QKD via BB84

Rekonstruktion und Optimierung eines Versuchs
für das Fortgeschrittenenpraktikum

BACHELORARBEIT

zur Erlangung des akademischen Grades
Bachelor of Science (B. Sc.)
im Lehramtsstudium (Kernfach: Physik; Zweitfach: Mathematik)

eingereicht an der
Mathematisch-Naturwissenschaftlichen Fakultät
Institut für Physik
Humboldt-Universität zu Berlin

von
Kilian-Kristoph Schumann
geboren am 23.08.1991 in Berlin

Betreuung:

1. *Prof. Dr. Oliver Benson*
2. *Prof. Dr. Burkhard Priemer*

eingereicht am: *24. Oktober 2016* - ***nachträglich editierte Fassung!***

Abstract

Quantum cryptography offers great possibilities whenever unconditional security is needed. It is the only encryption scheme that is truly secure without requiring the communication parties to share a key initially. However, it is difficult to implement a realisation that leaves no possibillity to be intercepted by a potential eavesdropper.

In this thesis a setup for Quantum Key Distribution (QKD) based on the BB84 protocol was reconstructed and improved. Students may work on this subject during an advanced lab experiment. An attenuated laser and a single photon source based on defect centres in diamond nanocrystals are available as light sources. An exemplary measurement obtained a raw bit rate of 20.7 ± 0.4 kBits/s with an error rate of 6.01% using the laser and 1.42 ± 0.02 kBits/s with 6.93% using the single photon source.

In addition to the physical perspective, the setup is also reviewed with regard to its pedagogical aspects such as educational objectives and the design of the manual. As a result the thesis provides a completed setup to be used as an advanced lab experiment right away.

Keywords:
Quantum Key Distribution, BB84, single photon source,
advanced lab experiment

Zusammenfassung

Quantenkryptographie ermöglicht als einziges Verschlüsselungsverfahren bedingungslose Sicherheit, ohne dass die Kommunikationsparteien bereits über einen gemeinsamen Schlüssel verfügen. So großartig das klingt, so schwierig ist jedoch eine praktische Umsetzung, in der keine Angriffsmöglichkeiten gelassen werden.

In dieser Arbeit wurde ein Aufbau zum Quantenschlüsselaustausch (QKD) nach dem BB84-Protokoll rekonstruiert und für den Einsatz als Versuch im Fortgeschrittenenpraktikum optimiert. Dabei stehen als Lichtquelle sowohl ein gedämpfter Laser als auch eine Einzelphotonenquelle auf Basis von Defektzentren in Nanodiamanten zur Verfügung. Unter Verwendung des Lasers wurde bei einer exemplarischen Messung eine Übertragungsrate von $20{,}7 \pm 0{,}4\,\mathrm{kBits/s}$ bei einer Fehlerrate von 6,01% erreicht, unter Verwendung der Einzelphotonenquelle dagegen $1{,}42 \pm 0{,}02\,\mathrm{kBits/s}$ bei 6,93%.

Ergänzend zur physikalischen Sichtweise wurde der Aufbau auch unter didaktischen Gesichtspunkten betrachtet. Es wurden Lehrziele für den Einsatz als Praktikumsversuch formuliert und eine Versuchsanleitung erstellt. Als Ergebnis steht ein fertiger Versuch zur Verfügung, der ab sofort im Fortgeschrittenenpraktikum eingesetzt werden kann.

Schlagwörter:
Quantenschlüsselaustausch, BB84, Einzelphotonenquelle,
Fortgeschrittenenpraktikum

Inhaltsverzeichnis

Kapitel 1

Einleitung

1.1 Kryptologie und Quantenkryptographie

Zur Bedeutung der Kryptologie

Seit Jahrtausenden beschäftigt sich der Mensch mit der geheimen Übertragung und Aufbewahrung von Nachrichten. Oft war es essentiell für den Verlauf von Kriegen und Intrigen, einerseits die Verschlüsselungen des Gegners zu brechen, andererseits die unbefugte Entschlüsselung der eigenen Nachrichten zu verhindern (vgl. Singh, 2001, S. 9).
Aus diesen beiden Anlässen entwickelte sich die Wissenschaft der **Kryptologie** mit ihren beiden Unterdisziplinen:

- **Kryptographie** – die Wissenschaft der Verschlüsselung und
- **Kryptoanalyse** – die Wissenschaft der (unbefugten) Entschlüsselung.

Unterscheiden lassen sich innerhalb der Kryptographie **Transpositionen** als Vertauschung der Reihenfolge der Zeichen innerhalb der Nachricht von **Substitutionen** als Ersetzen von Buchstaben oder Wörtern durch andere Zeichen. Werden Wörter ersetzt, spricht man von einer **Codierung**, bei Buchstaben dagegen von einer **Chiffrierung**. Beispiel einer Chiffrierung wäre die schon von Cäsar verwendete Verschiebung des Alphabets um eine feste Zahl. Cäsar verschob jeden Buchstaben um drei Stellen, somit ergab sich die Substitution A → D, B → E, C → F, ...
Die Verschlüsselung einer Nachricht ist ferner davon abzugrenzen, sie zu verbergen – ein Gebiet, mit dem sich die **Steganographie** beschäftigt, das für diese Arbeit aber nicht weiter relevant ist (vgl. Singh, 2001, S. 18 ff., 26, 32, 47 f.). Eine Übersicht liefert Abb. 1.1 .
Die meisten Verschlüsselungen benutzen als Verfahren Substitutionen, Transpositionen oder Kombinationen daraus. Kennzeichnend für viele Verschlüsselungen ist außerdem, dass ein **Schlüssel** zur Umwandlung des sogenannten **Klartextes** (d.h. der geheim zu haltenden Nachricht) in den sogenannten **Geheimtext** benutzt wird. Die Sicherheit der Verschlüsselung sollte sich dabei nach dem *Kerckhoffs'sche Maxime* genannten Grundsatz allein auf die Geheimhaltung dieses Schlüssels gründen (Singh, 2001, S. 27).
Der Einsatz eines Schlüssels erfordert jedoch immer, dass die **Senderin** der Nachricht, meist Alice genannt, dem **Empfänger**, meist Bob genannt, neben dem Geheimtext auch den Schlüssel zukommen lassen muss, ohne dass eine potentielle **Lauscherin**, meist Eve (nach englisch *eavesdropping* = lauschen) genannt, diesen abhören könnte.

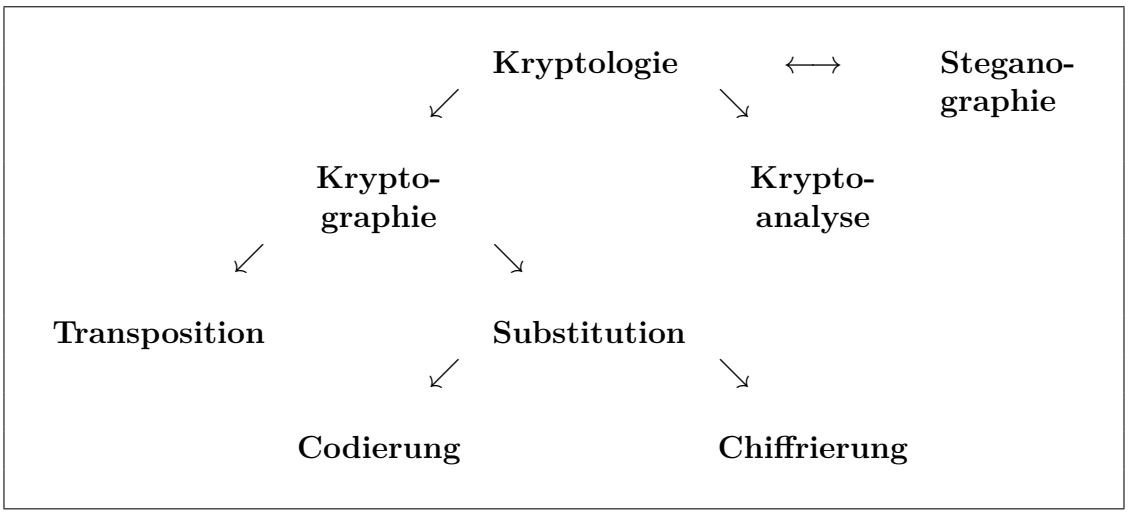


Abbildung 1.1 – Teile der Kryptographie (nach Singh, 2001, S. 48).
Anders als die Steganographie, das Verbergen von Nachrichten, beschäftigt sich die Kryptologie mit ihrer Ver- und Entschlüsselung (Kryptographie und -analyse). Dabei können die Bestandteile der Nachricht entweder in ihrer Reihenfolge oder in ihrer Repräsentation durch Zeichen verändert werden (Transposition und Substitution), wobei Letzteres auf Wort- oder Buchstabenebene geschehen kann (Codierung und Chiffrierung).

Selbst wenn eine Verschlüsselung sicherstellt, dass eine Lauscherin den Geheimtext ohne Schlüssel nie entschlüsseln kann, bleibt das Problem des sicheren Schlüsselaustauschs. Dass solche Verschlüsselungen existieren, wird in Abschnitt 2.1 gezeigt. Der Aufwand des Schlüsselaustauschs nimmt logischerweise mit steigender Anzahl der zu übertragenden Nachrichten zu. Dieses Problem hat in letzter Zeit eine deutliche Relevanz bekommen.

Kryptologie heute

Durch die digitale Revolution, die der Entwicklung von Computer und Internet folgte, ist zum einen die Menge der alltäglich übertragenden Information gigantisch geworden, zum anderen lässt sich diese Information mühelos und unbemerkt duplizieren. Die Verbreitung von Internetbanking, sozialen Netzwerken wie Facebook, Twitter oder Xing und Instant-Messaging-Diensten wie WhatsApp, Skype oder Snapchat erzeugt Unmengen sensibler Daten, die vor illegalem Zugriff sowohl Krimineller als auch staatlicher Agenturen wie NSA oder BKA geschützt werden müssen.
Die Verschlüsselung der digitalen Kommunikation erfolgt derzeit auf Basis asymmetrischer Verfahren (vgl. z.B. WhatsApp, 2016; Singh, 2001, S. 372) wie OpenPGP, S/MIME oder SSL/TLS, bei denen unterschiedliche Schlüssel zur Ver- und Entschlüsselung eingesetzt werden: Bob besitzt einen privaten Schlüssel, den er geheim hält, und einen öffentlichen, der für Alice (und alle anderen, also auch Eve) zugänglich ist. Aus dem mit Bobs öffentlichen Schlüssel erzeugtem Geheimtext kann der Klartext durch diesen nicht wieder zurückgewonnen werden, sondern nur durch Bobs privaten Schlüssel (vgl. Singh, 2001, S. 325 ff.).
Der Vorteil der Methode liegt darin, dass nicht vor jeder Informationsübertragung ein Schlüssel zwischen Senderin und Empfänger ausgetauscht werden muss.

Der Nachteil besteht jedoch in einer teilweisen Verletzung der Kerckhoffs'schen Maxime: Die Sicherheit des Verfahrens hängt nicht nur von der Geheimhaltung des privaten Schlüssels ab, sondern auch davon, dass dieser nicht aus dem öffentlichen Schlüssel ermittelt werden kann. In der Praxis wird dies meist durch den Einsatz mathematischer Probleme erreicht, die zu dieser Zeit nicht effizient gelöst werden können, so etwa das Faktorisieren einer sehr großen Zahl. Die Entwicklung effizienterer Algorithmen oder eine entsprechende Erhöhung der Rechenleistung von Computern macht diese Verfahren somit potentiell angreifbar. Nützlich für die Kryptoanalyse wäre in diesem Zusammenhang ein funktionierender Quantencomputer, für den bereits Algorithmen (z.B. der Shor-Algorithmus zum Faktorisieren einer Zahl, siehe (s.) P. W. Shor, 1997) entwickelt wurden, welche die zur Zeit hauptsächlich eingesetzte asymmetrische Verschlüsselung wertlos machen würde (vgl. Singh, 2001; Nielsen & Chuang, 2005, S. 386 f. bzw. S. 6).

Quantenkryptographie

Doch nicht nur die Kryptoanalytik hat ein Auge auf mögliche Anwendungen der Quantenmechanik geworfen. Auch für die Kryptographie werden bahnbrechende neue Entwicklungen durch dieses physikalische Gebiet erhofft, da die Quantenkryptographie, zumindest in der Theorie, absolute Geheimhaltung gewährt – nicht nur gegenüber derzeitigen Methoden sondern auch gegenüber Quantencomputern und allen weiteren denkbaren Versuchen eines mit unbegrenzter Zeit und Ressourcen ausgestatteten Angreifers. Möglich wird diese bedingungslose Sicherheit (die auf englisch sog. *unconditional security*) durch Ausnutzung fundamentaler physikalischer Gesetze (vgl. Singh, 2001, S. 400 ff.).
Die Kommunikation wird in der Quantenkryptographie über zwei Kanäle realisiert, einen klassischen und einen quantenmechanischen. Zuerst werden zufällig gewählte Zeichen über den quantenmechanischen Kanal übermittelt und zur Erzeugung eines Schlüssels verwendet. Anschließend wird der mit diesem Schlüssel durch klassische kryptografische Verfahren erzeugte Geheimtext über den (nicht abhörsicheren) klassischen Kanal übertragen. Dabei kann zwar nicht ausgeschlossen werden, dass auch der Quantenkanal abgehört wird, jedoch kann das nie unbemerkt geschehen. Die Lauscherin fällt somit schon auf, während der Schlüssel ausgetauscht wird, bevor also die eigentliche Nachricht gesendet wird. Aus diesem Grund kann er zwar im schlimmsten Fall die Kommunikation unterbinden, aber nicht einmal ansatzweise Informationen über den Inhalt der Nachricht erhalten. Die Quantenkryptographie schützt damit nicht nur den Inhalt der Nachricht, sondern erlaubt es auch, eine Lauscherin sofort zu entdecken (vgl. Singh, 2001, S. 411 ff.).
Auf den detaillierten Ablauf und die Sicherheit des Verfahrens wird in Abschnitt 2.4 näher eingegangen.

1.2 Lernort Labor und das Fortgeschrittenenpraktikum

1.2.1 Charakteristika des Labors als Lernort

Die Lehrform Labor findet sich innerhalb der Hochschulausbildung fast ausschließlich im Bereich der Naturwissenschaften (vgl. Bruchmüller & Haug, 2001, S. 25). In diesen Studiengängen kommt ihm allerdings eine herausragende Bedeutung zu, da es der künftigen Arbeitssituation eines Naturwissenschaftlers in Industrie oder Forschung weitgehend entspricht. Neben der Vermittlung von fachlichen Kenntnissen stehen im Labor aus diesem Grund vor allem prozessbezogene Experimentier- und Problemlösekompetenzen im Mittelpunkt. Diese dienen zur Vorbereitung nicht nur auf das Berufsleben, sondern auch auf die Abschlussarbeiten, in denen ein experimentelles oder theoretisches Problem selbstständig gelöst werden soll (vgl. Bruchmüller & Haug, 2001, S. 25, 65, 67).
Charakteristisch für den Lernort Labor ist also – gerade im Vergleich zu anderen Lehrformen wie Vorlesung oder Seminar (vgl. auch Bruchmüller & Haug, 2001, S. 45, 64):

- Fokus auf motorische Fähigkeiten und Eigenerfahrung;
- Vermittlung von Experimentierkompetenzen;
- Vermittlung von Problemlösekompetenzen;
- hohe Übereinstimmung mit möglichem beruflichem Tätigkeitsfeld.

Zum letzten Punkt ist allerdings anzumerken, dass es auch grundlegende Unterschiede zwischen dem Labor im Hochschul- und im Berufsalltag gibt, so z.B. in der Bedeutung von Kosten- und Zeitfaktoren, den Konsequenzen von Fehlern oder der Präsentation von Ergebnissen (vgl. Bruchmüller & Haug, 2001, S. 73 ff.). Doch auch unter Beachtung dieser Einschränkung kann der Lehrform Labor eine hohe Bedeutung in Hinblick auf die mögliche Arbeitssituation eingeräumt werden.

1.2.2 Drei-Stufen-Modell der Laborarbeit

Bruchmüller und Haug (2001, S. 66-77) unterteilen die Laborarbeit im Rahmen der Hochschulausbildung in drei sowohl der zeitlichen Abfolge als auch dem Niveau nach aufeinander folgende Stufen. Stufe I steht dort für am Beginn des Studiums angesiedelte Übungs- und Praktikums-Versuche mit umfangreicher, starrer Anleitung und wenig Raum für Mitbestimmung. Stufe III dagegen umfasst vollkommen selbstständige wissenschaftliche Arbeiten wie Semester- oder Abschlussarbeiten, in denen kaum Vorgaben gemacht werden. Als Brücke zwischen beiden soll Stufe II dienen, deren Funktion es ist, zu mehr eigenständiger Laborarbeit hinzuführen, etwa durch den Einsatz von Übungsversuchen mit Varianten, Wahlversuchen oder sog. Mini-Projekten (vgl. zu letzterem Bruchmüller & Haug, 2001, S. 108 ff.). Der Schwerpunkt in der Zielsetzung von Stufe I liegt auf einer Veranschaulichung der in der Vorlesung gelernten Theorie sowie im Erwerb grundlegender Erfahrungen. In Stufe II und III geht es dagegen eher um den Erwerb von Problemlösungsverhalten, um Kommunikationsfähigkeit, Handlungs-, Entscheidungs- und Sachkompetenz (vgl. Bruchmüller & Haug, 2001, S. 70 ff.).

1.2.3 Ziele und Rahmenbedingungen des Fortgeschrittenenpraktikums

Im Verlauf des Physikstudiums an der Humboldt-Universität zu Berlin kommen die Studierenden im Rahmen verschiedener Praktika mit dem Lernort Labor in Berührung. Das Fortgeschrittenenpraktikum (F-Praktikum) ist dabei am Ende des Monobachelors Physik angesiedelt – zwischen Grundpraktikum, welches als typischer Vertreter von Stufe I des Drei-Stufen-Modells nach Bruchmüller und Haug (2001, s. auch vorherigen Abschnitt) angesehen werden kann, und der Bachelorarbeit, die auf Stufe III dieses Modells anzusiedeln ist. Demzufolge sollte das F-Praktikum Stufe II entsprechen, deren Ziel es ja ist, zu mehr selbstständiger Laborarbeit hinzuführen.
In der Tat ist Selbstständigkeit eines der in der Studienordnung genannten Lern- und Qualifikationsziele, welche konkret lauten:

> „Die Studierenden lösen komplexe experimentelle Fragestellungen der modernen Physik mittels eigener und weitgehend selbständiger praktisch-experimenteller Tätigkeit. Sie sind in der Lage, die Nutzung experimenteller Grundprinzipien, Techniken und Geräte einzuschätzen, und bewerten und dokumentieren experimentelle Ergebnisse eigenständig.“ (Humboldt-Universität zu Berlin, 2014, S. 25)

Das Modul *P8.a Fortgeschrittenenpraktikum I* ist laut dem in der Studienordnung genannten idealtypischen Studienverlaufsplan im 5. Semester zu belegen, es können darüber hinaus aber auch Versuche im Rahmen eines Wahlmoduls im 4. oder 6. Semester des Monobachelors oder im 1. Semester des Lehramtsmasters mit erstem oder zweitem Fach Physik bearbeitet werden (vgl. Humboldt-Universität zu Berlin, 2014, 2015, S. 36 bzw. 17 f.). In jedem Fall werden durch die Studierenden aus einem Angebot von Versuchen mehrere ausgewählt und mittels der im Internet verfügbaren Versuchsanleitung eigenständig vorbereitet. Diese Herangehensweise, Wahlversuche anzubieten, spricht ebenfalls für eine Einordnung des F-Praktikum in Stufe II.
Angeboten werden die Versuche direkt von den einzelnen Arbeitsgruppen des Instituts für Physik, die Betreuung erfolgt zumeist von Doktoranden oder festangestellten Wissenschaftlern. Ein einzelner Versuch hat dabei eine Dauer von ein bis zwei Tagen und wird mit einem Bericht abgeschlossen, der laut Studienordnung etwa 10 Seiten umfassen sollte.
Als fachliche Voraussetzungen für das Modul wird in der Studienordnung empfohlen, die Vorlesungen zur Experimentalphysik und das Grundpraktikum abgeschlossen zu haben (vgl. Humboldt-Universität zu Berlin, 2014, S. 25). Aufgrund der verschiedenen möglichen Studiengänge und Fachsemester der Teilnehmenden ist nichtsdestotrotz mit einem unterschiedlichen Stand der Vorkenntnisse zu rechnen.
Diese Ziele und Rahmenbedingungen sind zu beachten, wenn ein neuer F-Praktikum-Versuch erstellt werden soll. Sie werden demzufolge in Abschnitt 4.1 wieder aufgegriffen, wenn auf die Ziele des QKD-Versuchs eingegangen wird.

1.3 Zielstellung und Struktur der Arbeit

Diese Arbeit knüpft an einen Versuch zum Thema Quantenschlüsselaustausch (*Quantum Key Distribution*, QKD) an, der früher von der Arbeitsgruppe Nanooptik im Rahmen des F-Praktikums angeboten, dann aber eingestellt wurde. In den letzten Jahren wurde der Aufbau größtenteils im Rahmen der Dissertationen von Tim Schröder (2012) und Matthias Leifgen (2016) überarbeitet und erweitert (Leifgen, 2016; Kewitsch, 2013; Riemann, 2013; Schröder, 2012).
Ziel der Arbeit ist die Neukonzipierung des F-Praktikum-Versuchs unter Einbeziehung der hinzugekommenen Geräte, allen voran einer kompakten Einzelphotonenquelle auf Basis von Defektzentren in Nanodiamanten, und die Erstellung einer Versuchsanleitung auf hochschuldidaktischer Basis.
Dementsprechend gliedert sich der folgende Text in die Kapitel 2 Theoretische Beschreibung, 3 Experimentelle Umsetzung und 4 Didaktische Aufbereitung. In dieser Einleitung wurde dabei ein Überblick über Kryptologie und Quantenkryptographie (Abschnitt 1.1), sowie den Lernort Labor und das Fortgeschrittenenpraktikum (Abschnitt 1.2) gegeben. Der folgende theoretische Teil thematisiert die kryptographischen, physikalischen und informationstheoretischen Grundlagen der Arbeit (Abschnitt 2.1, 2.2 und 2.3) und stellt das verwendete Übertragungsprotokoll BB84 vor (Abschnitt 2.4). Der experimentelle Teil beschreibt den konkreten Versuch, wie er innerhalb dieser Bachelorarbeit zusammengesetzt wurde, in seinem Aufbau (Abschnitt 3.1), seiner Umsetzung des Übertragungsprotokolls (Abschnitt 3.2) und der Ansteuerung der Geräte (Abschnitt 3.3). Darüber hinaus wird in diesem Teil die Durchführung einer QKD-Übertragung unter Verwendung sowohl eines Lasers als auch einer Einzelphotonenquelle dargestellt. Dazu werden exemplarische Ergebnisse beschrieben und diskutiert (Abschnitt 3.4 und 3.5). Der didaktische Teil widmet sich der Versuchsanleitung, wofür zuerst auf die Lehrziele des Versuchs (Abschnitt 4.1) eingegangen wird, wonach die Gestaltung der Versuchsanleitung (Abschnitt 4.2) beschrieben wird. Den Abschluss bildet ein Ausblick auf den Einsatz des Experiments als F-Praktikum-Versuch (Kapitel 5).

