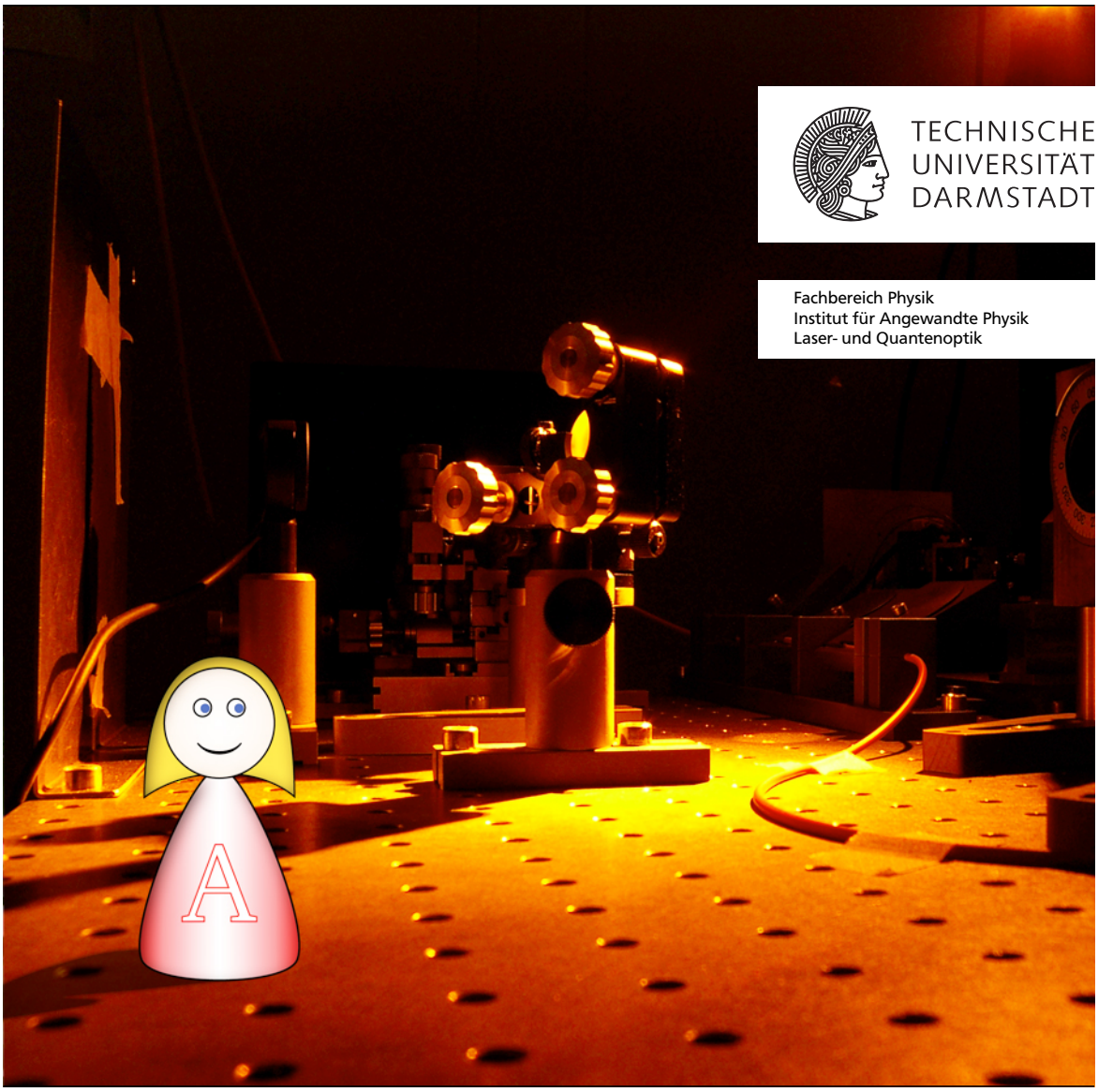
Optimierung von Spontaner Parametrischer Fluoreszenz in PPKTP für ein Alice-Modul

Optimization of Spontaneous Parametric Down-Conversion in PPKTP for an Alice module

Bachelor-Thesis von Mischa Hildebrand

Juli 2009



Optimierung von Spontaner Parametrischer Fluoreszenz in PPKTP für ein Alice-Modul
Optimization of Spontaneous Parametric Down-Conversion
in PPKTP for an Alice module

vorgelegte Bachelor-Thesis von Mischa Hildebrand

1. Gutachten: Prof. Dr. Thomas Walther
2. Gutachten: Dr. Mathias Sinther

Tag der Einreichung:

Erklärung zur Bachelor-Thesis

Hiermit versichere ich die vorliegende Bachelor-Thesis ohne Hilfe Dritter nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, den 21. Juli 2009

_____

(Mischa Hildebrand)

Zusammenfassung

In meiner Bachelor-Thesis habe ich am Aufbau des Sender-Moduls einer quantenkryptografischen Übertragungsstrecke gearbeitet. Dabei habe ich im Wesentlichen versucht, eine maximale Effizienz der spontanen parametrischen Fluoreszenz im verwendeten PPKTP-Kristall zu erreichen.

Kapitel 1 gibt zunächst eine phänomenologische Einführung in die Quantenkryptografie und erläutert, worin deren Vorteile gegenüber der klassischen Kryptografie liegen. In Kapitel 2 werden die kryptografischen und physikalischen Grundlagen für die durchgeführten Experimente gelegt. Das dieser Arbeit zu Grunde liegende BB84-Protokoll wird in zehn Schritten anschaulich erklärt. Kapitel 3 führt in den Versuchsaufbau ein und erläutert, wie das BB84-Protokoll im Experiment implementiert werden soll. Im Anschluss folgt eine Vorstellung sowie eine Analyse der Messungen, welche im Rahmen dieser Arbeit durchgeführt wurden.

Inhaltsverzeichnis

1 Einleitung

1.1 Ein Quantensprung des Menschen

Die Lebensweise des Menschen hat sich im vergangenen Jahrhundert so schnell verändert wie niemals zuvor. Dank bahnbrechender Entdeckungen in der Physik und den anderen Naturwissenschaften genießen wir heute einen technologischen Standard, den sich frühere Generationen nicht einmal hätten vorstellen können. Es ist für uns zur Selbstverständlichkeit geworden, in jedem Haus elektrischen Strom zur Verfügung zu haben, mit dem die Heizung, der Elektroherd, der Kühlschrank, der Fernseher und der Computer betrieben werden. Durch Autos, Züge und Flugzeuge sind wir individuell mobil geworden und können innerhalb weniger Stunden Hunderte von Kilometern zurücklegen.

Vieles ist in den letzten Jahrzehnten digitalisiert worden: Wir bezahlen fast schon häufiger mit Kreditkarte als mit Bargeld, tätigen Überweisungen über das Internet bequem von zu Hause, wir schreiben uns und telefonieren sogar über das Internet, auf das wir (und jeder andere!) von fast überall zugreifen können.

Immer wichtiger wird deshalb die Frage nach der Sicherheit solcher Technologien: Wie gelingt es, Informationen zwischen zwei Parteien derart auszutauschen, dass sie niemand außer dem Sender und dem gewünschten Empfänger lesen oder gar manipulieren kann?

Obwohl die Verschlüsselung im privaten Bereich erst seit Beginn des Computer-Zeitalters eine wesentliche Rolle spielt, beschäftigt diese Frage den Menschen schon seit geraumer Zeit: Bereits vor über 4000 Jahren entwickelten die Ägypter einfache Methoden, um Informationen geheim zu halten und auch in Indien, China und Japan gab es erste Ansätze für Verschlüsselungsverfahren. Um 400 v. Chr. verwendeten die Spartaner im antiken Griechenland eine sog. *Skytale* zur Verschlüsselung militärischer Nachrichten (Abb. 1.1) [Ser06]:

Ein langer Streifen aus Pergament oder Leder wurde um einen Stab gewickelt und entlang des Stabs mehrzeilig mit der Nachricht beschrieben. Dann wurde der Streifen wieder abgewickelt und ein Bote überbrachte ihn dem Empfänger. Da die Buchstaben auf dem abgewickelten Streifen nicht mehr in der richtigen Reihenfolge standen, konnte niemand unterwegs die Nachricht entziffern – die einzelnen Buchstaben ergaben nur dann einen Sinn, wenn der Streifen um einen Stab mit genau demselben Durchmesser gewickelt wurde, den auch der Stab des Senders hatte.

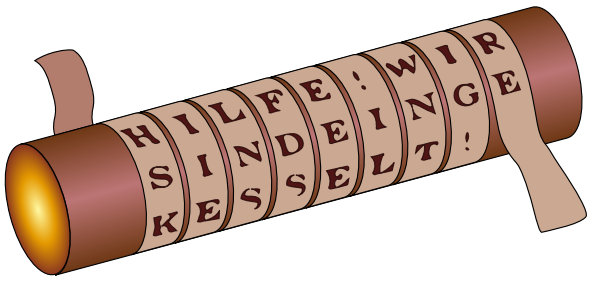


Abbildung 1.1: Skytale: Verschlüsselungsrolle der Spartaner

Ein anderes Verschlüsselungsverfahren verwendete Cäsar, wenn er geheime Botschaften an seine Generäle übermittelte: Er ersetzte in seiner Nachricht jeden Buchstaben durch seinen dritten Folgebuchstaben, d.h. A → D, B → E, C → F, usw. Die Nachricht konnte vom Empfänger nur dann gelesen werden, wenn dieser zuerst die umgekehrte Ersetzung durchführte.

1.2 Wie sicher ist sicher?

Cäsars Verschlüsselungssystem ist natürlich einfach zu knacken. Wenn alle Buchstaben um eine feste Anzahl an Stellen verschoben werden, so würde man höchstens 26 Versuche benötigen, um die richtige Verschiebungsanzahl zu finden und die Botschaft lesen zu können. Auch das durchdachte System der Spartaner könnte durch Ausprobieren vieler Stäbe verschiedenen Durchmessers mit recht geringem Aufwand geknackt werden.

Im Laufe der Jahrhunderte wurden zwar immer neue, kompliziertere und schwerer zu brechende Verschlüsselungsmechanismen entwickelt. Das Grundproblem der Kryptografie ist allerdings seit den ersten Verschlüsselungsversuchen der Ägypter unverändert geblieben: Einerseits muss die Nachricht vom Sender mit einem nicht-trivialen Schlüssel kodiert werden; andererseits muss dem Empfänger bekannt sein, wie er die kodierte Nachricht wieder dekodieren kann – er benötigt ebenfalls einen Schlüssel. Dieser muss ihm vom Sender irgendwie übermittelt werden und zwar so, dass keine unberechtigte Drittperson darauf Zugriff bekommen kann.

Da aber alle klassischen elektronischen Übertragungswege prinzipiell abgehört werden können, stellt gerade die Übertragung des Schlüssels das essenzielle Problem der Kryptografie dar.[1] Die einzige Möglichkeit zum sicheren Austausch eines Schlüssels ist ein persönliches Treffen des Senders mit dem Empfänger, doch die Unpraktikabilität dieses Verfahrens in der globalisierten Welt ist offensichtlich.

Im Jahr 1976 lösten die Kryptologen Martin Hellman und Whitfield Diffie dieses Problem auf eine völlig unkonventionelle Art und Weise: Sie schlugen vor, zwei *verschiedene* Schlüssel zum Kodieren und Dekodieren der Nachricht zu verwenden [DH76]. Der Kodierungsschlüssel *(public key)* kann öffentlich bekannt gegeben werden und bedarf keiner besonderen Geheimhaltung. Es ist also grundsätzlich jeder Person möglich, eine Nachricht zu verschlüsseln. Der Dekodierungsschlüssel *(private key)* hingegen ist nur dem Empfänger bekannt, sodass nur dieser die Nachrichten lesen kann, welche mit dem *public key* kodiert wurden.

Damit dieses System funktioniert, müssen *public key* und *private key* natürlich in irgendeiner Weise miteinander zusammenhängen. Wenn 🗎 die sicher zu übertragende Nachricht darstellt, V die Verschlüsselungsprozedur und E die Entschlüsselungsprozedur, so muss natürlich gelten [RSA78]:

$$E\left(V(🗎)\right) = 🗎 \quad , \tag{1.1}$$

d.h. E muss in gewisser Weise eine Art Umkehrfunktion zu V sein. Diese Verbindung von E und V gibt potenziellen Abhörern eine Angriffsfläche, um den *private key* zu ermitteln. Um

[1] Aus diesem Grund spricht man im Englischen bei der Verschlüsselung über Quantenkanäle auch von der *Quantum Key Distribution* (kurz: QKD) statt von der *Quantum Cryptography*, vgl. Kapitel 2.

diese aber so gering wie möglich zu halten, verwendet man in der Praxis zur Generierung der Schlüssel Funktionen, deren Umkehrfunktionen ohne zusätzliche Informationen (die nur der Empfänger besitzt) mit heutiger Rechenleistung quasi nicht bestimmt werden können. Solche Funktionen werden als *Einwegfunktionen* bezeichnet.

Eine erste praktische Implementierung des *Public Key Verfahrens* veröffentlichten im Jahr 1978 die Wissenschaftler RONALD L. RIVEST, ADI SHAMIR und LEONARD ADLEMAN [RSA78]. Der nach ihnen benannte *RSA-Algorithmus* basiert auf der Zerlegung sehr großer Zahlen in ihre Primfaktoren – eine Aufgabe, die heutige Computer in vertretbaren Zeiträumen nicht leisten können. RSA erfüllt also die Forderung nach einer genügend guten Einwegfunktion und wird daher heute bei vielen Übermittlungen und Transaktionen als Kryptosystem verwendet. Es gilt als sicheres Verschlüsselungsverfahren.

Nach diesen Erläuterungen dürfte nun aber klar geworden sein, dass die Sicherheit jedes gegenwärtigen (klassischen) Kryptosystems nur eine relative Sicherheit ist. JONATHAN KNUDSEN schreibt in seinem 1998 veröffentlichten Buch *Java Cryptography* [Knu98]:

> *In truth, there is no absolute security. Every system can be broken, given enough time and money. Let me say that again, every system can be broken.*

Tatsächlich haben Wissenschaftler in den letzten Jahren mit dem Konzept des *Quantencomputers* eine Möglichkeit gefunden, welche das RSA-Verfahren schon in naher Zukunft schlagartig unsicher machen könnte.[2] Sobald der erste Quantencomputer in Betrieb geht, könnten alle RSA-verschlüsselten Nachrichten, Bankkonten etc. innerhalb weniger Minuten mühelos geknackt werden [Ser06, S. 8].

1.3 Eines ist sicher: Quantenkryptografie

Es ist bemerkenswert, dass gerade die Quantenmechanik, welche die Sicherheit heutiger Kryptosysteme aufs Spiel setzt, zur Entwicklung eines Forschungsgebiets geführt hat, das sich mit der Umsetzung von endgültig sicheren Verschlüsselungsverfahren beschäftigt: der Quantenkryptografie. Sie nutzt die Eigenschaft von quantenmechanischen Zuständen, dass im Allgemeinen keine Messung vorgenommen werden kann, ohne den Zustand selbst zu verändern. Es besteht für Sender und Empfänger daher stets die Möglichkeit zu überprüfen, ob ihre Nachrichtenübertragung abgehört wird und sie in diesem Fall sofort zu unterbrechen.

Im Gegensatz zu allen anderen bis heute entwickelten Verschlüsselungsverfahren basiert Übertragungssicherheit bei der Quantenkryptografie nicht auf der mathematischen Schwierigkeit, den Dekodierungsschlüssel zu ermitteln, sondern auf physikalischen Naturgesetzen. Es besteht somit *prinzipiell* keine Möglichkeit eines erfolgreichen Lauschangriffs. Im schlimmsten Fall kann die Übertragung höchstens gestört werden, sodass ein neuer Anlauf der Nachrichtenübermittlung vorgenommen werden muss. Entgegen KNUDSENS Behauptung ist die Quantenkryptografie also sehr wohl in der Lage, eine absolute Übertragungssicherheit zu garantieren. Wie dies funktioniert, wird im Abschnitt 2.3 des nächsten Kapitels erläutert.

[2] Quantencomputer sind keine alltagstauglichen Rechner, sondern nur für spezielle Aufgaben sinnvoll einsetzbar. Eine dieser Aufgaben ist aber gerade die Primfaktorzerlegung, die ein Quantencomputer z. B. mittels des *Shor-Algorithmus* in sehr viel kürzerer Zeit erledigen könnte als ein klassischer Computer [Hof08, Kap. 8].

1.4 Motivation dieser Arbeit

Es ist das Ziel der Arbeitsgruppe „Laser- und Quantenoptik“ an der TU Darmstadt, eine quantenkryptografische Übertragungsstrecke praktisch zu realisieren. Ein Empfangsmodul *(Bob)* wurde bereits im November 2008 von Daniel Rieländer fertiggestellt [Rie08]. Die vorliegende Bachelor-Thesis hat nun zum Ziel, ein funktionsfähiges Sender-Modul möglichst weit aufzubauen. Sender und Empfänger sollen in diesem Experiment über das sog. *BB84-Protokoll* miteinander kommunizieren (vgl. Abschnitt 2.3.1). Über die kryptografischen und physikalischen Grundlagen informiert das nächste Kapitel.

