst für die Verwendung verschränkter Teilchen formuliertes Mehrparteien-Kommunikationsprotokoll mittels sequenzieller Übertragung eines einzelnen Qubits auf analoge Weise mit verhältnismäßig geringerem Aufwand realisiert werden kann. Dieser Ansatz soll im Folgenden dazu verwendet werden, ein anderes typisches Kommunikationsproblem für mehrere Parteien, das sog. „Secret-Sharing“, auf quantenmechanischem Weg zu lösen. Dieses Kapitel erklärt daher zunächst allgemein was man unter dem Begriff „Secret-Sharing“ zu verstehen hat. Es zeigt klassische Verfahren auf, die zur Lösung eines derartigen Kommunikationsszenarios gewöhnlich verwendet werden. Dem gegenübergestellt werden quatenmechanische verschränkungsbasierte Protokolle. Ein neues Protokoll wird eingeführt, das mit einzelnen Photonen eine äquivalente Problemlösung liefert. Ausgehend von dem Versuchsaufbau aus Kapitel 3 werden die experimentelle Implementierung dieses Protokolls sowie die gewonnen Ergebnisse präsentiert.

4.1 Theoretische Grundlagen

4.1.1 „Secret-Sharing“ - Das Problem

Wie der Name „Secret-Sharing“ bereits vermuten lässt, behandelt dieses Kommunikationsproblem die Aufteilung eines Geheimnises. Dabei ist in der Tat gemeint, dass die geheime Nachricht auf mehrere Parteien aufgeteilt und nicht einfach nur verteilt wird. Das Prinzip lässt sich am besten an Hand eines Standardbeispiels verdeutlichen [51]:

Die Aktivierung der Abschußsequenz von Nuklearraketen sei durch einen geheimen Code geschützt. Es soll sichergestellt werden, dass die Entscheidungsgewalt über deren Abschuß nicht alleine bei einer Person liegt. Vielmehr soll es dafür mindestens dreier

Personen bedürfen. Eine Möglichkeit dieses Problem zu lösen besteht darin, den Code in drei Teile zu zerlegen und diese an drei Personen zu verteilen. Jede Einzelperson für sich genommen kann dabei nichts bewirken, da sie nur ein drittel der benötigten Information besitzt. Selbst zwei Personen zusammen wären nicht ausreichend. Lediglich die Zusammenarbeit aller drei kann den Abschuß initialisieren. Dieses Szenario impliziert eine Menge an Variationen. Beispielsweise könnte man verlangen, dass entweder der Präsident alleine oder drei seiner wichtigsten Minister zusammen die Rakete starten können. Es wäre auch noch komplizierter denkbar, z.B. der Präsident alleine oder drei Minister oder falls weder drei Minister noch der Präsident abkömmlich sind, reicht ein Minister zusammen mit fünf Beschäftigten des Verteidigungsministeriums, von denen mindestens vier bereits länger als zehn Jahre dort arbeiten, usw. Alle Aufteilungsmöglichkeiten die man dabei im Kopf haben mag, lassen sich mathematisch durch den Begriff des (m, n)-Schwellenschemas modellieren. Bei einem (m, n)-Schwellenschema wird eine geheime Nachricht in n Teile zerteilt, wovon jede beliebige Kombination von m Teilen ausreicht um die Nachricht zu rekonstruieren.

4.1.2 Klassische „Secret-Sharing“ Protokolle

Es gibt eine Reihe von klassischen „Secret-Sharing“ Protokollen, wovon hier zwei exemplarisch vorgestellt werden sollen. Das erste ist sehr allgemein und soll dem Leser lediglich eine Idee vermitteln wie ein (m, n)-Schwellenschema, mit $m \neq n$, mathematisch in einer Weise umgesetzt werden kann, dass tatsächlich jede beliebige Teilmenge von m Parteien ein auf n Parteien verteiltes Geheimnis rekonstruieren kann. Es ist für das Verständnis der weiteren Abschnitte nicht zwingend erforderlich und kann daher beim Lesen auch übersprungen werden. Das zweite Protokoll ist sehr einfach und zeigt wie eine Person Alice eine geheime Nachricht derart an zwei Parteien Bob und Charlie verteilen kann, dass nur beide gemeinsam in der Lage sind die Nachricht zu lesen. Es stellt die Verknüpfung zwischen klassischen und quantenmechanischen Protokollen her.

4.1.2.1 Ein (m, n)-Schwellenschema

Das nachfolgende Protokoll basiert auf der Verwendung von polynomialen Gleichungssystemen und beruht auf der Tatsache, dass zur eindeutigen Bestimmung vom m Unbekannten genau m Gleichungen gelöst werden müssen [51]:

1. Man wähle eine Primzahl p, die sowohl größer als die maximale Anzahl an Geheimnisteilen n als auch größer als die maximal mögliche Länge des Geheimnises ist und generiere ein beliebiges Polynom vom Grad $m - 1$:

$$F(x) = (c_{m-1}x^{m-1} + c_{m-2}x^{m-2} + \cdots + c_{m-(m-1)}x^{m-(m-1)} + c_{m-m}x^{m-m}) \mod p \tag{4.1}$$

2. Die Koeffizienten $c_{m-1}, \ldots, c_{m-(m-1)}$ sind zufällig und geheim und der Letzte c_{m-m} ist das aufzuteilende Geheimnis M.

3. Man erzeuge die n Geheimnisteile k_i mit $i = 1, 2, \ldots, n$ in der Weise, dass

$$k_i = F(x_i), \text{ mit } x_i = i \tag{4.2}$$

gilt.

4. Man vernichte bzw. lösche alle Koeffizienten $c_{m-1}, \ldots, c_{m-(m-1)}$ und verteile die k_i an die beteiligten Parteien.

5. Zur Rekonstruktion muss das Gleichungssystem

$$\begin{aligned}
&(c_{m-1}l_1^{m-1} + c_{m-2}l_1^{m-2} + \cdots + c_{m-(m-1)}l_1^{m-(m-1)} + c_{m-m}l_1^{m-m}) \mod p = k_{l_1}\\
&(c_{m-1}l_2^{m-1} + c_{m-2}l_2^{m-2} + \cdots + c_{m-(m-1)}l_2^{m-(m-1)} + c_{m-m}l_2^{m-m}) \mod p = k_{l_2}\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots\\
&(c_{m-1}l_{m-1}^{m-1} + c_{m-2}l_{m-1}^{m-2} + \cdots + c_{m-(m-1)}l_{m-1}^{m-(m-1)} + c_{m-m}l_{m-1}^{m-m}) \mod p = k_{l_{m-1}}\\
&(c_{m-1}l_m^{m-1} + c_{m-2}l_m^{m-2} + \cdots + c_{m-(m-1)}l_m^{m-(m-1)} + c_{m-m}l_m^{m-m}) \mod p = k_{l_m}
\end{aligned} \tag{4.3}$$

gelößt werden, wobei $\{l_1, l_2, \ldots, l_m\}$ eine von $\left(\begin{array}{c} n \\ m \end{array} \right) = \frac{n!}{(n-m)!m!}$ möglichen m-elementigen Teilmengen von $\{1, 2, \ldots, n\}$ ist.

Um die m Unbekannten zu finden, bedarf es genau der m Gleichungen. Mehr als m Gleichungen sind redundant und bereits $m - 1$ zur eindeutigen Lösung nicht ausreichend. Dieses Verfahren bietet, analog zum „one-time-pad“ (siehe Kapitel 1.3), perfekte Sicherheit, sofern die Koeffizienten zufällig ausgewählt werden. Selbst mit unbegrenzter Rechenleistung können $m - 1$ Personen das Geheimnis nicht aufdecken, da eine Suche über alle Möglichkeiten lediglich ergibt, dass jede denkbare Nachricht als Geheimnis in Frage kommt.

4.1.2.2 Ein einfaches $(2, 2)$-Schwellenschema

Das nun folgende Protokoll ist wesentlich einfacher, läßt aber mehr Gemeinsamkeiten zwischen der in Kapitel 1.3 angesprochenen Kryptographie und „Secret-Sharing“ erkennen. Eine Person, Alice, will ein Geheimnis an zwei Personen Bob und Charlie derart verteilen, dass ausschließlich beide zusammen in der Lage sind die Nachricht zu rekonstruieren. Das entspricht einem $(2, 2)$-Schwellenschema. Um dies zu erreichen, kann Alice wie folgt vorgehen:

1. Das zu verteilende Geheimnis sei ein Bit-String der Länge l. Alice generiert einen zufälligen Bitstring der gleichen Länge, also eine zufällige Abfolge von Nullen und Einsen.

2. Sie addiert die beiden Strings, Geheimnis und Zufallsstring, bitweise Modulo zwei, wobei sich die Zufälligkeit des einen auf den Summenstring überträgt.

3. Alice sendet je einen der zufälligen, aber untereinander korrelierten Strings zu Bob und zu Charlie.

Sowohl für Bob, als auch für Charlie stellt sich der Bit-String, den sie erhalten als scheinbar zufällige Reihung von Nullen und Einsen dar. Wenn beide jedoch zusammen arbeiten und ihre Strings erneut addieren, wird die Nachricht preisgegeben.

Wie bei der Kryptographie bleibt aber auch hier bei beiden Protokollen die Frage zu klären, wie die Parteien trotz Lauschangriffen von Außenstehenden auf sichere Weise in den Besitz der Teilgeheimnisse kommen. Ein weiteres Problem, das sich bei „Secret-Sharing“ Protokollen ergibt, ist die Anwesenheit von Betrügern innerhalb der beteiligten Personen. Es kann nicht ausgeschlossen werden, dass eine der Parteien versucht in den Besitz der anderen Teilgeheimnisse zu kommen um die Nachricht alleine rekonstruieren zu können.

4.1.3 Ein verschränkungsbasiertes quantenmechanisches Protokoll

Sowohl die sichere Verteilung der Teilgeheimnisse gegen Abhörattacken von außerhalb als auch die Enttarnung von Betrügern innerhalb der beteiligten Parteien, kann durch die Verwendung quantenmechanischer Protokolle sichergestellt werden.

Grundsätzlich könnte Alice ein beliebiges Quantenkryptographieprotokoll, beispielsweise das in Abschnitt 1.3 angesprochene Ekert Protokoll, verwenden um die Teilgeheimnisse sicher an Bob und Charlie zu übermitteln. Die Aufteilung der Nachricht in Teilstücke würde hierbei nach wie vor durch klassische Protokolle erfolgen, lediglich deren sichere Übertragung würde quantenmechanisch durchgeführt. Alice müßte dafür allerdings sowohl mit Bob als auch mit Charlie einen Übertragungsschlüssel etablieren, der dann jeweils für den sicheren Austausch der beiden Geheimnisteile verwendet werden kann, was mit einigen Kommunikationsschritten, bereits im Vorfeld des eigentlichen „Secret-Sharing“ Protokolls, verbunden wäre. Darüberhinaus ist die Aufteilung einer Nachricht, wie sie im obigen Protokoll 4.1.2.2 beschrieben ist, für mehr als zwei Parteien keine triviale Angelegenheit mehr. Es gibt ein Quanten „Secret-Sharing“ Protokoll [52], das mit Hilfe eines verschränkten Mehrteilchenzustands sowohl die sichere Auf- als auch Verteilung eines Geheimnisses auf einfache Weise bewerkstelligt. Da das

Prinzip dieses Protokolls später auf die Verwendung einzelner Qubits übertragen wird, soll es hier vorgestellt werden:

Von den Parteien Alice, Bob und Charlie besitzt jede ein Photon des Drei-Teilchen GHZ-Zustands

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|HHH\rangle + |VVV\rangle\right). \tag{4.4}$$