Kapitel 2

Theoretische Beschreibung

Dieses Kapitel betrachtet die Grundlagen, die für das Verständnis des QKD-Aufbaus benötigt werden. Da in der QKD ein Schlüssel und nicht die eigentliche Nachricht übermittelt wird, ist es unumgänglich, das Verfahren mit einer klassischen Verschlüsselung auf Basis eines Schlüssels zu kombinieren. Zur Gewährleistung der bedingungslosen Sicherheit kommt dafür nur das *One-Time-Pad*-Verfahren in Betracht, welches im ersten Abschnitt beschrieben wird. Danach werden im zweiten Abschnitt in möglichst kompakter Form wesentliche Aspekte des Einsatzes und Nachweises einzelner Photonen zur Übertragung des Schlüssels benannt, da die Sicherheit der QKD auf einer Gewährleistung des Einzelphotonencharakters beruht. Der dritte Abschnitt führt in Quanteninformationsverarbeitung ein, wodurch eine Übertragung von Informationen mittels Photonen erst ermöglicht wird. Zuletzt wird im vierten Abschnitt das hier konkret verwendete Übertragungsprotokoll BB84 bezüglich seines Prinzips und Ablaufs vorgestellt.

2.1 Das *One-Time-Pad*-Verfahren

Das *One-Time-Pad* (OTP)-Verfahren, von Singh (2001, S. 145) gar als „heiliger Gral der Kryptographie“ bezeichnet, ist ein klassisches Verschlüsselungsverfahren, welches unter gewissen Voraussetzungen als einziges klassisches Verfahren eine absolut sichere Verschlüsselung ermöglicht.

Durchführung einer Chiffrierung

Grundlage einer Verschlüsselung mit dem OTP-Verfahren ist der sowohl bei der Senderin als auch beim Empfänger vorliegende Schlüssel, an den gewisse Anforderungen gestellt werden müssen, wie im nächsten Abschnitt diskutiert wird. Da für die Quantenkryptographie nur binäre Daten betrachtet werden, wird auch im Folgenden davon ausgegangen, dass sowohl Klartext als auch Schlüssel in dieser Form vorliegen. Um z.B. einen Text zu chiffrieren, kann der Klartext dafür zuerst über eine ASCII-Tabelle in eine binäre Form gebracht werden.
Um zu verschlüsseln wird jedes Bit des Klartextes mit einem Bit des Schlüssels binär addiert, das Ergebnis also modulo 2 genommen, wodurch sich insbesondere die Summe $1+1 = 0$ ergibt. Die so erhaltenen Bits bilden dann den binären Geheimtext, der ggf. wiederum in Zeichen zurückübersetzt wird. Dies ist in Abb. 2.1 an einem Beispiel dargestellt.

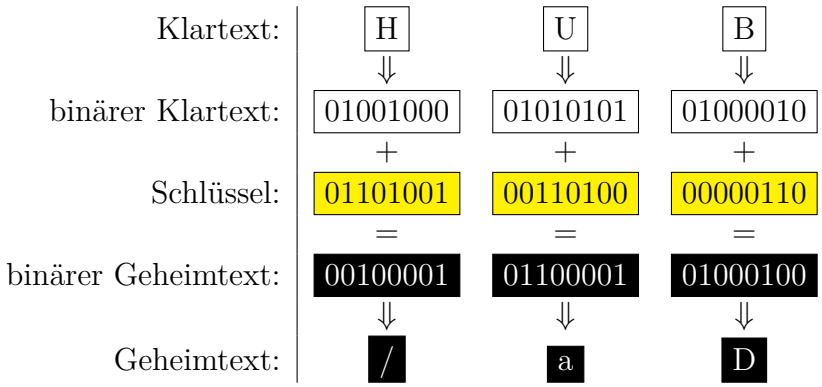


Abbildung 2.1 – Beispiel einer Chiffrierung in binärer Form nach dem OTP-Verfahren (nach Benson, 2016, S. 48).
Der Klartext H U B wird über eine ASCII-Tabelle in eine binäre Form gebracht und mit dem vorher übermittelten Schlüssel binär addiert. Der so entstandene Geheimtext kann binär oder als Zeichenfolge / a D dargestellt werden.

Der Empfänger der Nachricht geht zum Entschlüsseln wie die Senderin vor und addiert ebenfalls den Schlüssel binär und bitweise zu dem Geheimtext, um den Klartext zu erhalten. Möglich ist das, weil die Bit-Werte 0 und 1 additiv invers zu einander (modulo 2) sind, Subtraktion zweier Bits also das gleiche Ergebnis wie Addition ergibt.

Voraussetzungen des Verfahrens

Als Erfinder des OTP-Verfahrens wird meist G. Vernam gesehen, der es erstmalig zum Patent anmeldete (Vernam, 1919).
Er schreibt zu den Voraussetzungen des Verfahrens:

> „If the key [...] is made very long, so that it *never repeats* and if any portion of this key is *never used for more than one message*, the operation of 'breaking' the cipher becomes very much more difficult. If, now, instead of using English words or sentences, we employ a key *composed of letters selected absolutely at random*, a cipher system is produced, which is *absolutely unbreakable*." (entnommen aus Vernam, 1926, S. 12, eigene Hervorhebung)

Gefordert wird also:

1. Der Schlüssel ist, ohne sich zu wiederholen, so lang wie der Klartext.
2. Der Schlüssel (bzw. Teile daraus) wird nur einmal eingesetzt.
3. Der Schlüssel ist aus unvorhersagbar zufälligen Buchstaben zusammengesetzt.

Unter diesen Voraussetzungen ist im Rahmen der Kommunikationstheorie beweisbar, dass der Klartext ohne Kenntnis des Schlüssels nicht ermittelt werden kann (Shannon, 1949, S. 682). Die drei Voraussetzungen erreichen, dass der Schlüssel keinerlei Struktur (einer Wiederholung von Zeichenfolgen innerhalb des Schlüssels oder von vorherigen Schlüsseln oder einer Sprache) aufweist, die einen Ansatz zur

Entschlüsselung geben könnte. Es könnte hier argumentiert werden, dass durch Ausprobieren aller nur möglichen Schlüssel der richtige sicher gefunden werden müsste, sodass die Entschlüsselung nur eine Frage der Zeit und der zur Verfügung stehenden Rechenkapazität wäre. Dieses Argument ist nicht falsch, übersieht jedoch, dass dabei auch *alle* möglichen Texte von der Länge des Klartextes erhalten werden und somit nicht entschieden werden kann, welcher davon die eigentliche Nachricht darstellt (vgl. Singh, 2001, S. 152 f.).

Schlüsselübertragung – lediglich eine Verlagerung des Problems?

Das Problem der geheimen Nachrichtenübertragung ist mithilfe des OTP-Verfahrens darauf verlagert, einen Schlüssel sicher zu übertragen. Auf den ersten Blick ist damit wenig gewonnen: Steht ein Weg zur Verfügung, einen Schlüssel zu übertragen, ohne dass er kopiert werden kann, ist eine Verschlüsselung nicht notwendig, da dann auch gleich der (unverschlüsselte) Klartext übermittelt werden könnte. Der Vorteil liegt jedoch in der Möglichkeit, dem Empfänger auf einmal einen ganzen Block voller Schlüssel (nämlich das namensgebende *One-Time-Pad*) zukommen zu lassen, die dann später für viele Nachrichten verwendet werden können (nach diesem Prinzip funktionieren z.B. auch TAN-Listen wie sie für die Authentifizierung beim Online-Banking verwendet werden). Dabei muss nur sichergestellt werden, dass ein Kopieren des Schlüsselblocks nicht unbemerkt geschehen kann. Werden nämlich Unregelmäßigkeiten entdeckt, die auf ein Einmischen eines Dritten hindeuten, wird der Schlüsselblock einfach nicht verwendet und alles, was der Angreifer erbeuten konnte, ist eine Reihe sinnloser Zeichen.
Allerdings ist es mit klassischen Verfahren schwer und aufwändig, jegliches Kopieren zu bemerken, gerade wenn die Nachrichten (wie in der Internetkommunikation) über weite Strecken und in Kabeln übertragen werden. Auch beruht die absolute Sicherheit des OTP-Verfahrens auf der Zufälligkeit des Schlüssels, was gewaltige Anforderungen stellt, da keine Pseudozufallszahlen, wie sie in Computern verwendet werden, benutzt werden können (vgl. Singh, 2001, S. 154 f.).
Und an dieser Stelle kommt die Quantenphysik ins Spiel. Denn wie bereits in Abschnitt 1.1 erwähnt und in Abschnitt 2.4 näher ausgeführt, ermöglicht es die Quantenkryptographie, eine Lauscherin sofort zu entdecken. Auch das Problem der Erzeugung großer Mengen von echten Zufallszahlen in kurzer Zeit lässt sich durch quantenmechanische Geräte (wie z.B. des in Leifgen et al., 2011, S. 154 ff. beschrieben) lösen.

2.2 Einzelphotonen als physikalische Grundlage der Quantenkryptographie

Die Sicherheit der Quantenkryptographie beruht zum einen auf der Verwendung des OTP-Verfahrens, zum anderen darauf, jeden Lauschangriff auf die Schlüsselübertragung zu bemerken. Für Letzteres ist es in den meisten Fällen unerlässlich, einzelne Photonen zur Schlüsselübertragung zu verwenden. Denn wenn auch nur zwei Photonen dieselbe Information tragen, ist es prinzipiell möglich über einen sogenannten *photon number splitting*-Angriff unbemerkt an eine Kopie der Information zu gelangen. Bei diesem wird ein Photon abgezweigt und für spätere Messungen in einem Quantenspeicher gelagert (vgl. dazu auch Leifgen, 2016, S. 53 ff.).
Nachfolgend wird einerseits eine Einzelphotonenquelle (*single photon source*, SPS) auf Basis von Defektzentren in Nanodiamanten vorgestellt und andererseits das Verfahren der Autokorrelationsmessung als Nachweis von einzelnen Photonen beschrieben.

2.2.1 Defektzentren in Nanodiamanten

Ein vielversprechender Kandidat für eine SPS sind Defektzentren in Diamanten. Die räumliche Ausdehnung der Diamanten liegt dabei oft in der Größenordnung von Nanometern, weshalb sie als Nanodiamanten bezeichnet werden. Ein Defektzentrum ist eine durch den Eintrag von Fremdatomen oder Fehlstellen im Kristallgitter des Kohlenstoffs erzeugte Struktur und makroskopisch für die Färbung des Diamanten verantwortlich (vgl. Aharonovich et al., 2011, S. 2).
Mikroskopisch gesehen wäre die einfachste Struktur, die für eine SPS in Frage kommt, ein Zwei-Niveau-System aus einem Grund- und einem angeregten Zustand. Es verhält sich wie ein einzelnes Atom und sendet bei entsprechender optischer Anregung Photonen mit definierten Eigenschaften aus. Meist handelt es sich in der Praxis jedoch um Drei- oder Mehr-Niveau-Systeme, die metastabile Zustände zwischen Grund- und angeregtem Zustand enthalten (vgl. Abb. 2.2, s. auch Aharonovich et al., 2011, S. 4).

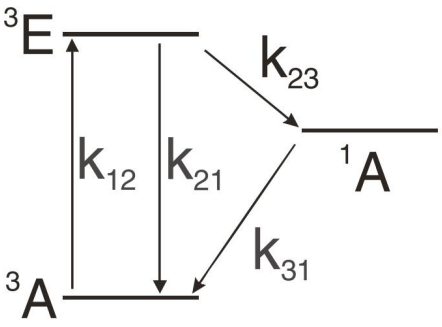


Abbildung 2.2 – Drei-Niveau-Schema zur Beschreibung eines NV-Zentrums (entnommen aus Jelezko & Wrachtrup, 2006, S. 3211).
Aus dem Grundzustand ^3A werden Elektronen mit einer Rate von k_{12} in den angeregten Zustand ^3E gehoben, aus dem sie mit k_{21} wieder nach ^3A zurück oder mit k_{23} in einen metastabilen Zustand ^1A übergehen können. k_{31} bezeichnet die Rate des Übergangs von dem metastabilen Zustand ^1A in den Grundzustand ^3A.

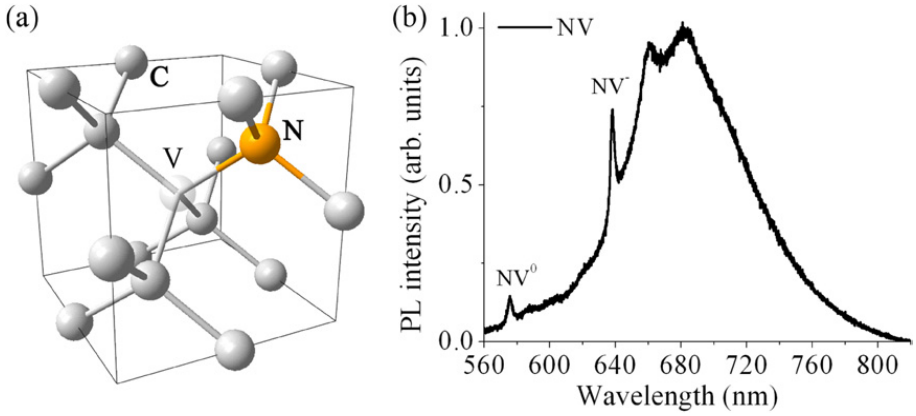


Abbildung 2.3 – Kristallographisches Modell und Spektrum eines NV-Zentrums (entnommen aus Aharonovich et al., 2011, S. 5).
a) Bei einem NV-Zentrum ersetzt ein Stickstoffatom (in der Abb. orange und mit N gekennzeichnet) ein Kohlenstoffatom in der Kristallstruktur des Diamants, benachbart dazu tritt eine Lücke (in der Abb. transparent und mit V gekennzeichnet) auf.
b) Das Spektrum bei Raumtemperatur weist zwei charakteristische Spitzen bei 575 nm (neutrales NV-Zentrum) und 637 nm (negativ geladenes NV-Zentrum) auf.

Die hier verwendete SPS enthält Stickstoff-Fehlstellen-Zentren (*nitrogen-vacancy center*, NV), bei denen ein Kohlenstoffatom des Diamants durch ein Stickstoffatom ersetzt wird und dazu benachbart eine Lücke (englisch *vacancy*) im Kristallgitter auftritt (vgl. Abb. 2.3a). Dieses NV-Zentrum wird durch grünes Laserlicht angeregt und sendet Photonen im sichtbaren roten und infraroten Bereich aus (vgl. Abb. 2.3b). Dabei kann es als Drei-Niveau-System betrachtet werden (vgl. Aharonovich et al., 2011, S. 5).
Der herausragende Vorteil in der Verwendung von NV-Zentren als SPS liegt in der einfachen Handhabung. So muss die Quelle nicht gekühlt werden und kann in kompakter Bauform realisiert werden (vgl. Schröder, 2012, S. 15).

2.2.2 Autokorrelation von Photonen

Die Anzahl von Photonen, die mit einem zeitlichen Abstand von τ von einer Quelle erzeugt werden, lässt sich über die Korrelationsfunktion zweiter Ordnung beschreiben (Walls & Milburn, 2008, S. 39):

$$G^{(2)}(\tau) = \langle : I(t)I(t+\tau) : \rangle \tag{2.1}$$

Dabei ist I der Intensitätsoperator, $: \cdots :$ entspricht der Normalordnung und $\langle \ldots \rangle$ gibt an, dass es sich um einen Mittelwert handelt.
Wird diese Funktion hinsichtlich dem Quadrat der mittleren Intensität zum Zeitpunkt t normiert, ergibt sich die normierte Korrelationsfunktion zweiter Ordnung $g^{(2)}(\tau)$, formal definiert (vgl. Jelezko & Wrachtrup, 2006, S. 3213):

$$g^{(2)}(\tau) = \frac{G^{(2)}(\tau)}{|\langle I(t) \rangle|^2} = \frac{\langle : I(t)I(t+\tau) : \rangle}{|\langle I(t) \rangle|^2}. \tag{2.2}$$

Betrachtet man die normierte Funktion zu $\tau = 0$, also Photonen, die zur gleichen Zeit detektiert werden, so ergibt sich für Photonenzahlzustände $|n\rangle$ aus n Photonen im selben Zustand (Walls & Milburn, 2008, S. 41):

$$g^{(2)}(0) = 1 - \frac{1}{n}. \tag{2.3}$$

Wurde also nur ein Photon erzeugt, kann $g^{(2)}(0) = 0$ erwartet werden, bei zwei Photonen $g^{(2)}(0) = \frac{1}{2}$ und so weiter. Da in der Praxis noch Effekte wie z.B. die Wechselwirkung mit Elektronen an der Oberfläche der Probe auftreten, die im Modell vernachlässigt werden, wird der ideale Wert $g^{(2)}(0) = 0$ allerdings auch für Einzelphotonenquellen nicht immer erreicht. Solange jedoch $g^{(2)}(0) < \frac{1}{2}$ kann davon ausgegangen werden,dass das detektierte Licht einen dominierenden Anteil von Einzelphotonen enthält (vgl. Aharonovich et al., 2011, S. 3).
Im Fall eines Drei-Niveau-Systems (vgl. Abb. 2.2) mit Übergangsraten k_{ij} von dem i-ten in den j-ten Zustand, kann die Autokorrelation in guter Näherung von einer Funktion der folgenden Form beschrieben werden (vgl. Jelezko & Wrachtrup, 2006, S. 3213):

$$g^{(2)}(\tau) = 1 - (K+1)\, e^{k_+\tau} + K e^{k_-\tau}, \quad \text{für } \tau \geqslant 0 \tag{2.4}$$

Dabei ist $k_\pm = -\frac{1}{2}P \pm \sqrt{\frac{1}{4}P^2 - Q}$ mit $P = k_{21} + k_{12} + k_{23} + k_{31}$ und $Q = k_{31} \cdot (k_{21} + k_{12}) + k_{23} \cdot (k_{31} + k_{12})$, sowie $K = \frac{k_- + k_{31} - k_{12}\frac{k_{23}}{k_{31}}}{k_+ - k_-}$ (vgl. Jelezko & Wrachtrup, 2006, S. 3213). Diese Form ist nützlich, wenn der Verlauf einer Autokorrelation gemessen wurde und durch eine theoretische Funktion beschrieben werden soll.

2.3 Quanteninformationsverarbeitung

Da sich jegliche Information als Folge von Nullen und Einsen ausdrücken lässt, genügt es, im Folgenden als Klartext und Schlüssel lediglich binäre Folgen von Bits bzw. Bytes zu betrachten. Ein Byte entspricht dabei acht Bit: $1\,\mathrm{B} = 8\,\mathrm{Bit}$. In Anlehnung an das binäre System aus der klassischen Informationsverarbeitung werden die Informationseinheiten in der Quanteninformationsverarbeitung Quantenbits (Qubits) genannt.

Theoretische Beschreibung von Quantenbits

So wie ein klassisches Bit einen Zustand – entweder 0 oder 1 – besitzt, hat auch ein Qubit einen Zustand, der konventionell in Dirac-Notation als $|\Psi\rangle$ ausgedrückt wird. Der Unterschied zwischen Bits und Qubits besteht darin, dass Qubits nicht nur in den Zuständen $|0\rangle$ oder $|1\rangle$, sondern auch in Linearkombinationen dieser Zustände, sogenannten Superpositionen, auftreten können:

$$|\Psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle\,, \qquad \text{mit } \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1. \tag{2.5}$$

Anders ausgedrückt kann der Zustand $|\Psi\rangle$ des Qubits als Einheitsvektor in einem zweidimensionalen, komplexen Vektorraum beschrieben werden, wobei die Zustände $|0\rangle$ und $|1\rangle$ eine orthonormale Basis dieses Vektorraums bilden (Nielsen & Chuang, 2005, S. 13). Bei einer Messung in dieser Basis kollabiert der Zustand des Qubits in einen der Basiszustände, wobei die Beträge von α und β der Wahrscheinlichkeitsdichte entsprechen, den Wert 0 bzw. 1 zu erhalten:

$$|\langle 0|\Psi\rangle|^2 = |\alpha|^2 \qquad \text{und} \qquad |\langle 1|\Psi\rangle|^2 = |\beta|^2.$$

Der Kollaps der Wellenfunktion bewirkt insbesondere, dass eine weitere Messung in dieser Basis mit Sicherheit den gleichen Zustand wie die vorhergehende ergibt. Jegliche Information über den ursprünglichen Zustand geht somit durch die erste Messung verloren.
Für die weiteren Schritte ist darüber hinaus ein Paar von Zuständen $|+\rangle$ und $|-\rangle$ von Bedeutung, die sich wie folgt definieren lassen (vgl. Nielsen & Chuang, 2005, S. 22):

$$|+\rangle = \frac{|0\rangle + e^{i\kappa}\,|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle + e^{i(\kappa+\pi)}\,|1\rangle}{\sqrt{2}}, \qquad \text{mit } \kappa \in [0, \pi]\,. \tag{2.6}$$

Sie bilden ebenfalls eine orthonormale Basis des gleichen Vektorraumes und haben dabei die besondere Eigenschaft, mit gleicher Wahrscheinlichkeit den Zustand $|0\rangle$ und $|1\rangle$ bei einer Messung in dieser Basis zu ergeben:

$$\begin{aligned}
|\langle 0|+\rangle|^2 &= \left|\frac{1}{\sqrt{2}}\langle 0|0\rangle + \frac{1}{\sqrt{2}}e^{i\kappa}\langle 0|1\rangle\right|^2 &&= \frac{1}{2}\cdot|1+0|^2 = \frac{1}{2}\\
|\langle 1|+\rangle|^2 &= \left|\frac{1}{\sqrt{2}}\langle 1|0\rangle + \frac{1}{\sqrt{2}}e^{i\kappa}\langle 1|1\rangle\right|^2 &&= \frac{1}{2}\cdot|0+e^{i\kappa}|^2 = \frac{1}{2}\\
|\langle 0|-\rangle|^2 &= \left|\frac{1}{\sqrt{2}}\langle 0|0\rangle + \frac{1}{\sqrt{2}}e^{i(\kappa+\pi)}\langle 0|1\rangle\right|^2 &&= \frac{1}{2}\cdot|1+0|^2 = \frac{1}{2}\\
|\langle 1|-\rangle|^2 &= \left|\frac{1}{\sqrt{2}}\langle 1|0\rangle + \frac{1}{\sqrt{2}}e^{i(\kappa+\pi)}\langle 1|1\rangle\right|^2 &&= \frac{1}{2}\cdot|0+e^{i(\kappa+\pi)}|^2 = \frac{1}{2}.
\end{aligned}$$

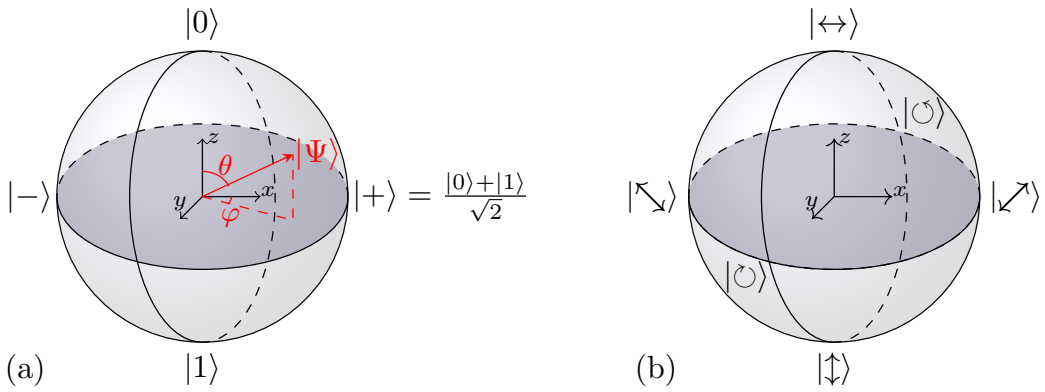


Abbildung 2.4 – Bloch- und Poincaré-Kugel.
a) Bloch-Kugel zur Veranschaulichung des Vektorraumes, in dem das Qubit im Zustand $|\Psi\rangle$ sich in einer Überlagerung der Basiszustände $|0\rangle$ und $|1\rangle$ befindet. Bei einer Messung kollabiert der Zustand $|\Psi\rangle$ in einen dieser Basiszustände. Zustände, die auf gegenüberliegenden Seiten der Kugel liegen, sind orthogonal zueinander. Zustände auf dem Äquator kollabieren mit gleicher Wahrscheinlichkeit in einen der Basiszustände $|0\rangle$ oder $|1\rangle$. Dabei ist $|\Psi\rangle = |0\rangle$ für $\theta = 0$, $|\Psi\rangle = |1\rangle$ für $\theta = \pi$ und $|\Psi\rangle = \frac{|0\rangle + e^{i\cdot\varphi}|1\rangle}{\sqrt{2}}$ für $\theta = \frac{\pi}{2}$, wobei φ jeweils beliebig ist. Insbesondere gilt: $|\Psi\rangle = |+\rangle$ für $\theta = \frac{\pi}{2}, \varphi = \kappa$ und $|\Psi\rangle = |-\rangle$ für $\theta = \frac{\pi}{2}, \varphi = \kappa + \pi$ (in der Abb. für $\kappa = 0$ eingezeichnet).
b) Poincaré-Kugel zur Veranschaulichung der konjugierten Basen des polarisierten Lichts. Jedes der drei Paare gegenüberliegender Zustände bildet dabei eine Orthonormalbasis. Operationen an den Zuständen können durch Rotation der Poincaré-Kugel dargestellt werden. Da sich jeder der eingezeichneten Zustände auf einem Äquator bezüglich der anderen beiden Basen befindet, ist das Resultat bei Messung in einer dieser anderen Basis vollkommen zufällig.