2 Grundlagen

2.1 Grundzüge der Kryptografie

Die Sicherheit von Information ist heute ein wichtiges Forschungsgebiet, mit dem sich die *Kryptologie* beschäftigt. Sie spaltet sich auf in die beiden Teilbereiche *Kryptografie* und *Kryptoanalyse*. Das Ziel der Kryptografie ist die Entwicklung von Verschlüsselungsverfahren zur sicheren Datenübertragung, wohingegen die Kryptoanalyse nach Methoden sucht, um existente Verschlüsselungsverfahren zu brechen und Information aus verschlüsselten Nachrichten zu extrahieren.

Zur Zeit liegen die Kryptografen im Rennen vorne: Mit dem RSA-Verfahren ist es ihnen gelungen, einen verschlüsselten Datenaustausch zu etablieren, für den die Kryptoanalytiker bis heute keine realistische Abhörmöglichkeit gefunden haben. Wie in Abschnitt 1.2 erwähnt, könnte sich dies in einigen Jahrzehnten aber ruckartig ändern. Im Folgenden werden die wichtigsten Aspekte der modernen Kryptografie erläutert.

2.1.1 Gestatten: Alice & Bob

Die Standardsituation der Kryptografie ist in Abbildung 2.1 dargestellt: Ein Sender *A* möchte eine Nachricht an einen Empfänger *B* schicken, ohne dass ein beliebiger Angreifer *E* Zugriff auf die Inhalte der Nachricht bekommen kann. Da diese Situation immer wieder auftritt, ist es in der Kryptologie Konvention, den Sender der Nachricht personifiziert als *Alice* und den Empfänger als *Bob* zu bezeichnen (entsprechend dem *A*- bzw. *B*-Teilnehmer in der Telekommunikation). *Eve*[1] ist dagegen ein Pseudonym für jede Person, die einen Lauschangriff auf die Übertragung starten kann. Ihr werden alle physikalischen Möglichkeiten des Abhörens zugesprochen.

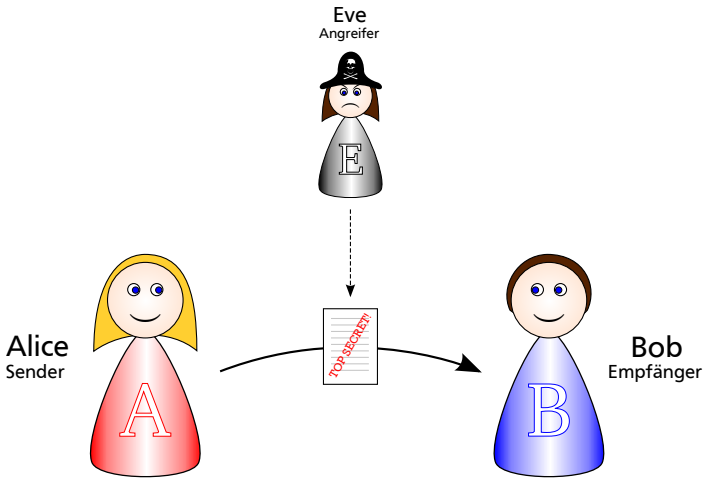


Abbildung 2.1: Namenskonventionen der Kryptologie

[1] abgeleitet vom englischen *eavesdropping*: Lauschen, Abhören

2.1.2 Substitution & Transposition

Wie kann man nun eine Nachricht in der Praxis verschlüsseln? Betrachten wir einen gegebenen, festen Zeichensatz – z. B. das deutsche Alphabet – und eine zu übermittelnde Nachricht:

$$\text{📄} \quad = \quad \text{“HEUTE KOSTENLOS KUCHEN!”}$$

Die Nachricht selbst wird in der Kryptografie als *Klartext* bezeichnet; im Gegensatz dazu nennt man die verschlüsselte Nachricht *Kryptogramm*. Es gibt nun genau zwei Möglichkeiten, die Nachricht zu verschlüssen [Ser06, Kap. 1]:

1. **Substitution:**
   Man ersetzt jeden Buchstaben des Klartextes durch einen anderen Buchstaben.
2. **Transposition:**
   Man setzt die einzelnen Buchstaben jeweils an eine andere Position, z. B. durch wiederholte Vertauschung jeweils zweier Buchstaben.

Eine der einfachsten Realisierungen der ersten Methode verwendete Cäsar bei seinem Verschlüsselungsverfahren (vgl. Abschnitt 1.1), welches wir mit V_S bezeichnen wollen. Wendet man dieses auf die Nachricht 📄 an, so ergibt sich:

$$V_S(\text{📄}) \quad = \quad \text{“KHXWH NRVWHQORV NXFKHQ!”} \quad ,$$

wobei die folgenden Substitutionsregeln angewendet wurden:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Für das deutsche Alphabet mit 26 Buchstaben gibt es insgesamt 26! mögliche Substitutionsregelsätze, wobei es natürlich der Sicherheit förderlich ist, wenn nicht jeder Buchstabe gerade nach demselben Muster ersetzt wird (wie hier die Verschiebung um drei Buchstaben).

Die ebenfalls in Abschnitt 1.1 erwähnte Skytale ist hingegen ein Verschlüsselungsverfahren, bei dem von der Transposition Gebrauch gemacht wird. Durch das Abwickeln des Nachrichtenstreifens vom Stab werden die Buchstaben räumlich in eine andere Anordnung gebracht. Permutiert man die Buchstaben untereinander nur innerhalb der Zeile, so könnte das Kryptogramm der Nachricht so aussehen:

$$V_T(\text{📄}) \quad = \quad \text{“NEUE KOKOSSCHUTT LEHNE!”} \quad ,$$

wobei die Buchstabenpositionen als Beispiel nach den folgenden Transpositionsregeln vertauscht wurden (Leer- und Ausrufezeichen wurden als Zeichen mitgezählt):

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
20	19	14	16	2	17	6	9	11	15	4	21	18	7	10	5	8	3	12	13	22	1	23

Während die Verschlüsselung einer längeren Nachricht per Substituation i. d. R. durch Häufigkeitsanalysen recht einfach geknackt werden kann[2], ist die Dechiffrierung einer per Transposition verschlüsselten Nachricht ohne Kenntnis des Schlüssels schon schwieriger. Um maximale Sicherheit zu gewährleisten, verwenden moderne Verschlüsselungsverfahren zum Kodieren einer Nachricht meist eine Superposition aus Substitution und Transposition, d.h. beide Verfahren werden in beliebiger Reihenfolge hintereinander angewendet [Pet06, S. 6].

2.1.3 Symmetrische und asymmetrische Verschlüsselung

Bis in die frühen 1970er Jahre war nur die sog. *symmetrische Verschlüsselung* bekannt. Wie der Begriff impliziert, wird dabei eine Nachricht mit *demselben* Schlüssel entschlüsselt, mit dem sie auch verschlüsselt wurde. Anschaulich entspricht dieses Verfahren einem einfachen Schließfach: Alice öffnet das Fach mit dem passenden Schlüssel, hinterlegt eine Nachricht und schließt das Fach wieder. Sie übergibt den Schlüssel (oder eine Kopie desselben) an Bob, der das Schließfach wieder öffnen kann, indem er den Schlüssel einfach in die andere Richtung dreht (Symmetrie).

Solche symmetrischen Kryptosysteme haben einen wesentlichen Nachteil, wenn man allein die Gültigkeit der klassischen Physik voraussetzt und und quantenmechanische Effekte außer Acht lässt: Damit der Nachrichtenaustausch sicher erfolgen kann, muss Alice den Schlüssel derart an Bob übergeben, dass für keine dritte Partei (Eve) die Möglichkeit besteht, ebenfalls in Besitz des Schlüssels zu gelangen oder eine Kopie anzufertigen. Dies ist klassisch aber nur dann möglich, wenn sich Alice und Bob persönlich treffen, wie bereits in Abschnitt 1.2 angesprochen.

Aus praktischen Gründen behilft man sich heute daher meistens mit der *asymmetrischen Verschlüsselung*, deren Konzept in Abbildung 2.2 dargestellt ist. Statt einem einzigen Schlüssel zum Kodieren und Dekodieren werden bei der asymmetrischen Verschlüsselung zwei *verschiedene* Schlüssel verwendet:

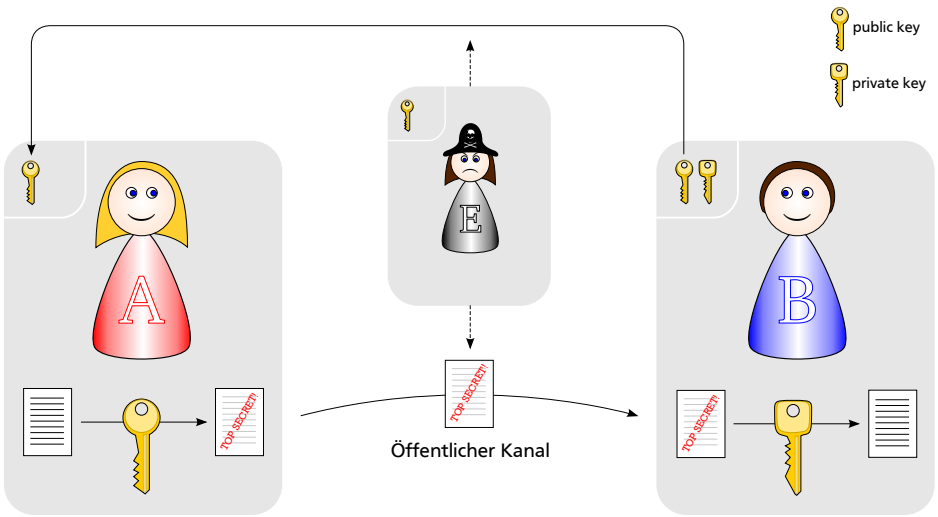


Abbildung 2.2: Schematische Darstellung eines asymmetrischen Kryptosystems

[2] Der Buchstabe *E* kommt im Deutschen z.B. mit 17,4% mit Abstand am häufigsten vor, gefolgt vom *N* mit 9,8%, dem *I* mit 7,6% usw. [Beu05, S. 10]

Bob bestimmt zunächst einen zufälligen Schlüssel *(private key)*, aus dem er mittels einer Einwegfunktion (vgl. Abschnitt 1.2) einen zweiten Schlüssel *(public key)* generiert. Diesen *public key* versendet er über einen öffentlichen Kanal an Alice, die damit ihre Nachricht verschlüsselt. Da der Schlüssel öffentlich übertragen wird, kann auch Eve Zugriff darauf erhalten. Nun versendet Alice ihr Kryptogramm wieder über einen öffentlichen Kanal an Bob. Eve kann auch diese Übertragung abfangen. Sie kann allerdings keine Information aus der Nachricht gewinnen, da sie wie Alice nur den *public key* besitzt, mit dem eine Nachricht lediglich *ver*schlüsselt werden kann. Bob kann hingegen das Kryptogramm einfach mit seinem *private key* entschlüsseln und die Nachricht im Klartext lesen.

Da das Charakteristikum der asymmetrischen Verschlüsselung der öffentliche Schlüssel ist, wird dieses Verfahren synonym auch als *Public Key Verschlüsselung* bezeichnet. Ein passendes Analogon ist z. B. ein Postbriefkasten: Während jede Person Nachrichten einwerfen kann, ist nur der Postbote in der Lage, die Nachrichten mit seinem Briefkastenschlüssel zu entnehmen und – wenn man ihm böse Absichten unterstellt – auch zu lesen.

Zwar steht die asymmetrische Verschlüsselung durch Verwendung des öffentlichen Schlüssels nicht vor dem Problem der Schlüsselverteilung, doch auch dieses Verfahren hat Nachteile: Einerseits ist es gegenüber dem symmetrischen Verfahren wesentlich langsamer und bei Versendung einer Nachricht an mehrere Empfänger muss diese für jeden Empfänger einzeln verschlüsselt werden. Andererseits basiert die asymmetrische Verschlüsselung stets auf der unbewiesenen Annahme, dass ein potenzieller Angreifer Eve aufgrund des hohen Rechenaufwands nicht in der Lage ist, den *private key* zu ermitteln.

Um die Nachteile von symmetrischer und asymmetrischer Verschlüsselung zu minimieren, werden in der Praxis häufig sog. *Hybridverfahren* eingesetzt, bei denen die initiale Verbindung meist asymmetrisch hergestellt wird, während die eigentliche Nachrichtenübermittlung dann symmetrisch erfolgt.

2.1.4 Das *One-Time-Pad*

Im Gegensatz zur *Public Key Verschlüsselung* kann ein symmetrisches Verschlüsselungsverfahren unter gewissen Umständen *absolut* sicher sein. Gilbert Vernam entwickelte 1926 ein solches Verfahren, welches z. B. in der Quantenkryptografie Anwendung findet und unter dem Namen *One-Time-Pad* bekannt ist. Erst nach dem Zweiten Weltkrieg bewies Claude Shannon (1949), dass dieses Verschlüsselungsverfahren perfekte Sicherheit bietet, wenn nur Alice und Bob den Schlüssel besitzen und die folgenden Bedingungen erfüllt sind [KM08]:

1. Der Schlüssel ist mindestens so lang wie die zu verschlüsselnde Nachricht.
2. Der Schlüssel ist rein zufällig.
3. Der Schlüssel darf nur ein einziges Mal verwendet werden.

Klassische Computer tauschen Informationen untereinander über *Bits* aus, wobei ein Bit entweder den Zustand 0 oder den Zustand 1 haben kann. Die Anwendung des *One-Time-Pad* soll daher nun anhand des Binärsystems erläutert werden (nach [Rie08]): Angenommen, Alice möchte die folgende Nachricht verschlüsselt an Bob senden:

$$\text{📄} = \text{“TU”} ,$$

Stelle i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	T								U							
Klartext (Binär)	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1
Schlüssel	1	1	1	0	0	1	1	0	0	1	1	0	1	0	1	0
XOR-Wert (Kryptogramm)	1	0	1	1	0	0	1	0	0	0	1	1	1	1	1	1

Tabelle 2.1: Kodierung der Nachricht „TU“ mit dem *One-Time-Pad*-Verfahren

Stelle i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Kryptogramm	1	0	1	1	0	0	1	0	0	0	1	1	1	1	1	1
Schlüssel	1	1	1	0	0	1	1	0	0	1	1	0	1	0	1	0
XOR-Wert (Klartext)	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1
	T								U							

Tabelle 2.2: Dekodierung des in Tabelle 2.1 generierten Kryptogramms

Dann wandelt sie zunächst die einzelnen Buchstaben in ihren entsprechenden Binärcode um, wie in Tab. 2.1 dargestellt. Als Schlüssel generiert sie nun eine rein zufällige Binärzeichenfolge derselben Länge. Aus dem i-ten Zeichen des Klartextes und dem i-ten Zeichen des Schlüssels bildet sie dann den sog. *XOR*-Wert.[3] Die Zeichenfolge der *XOR*-Werte ist schließlich das Kryptogramm, welches an Bob geschickt wird. Es ist wie der Schlüssel komplett zufällig und enthält keine Informationen mehr über den Inhalt der Nachricht.

Bob empfängt das Kryptogramm von Alice und kann mit seiner Kopie des Schlüssels wieder den *XOR*-Wert aus Kryptogramm- und Schlüssel-Bits bilden (Tab. 2.2). (Die *XOR*-Abbildung zweier Bits hat also die besondere Eigenschaft, ihre eigene Umkehrabbildung zu sein.) Durch Rücktransformation des daraus erhaltenen Binär-Klartextes in Buchstaben erhält Bob die ursprüngliche Nachricht. Das einzige Problem des *One-Time-Pad*-Verfahrens ist die absolut sichere Schlüsselverteilung *(key distribution)*. Dieses vermag die Quantenkryptografie zu lösen (siehe Abschnitt 2.3).

2.2 Physikalische Grundlagen

Im vorigen Abschnitt wurde bereits erläutert, dass eine absolut sichere Schlüsselübertragung über größere Distanzen mit Hilfe klassischer Physik nicht möglich ist. Im Folgenden sollen daher zunächst einige wichtige Konzepte der modernen Physik vorgestellt werden, welche für das Verständnis der vorliegenden Arbeit von fundamentaler Bedeutung sind.

[3] *XOR* steht für *e**x**clusive **or***. Der *XOR*-Wert zweier Bits b_1 und b_2 ist 1, wenn eines der beiden Bits den Wert 1 und das andere den Wert 0 hat; ansonsten ist der *XOR*-Wert 0. Mathematisch kann man den *XOR*-Wert wie folgt berechnen:

$$XOR(b_1, b_2) = (b_1 + b_2) \bmod 2$$

2.2.1 Quantenmechanik

In den ersten Jahrzehnten des 20. Jahrhunderts stellten zwei neu entdeckte Prinzipien das klassische Weltbild der Physik auf den Kopf: das Relativitätsprinzip und das Quantisierungsprinzip. Beide entziehen sich auch heute noch der menschlichen Vorstellungskraft und sind in vielen Bereichen äußerst kontraintuitiv. Während das Relativitätsprinzip nur bei sehr hohen Geschwindigkeiten ein von der klassischen Physik stark abweichendes Verhalten postuliert, zeigt das Quantisierungsprinzip vor allem im mikroskopischen Bereich seine nicht-klassischen Auswirkungen. Letzteres besagt, dass viele physikalische Größen nicht kontinuierlich jeden beliebigen Wert, sondern nur bestimmte diskrete Werte annehmen können – sie sind quantisiert.