Dieser Zustand ist verschränkt. Er kann weder als Produkt von drei Ein-Teilchen Zuständen, noch als Produkt eines Einteilchen Zustands mit einem verschränkten Zwei-Teilchen Zustand geschrieben werden. Die Korrelationsfunktion E für diesen Drei-Photonen Zustand ist definiert als der Erwartungswert des Produkts dreier lokaler Messresultate. Die Messung einer elliptischen Polarisation in drei Moden $j = a, b, c$ läßt sich durch die Operatoren

$$\hat{\sigma}_j(\phi_i) = \sum_{k_j} k_j \,|\, k_j, \phi_j \,\rangle\langle\, k_j, \phi_j \,|\, \tag{4.5}$$

darstellen, wobei jeweils das gemessene Teilchen in die Eigenzustände von $\hat{\sigma}$

$$|\, k_j, \phi_j \,\rangle = \frac{1}{\sqrt{2}}\left(|\, H \,\rangle + k_j e^{i\phi}|\, V \,\rangle\right) \tag{4.6}$$

mit den lokalen Reslutaten $k_j = \pm 1$ projiziert wird. Somit ergibt sich für die Korrelationsfunktion

$$\begin{aligned} E(\phi_a, \phi_b, \phi_c) &= \langle \hat{\sigma}_a(\phi_a)\hat{\sigma}_b(\phi_b)\hat{\sigma}_c(\phi_c)\rangle \\ &= \cos(\phi_a + \phi_b + \phi_c). \end{aligned} \tag{4.7}$$

Bei der Durchführung des Protokolls wählt jede Partei zufällig zwischen zwei verschiedenen Polarisationsmessungen aus, zum einen $\hat{\sigma}(0)$ mit den Eigenvektoren

$$|\pm x\,\rangle = \frac{1}{\sqrt{2}}\left(|\, H \,\rangle \pm |\, V \,\rangle\right) \tag{4.8}$$

und zum anderen $\hat{\sigma}(\pi/2)$ mit den Eigenvektoren

$$|\pm y\,\rangle = \frac{1}{\sqrt{2}}\left(|\, H \,\rangle \pm i|\, V \,\rangle\right). \tag{4.9}$$

Messen Alice, Bob and Charlie beispielsweise alle in der Basis $|\pm x\,\rangle$ läßt sich $|GHZ\,\rangle$ in folgender Form schreiben

$$\begin{aligned} |GHZ\,\rangle = \frac{1}{2\sqrt{2}}[&(|+x\,\rangle_a|+x\,\rangle_b + |-x\,\rangle_a|-x\,\rangle_b)\,|+x\,\rangle_c \\ &+ (|+x\,\rangle_a|-x\,\rangle_b + |-x\,\rangle_a|+x\,\rangle_b)\,|-x\,\rangle_c]. \end{aligned} \tag{4.10}$$

In dieser Schreibweise sieht man unmittelbar, dass Charlie das Resultat $k_c = +1$ für $k_a = k_b$ bzw. $k_c = -1$ für $k_a = -k_b$ erhält. Um den Wert von Alices Bit k_a in Erfahrung zu bringen, benötigt er allerdings das Ergebnis für k_b von Bob.

Nach der Messung geben Bob und Charlie die gewählten Basen bekannt; somit kann Alice die Durchgänge, bei denen alle Ergebnisse (anti-)korreliert sind auswählen. Da jede Partei zufällig zwischen den beiden Basen wechselt, wird dabei im Mittel die Hälfte aller Durchgänge verworfen. Tabelle 4.1 zeigt die Kombinationen der Basiswahl, die zu (anti-)korrelierten Ergebnissen führen. In diesen Fällen können Bob und Charlie

	Alice	Bob	Charlie
gewählte Basis	$\|\pm x\rangle$	$\|\pm x\rangle$	$\|\pm x\rangle$
	$\|\pm x\rangle$	$\|\pm y\rangle$	$\|\pm y\rangle$
	$\|\pm y\rangle$	$\|\pm x\rangle$	$\|\pm y\rangle$
	$\|\pm y\rangle$	$\|\pm y\rangle$	$\|\pm x\rangle$

Tabelle 4.1: Basiskombinationen, die zu (anti-)korrelierten Ergebnissen führen.

gemeinsam den Bitwert von Alice aufdecken, indem sie ihre Resultate vergleichen. Bob und Charlie können dafür z.B. Tabelle 4.2 verwenden.

Die Sicherheit dieses Protokolls gegenüber Abhörattacken durch Aussenstehende folgt analog zur Quantenkryptographie (siehe Abschnitt 1.3). Es soll daher der Fall betrachtet werden, bei dem eine der beteiligten Parteien betrügt und versucht das Geheimnis alleine, ohne die Mithilfe des Partners zu rekonstruieren.

Angenommen Bob ist unehrlich und konnte, wie auch immer, zweier Photonen habhaft werden, seinem eigenen und Charlies. Sein Ziel ist es, durch eine Messung an beiden Teilchen Alices Bit zu erfahren und bei diesem Versuch unentdeckt zu bleiben, wenn er nach der Messung, eines der Teilchen zu Charlie weitersendet. Um dies zu erreichen, muß er, ohne Alices Basiswahl zu kennen, seine beiden Photonen in der Zwei-Teilchen Basis $1/\sqrt{2}\,(|HH\rangle \pm |VV\rangle)$ oder $1/\sqrt{2}\,(|HH\rangle \pm i|VV\rangle)$ messen. Da Alice zufällig zwischen einer Messung in der $|\pm x\rangle$-Basis und der $|\pm y\rangle$-Basis wechselt, wird er mit Wahrscheinlichkeit 1/2 die falsche Wahl treffen. Ist dies der Fall, treten nach der Weitersendung eines der Teilchen, bei der finalen Ein-Teilchen Messung in der $|\pm x\rangle$- bzw. $|\pm y\rangle$-Basis durch Charlie und ihn selbst mit fünfzigprozentiger Wahrscheinlichkeit keine korrekten GHZ-Korrelationen auf. Die gesamte Fehlerwahrscheinlichkeit ist daher 1/4; 1/2 die falsche Basis zu wählen und 1/2 am Ende das falsche Endergebnis zu erhalten. Eine ausführlichere Betrachtung dieser und komplizierterer Betrugsstrategien findet sich in [52]. Die experimentelle Umsetzbarkeit des eben vorgestellten Protokolls durch die Verwendung eines „Pseudo-GHZ-Zustands“[1] wurde in [53] demonstriert. In dieser Arbeit soll im folgenden gezeigt werden, wie sich das Prinzip dieses Protokolls auf die Verwendung einzelner unverschränkter Photonen übertragen lässt.

[1] Es wird ein Energie-Zeitverschränkter Zwei-Photonen Zustand verwendet.

	...	Charlie	...
⋮	⋱		...
Bob		Alice	
⋮	⋮		⋱

	$\|+x\rangle$	$\|-x\rangle$	$\|+y\rangle$	$\|-y\rangle$
$\|+x\rangle$	$\|+x\rangle$	$\|-x\rangle$	$\|-y\rangle$	$\|+y\rangle$
$\|-x\rangle$	$\|-x\rangle$	$\|+x\rangle$	$\|+y\rangle$	$\|-y\rangle$
$\|+y\rangle$	$\|-y\rangle$	$\|+y\rangle$	$\|-x\rangle$	$\|+x\rangle$
$\|-y\rangle$	$\|+y\rangle$	$\|-y\rangle$	$\|+x\rangle$	$\|-x\rangle$

Tabelle 4.2: Messkorrelation für GHZ-Zustand.

4.1.4 Eine Lösung mit einzelnen Qubits

Ausgehend von dem in Kapitel 3 beschriebenen Experiment entstand die Idee zu einem Quanten-„Secret-Sharing“ Protokoll, bei dem die Auf- und Verteilung des Geheimnisses durch die sequentielle Kommunikation einzelner Qubits erfolgt. Dieser Abschnitt beschreibt das Protokoll zunächst für drei Personen und stellt dann dessen kanonische Erweiterung auf N Personen vor.

4.1.4.1 Einzel-Qubit 3-Parteien „Secret-Sharing“

Die teilnehmenden Parteien seien wieder Alice, Bob und Charlie genannt.

Alice präpariert ein Photon zufällig in einem der vier Zustände

$$|\pm x\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle \pm |V\rangle\right), \tag{4.11}$$

$$|\pm y\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle \pm i|V\rangle\right). \tag{4.12}$$

Ein Zustands-Paar kodiert dabei ein Bit-Paar, das heißt $|+x\rangle \mathrel{\widehat{=}} +1$ bzw. $|-x\rangle \mathrel{\widehat{=}} -1$ und analog für $|\pm y\rangle$. Ein Bit wird hier aus praktischen Gründen mit den Werten ± 1, anstelle der sonst üblichen $0, 1$ bezeichnet. Der Zustand des Photons lässt sich dann in der Form

$$|\chi\rangle_A = \frac{1}{\sqrt{2}}\left(|H\rangle + e^{i\phi_A}|V\rangle\right), \tag{4.13}$$

mit $\phi_A = 0$, $\phi_A = \pi/2$, $\phi_A = \pi$ oder $\phi_A = 3\pi/2$ darstellen. Die Messung eines der Zustände $|\pm x\rangle$ in der $|\pm y\rangle$-Basis und vice versa führt zu einem völlig zufälligen Resultat. Alice sendet das so präparierte Photon zu Bob, der die unitäre Transformation

$$U(\phi_B) = |H\rangle\langle H| + e^{i\phi_B}|V\rangle\langle V| \tag{4.14}$$

anwendet, wobei er zufällig zwischen $\phi_B = 0$, $\phi_B = \pi/2$, $\phi_B = \pi$ und $\phi_B = 3\pi/2$ wechselt. Dies resultiert im Zustand

$$|\chi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + e^{i(\phi_A+\phi_B)}|V\rangle\right). \tag{4.15}$$

Anschließend sendet er das Teilchen weiter zu Charlie, der eine ähnliche Transformation durchführt. Charlie variiert zufällig zwischen $\phi_C = 0$ und $\phi_C = \pi/2$. Nach der Aktion von Charlie befindet sich das Photon im Zustand

$$|\chi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + e^{i(\phi_A+\phi_B+\phi_C)}|V\rangle\right). \tag{4.16}$$

Abschließend misst Charlie das Photon in der Basis $\{1/\sqrt{2}\,(|H\rangle \pm |V\rangle)\}$. Der zufällige Phasenschub ϕ_C zusammen mit der Messung in der Basis $\{1/\sqrt{2}\,(|H\rangle \pm |V\rangle)\}$ kann auch als zufällige Messung in den Basen $|\pm x\rangle$ oder $|\pm y\rangle$ aufgefasst werden. Dabei erhält Charlie das Ergebnis $1/\sqrt{2}\,(|H\rangle + |V\rangle)$ mit der Wahrscheinlichkeit

$$p(\phi_A, \phi_B, \phi_C, +) = \frac{1}{2}\left(1 + \cos(\phi_A + \phi_B + \phi_C)\right) \tag{4.17}$$

und das Ergebnis $1/\sqrt{2}\,(|H\rangle - |V\rangle)$ mit der Wahrscheinlichkeit

$$p(\phi_A, \phi_B, \phi_C, -) = \frac{1}{2}\left(1 - \cos(\phi_A + \phi_B + \phi_C)\right). \tag{4.18}$$

Der Erwartungswert dieser Resultate ist gegeben durch

$$\begin{aligned} E(\phi_A + \phi_B + \phi_C) &= p(\phi_A, \phi_B, \phi_C, +) - p(\phi_A, \phi_B, \phi_C, -) \\ &= \cos(\phi_A + \phi_B + \phi_C). \end{aligned} \tag{4.19}$$

Das entspricht exakt der Korrelationsfunktion des Dreiparteien GHZ-„Secret-Sharing“ Protokolls des vorangegangenen Abschnitts (vergleiche Gleichung 4.7).