Zwei Basen mit dieser Eigenschaft werden als miteinander konjugiert bezeichnet und spielen für die Quantenkryptographie eine wichtige Rolle (s. Abschnitt 2.4).
Unter den in Gleichung (2.5) genannten Bedingungen lässt sich der den Zustand des Qubits beschreibende Einheitsvektor auch über den Winkel φ zur x- bzw. θ zur z-Achse ausdrücken:

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right) \cdot |0\rangle + e^{i\cdot\varphi} \cdot \sin\left(\frac{\theta}{2}\right) \cdot |1\rangle\,, \qquad \text{mit } \theta \in [0,\pi]\,, \varphi \in [0,2\pi]\,. \tag{2.7}$$

Dies führt zu einer anschaulichen Darstellung als Punkte in Polarkoordinaten auf der Oberfläche einer Einheitskugel, der sogenannten Bloch-Kugel (s. Abb. 2.4a, vgl. auch Nielsen & Chuang, 2005, S. 15).
Innerhalb des hier beschriebenen Versuchs werden diese theoretisch beschriebenen Zustände durch polarisiertes Licht realisiert, wie im folgenden Abschnitt dargestellt wird.

Polarisierte Photonen als Quantenbits

Um die im letzten Abschnitt eingeführten Zustände von Qubit in der Praxis umzusetzen, können neben anderen Möglichkeiten polarisierte Photonen eingesetzt werden. Eine mögliche Basis bilden dabei linear horizontal und vertikal polarisierte Photonen, wovon konventionell horizontal polarisierten Photonen im Zustand $|\leftrightarrow\rangle$ der Wert 0 und vertikal polarisierten Photonen im Zustand $|\updownarrow\rangle$ der Wert 1 zugeordnet werden. Diese Basis wird auch als rektilineare Basis (HV-Basis) bezeichnet.
Eine andere Wahl von Basiszuständen ist durch zirkular polarisierte Photonen in den Basiszuständen $|\circlearrowright\rangle$ (entspricht Wert 0) und $|\circlearrowleft\rangle$ (Wert 1) gegeben. Diese zirkulare Basis (RL-Basis) ist mit der HV-Basis konjugiert, die Zustände $|\leftrightarrow\rangle$,$|\updownarrow\rangle$ und $|\circlearrowright\rangle$,$|\circlearrowleft\rangle$ verhalten sich also zueinander so wie $|0\rangle, |1\rangle$ und $|+\rangle, |-\rangle$. Eine dritte Möglichkeit wäre die Verwendung von diagonal polarisierten Photonen, da die Diagonalbasis sowohl mit der HV- als auch der RL-Basis konjugiert ist.
Analog zur Bloch-Kugel kann auch dieser Sachverhalt auf einer Kugeloberfläche dargestellt werden, der sogenannten Poincaré-Kugel (s. Abb. 2.4b). Dies hat den Vorteil, dass Polarisationsmanipulationen als Rotation in der Poincaré-Kugel dargestellt werden können. In Bezug auf die Bloch-Kugel gilt für die Winkel der Basisvektoren:

$$|\Psi\rangle = |\leftrightarrow\rangle \quad \text{für } \theta = 0, \qquad |\Psi\rangle = |\updownarrow\rangle \quad \text{für } \theta = \pi$$
$$|\Psi\rangle = |\circlearrowright\rangle \quad \text{für } \theta = \frac{\pi}{2} \text{ und } \varphi = \frac{\pi}{2}, \qquad |\Psi\rangle = |\circlearrowleft\rangle \quad \text{für } \theta = \frac{\pi}{2} \text{ und } \varphi = \frac{3\pi}{2}$$

Für das in dieser Arbeit eingesetzte BB84-Protokoll der Quantenkryptographie werden nur zwei konjugierte Basen benötigt. Aufgrund der hier verwendeten Geräte werden dafür die HV- und RL-Basis verwendet. Die Diagonalbasis wird dagegen im weiteren Verlauf nicht mehr betrachtet, obwohl sie in manchen anderen Umsetzungen der Quantenkryptographie an Stelle der RL-Basis eingesetzt wird.

Bauteile zur Polarisationsmanipulation

Um Informationen mittels Qubits zu übertragen, ist es nötig, ihre Zustände beliebig manipulieren zu können. Werden polarisierte Photonen verwendet, kommt dafür eine Reihe von Bauteilen zum Einsatz, deren Wirkungsweise in idealisierter Form im Folgenden dargestellt ist:

Linearer Polarisator

Ein linearer Polarisator lässt nur Photonen einer bestimmten (linearen) Polarisation passieren. Photonen anderer Polarisation werden aber nicht zwingend blockiert. Wird ein Lichtstrahl mit Polarisation ϕ durch einen im Winkel χ orientierten Polarisator gesendet, werden die einzelnen Photonen mit einer Wahrscheinlichkeit von $\cos^2(\phi - \chi)$ transmittiert und mit einer Wahrscheinlichkeit von $\sin^2(\phi - \chi)$ absorbiert. Deterministisch verhalten sich die Photonen nur, wenn beide Achsen parallel (sichere Transmission) oder orthogonal (sichere Absorption) sind (Bennett & Brassard, 1984, S. 8).
Der lineare Polarisator projiziert den Zustand des eingestrahlten Photons auf den durch seinen Winkel vorgegebenen Basiszustand. Somit werden, wie im letzten Abschnitt genannt, zirkular polarisierte Photonen zu 50% transmittiert.
Schematisch ist die Wirkungsweise eines horizontal bzw. vertikal ausgerichteten Polarisationsfilters in Abb. 2.5a,b dargestellt.

Polarisations-Strahlteilerwürfel

Bei einem Polarisations-Strahlteilerwürfel (*polarising beam splitter*, PBS) werden alle horizontal polarisierten Photonen ohne Richtungsänderung transmittiert und alle vertikal polarisierten Photonen um 90° gegenüber der Einfallrichtung der Photonen reflektiert (schematisch in Abb. 2.5c dargestellt).
Wie bei einem linearen Polarisator werden dabei Photonen, die weder horizontal noch vertikal polarisiert sind, mit einer von ihrer Polarisation abhängigen Wahrscheinlichkeit transmittiert oder reflektiert. Bei linear diagonal und zirkular polarisierten Photonen beträgt diese Wahrscheinlichkeit 50%.

Verzögerungsplatten ($\frac{\lambda}{n}$-Plättchen)

Allgemein betrachtet verschiebt ein $\frac{\lambda}{n}$-Plättchen die Phase des in Richtung seiner Achse schwingenden Anteils der Lichtwelle um den n-ten Teil der Wellenlänge des Lichts. Bei bestimmten Werten von n und bestimmten Winkeln zur Polarisationsrichtung kann es dadurch auch die Polarisation gezielt in der für die QKD benötigten Weise manipulieren. Im Detail kann die Wirkungsweise eines $\frac{\lambda}{n}$-Plättchen über den Jones-Formalismus berechnet werden (s. dazu Demtröder, 2006, S. 289).

$\frac{\lambda}{2}$-Plättchen

Ein $\frac{\lambda}{2}$-Plättchen wird in diesem Zusammenhang dazu verwendet, die Polarisationsrichtung des einfallenden Lichtes um einen Winkel zwischen 0° und 180° zu ändern. Für dieser Arbeit sind solche $\frac{\lambda}{2}$-Plättchen relevant, die im 45°-Winkel zur horizontal-vertikalen Polarisation ausgerichtet sind. Sie drehen die Polarisation der einfallenden Photonen um 90°, sodass horizontal und vertikal polarisierte Photonen ineinander überführt, die Zustände $|\leftrightarrow\rangle$ und $|\updownarrow\rangle$ also vertauscht werden können (schematisch in Abb. 2.5d dargestellt). Zirkular polarisierte Photonen werden in ihrem Polarisationszustand durch ein $\frac{\lambda}{2}$-Plättchen nicht verändert.

$\frac{\lambda}{4}$-Plättchen

Ein $\frac{\lambda}{4}$-Plättchen wirkt, wenn es ebenfalls im 45°-Winkel zur horizontal-vertikalen Polarisation gestellt ist, prinzipiell ähnlich wie ein $\frac{\lambda}{2}$-Plättchen. Es wandelt jedoch die beiden Zustände der HV-Basis nicht in einander, sondern in die entsprechenden Zustände der RL-Basis um und umgekehrt. Damit der oben festgelegte Bit-Wert dieser Zustände dabei erhalten bleibt, muss für die Umwandlung von linear polarisierten Photonen in zirkular polarisierte ein $+\frac{\lambda}{4}$-Plättchen verwendet werden, zur Umwandlung von zirkular polarisierten Photonen in linear polarisierte dagegen ein $-\frac{\lambda}{4}$-Plättchen (vgl. Demtröder, 2006, S. 289).
In Abb. 2.5 sind nach dem gleichen Schema wie zuvor auch die Wirkungsweise eines $+\frac{\lambda}{4}$-Plättchen (2.5e) bzw. $-\frac{\lambda}{4}$-Plättchen (2.5f) dargestellt.

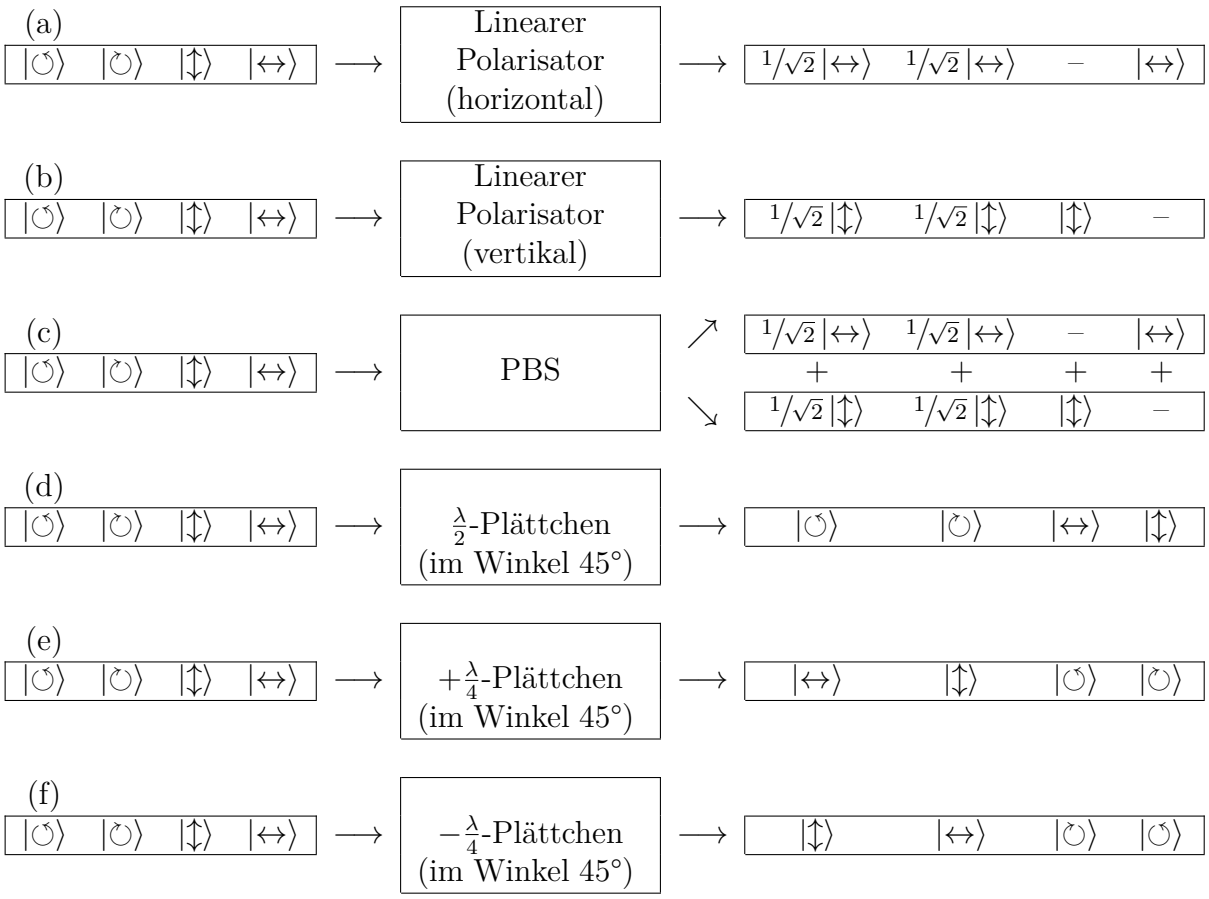


Abbildung 2.5 – Schematische Darstellung der Wirkungsweise verschiedener Bauteile zur Polarisationsmanipulation.
a) Linearer Polarisator in horizontaler Ausrichtung;
b) Linearer Polarisator in vertikaler Ausrichtung;
c) Polarisations-Strahlteilerwürfel (PBS);
d) $\frac{\lambda}{2}$-Plättchen im 45°-Winkel zur horizontal-vertikalen Polarisation;
e) $+\frac{\lambda}{4}$-Plättchen im 45°-Winkel zur horizontal-vertikalen Polarisation;
f) $-\frac{\lambda}{4}$-Plättchen im 45°-Winkel zur horizontal-vertikalen Polarisation.

Mit diesen Bauteilen ist es also möglich, eine Lichtquelle linear zu polarisieren, dann beliebige Qubit-Zustände mit $\frac{\lambda}{2}$- oder $\frac{\lambda}{4}$-Plättchen einzustellen. Genauso können über diese Plättchen in Verbindung mit Detektoren an den beiden Ausgängen eines PBS Messungen der Polarisation durchgeführt werden. Im Abschnitt 3.2 wird gezeigt, wie damit eine Übertragung nach dem BB84-Protokoll umgesetzt werden kann. Zunächst jedoch wird dieses Protokoll im nächsten Abschnitt vorgestellt.

2.4 Das BB84-Protokoll

Erste Gedanken über Quantenkryptographie gehen in die 1960er Jahre zurück, das erste kryptographische Verfahren auf Basis der Quantenmechanik wurde allerdings erst 1984 von Charles Bennett und Gilles Brassard präsentiert, woraus sich die Bezeichnung BB84-Protokoll (BB84) ergab (vgl. Singh, 2001, S. 400 ff.).

2.4.1 Prinzip des Protokolls

Wenn polarisierte Photonen als elementares Quantensystem benutzt werden, um digitale Informationen zu übertragen, erlaubt die Heisenberg'sche Unschärferelation kryptographische Systeme, die mit traditionellen Übertragungsmedien unerreichbar wären. Dazu gehört z.B. ein Übertragungskanal, der prinzipiell nicht unbemerkt abgehört werden kann, da jeder Lauschangriff die Übertragung mit hoher Wahrscheinlichkeit zu stark stört, um unbemerkt zu bleiben. Solch ein Quantenkanal kann in Verbindung mit einem gewöhnlichen ungesicherten klassischen Kanal verwendet werden, um einen Zufallsschlüssel zu übertragen, wobei sichergestellt ist, dass er für alle Anderen unbekannt bleibt (Bennett & Brassard, 1984, S. 7).
Dabei können die Nutzer, indem sie sich anschließend über einen gewöhnlichen klassischen Kanal absprechen, der sogar passiv belauscht werden darf, mit großer Sicherheit bestimmen, ob die eigentliche Quantenübertragung gestört wurde, wie es bei einem Lauschangriff der Fall wäre (selbst wenn der klassische Kanal aktiv belauscht wird, können beide Nutzer immer noch geheime Daten übertragen, wenn zu Beginn geteilte Daten vorliegen, es sei denn, die Lauscherin unterdrückt die Kommunikation komplett). Wenn die Übertragung nicht gestört wurde, kann der Zufallsschlüssel in dem *One-Time-Pad*-Verfahren Verwendung finden, um die anschließende Kommunikation zu verschlüsseln (Details dazu sind in Abschnitt 2.1 dargestellt). Wurde die Übertragung dagegen gestört, wird sie verworfen und wiederholt, wobei die eigentliche Kommunikation verschoben wird, bis genug Daten erfolgreich übertragen wurden, um daraus einen Schlüssel für das *One-Time-Pad* zu erstellen (Bennett & Brassard, 1984, S. 9).

2.4.2 Ablauf des Protokolls

Werden Senderin und Empfänger der geheimen Nachrichten wieder als Alice und Bob bezeichnet, läuft eine Übertragung mittels BB84 in fünf Schritten ab, die auch noch einmal in Abb. 2.6 illustriert sind:

1. Alice wählt eine zufällige Bit-Folge und eine zufällige Folge von Polarisationsbasen (rektilinear oder zirkular) und sendet Bob eine Kette aus Photonen. Jedes Photon repräsentiert dabei 1 Bit der Folge in der für dieses Bit gewählten Basis.

2. Wenn Bob diese Photonen empfängt, entscheidet er für jedes zufällig und unabhängig von Alice, in welcher der beiden Basen er die Polarisation misst.

3. Das Resultat der Messung interpretiert Bob als binäre 0 oder 1.

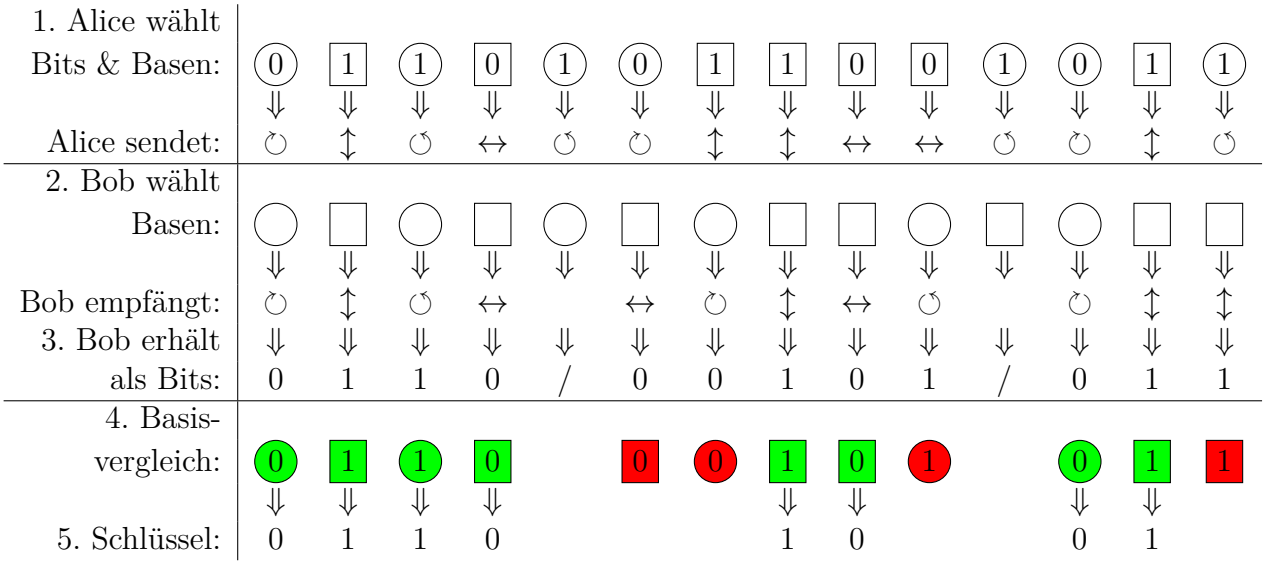


Abbildung 2.6 – Ablauf des BB84-Protokolls in 5 Schritten innerhalb von drei Phasen:
Die Senderin (Alice) übermittelt dem Empfänger (Bob) über einen Quantenkanal eine zufällige Folge von Bits in zufällig gewählten Basen (□ steht dabei für die rektilineare Basis, ◯ für die zirkulare). Bob misst in ebenfalls zufällig und unabhängig von Alice gewählten Basen und erhält daraus eine Folge von Bits (wobei es zu Übertragungsverlusten kommen kann, die mit / markiert wurden). Zuletzt vergleichen Alice und Bob die korrekt übertragenen Bits (grün markiert) und bestimmen daraus den Schlüssel.

4. Alice und Bob bestimmen zuerst, welche Photonen empfangen und welche von diesen in der korrekten Basis gemessen wurden.

5. Verlief die Übertragung ungestört, sollten die von diesen Photonen repräsentierten Bits bei Alice und Bob übereinstimmen, obwohl diese Daten niemals über einen öffentlichen Kanal verglichen wurden.

Wenn Bob die Polarisation in der falschen Basis misst, entsteht bei der Messung ein zufälliges Ergebnis, bei dem jede Information verlorengeht, wie in Abschnitt 2.3 erläutert wurde. Somit erhält Bob nur von im Mittel der Hälfte der detektierten Photonen brauchbare Daten – nämlich von denen, deren Polarisationsbasis er korrekt geraten hat. Dass nicht alle Photonen detektiert werden, geht dabei auf Unzulänglichkeiten der Geräte zurück, so können einige Photonen während der Übertragung verloren gehen oder werden durch Bobs unvollkommenen Detektoren nicht registriert (Bennett & Brassard, 1984, S. 9).
Die letzten beiden Schritte des Protokolls erfolgen über einen gewöhnlichen öffentlichen Kommunikationskanal, von dem angenommen wird, dass er zwar abgehört werden kann, aber keine Nachrichten hinzugefügt oder verändert werden können (z.B. durch Authentifizierungsverfahren). War die Übertragung erfolgreich, trägt voraussichtlich jedes Photon ein zufälliges Bit an Information (z.B. ob ein Photon in der rektilinearen Basis vertikal oder horizontal polarisiert war), welche nur Alice und Bob bekannt ist.