Ausgehend von dieser Entdeckung[4] entwickelte Werner Heisenberg 1925 die *Matrizenmechanik*, Erwin Schrödinger unabhängig davon ein Jahr später die *Wellenmechanik* [Rot09]. Schon kurz darauf konnte Schrödinger zeigen, dass seine Wellenmechanik der Matrizenmechanik äquivalent ist. Paul A. M. Dirac gelang schließlich im Jahr 1930 die Vereinheitlichung beider Formulierungen. Die Ausführungen in seinem Werk *„The principles of quantum mechanics“* gelten als Grundstein der modernen Quantenmechanik und sind heute noch in unveränderter Form gültig.

Im Gegensatz zur klassischen Physik ist es in der Quantenmechanik nicht mehr möglich, physikalische Messgrößen – genannt *Observablen* – zu einem beliebigen Zeitpunkt genau vorherzusagen, wenn die gesamte Anfangskonfiguration des betrachteten Systems zu einem Zeitpunkt t_0 bekannt ist. Stattdessen können nur noch Wahrscheinlichkeitsaussagen über den Ausgang einer Messung gemacht werden. Man kann dies so interpretieren, als würde eine solche Messgröße vor der Messung gar nicht definiert sein und überhaupt erst mit der Messung real werden. Aus diesem Grund wird in der Quantenmechanik strikt zwischen dem Zustand eines Systems und den Observablen unterschieden.

Ein quantenmechanischer Zustand enthält die gesamte Information über das betrachtete System. Er wird durch einen (normierten) Vektor im Hilbertraum $\mathscr{H}$ beschrieben, welcher in der *Bra-Ket-Notation* wie folgt geschrieben wird:

$$\left|\psi, t\right\rangle \tag{2.1}$$

Für zwei Zustandsvektoren $\left|\psi_1, t\right\rangle$ und $\left|\psi_2, t\right\rangle$ gilt das *Superpositionsprinzip*, d. h. jede Linearkombination dieser Zustandsvektoren

$$\left|\psi, t\right\rangle \;=\; c_1 \left|\psi_1, t\right\rangle \;+\; c_2 \left|\psi_2, t\right\rangle \tag{2.2}$$

ist wieder ein möglicher Zustand.

Eine Observable wird durch einen *hermiteschen Operator* $\hat{O}$ repräsentiert[5], für den definitionsgemäß gilt:

$$\hat{O}^\dagger \;=\; \left(\hat{O}^*\right)^T \;\equiv\; \hat{O} \tag{2.3}$$

[4] Schlüsselexperimente zur Quantisierung waren u. a. die Schwarzkörperstrahlung und der fotoelektrische Effekt.

[5] Die Eigenwerte eines hermiteschen Operators sind stets reell – genau wie alle physikalischen Messgrößen.

Für jede klassische Observable ist über Korrespondenzregeln ein zugehöriger Operator definiert. Die Messung einer Observablen kann stets nur Eigenwerte o_i des Operators als Ergebnis haben, welche über dessen Eigenwertgleichung definiert sind:

$$\hat{O}\left|o_i\right\rangle = o_i\left|o_i\right\rangle \tag{2.4}$$

Der Zustand des Systems nach der Messung ist dann $\left|o_i\right\rangle$. Die Wahrscheinlichkeit dafür, als Messergebnis der Observablen $\hat{O}$ den Eigentwert o_i zu erhalten, ist durch das Betragsquadrat des Skalarprodukts aus dem Zustand $\left|\psi, t\right\rangle$ vor und dem Zustand $\left|o_i\right\rangle$ nach der Messung gegeben:

$$P(o_i) = \left|\left\langle o_i \,|\, \psi, t\right\rangle\right|^2 \tag{2.5}$$

Ausführliche und gut verständliche Erläuterungen zu diesem mathematischen Formalismus findet man z. B. im Lehrbuch von R. Shankar [Sha94].

2.2.2 Das *No Cloning*-Theorem

Eine Folge der Quantenmechanik ist das *No Cloning*-Theorem, welches einen sicheren Schlüsselaustausch beim sog. *BB84-Protokoll* ermöglicht (vgl. Abschnitt 2.3.1):

> *Es ist unmöglich, eine ideale Kopie eines beliebigen unbekannten Quantenzustands $\left|\psi\right\rangle$ anzulegen.*

Den einfachen Beweis dieser Aussage veröffentlichten die Physiker William K. Wootters und Wojciech Zurek 1982 in der Fachzeitschrift *Nature* [WZ82]. Er wird als Widerspruchsbeweis geführt (siehe auch [GRTZ02]):

Angenommen, es würde eine Maschine existieren, welche perfekte Kopien eines unbekannten Quantenzustands $\left|\psi_1\right\rangle$ anlegen kann. Sie würde also folgendes bewirken:

$$\left|M_0\right\rangle\left|\psi_1\right\rangle \rightarrow \left|M_1\right\rangle\left|\psi_1\right\rangle\left|\psi_1\right\rangle \tag{2.6}$$

$\left|M_0\right\rangle$ beschreibt dabei den Zustand der Kopiermaschine vor dem Kopieren, $\left|M_1\right\rangle$ ihren Zustand danach. Da die Kopiermaschine in der Lage sein soll, jeden beliebigen Zustand zu kopieren, muss dieselbe Gleichung auch für einen Zustand $\left|\psi_2\right\rangle$ gelten:

$$\left|M_0\right\rangle\left|\psi_2\right\rangle \rightarrow \left|M_2\right\rangle\left|\psi_2\right\rangle\left|\psi_2\right\rangle \tag{2.7}$$

Nach dem Superpositionsprinzip ist nun auch

$$\left|\psi_S\right\rangle = c_1\left|\psi_1\right\rangle + c_2\left|\psi_2\right\rangle \tag{2.8}$$

wieder ein möglicher Quantenzustand, welchen die Kopiermaschine gemäß ihrer Definition ebenfalls kopieren können muss:

$$\left|M_0\right\rangle\left|\psi_S\right\rangle \rightarrow \left|M_S\right\rangle\left|\psi_S\right\rangle\left|\psi_S\right\rangle \tag{2.9}$$

Setzen wir in die rechte Seite noch den Ausdruck (2.8) für $|\psi_S\rangle$ ein, so erhalten wir:

$$\begin{aligned} |M_0\rangle\,|\psi_S\rangle \quad &\rightarrow \quad |M_S\rangle\left(c_1\,|\psi_1\rangle + c_2\,|\psi_2\rangle\right)\left(c_1\,|\psi_1\rangle + c_2\,|\psi_2\rangle\right) \\ &= \quad c_1^2\,|M_S\rangle\,|\psi_1\rangle\,|\psi_1\rangle \\ &\quad + c_2^2\,|M_S\rangle\,|\psi_2\rangle\,|\psi_2\rangle \\ &\quad + c_1c_2\,|M_S\rangle\,|\psi_1\rangle\,|\psi_2\rangle \\ &\quad + c_2c_1\,|M_S\rangle\,|\psi_2\rangle\,|\psi_1\rangle \end{aligned} \tag{2.10}$$

Schreibt man aber $|\psi_S\rangle$ nach Gleichung (2.8) *zuerst* als Superposition und wendet für $|\psi_1\rangle$ und $|\psi_2\rangle$ die Transformationsregeln aus (2.6) und (2.7) einzeln an, so ergibt sich:

$$\begin{aligned} |M_0\rangle\,|\psi_S\rangle \quad &= \quad |M_0\rangle\left(c_1\,|\psi_1\rangle + c_2\,|\psi_2\rangle\right) \\ &= \quad c_1\,|M_0\rangle\,|\psi_1\rangle + c_2\,|M_0\rangle\,|\psi_2\rangle \\ &\rightarrow \quad c_1\,|M_1\rangle\,|\psi_1\rangle\,|\psi_1\rangle + c_2\,|M_2\rangle\,|\psi_2\rangle\,|\psi_2\rangle \end{aligned} \tag{2.11}$$

Die Ergebnisse des (selben!) Kopiervorgangs auf der rechten Seite von (2.10) und (2.11) unterscheiden sich voneinander – unabhängig davon, was die Maschinenzustände $|M_0\rangle$, $|M_1\rangle$ und $|M_2\rangle$ sind. Zur Herleitung beider Ausdrücke wurde nur die Linearität der Quantenmechanik und das Superpositionsprinzip verwendet; folglich muss also unsere Annahme falsch gewesen sein. Eine perfekte Kopiermaschine kann es nicht geben.

2.2.3 Nichtlineare Optik und spontane parametrische Fluoreszenz

In der modernen Optik spielt die *elektrische Polarisation* $\vec{P}$ eine wichtige Rolle. Sie gibt an, in welcher Richtung die Elektronen in einem nicht-leitenden Material (z. B. in einem Kristall) schwingen, wenn sie durch eine von außen einfallende elektromagnetische Welle mit dem Feldvektor $\vec{E}(\vec{x},t)$ angeregt werden. Im Allgemeinen kann die Polarisation als Reihe wie folgt geschrieben werden:

$$\vec{P}(\vec{x},t) \;=\; \varepsilon_0\left(\widetilde{\chi}^{(1)}\,\vec{E}(\vec{x},t) + \widetilde{\chi}^{(2)}\,\vec{E}^{\,2}(\vec{x},t) + \widetilde{\chi}^{(3)}\,\vec{E}^{\,3}(\vec{x},t) + \ldots\right) \tag{2.12}$$

Dabei ist ε_0 die elektrische Feldkonstante und $\widetilde{\chi}^{(i)}$ die Suszeptibilität i-ter Ordnung. Letztere wird allgemein durch einen Tensor $(n+1)$-ter Stufe dargestellt, welcher sich über die Ausnutzung von Kristallsymmetrien oft stark vereinfachen lässt. Bei einem Festkörper ist $\widetilde{\chi}^{(2)}$ betraglich um etwa 11 Zehnerpotenzen kleiner als $\widetilde{\chi}^{(1)}$; die Suszeptiblitäten höherer Ordnung sind nochmals kleiner [Hal08]. Bei niedrigen Feldstärken kann man daher die Terme ab der zweiten Ordnung vernachlässigen und man erhält eine lineare Abhängigkeit der Polarisation von der elektrischen Feldstärke:

$$\vec{P}(\vec{x},t) \;=\; \varepsilon_0\,\chi\,\vec{E}(\vec{x},t) \tag{2.13}$$

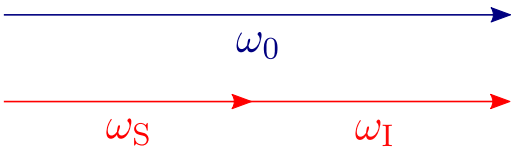


Abbildung 2.3: Bei der spontanen parametrischen Fluoreszenz (SPDC) wird ein Photon der Frequenz ω_0 in zwei Photonen mit den Frequenzen ω_S und ω_I umgewandelt.

(Da $\widetilde{\chi}^{(1)}$ als Tensor nullter Stufe ein Skalar ist, wurde die Tensor-Schreibweise weggelassen.) Dies bedeutet aber gerade, dass die Polarisation stets parallel zum elektrischen Feldvektor orientiert ist. Falls Gleichung (2.13) in guter Näherung erfüllt ist, spricht man von *linearer Optik*. Da $\vec{E}$ und $\vec{P}$ stets gleichphasig schwingen, strahlen die Elektronen im Festkörper elektromagnetische Wellen ab, welche dieselbe Frequenz wie die Einfallswelle haben – die Frequenz einer elektromagnetischen Welle beim Durchqueren eines Mediums bleibt daher unverändert.

Seit der Erfindung des Lasers im Jahr 1960 durch Theodore H. Maiman [Hec05, S. 933] stehen Quellen elektromagnetischer Strahlung zur Verfügung, mit denen sehr hohe elektrische Feldstärken der emittierten Welle erreicht werden können. Damit ist es möglich geworden, auch Effekte der *nichtlinearen Optik* zu beobachten, welche durch die Terme zweiter und höherer Ordnung in Gleichung (2.12) hervorgerufen werden. Dazu zählen z. B. Frequenzverdopplung, Summenfrequenzerzeugung und Differenzfrequenzerzeugung.

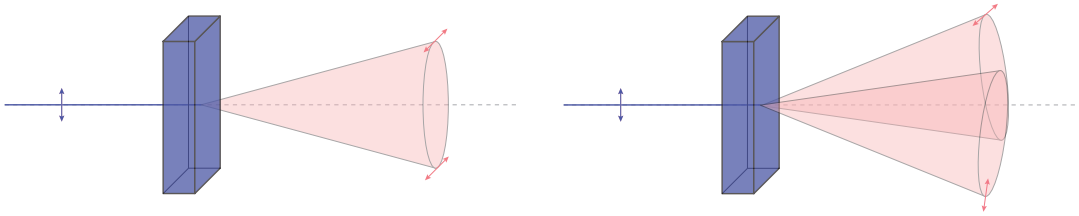
Ein weiterer nichtlinearer Effekt ist die sog. *spontane parametrische Fluoreszenz* (Englisch: ***s**pontaneous **p**arametric **d**own-**c**onversion (SPDC)*). Im Gegensatz zu den drei genannten Effekten ist sie rein quantenmechanischer Natur und kann nicht mehr klassisch erklärt werden. Strahlt man mit einer elektromagnetischen Welle der Frequenz ω_0 in einen nichtlinearen Kristall ein, so kann ein Photon der Einfallswelle in zwei Photonen mit den Frequenzen ω_S und ω_I umgewandelt werden.[6] Natürlich muss dabei die Impuls- und Energieerhaltung erfüllt sein; es gilt also:

$$\omega_0 = \omega_S + \omega_I \tag{2.14}$$

Je nach Beschaffenheit des Kristalls können die entstandenen Photonen unterschiedlich polarisiert sein. Betrachtet man das einfallende Photon als außerordentlich polarisiert, so unterscheidet man folgende Typen der SPDC [Mec07]:

- **SPDC Typ I:**
  Beide erzeugten Photonen sind ordentlich und damit parallel zueinander polarisiert. Sie werden diametral auf einem Konus emittiert, dessen Öffnungswinkel von ihrer Wellenlänge abhängt. (Abb. 2.4a)
- **SPDC Typ II:**
  Eines der beiden erzeugten Photonen ist ordentlich, das andere außerordentlich polarisiert. Sie werden auf zwei unterschiedlichen Konen emittiert, die i. A. zum Einfallsstrahl geneigt sind. (Abb. 2.4b)

[6] Die erzeugten Photonen mit den Frequenzen ω_S und ω_I werden aus historischen Gründen als *Signal* und *Idler* bezeichnet [Hut07].



(a) Typ I **(b)** Typ II

Abbildung 2.4: Polarisation und Emissionskonen der im Kristall erzeugten Photonen bei der spontanen parametrischen Fluoreszenz

Um den Effekt der spontanen parametrischen Fluoreszenz überhaupt beobachten zu können, ist es außerdem nötig, dass die *Phasenanpassungsbedingung* erfüllt ist:

$$\vec{k}_0 = \vec{k}_S + \vec{k}_I \tag{2.15}$$

Dabei stellt $\vec{k}_i$ den Wellenvektor der zugehörigen Welle dar mit $|\vec{k}_i| = n(\omega_i)\,\omega_i$; $n(\omega_i)$ ist der frequenzabhängige Brechungsindex. Die Phasenanpassung ist nötig, da andernfalls die entstehenden Sekundärwellen destruktiv miteinander interferieren würden und sich somit keine makroskopische Welle ausbilden könnte. Schließlich ist die SPDC ein spontaner Prozess, welcher an jedem Ort im Kristall auftreten kann.

Man kann eine Phasenanpassung erreichen, indem man einen doppelbrechenden Kristall verwendet und dessen optische Achse derart ausrichtet, dass die Brechungsindizes der Anpassungsbedingung genügen. In dem in dieser Arbeit beschriebenen Aufbau wird hingegen eine *Quasiphasenanpassung* vorgenommen: Dabei wird die nichtlineare Suszeptibilität zweiter Ordnung $\chi^{(2)}$ im Kristall jeweils im Abstand von einer Kohärenzlänge „umgepolt“ (Vorzeichenumkehr), sodass die entstandenen Phasendifferenzen zwischen Einfallswelle und Signal- bzw. Idlerwelle gerade ausgeglichen werden. Eine ausführliche Behandlung der Phasenanpassung findet man in [Eul09, S. 18–28].