Um feststellen zu können, wann obige Schritte zur Etablierung eines gemeinsamen Bits beitragen, teilt Bob seine Aktionen in zwei Klassen ein, in eine Klasse X, bei der $\phi_B \in \{0, \pi\}$ und eine Klasse Y, bei der $\phi_B \in \{\pi/2, 3\pi/2\}$ gilt. Nach jedem vollständigen Durchlauf informiert Bob Alice, ob sein Phasenschub der Klasse X oder Y angehört. Charlie unterrichtet Alice ob seine Messung in der $|\pm x\rangle$- oder $|\pm y\rangle$-Basis durchgeführt wurde. Alice kann so die Durchgänge auswählen, in denen es zu (anti-) korrelierten Ergebnissen kommt (siehe Tabelle 4.3), was sich im Durchschnitt in der Hälfte aller Fälle ereignet. Es sei betont, dass Bob den Wert von ϕ_B und Charlie das

Präparationsbasis von Alice	Klasse von Bob	Messbasis von Charlie
$\|\pm x\rangle$	X	$\|\pm x\rangle$
$\|\pm x\rangle$	Y	$\|\pm y\rangle$
$\|\pm y\rangle$	X	$\|\pm y\rangle$
$\|\pm y\rangle$	Y	$\|\pm x\rangle$

Tabelle 4.3: Kombinationen, die zu (anti-)korrelierten Ergebnissen führen.

Ergebnis der Messung *nicht* bekanntgeben. Alice teilt beiden die gewählten Mess-bzw.

Präparationsbasen, sowie die von Bob gewählte Klasse mit. Charlie kann ausgehend von seinem Messresultat nur auf den Wert von Alices Bit schließen, falls er den Wert von ϕ_B erfährt, und bedarf daher der Hilfe von Bob. Selbige Überlegung gilt umgekehrt analog für Bob, der das Messergebnis von Charlie benötigt. Nachdem eine ausreichende Menge an gültigen Durchgängen vorliegt, wählt Alice daraus wahllos einen Teil aus, für den die Korrelationen öffentlich überprüft werden.

4.1.4.2 Lauschangriffe und Betrügereien

Angenommen Bob ist unehrlich und sein Ziel ist es, ohne die Mithilfe von Charlie den Wert von Alices Bit zu erfahren, indem er eine Polarisationsmessung an dem Photon durchführt, bevor er $U(\phi_B)$ anwendet und das Photon zu Charlie weitersendet. Er kann diese Messung entweder in der $|\pm x\rangle$- oder der $|\pm y\rangle$-Basis vollziehen. Da Alice jedoch beliebig zwischen den Basen wechselt wird Bob in der Hälfte der Fälle seine Wahl falsch treffen, was ein zufälliges Messresultat zur Folge hat. Er wendet auf den Zustand, in den das Photon durch seine Messung projiziert wird, $U(\phi_B)$ an und sendet den resultierenden Zustand weiter zu Charlie. Misst Charlie derart, dass dieser Durchgang für eine Korrelation in Frage kommt, hat Bob, sollte es zum öffentlichen Vergleich kommen, eine fünfzigprozentige Chance, dass Charlies Messergebnis mit den vermeintlichen Einstellungen kompatibel ist. Das wird am einfachsten an einem Beispiel deutlich:

Bob mißt in der $|\pm x\rangle$-Basis, danach sei der Zustand $|+x\rangle$ und er wendet darauf $U(\phi_B)$ mit $\phi_B = \pi/2$ an. Die folgenden zwei Fälle, die gleichwahrscheinlich auftreten, sind zu unterscheiden:

1. Alice hat das Photon in der $|\pm x\rangle$-Basis präpariert. Das Protokoll läuft ohne Fehler wie gewohnt ab und Bob weiß Alices Bitwert aus seinem Messresultat.

2. Alice hat das Photon in der $|\pm y\rangle$-Basis präpariert, z.B. $\phi_A = 3\pi/2$. Bobs Messresultat ist folglich zufällig und sei $|+x\rangle$. Charlie wählt die $|\pm x\rangle$-Basis und Alice erkennt diesen Durchgang als gültig an, siehe Tabelle 4.3 Zeile 4. (Würde Charlie in der $|\pm y\rangle$-Basis messen, würde dieser Durchgang von Alice verworfen werden). Aufgrund von Bobs Messung und seiner anschließenden Transformation erhält Charlie das Photon im Zustand $U(\phi_B)|+x\rangle = U(\pi/2)|+x\rangle = |+y\rangle$, anstelle von $U(\phi_A + \phi_B)|+x\rangle = U(3\pi/2 + \pi/2)|+x\rangle = |+x\rangle$. Charlies Messung in der Basis $|\pm x\rangle$ ergibt daher zufällig eine der beiden Möglichkeiten:

   (a) Er erhält das Ergebnis $|+x\rangle$. Dieses Resultat ist in Übereinstimmung mit $U(\phi_A + \phi_B)|+x\rangle$.

   (b) Er erhält das Ergebnis $|-x\rangle$. Bob induziert einen Fehler, da das Messresultat nicht mit den Einstellungen kompatibel ist.

Die Gesamtwahrscheinlichkeit, dass Bob durch sein Verhalten einen Fehler herbeiführt, beträgt 1/4; 1/2 die falsche Basis zu wählen und 1/2, dass Charlies Messergebnis nicht zu den angegebenen Einstellungen kompatibel ist (vergleiche Abschnitt 4.1.3).

Mit einem ähnlichen Problem sieht sich auch ein externer Abhörer Eve bei einer sogenannten „intercept/resend“-Attacke (siehe Seite 30) konfrontiert. Eve wählt mit Wahrscheinlichkeit ein halb die falsche Messbasis, was dann wiederum in der Hälfte der Fälle dazu führt, dass der von Charlie am Ende detektierte Zustand nicht mit den erwarteten Korrelationen für die verwendeten Einstellungen der beteiligten Parteien übereinstimmt. Der Abhörer verursacht so eine Fehlerrate von 25 %. Die Sicherheit dieses Protokolls gegen Lauschangriffe von unbeteiligten Personen ergibt sich ebenfalls aus der bewiesenen Sicherheit des von Bennett und Brassard vorgeschlagenen Quantenkryptographieprotokolls (BB84) [5]. Die Kommunikation eines einzelnen Qubits nach obigem Schema zwischen jeweils zwei Parteien, kann wie ein BB84 Protokoll in den Basen $|\pm x\rangle$ und $|\pm y\rangle$ verstanden werden.

In den vorangegangenen Absätzen wurde davon ausgegangen, dass bei einem Betrugs- bzw. Abhörversuch die Messung in einer der Basen erfolgt, die auch für den Protokollablauf verwendet wird. Dies scheint zunächst die natürliche Wahl zu sein. Für das BB84-Protokoll kann gezeigt werden, dass der Informationsgewinn für den Abhörer bei einer „intercept/resend“-Attacke in einer Protokoll-Basis am höchsten ist, was die gültigen Durchgänge angeht; das heißt für die Durchgänge, bei denen die beteiligten Parteien die gleichen Basiseinstellungen verwendet haben. Der Informationsgewinn bezüglich aller Durchgänge ist für die Verwendung einer Zwischenbasis, der sog. Breidbart-Basis maximal (siehe [54]). Die Breidbart-Basis hat die Eigenschaft, dass sie zwischen den Protokollbasen liegt und dabei minimalen Abstand zu beiden besitzt, in dem Sinn, dass ihre Basisvektoren gleich großen Überlapp mit den Basisvektoren der einen und der anderen Protokollbasis bilden. Da bei der Versuchsdurchführung eine Abhörattacke in der Breidbartbasis simuliert wird, soll hier kurz auf die benötigte Theorie eingegangen werden (siehe [55]). Die Protokollbasen seien $\{|\chi_1^a\rangle, |\chi_2^a\rangle\}$ und $\{|\chi_1^b\rangle, |\chi_2^b\rangle\}$, und die Breidbartbasis sei $\{|\chi_1^c\rangle, |\chi_2^c\rangle\}$, dann gilt

$$|\langle \chi_k^c \mid \chi_k^a \rangle| = \left|\langle \chi_k^c \mid \chi_k^b \rangle\right| = \text{maximal, mit } k \in \{1,2\} \tag{4.20}$$

und

$$|\langle \chi_k^c \mid \chi_l^a \rangle| = \left|\langle \chi_k^c \mid \chi_l^b \rangle\right| = \text{minimal, mit } l \in \{1,2\} \text{ und } k \neq l. \tag{4.21}$$

Die Zustände, die diese Bedingungen erfüllen, sind gegeben durch

$$|\chi_k^c\rangle = \frac{1}{\sqrt{2+\sqrt{2}}}\left(|\chi_k^a\rangle + |\chi_k^b\rangle\right) \tag{4.22}$$

und es ist

$$|\langle \chi_k^c \mid \chi_k^a \rangle| = \left|\langle \chi_k^c \mid \chi_k^b \rangle\right| = \frac{\sqrt{2+\sqrt{2}}}{2}$$

$$|\langle \chi_k^c \mid \chi_l^a \rangle| = \left|\langle \chi_k^c \mid \chi_l^b \rangle\right| = \frac{\sqrt{2-\sqrt{2}}}{2}. \tag{4.23}$$

Die Wahrscheinlichkeit das richtige bzw. falsche Resultat zu messen beträgt folglich

$$p = |\langle \chi_k^c \mid \chi_k^a \rangle|^2 = \left|\langle \chi_k^c \mid \chi_k^b \rangle\right|^2 = \frac{2+\sqrt{2}}{4} \tag{4.24}$$

bzw.

$$q = |\langle \chi_k^c \mid \chi_l^a \rangle|^2 = \left|\langle \chi_k^c \mid \chi_l^b \rangle\right|^2 = \frac{2-\sqrt{2}}{4}. \tag{4.25}$$

Versucht Bob bzw. Eve einen Betrug in der Breidbartbasis, ist die Information, die er oder sie über Alices Bit gewinnt, gegeben durch die Shannon Information

$$I_{bb} = 1 + p\log_2(p) + q\log_2(q). \tag{4.26}$$

Die Wahrscheinlichkeit, bei dieser Attacke ein Fehler in Charlies Messung zu verursachen ist

$$p_{err} = 1 - (p^2 + q^2) = \frac{1}{4}. \tag{4.27}$$

Die Resistenz des Einzel-Qubit „Secret-Sharing“-Protokolls gegenüber verallgemeinerten Attacken, die einem Abhörer die Verwendung von Hilfsqubits und Verschränkung gestatten, bleibt zu prüfen, ist allerdings nicht Gegenstand dieser Arbeit.

4.1.4.3 Einzel-Qubit N-Parteien „Secret-Sharing“

Das Protokoll, das in vorangegangenem Abschnitt für drei Personen beschrieben wurde, kann auf kanonische Weise auf $N > 3$ Parteien übertragen werden, was im folgenden gezeigt wird.