2.4.3 Sicherheit des Protokolls

Das Ungewöhnliche am BB84-Protokoll ist die zufällige Basiswahl von Bob. Auf den ersten Blick mag sie seltsam erscheinen – muss doch etwa die Hälfte der übertragenen Bits verworfen werden – bildet aber die Grundlage für die Sicherheit des Protokolls. Eine Lauscherin (wieder Eve) hat prinzipiell mehrere Möglichkeiten, um an Informationen zu gelangen. Wird jedoch für jedes Schlüsselbit nur ein Photon übertragen (wie in Abschnitt 2.2 beschrieben), kann sie das Signal nicht teilen, um unbemerkt Messungen durchzuführen. Da sie einen beliebigen unbekannten Quantenzustand des Photons auch nicht kopieren kann (*no-cloning-theorem*, s. auch Wootters & Zurek, 1982), bleibt ihr nur ein sogenannter *intercept-resend*-Angriff. Bei diesem unterbricht Eve die Übertragung, misst alle von Alice gesendeten Photonen und sendet identische Photonen an Bob. Da sie jedoch nicht weiß, welche Basis Alice jeweils verwendet hat, muss sie sich ebenso wie Bob zufällig entscheiden. Wählt sie die gleiche Basis wie Alice, kann sie Bob das korrekte Photon weitersenden. Bei der anderen Basis schließt Eve dagegen in der Hälfte der Fälle auf das falsche Bit und sendet Bob einen falschen Wert.
Wurde die Übertragung nicht abgehört, sollten die von Alice und Bob verglichenen Bits idealerweise zu 100% übereinstimmen. Dieser Wert kann jedoch bei realen Übertragungen nie erreicht werden, da immer Verluste bei der Übertragung oder Detektion auftreten. Nicht jede Abweichung ist also zwingend einer Lauscherin zuzuordnen, sicherheitshalber sollte aber davon ausgegangen werden. Wurde die Übertragung vollständig abgehört, sollten immer noch im Mittel 75% der verglichenen Bits übereinstimmen. Diese Zahl erklärt sich dadurch, dass Eve bei im Mittel 50% von diesen Bits die korrekte Basis gewählt hatte und somit den korrekten Bit-Wert an Bob übertragen konnte. Bei den anderen 50% hatte sie trotz falscher Basis immer noch etwa die Hälfte der Bit-Werte korrekt weitergeben können. Insgesamt wurden also $50\% + 50\% \cdot 50\% = 75\%$ der von Alice und Bob in derselben Basis gemessenen Bits von Eve richtig weitergegeben.
Wurden mehr als 88% richtig übertragen, kann der Schlüssel durch anschließende Prozesse (wie *error correction* und *privacy amplification*) soweit verbessert werden, dass eine sichere Übertragung dennoch möglich ist (vgl. W. Shor & Preskill, 2000, S. 444). In diesem Fall können die übertragenen Bits als Schlüsselblock für anschließende geheime Kommunikation per *One-Time-Pad*-Verfahren über einen öffentlichen Kanal verwendet werden. Sobald dieser Schlüsselblock verbraucht wurde, wird das Protokoll wiederholt, um eine neue Menge zufälliger Daten über den Quantenkanal zu senden (Bennett & Brassard, 1984, S. 9).
An dieser Stelle ist geklärt, wie Alice und Bob über das BB84-Protokoll und das OTP-Verfahren miteinander kommunizieren können und warum Eve sie nicht unbemerkt belauschen kann. Auch wurde beschrieben, wie polarisierte Photonen zur physikalischen Realisierung des Protokolls verwendet werden und eine Möglichkeit zum Erzeugen und Nachweisen von Einzelphotonen genannt.
Nun kann sich also der konkreten praktischen Umsetzung gewidmet werden, die mit dem in dieser Arbeit verwendeten Versuchsaufbau realisiert wurde.

Kapitel 3

Experimentelle Umsetzung

In dieser Bachelorarbeit wurde der zuletzt von Matthias Leifgen (2016) verwendete Versuchsaufbau zur QKD einerseits rekonstruiert, andererseits im Hinblick auf das F-Praktikum optimiert. Konkret wurden die Bestandteile, die in der Zwischenzeit an verschiedenen Orten eingelagert worden waren, neu zusammengesetzt. Auch wurden die beteiligten Geräte auf Funktionsfähigkeit überprüft und teilweise ersetzt, eine Sicherheitsschaltung installiert, um eine versehentliche Beschädigung der teuren und empfindlichen Einzelphotonendetektoren zu verhindern, sowie die Ansteuerung mittels *LabView* überarbeitet und vereinfacht, wobei auch die zugrunde liegende Programmierung einheitlicher und übersichtlicher gestaltet wurde.

Im Folgenden wird der durch diese Arbeit konzipierte Aufbau mit seinen Geräten und deren Ansteuerung, insbesondere im Hinblick auf die in der Umsetzung des BB84-Protokolls gestellten Anforderungen beschrieben. Anschließend werden die Ergebnisse einer beispielhaften Messung aufgeführt und diskutiert.

3.1 Aufbau

Die gesamte experimentelle Realisierung ist kompakt gestaltet, sodass der optische Aufbau in einem Kasten mit den Maßen $122 \times 60 \times 30\,\mathrm{cm}^3$ Platz findet und zusammen mit den weiteren Geräten auf einem einzigen Tisch angeordnet werden kann. Daraus ergibt sich eine Freistahlstrecke von etwa einem halben Meter zwischen den Apparaten von Senderin und Empfänger (im Folgenden wieder als Alice und Bob bezeichnet). Wenngleich eine Trennung der Apparate von Alice und Bob der Anwendungssituation eher entsprochen hätte, wurde zugunsten eines kompakten Aufbaus darauf verzichtet. Ebenfalls aus Gründen der Praktikabilität wird zur Ansteuerung aller Geräte ein einzelner Computer verwendet.

Eine Übersicht über den aktuellen Aufbau ist in Abb. 3.1b im Vergleich zu dem Aufbau von 2012 (Abb. 3.1a) dargestellt und wird im Folgenden näher erläutert. Photonen werden entweder mittels einer Laserdiode (QL65D6SA, Roithner, Treiber: iC-NZN EVAL, ic-Haus) mit einer Wellenlänge von 650 nm oder einer kompakten Einzelphotonenquelle (SPS) auf Basis von NV-Zentren erzeugt. Der Laser kann dabei entweder durchgehend Photonen im sog. Dauerstrichbetrieb aussenden oder alle 2,5 µs einzelne Pulse. Mit einem $\frac{\lambda}{2}$-Plättchen (PRM1/M, ThorLabs) wird die Polarisation dieser Photonen anschließend auf die vertikale Polarisationsrichtung eines linearen Polarisators (RSP05/M, ThorLabs) eingestellt.

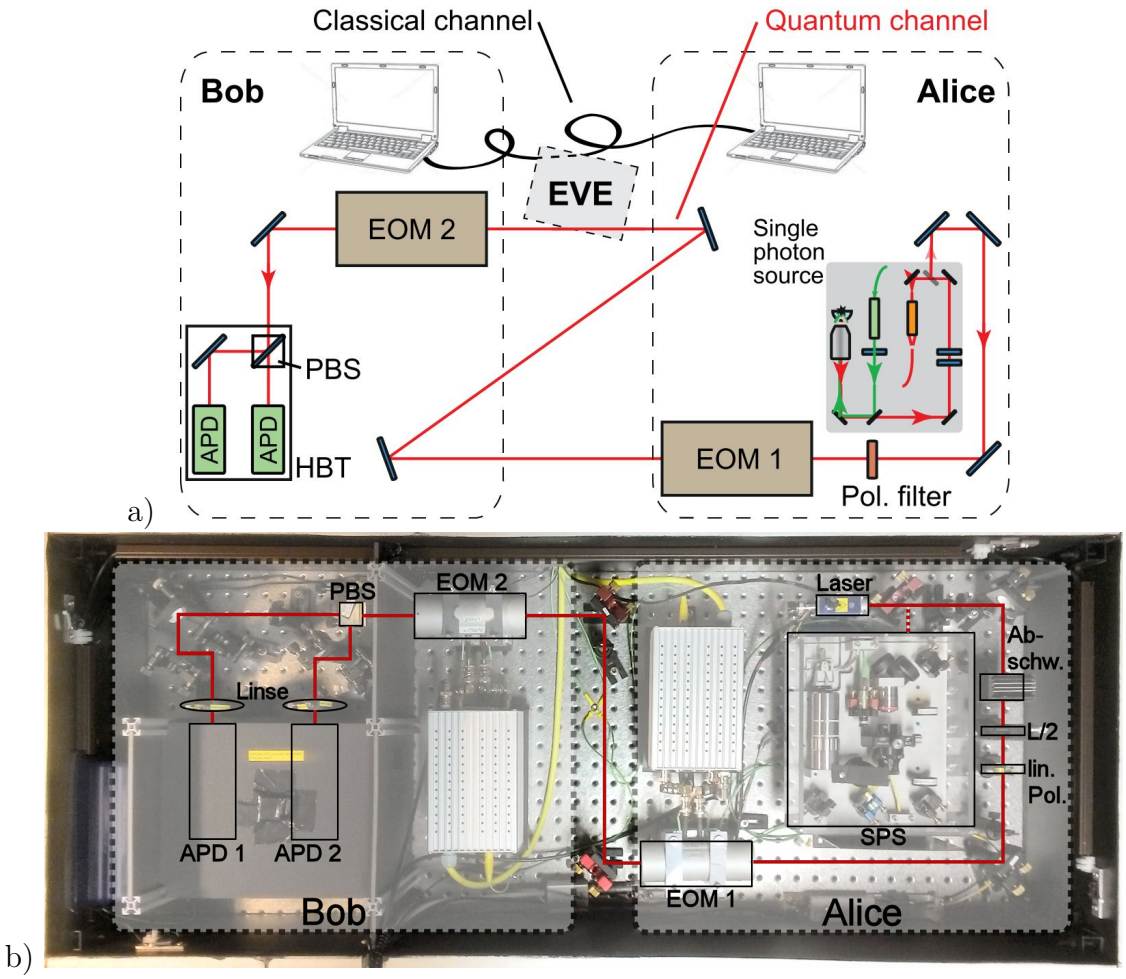


Abbildung 3.1 – Darstellung des verwendeten QKD-Aufbaus.
a) Schema des Aufbaus von 2012 (entnommen aus Schröder, 2012, S. 156);
b) Fotografische Darstellung des aktuellen Aufbaus.
Alice und Bob können über zwei Kanäle kommunizieren, Eve in beide eingreifen. Über den Quantenkanal werden Photonen eines abgeschwächten Lasers oder einer Einzelphotonenquelle (*single photon source*, SPS) gesendet. Alice stellt mit Hilfe von $\frac{\lambda}{2}$-Plättchen (L/2) und linearem Polarisator (lin. Pol.) Photonen mit definierter Polarisation bereit. Mit dem Elektrooptischen Modulator (EOM 1) kann sie Basis und Bit einstellen. Bob detektiert die über einen weiteren EOM (EOM 2) und einen Polarisations-Strahlteilerwürfel (PBS) je nach übermitteltem Bit-Wert getrennten Photonen mittels zwei Lawinenphotodioden (APDs).
Werden die EOMs so eingestellt, dass die Photonen nach EOM 2 zirkular polarisiert sind, fungiert das Ensemble von PBS und APDs als Hanbury Brown & Twiss Aufbau (HBT). Im Gegensatz zu (a) wird in dieser Arbeit und im F-Praktikums-Versuch ein einzelner Computer zur Steuerung verwendet, damit die experimentelle Komplexität reduziert werden kann.

Da alle Photonen nun dieselbe Polarisation aufweisen, können sämtliche von Alice wählbaren Bit-Werte in den zugehörigen Polarisationsbasen (vgl. Abschnitt 2.4) durch den Einsatz von $\frac{\lambda}{2}$- und $\frac{\lambda}{4}$-Plättchen realisiert werden.
Um diese Einstellung innerhalb einer möglichst kurzen Zeitspanne wechseln zu können, kommt dafür ein Elektrooptischer Modulator (EOM, im Folgenden EOM 1) auf Basis von Kaliumdideuteriumphosphat-Kristallen (LM0202 P VIS, Linos) zum Einsatz, der je nach angelegter Spannung wie ein $\frac{\lambda}{2}$- oder $\frac{\lambda}{4}$-Plättchen wirkt.

Nun verlassen die Photonen Alice's Aufbau um nach etwa einem halben Meter Freistrahlstrecke bei Bob anzukommen. Bei diesem erfolgt die Basiswahl ebenfalls über einen EOM (im Folgenden EOM 2) in Verbindung mit einem Polarisations-Strahlteilerwürfel (PBS). Der EOM lässt dabei je nach Bobs Messbasis die ankommenden Photonen in ihrer Polarisationsbasis oder vertauscht lineare und zirkulare Polarisation miteinander. Durch den PBS werden daraufhin linear polarisierte Photonen mit Sicherheit an einem von zwei Detektoren registriert, zirkular polarisierte dagegen unvorhersagbar an einem der beiden Detektoren. Details zur Messung in beiden Basen sind in Abschnitt 3.2 dargestellt. Zur Detektion der Photonen werden Lawinenphotodioden (*avalanche photodiode*, APD) auf Siliziumbasis (SPCM-AQRH-33, Excelitas) verwendet, auf die mit einer Linse fokussiert wird. Da die vom Laser ausgestrahlte Leistung für diese viel zu hoch ist und sie überlasten würde, kommen Abschwächer zur Reduktion der Laserleistung zum Einsatz.

Kompakte Einzelphotonenquelle

Die kompakte Einzelphotonenquelle wurde im Rahmen von Tim Schröders Dissertation (2012) gefertigt und ist dort ausführlich beschrieben (s. Schröder, 2012, Kapitel 8, S. 145 ff.). Eine Übersicht über den Aufbau ist in Abb. 3.2 dargestellt.

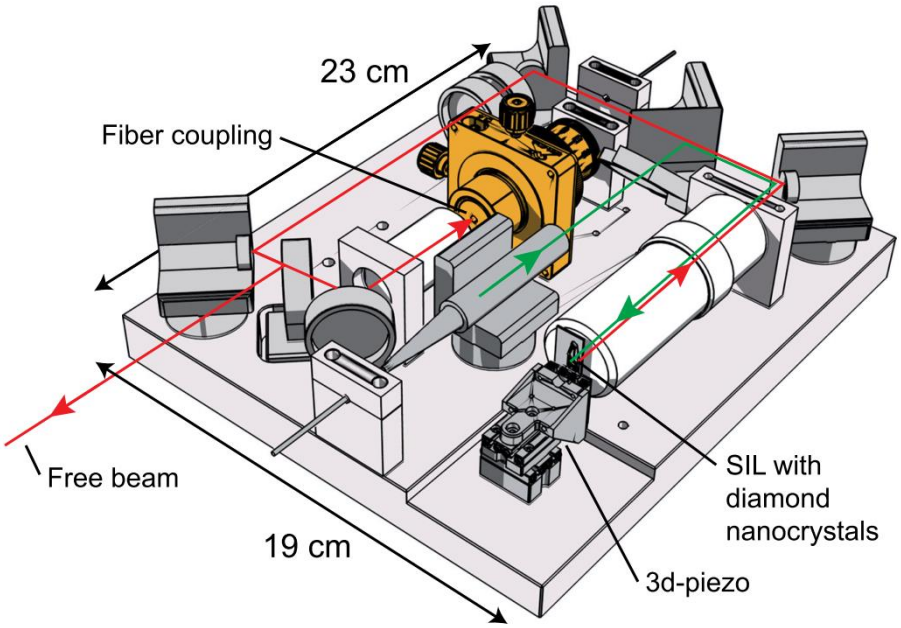


Abbildung 3.2 – Darstellung der verwendeten Einzelphotonenquelle (entnommen aus Schröder, 2012, S. 148).
Unten im Bild befindet sich die Probe mit den Naondiamanten zusammen mit der Öl-Immersionslinse (SIL) auf einem 3D-Piezo-Tisch. Der grüne Anregungslaser (532 nm) wird über eine Faser eingekoppelt, über einen dichroitischen Spiegel (nicht im Bild) durch das Objektiv auf die SIL gelenkt und regt dort ein NV-Zentrum zur Aussendung von einzelnen Photonen an. Diese können den dichroitischen Spiegel im Gegensatz zu den reflektierten Photonen des Anregungslasers ungehindert passieren und werden per Freistrahlkopplung zu Alice' Aufbau gelenkt.

Die Erzeugung der Photonen geschieht in Nanodiamanten mit NV-Defektzentren, die auf einer Öl-Immersionslinse (*solid immersion lens*, SIL) aufgebracht sind. Diese sorgt zusammen mit einem Objektiv durch einen höheren Brechungsindex zwischen Objekt und Linse für eine effizientere Aufsammlung der Photonen. Die dreidimensionale Positionierung der Probe erfolgt dabei mittels eines Piezo-Tisches (SLC-1720-S-HV, SmarAct, Treiber: MCS-3D, SmarAct). Ein 532 nm-Laser (etwa 100 µW) regt die NV-Defektzentren bei Raumtemperatur an. Um die emittierten Photonen von dem reflektierten Laserlicht zu trennen, wird ein dichroitischer Spiegel verwendet. Ein Kurzpassfilter (785 nm, im Bild nicht zu sehen) und zwei Langpassfilter (620 nm, im Bild nicht zu sehen) filtern verbleibendes Licht aus. Die Photonen der SPS können nun entweder in eine Faser eingekoppelt oder per Freistrahl weitergeleitet werden, wobei in dieser Arbeit Letzteres eingesetzt wird (vgl. Schröder, 2012, S. 146 f.).

Hanbury Brown & Twiss Aufbau

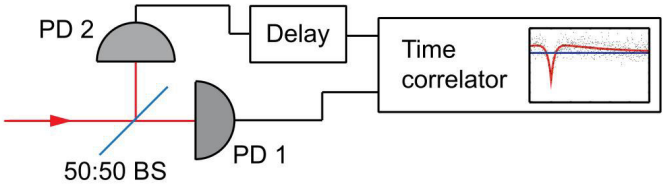


Abbildung 3.3 – Darstellung des Hanbury Brown & Twiss Aufbaus zur Bestimmung der Autokorrelation (entnommen aus Schröder, 2012, S. 11).
Die eingestrahlten Photonen werden durch einen 50:50-Strahlteiler (in der Abb. 50:50-BS) mit gleicher Wahrscheinlichkeit an einem von zwei Photodetektoren (in der Abb. PD) registriert, die eine Zeitmessung starten bzw. stoppen (in der Abb. am „Time correlator“). Einer der beiden Kanäle wird dabei gegenüber dem anderen verzögert (in der Abb. am „delay“), um eine Verschiebung des zeitlichen Nullpunktes zu erreichen.

Um eine Autokorrelationsmessung durchzuführen, kann der vorhandene Aufbau als sogenannter Hanbury Brown & Twiss Aufbau (HBT, s. auch Abb. 3.3) verwendet werden. Dieser besteht aus einem Gerät zur Zeitmessung im Nanosekundenbereich, einem 50:50-Strahlteiler, und zwei Einzelphotonendetektoren, von denen der eine als Start-, der andere als Stop-Signalgeber für die Zeitmessung fungiert. Die am Strahlteiler ankommenden Photonen werden zu gleicher Wahrscheinlichkeit an einem der beiden Detektoren registriert. Wird die Anzahl an Koinzidenzen zwischen beiden Detektoren über der zeitlichen Verzögerung τ zwischen zwei Ereignissen aufgetragen, ergibt sich ein charakteristischer Verlauf, der als Maß für die Korrelationsfunktion zweiter Ordnung $G^{(2)}(\tau)$ genommen werden kann.
Da in dem in dieser Arbeit verwendeten Aufbau zwei APDs als Detektoren und ein PBS zur Verfügung stehen, müssen lediglich beide EOMs so eingestellt werden, dass sie zusammen wie ein $\frac{\lambda}{4}$-Plättchen wirken und so am PBS einfallende Photonen mit gleicher Wahrscheinlichkeit an einer der beiden APDs registriert werden.

3.2 Umsetzung des BB84-Protokolls

In Abschnitt 2.4 wurden fünf charakteristische Schritte des BB84-Protokolls ausgemacht, die noch einmal kurz wiederholt werden sollen:

1. Alice wählt Bits und Basen;
2. Bob wählt Basen;
3. Bob empfängt Bits;
4. Vergleich der Basiswahl von Alice und Bob;
5. Bestimmung des Schlüssels.

Die Übertragung erfolgt dabei bitweise, die Schritte 1 - 3 werden also für jedes Bit separat durchlaufen. Die Schritte 4 und 5 können getrennt davon entweder schon permanent während der Übertragung oder einmalig im Anschluss durchgeführt werden. Im Folgenden wird erläutert, wie diese Schritte mit dem in dieser Arbeit verwendeten Versuchsaufbau umgesetzt werden können.

Schritt 1: Repräsentation des Bits durch die Polarisation des Photons und Basiswahl bei Alice

Zu Beginn werden durch Zufallszahlen Alice' Bit und Basis sowie Bobs Basis beim Messen festgelegt. Die Zufallszahlen werden dabei aus einer Datei eingelesen und stammen idealerweise von einem echten Zufallszahlengenerator (wie z.B. des in Leifgen et al., 2011, S. 154 ff. beschrieben). Durch einen linearen Polarisator wird sichergestellt, dass jedes Photon zu Beginn der Übertragung vertikal polarisiert ist. Diese Polarisation wird bei Alice mithilfe von EOM 1 so manipuliert, dass sie dem zu dem Bit gehörenden Basiszustand in der gewählten Basis entspricht: Will Alice Bit 0 in Basis 0 senden, belässt sie die vertikale Polarisation unverändert, für Bit 1 in Basis 0 lässt sie EOM 1 wie ein $\frac{\lambda}{2}$-Plättchen wirken, um die Polarisation um 90° zu drehen. In Basis 1 dagegen muss Alice das Photon zirkular polarisieren. Dafür stellt sie ihren EOM je nach Bit-Wert als $+\frac{\lambda}{4}$- (Bit 0) oder $-\frac{\lambda}{4}$-Plättchen (Bit 1) ein.

Schritt 2 & 3: Basiswahl und Detektion des Photons bei Bob

Bei Bob wird EOM 2 zur Basiswahl verwendet. Will Bob in der HV-Basis (Basis 0) messen, lässt er EOM 2 als $\frac{\lambda}{2}$-Plättchen wirken, was die Polarisationsbasis des Photons bestehen lässt. Will er dagegen in der RL-Basis (Basis 1) messen, wirkt sein EOM als $+\frac{\lambda}{4}$-Plättchen und wandelt zirkulare in lineare Polarisation und umgekehrt. Durch einen PBS hinter EOM 2 wird das Photon dann entsprechend seiner Polarisation an einer von zwei APDs registriert, sofern es linear polarisiert ist. Ist es dagegen zirkular polarisiert, wird es mit gleicher Wahrscheinlichkeit an einem der beiden Detektoren registriert (s. Abschnitt 2.3). Da horizontal polarisierte Photonen dabei an APD 1 registriert werden, wird der Bit-Wert 0 dieser APD zugewiesen.
Diese Einstellungen und Zuordnungen ermöglichen eine Übertragung nach den in Abschnitt 2.3 und 2.4 gezeigten Prinzipien, wie im Folgenden gezeigt wird.

- Sendet Alice Bit 0 in Basis 0, so bleibt das Photon hinter EOM 1 im Zustand $|\updownarrow\rangle$. EOM 2 wandelt diesen in $|\leftrightarrow\rangle$, sofern Bob sich ebenfalls für Basis 0 entscheidet, und in $|\circlearrowright\rangle$, falls er Basis 1 wählt. Durch Verwendung des PBS wird der Zustand $|\leftrightarrow\rangle$ mit Sicherheit an APD 1 (Bit 0) registriert, $|\circlearrowright\rangle$ dagegen zu je 50% an einer der beiden APDs.

- Sendet Alice dagegen Bit 1 in Basis 0 und misst Bob in derselben Basis, wirken beide EOMs als $\frac{\lambda}{2}$-Plättchen, wodurch das Photon im Zustand $|\updownarrow\rangle$ an APD 2 (Bit 1) registriert werden kann. Wählt Bob die falsche Basis, erhält er ein Photon im Zustand $|\circlearrowleft\rangle$, welcher durch den PBS ebenfalls zu je 50% an einer der beiden APDs registriert wird.