2.3 Quantenkryptografie

Nachdem nun alle nötigen Grundlagen geschaffen wurden, soll im letzten Teil dieses Kapitels das Konzept der Quantenkryptografie vorgestellt werden. In Abschnitt 2.1.4 wurde mit dem *One-Time-Pad* ein symmetrisches Verschlüsselungsverfahren eingeführt, welches eine absolut sichere Datenübertragung ermöglicht. Für dessen Implementierung ist es nötig, dass sowohl Alice als auch Bob in Besitz des Schlüssels sind, d. h. praktisch betrachtet müssen Alice und Bob bereits vor dem eigentlichen Informationsaustausch eine Datenübermittlung starten, um ihren Schlüssel abzugleichen (Schlüsselaustausch bzw. Schlüsselverteilung). Dieser Vorgang ist klassisch nicht sicher ausführbar; die Quantenkryptografie nutzt dagegen fundamentale Prinzipien der Quantenmechanik, auf deren Basis eine abhörsichere Schlüsselverteilung erfolgen kann. Da dies im Wesentlichen die einzige Aufgabe der Quantenkryptografie ist, wird in der Fachliteratur häufig der englische Begriff *Quantum Key Distribution (QKD)* verwendet – gelegentlich findet man auch die deutsche Bezeichnung *Quanten-Schlüsselverteilung*.

Es existieren gegenwärtig zwei unterschiedliche Ansätze der *Quantum Key Distribution*, welche von verschiedenen Prinzipien der Quantenmechanik Gebrauch machen:

- **Das *BB84-Protokoll*** (1984) basiert auf dem *No Cloning*-Theorem und verwendet die Tatsache, dass ein quantenmechanischer Zustand i. A. nicht gemessen werden kann, ohne den Zustand selbst zu verändern.
- **Das *Ekert-Protokoll*** (1991) nutzt zur Schlüsselübertragung *verschränkte Quantenzustände*[7] und sichert sich über sog. *Bell-Tests* gegen Lauschangriffe ab.

Zur Realisierung der quantenkryptografischen Übertragungsstrecke wird in dieser Arbeit das BB84-Protokoll verwendet. Dieses soll daher im Folgenden ausführlich beschrieben werden.

2.3.1 Das BB84-Protokoll

Das erste QKD-Protokoll wurde im Jahr 1984 von CHARLES H. **B**ENNETT und GILLES **B**RASSARD entwickelt. Es wird nach seinen Erfindern heute als *BB84-Protokoll* bezeichnet und kann mit jedem beliebigen Zwei-Zustands-Quantensystem implementiert werden.

In dieser Arbeit wird als Zweier-Zustand die lineare Polarisation von Photonen verwendet. Diese wird entweder in der Basis $\oplus$ oder in der Basis $\otimes$ gemessen, wobei eine Messung in der ersten Basis nur das Ergebnis $\circ\!\!|$ oder $\ominus$ und eine Messung in der zweiten Basis nur das Ergebnis $\diagdown$ oder $\oslash$ liefern kann. Die hier verwendeten Symbole entsprechen in der genannten Reihenfolge den Polarisationen horizontal, vertikal, $+45\,^\circ$ zur Vertikalen und $-45\,^\circ$ zur Vertikalen. Um die verschieden polarisierten Photonen als Informationsträger nutzen zu können, ordnet man ihnen in ihrer Eigenbasis Binärwerte wie folgt zu [NO08, Kapitel 3]:

$$\begin{aligned} \oplus\text{-Basis:}\quad & 0 \mapsto \circ\!\!|, \quad 1 \mapsto \ominus \\ \otimes\text{-Basis:}\quad & 0 \mapsto \diagdown, \quad 1 \mapsto \oslash \end{aligned} \tag{2.16}$$

Als Analogon der Bits in der klassischen Informationstheorie werden die Informationsträger in der Quantenkryptografie als *Qubits* bezeichnet. Während klassische Bits nur die diskreten Werte 0 und 1 annehmen können, kann ein Qubit nach dem Superpositionsprinzip allerdings jeden beliebigen (normierten) Zustand annehmen, der eine Linearkombination der Grundzustände $|0\rangle$ und $|1\rangle$ ist:

$$\big|\psi\big\rangle \;=\; \alpha\,|0\rangle + \beta\,|1\rangle \qquad\qquad \text{mit } \alpha,\beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1 \tag{2.17}$$

Um Unklarheiten zu vermeiden, ist es wichtig, die Zustände von den Messgrößen (Observablen) klar zu unterscheiden: Ein Qubit kann zwar vor der Messung einen gemischten Superpositions*zustand* wie in (2.17) haben; eine Messung der *Observablen* wird aber *immer* den Wert 0 oder 1 liefern – nicht etwa 0,5 oder ähnliches.

[7] Quantenverschränkung ist ein aus der Quantenmechanik resultierendes Phänomen, welches ALBERT EINSTEIN, BORIS PODOSLKI und NATHAN ROSEN bereits 1935 in dem nach ihnen benannten *EPR-Paradoxon* beschrieben. Danach können zwei Teilchen, welche zu irgendeinem früheren Zeitpunkt miteinander in Wechselwirkung gestanden haben, in ihren Eigenschaften gekoppelt sein, d. h. wenn in einem Zweizustandssystem am Teilchen *A* der Zustand $|1\rangle$ gemessen wird, so kann man sicher sein, dass die Zustandsmessung des Teilchens *B* den komplementären Zustand $|0\rangle$ liefert und umgekehrt, wobei das Messergebnis der ersten Messung von vorneherein *nicht* feststeht. Mehr dazu findet man z. B. in [Zei08].

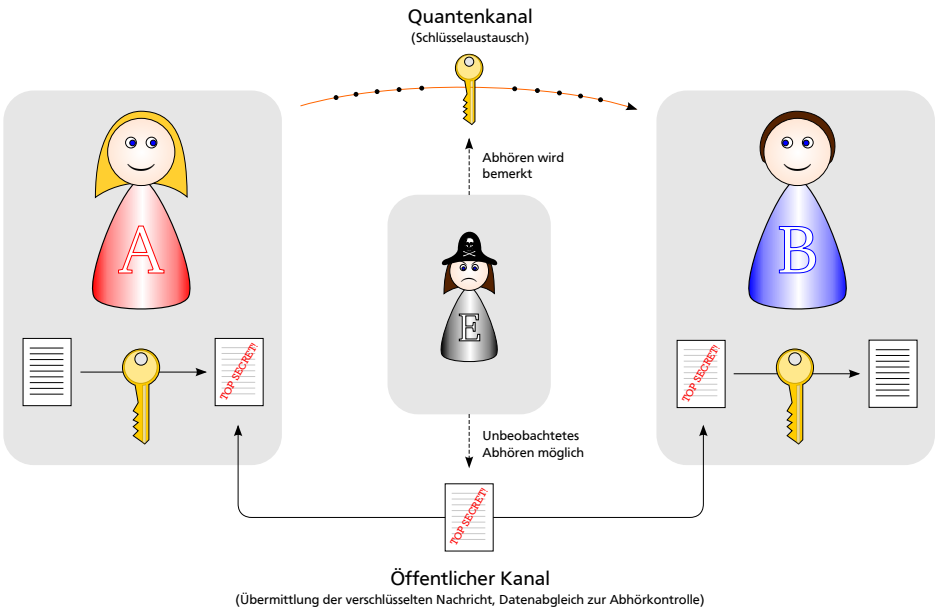


Abbildung 2.5: Schematische Darstellung der verschlüsselten Nachrichtenübermittlung beim BB84-Protokoll

Das BB84-Protokoll sieht nun vor, dass Alice und Bob durch einen Quantenkanal *und* einen klassischen (öffentlichen) Kanal miteinander verbunden sind, wobei der Quantenkanal ausschließlich zur Schlüsselübertragung und der klassische Kanal im Wesentlichen zur (kodierten) Nachrichtenübermittlung sowie zur Kontrolle von Lauschangriffen verwendet wird (Abb. 2.5). Der sichere Schlüsselaustausch über das BB84-Protokoll vollzieht sich nun in zehn Schritten wie folgt: (Die Schritte 1–6 sind in Tabelle 2.3 skizziert.)

1. Alice wählt eine zufällige Bitfolge der Länge N, welche sie an Bob übertragen möchte, beispielsweise: $K_0 = 001010110$ ($N = 9$).

2. Alice wählt N mal zufällig eine der beiden Basen aus, z. B.: $\otimes \oplus \otimes \oplus \oplus \oplus \otimes \oplus \oplus$.

3. Sie präpariert nun N Photonen derart, dass die Messung ihrer Polarisation in der in Schritt 2 jeweils gewählten Basis die Bitfolge aus Schritt 1 als Ergebnis hat, wenn man die Zuordnungen aus (2.16) verwendet. Diese Photonen sendet sie über einen Quantenkanal an Bob: $|\oslash\rangle\,|\odot\rangle\,|\oslash\rangle\,|\odot\rangle\,|\ominus\rangle\,|\odot\rangle\,|\oslash\rangle\,|\ominus\rangle\,|\odot\rangle$.

4. Bob empfängt die N Photonen in dieser Reihenfolge. Da er nicht weiß, in welcher Basis Alice die einzelnen Photonen kodiert hat, wählt er ebenfalls N mal zufällig eine der beiden Basen aus (wie Alice in Schritt 2), z. B.: $\oplus \oplus \otimes \otimes \oplus \otimes \otimes \otimes \oplus$.

5. Bob misst die Photonen in der jeweils von ihm gewählten Basis und wandelt das Ergebnis nach (2.16) wieder in eine Bitfolge um. Dieser sog. *Raw Key* stimmt natürlich nicht überall mit der Bitfolge von Alice überein: $K_\mathrm{R} = 101011100$.

6. Alice und Bob tauschen nun über einen klassischen (potenziell abhörbaren) Kanal aus, für welche Basis sie sich jeweils entschieden haben – ohne dabei das Messergebnis mitzuteilen. Stimmt ihre Basiswahl bei einem Photon überein, so können beide sicher sein, dass Bobs Bit (aus K_R) mit dem von Alice (aus K_0) identisch ist. Falls Bob aber

in einer anderen Basis als Alice gemessen hat, so unterscheidet sich das entsprechende Bit in K_0 und K_R in etwa 50 % der Fälle.

Alice und Bob streichen daher aus ihrer Bitfolge alle Bits heraus, bei denen sie eine unterschiedliche Basis gewählt haben. Die verbleibende Bitfolge wird als *Sifted Key* bezeichnet und ist bei Alice und Bob idealerweise identisch: $K_S = 01110$.

7. Bevor Alice und Bob den Schlüssel K_S zur sicheren Datenübertragung einsetzen können, müssen sie überprüfen, ob der von ihnen benutzte Quantenkanal von Eve abgehört wurde. Dies können sie feststellen, indem sie einige Bits aus dem *Sifted Key* wiederum zufällig auswählen und über den klassischen Kanal miteinander vergleichen. Liegt die Fehlerrate (genannt ***Q**uantum **B**it **E**rror **R**ate*, kurz: *QBER*) unter 14,6 %, so kann mit Sicherheit gesagt werden, dass Eve nicht genügend Information besitzt, um eine mit K_S kodierte Nachricht zu entschlüsseln [Wei03, S. 40]. In diesem Fall kann der sichere Datenaustausch mit Schritt 8 fortgesetzt werden.

   Anderenfalls muss davon ausgegangen werden, dass die Schlüsselübertragung unsicher war. Der *Sifted Key* wird dann verworfen und ein neuer Versuch wird z. B. über einen anderen Quantenkanal gestartet, wobei wieder bei Schritt 1 begonnen wird.

8. Nun sind Alice und Bob theoretisch in Besitz eines sicheren Schlüssels. In der Praxis ist allerdings eine perfekte Quantenübertragung nicht zu realisieren, weshalb die *Sifted Keys* von Alice und Bob etwas voneinander abweichen werden. Um diese Fehler aus den beiden Bitfolgen zu entfernen, wenden Alice und Bob sog. *Fehlerkorrekturprotokolle* an (vgl. Abschnitt 2.3.2).

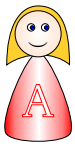
																				
Schritt	**Alice**											**Bob**							
1	0	0	1	0	1	0	1	1	0										
2	⊗	⊕	⊗	⊕	⊕	⊕	⊗	⊕	⊕										
3	$\|\oslash\rangle$	$\|\oplus\rangle$	$\|\oslash\rangle$	$\|\oplus\rangle$	$\|\ominus\rangle$	$\|\oplus\rangle$	$\|\oslash\rangle$	$\|\ominus\rangle$	$\|\oplus\rangle$		⟶	$\|\oslash\rangle$	$\|\oplus\rangle$	$\|\oslash\rangle$	$\|\oplus\rangle$	$\|\ominus\rangle$	$\|\oplus\rangle$	$\|\oslash\rangle$	$\|\ominus\rangle$	$\|\oplus\rangle$
4												⊕	⊕	⊗	⊗	⊕	⊗	⊗	⊗	⊕
5												1	0	1	0	1	1	1	0	0
6	✘	0	1	✘	1	✘	1	✘	0			✘	0	1	✘	1	✘	1	✘	0
K_S	01110										=	01110								

Tabelle 2.3: Veranschaulichung des BB84-Protokolls bis zur Erstellung des *Sifted Keys*:
Die Basen, welche Alice und Bob zufällig gleich ausgewählt haben, sind grün dargestellt; rot sind dagegen die Bits gekennzeichnet, welche Bob aufgrund seiner falschen Basiswahl rein zufällig erhalten hat. Diese werden in Schritt 6 verworfen, um den *Sifted Key* K_S zu generieren, welcher im Idealfall bei Alice und Bob identisch ist.
(Aus didaktischen Gründen ist in der Tabelle der Fall der idealen Übertragung dargestellt, bei der von außen kein Lauschangriff unternommen wurde und weder Dämpfung noch Rauschen vorliegt.)

9. Nach der Fehlerkorrektur sind Alice und Bob mit beinahe 100 %-iger Wahrscheinlichkeit in Besitz desselben geheimen Schlüssels K'_S. Um die Sicherheit ihrer Übertragung noch weiter zu erhöhen, können sie nun sog. *Privacy Amplification*-Protokolle anwenden, welche den relativen (möglichen) Informationsgewinn von Eve weiter reduzieren (vgl. [GRTZ02, S. 150]). (Informationsgewinn ist dabei natürlich auf den Schlüssel K'_S bezogen und *nicht* auf die noch zu übermittelnde Nachricht.)

10. Im letzten Schritt verfügen Alice und Bob nun über einen absolut sicheren Binärschlüssel K_F, welchen Alice verwendet, um ihre Nachricht mit der *One-Time-Pad*-Methode zu verschlüsseln und über den klassischen Kanal sicher an Bob zu übertragen.

2.3.2 Lauschangriffe, Fehlerkorrektur und Sicherheit

Um sich davon überzeugen zu können, dass das gerade erläuterte Verfahren tatsächlich absolute Sicherheit bietet, ist es nötig, die Nachrichtenübermittlung aus Eves Perspektive zu betrachten: Welche Möglichkeiten hat sie, um aus der Schlüsselübertragung Informationen zu gewinnen?

Würde Eve einfach alle oder einen großen Teil der Photonen abfangen, so würden Alice und Bob ihren Lauschangriff spätestens in Schritt 6 bemerken, da Bob wesentlich weniger Photonen empfangen hat als Alice losgeschickt hat. Die einfachste Methode des Abhörens für Eve ist daher die sog. *Intercept-Resend Attack*:

Dabei misst sie zunächst die Polarisation eines Photons in einer von ihr zufällig ausgewählten Basis und schickt dann ein neues Photon in der von ihr gemessenen Polarisation weiter. Hat sie (in etwa 50 % der Fälle) dieselbe Basis wie Alice gewählt – nehmen wir o. B. d. A. an, es sei die Basis $\oplus$ –, so stimmt der Polarisationszustand des von ihr an Bob gesandten Photons mit dem des von Alice abgeschickten überein und Eve würde nicht weiter auffallen. Hat sie aber die andere Basis $\otimes$ gewählt, so ist ihr Messergebnis in dieser Basis rein zufällig und sie wird dementsprechend ein Photon an Bob senden, welches entweder den Polarisationszustand $|\oslash\rangle$ oder $|\oslash\rangle$ besitzt. Misst Bob in der gleichen Basis wie Alice ($\oplus$), so wird er in beiden Fällen ein rein zufälliges Messergebnis in seiner Basis erhalten, sodass sein Bit in der Hälfte der Fälle nicht mit dem von Alice übereinstimmt.

Damit verursacht Eve insgesamt eine Fehlerrate (QBER) von 25 % in der Schlüsselübertragung, welche von Alice und Bob in Schritt 7 einfach festgestellt werden kann. Nun kann sich Eve aber auch andere ausgeklügelte Abhörmethoden einfallen lassen und damit QBERs erreichen, die deutlich unter 25 % liegen. Wie Christopher Fuchs et al. aber 1997 gezeigt haben [FGG+97], würde selbst ein idealer Lauschangriff stets eine QBER von etwas mehr als 14,6 % verursachen, sodass ein Schlüsselaustausch bei einer QBER kleiner diesem Wert immer als absolut sicher betrachtet werden kann.