Anstelle eines Bobs können beliebig viele $N-2$ Bobs $B_1, \ldots, B_{N-2}$ zwischen Alice und Charlie eingeführt werden. Alice präpariert wieder willkürlich einen der vier Zustände

$$|\pm x\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle \pm |V\rangle\right), \tag{4.28}$$

$$|\pm y\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle \pm i|V\rangle\right), \tag{4.29}$$

was sich in der Form

$$|\chi\rangle_A = \frac{1}{\sqrt{2}}\left(|H\rangle + e^{i\phi_A}|V\rangle\right), \tag{4.30}$$

mit $\phi_A = 0$, $\phi_A = \pi/2$, $\phi_A = \pi$ oder $\phi_A = 3\pi/2$ darstellen läßt. Jeder der $N-2$ Bobs B_k $(k = 1, 2, \ldots, N-2)$ führt die unitäre Transformation

$$U(\phi_{B_k}) = |\,H\,\rangle\langle\,H\,| + e^{i\phi_{B_k}}\,|\,V\,\rangle\langle\,V\,| \tag{4.31}$$

aus, wobei zufällig zwischen $\phi_{B_k} = 0$, $\phi_{B_k} = \pi/2$, $\phi_{B_k} = \pi$ und $\phi_{B_k} = 3\pi/2$ gewechselt wird. Bei einer Messung durch Charlie in der Basis $\{1/\sqrt{2}\,(|\,H\,\rangle \pm |\,V\,\rangle)\}$ zusammen mit der beliebigen Wahl von $\phi_C = 0$ oder $\phi_C = \pi/2$, ergibt sich die Wahrscheinlichkeit das Ergebnis $1/\sqrt{2}\,(|\,H\,\rangle + |\,V\,\rangle)$ zu erhalten als

$$p(\phi_A, \phi_{B_1}, \ldots, \phi_{B_{N-2}}, \phi_C, +) = \frac{1}{2}\left(1 + \cos\left(\phi_A + \sum_k \phi_{B_k} + \phi_C\right)\right) \tag{4.32}$$

und für das Ergebnis $1/\sqrt{2}\,(|\,H\,\rangle - |\,V\,\rangle)$ als

$$p(\phi_A, \phi_{B_1}, \ldots, \phi_{B_{N-2}}, \phi_C, -) = \frac{1}{2}\left(1 - \cos\left(\phi_A + \sum_k \phi_{B_k} + \phi_C\right)\right). \tag{4.33}$$

Der Erwartungswert dieser Resultate folgt analog zum Dreiparteien Fall

$$\begin{aligned} E(\phi_A, \phi_{B_1}, \ldots, \phi_{B_{N-2}}, \phi_C) &= p(\phi_A, \phi_{B_1}, \ldots, \phi_{B_{N-2}}, \phi_C, +) - p(\phi_A, \phi_{B_1}, \ldots, \phi_{B_{N-2}}, \phi_C, -) \\ &= \cos\left(\phi_A + \sum_k \phi_{B_k} + \phi_C\right). \end{aligned} \tag{4.34}$$

Damit Alice die gültigen Durchgänge auswählen kann, für die $|\cos(\phi_A + \sum_k \phi_{B_k} + \phi_C)| = 1$ ist, teilt ihr jeder Bob die Klassenzugehörigkeit von $U(\phi_{B_k})$ mit und Charlie gibt ihr die Wahl der Messbasis bekannt. Alice überprüft einen Teil der Korrelationen um Betrug oder Lauschangriff auszuschließen und gibt daraufhin jedem alle Klassen sowie Präparations- und Messbasis bekannt. Charlie kann nur in Kooperation mit allen Bobs Alices Bitwert in Erfahrung bringen. Des Gleichen gilt für jeden Bob in Bezug auf Charlie und die restlichen Bobs. Es bedarf genau $N-2$ Bobs und Charlie, d.h. $N-1$ Personen, um die geheime Nachricht zu rekonstruieren; jede $N-2$ elementige Untergruppe von Parteien ist dazu nicht in der Lage.

4.2 Implementierung

Das in Abschnitt 4.1.4.3 beschriebene Protokoll soll experimentell für $N = 6$, Alice, Charlie und vier Bobs, realisiert werden. Die hierfür benötigten Voraussetzungen sind bereits durch das in Kapitel 3 vorgestellte Experiment größtenteils geschaffen. Im folgenden wird daher meistens auf das vorangegangene Kapitel verwiesen und lediglich die benötigten Modifikationen des bereits vorhandenen Versuchaufbaus erklärt.

4.2.1 Realisierung der unitären Transformation

Um zu erkennen, wie sich die unitäre Transformation

$$U(\phi) = |\,H\,\rangle\langle\,H\,| + e^{i\phi}\,|\,V\,\rangle\langle\,V\,| \tag{4.35}$$

experimentell realisieren läßt, bedarf es lediglich einer etwas anderen Darstellungsweise. $U(\phi)$ projiziert den Polarisationszustand $|\,H\,\rangle$ auf sich selbst, d.h. läßt ihn unverändert und bildet den Vektor $|\,V\,\rangle$ auf $e^{i\phi}|\,V\,\rangle$ ab. Sie kann daher in der Form

$$U(\phi) = \begin{cases} |\,H\,\rangle \rightarrow |\,H\,\rangle \\ |\,V\,\rangle \rightarrow e^{i\phi}|\,V\,\rangle \quad , \end{cases} \tag{4.36}$$

geschrieben werden. Unter der Voraussetzung, dass ϕ nur die Werte $0, \pi/2, \pi, 3\pi/2$ annehmen kann, ist Gleichung 4.36 äquivalent zu

$$U(x_j) = \begin{cases} |\,H\,\rangle \rightarrow |\,H\,\rangle \\ |\,V\,\rangle \rightarrow e^{i(\pi/2)x_j}|\,V\,\rangle, \quad \text{für } x_j = \{0,1,2,3\}, \end{cases} \tag{4.37}$$

was dem Phasenoperator $\hat{\phi}$ aus Gleichung 3.8 identisch ist. Wie in Abschnitt 3.2.1 ausführlich beschrieben, kann diese Transformation durch geeignete Orientierung eines YVO_4-Kristalls erreicht werden.

4.2.2 Experimenteller Aufbau

Da die unitäre Transformation $U(\phi)$ dem Phasenoperator $\hat{\phi}$ entspricht, ist der experimentelle Aufbau des „Secret-Sharing“ Protokolls dem des vorangegangenen Kapitels sehr ähnlich. Er gliedert sich ebenfalls in drei Teile.

Am Beginn steht die Quelle zur Erzeugung der Einzelphotonen sowie die Präparation des Anfangszustands. Dieser Teil entspricht Alice. Da in diesem Protokoll der Polarisationszustand des Photons jedoch nicht konstant $|+\rangle$ ist, sondern die Präparation zwischen den Basen $|\pm x\,\rangle$ und $|\pm y\,\rangle$ gewechselt werden muss, wird zum einen die $\frac{\lambda}{2}$-Platte motorisiert und zum anderen im Strahlengang eine $\frac{\lambda}{4}$-Platte bei einer Winkelstellung von $45\,^\circ$ ergänzt. Der Polarisator im Triggerarm transmittiert vertikale Polarisation, d.h. es wird davon ausgegangen, dass nur horizontale Signalphotonen zu einer Koinzidenz führen. Diese können durch Verfahren der $\frac{\lambda}{2}$-Platte auf die Positionen $0\,^\circ$, $45\,^\circ$, $22,5\,^\circ$ und $-22,5\,^\circ$ in Kombination mit der $\frac{\lambda}{4}$-Platte wahlweise in die Polarisationszustände $|\,R\,\rangle$, $|\,L\,\rangle$, $|+\rangle$ und $|-\rangle$ überführt werden, was $|\pm y\,\rangle$ und $|\pm x\,\rangle$ entspricht. Die Winkelveränderung erfolgt gemäß vier Computer-generierter Zufallszahlen (0, 1, 2, 3). Die Stellung der $\frac{\lambda}{4}$-Platte bleibt aber stets auf $45\,^\circ$ fixiert.

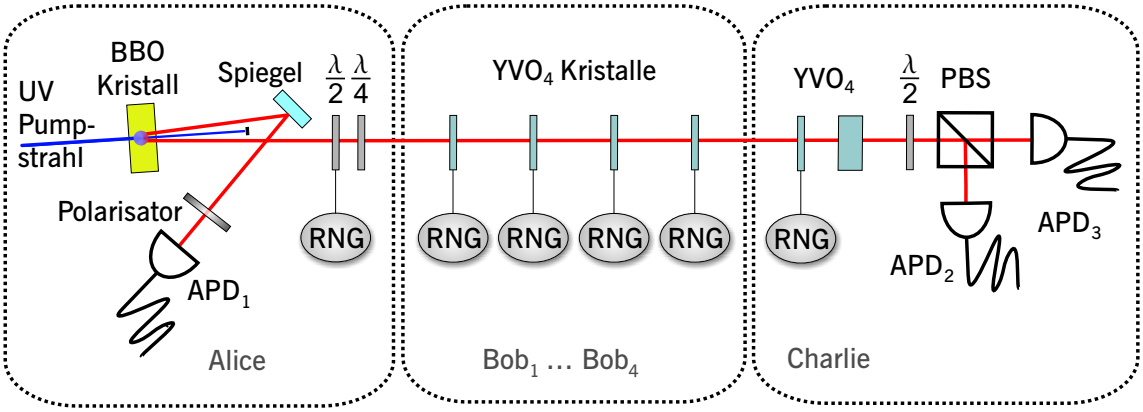


Abbildung 4.1: Schematische Darstellung des experimentellen Aufbaus.

Daran schließt sich der zweite Teil an, in dem Bob B_1 bis Bob B_4 jeweils die unitäre Transformation $U(\phi_{B_k})$ ausführen. Jeder besitzt dafür einen motorisierten YVO_4-Kristall. Der Gesamtphasenschub für $\phi_{B_k} + \phi_C = 0$ wird wieder am Ende durch einen Kristall der fünffachen Dicke kompensiert. Die Bewegung der Kristalle wird ebenfalls entsprechend vier Zufallszahlen vollzogen. An alle in diesem Experiment erzeugten Zufallszahlen werden, abgesehen von einer Gleichverteilung, keine weiteren Bedingungen gestellt, sie genügen insbesondere *nicht* Gleichung 3.2. In Abbildung 4.2 soll dies durch sechs einzelne Zufallszahlengeneratorsymbole (RNG) ausgedrückt werden.

Am Ende steht die Zustandsdetektion durch Charlie. Sie besteht aus einem motorisierten YVO_4-Kristall, einer $\frac{\lambda}{2}$-Platte in der Winkelstellung $22,5\,^\circ$ gefolgt von einem polarisierenden Strahlteiler (PBS). Die $\frac{\lambda}{2}$-Platte in Kombination mit dem PBS entspricht einer Detektion in der $|\pm x\rangle$-Basis. Für eine Kristallstellung, bei der $\phi_C = 0$ ist, bleibt dies unverändert. Wird der Kristall in eine Position gedreht bei der $\phi_C = \pi/2$ ist, findet ein Wechsel in die $|\pm y\rangle$-Basis statt. Charlie kann auf diese Weise beliebig zwischen einer Analyse der Polarisationszustände $|+\rangle$, $|-\rangle$ oder $|R\rangle$, $|L\rangle$ wählen.

Da für dieses Experiment die Detektionseffizienz keine ausschlaggebende Rolle spielt, werden die SLiK$^{\text{TM}}$Module gegen die in Abschnitt 2.2.3 beschriebenen passiv gequenchten APDs ausgetauscht. Die Elektronik zur Aufnahme der Koinzidenzen bleibt, abgesehen von den Detektoren, unverändert (siehe Abbildung 3.7).