- Entscheidet sich Alice für Basis 1, ergibt sich an EOM 1 je nach Bit-Wert der Zustand $|\circlearrowright\rangle$ (Bit 0) oder $|\circlearrowleft\rangle$ (Bit 1). Misst Bob in Basis 0, ist das Resultat wiederum nicht vorhersagbar, bei Basis 1 misst er dagegen mit Sicherheit Alice' Bit 0 an APD 1 (da EOM 2 $|\circlearrowright\rangle$ in $|\leftrightarrow\rangle$ wandelt) bzw. Bit 1 an APD 2 (indem $|\circlearrowleft\rangle$ in $|\updownarrow\rangle$ gewandelt wird).

Schritt 4 & 5: Vergleich der Basen und Bestimmung der Fehlerrate

Während der Übertragung der Bits wird auf dem zur Steuerung verwendeten Computer eine Datei angelegt, die pro übertragenem Bit Folgendes (in der dargestellten Reihenfolge) enthält:

Basis & Bit Alice (2 Bits) | Basis Bob (2 Bits) | Detektion APD 1 & 2 (2 Bits)

Mittels eines separaten Auswertungstools (s. Abschnitt 3.3) wird damit bestimmt,

1. welche Übertragungen verworfen werden müssen, weil entweder keine oder beide APDs ein Photon detektierten,

2. welche Übertragungen verworfen werden müssen, weil Alice und Bob verschiedene Basen gewählt haben und

3. welche Fehlerrate (*quantum bit error rate*, QBER) bei den verbliebenen Übertragungen erreicht wurde.

Es ist also zu bemerken, dass der vollständige Schlüssel verglichen wird und somit nicht anschließend für eine geheime Kommunikation zur Verfügung steht. Da für den Versuch aber ein Nachweis der Funktionalität eines Schlüsselaustauschs nach BB84 im Vordergrund steht, stellt dieser Umstand kein Problem dar. Wie bei einer echten Übertragung, bei der nur etwa ein Drittel des Schlüssels verglichen wird (vgl. Bennett & Brassard, 1984, S. 9), kann auch hierbei 11% als Obergrenze für einen noch akzeptablen Wert von QBER angenommen werden (vgl. W. Shor & Preskill, 2000, S. 444).

3.3 Ansteuerung der Geräte

Field programmable gate array und *LabView*

Der gesamte Versuchsaufbau wird mittels einem *field programmable gate array* (kurz FPGA, NI-R7813, National Instruments) gesteuert, deren Programmierung mittels *LabView* (Version 2011, National Instruments) erfolgt. Zur Interaktion stehen ebenfalls zwei *LabView*-Programme zur Verfügung.

Programm „fpga3.vi“ zur Steuerung des Versuchsaufbaus und Durchführung der Übertragung

Die Programmierung des FPGA erfolgt über *LabView*, wofür das im Hintergrund laufende Programm „fpga3.vi“ zum Einsatz kommt, welches hauptsächlich in der Masterarbeit von Georg Kewitsch (2013) entstanden ist.
Die Übertragung eines Bits nimmt dabei 100 Takte des FPGA in Anspruch. Bei einer Taktrate von 40 MHz können also maximal (bei voller Effizienz der Photonenerzeugung und -detektion, sowie ohne Verluste innerhalb der Übertragungsstrecke) 400 kBit pro Sekunde übertragen werden. Die tatsächlich erreichten Werte liegen jedoch weit unterhalb dieses Maximalwertes. Die Dauer eines Taktes liegt entsprechend bei 25 ns.

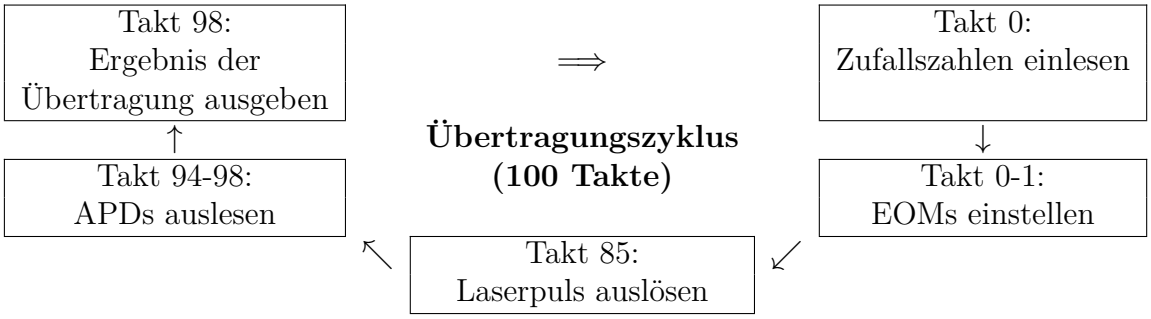


Abbildung 3.4 – Ablauf eines FPGA-Zyklus von 100 Takten.
In jeder Übertragung werden zuerst in Takt 0 Zufallszahlen, die von dem steuernden Programm „GUI.vi“ bereitgestellt werden, in das FPGA eingelesen und anhand dieser Werte die EOM-Spannungen eingestellt. In Takt 85 wird dann der Laserpuls ausgelöst und somit die optische Übertragung gestartet. Die erzeugten Photonen passieren beide EOMs, wobei sie entsprechend der gewählten EOM-Spannungen polarisiert werden. Von Takt 94 bis 98 werden die an den APDs ankommenden Photonen registriert und zuletzt in Takt 98 an das steuernde Programm ausgegeben, von dem sie gespeichert werden.

Innerhalb eines Übertragungszyklus von 100 Takten werden zu Beginn (Takt 0, vgl. auch Abb. 3.4) 4 Bit an Zufallsdaten aus dem Programm „GUI.vi“ eingelesen und die entsprechenden Spannungen für beide EOMs (als binärer Wert zwischen 0 und 1024) aus einer Liste ausgewählt, die im Vorfeld ebenfalls mit „GUI.vi“ erstellt werden muss. Diese Werte werden dann über einen Digital-Analog-Wandler in Spannungen umgewandelt und über einen Verstärker auf die EOMs gegeben. Da diese einige Zeit für die Umstellung brauchen, wartet das Programm etwa 2 µs bis Takt 85, bevor ein Signal an den Laser gesendet wird, das im gepulsten Betrieb den Puls auslöst.

9 Takte (also 225 ns) später werden 4 Takte (bzw. 100 ns) lang die APD-Signale aufgezeichnet. Dabei wird binär für jede APD getrennt gespeichert, ob (mindestens) ein Photon detektiert wurde (Bit 1) oder nicht (Bit 0). Auch wird innerhalb des Zeitraums von Takt 85 bis 99 in jedem Takt gezählt, wie viele Photonen innerhalb von 10.000 Durchläufen (also 25 ms) an jeder APD registriert wurden. Diese Werte werden in „GUI.vi“ als Histogramm dargestellt. Abschließend wird in Takt 98 das Ergebnis der Übertragung als 6 Bit langer Wert an das Programm „GUI.vi“ übergeben und von diesem zur späteren Analyse gespeichert.

Programm „GUI.vi“ zur Einrichtung der EOMs und Steuerung der QKD-Übertragung

Das Programm „GUI.vi“, das im Zuge dieser Arbeit weitgehend überarbeitet wurde, erlaubt den Wechsel zwischen Dauerstrichbetrieb und gepulstem Betrieb am Laser, die Steuerung der EOMs und zeigt die APD-Zählraten in Echtzeit an. Die Benutzeroberfläche ist in Abb. 3.5 dargestellt. An den EOMs können über eine Skala in ganzzahligen Schritten von 0 bis 1024 Spannungen im Bereich von ±250 V angelegt werden. Die detektierten Photonen werden getrennt nach den APDs in zwei Histogrammen in der Form Zählrate pro Takt aufgetragen (in der Abb. gelb markiert).
Das Programm erlaubt darüber hinaus auch Scans über den gesamten möglichen Bereich von Spannungen der EOMs (Steuerung in der Abb. grün markiert). Dabei werden für jede APD die Zählraten in Abhängigkeit von beiden EOM-Spannungen als Intensitätsverteilung dargestellt (in der Abb. rot markiert). Die EOM-Spannungen werden wiederum als ganzzahliger Wert zwischen 0 und 1024 ausgedrückt. Weiße Bereiche deuten dabei auf eine hohe, schwarze auf eine niedrige und blaue auf eine mittelhohe Zählrate hin.
Daneben wird im dritten Bild auch der Kontrast K der APD-Zählraten R_i:

$$K = \frac{|R_{\text{APD 1}} - R_{\text{APD 2}}|}{R_{\text{APD 1}} + R_{\text{APD 2}}} \tag{3.1}$$

dargestellt (in der Abb. ebenfalls rot markiert). In diesem Diagramm stehen weiße Bereiche für einen Kontrast $K \geq 90\%$ und schwarze für $K \leq 10\%$. Zur Basiswahl von Alice und Bob (s. Abschnitt 3.2) werden für die EOMs sowohl Spannungspaare mit möglichst hohem Kontrast (Paare gleicher Basen) als auch mit möglichst niedrigem Kontrast (Paare verschiedener Basen) benötigt, wozu diese Darstellung herangezogen werden kann (s. dazu auch die Darstellung in Abschnitt 3.4).
Da die ±250 V schon innerhalb der Skalenwerte 100−930 für EOM 1 und 90−930 für EOM 2 angenommen wurden, sind alle Scans auf diesen Bereich beschränkt worden. Die Dauer eines Scans ist dabei von der eingestellten Schrittweite abhängig und beträgt z.B. bei einer Schrittweite von 30 etwa eine Minute, bei einer Schrittweite von 10 dagegen schon über zehn Minuten.
Während der Übertragung stellt das Programm „GUI.vi“ die von dem FPGA benötigten Zufallszahlen bereit, die über einen Dateidialog ausgewählt werden. Echte Zufallszahlen können dabei über die Webseite der Arbeitsgruppe Nanooptik bezogen werden. Alternativ kann die Datei „sampledata-600MB.bin“ im Ausführungsverzeichnis des Programms verwendet werden. Ebenfalls speichert das Programm die durch die „fpga3.vi“ aufgenommenen Daten in einer Datei „key.bin“ zur späteren oder zeitgleichen Analyse durch „analyser_ qkd.exe“ im Ausführungsverzeichnis ab.

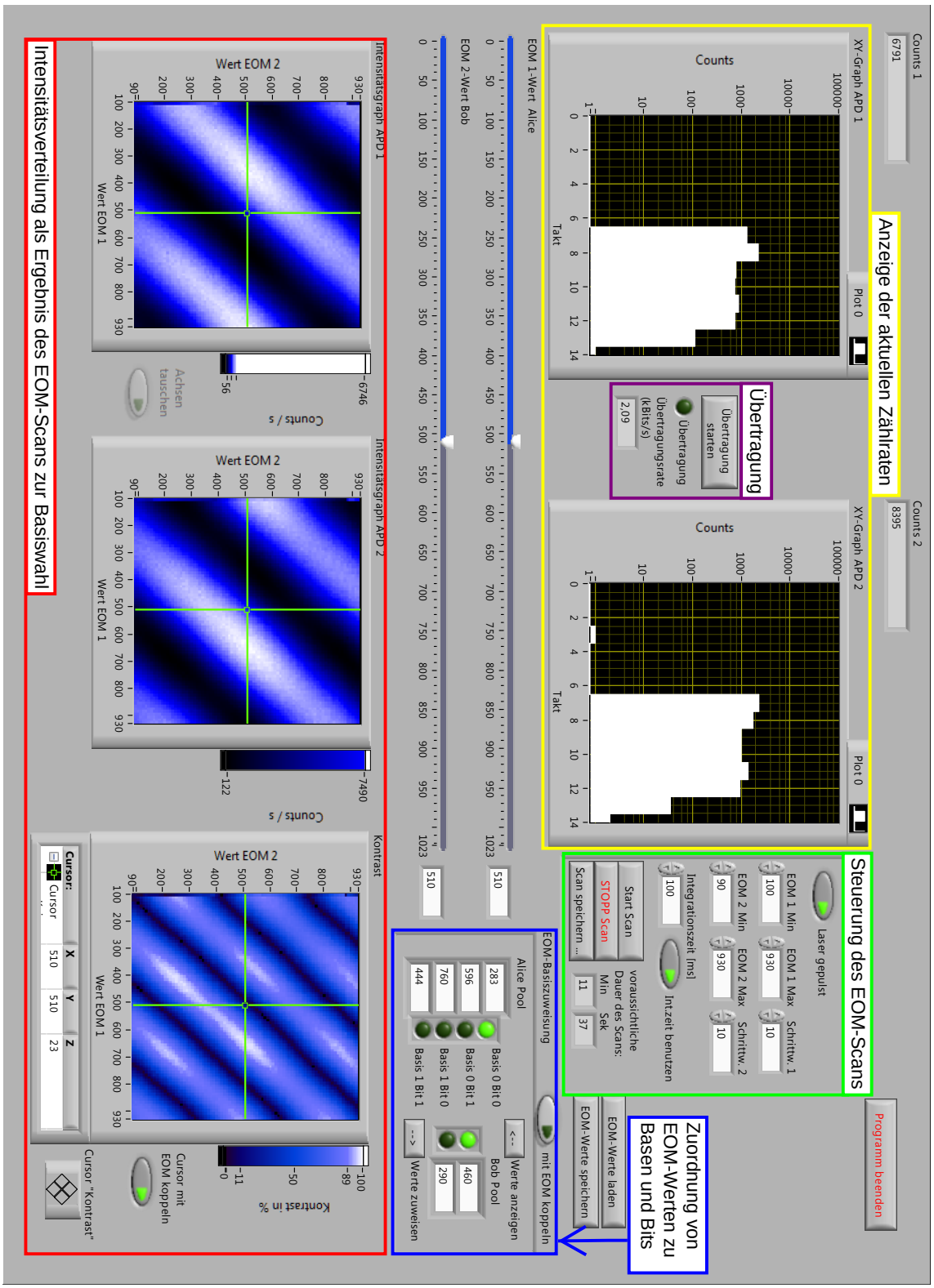


Abbildung 3.5 – Benutzeroberfläche des *LabView*-Programms „GUI.vi“.
Gelb markiert: Echtzeitanzeige der APD-Zählraten, darin (violett markiert) Steuerung der QKD-Übertragung.
Rot markiert: Darstellung der APD-Zählraten und des Kontrastes K in Abhängigkeit der EOM-Werte von EOM 1 und 2 als Ergebnis eines EOM-Scans (Steuerung dazu grün markiert). Zur manuellen Feineinstellung der EOM-Werte gibt es zwei Regler, die sich in der Mitte der Benutzeroberfläche befinden (nicht markiert). Die anschließende Zuweisung zu den Basen und Bits befindet sich ebenfalls hier (blau markiert).

Programm „ScanSoft_ SmarAct_ 2011.vi“ zur Steuerung des Piezo-Treibers

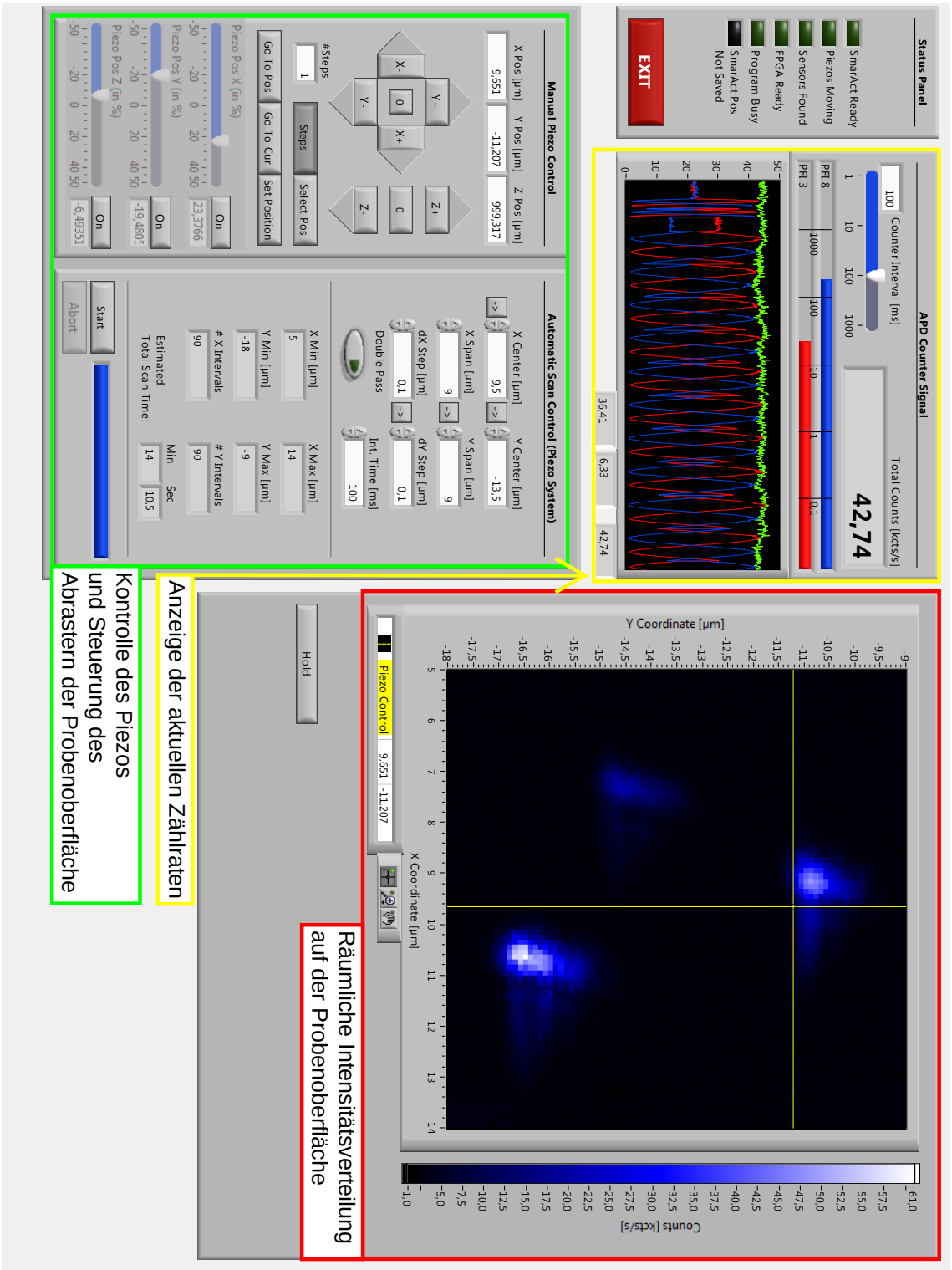


Abbildung 3.6 – Benutzeroberfläche des Programms „ScanSoft_ SmarAct_ 2011.vi“.
Gelb markiert: Echtzeitanzeige der APD-Zählraten.
Rot markiert: Darstellung der summierten Zählrate in Abhängigkeit von der räumlichen Position des Piezo-Tisches als Ergebnis eines Scans der Probenoberfläche.
Grün markiert: Positionierung des Piezo-Tisches und Steuerung des Scans.

Das innerhalb der Arbeitsgruppe entstandene Programm „ScanSoft_ SmarAct_ 2011.vi“ zur Steuerung des Piezo-Treibers wurde für diese Arbeit unverändert übernommen. Die Benutzeroberfläche ist in Abb. 3.6 dargestellt. Das Programm stellt ebenfalls die Zählrate der APDs (in der Abb. gelb markiert) einzeln und unter der Bezeichnung „Total Counts“, im Folgenden kurz C_T, in Summe dar. Neben dieser auch für eine Darstellung des Verlaufs während eines EOM-Scans nützlichen Funktion wird das Programm zur Positionierung des Piezo-Tisches mit den Nanodiamanten in allen drei Raumrichtungen x, y und z verwendet und ermöglicht auch automatische Scans (in der Abb. grün markiert). Als Ergebnis eines solchen Scans wird eine Intensitätsverteilung angezeigt, die die gemessene summierte Zählrate in Abhängigkeit von der räumlichen Position anzeigt (in der Abb. rot markiert). Weiße Bereiche deuten dabei auf ein oder mehrere NV-Zentren hin. Nach einem Scan kann die Position des Piezo-Tisches dann so eingestellt werden, dass die Photonen eines der gefundenen NV-Zentren für weitere Messungen und Übertragungen verwendet werden können.

Programm „analyser_ qkd.exe“

Die Auswertung des übertragenen Schlüssels erfolgt mittels des in der Arbeitsgruppe entstandenen Programms „analyser_ qkd.exe“. Dieses bestimmt in Echtzeit, bei wie vielen Übertragungen (jeweils als absoluter und relativer Wert)

1. an genau einer APD Photonen detektiert wurden,

2. die gleiche Basis von Alice und Bob gewählt wurde,

3. das korrekte Bit von Bob registriert wurde.

Letzteres wird dabei in Relation zu den in gleicher Basis übertragenen Bits angegeben und führt auf die Fehlerrate QBER.

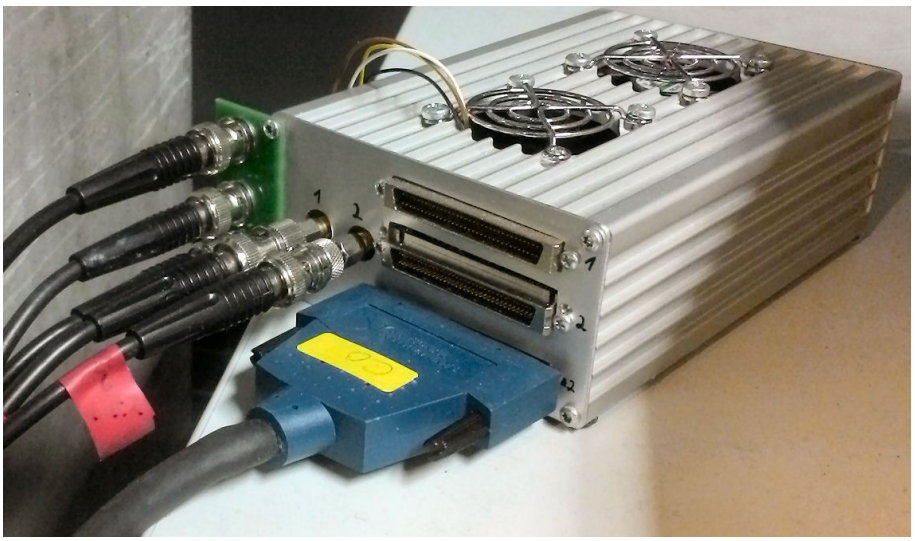
Digital-Analog-Wandler

Für die EOMs werden analoge Signale im Bereich $\pm 250\,\mathrm{V}$ benötigt. Dazu wird zuerst mittels eines in der Arbeitsgruppe hergestellten Digital-Analog-Wandlers (*digital analog converter* , DAC, dargestellt in Abb. 3.7a) das digitale Signal zwischen 0 und 1024 in eine Spannung im Bereich $\pm 5\,\mathrm{V}$ umgewandelt. Anschließend wird dieses Signal über je einen ebenfalls in der Arbeitsgruppe hergestellten Treiber pro EOM auf $\pm 250\,\mathrm{V}$ verstärkt. An dem DAC befinden sich darüber hinaus ein Anschluss zum Auslösen des Lasers im gepulsten Betrieb sowie die Eingänge für die APD-Signale.

SmarAct-Piezo-Treiber

Der Piezo-Tisch zur Positionierung der Nanodiamanten wird über einen Piezo-Treiber (MCS-3D, SmarAct, dargestellt in Abb. 3.7b) gesteuert, der über einen USB-Anschluss mit dem Computer verbunden werden oder manuell bedient werden kann.