Zum Schluss dieses Kapitels sollen nun noch die Schritte 8 und 9 des BB84-Protokolls anhand von Beispielen plausibel gemacht werden: Aufgrund der nicht zu vermeidenden Dunkelzählraten heutiger Photonendetektoren (Rauschen) und der Dämpfung des Übertragungswegs besitzen Alice und Bob in Schritt 8 leicht verschiedene *Sifted Keys*. Zur Korrektur bzw. Angleichung der *Sifted Keys* kann nun z. B. das Fehlerkorrekturprotokoll *Cascade* angewendet werden, welches 1993 von Gilles Brassard und Louis Salvail vorgeschlagen wurde [Wei03, S. 46]:

Alice und Bob teilen ihre *Sifted Keys* in Blöcke der gleichen Länge N_B auf. Sie ermitteln die Parität[8] jedes einzelnen Blocks und vergleichen diese miteinander über den klassischen Kanal. Falls die berechneten Paritäten eines Blocks nicht übereinstimmen, so wissen Alice und Bob, dass eine ungerade Anzahl an Bit-Fehlern in diesem Block stecken muss. Sie teilen diesen Block dann in kleinere Blöcke und suchen nach demselben Schema rekursiv weiter nach Fehlern, bis die Parität der kleinsten Blöcke 0 ist und damit nur noch eine gerade Anzahl an Fehlern in diesen Blöcken enthalten sein kann (möglicherweise ist es gar kein Fehler). Nachdem alle Blöcke verarbeitet wurden, permutieren Alice und Bob die Bits ihrer gegenwärtigen Bitfolge und starten dasselbe Verfahren erneut – diesmal mit einer anderen Blockgröße. Nach einigen Durchläufen dieses Verfahrens sind die korrigierten *Sifted Keys* von Alice und Bob mit an 100 % grenzender Wahrscheinlichkeit exakt identisch und können bereits als Schlüssel eines *One-Time-Pads* eingesetzt werden (sofern die QBER dies erlaubt).

Im Schritt 9 kennen Alice und Bob nun einerseits die Fehlerrate ihres nunmehr identischen Schlüssels; andererseits können sie beurteilen, wieviel Information Eve durch die Fehlerkorrektur in Schritt 8 maximal erlangen konnte. Damit sind sie in der Lage auszurechnen, wie lang der finale Schlüssel zur sicheren Übertragung maximal noch sein darf. Mithilfe von *Hash-Funktionen* kann daraus schließlich der finale Schlüssel K_F bestimmt werden, mit dem Alice und Bob dann über einen öffentlichen Kanal sicher kommunizieren können.

Eine gut verständliche weiterführende Behandlung von Lauschangriffen und Sicherheitsrisiken der *Quantum Key Distribution* findet man in der Diplomarbeit von Henning Weier [Wei03], auf dessen Ausführungen dieser Abschnitt gestützt ist.

[8] Die Parität einer Bitfolge ist 0, wenn die Quersumme der Bitfolge gerade ist; sonst ist die Parität 1. Sie ist also die Erweiterung des in der Fußnote auf Seite 15 eingeführten *XOR*-Werts auf N Bits.

3 Experiment

3.1 Aufbau des Alice-Moduls

Im Rahmen meiner Bachelor-Thesis habe ich am aktuellen *QKD*-Projekt der Arbeitsgruppe „Laser- und Quantenoptik“ an der TU Darmstadt mitgearbeitet, dessen langfristiges Ziel es ist, eine funktionsfähige quantenkryptografische Übertragungsstrecke mittels des BB84-Protokolls praktisch zu implementieren.

Nach den Ausführungen im vorangegangenen Kapitel wird dafür im Wesentlichen ein Sender-Modul (Alice) und ein Empfänger-Modul (Bob) benötigt, welche beide die Vorgaben des BB84-Protokolls erfüllen müssen. Der Bau eines Empfänger-Moduls zur Einzelphotonen-Detektion wurde im Jahr 2006 von Christoph Söller initiiert [Söl06] und im November 2008 von Daniel Rieländer erfolgreich fertiggestellt [Rie08]. Die vorliegende Arbeit beschäftigt sich nun mit dem Aufbau eines entsprechenden Sender-Moduls, das nach Abschnitt 2.3.1 für eine große Anzahl von Photonen folgende Aufgaben leisten können muss:

1. Zufällige Wahl eines Bits 0 oder 1.
2. Zufällige Wahl einer Basis $\oplus$ oder $\otimes$.
3. Erzeugung eines Photons, dessen Polarisationzustand je nach gewählter Basis
   - $|\circlearrowleft\rangle$ oder $|\circlearrowright\rangle$ ist, falls 0 als Bit gewählt wurde bzw.
   - $|\ominus\rangle$ oder $|\oslash\rangle$, falls 1 als Bit gewählt wurde.
4. Senden des so präparierten Photons über einen Quantenkanal an Bob.

Dabei ist es unerlässlich, dass Alice ein „Gedächtnis“ hat: Sie muss in der Lage sein, ihr jeweils gewähltes Bit und ihre gewählte Basis zu protokollieren, da sonst Schritt 6 des BB84-Protokolls (die Generierung eines *Sifted Keys*, siehe S. 22) nicht ausgeführt werden kann.

Die zufällige Wahl einer Basis kann z. B. mit Hilfe eines *elektro-optischen Modulators (EOM)* umgesetzt werden [Cop09, S. 24]. Unter anderem aus Kostengründen wurde sich in dieser Arbeit aber für eine andere Realisierung entschieden, welche den Vorteil hat, dass sie eine echt-zufällige Wahl trifft und keinen Zufallsgenerator benötigt, der Basen nur pseudo-zufällig auswählen kann. Diese wird im Folgenden zusammen mit der Funktionsweise des Sender-Moduls erläutert.

Der Aufbau unseres Alice-Moduls ist in Abbildung 3.1 schematisch dargestellt: Ein Laser[1] emittiert Photonen mit einer Wellenlänge von 405 nm. Im Strahlteiler BS 1 *(**b**eam**s**plitter)* werden etwa 50 % der Photonen nach rechts abgelenkt, während die anderen 50 % den Strahlteiler ungehindert passieren und dann vom Spiegel M 1 ebenfalls nach unten abgelenkt werden.

Beide Photonenstrahlen treffen nun jeweils auf einen dichroitischen Spiegel (***d**ichroic **m**irror*, DM 1 bzw. DM 2), welcher Licht der Wellenlänge 810 nm transmittiert, Licht mit

[1] *External Cavity Diode Laser (ECDL)*

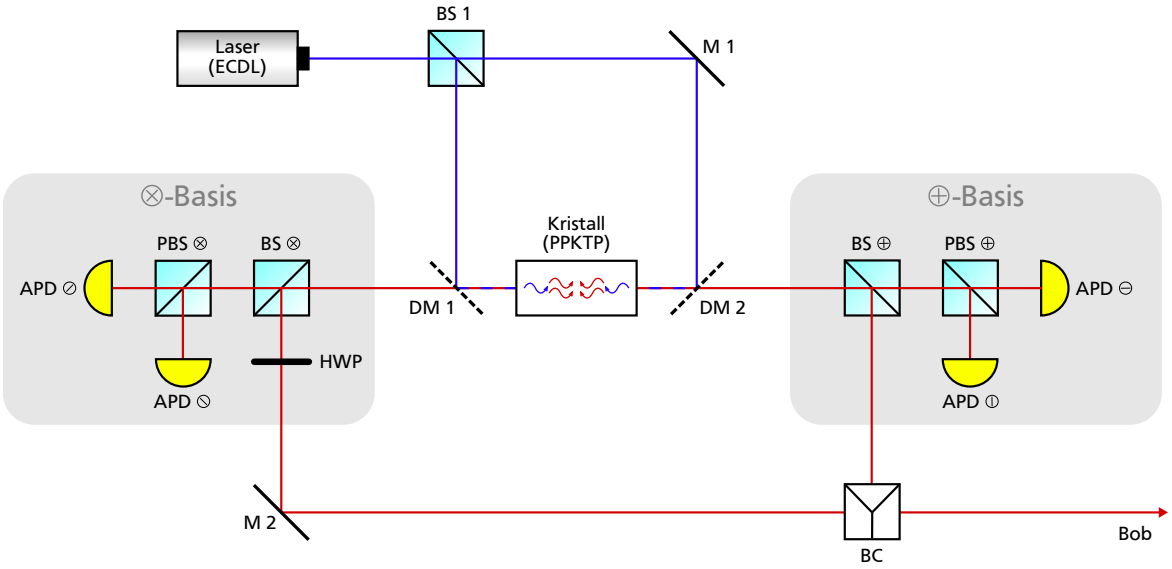


Abbildung 3.1: Schematischer Aufbau des Alice-Moduls. Faserkoppler, Linsen usw. sind der Übersichtlichkeit halber weggelassen. (In den Kristall wird mit Hilfe von 10×-Mikroskop-Objektiven eingekoppelt.)

der halben Wellenlänge 405 nm aber reflektiert. Folglich werden die von BS 1 und M 1 kommenden Strahlen von gegenüberliegenden Seiten in einen PPKTP-Kristall eingekoppelt.

In diesem Kristall findet spontane parametrische Fluoreszenz (SPDC) des Typs II statt (vgl. Abschnitt 2.2.3), sodass einige der blau-violetten Pumpphotonen (405 nm) in jeweils zwei senkrecht zueinander polarisierte infrarote Photonen umgewandelt werden, deren Wellenlängen zwar verschieden sein können, aber etwa im Bereich von 810 nm liegen. Während die nicht umgewandelten blau-violetten Photonen auf der anderen Seite des Kristalls wieder von den dichoitischen Spiegeln abgelenkt werden, können die durch SPDC erzeugten Photonen DM 1 und DM 2 passieren. Abhängig von der Seite, von welcher ihre „Mutterphotonen“ in den Kristall eingekoppelt wurden, gelangen sie nun entweder links oder rechts in einen Detektorkomplex (grau hinterlegt). Wie eingezeichnet, entspricht der linke Komplex der ⊗-Basis, der rechte Komplex dagegen der ⊕-Basis. Die Wahl der Basis wird also vom Strahlteiler BS 1 völlig zufällig getroffen – vorausgesetzt, er ist exakt gerade ausgerichtet und teilt den Strahl tatsächlich im Verhältnis 50:50. Damit ist Punkt 2 der Anforderungsliste an Alice erfüllt.

Aus Abbildung 3.1 geht hervor, dass die beiden Detektorkomplexe genau spiegelsymmetrisch aufgebaut sind; der einzige Unterschied ist die $\lambda/2$-Platte HWP (*half wave plate*), welche im ⊗-Komplex zusätzlich in den Strahlengang eingebracht wird. Mit ihr wird die Polarisation der ⊙- bzw. ⊖-polarisierten Photonen um 45 ° gedreht, sodass diese in die ⊗-Basis transformiert werden. In jedem Detektorkomplex geschieht nun folgendes (wir verwenden den rechten Komplex ⊕ als Referenz):

Ein durch SPDC entstandenes Photonenpaar mit komplementärer Polarisation erreicht den ersten Strahlteiler BS ⊕. Dieser transmittiert und reflektiert mit einer Wahrscheinlichkeit von jeweils 50 %. Während in der Hälfte der Fälle entweder beide Photonen transmittiert oder beide Photonen reflektiert werden, wird in der anderen Hälfte der Fälle entweder das ⊙-polarisierte Photon transmittiert und das ⊖-polarisierte Photon reflektiert oder umgekehrt.

Im ersten Fall sendet Alice entweder gar kein Photon an Bob (weil sie beide Photonen selbst detektiert) oder sie sendet beide Photonen an Bob, hat aber selbst kein Photon detektiert. Auf diese Weise kann also keine Information ausgetauscht werden. Im zweiten Fall kann Alice ein Photon an Bob schicken (das an BS $\oplus$ abgelenkte), während sie das andere selbst auswerten kann. Dies geschieht mit einem polarisierenden Strahlteilter PBS $\oplus$ *(**p**olarising **b**eam**s**plitter)* und zwei Einzelphotonendetektoren APD $\circleddash$ und APD $\ominus$:[2]

Ist das Photon $\circleddash$-polarisiert, so wird es von PBS $\oplus$ abgelenkt und vom Detektor APD $\circleddash$ registriert. Alice weiß dann, dass sie ein $\ominus$-polarisiertes Photon an Bob geschickt hat. Ist das Photon hingegen $\ominus$-polarisiert, so wird es von PBS $\oplus$ transmittiert und vom Detektor APD $\ominus$ registriert. Alice weiß dann, dass sie ein $\circleddash$-polarisiertes Photon an Bob geschickt hat und der Polarisationszustand des gesendeten Photons kann in beiden Fällen protokolliert werden.

Die Wahl der zufälligen Bitfolge, welche Punkt 1 der Anforderungsliste verlangt, wird also von den Strahlteilern BS $\oplus$ und BS $\otimes$ übernommen, da sie zufällig „entscheiden“, welches der beiden komplementär polarisierten Photonen sie transmittieren und welches sie reflektieren. Punkt 3 der Liste ist ebenfalls bereits implizit erfüllt, denn in diesem Aufbau werden *zuerst* zwei Photonen mit zufälliger (aber komplementärer) Polarisation erzeugt und erst durch Messung des einen wird die zugehörige Bitfolge bekannt, welche Alice über Photonen kodiert an Bob geschickt hat.

Mittels eines polarisationserhaltenden ***B**eam **C**ombiners* (BC) werden die beiden Strahlen aus der $\oplus$-Basis und der $\otimes$-Basis kombiniert und z. B. über ein Glasfaserkabel an Bob übertragen. Damit ist auch Punkt 4 der Anforderungsliste erfüllt.

3.2 Übersicht der vorgenommenen Messungen

Für eine sichere Übertragung mit dem im vorigen Abschnitt vorgestellten Alice-Modul ist es notwendig, eine möglichst große Effizienz der SPDC im Kristall zu erreichen, wobei gleichzeitig die Anzahl der *zufälligen Koinzidenzen* gering gehalten werden muss. Zufällige Koinzidenzen sind Ereignisse, bei denen innerhalb des eingestellten Koinzidenz-Zeitfensters *(Gate)* ein Photon an Bob geschickt wird und eines von Alice ausgewertet wird, wobei die beiden Photonen nicht aus demselben SPDC-Prozess stammen. Sie sind folglich nicht miteinander korreliert und tragen daher keine bzw. falsche Information.

Ein Großteil meiner Arbeit bestand deshalb darin, die SPDC-Effizienz zu optimieren. Dazu wurde zunächst überprüft, ob der verwendete Laser derart eingestellt werden kann, dass er bei konstanten Randbedingungen auf einer Wellenlänge von 405 nm im *single mode*-Betrieb emittiert. Weiterhin wurden alle in den Kristall eingearbeiteten Wellenleiter untersucht, mit dem Ziel, einen Kanal mit der größtmöglichen SPDC-Effizienz zu finden. Schließlich wurde noch ermittelt, inwieweit die SPDC-Effizienz von der Kristalltemperatur und der eingestrahlten Laserleistung abhängt.

[2] APD ist die Abkürzung für ***a**valanche **p**hoto**d**iode*, auf Deutsch: *Lawinen-Photodiode*. APDs sind Halbleiterdioden, die im Geigermodus betrieben werden. Sie stellen das Halbleiter-Analogon zu *Photomultipliern* dar. Weitere Informationen zur Funktionsweise von APDs findet man in [Cop09, S. 16].

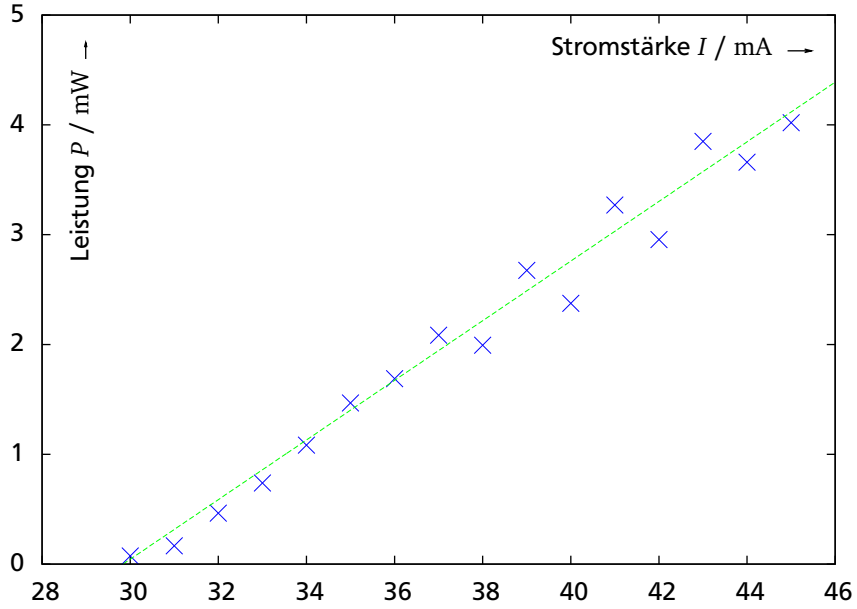


Abbildung 3.2: Leistungskennlinie des verwendeten ECDLs. Im oberen Stromstärke-Bereich sind deutliche Abweichungen vom linearen Verlauf zu erkennen – der Laser emittiert dort zum Teil multi-modisch.

3.3 Charakterisierung des verwendeten Lasers

Zu Beginn dieser Arbeit bestand die Vermutung, dass der im Versuchsaufbau verwendete Laser nicht im *single mode*-Betrieb läuft. Dies ist für eine hohe SPDC-Effizienz aber erforderlich. Der Laser (ECDL) wurde daher unter Zuhilfenahme eines *Optical Spectrum Analyzers (OSA)* zunächst exakt auf eine Emissionswellenlänge von 405 nm eingestellt und anschließend detailliert untersucht.