4.2.3 Umsetzung von Lauschangriffen

Nach der Durchführung des Protokolls soll eine „intercept/resend“-Attacke in den Protokollbasen $\{|\pm x\rangle\}, \{|\pm y\rangle\}$ sowie der Breidbartbasis $\{|\pm bb\rangle\}$ simuliert werden, um zu zeigen, dass die Fehlerrate in der Tat signifikant ansteigt. Der Lauschangriff soll zwischen Alice und Bob B_1 erfolgen, da dies für einen aussenstehenden Abhörer die einzig

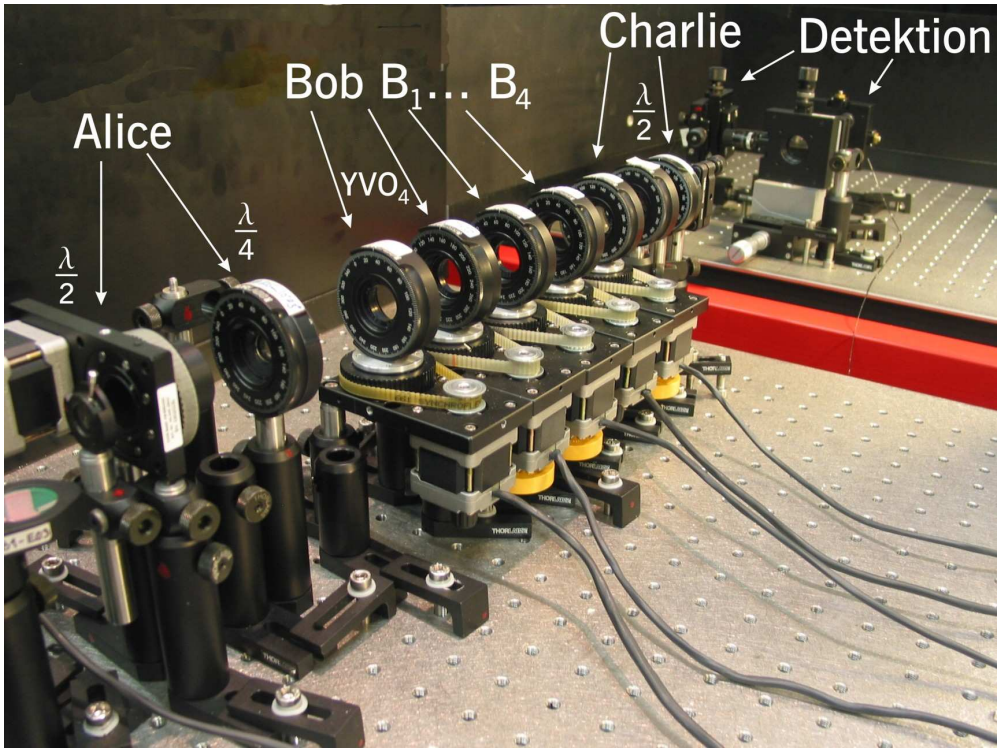


Abbildung 4.2: Foto des experimentellen Aufbaus.

sinnvolle Position darstellt, will er einer Transformation von Alices Bit durch einen der Bobs zuvorkommen. Für die Basis $\{|\pm x\rangle\}$ wird daher an dieser Stelle ein Polarisator in der Winkelstellung 45 ° eingebracht. Bei nicht-linearen Polarisationen bedarf es zusätzlich zweier Wellenplatten. Ein Polarisator mit Transmission für horizontale Polarisation zwischen zwei $\frac{\lambda}{4}$-Platten jeweils bei den Winkeln 45 ° und −45 ° stellt einen Angriff in der $\{|\pm y\rangle\}$-Basis dar. Die Vektoren der Breidbartbasis sind gegeben durch

$$|+bb\rangle = \frac{1}{\sqrt{2+\sqrt{2}}}\left(|+x\rangle + |+y\rangle\right) = \frac{1}{\sqrt{2}}\left(|H\rangle + e^{i\pi/4}|V\rangle\right) \tag{4.38}$$

$$|-bb\rangle = \frac{1}{\sqrt{2+\sqrt{2}}}\left(|-x\rangle + |-y\rangle\right) = \frac{1}{\sqrt{2}}\left(|H\rangle - e^{i\pi/4}|V\rangle\right). \tag{4.39}$$

Um auf einen dieser Vektoren zu projizieren, bedarf es eines Polarisators in einer Stellung von 22, 5 ° inmitten zweier $\frac{\lambda}{4}$-Platten bei den Winkeln −45 ° und +45 °.

4.3 Daten und Ergebnisse

Ziel des Experiments ist die Auf- und Verteilung einer gewissen Menge an Bits in einer bestimmten Versuchszeit. Dafür wird das Protokoll wiederholt durchgeführt. Dabei

ergibt nicht jede Ausführung einen Bitwert. Auf Grund der Beschaffenheit des Protokolls, führt im Mittel nur jeder zweite Durchgang zu einem (anti-)korrelierten Bit, was im Experiment jedoch ebenfalls nicht zu erreichen ist. Dies hat verschiedene Ursachen, zum einen führt nicht jede Triggerphotondetektion zu einem Koinzidenzereignis und zum anderen treten selbst bei erfolgreicher paarweiser Detektion Fehler in der Polarisationsanalyse auf. Ersteres beeinflußt im wesentlichen die benötigte Messzeit, während letzteres die Qubit-Fehlerrate (QBER) bestimmt. Die nachfolgenden Abschnitte zeigen wieviele Bits mit dem in 4.2.2 beschriebenen Setup bei einer vorgegebenen Zahl an Durchführungen und der dafür benötigten Zeit mit einer bestimmten Fehlerrate ausgetauscht bzw. verteilt werden können.

4.3.1 Datenauswertung

Das Protokoll wurde 25000 mal wiederholt. Eine Durchführung besteht aus der Erzeugung von sechs Zufallszahlen, dem Verfahren der Motoren auf die entsprechenden Positionen und einer Messung der Polarisation mit einer Integrationszeit von 200 μs. Die Dauer hierfür beträgt ähnlich dem Kommunikationskomplexitätsexperiment ca. eine Sekunde, was letztlich eine gesamte Versuchsdauer von annähernd sieben Stunden ergibt. Bei der Auswertung werden aus allen Ereignissen jene selektiert, bei denen während der Integrationszeit ein Photon im Triggerarm registriert wurde. Dies ist bei $Z_{sift} = 9129$ Durchgängen der Fall, was $36,52\,\%$ der Gesamtzahl entspricht. Dabei wurde $Z_{koin} = 2107$ Mal das Partnerphoton ebenfalls detektiert, woraus ein Koinzidenz- zu Einzelzählratenverhältnis von $23,08\,\%$ folgt. Dieser Wert ist durch die Verwendung weniger effizienter Detektoren gegenüber dem Ergebnis aus Abschnitt 3.3.3 deutlich verringert. Die Zahl der Ereignisse bei denen $|\cos(\phi_A + \sum_k \phi_{B_k} + \phi_C)| = 1$ gilt, beläuft sich auf $Z_{fin} = 982$, wovon $Z_{nofl} = 506$ mal die Ergebnisse korreliert und $Z_{flip} = 476$ mal antikorreliert sind. Der Wert von Z_{fin} stimmt in etwa mit dem überein, was man für eine Ein-Photonereignisrate des Triggerarms von $36\,\%$ und dem Koinzidenz- zu Einzelzählratenverhältnis von $23\,\%$ erwartet:

$$25000 \cdot 0,36 \cdot 0,23 = 1035.$$

Bei $Z_{corr} = 959$ Koinzidenzen wurde das Signalphoton in Übereinstimmung mit den Basis- bzw. Phaseneinstellungen der sechs Parteien gemessen, während bei $Z_{wro} = 23$ die Messung damit nicht im Einklang war. Daraus folgt für die Qubit-Fehlerrate $QBER = Z_{wrong}/Z_{fin} = 2,34\,\%$. Tabelle 4.4 zeigt die ersten 32 Bits (= 8 Bytes) von Z_{fin}. Zu sehen ist jeweils Alices Bit b_A und die verwendete Präparationsbasis. Dem gegenüber steht der gemessene Bit Wert b_C von Charlie in der entsprechenden Basis. Eine Detektion im transmittierten Ausgang des polarisierenden Strahlteilerwürfels wird mit $b_C = +1$ und dementsprechend im reflektierten mit $b_C = -1$ assoziiert. Das entspricht zugleich einer Messung von $\cos(\phi_{ges})$ mit $\phi_{ges} = \phi_A + \sum_{k=1}^{4} \phi_{B_k} + \phi_C$ und $b_C = \cos(\phi_{ges})$. Das folgt unmittelbar aus Gleichung 4.32 und 4.33 sowie der Tatsache, dass der Zustand $|+x\rangle$ stets im transmittierten und der Zustand $|-x\rangle$ stets im

reflektierten Ausgang detektiert wird. Ferner findet man in Tabelle 4.4 die Werte von $\sum_{k=1}^{4} \phi_{B_k}$, $\sum_{k=1}^{4} \phi_{B_k} + \phi_C$ und $\cos(\phi_{ges})$. Aus der Gleichung

$$b_C = \cos\left(\phi_A + \sum_{k=1}^{4} \phi_{B_k} + \phi_C\right) \tag{4.40}$$

kann dann mit bekanntem b_C und $\sum_{k=1}^{4} \phi_{B_k} + \phi_C$ der Wert von ϕ_A und somit von b_A berechnet werden, wobei gilt $\phi_A \in \{0, \pi/2\} \mathrel{\widehat{=}} b_A = +1$ und $\phi_A \in \{\pi, 3\pi/2\} \mathrel{\widehat{=}} b_A = -1$.

4.3.2 Fehler der Fehlerrate

Im Abschnitt 3.3.3 des vorangegangenen Kapitels wurde der Fehler der experimentell bestimmten Erfolgsrate durch mehrmaliges Auswerten der Daten und Plotten der dabei leicht unterschiedlichen Einzelwerte grafisch bestimmt. In diesem Fall wurde diese Lösung gewählt, da ein statistischer Beitrag sowohl vom Rateprozess im Falle ausgebliebener Koinzidenzdetektionen, als auch von der Anzahl fehlerhafter Koinzidenzdetektionen zu beachten war. Da im „Secret-Sharing“-Protokoll der Prozess des Ratens wegfällt, kann der Fehler der $QBER$ durch Annahme einer binomialen Verteilung einfach berechnet werden. Die Binomialverteilung

$$f(x) = \begin{pmatrix} n \\ x \end{pmatrix} \cdot p^x \cdot (1-p)^{n-x} \tag{4.41}$$

gibt die Wahrscheinlichkeit an, mit der ein bestimmtes Ereignis bei n Ausführungen eines Experiments x mal auftritt, wenn die Wahrscheinlichkeit bei einer einzelnen Durchführung p beträgt. Für den Erwartungswert μ und die Varianz σ^2 gilt

$$\begin{aligned} \mu &= np \\ \sigma^2 &= np(1-p). \end{aligned} \tag{4.42}$$

Das Verhältnis von Standardabweichung σ zur Anzahl der Ausführungen n soll in diesem Zusammenhang als Mass für den Fehler betrachtet werden. Für $p = 0,0234$ und $n = 982$ ergibt sich

$$\frac{\sigma}{n} = 0,0048. \tag{4.43}$$

Somit lässt sich festhalten, dass mit dem Aufbau aus Abbildung 4.2 in annähernd sieben Stunden 982 Bits mit einer Fehlerrate von $2,34 \pm 0,48\,\%$ zwischen fünf Personen aufgeteilt werden können.