(a)



(b)

Abbildung 3.7 – Foto des Digital-Analog-Wandlers und des Piezo-Treibers.
a) Digital-Analog-Wandler mit Anschluss an den PC (unten) und zu den EOMs (links davon, markiert mit „1“ und „2“) sowie zu APD 1 und 2 und dem Laser (ganz links, Benennung von unten nach oben).
b) Piezo-Treiber mit digitaler Anzeige der Position des Piezo-Tisches in drei Raumrichtungen. Einheit der Anzeige sind nm, das „,“ fungiert als Tausender-Trennzeichen.

TimeHarp

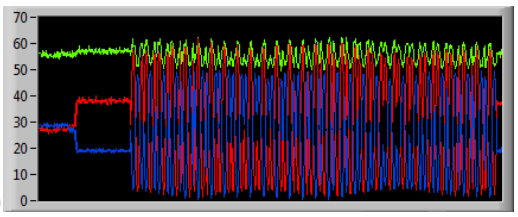
Für die Autokorrelationsmessung der SPS mittels des Hanbury Brown & Twiss Aufbaus kommt eine *TimeHarp*-Karte (TimeHarp200, PicoQuant) zum Einsatz, die über ein dazugehöriges Programm gesteuert wird. Dazu werden die APDs von dem Digital-Analog-Wandler getrennt und direkt an die *TimeHarp*-Karte angeschlossen. Damit der PBS als 50:50-Strahlteiler wirkt, müssen die EOMs so eingestellt werden, dass beide APD-Signale möglichst gleich sind. Vor einer Messung müssen dabei die Einstellungen „Level“ für den „Sync“-Kanal und „ZeroCr.“ sowie „Discr.“ für den „CFD“-Kanal im „TimeHarp Control Panel“ angepasst werden. Die angezeigte Zählrate sollte in etwa der von ScanSoft entsprechen, ggf. müssen auch die EOM-Spannungen nachjustiert werden (bis beide Kanäle im *TimeHarp*-Programm etwa gleich viele Counts zeigen). Der zeitliche Nullpunkt $\tau = 0$ kann bestimmt werden, indem eine APD per T-Stück an beide Kanäle angeschlossen wird. Mit diesem Aufbau kann anschließend die Autokorrelation $G^{(2)}(\tau)$ gemessen werden.

3.4 Exemplarische Übertragung und Auswertung der Messergebnisse

Die im Folgenden dargestellten Messungen sollen die Funktionsfähigkeit der verwendeten Geräte und Ansteuerung nachweisen. Auch können sie exemplarische Vergleichswerte für Versuchsdurchführungen im Rahmen des F-Praktikums geben. Als Grundlage für spätere Versuchsbetreuende wird in der Beschreibung der Durchführung und Beurteilung der einzelnen Ergebnisse dabei sehr detailliert vorgegangen.
Die Übertragungen unter Verwendung des Lasers und der Einzelphotonenquelle wurden innerhalb eines Tages direkt hintereinander ausgeführt, was in etwa 3,5 Stunden in Anspruch nahm. Für die Autokorrelationsmessungen an den drei zur Übertragung verwendeten NV-Zentren werden dagegen Daten verwendet, die schon früher aufgenommen und ausgewertet wurden. Da NV-Zentren in Diamant langzeitstabil emittieren, kann eine daraus resultierende Abweichung ausgeschlossen werden (vgl. Aharonovich et al., 2011, S. 3).

Einrichtung der Übertragung unter Verwendung des Lasers

Zu Beginn wurde der Laser im Dauerstrichbetrieb gestartet. Alle Abschwächer wurden entfernt, wodurch der Laserpunkt auf einem Schirm (hier wurde ein Stück Papier verwendet) mit bloßem Auge gut wahrnehmbar war. Nun konnte mit Hilfe von vier den Strahlengang markierenden Irisblenden die Ausrichtung der Spiegel nachjustiert werden, um zu gewährleisten, dass die EOMs gerade durchquert und die APDs mittig getroffen wurden.
Anschließend wurden Abschwächer mit einer Gesamtabschwächung von $A = 10^{9,0}$ in den Strahlengang gestellt und der Deckel des Kastens geschlossen. Nach Einschalten der APDs zeigte das Programm „ScanSoft_ SmarAct_ 2011.vi“ eine Gesamtzählrate von $C_T = 55 \pm 2\,\mathrm{kcts/s}$ für beide APDs an. Die angegebene Unsicherheit bezieht sich dabei auf Schwankungen in der Anzeige während des Ablesens. Innerhalb der folgenden halben Stunde erhöhte sich dieser Wert auf etwa $C_T = 65 \pm 2\,\mathrm{kcts/s}$, was vermutlich auf Schwankungen in der Leistung des Lasers zurückgeführt werden kann. Daher empfiehlt es sich im F-Praktikum, den Laser eine Weile vor Beginn der Messungen (0,5 bis 1 h) im Dauerstrichbetrieb einzuschalten, damit sich die Leistung bis zu den Messungen stabilisiert. Die meisten Scans und vor allem die Übertragungen wurden allerdings jeweils innerhalb weniger Minuten durchgeführt, sodass die Gesamtzählrate als konstant (im Rahmen der angegebenen Unsicherheit) in diesem Zeitraum angesehen werden kann.
Zur Überprüfung des Strahlenganges wurde mit dem Programm „GUI.vi“ ein grober Scan (bei einer Schrittweite von je 30 EOM-Werten) durchgeführt, anschließend nachjustiert und erneut gescannt. Der erste Scan (Abb. 3.8a) zeigt deutliche Unterschiede zwischen den Maximalwerten beider Zählraten. Die Maxima von APD 1 (blau) liegen durchgehend unter denen von APD 2 (rot) und die Gesamtzählrate (grün) weist starke Schwankungen auf. Dies deutet darauf hin, dass der Strahlengang noch nicht optimal ist und nachjustiert werden muss. Auch treten leichte periodische Schwankungen der Zählraten innerhalb einer APD auf, die auf den linearen Polarisator zurückgeführt werden können. Die Schwankungen sind in diesem Scan allerdings nicht erheblich und bezüglich der Stellung des linearen Polarisators minimal. Bei stärkeren Schwankungen sollte dagegen erst am linearen Polarisator, dann am $\frac{\lambda}{2}$-Plättchen nachjustiert werden.

(a) 

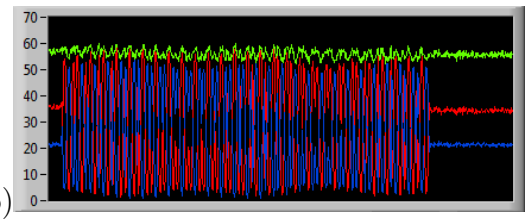
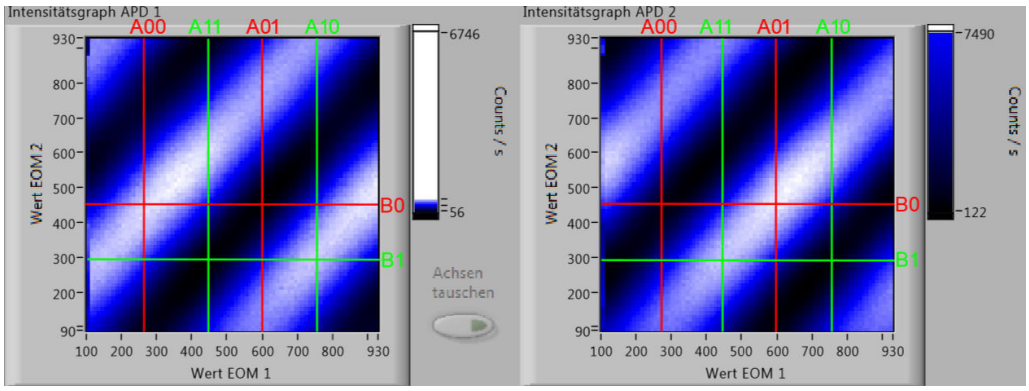
(b) 

Abbildung 3.8 – APD-Zählraten vor und nach der Justage des Strahlenganges.
a) Der grobe Scan über der EOMs zeigt, dass die Maxima von APD 1 (blau) durchgehend deutlich unter denen von APD 2 (rot) liegen. Die Gesamtzählrate (grün) schwankt dabei stark. Dies deutet darauf hin, dass APD 1 noch nicht mittig getroffen wird.
b) Nach der Justage des Strahlenganges liegen beide Signale annähernd gleich auf. Die Schwankungen innerhalb einer APD sind dabei noch nicht so stark, dass ein Nachjustieren des linearen Polarisators nötig wäre.

Nachdem der Strahlengang erneut justiert wurde (Abb. 3.8b), liegen die Maxima von APD 1 zwar weiterhin unter denen von APD 2, allerdings in einem tolerierbaren Maße. Dieser kleine Unterschied wird vermutlich durch mehr Streulicht auf APD 2 verursacht, das aus der Geometrie des Aufbaus resultiert.

Anschließend konnte ein feiner EOM-Scan (Schrittweite 10 EOM-Werte) zur Basiswahl durchgeführt werden, dessen Ergebnis in Abb. 3.9 zu sehen ist. Anhand dieses Scans wurden die Spannungen festgelegt, die für die folgenden Schlüsselübertragungen an EOM 1 (Alice' EOM) und EOM 2 (Bobs EOM) zur Übertragung des jeweiligen Bits in der jeweiligen Basis benötigt wurden (vgl. Abschnitt 3.2). Die EOM-Spannungen wurden dabei so gewählt, dass sich bei gleicher Basiswahl von Alice und Bob sehr geringe Zählraten an APD 1 bei Bit 0 bzw. APD 2 bei Bit 1 ergaben. Bei verschiedenen Basen traten dagegen annähernd gleiche Zählraten an beiden APDs auf. Im ersten Fall wurde somit ein möglichst hoher, im zweiten ein möglichst niedriger Kontrast erreicht (vgl. dazu Tab. 3.1). Wie in Abschnitt 3.2 dargestellt, erlauben die EOMs somit genau dann eine eindeutige Identifizierung des von Alice gesendeten Bits bei Bob, wenn er die gleiche Basis verwendet. Sonst ist das Ergebnis von Bob absolut zufällig.
Die Ermittlung des Kontrastes erfolgte nach Gleichung (3.1). Die Unsicherheit ergab sich anhand einer Gauß'schen Fehlerfortpflanzung aus den Unsicherheiten der Zählraten.

(a)



(b)

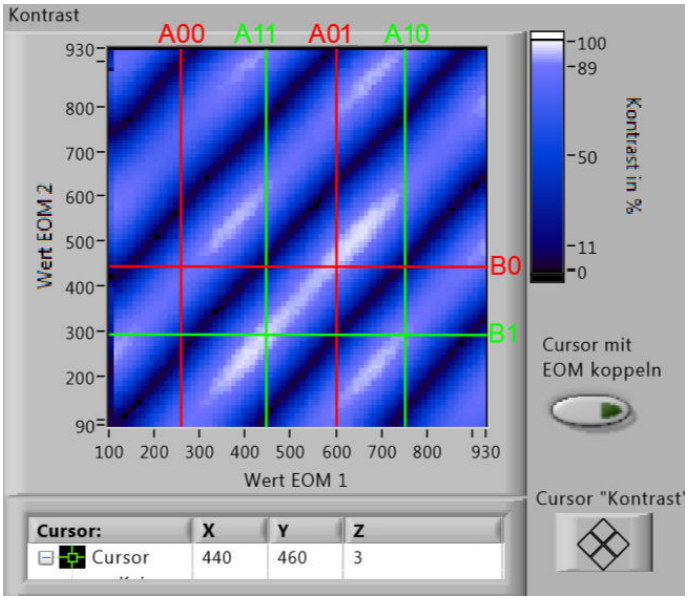


Abbildung 3.9 – EOM-Scan zur Basiswahl.
Als Ergebnis des EOM-Scans zeigt das Programm „GUI.vi“ sowohl die Intensitätsgraphen der APDs (in der Abb. a) als auch den sich daraus ergebenen Kontrast K (in der Abb. b) an. Zur besseren Übersicht wurde das Kontrastdiagramm in dieser Abb. getrennt von den Intensitätsgraphen dargestellt. Darüber hinaus sind die Alice und Bob zugeordneten EOM-Werte in rot (Basis 0) und grün (Basis 1) eingezeichnet und entsprechend beschriftet („A“ für Alice, „B“ für Bob gefolgt von den Werten für Basis und (bei Alice) Bit. Die Werte können einschließlich der dort gemessenen Zählraten bzw. dem Kontrast im einzelnen Tab. 3.1 entnommen werden.
An den Kreuzungspunkten, welche die gleiche Basis für Alice und Bob repräsentieren (A00B0, A01B0, A10B1 und A11B1), ist eines der beiden APD-Signale nahe seiner maximalen Zählrate (weiß in der Farbskala von a), während das andere sich nahe seiner minimalen Zählrate (schwarz in der Farbskala von a) befindet. Ist die Zählrate von APD 1 maximal, wird der Wert dem Bit 0 zugeordnet, sonst Bit 1.
Die Kreuzungspunkte, die verschiedene Basen von Alice und Bob repräsentieren (A00B1, A01B1, A10B0 und A11B0), weisen dagegen etwa gleiche Zählraten für beide APD-Signale auf (blau in der Farbskala von a, schwarz in der Farbskala von b).

Alice			Bob		Zählrate an		Kontrast
Basis	Bit	EOM-Wert	Basis	EOM-Wert	APD 1 (in kcts/s)	APD 2 (in kcts/s)	K (in %)
0	0	283	0	460	56 ± 2	$3{,}3 \pm 0{,}3$	89 ± 1
0	1	596	0	460	$1{,}0 \pm 0{,}1$	61 ± 2	97 ± 1
1	0	760	0	460	30 ± 1	30 ± 1	0 ± 3
1	1	444	0	460	29 ± 1	31 ± 1	3 ± 3
0	0	283	1	290	28 ± 1	30 ± 1	3 ± 3
0	1	596	1	290	28 ± 1	30 ± 1	3 ± 3
1	0	760	1	290	54 ± 2	$3{,}3 \pm 0{,}3$	90 ± 2
1	1	444	1	290	$0{,}9 \pm 0{,}3$	59 ± 2	97 ± 1

Tabelle 3.1 – EOM-Scan zur Basiswahl unter Verwendung des Lasers.
Ergänzend zu Abb. 3.9 stellt diese Tabelle dar, welche EOM-Werte den einzelnen Basen und Bits von Alice und Bob zugeordnet wurden, welche Zählraten dabei an beiden APDs gemessen wurden und welcher Kontrast sich daraus ergab.

Durchführung der Übertragung unter Verwendung des Lasers im Dauerstrich- und gepulstem Modus

Nachdem die im letzten Abschnitt beschriebenen Vorbereitungen getroffen wurden, konnte mit der Schlüsselübertragung begonnen werden. Dazu wurden sowohl der Betriebsmodus des Lasers als auch die Abschwächung variiert. Tab. 3.2 führt die dabei erreichten Übertragungs- und Fehlerraten für eine Abschwächung von 9,0 Größenordnungen im Dauerstrichbetrieb und für Abschwächungen zwischen 6,0 und 9,0 Größenordnungen im gepulsten Betrieb auf. Die angegebene Unsicherheit der Übertragungsrate bezieht sich dabei auf Schwankungen der Anzeige während des Ablesens. Die Fehlerrate wurde nach etwa 100 ± 10 kBit mittels des Programms „analyser_ qkd.exe“ bestimmt und wird ohne Unsicherheit angegeben, da es sich um einen relativen Wert bezogen auf den Datensatz der entsprechenden Übertragung handelt.

Modus	A	C_T (in kcts/s)	R (in kBits/s)	QBER (in %)
gepulst	$10^{6,0}$	430 ± 3	162 ± 2	4,98
gepulst	$10^{6,5}$	152 ± 2	61 ± 1	5,98
gepulst	$10^{7,0}$	50 ± 1	$20{,}7 \pm 0{,}4$	6,01
gepulst	$10^{7,5}$	$13{,}7 \pm 0{,}5$	$5{,}9 \pm 0{,}1$	6,53
gepulst	$10^{8,0}$	$5{,}5 \pm 0{,}3$	$2{,}40 \pm 0{,}05$	7,14
gepulst	$10^{8,5}$	$1{,}8 \pm 0{,}2$	$0{,}72 \pm 0{,}01$	8,17
gepulst	$10^{9,0}$	$0{,}7 \pm 0{,}1$	$0{,}28 \pm 0{,}02$	10,09
Dauerstrich	$10^{9,0}$	65 ± 2	$2,07 \pm 0{,}03$	6,33

Tabelle 3.2 – Übertragungs- und Fehlerraten bei verschiedenen Abschwächungen und Betriebsmodi des Lasers.
Geordnet nach Betriebsmodus und Abschwächung A sind die Gesamtzählrate C_T beider APDs sowie die in der Übertragung erreichte Übertragungsrate R und Fehlerrate QBER dargestellt.

Betrachtet man bei den Ergebnissen zuerst die Abhängigkeit der summierten Zählrate C_T von Modus und Abschwächung A, so fällt auf, dass die Zählrate im gepulsten Modus um etwa zwei Größenordnungen kleiner als im Dauerstrichbetrieb ausfällt. Erwartungsgemäß nimmt die Zählrate dabei pro Größenordnung, die in der Abschwächung dazu kommt, um ebenfalls etwa eine Größenordnung ab.
Die Übertragungsrate R verhält sich im gepulsten Modus ähnlich wie die Zählrate C_T, ein proportionaler Zusammenhang zwischen beiden Größen wirkt naheliegend. Dies steht in guter Übereinstimmung mit den Erwartungen: Je mehr Photonen insgesamt registriert werden, umso mehr Bits können auch übertragen werden. Im Dauerstrichbetrieb ist die Übertragungsrate dagegen erheblich (etwa eine Größenordnung) kleiner, als bei gleicher Zählrate im gepulsten Betrieb.
Alle Einstellungen weisen eine Fehlerrate QBER auf, die zwischen 4,98% und 10,09% und somit unter der in Abschnitt 2.4 benannten Obergrenze von 11% liegt, kämen also in Hinblick auf diesen Punkt für für eine Anwendung in der QKD in Frage. Im gepulsten Betrieb werden dabei niedrigere Fehlerraten als im Dauerstrichbetrieb bei gleichen Zählraten erreicht, des Weiteren nimmt die Fehlerrate mit abnehmender Zählrate zu. Für eine Anwendung in der QKD ist somit der gepulste Betrieb geeigneter als der Dauerstrichbetrieb.

Einrichtung und Durchführung der Übertragung unter Verwendung der Einzelphotonenquelle

Nachdem die Übertragung mit dem Laser abgeschlossen war, konnte die Einzelphotonenquelle (SPS) in Betrieb genommen werden. Dafür wurden alle Abschwächer aus dem Strahlengang entfernt, der Laser ausgeschaltet und ein optionaler Spiegel mit magnetischem Halter zwischen Laser und erste Irisblende gestellt. Anschließend wurden die Langpassfilter aus dem Aufbau entfernt und der Piezo-Tisch auf etwa 1.000.000 nm in z-Richtung gefahren (s. dazu Abschnitt 3.3). Der nun eingeschaltete Anregungslaser erzeugte dadurch einen grünen Laserpunkt, der mit bloßem Auge auf einem Schirm wahrgenommen werden konnte. Mit diesem wurde die SPS bezüglich der ersten beiden Irisblenden in den durch den Laser vorgegebenen Strahlengang eingekoppelt. Bei geschlossenem Kastendeckel und mit wieder eingesetzten Langpassfiltern ergab sich an den APDs lediglich ein schwaches Signal mit einer Gesamtzählrate von $C_T = 2{,}0 \pm 0{,}2\,\mathrm{kcts/s}$, da die Position des Piezo-Tisches noch nicht auf ein NV-Zentrum ausgerichtet wurde. Aus diesem Grund wurde anschließend im Programm „ScanSoft_ SmarAct_ 2011.vi“ ein grober Scan der Probe in der xy-Ebene durchgeführt, um NV-Zentren zu finden. Als höchste Zählrate ergab sich dabei an den Koordinaten $(-1{,}3\,\mu\mathrm{m}; -3{,}6\,\mu\mathrm{m}; 999{,}8\,\mu\mathrm{m})$ ein Wert von $79 \pm 2\,\mathrm{kcts/s}$. Dieser Punkt wird im Folgenden als „NV 1“ bezeichnet und ist in Abb. 3.10a zu sehen. Die z-Position des Piezo-Tisches wurde im Folgenden nicht mehr verändert, die z-Koordinate wird aus diesem Grund nicht mehr gesondert angegeben. Eine Abschätzung der Unsicherheit erwies sich als schwierig, da die Anzeigegenauigkeit deutlich über der Langzeitpositionsgenauigkeit lag, bei der sich teilweise Abweichungen von 0,2 µm bis zu 2 µm im Zeitraum von zwei Monaten ergaben. Die Koordinaten dienen somit eher einer groben Orientierung und eignen sich nicht für einen direkten Vergleich mit Messungen im F-Praktikum.
Bei der Wahl der EOM-Spannungen für Alice und Bob wurde von den unter dem Laser ermittelten Werten ausgegangen. Anschließend wurden die Werte von Alice bezüglich der Zählraten bei verschiedenen Basen von Alice und Bob optimiert.

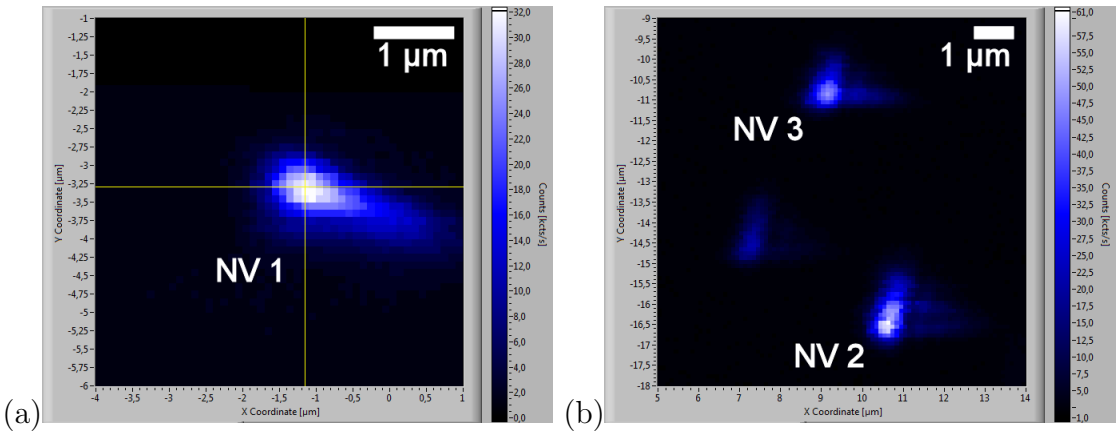


Abbildung 3.10 – NV-Zentren, die zur Übertragung verwendet wurden.
a) NV-Zentrum „NV 1“ an den Koordinaten (−1,3 µm; −3,6 µm). Die Zählrate betrug abweichend zur Abb. 79 ± 2 kcts/s, lediglich zum Zeitpunkt des Scans war sie mit 28 ± 1 kcts/s geringer, da anschließend noch einmal nachjustiert wurde.
b) Drei NV-Zentren, wobei im Folgenden am Zentrum „NV 2“ an den Koordinaten (11,2 µm; −16,9 µm) und „NV 3“ an den Koordinaten (9,6 µm; −11,2 µm) Übertragungen durchgeführt wurden.

Die sich ergebenen Werte und Zählraten sind in Tab. 3.3 dargestellt. Die Unsicherheit des Kontrasts wurde auch hier per Gauß'scher Fehlerfortpflanzung aus den Unsicherheiten der Zählraten ermittelt.