3.3.1 Kennlinie

Einen ersten Anhaltspunkt für die *single mode*-Eigenschaften des Lasers liefert seine Leistungskennlinie, die in Abbildung 3.2 geplottet ist. Im unteren Stromstärkebereich bis etwa 37 mA steigt die Strahlleistung wie erwartet etwa linear an. Oberhalb dieser Stromstärke kommt es aber bei jedem zweiten Messpunkt zu einem deutlichen Leistungsabfall, obwohl die Stromstärke weiter erhöht wurde. Dieses Verhalten ist nur damit zu erklären, dass der ECDL kurz vor diesen Punkten vom *single mode*-Betrieb in den *multi mode*-Betrieb springt, d. h. es bilden sich dort mehrere longitudinale Moden aus. Zur Berechnung der grünen Fitgeraden in Abbildung 3.2 wurden daher im Stromstärke-Bereich über 37 mA nur die oberen Datenpunkte herangezogen.

Durch die Rekonfiguration des Lasers auf eine Emissionswellenlänge von 405 nm (vorher: 404 nm) konnte die niedrige Laserschwelle von ca. 28 mA der Vorgängerarbeit [Cop09, S. 14] nicht mehr erreicht werden. Sie liegt nun bei etwa 30 mA.

3.3.2 Überprüfung der Singlemode-Eigenschaften

In der Hoffnung, eine oder mehrere Konfigurationen zu finden, in denen der ECDL mit Sicherheit im *single mode*-Betrieb läuft, wurde die Temperatur der Laserdiode zwischen 20,0 °C und 21,6 °C in 0,1 °C-Schritten variiert. Dafür musste zunächst der *PI*-Regler der Temperatursteuerung neu eingestellt werden, da die Einstellung einer neuen Temperatur immer mit einer nur sehr schwach gedämpften Oszillation der momentanen Dioden-Temperatur um den Soll-Wert verbunden war. Nachfolgend wurde für jede eingestellte Temperatur der Stromstärke-Bereich von der Laserschwelle bis 60 mA durchfahren. Mithilfe eines *Fabry-Pérot-Interferometers (FPI)* wurden auf dem Oszilloskop die auftretenden Moden betrachtet. Alle Stromstärke-Bereiche, in denen der ECDL nur *eine* schmalbandige Mode aufwies, wurden notiert.

Es ergaben sich pro Temperatur jeweils vier bis neun *single mode*-Bereiche, welche i. d. R. aber nur maximal 0,5 mA breit waren. Nach der Messung stellte sich heraus, dass die notierten *single mode*-Konfigurationen *nicht reproduzierbar* sind; die ermittelten Daten werden daher in dieser Arbeit nicht aufgeführt. Es bleibt anzumerken, dass der *single mode*-Betrieb des verwendeten Lasers vor jeder Messung erneut zu überprüfen ist, welche diesen voraussetzt. Für die nachfolgenden Messungen wurde eine grobe Überprüfung stets mithilfe einer Leistungsmessung des Laserstrahls vorgenommen: Dabei wurde die Stromstärke langsam erhöht, bis die Leistung plötzlich wieder abnahm (vgl. Abb. 3.2); anschließend wurde die Stromstärke wieder etwas zurückgedreht. Da bei den betrachteten Temperaturen keine wesentlichen Unterschiede in der Qualität des Laserstrahls zu erkennen waren, wurde die Laserdiode für alle folgenden Messungen konstant auf einer Temperatur von 20,9 °C gehalten (Raumtemperatur).

3.3.3 Strahlprofil

Zur Unterbindung von Transversalmoden im Laserstrahl wurde eine *single mode*-Faser bestellt, in die der Laserstrahl im späteren Aufbau eingekoppelt wurde (siehe z. B. Abb. 3.4 auf S. 32). Zur Wahl eines geeigneten Faserkopplers war es notwendig, das genaue Strahlprofil des ECDLs zu kennen. Wir haben dieses zunächst per Augenmaß mit Millimeterpapier bestimmt und ermittelten ein elliptisches Strahlprofil von etwa 4,0 mm × 2,0 mm. Eine genauere Analyse mit der *Wincam* und der Analyse-Software *Data Ray* lieferte Hauptachsen von 5,0 mm und 1,7 mm. Eine grafische Darstellung des mit der *Wincam* ermittelten Strahlprofils ist in Abbildung 3.3 zu sehen.

3.4 Untersuchung des PPKTP-Kristalls

In den im Experiment verwendeten PPKTP-Kristall sind laut Hersteller insgesamt 56 Wellenleiter *(Waveguides)* eingearbeitet, welche in acht Gruppen gegliedert sind und die Effektivität nichtlinearer optischer Effekte im Kristall deutlich steigern sollen. Sie haben einen geringfügig höheren Brechungsindex ($n_W \approx 1{,}84$) als der Kristall ($n_K \approx 1{,}83$) und bewirken somit eine Totalreflexion des im richtigen Winkelbereich eingestrahlten Lichts. (Die Numerische Apertur beträgt NA $\approx 0{,}2$.)

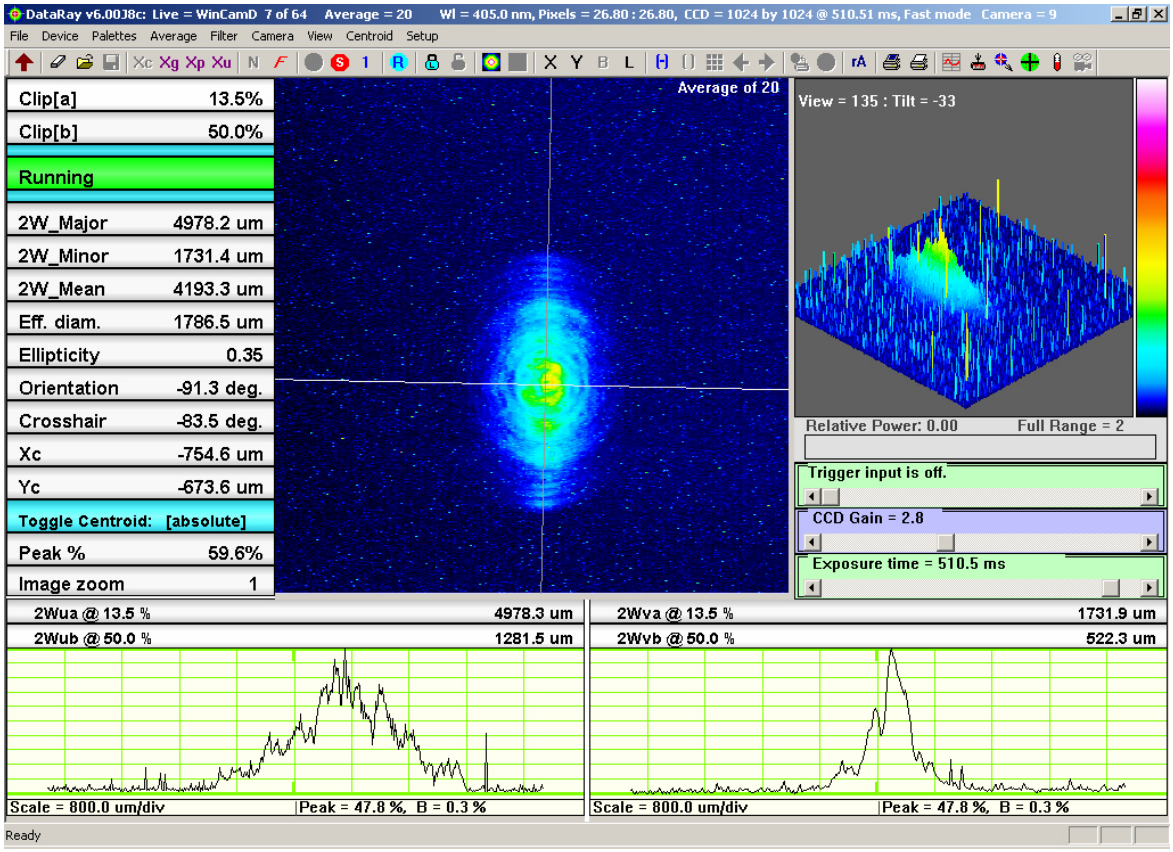


Abbildung 3.3: Screenshot des Laserstrahl-Analyse-Programms *Data Ray* mit den Messergebnissen einer Strahlanalyse mit der *Wincam*. Links unten im Bild ist der vertikale Intensitätsverlauf über die große Halbachse dargestellt, rechts daneben der horizontale Intensitätverlauf über die kleine Halbachse.

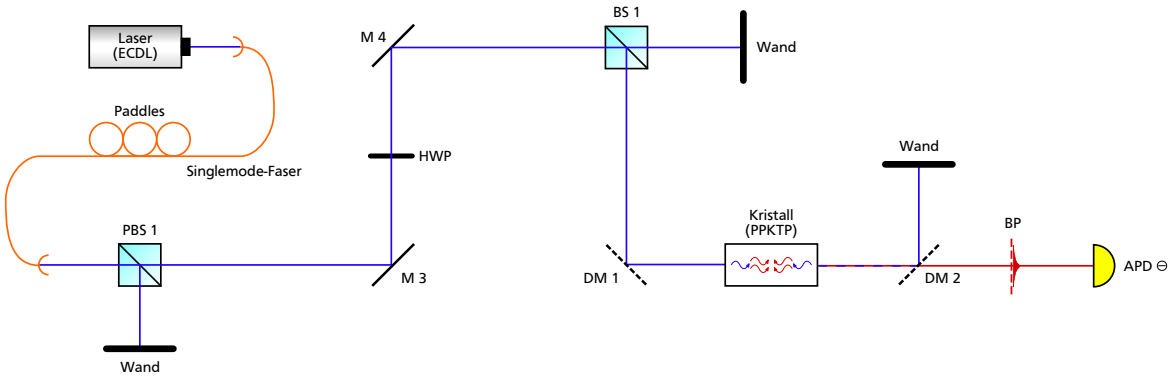


Abbildung 3.4: Versuchsaufbau zur Messung der Temperaturabhängigkeit der SPDC-Effizienz. Der Aufbau ähnelt dem aus Abb. 3.1, jedoch ist der linke Zweig des Alice-Moduls nicht aufgebaut (⊗-Komplex). Der rechte Zweig (⊕-Komplex) besteht in diesem Aufbau zunächst nur aus *einem* Photonendetektor. Da nur von einer Seite in den Kristall eingekoppelt wird, ist der Strahl hinter dem Strahlteiler BS 1 und über dem dichroitischen Spiegel DM 2 blockiert. Der polarisierende Strahlteiler PBS 1 dient dazu, die Polarisationsrichtung vorzugeben, welche mit der $\lambda/2$-Platte HWP gedreht wird. Die Bezeichnungen der Bauelemente entsprechen denen aus Abbildung 3.1.

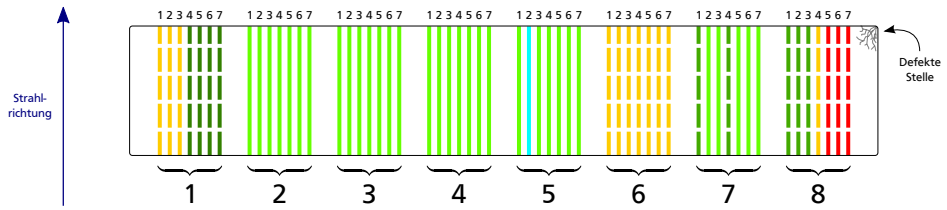


Abbildung 3.5: Nummerierung und Qualität der Wellenleiter im verwendeten PPKTP-Kristall. Grün: Durchschnittliche bis gute SPDC-Effizienz, (dunkel)grün gestrichelt: unterdurchschnittliche SPDC-Effizienz, gelb gestrichelt: sehr niedrige SPDC-Effizienz, rot gestrichelt: kein nachweisbarer SPDC-Effekt. Türkis dargestellt ist der Wellenleiter mit der maximalen SPDC-Effizienz. Die Darstellung ist nicht maßstabsgetreu: In Wirklichkeit ist der Kristall in Strahlrichtung im Verhältnis wesentlich länger.

Um festzustellen, bei welcher Kristalltemperatur ein Optimum an SPDC vorliegt und gleichzeitig diejenigen Wellenleiter im Kristall ausfindig machen zu können, welche die größte SPDC-Effizienz liefern, haben wir mehrere Messreihen mit dem Aufbau aus Abbildung 3.4 durchgeführt, bei denen wir wie folgt vorgegangen sind:

Zunächst haben wir die Wellenleiter wie in Abbildung 3.5 gezeigt durchnummeriert.[3] Die notwendige Orientierung dafür liefern eine (sichtbare) defekte Stelle des Kristall an einer Ecke sowie die etwas größeren Abstände zwischen zwei Wellenleiter-Gruppen ($d_G \approx 70\,\mu m$). (Der Abstand zwischen zwei benachbarten Wellenleitern innerhalb einer Gruppe beträgt $d_W \approx 30\,\mu m$.)

Bei einer festen Kristalltemperatur T_i wurde dann für jede Gruppe der Wellenleiter mit der größten Zählrate gesucht. Dabei wurden für die optimale Justierung jeweils etwa 15 min aufgewandt, um möglichst vergleichbare Messergebnisse zu erhalten und nicht versehentlich eine zu niedrige Zählräte zu notieren, welche durch fehlerhafte Justage zustande kam.

Sobald der Wellenleiter mit der maximalen Zählrate N_{max} gefunden war, wurde letztere zusammen mit der Wellenleiter-Nummer notiert. Dann wurde (zur späteren Normierung) die Leistung des Laserstrahls unmittelbar vor der Kristalleinkopplung gemessen, da diese über einen längeren Messzeitraum nicht konstant war. Nun wurde die $\lambda/2$-Platte im Strahlengang so lange gedreht, bis ein Minimum der Zählrate N_{min} gefunden war (ca. 45 °). Erneut wurde die Leistung vor dem Kristall gemessen und zusammen mit der Minimalzählrate ebenfalls notiert. Im Anschluss daran wurde die $\lambda/2$-Platte wieder auf den Maximalwert zurückgedreht und dieselbe Messung wurde mit der nächsten Wellenleiter-Gruppe durchgeführt. Nachdem die Daten des besten Wellenleiters in der achten Gruppe aufgenommen waren, wurde die Kristalltemperatur um etwa 5 °C erhöht und die nächste Messreihe wurde nach dem selben Schema aufgenommen.

Ein erstes experimentell direkt zugängliches Indiz für die Effizienz der SPDC eines Wellenleiters lieferte die Maximalzählrate, welche zwischen den Wellenleitern durchaus stark variierte. Nach ihr wurden jeweils die zur Messung verwendeten Wellenleiter einer Gruppe ausgewählt. Wesentlich aussagekräftiger ist aber die Differenz $N_{SPDC} = N^{(1)}_{max} - N^{(1)}_{min}$, welche die Anzahl der durch SPDC erzeugten Photonen-Counts widerspiegelt. Dabei steht $N^{(1)}_{max}$ für die auf 1 µW Eingangsleistung normierte Maximalzählrate, $N^{(1)}_{min}$ für die auf 1 µW normierte Minimalzählrate.

[3] Als Kurzschreibweise wird im Folgenden die Bezeichnung {Gruppen-Nummer}.{Wellenleiter-Nummer} verwendet. Mit 5.2 ist beispielsweise der 2. Wellenleiter in der 5. Gruppe von links gemeint.

3.4.1 Charakterisierung der Wellenleiter

Auch wenn während der Messung auffiel, dass man trotz der langen und präzisen Justage eines Wellenleiters nie ganz sicher sein kann, auch wirklich die optimale Einstellung gefunden zu haben, so ließen sich doch klare Tendenzen erkennen (vgl. auch Abb. 3.5):

- Der Hersteller des PPKTP-Kristalls hat in seinem *KTP Waveguide Coupling Manual* bereits eingeräumt:

  > *The first and last few guides in groups 1 and 8, respectively, can be lost during the fabrication process.*

  Diesen Sachverhalt konnten wir bestätigen: Einerseits wiesen alle Wellenleiter der ersten und achten Gruppe insgesamt eine unterdurchschnittliche SPDC-Effizienz auf (in der Grafik dunkelgrün gestrichelt dargestellt). Andererseits wurden die Wellenleiter in beiden Gruppen zum Rand hin immer schwächer; die letzten drei Wellenkanäle der achten Gruppe waren gar nicht mehr sichtbar und es konnte keine vom Untergrund verschiedene Zählrate festgestellt werden (rot gestrichelt dargestellt).

- Alle Wellenleiter der sechsten Gruppe waren nur sehr schwach zu sehen und wiesen bei fast jeder Temperatur die niedrigste Zählrate auf (gelb gestrichelt dargestellt). Auch die Zahl N_{SPDC} war bei den Wellenleitern in dieser Gruppe stets weit unterdurchschnittlich.

- Die meisten anderen Wellenleiter wiesen im Mittel eine vergleichbare Zählrate und SPDC-Effizienz auf (hellgrün durchgezogene Linien), wobei die Wellenleiter der vierten und fünften Gruppe i. d. R. die besten Resultate lieferten.