b_A	Basis	b_C	Basis	$\sum_{k=1}^{4} \phi_{B_k}$	$\sum_{k=1}^{4} \phi_{B_k} + \phi_C$	$\cos(\phi_{ges})$
$+1$	$\|\pm y\rangle$	-1	$\|\pm y\rangle$	$8\pi/2$	$9\pi/2$	-1
-1	$\|\pm x\rangle$	$+1$	$\|\pm y\rangle$	$5\pi/2$	$6\pi/2$	$+1$
$+1$	$\|\pm x\rangle$	-1	$\|\pm y\rangle$	$5\pi/2$	$6\pi/2$	-1
$+1$	$\|\pm y\rangle$	-1	$\|\pm y\rangle$	$4\pi/2$	$5\pi/2$	-1
$+1$	$\|\pm x\rangle$	$+1$	$\|\pm y\rangle$	$7\pi/2$	$8\pi/2$	$+1$
$+1$	$\|\pm y\rangle$	-1	$\|\pm x\rangle$	$5\pi/2$	$5\pi/2$	-1
$+1$	$\|\pm x\rangle$	-1	$\|\pm y\rangle$	$9\pi/2$	$10\pi/2$	-1
-1	$\|\pm x\rangle$	$+1$	$\|\pm x\rangle$	$6\pi/2$	$6\pi/2$	$+1$
$+1$	$\|\pm x\rangle$	$+1$	$\|\pm y\rangle$	$3\pi/2$	$4\pi/2$	$+1$
-1	$\|\pm y\rangle$	$+1$	$\|\pm x\rangle$	$9\pi/2$	$9\pi/2$	$+1$
-1	$\|\pm x\rangle$	$+1$	$\|\pm x\rangle$	$6\pi/2$	$6\pi/2$	$+1$
$+1$	$\|\pm y\rangle$	-1	$\|\pm x\rangle$	$1\pi/2$	$1\pi/2$	-1
-1	$\|\pm y\rangle$	-1	$\|\pm x\rangle$	$7\pi/2$	$7\pi/2$	-1
-1	$\|\pm x\rangle$	-1	$\|\pm y\rangle$	$7\pi/2$	$8\pi/2$	-1
$+1$	$\|\pm x\rangle$	$+1$	$\|\pm y\rangle$	$7\pi/2$	$8\pi/2$	$+1$
$+1$	$\|\pm y\rangle$	$+1$	$\|\pm y\rangle$	$10\pi/2$	$11\pi/2$	$+1$
-1	$\|\pm y\rangle$	$+1$	$\|\pm x\rangle$	$5\pi/2$	$5\pi/2$	$+1$
$+1$	$\|\pm y\rangle$	-1	$\|\pm x\rangle$	$9\pi/2$	$9\pi/2$	-1
$+1$	$\|\pm x\rangle$	$+1$	$\|\pm x\rangle$	$8\pi/2$	$8\pi/2$	$+1$
-1	$\|\pm y\rangle$	-1	$\|\pm x\rangle$	$3\pi/2$	$3\pi/2$	-1
$+1$	$\|\pm x\rangle$	-1	$\|\pm y\rangle$	$5\pi/2$	$6\pi/2$	-1
-1	$\|\pm y\rangle$	-1	$\|\pm x\rangle$	$7\pi/2$	$7\pi/2$	-1
-1	$\|\pm y\rangle$	$+1$	$\|\pm y\rangle$	$4\pi/2$	$5\pi/2$	$+1$
$+1$	$\|\pm y\rangle$	-1	$\|\pm y\rangle$	$8\pi/2$	$9\pi/2$	-1
-1	$\|\pm y\rangle$	$+1$	$\|\pm y\rangle$	$8\pi/2$	$9\pi/2$	$+1$
$+1$	$\|\pm y\rangle$	$+1$	$\|\pm y\rangle$	$6\pi/2$	$7\pi/2$	$+1$
$+1$	$\|\pm x\rangle$	-1	$\|\pm x\rangle$	$6\pi/2$	$6\pi/2$	-1
$+1$	$\|\pm x\rangle$	$+1$	$\|\pm y\rangle$	$7\pi/2$	$8\pi/2$	$+1$
$+1$	$\|\pm y\rangle$	-1	$\|\pm y\rangle$	$4\pi/2$	$5\pi/2$	-1
-1	$\|\pm x\rangle$	$+1$	$\|\pm x\rangle$	$6\pi/2$	$6\pi/2$	$+1$
$+1$	$\|\pm y\rangle$	-1	$\|\pm y\rangle$	$4\pi/2$	$5\pi/2$	-1
$+1$	$\|\pm y\rangle$	-1	$\|\pm x\rangle$	$5\pi/2$	$5\pi/2$	-1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Tabelle 4.4: Datenauszug von Z_{fin}. Zu sehen ist Alices Bit b_A sowie die Präparationsbasis, Charlies Bit b_C mit der Detektionsbasis und die Werte von $\sum_{k=1}^{4} \phi_{B_k}$, $\sum_{k=1}^{4} \phi_{B_k} + \phi_C$ und $\cos(\phi_{ges})$.

4.3.3 Simulation der Lauschangriffe

Eine „intercept/resend“-Attacke wurde wie in Abschnitt 4.2.3 beschrieben durch Einbringen der entsprechenden optischen Komponenten zwischen Alice und Bob B_1 für die Basen $\{|\pm x\rangle\}, \{|\pm y\rangle\}$ und $\{|\pm bb\rangle\}$ simuliert. Die Ergebnisse sind in Tabelle 4.5 zusammengefasst. Die Fehlerrate liegt in allen Fällen über 25 %. Für lineare Polarisation ist sie nahe am theoretischen Wert von 25 %, während sie bei den elliptischen Polarisationen mit ca. 30 % sogar darüber liegt, was auf zusätzliche Fehler durch die Wellenplatten zurückzuführen ist. Das Koinzidenz- zu Einzelzählratenverhältnis ist mit 8 bis 9 % um mehr als die Hälte geringer als im Fall ohne Abhörattacke. Das liegt zum einen daran, dass auf Grund des Polarisators nurmehr die Hälfte aller Signalphotonen die Detektoren erreicht und zum anderen an höheren Absorptionsverlusten, hervorgerufen durch die zusätzlich eingebrachten optischen Komponenten.

Die Verwendung eines Polarisators ist zwar für einen realistischen Abhörversuch nicht sehr geeignet, da im Mittel die Hälfte aller Photonen absorbiert wird, was in der Regel nicht unbemerkt bleiben dürfte. Sie zeigt allerdings dennoch dass die Qubit-Fehlerrate deutlich ansteigt, verglichen mit der zuvor erzielten Rate von $2,34\,\%$.

Abschließend lässt sich sagen, dass das in Abschnitt 4.1.4 vorgeschlagene „Secret-Sharing“-Protokoll erfolgreich experimentell umgesetzt und demonstriert werden konnte. Die Rate von 982 Bits in sieben Stunden ist zwar für jede realistische Anwendung zweifelsfrei zu wenig, läßt sich aber verbessern. Alleine die Verwendung effizienterer Detektoren, wie in Kapitel 3, und damit ein höheres Koinzidenz- zu Einzelzählratenverhältnis könnten die Menge etablierter Bits deutlich steigern. Da ein Großteil der Zeit für die Bewegung der Motoren verloren geht, wäre die Verwendung akusto- oder elektrooptischer Komponenten zur Erzeugung der Phasenschübe anzudenken.

(a) „intercept/resend“-Attacke in der $|\pm x\rangle$-Basis

Gesamtzahl der Durchgänge:	27501	
Ein-Photon Triggerereignisse:	9814	35,686 %
Koinzidenz-/Einzelzählrate:		8,99735 %
Ein-Photon Triggerereignisse mit Koinzidenz:	452	1,64358 %
Falsche Koinzidenzen:	114	25,2212 %
korrekte Koinzidenzen:	338	74,7788 %
Qubit Fehlerrate $QBER$:		$25,2212 \pm 2,04$ %

(b) „intercept/resend“-Attacke in der $|\pm y\rangle$-Basis

Gesamtzahl der Durchgänge:	24993	
Ein-Photon Triggerereignisse:	9188	36,7623 %
Koinzidenz-/Einzelzählrate:		8,5328 %
Ein-Photon Triggerereignisse mit Koinzidenz:	409	1,63646 %
Falsche Koinzidenzen:	124	30,3178 %
korrekte Koinzidenzen:	285	69,6822 %
Qubit Fehlerrate $QBER$:		$30,3178 \pm 2,27273$ %

(c) „intercept/resend“-Attacke in der $|\pm bb\rangle$-Basis

Gesamtzahl der Durchgänge:	38174	
Ein-Photon Triggerereignisse:	13706	35,904 %
Koinzidenz-/Einzelzählrate:		8,29564 %
Ein-Photon Triggerereignisse mit Koinzidenz:	588	1,54032 %
Falsche Koinzidenzen:	178	30,2721 %
korrekte Koinzidenzen:	410	69,7279 %
Qubit Fehlerrate $QBER$:		$30,2721 \pm 1,89468$ %

Tabelle 4.5: Messergebnisse für die Simulation einer „intercept-resend“-Attacke in verschiedenen Basen.

Kapitel 5

Schlußbetrachtung und Ausblick

Ziel dieser Arbeit war die Entwicklung einer kompakten Quelle zur effizienten Erzeugung polarisationsverschränkter Photonen im nahen infraroten Wellenlängenbereich und deren Anwendung in verschiedenen Experimenten der Quantenkommunikation.

Es wurde zu Beginn gezeigt, dass die Verwendung einer blauen Laserdiode anstelle eines Ionenlasers als Pumpquelle für spontane parametrische Fluorezenz neben einer kompakten Bauweise bei optimierten Koplungsbedingungen auch eine effiziente Erzeugung polarisationsverschränkter Photonenpaare ermöglicht. Die erzielten Zählraten sowie der einfache Aufbau machen die Quelle zum idealen Werkzeug für eine Vielzahl von Anwendungen. Ihr Einsatz in Praktikumsversuchen für Studenten oder Demonstrationen in Vorlesungen ist ebenso denkbar wie die Verwendung in herkömmlichen Laborexperimenten. Die erzeugte Polarisationsverschränkung wurde auf verschiedene Arten überprüft und bewährte sich bei der näheren Untersuchung quantenmechanischer Korrelationen. Sie erlaubte insbesondere erfolgreich die systematische Rekonstruktion der Schranken des CHSH-Operators. Die Entwicklung der Quelle stellt ferner einen weiteren Schritt in Richtung einer realistischen Anwendung der Quantenkryptographie dar. Dieser Weg mit dem langfristigen Ziel eines endverbraucherfreundlichen verschränkungsbasierten Kryptographiesystems darf nicht aus den Augen verloren werden, soll die Quantenkryptographie nicht eine physikalische Spielerei bleiben. Die ersten Experimente mit einer ähnlichen Quelle ausserhalb einer Laborumgebung in einer Feldanwendung fanden bereits statt [56] und man darf zuversichtlich auf weitere hoffen.

Im weiteren Verlauf der Arbeit zeigte sich ebenfalls die vielseitige Einsetzbarkeit der Quelle. Die zeitlichen Korrelationen zwischen den paarweise generierten Photonen wurden in den darauffolgenden Experimenten zur Erzeugung von Einzelphotonenzuständen verwendet. Der erste Versuch beschäftigte sich mit der Realisierung eines Mehr-Parteien Quantenkommunikationskomplexitätsprotokolls, bei dem fünf Personen durch die sequenzielle Kommunikation eines einzelnen Qubits eine Modulo-4 Summe berechnen.

Zur dessen Durchführung bedurfte es der Implementierung eines, durch die teilnehmenden Parteien kontrollierbaren, relativen Phasenschubs zwischen horizontaler und vertikaler Polarisationskomponente der kommunizierten Photonen. Dafür wurde eigens eine Technik entwickelt, die doppelbrechende Kristalle nach dem Vorbild von Wellenplatten verwendet. Mit dem Verfahren war es möglich, fünf relative Phasen additiv richtig mit einer Ungenauigkeit von lediglich 2 % zu setzen. Zusammen mit dem Einsatz effizienter Detektoren erlaubte die erfolgreiche Umsetzung des Versuchs erstmals die Demonstration der Überlegenheit einer breiten Klasse quantenmechanischer Protokolle verteilter Berechnungen gegenüber ihren klassischen Entsprechungen unter realistischen Bedingungen. Ein Qubit ersetzte zwei Bit an klassischer Kommunikation. Die Kommunikationskomplexität schneidet hier mit dem vermeintlichen Widerspruch zu Holevos Theorem darüberhinaus ein interessantes Streitthema an. Zur Festlegung eines quantenmechanischen Zustandes bedarf es im Allgemeinen einer unendlichen Menge an Information. Ob diese Menge allerdings auch dem realen Informationsgehalt des Quants entspricht, wird von vielen bezweifelt, denn obwohl ein Quant zwar eine kontinuierliche Menge an ununterscheidbaren Zuständen annehmen kann, ist dennoch nur eine diskrete Menge unterscheidbarer Zustände in Form einer Messung zugänglich. Wenn aber ein Qubit, wie gezeigt wurde, zwei Bits an klassischer Kommunikation ersetzen kann, müssen diese zwei Bits dann nicht in irgendeiner Weise in dem Qubit enthalten sein? Eine Variation des Protokolls, bei dem eine noch größere Menge Bits substituiert wird und die daher diese Frage noch deutlicher aufwirft, befindet sich bereits in Vorbereitung.