Alice			Bob		Zählrate an		Kontrast
Basis	Bit	EOM-Wert	Basis	EOM-Wert	APD 1 in kcts/s	APD 2 in kcts/s	K in %
0	0	268	0	460	73 ± 3	3,5 ± 0,5	91 ± 2
0	1	615	0	460	1,2 ± 0,2	78 ± 2	97 ± 1
1	0	775	0	460	39 ± 1	39 ± 1	0 ± 2
1	1	426	0	460	38 ± 1	38 ± 1	0 ± 2
0	0	268	1	290	39 ± 1	39 ± 1	0 ± 2
0	1	615	1	290	39 ± 1	39 ± 1	0 ± 2
1	0	775	1	290	74 ± 2	4,8 ± 0,5	88 ± 2
1	1	426	1	290	2,2 ± 0,5	80 ± 1	95 ± 2

Tabelle 3.3 – EOM-Scan zur Basiswahl unter Verwendung der Einzelphotonenquelle. Analog zu Tab. 3.1 unter Verwendung des Lasers stellt diese Tabelle zum einen dar, welche EOM-Werte den einzelnen Basen und Bits von Alice und Bob zugeordnet wurden, zum anderen, welche Zählraten dabei an beiden APDs gemessen wurden.

Im Vergleich zur Basiswahl mit dem Laser sind alle Zählraten dabei höher. Allerdings ist auch die zuvor bestimmte Gesamtzählrate C_T für die SPS höher als für den Laser. Der Kontrast stimmt im Rahmen der Unsicherheit mit den am Laser erhaltenen Werten überein.

Mit dem so eingestellten Aufbau wurden für NV 1 - 3 Übertragungen durchgeführt, wie in Tabelle 3.4 zu sehen ist.
Die Gesamtzählrate C_T ist dabei bei NV 1 am höchsten, bei NV 2 niedriger und

NV-Zentrum	Koordinaten $(x;y)$ in µm	C_T (in kcts/s)	R (in kBits/s)	QBER (in %)
NV 1	$(-1{,}3;-3{,}6)$	79 ± 1	$2{,}64 \pm 0{,}03$	6,29
NV 2	$(11{,}2;-16{,}9)$	55 ± 5	$1{,}76 \pm 0{,}04$	7,36
NV 3	$(9{,}6;-11{,}2)$	42 ± 2	$1{,}42 \pm 0{,}02$	6,93

Tabelle 3.4 – Übertragungs- und Fehlerraten bei verschiedenen NV-Zentren.
Für drei NV-Zentren sind neben den Koordinaten die summierte Zählrate (C_T) sowie die in der Übertragung erreichte Übertragungsrate R und Fehlerrate QBER dargestellt.

bei NV 3 am niedrigsten. Die unter dem Laser im Dauerstrichbetrieb erreichte Gesamtzählrate (65 ± 2 kcts/s) liegt dabei zwischen den an NV 1 und NV 2 erreichten Werten. Dies lässt einen gewissen Vergleich zwischen dem Laser im Dauerstrichbetrieb und der SPS zu, die ebenfalls im Dauerstrichbetrieb verwendet wurde.
Die Übertragungsraten R sind denen des Lasers im Dauerstrichbetrieb vergleichbar und liegen somit ebenfalls deutlich unter den bei ähnlichen Zählraten im gepulsten Betrieb erreichten.
Die Fehlerraten QBER liegen mit 6,29% bis 7,36% ebenso wie beim Laser unter der in Abschnitt 2.4 benannten Obergrenze von 11%. Die Übertragungsrate ähnelt der des Lasers im Dauerstrichbetrieb. Auffällig ist, dass für NV 3 ein geringerer Fehler als bei NV 2 auftritt, obwohl sowohl Zähl- als auch Übertagungsraten unter den Werten von NV 2 liegen. Da NV 2 allerdings eine höhere Schwankung in der Zählrate aufweist, könnte darin ein Zusammenhang mit dem höheren Fehler in der Übertragung vermutet werden. Im Vergleich zu den beim Laser ermittelten Fehlerraten ordnen sich die Werte für NV 1 und NV 3 gut in die Reihe von bei ähnlichen Zählraten aufgenommenen Werten ein, lediglich für NV 2 ist die Fehlerrate höher als im Vergleich zu erwarten gewesen wäre.

Überprüfung der Autokorrelation

Um den Einzelphotonencharakter der NV-Zentren zu überprüfen, wurde mittels des Programms *TimeHarp* die Autokorrelation der Photonen in einem Hanbury Brown & Twiss Aufbau (HBT) bestimmt.
Als Ergebnis der Messung sind in Abb. 3.11 die Verläufe der Autokorrelationsfunktionen dargestellt. Für die Anpassung (in der Abb. rot eingezeichnet) wurde dabei $g^{(2)}(\tau)$ nach Gleichung (2.4) in leicht abgewandelter Form verwendet:

$$f(x) = C_1 \cdot g^{(2)}\left(|x - x_0|\right) + C_0 = C_1 \cdot \left(1 - (K+1)\, e^{k_+|x-x_0|} + K e^{k_-|x-x_0|}\right) + C_0 \tag{3.2}$$

Die Konstante C_0 gibt dabei den unkorrelierten Untergrund an, da in der Messung die Koinzidenzen im Nullpunkt x_0 nicht auf Null abfallen. Da dieser Nullpunkt bei der Messung verschoben wurde, ist es nötig, als Argument der $g^{(2)}$-Funktion den Abstand $|x - x_0|$ zu diesem Punkt zu verwenden. Die Konstante C_1 entspricht dem Quadrat der mittleren Intensität $|\langle I \rangle|^2$ in Gleichung (2.2) und trägt der Tatsache Rechnung, dass die Messergebnisse unnormiert und somit ein Maß für $G^{(2)}(\tau)$ und nicht $g^{(2)}(\tau)$ sind.

Die Summe $C_1 + C_0 = C_1'$ kann bei der Anpassung vorgegeben werden und dafür über die Zählraten R_i an APD i, der zeitlichen Auflösung t_{bin} und der Messdauer t_{int} mittels folgender Formel berechnet (vgl. Kroh, 2012, S. 61 f.):

$$C_1' = R_1 \cdot R_2 \cdot t_{bin} \cdot t_{int} \tag{3.3}$$

Für NV 1 ergab sich dabei ein Wert von $C_1 = 129{,}8$, für NV 2 $C_1 = 142{,}8$ und für NV 3 $C_1 = 31{,}6$
Die sich aus der Anpassung ergebenen Werte der Fit-Parameter C_1, C_0, K, k_1 und k_2 sind in Tabelle 3.5 dargestellt. In Abb. 3.11 wurde dabei der Nullpunkt der x-Achse auf x_0 gelegt.

	x_0	C_0	C_1	K	k_+ in $\frac{1}{\text{ns}}$	k_- in $\frac{1}{\text{ns}}$
NV 1	$194{,}1 \pm 0{,}4$	107 ± 1	35 ± 2	2 ± 15	$0{,}03 \pm 0{,}03$	$0{,}02 \pm 0{,}03$
NV 2	$194{,}3 \pm 0{,}3$	$30{,}4 \pm 0{,}9$	19 ± 2	$0{,}5 \pm 0{,}1$	$0{,}08 \pm 0{,}01$	$0{,}015 \pm 0{,}008$
NV 2	$194{,}6 \pm 0{,}2$	$13{,}1 \pm 0{,}7$	18 ± 7	$0{,}8 \pm 0{,}6$	$0{,}062 \pm 0{,}005$	$0{,}005 \pm 0{,}005$

Tabelle 3.5 – Autokorrelationsmessung mit *TimeHarp*.
Aufgeführt sind für drei NV-Zentren die Fit-Parameter, die sich aus der in Abb. 3.11 dargestellten Anpassung ergeben. Die Unsicherheiten sind dabei ebenfalls aus der Anpassung entnommen.

Der Wert $g^{(2)}(0)$ kann dann aus C_0 und C_1 wie folgt ermittelt werden:

$$g^{(2)}(0) = \frac{C_0}{C_1 + C_0} \tag{3.4}$$

Für die drei betrachteten NV-Zentren ergaben sich damit Werte von:

$$\begin{aligned}
\text{NV 1: } g^{(2)}(0) &= 0{,}75 \pm 0{,}01 \\
\text{NV 2: } g^{(2)}(0) &= 0{,}62 \pm 0{,}02 \\
\text{NV 3: } g^{(2)}(0) &= 0{,}415 \pm 0{,}095
\end{aligned}$$

Die Unsicherheit ist dabei per Gauß'scher Fehlerfortpflanzung aus der Unsicherheit von C_0 ermittelt worden. Nur NV 3 weist also Einzelphotonencharakter auf, bei NV 1 und NV 2 liegen die Werte über der Obergrenze von 0,5. Da es für die Sicherheit des BB84-Protokolls unerlässlich ist, dass pro Übertragung nur ein einziges Photon die Information trägt, sollte also nur NV 3 für eine Anwendung in der QKD verwendet werden. Diesen Umstand gilt es auch bei der Verwendung des Lasers zu berücksichtigen, wie im nächsten Abschnitt ausführlicher diskutiert werden soll.

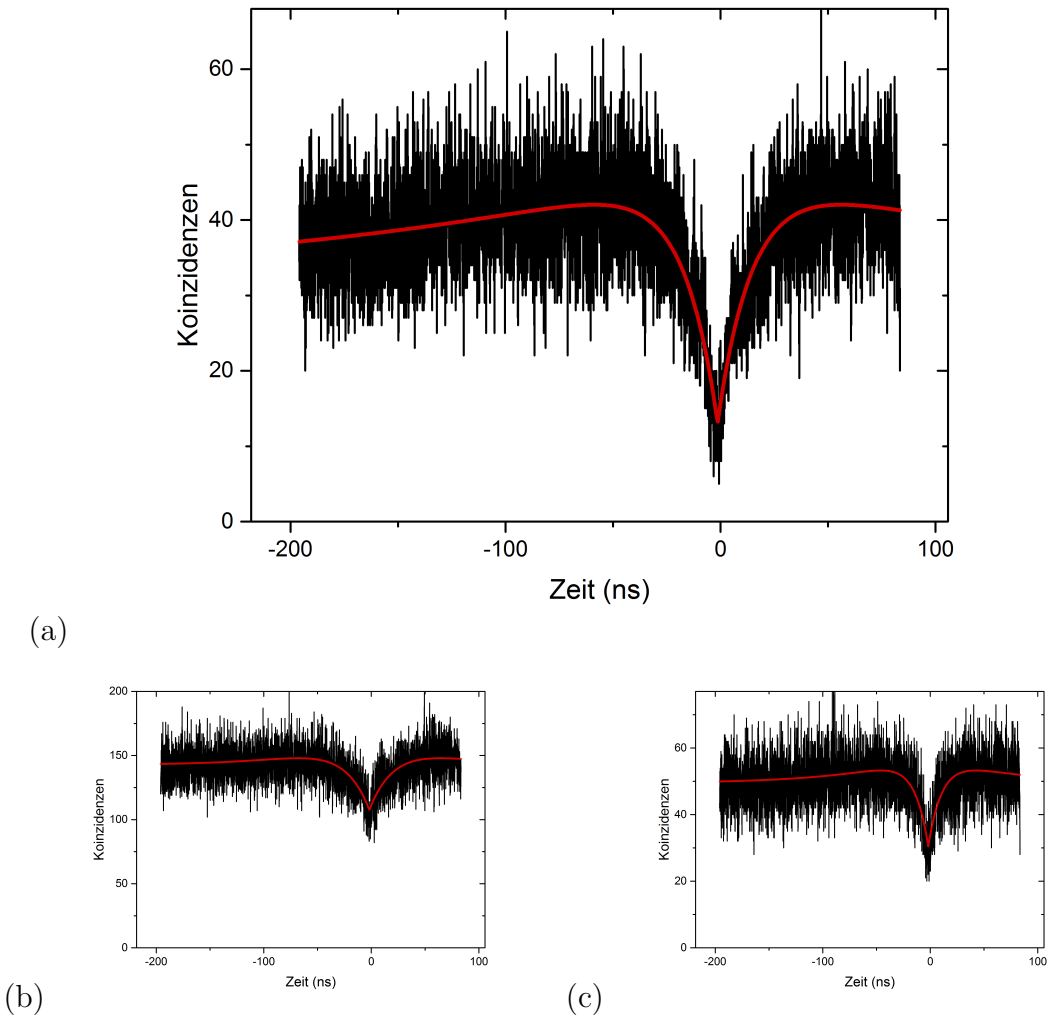


Abbildung 3.11 – Autokorrelationsmessung mit *TimeHarp*.
Dargestellt ist der Verlauf der Autokorrelation für NV 3 (a), NV 1 (b) und NV 2 (c). Zur Anregung wurde dabei ein 532 nm-Laser mit etwa 100 µW Leistung bei Raumtemperatur verwendet. Die Messdauer betrug 600 s für NV 1 und NV 3, sowie 300 s für NV 2. Als Zählraten wurden dabei an den Anschlüssen „Sync“ und „CFD“ im Mittel Werte von 57,3 bzw. 51,3 kcts/s bei NV 1, 43,0 bzw. 45, 1 kcts/s bei NV 2 und 24,6 bzw. 29, 1 kcts/s bei NV 3 erreicht.
Als Ergebnis der Messung wurden folgende Werte für die normierte Autokorrelationsfunktion zweiter Ordnung im Nullpunkt ermittelt: $g^{(2)}(0) = 0{,}75 \pm 0{,}01$ für NV 1, $g^{(2)}(0) = 0{,}62 \pm 0{,}02$ für NV 2 und, $g^{(2)}(0) = 0{,}415 \pm 0{,}095$ für NV 3.

3.5 Diskussion der Ergebnisse

Im Zusammenhang mit den im F-Praktikum gestellten Aufgaben wird der Fokus in dieser Diskussion auf die Eignung der verwendeten Geräte für eine kommerzielle Anwendung gelegt.

Ein für die QKD besonders wichtiger Aspekt ist dabei die Sicherheit der Übertragung gegenüber einem Angreifer. Wie in Abschnitt 2.2 angeführt, ist es dafür unerlässlich, dass pro übertragenem Bit nur ein Photon mit der entsprechenden Polarisation versehen wurde. Ideal wären also polarisationsverändernde Geräte, die so schnell schalten, dass die jeweilige Einstellung nur für den Durchgang eines Photons angenommen wird. Die verwendeten EOMs schalten zwar schnell genug, um eine Übertragung von bis zu 400 kBit/s zu erlauben, benötigen jedoch immer noch 85 Takte der FPGA, also über 2 µs, um ihre Einstellung zu wechseln, während die eigentliche Übertragung nur 15 Takte in Anspruch nimmt, wie ausführlicher in Abschnitt 3.3 ausgeführt wurde. Da also die Einstellung der EOMs nur alle 2,5 µs gewechselt wird, werden alle in dieser Zeit ausgesendeten Photonen gleich polarisiert. Ein schnellerer EOM-Treiber würde somit auch die Sicherheit der Übertragung erhöhen. Laut Schröder (2012, S. 158 f.) war die Schaltrate der EOM-Treiber darüber hinaus der hauptsächliche limitierende Faktor für seine Übertragungsrate.

Befindet sich die Quelle im Dauerstrichbetrieb, werden durch eine Quanteneffizienz der APDs von 65% ab einer Zählrate von etwa $C_T = \frac{0{,}65\,\mathrm{ct}}{2{,}5\,\mu\mathrm{s}} = \frac{260\,\mathrm{cts}}{1\,\mathrm{ms}} = 260\,\mathrm{kcts/s}$ im Mittel mehr als ein Photon pro Übertragungszyklus ausgesendet. Die hier beim Laser und der SPS gemessenen Zählraten liegen deutlich unter diesem Wert, sodass die Wahrscheinlichkeit, mehr als ein Photon mit derselben Information zu versehen, eher gering ist, wenngleich es nicht ausgeschlossen werden kann. Besser verhält sich in dieser Hinsicht eine gepulst betriebene Quelle, da diese nur in einem kurzen Zeitintervall Photonen aussendet. Bei dem hier eingesetzten Laser wurden im gepulsten Betrieb bei der geringsten Abschwächung $A = 10^{6{,}0}$ innerhalb von 7 Takten etwa 1.000 Photonen in 10.000 Übertragungen pro Takt an einer APD registriert (vgl. Abb. 3.5 in Abschnitt 3.3). Wird davon ausgegangen, dass in den restlichen Takten keine Photonen registriert wurden, ergeben sich im Mittel 1,4 detektierte Photonen pro Übertragung. Bei einer Quanteneffizienz der APDs von 65% kann also unter Vernachlässigung von Verlusten innerhalb von Bobs Aufbau oder der Übertragungsstrecke davon ausgegangen werden, dass sich im Mittel mindestens 2 Photonen in einer Übertragung befinden. Wird die Abschwächung um eine Größenordnung auf $A = 10^{7{,}0}$ erhöht, sollte dieser Wert um eine Größenordnung abnehmen. Ab dieser Abschwächung kann also mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass nur ein Photon pro Übertragungszyklus ausgesendet wurde. Trotz allem beziehen sich diese Aussagen nur auf im Mittel erreichte Werte. Eine Garantie dafür, dass keine zwei Photonen zur selben Zeit ausgesendet werden, liefert nur eine echte Einzelphotonenquelle. Alle diese Abschätzungen vernachlässigen darüber hinaus Photonen, die während der Übertragung absorbiert wurden. Einem Angreifer wäre es allerdings trotzdem möglich gewesen, durch diese Photonen Informationen zu erhalten, sofern sie nicht schon in Alice' Aufbau absorbiert wurden.

Bei einer SPS ist allerdings zu beachten, dass nicht jeder im Scan der Probe entdeckte Punkt nur aus einem NV-Zentrum besteht. Wie die Überprüfung der Autokorrelation gezeigt hat, konnte nur bei einem von drei im Scan gefundenen Punkten von einer Einzelphotonenartigkeit gesprochen werden. Darüber hinaus darf nicht vergessen werden, dass die SPS in dieser Arbeit nicht gepulst betrieben werden

konnte. Wenngleich also die gleichzeitige Erzeugung von zwei oder mehr Photonen ausgeschlossen werden kann (zumindest bei entsprechendem Wert von $g^{(2)}(0)$), ist es wahrscheinlich, dass ein zweites Photon nach 50 ns detektiert wird (vgl. Abb. 3.11), sodass innerhalb der 2,5 µs, in denen der EOM in einer Einstellung verweilt, im Mittel 50 Photonen erzeugt und in die Übertragung gebracht werden könnten. Ein guter Wert für die Autokorrelation allein reicht deshalb nicht aus, um eine sichere Übertragung zu gewährleisten.

Wenngleich eine gepulst betriebene SPS die beste Sicherheit verspricht, gibt es Möglichkeiten, auch für einen gepulsten Laser die Sicherheit erheblich zu erhöhen, z.B. die *decoy-state*-Methode (vgl. dazu Leifgen, 2016, S. 55 f.).

Da alle aufgetretenen Übertragungsfehler dem Eingreifen einer Lauscherin zugeordnet werden müssen (vgl. Abschnitt 2.4), ist eine niedrige Fehlerrate ein für die Sicherheit relevanter Punkt. Darüber hinaus sind eine möglichst niedrige Fehlerrate und eine möglichst hohe Übertragungsrate auch wichtige Aspekte für eine effiziente Übertragung mittels des Aufbaus. Bei den hier gemessenen Daten war die Fehlerrate QBER dabei abgesehen von NV 2 immer für höhere Übertragungsraten niedriger. Die höchste Übertragungsrate konnte mit dem gepulsten Laser bei minimaler Abschwächung erreicht werden und betrug etwa $R = 150\,\text{kBits/s}$. Die zugehörige Fehlerrate war mit QBER= 5% minimal. Wie jedoch im vorherigen Absatz diskutiert, liegt der Nachteil der geringen Abschwächung in einer höheren Wahrscheinlichkeit, mehr als ein Photon für die Übertragung eines Bits verwendet zu haben, was ein Sicherheitsrisiko darstellt. Für das NV-Zentrum, dem ein Einzelphotonencharakter nachgewiesen werden konnte, ergab sich demgegenüber eine Übertragungsrate von nur etwa 1 kBits/s bei einer Fehlerrate von 7%. Die höhere Sicherheit geht hier also zu Lasten einer deutlich längeren Übertragungszeit bzw. einer deutlich geringeren Menge an übertragenen Daten.

Beim Laser erhöhte sich die Übertragungsrate durch Nutzung des gepulsten Modus um eine Größenordnung, wenn die Werte mit ähnlichen Zählraten im Dauerstrichbetrieb verglichen werden. Das kann damit begründet werden, dass zur Ermittlung der Zählrate zu allen Zeiten ankommende Photonen registriert werden, für Übertragungen jedoch nur die innerhalb von 4 aus 100 Takten (also 100 ns von 2500 ns) eintreffenden. Daraus könnte abgeleitet werden, auch bei der SPS eine deutlich höhere Übertragungsrate durch eine gepulste Anregung zu erreichen. In diesem Zusammenhang können die von Schröder (2012) und Leifgen (2016) ermittelten Ergebnisse herangezogen werden, deren Aufbau bis auf wenige Details mit dem hier verwendeten identisch war. Allerdings konnte in diesen Arbeiten ein gepulst betriebener Anregungslaser verwendet werden (vgl. Schröder, 2012; Leifgen, 2016, S. 155 bzw. S. 65). Schröder (2012, S. 159) erreichte damit eine Übertragungsrate von 5 kBits/s bei einer Fehlerrate von 3,3% und Leifgen (2016, S. 74) sogar $8{,}9 \pm 0{,}1\,\text{kBits/s}$ bei einer Fehlerrate von $3{,}0 \pm 0{,}2\%$. Diese Raten sind erheblich besser als die hier erreichten, was wahrscheinlich nicht nur, aber auch auf die gepulste Anregung zurückgeführt werden kann.

Eine Alternative zu NV-Zentren bei der Erzeugung von einzelnen Photonen könnten Quantenpunkte darstellen. Diese sind allerdings schwerer zu handhaben und können nicht bei Raumtemperatur betrieben werden.

Als dritter Aspekt sollen noch die Anschaffungskosten der einzelnen Geräte Berücksichtigung finden. Bei der SPS handelt es sich um ein in der Arbeitsgruppe gefertigtes Einzelstück, das kommerziell nicht erhältlich ist. Die Komponenten des Lasers können dagegen für etwas über 100 € von verschiedenen Firmen bezogen wer-

den, sodass auch ein Austausch defekter Teile kein Problem darstellt. Den teuersten Posten stellen wahrscheinlich die APDs zur Photonendetektion dar, die pro Stück um 4.000 € kosten. Darüber hinaus sind diese Geräte sehr lichtempfindlich, weshalb ein sehr sorgfältiger Umgang unumgänglich ist. An dieser Stelle könnten Kosten gespart werden, indem nur eine APD zur Detektion verwendet wird. Bob kann dann nur einen Bit-Wert messen: Detektiert er zu einem bestimmten Zeitpunkt ein Photon, ordnet er es diesem Bit-Wert zu, detektiert er keines, geht er davon aus, dass es in der anderen Polarisation vorlag und ordnet es dem entsprechend anderen Bit-Wert zu. Der Nachteil des Verfahrens liegt allerdings darin, dass auch alle während der Übertragung absorbierten oder nicht detektierten Photonen diesem Bit-Wert zugeordnet werden müssen, wodurch sich die Fehlerrate erhöht. Auf der anderen Seite werden durch die Verwendung eines EOMs bei Bob schon zwei APDs eingespart, die sonst zur Messung in der RL-Basis verwendet werden müssten.
Auch die EOMs stellen mit etwa 2000 € pro Stück eine nicht geringe Investition dar. Der Betrieb mit Spannungen von $\pm 250\,\mathrm{V}$, die innerhalb von Mikrosekunden geschaltet werden müssen, bedarf darüber hinaus einer durchdachten Steuerung. Im vorliegenden Fall wurden auch diese in der Arbeitsgruppe entwickelt, für einen kommerziellen Einsatz müsste allerdings ein anderes Verfahren gefunden werden.
Den weiteren Geräten wie $\frac{\lambda}{2}$-Plättchen oder Spiegel kommt gegenüber diesen Ausgaben im Preis eine geringere Relevanz zu.