- Als bester Wellenleiter konnte eindeutig der zweite Wellenleiter in der fünften Gruppe identifiziert werden (türkis hervorgehoben). Er lieferte mit einer Ausnahme bei *jeder* Temperatur die größte Zahl an SPDC-Photonen-Counts N_{SPDC} bei vergleichsweise hohen Maximalzählraten N_{max}. Es wird daher an dieser Stelle klar empfohlen, diesen Wellenleiter zur Erzeugung von SPDC-Photonen zu verwenden.

Für zukünftige Arbeiten mit dem Kristall soll hier noch eine Rangfolge der fünf besten Wellenleiter gegeben werden (N_{SPDC} maximal):

1. – Gruppe 5, Wellenleiter 2
2. – Gruppe 4, Wellenleiter 7
3. – Gruppe 4, Wellenleiter 2
4. – Gruppe 3, Wellenleiter 7
5. – Gruppe 7, Wellenleiter 7

3.4.2 Temperaturabhängigkeit der SPDC

Eine allgemeingültige Aussage über die Abhängigkeit der SPDC-Effizienz von der Kristall-Temperatur fällt etwas schwer, da einerseits – wie bereits bemerkt – für jeden Wellenleiter eine erneute Justage erforderlich war, welche nicht notwendigerweise immer optimal durchgeführt wurde. Andererseits wiesen aber auch die einzelnen Wellenleiter unterschiedliche Temperatur-Abhängigkeiten auf.

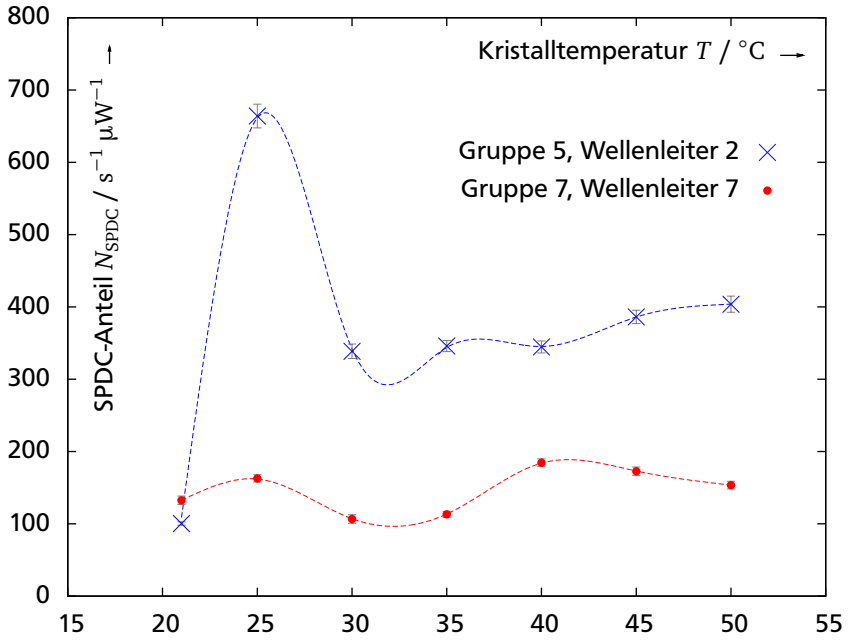


Abbildung 3.6: Temperaturabhängigkeit der auf 1 µW normierten SPDC-Photonen-Zählrate N_{SPDC} für zwei verschiedene Wellenleiter. Die Normierung ist sinnvoll, da die Abhängigkeit zwischen Pumpleistung und SPDC-Zählrate linear ist (vgl. Abschnitt 3.4.3).

Als Beispiel sind in Abbildung 3.6 die Temperatur-Kurven zweier Wellenleiter dargestellt. Aufgetragen sind jeweils die SPDC-Photonen-Counts N_{SPDC}, d. h. die Differenz zwischen minimaler und maximaler Zählrate beim Drehen der $\lambda/2$-Platte. Der besseren Sichtbarkeit halber sind die Datenpunkte jedes Wellenleiters jeweils durch *Splines* miteinander verbunden. Dies sind Funktionen, welche stückweise aus Polynomen zusammengesetzt sind und spezielle Anforderungen (wie etwas die stetige Differenzierbarkeit an den Datenpunkten) erfüllen. Aufgrund des verhältnismäßig großen Abstands der Messpunkte kann nicht davon ausgegangen werden, dass die wahre Temperatur-Kurve tatsächlich diesem Verlauf folgt.

Die Plots der beiden Wellenleiter scheinen zunächst wenig Gemeinsamkeiten zu haben. Es fällt jedoch auf, dass beide Kurven ein Maximum bei etwa 25 °C aufweisen und ein Minimum zwischen 30 °C und 35 °C. Diese Extrema fallen jedoch beim Wellenleiter 7.7 wesentlich weniger deutlich aus und könnten dort auch zufällig aufgrund nicht-perfekter Justage entstanden sein.

Abbildung 3.7 legt aber nahe, dass dieses Verhalten im Wesentlichen nicht-statistischer Natur ist und dem PPKTP-Kristall als ganzheitliche Eigenschaft zugeschrieben werden kann: Aufgetragen über der Kristalltemperatur ist die Größe $\langle N_{\mathrm{SPDC}} \rangle$, welche aus der Mittelung aller Messungen der Größe N_{SPDC} bei einer Temperatur hervorgeht (blau markiert):

$$\langle N_{\mathrm{SPDC}} \rangle = \frac{1}{8} \sum_{j=1}^{8} N_{\mathrm{SPDC},\,j} \tag{3.1}$$

Dabei bezeichnet $N_{\mathrm{SPDC},\,j}$ die SPDC-Photonen-Counts des für die jeweilige Temperatur besten Wellenleiters der Gruppe j. Da – wie in Abbildung 3.6 gezeigt – der Wellenleiter 5.2 ein extremes Maximum bei einer Temperatur von 25 °C aufweist, welches in dieser Ausprägung

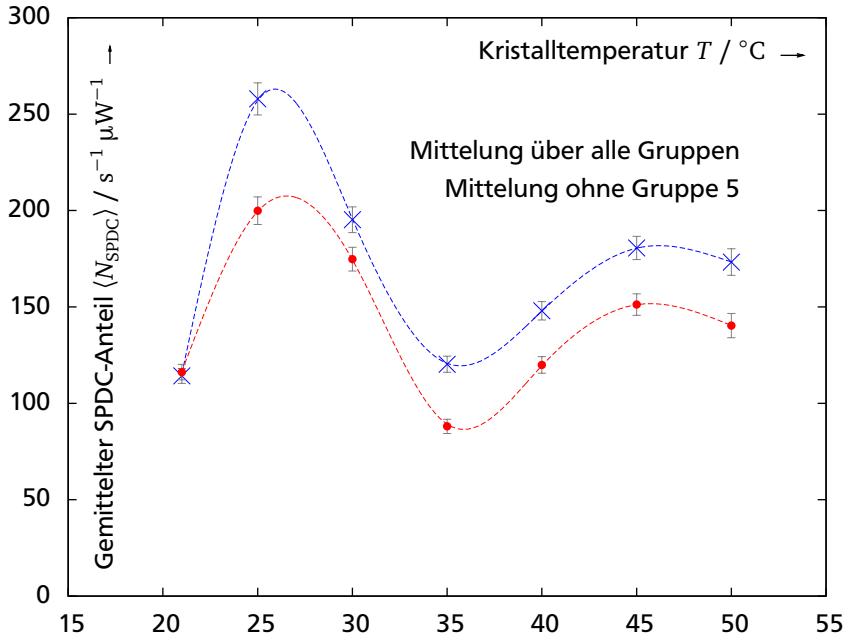


Abbildung 3.7: Temperaturabhängigkeit der mittleren SPDC-Photonen-Zählrate. Zur Mittelung wurde jeweils ein Wellenleiter aus jeder Gruppe verwendet (vgl. Gleichung 3.1).

bei keinem anderen Wellenleiter vorlag, wurde außerdem eine Mittelung ohne diesen Wellenleiter vorgenommen. Die berechneten Werte sind in Abbildung 3.7 rot dargestellt.

In jedem Fall tritt bei etwa 25 °C ein globales Maximum der SPDC-Photonen-Zählrate auf, wie bereits bei den beiden Einzelmessungen der Wellenleiter 5.2 und 7.7. Bei Raumtemperatur (21 °C) und bei etwa 35 °C wird die Zählrate im Schnitt minimal. Ein weiteres, etwas weniger ausgeprägtes Maximum tritt bei Temperaturen um 45 °C auf. Zur effizienten Erzeugung von SPDC-Photonen mit dem verwendeten PPKTP-Kristall sollte daher nach Möglichkeit der Bereich zwischen 30 °C und 40 °C, sowie Temperaturen unterhalb von 23 °C gemieden werden. Je nach Wellenleiter scheint eine Einkopplung bei 25 °C oder 45 °C sinnvoll zu sein.

Koinzidenz-Experiment zur Temperaturabhängigkeit

Nach der Evaluation dieser Messung wurde im nächsten Schritt der polarisierende Strahlteiler PBS⊕ und der Photonendetektor APD⏀ wie in Abbildung 3.8 eingebaut. Mit der in [Eul09, S. 35] beschriebenen Zählelektronik konnten so Koinzidenz-Ereignisse gemessen werden. Das *Gate* wurde auf 5 ns eingestellt, sodass ein in APD⊖ und ein in APD⏀ registriertes Signal immer dann als Koinzidenz gezählt wurde, wenn der zeitliche Abstand zwischen diesen Ereignissen innerhalb eines 5 ns-Intervalls lag.

Da sich bei den vorigen Untersuchungen der Wellenleiter 5.2 als zur Produktion von SPDC-Photonen am besten geeignet herausgestellt hat (vgl. Abschnitt 3.4.1), wurde dieser verwendet, um erneut eine Messung der Temperaturabhängigkeit vorzunehmen. Diesmal wurde statt der Größe N_{SPDC} die Anzahl der registrierten Koinzidenzen in einem Zeitintervall von 20 s aufgenommen. Je Temperatur wurden drei Messungen durchgeführt, um eine Abschätzung für den Fehler zu erhalten, anschließend wurde der Mittelwert gebildet und auf

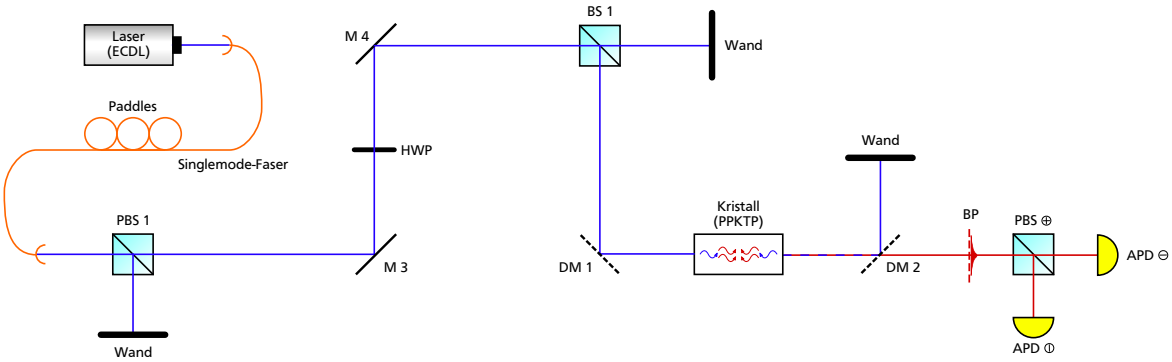


Abbildung 3.8: Versuchsaufbau zur Messung SPDC-Koinzidenzen. Gegenüber dem Aufbau aus Abb. 3.4 wurde nur der rechte Teil verändert: Hinter den Bandpassfilter BP wurde der Strahlteiler PBS ⊕ und der Einzelphotonenzähler APD ⊘ eingebaut.

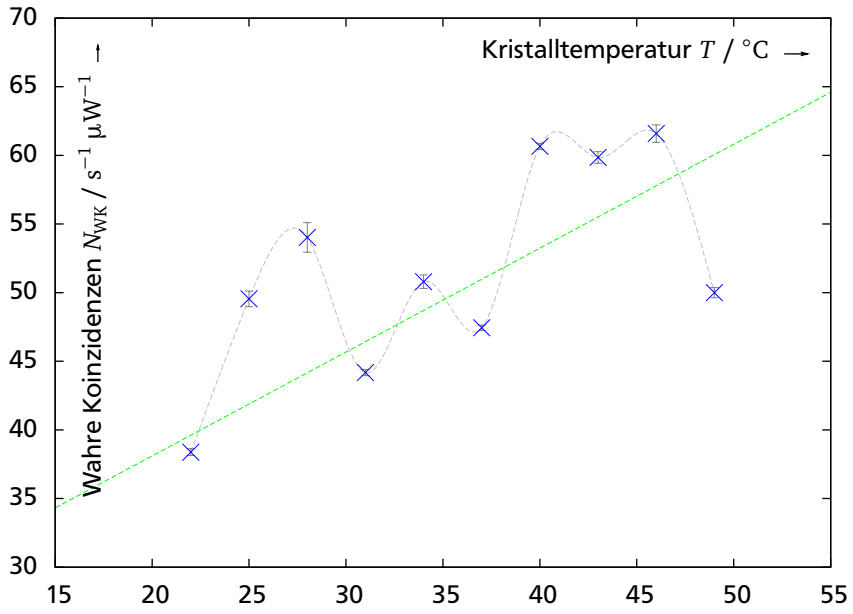


Abbildung 3.9: Temperaturabhängigkeit der SPDC-Koinzidenzen: Die Maxima sind etwa bei denselben Temperaturen wie in den Abb. 3.6 und 3.7 zu finden – die starken Schwankungen oberhalb von 30 °C stehen aber im Widerspruch zu den vorigen Messungen.

eine Sekunde sowie auf 1 µW Einstrahlungsleistung normiert. Das Temperaturintervall der Messpunkte wurde auf $\Delta T = 3\,°C$ verkleinert, um eine größere Datenauflösung zu erreichen.

Das Ergebnis der Messreihe zeigt Abbildung 3.9. Auch hier wurden die Datenpunkte durch Splines miteinander verbunden; zur Verdeutlichung der insgesamt steigenden Tendenz bei höheren Temperaturen wurde außerdem eine Gerade angefittet, die aber weit außerhalb der Fehlerschranken der Messpunkte verläuft. Zwar konnte die extrem hohe SPDC-Effizienz der vorigen Messung (Abb. 3.6) bei 25 °C nicht mehr erreicht werden. Dennoch konnte auch mit dieser Messung verifiziert werden, dass der SPDC-Effekt bei Temperaturen um 25 °C und in einem Bereich um 45 °C besonders häufig stattfindet. Es ist allerdings verwunderlich, dass der Verlauf der Koinzidenz-Messung insgesamt doch erheblich von dem Verlauf abweicht, welcher durch die Messmethode mit der $\lambda/2$-Platte ermittelt wurde. Während die Kurve des Wellenleiters 5.2 in Abbildung 3.6 oberhalb von 30 °C mit beinahe unveränderter SPDC-Zählrate auf einem Plateau verläuft, schwanken die gemessenen Koinzidenzen in Abbildung 3.9 deutlich.

Die Ursache dieser starken Unterschiede kann nicht eindeutig bestimmt werden. Möglicherweise hat jedoch eine fehlerhafte Einkopplung in die beiden APD-Koppler zu den Schwankungen beigetragen: Durch den verwendeten dichroitischen Spiegel DM 2 ist der Strahl ab dieser Position unsichtbar. Ungünstigerweise verändert der Bandpassfilter BP – wie später noch genauer beschrieben wird (Abschnitt 3.5) – den Strahlengang; die Ausrichtung der Faserkoppler kann also nicht durch kurzzeitiges Entfernen des Spiegels DM 2 aus dem Strahlengang mit Hilfe der CCD-Kamera voreingestellt werden. Da bei jeder Messung nun *zwei* Faserkoppler „blind“ neu einjustiert werden mussten, ist die Wahrscheinlichkeit höher, dass am gesamten System eine Fehljustage verursacht wurde. Die Experimentatoren gehen jedoch davon aus, dass eine mögliche Abweichung durch Fehljustage nicht in dem beschriebenen Ausmaß auftreten würde.

3.4.3 Leistungsabhängigkeit der SPDC

Zur Untersuchung der Leistungsabhängigkeit der SPDC-Effizienz wurde eine Kristalltemperatur von 46 °C eingestellt. Nach Abbildung 3.9 ist bei dieser Temperatur die SPDC-Effizienz beim Wellenleiter 5.2 am größten. Wieder wurden in drei unabhängigen Messungen (mit Bandpassfilter) die Koinzidenzen in einem Zeitintervall von 20 s bestimmt, gemittelt und auf eine Sekunde normiert. Die Leistung wurde in Schritten von etwa 30 µW erhöht.

Wie Abbildung 3.10 zeigt, besteht in guter Näherung ein linearer Zusammenhang zwischen der Laserstrahl-Leistung und der SPDC-Effizienz. Einen solchen Zusammenhang hat bereits Sabine Euler in ihrer Arbeit gefunden [Eul09, S. 45].