Da dieses Komplexitätsprotokoll zunächst für die Verwendung verschränkter Zustände erdacht und erst später in einer modifizierten Version für einzelne Photonen abgeändert wurde, gab das Experiment ferner einen Denkanstoß, der zur Idee eines Mehrparteien Quanten „Secret-Sharing“-Protokolls führte. Der letzte Teil der Arbeit stellte daher ein neues Verfahren ohne Verschränkung vor, bei dem eine Person ein Geheimnis an fünf weitere Personen aufteilt, indem sequentiell lediglich ein einzelnes Photon von Partei zu Partei gesendet wird. Dabei zeigte sich eine erstaunliche Analogie zu Protokollen, die auf verschränkte Zustände zurückgreifen. Mit dem vorgestellten Aufbau war es möglich 982 Bit in sieben Stunden mit einer Fehlerrate von 2,34 % zu etablieren. Dies ist für jede realistische Anwendung zweifelsfrei zu wenig, aber dennoch steigerungsfähig und in jedem Fall Beweis des Prinzips. Die Resistenz des Protokolls gegen „intercept/resend“ Abhörattacken wurde zunächst theoretisch diskuttiert und letztlich experimentell ebenfalls gezeigt. Zu klären bleibt die Frage nach der Sicherheit gegenüber kohärenten Lauschangriffen, die Hilfsqubits und Verschränkung mit einschließen. Allemal ist es eine interessante Beobachtung, dass sich bestimmte Kommunikationsprobleme in äquivalenter Weise sowohl mit Hilfe von einzelnen als auch verschränkten Quantensystemen lösen lassen. Sie sollte Anstoß für die Suche und das Formulieren allgemeiner Kriterien dieser Äquivalenz sein. Das könnte wiederum zu experimentell einfacher umsetzbaren und skalierbaren Protokollen sowie einem besseren Verständnis für die Struktur quantenmechanischer Korrelationen bei Mehrteilchenver-

schränkung führen.

Anhang A

A.1 Matrixdarstellung verwendeter Vektoren und Operatoren

A.1.1 Vektoren

A.1.1.1 Polarisationsvektoren

$$|H\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |V\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{A.1}$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \tag{A.2}$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \tag{A.3}$$

$$|R\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \tag{A.4}$$

$$|L\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \tag{A.5}$$

A.1.1.2 Bell Zustände

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|HH\rangle + |VV\rangle\right) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{A.6}$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}\left(|HH\rangle - |VV\rangle\right) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} \tag{A.7}$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|HV\rangle + |VH\rangle\right) = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \tag{A.8}$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|HV\rangle - |VH\rangle\right) = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} \tag{A.9}$$

A.1.2 Operatoren

A.1.2.1 Pauli Matritzen, Einheitsmatrix

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{A.10}$$

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \mathbb{1}_4 = \mathbb{1} \otimes \mathbb{1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{A.11}$$

A.1.2.2 CHSH Observable

$$\hat{A}(\theta) = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix}, \qquad \hat{B}(\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix} \tag{A.12}$$

$$\hat{a}(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \hat{b}(\theta) = \begin{pmatrix} \cos(3\theta) & \sin(3\theta) \\ \sin(3\theta) & -\cos(3\theta) \end{pmatrix} \tag{A.13}$$

A.1.2.3 Lineare Verzögerungsplatten [1]

$$\mathbf{lam}(\delta, \varphi) = \begin{pmatrix} e^{i\delta/2}\cos^2(\varphi) + e^{-i\delta/2}\sin^2(\varphi) & 2i\sin(\varphi)\cos(\varphi)\sin(\varphi/2) \\ 2i\sin(\varphi)\cos(\varphi)\sin(\varphi/2) & e^{-i\delta/2}\cos^2(\varphi) + e^{i\delta/2}\sin^2(\varphi) \end{pmatrix} \tag{A.14}$$

$$\mathbf{lam2}(\varphi) = \mathbf{lam}(\pi, \varphi) = \begin{pmatrix} \cos(2\varphi) & \sin(2\varphi) \\ \sin(2\varphi) & -\cos(2\varphi) \end{pmatrix} \tag{A.15}$$

$$\mathbf{lam4}(\varphi) = \mathbf{lam}(\pi/2, \varphi) = \\ = \begin{pmatrix} e^{i\pi/4}\cos^2(\varphi) + e^{-i\pi/4}\sin^2(\varphi) & \sqrt{2}i\sin(\varphi)\cos(\varphi) \\ \sqrt{2}i\sin(\varphi)\cos(\varphi) & e^{-i\pi/4}\cos^2(\varphi) + e^{i\pi/4}\sin^2(\varphi) \end{pmatrix} \tag{A.16}$$

A.2 APD-Parameter und ihre Zusammenhänge[2]

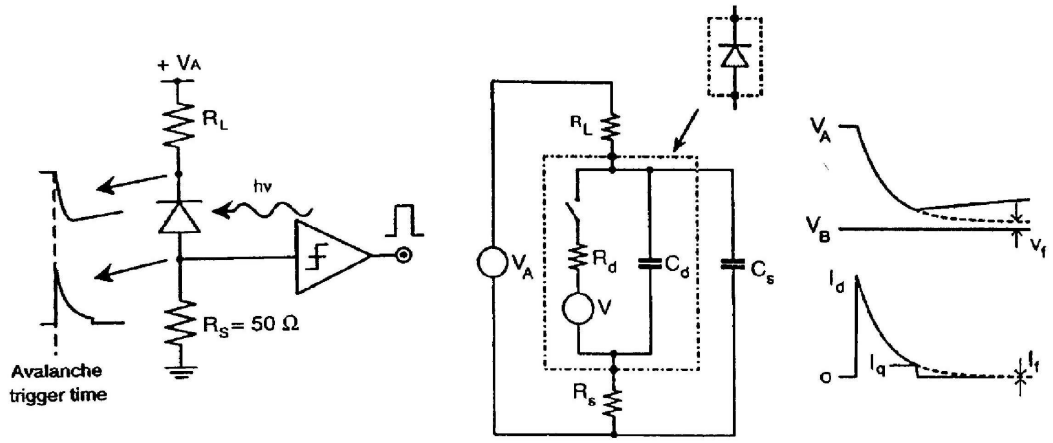


Abbildung A.1: Ersatzschaltbild einer APD mit den Kurven für Spannungs- und Stromverlauf bei einem Durchbruch

A.2.1 Temperatur

- bestimmt Dunkelzählrate
- bestimmt Durchbruchspannung
- sollte daher so niedrig und konstant wie möglich gehalten werden
- je kälter, desto niedriger die Dunkelzählrate aber keine signifikante Änderung von C_{dc} unter 30 ° C [57]

A.2.2 Quenching Widerstand

- bestimmt Totzeit
- bestimmt Sättigung
- sollte ungefähr bei $R_L = \frac{\Delta V}{50\ \mu A}$ liegen , mit $\Delta V = V_A - V_B$
- typische Werte: $\sim 100 - 500\,\mathrm{k\Omega}$

A.2.3 Meßwiderstand

- wandelt Strompuls in Spannungssignal um
- typische Werte: $\sim 50\,\mathrm{k\Omega}$

A.2.4 Betriebsspannung

- sollte $\sim 15 - 20$ Volt über der Durchbruchsspannung liegen
- hängt daher von der Temperatur ab (wegen V_B)
- bestimmt Dunkelzählrate
- bestimmt daher auch die Detektionseffizienz
- bestimmt Totzeit (je höher ΔV desto höher τ)

A.2.5 Durchbruchsspannung

- hängt von Temperatur ab (annähernd linear), sinkt wenn T abfällt.
- Abhängigkeit: $0,3\,\frac{V}{K}$

A.2.6 Dunkelzählrate

- nimmt mit Temperatur zu (einige 10000 Hz bei Zimmertemperatur, typisch $300 - 700$ Hz bei ca. $-20\,^\circ\,\mathrm{C}$)
- hängt von ΔV ab, ist aber ab 30 Volt über V_B annähernd konstant.
- bestimmt Detektionseffizienz.

A.2.7 Totzeit

- nimmt mit ΔV zu
- hängt von der Quenching-Schaltung ab: $\tau = R_L\ (C_d + C_s)$
- typische Werte $\sim 1 - 2\,\mu sec$
- bestimmt Sättigung

A.2.8 Sättigung

- hängt von Totzeit ab
- senkt die Detektionseffizienz

A.2.9 Detektionseffizienz

- $E \propto P_d = \eta P_b$

  P_d: Detektionswahrscheinlichkeit

  η: Quanteneffizienz $\rightarrow$ Wahrscheinlichkeit, daß ein Photon ein Elektron/Loch-Paar erzeugt

  $P_b = 1 - exp\left(-\frac{\Delta V}{V_c}\right)$: Durchbruchswahrscheinlichkeit $\rightarrow$ V_c Diodenspezifische Spannung (abhängig von Geometrie, Material, etc.)

- hängt von Dunkelzählrate ab

A.2.10 Koinzidenzrate

- abhängig von Dunkelzählrate
- abhängig von Detektionseffizienz
- Rate zufälliger Koinzidenzen: $C_{dc}^{coin} = C_{dc}^{1} C_{dc}^{2} \tau_{coin}$

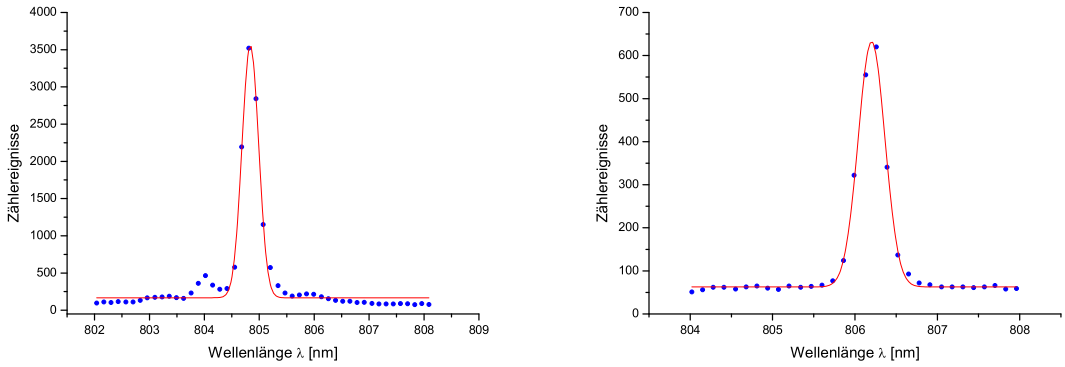
A.2.11 Koinzidenzzeitfenster

- bestimmt Rate zufälliger Koinzidenzen
- typische Werte einige n*sec*

A.3 Justierlaser

LG-Lasertechnologies, LG808-20-R1, Laserdiodenmodul:

- einstellbare Strahldivergenz; Grundeinstellung: kollimiert.
- einstellbare optische Ausgangsleistung 1,84 - 10,2 mW.
- Wellenlänge $\lambda = 804,8 - 806,2\,\text{nm}$.
- Stromversorgung: 5 V, DC



(a) Gemessene Wellenlänge (•) $\lambda = 804,8\,\text{nm}$ und spektralen Breite w $= 0,3\,\text{nm}$ bei 1,84 mW opt. Ausgangsleistung. Gaußfit (–): $y(\lambda) = y_0 + A\exp(-\frac{(x-x_0)^2}{2w^2})$.

(b) Gemessene Wellenlänge (•) $\lambda = 806,2\,\text{nm}$ und spektralen Breite w $= 0,32\,\text{nm}$ bei 10,2 mW opt. Ausgangsleistung. Gaußfit (–): $y(\lambda) = y_0 + A\exp(-\frac{(x-x_0)^2}{2w^2})$.

Abbildung A.2: Pumplaserspektrum

Literaturverzeichnis

[1] D.S. Kliger, J.W. Lewis, C.E. Randall. *Polarized Light In Optics And Spectroscopy.* Harcourt Brace Jovanovich (Academic Press, Inc.), 1990.

[2] S. Cova, M. Ghioni, A. Lacaita, C. Samori, und F. Zappa. *Avalanche photodiodes and quenching circuits for single-photon detection.* Appl. Opt., **35**, 1956-1976 (1996).

[3] E.Schrödinger. *Die gegenwärtige Situation in der Quantenmechanik.* Naturwissenschaften, **23**, 807(1935).

[4] M. D. Mermin. *Is the moon there when nobody looks? reality and the quatum theory.* Physics Today, **38**, (1985).