3.4.4 Zufällige Koinzidenzen

Bei allen in diesem Kapitel beschriebenen Koinzidenz-Experimenten lag die Zahl der zufälligen Koinzidenzen auf einem erfreulich niedrigen Niveau. Der Anteil der zufälligen Koinzidenzen an den Gesamtkoinzidenzen war nie größer als 2 %. Damit ist eine wesentliche Anforderung an die Sicherheit des Schlüsselaustauschs gut erfüllt. (In den Abbildungen 3.9 und 3.10 sind jeweils die *wahren* Koinzidenzen aufgetragen, welche sich durch Subtraktion der zufälligen Koinzidenzen von den Gesamtkoinzidenzen ergeben: $N_{\mathrm{WK}} = N_{\mathrm{GK}} - N_{\mathrm{ZK}}$.)

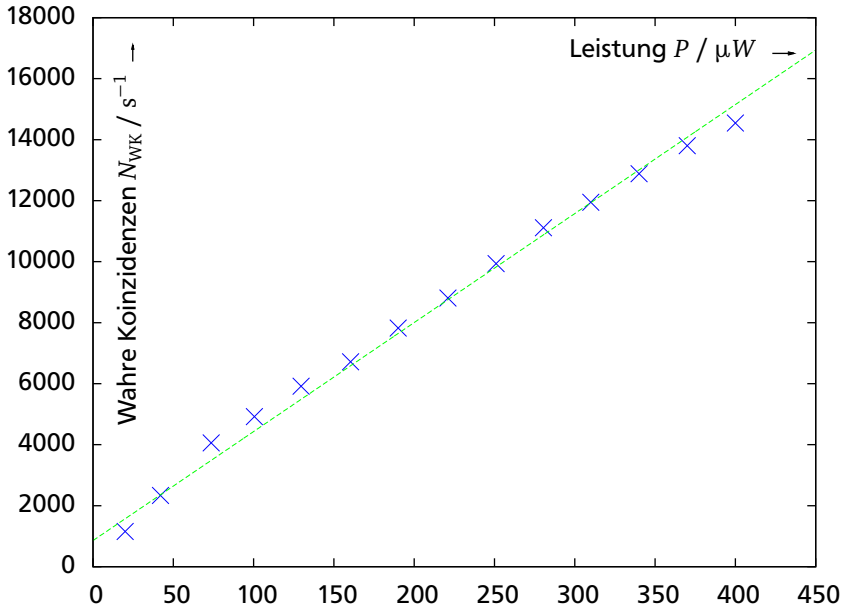


Abbildung 3.10: Leistungsabhängigkeit der SPDC-Koinzidenzen: Wie die Fitgerade verdeutlicht, existiert in guter Näherung ein linearer Zusammenhang zwischen der Pumpleistung und den auftretenden Koinzidenzen.

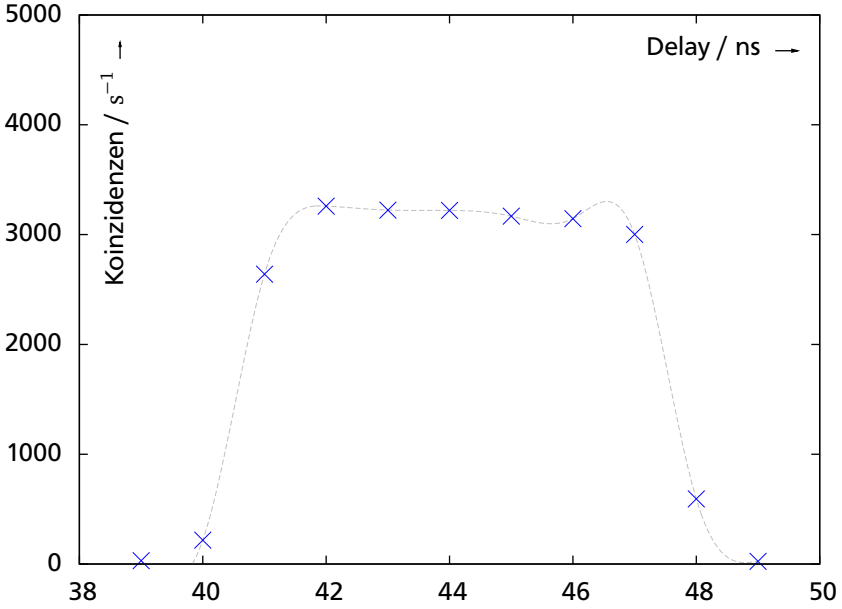


Abbildung 3.11: Delay-Plateau der Koinzidenzmessung: Das *Gate* ist mit einer Breite von 7 s etwas größer als vom Messgerät angezeigt wird.

3.5 Bemerkungen zur Messelektronik und zum Versuchsaufbau

Es wurde bereits erwähnt, dass in den Koinzidenz-Experimenten nach Einstellung ein *Gate* von 5 ns geöffnet wurde, wenn vom ersten APD ein Signal registriert wurde. Da die Verbindungskabel zwischen den einzelnen Kanälen der Zählelektronik unterschiedlich lang sind, musste dieses Signal um eine kurze Zeitspanne verzögert werden *(Delay)*.

Um das geeignete *Delay* zu finden, wurde das Signal eines einzigen APDs aufgeteilt und über dieselben Kabel an den Trigger-Eingang und den Zähleingang des Koinzidenz-Messgeräts gelegt. Das *Delay* wurde dann in Schritten von 1 ns solange erhöht, bis Koinzidenzen registriert wurden. Ab dieser *Delay*-Einstellung sollte sich eigentlich ein Plateau mit der Breite des *Gates* von 5 ns ergeben, auf dem etwa gleichviele Koinzidenzen angezeigt werden. Wie der Plot in Abbildung 3.11 zeigt, ist die tatsächliche Breite des Plateaus mit ∼7 ns etwas größer. Das vom Messgerät verwendete *Gate* scheint in Wirklichkeit also etwas größer zu sein als die Anzeige impliziert. Ein solches Verhalten wurde auch bereits in Vorgänger-Arbeiten entdeckt [Wal07, Eul09].

Des Weiteren fiel erneut auf, dass die beiden verwendeten APDs unterschiedlich gut Photonen detektieren. Einerseits ist die Dunkelzählrate des APDs mit der Modellbezeichnung AQR-14-FC stets um etwa 25 % größer als die des APDs mit der Modellbezeichnung AQR-13-FC. Zur genaueren Untersuchung der Unterschiede wurden bei einer festen Pumpleistung folgende Zählraten gemessen:

p-polariertes Licht (AQR-13-FC)	s-polarisiertes Licht (AQR-14-FC)	Koinzidenzen
35000 ± 1000	120000 ± 1000	3000 ± 100

Nach dieser Messung wurden die Fasern zwischen den s- bzw. p-Faserkopplern und den APDs jeweils mit dem anderen APD verbunden. Bei gleicher Pumpleistung und unveränderten Versuchsbedingungen wurden erneut die Zählraten bestimmt:

p-polariertes Licht (AQR-14-FC)	s-polarisiertes Licht (AQR-13-FC)	Koinzidenzen
53000 ± 1000	86000 ± 1000	3100 ± 10

Eigentlich hätte jeder der APDs nun etwa die Zählrate messen sollen, welche zuvor der jeweils andere APD registriert hat. Offensichtlich ist dies aber nicht der Fall: Beim p-polarisierten Licht zählt der APD AQR-14-FC etwa 1,5 mal so viele Photonen wie der APD AQR-13-FC; beim s-polarisierten Licht registriert er rund 40 % mehr Photonen-Counts. Um eine gleich hohe Ansprechwahrscheinlichkeit zu garantieren, wäre es daher hilfreich, zur Einzelphotonendetektion überall dasselbe Modell zu verwenden.

Abschließend bleibt noch die experimentell wichtige Bemerkung, dass der im Versuchsaufbau verwendete Bandpassfilter (810BP10) offensichtlich den Strahlengang verändert. Die durch ihn verursachte Ablenkung ist dabei abhängig von seiner Orientierung. Um mit dem Bandpassfilter überhaupt noch Koinzidenzen registrieren zu können, wurde dieser daher in einen Spiegelhalter eingebaut, wodurch nun eine Verkippung bezüglich aller drei Raumachsen möglich ist.

4 Zusammenfassung und Ausblick

In dieser Arbeit wurde die Grundidee des sicheren symmetrischen Schlüsselaustauschs über das BB84-Protokoll erläutert. Der Aufbau eines Sender-Moduls zur praktischen Implementierung dieses Protokolls wurde vorangetrieben und es wurde versucht, die Effizienz der spontanen parametrischen Fluoreszenz im dafür verwendeten PPKTP-Kristall zu steigern.

Es konnte eine grobe Temperaturabhängigkeit der SPDC-Effizienz nachgewiesen werden; außerdem wurde der Wellenleiter ermittelt, welcher den SPDC-Effekt im Kristall am intensivsten verstärkt. Mit diesen Erkenntnissen ist es nun möglich, die Versuchsparameter derart einzustellen, dass die mit dem beschriebenen Aufbau maximal mögliche Koinzidenzrate erreicht werden kann.

Als nächster Schritt sollte versucht werden, statt der beiden APDs das bereits fertiggestellte Bob-Modul zur Detektion der Koinzidenzen zu verwenden. Ein erster Versuch in dieser Richtung wurde von den Experimentatoren bereits unternommen, blieb aber erfolglos. Ein wesentliches Problem scheint die Strahlbreite zu sein – im Bob-Modul kommen wesentlich kleinere Optiken zum Einsatz als im beschriebenen Versuchsaufbau.[1] Dieses Problem könnte mit dem Einbau eines Teleskops gelöst werden.

Im Folgenden kann dann der Aufbau des gesamten Alice-Moduls, wie in Abbildung 3.1 gezeigt, vervollständigt werden. Eine Schwierigkeit wird hierbei darin bestehen, mit dem Laserstrahl von beiden Seiten gleichzeitig in den Kristall einzukoppeln. Außerdem müssen vier APDs betrieben werden, deren zugehörige Faserkoppler allesamt präzise einjustiert werden müssen. Berücksichtigt man, dass die Einkopplung des Laserstrahls in die *single mode*-Faser täglich neu justiert werden muss, so ist zu erwarten, dass der resultierende Aufbau recht instabil sein wird. Eine Verbesserung dieser Situation könnte durch die Inbetriebnahme der im Labor neu installierten Klimaanlage erfolgen.

[1] Während der Strahldurchmesser hinter dem Kristall etwa 7 mm beträgt, haben die im Bob-Modul verbauten APDs nur eine Detektionsfläche mit einem Durchmesser von 0,5 mm.

Literaturverzeichnis

[Beu05] Beutelspacher, Albrecht: *Kryptologie*. Vieweg+Teubner, 2005

[Cop09] Cop, Christian: *Erzeugung von Photonenpaaren durch SPDC in einem Wellenleiter eines PPKTP*, Technische Universität Darmstadt, Bachelor Thesis, 2009

[DH76] Diffie, Whitfield; Hellman, Martin E.: *New Directions in Cryptography*. 1976

[Eul09] Euler, Sabine: *Arbeit an einer Zweiphotonenquelle*, Technische Universität Darmstadt, Wissenschaftliche Hausarbeit, 2009

[FGG+97] Fuchs, Christopher A.; Gisin, Nicolas; Grifftiths, Robert B.; Niu, Chi-Sheng; Peres, Asher: Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy. In: *Physical Review* 56 (1997), S. 1163–1172

[GRTZ02] Gisin, Nicolas; Ribordy, Grégoire; Tittel, Wolfgang; Zbinden, Hugo: Quantum cryptography. In: *Reviews of modern Physics* 74 (2002), S. 145 – 195

[Hal08] Halfmann, Thomas: *Optics*. Technische Universität Darmstadt, Lecture Notes, 2008

[Hec05] Hecht, Eugene: *Optik*. 4. Auflage. Oldenbourg Wissenschaftsverlag, 2005 (3-486-27359-0)

[Hof08] Hofmeister, Matthias: *Quantum Computing verstehen*. 1. Auflage. Vieweg, 2008 (3-528-05921-4)

[Hut07] Huther, Lutz: *Photonenkorrelation bei der Spontanen Parametrischen Konversion*, Technische Universität Darmstadt, Bachelor Thesis, 2007

[KM08] Kaijser, Per; Markwitz, Wernhard: Quantenphysik und die Zukunft der Kryptographie. In: *Datenschutz und Datensicherheit* 32 (2008), S. 396–399

[Knu98] Knudsen, Jonathan: *Java Cryptography*. O'Reilly, 1998 (1-56592-402-9). `http://proquest.safaribooksonline.com/1565924029/ch00-1-fm2xml`

[Mec07] Mech, Alexandra: *Tests der Bellschen Ungleichung basierend auf spontaner parametrischer Konversion*, Technische Universität Darmstadt, Diplomarbeit, 2007

[NO08] Nakahara, Mikio; Ohmi, Tetsuo: *Quantum Comuting - From Linear Algebra to Physical Realizations*. Taylor & Francis Group, 2008 (978-0-7503-0983-7)

[Pet06] Petermann, Christian: *Erzeugung polarisationsverschränkter Photonen durch Spontaneous Parametric Down Conversion (SPDC)*, Technische Universität Darmstadt, Diplomarbeit, 2006

[Rie08] Rieländer, Daniel: *Aufbau eines Bob-Moduls für eine Heralded-Photonenquelle*, Technische Universität Darmstadt, Bachelor Thesis, 2008

[Rot09] ROTH, Robert: *Theoretische Physik II – Quantenmechanik*. Technische Universität Darmstadt, Vorlesungszusammenfassung, 2009

[RSA78] RIVEST, Ronald L.; SHAMIR, Adi; ADLEMAN, Leonard: *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. 1978

[Ser06] SERGIENKO, Alexander V.: *Quantum communications and cryptography*. Taylor & Francis Group, 2006 (0-8493-3684-8)

[Sha94] SHANKAR, Ramamurti: *Principles of Quantum Mechanics*. 2. Auflage. Springer Science+Business Media, 1994 (0-306-44790-8)

[Söl06] SÖLLER, Christoph: *Einzelphotonendetektion und Korrelationen bei der Spontaneous Parametric Down Conversion*, Technische Universität Darmstadt, Diplomarbeit, 2006

[Wal07] WALK, Stefan: *Photonenkorrelation bei der spontanen parametrischen Konversion*, Technische Universität Darmstadt, Diplomarbeit, 2007

[Wei03] WEIER, Henning: *Experimental Quantum Cryptography*, Technische Universität München, Diplomarbeit, 2003

[WZ82] WOOTTERS, William K.; ZUREK, Wojciech: A single quantum cannot be cloned. In: *Nature* 299 (1982), S. 802–803

[Zei08] ZEILINGER, Anton: Die Wirklichkeit der Quanten. In: *Spektrum der Wissenschaft* Ausgabe 11/08 (2008), S. 54–63

Danksagung

Ich bedanke mich natürlich bei allen netten Menschen, die mich während der Arbeit an dieser Bachelor-Thesis unterstützt haben. Herrn Prof. Walther danke ich insbesondere für das in mich gesteckte Vertrauen, welches ich bereits seit meinem ersten Studiumstag erfahren habe.

Ein ganz großes Dankeschön geht an meine Eltern, die meine studiumstechnischen Achterbahnfahrten in den letzten Jahren bemerkenswerterweise ausgehalten haben und von denen ich weiß, dass sie immer für mich da sind, falls mal irgendetwas schief laufen sollte (passiert ja bei mir häufiger mal… ☺).

Ebenso geht mein Dank an Michael Beier, welcher nicht nur alle Messungen mit mir zusammen durchgeführt und mir eine gute Einführung in das Projekt gegeben hat, sondern darüber hinaus mit seiner netten Art für viel Abwechslung und Spaß in der Dunkelkammer gesorgt hat. Zahlreiche Verbesserungsvorschläge von ihm haben dieser Arbeit den letzten Schliff gegeben. Bei Mathias Sinther möchte ich mich für die herzliche Offenheit und das Korrekturlesen dieser Arbeit bedanken.

Dann bedanke ich mich beim Exzenter-Schlüssel von *Schäfter+Kirchhoff*, dass er uns nach stundenlangen nervenaufreibenden und erfolglosen Messungen doch noch die zehnfache Zählrate gezaubert hat, sowie bei *Howard*, ohne den wir den Laserstrahl nicht hätten gerade ausrichten können. Weiterhin geht ein Dankeschön an den *Bingo-Ingo* von youFM fürs Aufmuntern im tiefen Dunkel, genauso an *Lady Gaga* und die Kollegen von *Carglass* (die, die reparieren und austauschen).

Zu guter Letzt geht ein dickes Dankeschön an die Crew, die freiwillig während der Bachelor-Thesis mit mir zu Mittag gegessen und gute Laune gemacht hat, sowie an meine großartige WG im alten Polizeipräsidium, die ich in Singapur sehr vermissen werde. Es war ein riesen Spaß, Jungs und Mädels!

Vielleicht sollte ich an dieser Stelle auch noch alle meine Freunde grüßen und zur Sicherheit überhaupt alle, die mich kennen… ich wünsche mir dazu den Song *Human* von den *Killers*, falls ihr den da habt. Ach – und Niko: Danke schonmal im Voraus fürs Getränke holen! ☺