[5] C.H. Bennett, G. Brassard. *Quantum Cryptography: Public Key Distribution and Coin Tossing.* Proc. of IEEE International Conference on Computers, Systems & Signal Processing, Bangalore, Indien, 175-179 (Dez. 1984).

[6] C. H. Bennett, G. Brassard, N. D. Mermin. *Quantum cryptography without Bell's theorem.* Phys. Rev. Lett., **68**, 557-559 (1992).

[7] Erwin Schrödinger. *Abhandlungen zur Wellenmechanik.* Analen der Physik, **Bd. 79**, IV. Folge (1926).

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

[9] Marek Zukowski . *Why are Bell Inequalities so exciting.* Vortrag in einem Gruppenseminar der Arbeitsgruppe von Prof. Weinfurter, (08.10.2003).

[10] J.F.Clauser, M.A.Horne, A.Shimony, R.A.Holt. *Proposed experiment to test local hidden-variable theories.* Phys. Rev. Lett., **23**, 880 (1969).

[11] Adán Cabello. *Proposed Experiment to test the Bounds of Quantum Correlations.* e-print arXive, quant-ph/0309172 v2 (8 Oct 2003).

[12] B.S. Cirel'son. *Quantum Generalizations of Bell's Inequality.* Lett. Math. Phys., **4**, 93 (1980).

[13] Dirk Bouwmeester, Artur Ekert, Anton Zeilinger (Eds.). *The Physics of Quantum Information.* (Springer-Verlag), 2000.

[14] G.S. Vernam. *Cipher printing telegraph systems for secret wire and radio telegraphic communications.* Journal of the American Institute of Electrical Engineers, **55**, 109-115 (1926).

[15] Claude Shannon . Communication theory of secrecy systems. Bell Syst. Tech. J, **28**, 656 (1949).

[16] S. Wiesner. *Conjugate coding.* SIGAT News, **15(1)**, 78-88 (1983).

[17] Artur K. Ekert. *Quantum Cryptography Based on Bell's Theorem.* Phys. Rev. Lett., **67**, 661 (1991).

[18] D.S. Naik, C.G. Peterson, A.G. White, A.J. Berglund, P.G. Kwiat. *Entangled State Quantum Cryptography: Eavesdropping on the Ekert Protokoll.* Phys. Rev. Lett., **84**, 4733 (2000).

[19] Thomas Durt, Dagomir Kaszlikowski, Jing-Ling Chen, L.C. Kwek. *Security of Quantum Key Distribution with entangled quNits.* e-print arXive, quant-ph/0302078 v1 (14 Apr 2003).

[20] E.P. Wigner. Am. J. Phys., **38**, 1005 (1970).

[21] Thomas Jennewein, Christoph Simon, Gregor Weihs, Harald Weinfurter, Anton Zeilinger. *Quantum Cryptography with Entangled Photons.* Phys. Rev. Lett., **84**, 4729 (2000).

[22] S. Castelletto, I.P. Degiovanni, M.L. Rastello. *Modified Wigner inequality for secure quantum-key distribution.* Phys. Rev. A, **67**, 044303 (2003).

[23] F.A. Bovino, A.M. Colla, G. Castagnoli, S. Castelletto, I.P. Degiovanni, M.L. Rastello. *Experimental Eavesdropping Attack against Ekert's Protokoll based on Wigner's Inequality.* e-print arXive, quant-ph/0308030 v1 (5 Aug 2003).

[24] Markus Aspelmeyer, Thomas Jennewein, Anton Zeilinger, Martin Pfennigbauer, Walter Leeb. *Long-Distance Quantum Communication with Entangled Photons using Satellites.* e-print arXive, quant-ph/0305105 (19 May 2003).

[25] Bahaa E. A. Saleh, Malvin Carl Teich. *Fundamentals of Photonics.* John Wiley & Sons, Inc., 1991.

[26] L. Mandel, E. Wolf. *Optical Coherence and Quantum Optics.* Cambridge University Press, 1995.

[27] M.Oberparleiter. *Effiziente Erzeugung Verschrnkter Photonenpaare*. Dissertation, 2002.

[28] J. Volz, Ch. Kurtsiefer, and Harald Weinfurter. *Compact all-solid-state source of polarization-entangled photon pairs*. Appl. Phys. Lett., **79**, 869-871 (2001).

[29] Ch. Kurtsiefer, M. Oberparleiter, H. Weinfurter. *High efficiency entangled photon pair collection in type II parametric fluorescence*. Phys. Rev. A, **64**, 023802 (2001).

[30] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden. *Pulsed energy-time entangled twin-photon source for quantum communication*. Phys. Rev. Lett., **82**, 25494-2597 (1999).

[31] S. Tanzilli, H. De Riedmatten, W. Tittel, H. Zbinden, P. Baldi, M. De Micheli, D. B. Ostrowsky, and N. Gisin. *Highly efficient photon-pair sorce using a periodically poled lithium niobate waveguide*. Electron. Lett., **37**, 26-28 (2001).

[32] D. Dehlinger and M. W. Mitchell. *Entangled photon apparatus for the undergraduate laboratory*. Am. J. Phys., **70**, 898-902 (2002).

[33] Ocean Optics Homepage. *http://www.oceanoptics.com/technical/opticalresolution.asp*. Auflösung [FWHM] = Einsatzbereich [nm]/Anzahl Detektor Pixel [px] x Spaltbreite [px].

[34] Daniel F. V. James, Paul G. Kwiat, William J. Munro, and Andrew G. White. *Measurement of qubits*. Phys. Rev. A, **64**, 052312 (2001).

[35] Tzu-Chieh Wei, Kae Nemoto, Paul M. Goldbart, Paul G. Kwiat, William J. Munro, and Frank Verstraete. *Maximal entanglement versus entropy for mixed quantum states*. Phys. Rev. A, **67**, 022110 (2003).

[36] Asher Peres. *Separability Criterion for Density Matrices*. Phys. Rev. Lett., **77**, 1413 (1996).

[37] Michal Horodecki, Pawel Horodecki, Ryszard Horodecki. *Separability of mixed states: necessary and sufficient conditions*. Phys. Lett. A, **223**, 1 (1996).

[38] G. Vidal, R. F. Werner. *Computable measure of entanglement*. Phys. Rev. A, **65**, 032314 (2002).

[39] F. A. Bovino G. Castagnoli, S. Castelletto, I.P. Degiovanni, M. L. Rastello, I. Ruo Berchera. *Experimental evidence of bounds of quantum correlations*. e-print arXive, quant-ph/0310042 (6 Oct 2003).

[40] Ernesto F. Galvão. *Feasible quantum communication complexity protocol*. Phys. Rev. A, **65**, 012318 (2001).

[41] Charles H. Bennett, Stephen Wiesner. *Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States.* Phys. Rev. Lett., **69**, 2881 (1992).

[42] A. C. Yao. *Some Complexity questions related to distributive computing (preliminary report).* Proc. 11th Ann. ACM Symp. on Theory of Computing, 209 (Atlanta, Georgia, May 1979).

[43] H. Buhrman, W. van Dam, P. Høyer, and A. Tapp. *Multiparty quantum communication complexity.* Phys. Rev. A, **60**, 2737 (1999).

[44] H. Buhrman, R. Cleve, W. van Dam. *Quantum Entanglement and Communication Complexity.* e-print arXive, quant-ph/9705033 (18 May 1997).

[45] C. Bruckner, M. Zukowski, J.-W. Pan, A. Zeilinger. *Violation of Bell's inequality: criterion for quantum communication complexity advantage.* e-print arXive, quant-ph/0210114 (14 Oct 2002).

[46] P. Xue, Y.-F. Huang, Y.-S. Zhang, C.-F. Li, and G.-C. Guo. *Reducing the communication complexity with quantum entanglement.* Phys. Rev. A, **64**, 032304 (2001).

[47] A. S. Holevo. *Bounds for the quantity of information transmitted by a quantum communication channel.* Problems of Information Transmission, 9:177-183 (1973).

[48] E. Galvão. *Foundations of quantum theory and quantum information applications.* Dissertation, 2002.

[49] M. Born, E. Wolf. *Principles of Otics.* Cambridge University Press, 1999.

[50] T. S. Larchuk, M. C. Teich, B. E. A. Saleh. *Statistics of Entangled-Photon Coincidences in Parametric Downconversion.* Fundamental Problems in Quantum Theory: A Conference Held in Honor of Professor A. Wheeler, **Volume 755 of the Annals of the New York Academy of Sciences**, (April 7, 1995).

[51] B. Schneier. *Applied Cryptography.* John Wiley & Sons, Inc., 1996.

[52] M. Hillery, V. Bužek, A. Berthiaume. *Quantum secret sharing.* Phys. Rev. A, **59**, 1829 (1999).

[53] W. Tittel, H. Zbinden, N. Gisin. *Experimental demonstration of quantum secret sharing.* Phys. Rev. A, **63**, 042301 (2001).

[54] B. Huttner, A. Ekert. *Information gain in quantum eavesdropping.* J. Mod. Opt., **41**, 2455 (1994).

[55] M. Bourennane. *Long Wavelength Quantum Cryptography, Single-Photon Detection, and Quantum Entanglement Applications.* Dissertation, 2001.

[56] M. Aspelmeyer, H. Bhm, T. Gyatso, T. Jennewein, R. Kaltenbaek, M. Lindenthal, G. Molina-Terriza, A. Poppe, K. Resch, M. Taraba, R. Ursin, P. Walther, A. Zeilinger. *Long-Distance Free-Space Distribution of Quantum Entanglement.* Sience, **301**, 621 (2003).

[57] M. Weber. *Wie man die Werte von σ_x, σ_y und σ_z eines Spin-$\frac{1}{2}$ Teilchens bestimmt.* Diplomarbeit, 2000.

Danksagung

Am Ende angelangt, möchte ich einigen Personen, die zum erfolgreichen Gelingen der Arbeit beigetragen haben meinen Dank aussprechen.

Bedanken möchte ich mich bei Herrn Prof. Harald Weinfurter, der mir durch die Aufnahme in seine Gruppe die Arbeit in einem für mich so faszinierenden Gebiet der Physik ermöglichte. Seine Ratschläge gaben oft, gerade in schwierigen Situationen, den Anstoß zum Weiterkommen.

Mein ganz besonderer Dank gebührt Herrn Dr. Mohamed Bourennane für die Betreuung. Er inspirierte uns zu neuen Ideen und half mir bei der Lösung vieler Probleme. Besonderen Dank möchte ich auch Herrn Pavel Trojek aussprechen für eine auf menschlicher wie fachlicher Ebene harmonische und hervorragende Zusammenarbeit, die, wie ich denke, sehr fruchtbar war. Desweiteren ergeht ein herzliches Dankeschön an Herrn Manfred Eibl und Herrn Nikolai Kiesel. Sie haben mir durch ihren physikalischen Sachverstand in einigen Diskussionen zu differenzierten Sichtweisen verholfen.

Ich danke ferner allen, die mir gelegentlich bei den „kleinen technischen Problemen des experimentellen Alltages“ weiterhalfen, Herrn Dr. Christian Kurtsiefer, Herrn Henning Weier, Herrn Tobias Schmitt-Manderbach, Herrn Carsten Schuck, Herrn Jürgen Volz und allen anderen Gruppenmitgliedern, Oliver Schulz, Markus Weber, Chunlang Wang, Gerhard Huber, Sascha Gärtner, Julia Lau, Johannes Vrana.

Für hilfreiche Diskussionen und Zusammenarbeit möchte ich mich auch bei Herrn Prof. Marek Żukowski und Herrn Dr. Adán Cabello bedanken.

Schließen möchte ich in tiefer Verbundenheit und Dankbarkeit zu meinen Eltern für ihr Vertrauen in mich und ihre bedingungslose Unterstützung, mentaler wie materieller Art, im Laufe meiner gesamten Ausbildung.

Erklärung

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

Christian Immanuel Thaddäus Schmid
München, den 12. Januar 2004