Zusammenfassend kann gesagt werden, dass sich sowohl der Laser als auch die Einzelphotonenquelle für eine Anwendung in der QKD eignen, jeweils allerdings einige Aspekte beachtet werden müssen.
Die Sicherheit der Übertragung ist dabei der ausschlaggebende Faktor, da dies den hauptsächlichen Zweck der Quantenkryptographie darstellt. Dafür ist vor allem darauf zu achten, dass pro übertragenem Bit nur ein Photon in dem jeweiligen Polarisationszustand Alice' Aufbau verlässt. Dies kann auf verschiedenen Wegen angestrebt werden, etwa durch Pulsen des Lasers oder eine Verringerung der Schaltzeiten der EOMs, muss jedoch stets aufs Neue sichergestellt werden.
Die Kosten der Geräte sind zum Teil beachtlich, lassen sich allerdings bei Verwendung des BB84-Protokolls nur auf Kosten anderer Parameter wie Übertragungs- oder Fehlerrate verringern.
Eine Einzelphotonenquelle erreicht insgesamt eine bessere Sicherheit, weist allerdings schlechtere Übertragungs- und Fehlerraten als ein Laser auf. Durch die Verwendung eines gepulsten Lasers zur Anregung der NV-Zentren sollte sich an dieser Stelle allerdings eine Verbesserung gegenüber dem hier beschriebenen Versuch ergeben können.

Kapitel 4

Didaktische Aufbereitung

In diesem Kapitel wird dargestellt, wie der zuvor beschriebene QKD-Aufbau im F-Praktikum eingesetzt werden kann. Dafür wird die Zielorientierung in der Lehre thematisiert, wobei auf den Unterschied von Lehr- und Lernzielen sowie Grob- und Feinzielen eingegangen wird. Dabei werden auch die Lehrziele des QKD-Versuchs angeführt. Anschließend wird die Gestaltung der Versuchsanleitung beschrieben.

4.1 Zielorientierung in der Lehre

4.1.1 Lehr- und Lernziele

Überall, wo Lehre in irgendeiner Art stattfindet, finden sich auch Absichten und Ziele der Beteiligten. Jeder wird dabei seine eigenen Ziele haben, doch gibt es auch Gemeinsamkeiten innerhalb der Gruppen von Lehrenden und Lernenden, die es sinnvoll erscheinen lassen, diese Ziele im Ganzen zu betrachten.
Die Ziele der Lernenden, im Folgenden als Lernziele bezeichnet, beschränken sich im Zusammenhang mit dem Lernort Labor unter Umständen darauf, den Versuch rasch und ohne negative Nebenerscheinungen abzuwickeln, können aber auch Erfolg, Wissenszuwachs oder Spaß beinhalten. Diese Lernziele sind dem Lehrenden im Allgemeinen nicht bekannt, er sollte jedoch davon ausgehen, dass sie sich nicht mit seinen eigenen Zielen decken, die im Folgenden als Lehrziele bezeichnet werden. Da der Lernende die Lehrziele von sich aus ebensowenig kennt wie der Lehrende die Lernziele, ist es ratsam, wenn wenigstens dieser seine Ziele offenlegt und möglichst auch noch Wege aufzeigt, ihr Erreichen zu überprüfen (vgl. Bruchmüller & Haug, 2001, S. 25).
Im Folgenden werden diese Lehrziele in Grob- und Feinziele aufgegliedert.

4.1.2 Grob- und Feinziele

Abgesehen von seiner persönlichen Absicht hat sich der Lehrende auch nach aus Gesetzen und Verordnungen stammenden übergeordneten Lehrzielen zu richten. In Bezug auf das F-Praktikum wird auf diese Thematik in Abschnitt 4.1.3 näher eingegangen. Aus beidem können dann bezogen auf das konkrete Thema sowohl Grob- als auch Feinziele formuliert werden (vgl. Bruchmüller & Haug, 2001, S. 26).

Für die in Abschnitt 1.2 eingeführten drei Stufen der Laborarbeit (I – grundlegende Übungsversuche, II – fortgeschrittenere Praktikumsversuche, III – eigenständige wissenschaftliche Arbeit) nennen Bruchmüller und Haug (2001, S. 71 f., 99 ff.) Grobziele und geben eine evaluierte Lehrzielbank aus 57 Feinzielen in operationalisierter Form an. Diese sind unabhängig vom konkreten Inhalt des Versuchs, müssen also je nach Thema ergänzt werden. Operationalisiert bedeutet dabei, dass alle Ziele die Form "Die Studierenden können . . . " haben.
Als Grobziele der Stufe II werden dabei benannt:

> - „Problemlöseverhalten erwerben;
> - Beziehungsstrukturen und Führungsstile erleben und üben;
> - Selbstständigkeit, Verantwortung für eigenes Tun erwerben;
> - Das selbst Erarbeitete in einer schriftlichen Ausarbeitung darstellen und anderen (z.B. in einem Lehrvortrag) vermitteln, [. . .]."
>
> (Bruchmüller & Haug, 2001, S. 72)

Aus der evaluierten Lehrzielbank wurden folgende 15 Ziele als relevant für den in dieser Arbeit beschriebenen QKD-Versuch angesehen:

> Die Studierenden können. . .
>
> - Literaturhinweise auswerten, Literatur gezielt suchen
> - Geeignete Geräte zum Versuch kombinieren
> - die Wirkungsweise von Geräten erklären
> - Bausteine/Geräte im Versuchsaufbau erkennen und benennen
> - die Übereinstimmung zwischen zugrundeliegendem Versuchsprinzip und dem vorliegenden Aufbau erkennen
> - Geräte justieren und/oder kalibrieren
> - mit Geräten/Aufbauten/Anlagen sicher umgehen
> - mit Versuchs-Software richtig und sicher umgehen
> - Sicherheits- und Schutzbestimmungen anwenden/einhalten
> - Beobachten und Messdaten übersichtlich festhalten
> - Daten in geeigneter Form darstellen, die Form dabei selbst wählen
> - dargestellte Daten erklären, Folgerungen ziehen
> - (Versuchs-) Abläufe und Zusammenhänge erläutern
> - zum Versuchsergebnis kritisch Stellung nehmen
> - Ergänzungen bzw. Alternativen zum Versuch vorschlagen
>
> (vgl. Bruchmüller & Haug, 2001, S. 99 ff.)

Diese Ziele dienten als Ausgangspunkt für die Formulierung eigener Grob- und Feinziele des QKD-Versuchs auf Grundlage der in der Studienordnung benannten übergeordneten Lehrzielen, worauf der folgende Abschnitt im Detail eingeht.

4.1.3 Lehrziele des QKD-Versuchs

Wie schon in der Einleitung in Abschnitt 1.2 behandelt, gibt es für das F-Praktikum übergeordnete Lehrziele aus der Studienordnung, die im Folgenden noch einmal gegliedert wiedergegeben werden (vgl. Humboldt-Universität zu Berlin, 2014, S. 25):

Die Studierenden können ...

1. komplexe experimentelle Fragestellungen der modernen Physik lösen;
2. dabei nach eigener und weitgehend selbstständiger praktisch-experimenteller Tätigkeit vorgehen;
3. die Nutzung experimenteller Grundprinzipien, Techniken und Geräte einschätzen;
4. experimentelle Ergebnisse eigenständig dokumentieren;

An persönlichen Zielen kommt dazu:

5. Interesse an Kryptologie in den Studierenden wecken;
6. den Studierenden einen Einblick in grundlegende Methoden in der Laseroptik vermitteln;
7. den Studierenden eine praxisnahe Orientierung mit einem forschungsnahen Kontext geben.

Von den übergeordneten Lehrzielen wird 1. dahingehend erfüllt, dass QKD eindeutig der modernen Physik angehört und innerhalb des Praktikumsversuches Teile einer Dissertation nachempfunden werden, die erst vor einigen Monaten abgeschlossen wurde. Auch sind einige der experimentellen Tätigkeiten durchaus als herausfordernd anzusehen, etwa die Basiswahl mit den EOMs oder das Finden der Einzelphotonen emittierenden NV-Zentren in Nanodiamanten.
Dagegen ist 2. bei dem vorliegenden Aufbau schwer innerhalb der gegebenen Zeit realisierbar, da einerseits nur die in Abschnitt 3.4 beschriebenen Daten gemessen werden können, der Versuch also wenig Varianten zulässt und andererseits die durchführbaren Schritte angeleitet werden müssen, da ihre Komplexität für eine explorative Aneignung zu hoch ist. Im Bewusstsein dieser Einschränkung wurde versucht, dafür zu 3. und 4. umso mehr Freiheiten zu geben und, auch im Hinblick auf 7., einen Kontext zu schaffen, in den die Durchführung eingebettet werden kann.
Das 5. Ziel wird durch eine Motivation in der Versuchsanleitung angestrebt, die das komplexe Thema pointiert zusammenfasst und seine Relevanz in der heutigen Zeit verdeutlicht. Zu 6. (und auch 3.) wird sich im Justieren des Strahlenganges, der Kalibrierung der EOMs oder der Autokorrelationsmessung an den Photonen der NV-Zentren Gelegenheit finden. Und 7. soll, wie bereits erwähnt, für die Auswertung eine Rolle spielen.

Anhand dieser Zielsetzungen können folgende Grobziele für den QKD-Versuch formuliert werden:

(A) Erwerb von grundlegendem Wissen über Quantenkryptographie & -informationsverarbeitung, insbesondere bezüglich des BB84-Protokolls;

(B) Selbstständige Aneignung von Kenntnissen über die im Aufbau verwendeten Geräte, insbesondere ihrer Wirkungsweise;

(C) Durchführung der experimentellen Tätigkeiten nach Anleitung durch den Versuchsbetreuenden;

(D) Auswertung der Daten in einem forschungsnahen Kontext, insbesondere vergleichende Beurteilung der verwendeten Geräte.

Die aus der evaluierten Lehrzielbank entnommenen Ziele (s. Abschnitt 4.1.2 bzw. Bruchmüller & Haug, 2001, S. 99 ff.) wurden teilweise umformuliert, ergänzt und dann den genannten Grobzielen als Feinziele zugeordnet. Eine ausführliche Aufstellung der zugehörigen Feinziele einschließlich ihrer Überprüfung ist in Tab. 4.1 dargestellt.

	Die Studierenden können ...	*indem Sie ...*
(A)	**Erwerb von grundlegendem Wissen über Quantenkryptographie & -informationsverarbeitung, insbesondere bezüglich des BB84-Protokolls.**	
(a-1)	fundamentale Unterschiede zwischen klassischer und Quantenkryptographie benennen,	in einem Gespräch mit dem Versuchsbetreuer die entsprechenden Abschnitte der Versuchsanleitung in eigenen Worten wiedergeben.
(a-2)	die Rolle des OTP-Verfahrens innerhalb der Quantenkryptographie erläutern,	
(a-3)	Grundbegriffe der Quanteninformationsverarbeitung im Hinblick auf die QKD einordnen,	eine Poincaré-Kugel korrekt beschriften und daran die Verwendung polarisierter Photonen als Qubits erklären.
(a-4)	die Reihenfolge der Schritte des BB84-Protokolls korrekt wiedergeben,	die schematische Darstellung der Übertragung korrekt ordnen und ergänzen
(B)	**Selbstständige Aneignung von Kenntnissen über die im Aufbau verwendeten Geräte, insbesondere ihrer Wirkungsweise.**	
(b-1)	Literatur zu den im Aufbau verwendeten Geräten gezielt suchen und entsprechende Literaturhinweise auswerten,	sich in Ihren Ausführungen auf die durch Eigenrecherche erworbenen Kenntnisse beziehen.
(b-2)	die Wirkungsweise der Geräte erklären,	eine entsprechende schematische Darstellung ergänzen und den Schritten des BB84-Protokolls zuordnen.
(b-3)	die Übereinstimmung zwischen zugrundeliegendem Versuchsprinzip und dem vorliegenden Aufbau erkennen,	
(b-4)	Bausteine/Geräte im Versuchsaufbau erkennen und benennen,	das in (b-2) und (b-3) verwendete Schema auf den Aufbau übertragen.

	Die Studierenden können ...	*indem Sie ...*
(C)	**Durchführung der experimentellen Tätigkeiten nach Anleitung durch den Versuchsbetreuenden.**	
(c-1)	den Strahlengang justieren,	drei zuvor verdrehte Spiegel korrekt einstellen und die restlichen Spiegel nachjustieren.
(c-2) (c-3)	mit Geräten, Aufbauten und Versuchssoftware richtig und sicher umgehen, um • den Aufbau für die Übertragung mit dem Laser bzw. der SPS einzurichten • diese unter verschiedenen Bedingungen durchzuführen	EOMs, APDs und später auch die SPS in Betrieb nehmen und mittels der zur Verfügung stehenden *LabView*-Programme ihre Funktionsweise überprüfen, sowie für die Übertragung einrichten und diese durchführen.
(c-4)	• Autokorrelationsmessungen vorzunehmen	die *TimeHarp*-Karte richtig verwenden und mittels des zugehörigen Programms bedienen.
(c-5)	Sicherheits- und Schutzbestimmungen einhalten.	× (selbsterklärend)
(D)	**Auswertung der Daten in einem forschungsnahen Kontext, insbesondere vergleichende Beurteilung der verwendeten Geräte.**	
(d-1)	experimentelle Ergebnisse eigenständig dokumentieren,	Beobachten und Messdaten unaufgefordert übersichtlich festhalten.
(d-2)	Daten kontextbezogen aufbereiten, in geeigneter Form darstellen und erklären,	einen Bericht über Verwendungsmöglichkeiten verschiedener Geräte für die QKD aus Sicht eines Forschenden verfassen.
(d-3)	(Versuchs-) Abläufe und Zusammenhänge erläutern,	
(d-4)	zum Versuchsergebnis kritisch Stellung nehmen	
(d-5)	Ergänzungen bzw. Alternativen zum Versuch vorschlagen,	

Tabelle 4.1 – Grob- und Feinziele des QKD-Versuchs.

Aus diesen Feinzielen kann zum einen der Ablauf des Versuchstages entnommen werden, zum anderen können daraus Aufgaben als Strukturierung für die Studierenden formuliert werden. Die dabei genannten Materialien sind Anhang B zu entnehmen.

4.2 Gestaltung der Versuchsanleitung

Bruchmüller und Haug (2001, S. 155 ff.) räumen der Versuchsanleitung eine herausragende Bedeutung für das Praktikum ein. Die Versuchsanleitung ist nicht nur das Erste von dem Versuch, mit dem die Studierenden in Berührung kommen, sie ist auch Motivation, Rahmen und Leitfaden für die Versuchsdurchführung (vgl. Bruchmüller & Haug, 2001, S. 155 f.).

Richtlinien zur Gestaltung

Eine wesentliche Aufgabe der Versuchsanleitung ist die Einweisung in die im Versuch verwendeten Geräte und Steuerungen. Diese sind den Teilnehmenden zu Beginn nicht in dem Maße bekannt, wie es für ein sicheres und erfolgreiches Arbeiten nötig wäre. Um in den Umgang mit den Geräten einzuweisen, können neben Hinweisen oder Kurzanleitungen in der Versuchsanleitung auch die Bedienungsanleitungen der Geräte zur eigenen Aneignung zur Verfügung gestellt werden (vgl. Bruchmüller & Haug, 2001, S. 157 f.).

Darüber hinaus sollte die Anleitung auch den Versuchsaufbau in Gänze beschreiben, wofür sich insbesondere Funktionsbilder und Ablaufdiagramme anbieten, die einen guten Überblick über den Aufbau und seine Funktion geben können. Die wesentlichen Elemente sollten dabei hervorgehoben sein (vgl. Bruchmüller & Haug, 2001, S. 163 f.).

Die Anleitung führt durch den Versuch, indem sie den Ablauf der durchzuführenden Schritte schildert. Die Durchführung von frei zu bearbeitenden Versuchsteilen sollte dabei im Vorfeld von den Teilnehmenden geplant und mit dem Betreuenden abgesprochen werden. Versuche, die mehr Gestaltungsmöglichkeit lassen, können dabei schwerer durch allgemeingültige Anleitungen beschrieben werden. Anders herum, je weniger Eingenanteil der Studierenden vorhanden ist, umso ausführlicher muss die Anleitung ausfallen (vgl. Bruchmüller & Haug, 2001, S. 161, 164). Im QKD-Versuch gibt es hinsichtlich der Beurteilung der Geräte einen weitgehend frei gestalteten Teil, für den dann auch nur Literaturhinweise gegeben und keine Vorgaben zur konkreten Ausarbeitung gemacht werden. Da jedoch, wie schon angeführt wurde, die mit dem Versuchsaufbau möglichen Messungen kaum Spielraum lassen, ist der auf die Handhabung der Geräte und Durchführung des Versuchs bezogene Teil der Anleitung wiederum sehr ausführlich gehalten.

Über den Versuch hinaus gibt die Versuchsanleitung Hinweise zur geforderten Ausarbeitung. Die einzelnen Teile dieses Berichts sollten dabei umso ausführlicher ausfallen, je größer der Eigenanteil der Teilnehmenden an der Planung und Durchführung der in diesem Teil beschriebenen Messungen sind (vgl. Bruchmüller & Haug, 2001, S. 161, 163).

In der Formulierung der hier erstellten Versuchsanleitung wurde sich darüber hinaus an vergleichbaren Versuchen orientiert, namentlich an dem Versuch „Paul-Falle“, der ebenfalls von der Arbeitsgruppe Nanooptik erstellt wurde und an dem Versuch „Magneto-optische Falle“, deren Anleitung von Marek Mandel in seiner Bachelorarbeit (2014) geschrieben wurde.

Inhalt und Aufbau der Versuchsanleitung

Die Anleitung ist in die fünf Kapitel Einleitung, Aufgaben, Theoretische Beschreibung, Aufbau und Durchführung der Messungen gegliedert, die im Folgenden kurz beschrieben werden sollen. Sie ist im Wortlaut in Anhang A zu finden.

Einleitung

Den Beginn der Anleitung bildet eine kurze Einleitung, die in das Thema einstimmen soll und einen Überblick über das Ziel des Versuchs gibt. Auch werden die Teilnehmenden explizit um eine Rückmeldung am Ende des Versuchs gebeten. Durch diese interne Evaluierung wird eine stetige Weiterentwicklung und Verbesserung der Anleitung ermöglicht.

Aufgaben

Als Nächstes sind die Aufgaben angegeben, die vor, während und nach dem Versuch bearbeitet werden sollen. Die Aufgaben sind dabei zur besseren Übersicht nummeriert. Dadurch soll auch gewährleistet werden, dass keine Aufgabe aus Versehen übergangen wird.

Zu Beginn wird eine kurze Einstimmung in den Kontext der Arbeit gegeben. Anschließend werden die Studierenden zur Vorbereitung aufgefordert, sich anhand der Versuchsanleitung mit den Themen des Versuchs vertraut zu machen. In Hinblick auf die offen gestellte Aufgabe sollen hierbei eigene Recherchen zu Kenndaten und Wirkungsweise der im Aufbau verwendeten Geräte angestellt werden. Dazu werden Literaturhinweise gegeben, die aber durch eigene Quellen ergänzt werden können und sollen. Um dabei eine unergiebige Suche nach den Datenblättern zu vermeiden, werden diese vom Versuchsbetreuenden zur Verfügung gestellt. Dies wurde auch in den Richtlinien als Möglichkeit genannt. Die Seriennummern der konkret verwendeten Geräte sind dabei im Kapitel Aufbau explizit benannt.

Zur Durchführung des Versuchs wird auf das entsprechende Kapitel in der Anleitung verwiesen. Allerdings wird betont, dass die dort geschilderte Vorgehensweise nicht bindend ist und letztendlich die Studierenden selbst entscheiden, was und in welchem Umfang sie messen wollen. Auch wird darauf hingewiesen, dass die Dokumentation vollkommen eigenständig erfolgt. Damit soll eine möglichst große Freiheit und Selbstständigkeit erreicht werden, wie in den Zielen (s. Unterabschnitt 4.1.3) gefordert. Die Teilnehmenden werden allerdings explizit aufgefordert, sich vor den Messungen einen Plan zu überlegen und diesen mit dem Versuchsbetreuenden abzusprechen. Als verpflichtende Aufgabe wird darüber hinaus gefordert, den Versuch für eine Übertragung einzurichten, die Übertragung unter verschiedenen Rahmenbedingungen durchzuführen und die Autokorrelation der dabei verwendeten NV-Zentren zu bestimmen. Dies soll verhindern, dass Teilnehmende versuchen, die Eignung der Geräte rein theoretisch oder allein auf Grund von Messungen anderer Versuchsgruppen einzuschätzen, wie es sonst ohne Konflikt mit der Aufgabenstellung möglich wäre. Denn wenn auch ein Vergleich mit anderen Messungen an diesem Aufbau für eine Diskussion wünschenswert ist, sollte sich die Argumentation vor allem auf die eigenen Messungen stützen.

Für die Auswertung des Versuchs muss ein Bericht bzw. Protokoll verfasst werden. Dieser orientiert sich an den gängigen Standards des F-Praktikums, die den Studierenden im Detail vom Versuchsbetreuenden vorgegeben werden. Als inhaltliche Ausrichtung dieses Berichts wird der Fokus wiederum auf die verwendeten Geräte gelenkt. Diese sollen im Hinblick auf eine kommerzielle Anwendung beurteilt werden, auch unter Einbeziehung von Grenzen und möglichen Alternativen.
Die Position der Aufgabenstellung am Beginn der Versuchsanleitung ermöglicht ein zielgerichtetes Durcharbeiten der Anleitung und gibt für die weitere Vorbereitung eine Richtung vor. Auch Bruchmüller und Haug (2001, S. 172) sprechen sich in diesem Kontext dafür aus, die Aufgabenstellung an den Beginn der Versuchsanleitung zu stellen.

Theoretische Beschreibung

Der theoretische Teil der Anleitung gibt die zur Bearbeitung nötigen Hintergrundinformationen. Darüber hinaus soll er auf die Besonderheiten der Quantenkryptographie hinweisen und Interesse an der Kryptologie wecken. Die Inhalte stammen aus dem theoretischen Teil dieser Arbeit, der auf fünf Seiten gekürzt wiedergegeben wird. Sie sind in die Abschnitte „*One Time Pad* zur klassischen Verschlüsselung“, „Einzelphotonen als Grundlage der Quantenkryptographie“, „Quanteninformationsverarbeitung“ und „Ablauf des BB84-Protokolls“ unterteilt.

Aufbau und Durchführung

Im Teil Aufbau wird nach dieser allgemeinen Einführung der konkrete Versuchsaufbau mit seinen Geräten und deren Ansteuerung auf acht Seiten beschrieben. Damit soll eine gründliche Auseinandersetzung mit dem Versuch im Vorfeld ermöglicht werden, die zu einem kompetenten Umgang am Versuchstag befähigt. Besonderen Wert wurde dabei auf eine übersichtliche Darstellung des Aufbaus und der zur Steuerung verwendeten Programme gelegt, wie in den Richtlinien gefordert. Der Teil Aufbau besteht dabei inhaltlich ebenfalls aus den entsprechenden Abschnitten dieser Arbeit in gekürzter Form.
Zuletzt wird im Teil Durchführung auf fünf Seiten in ausführlicher Form geschildert, welche Messungen mit dem Versuchsaufbau möglich sind und wie dafür konkret vorgegangen werden kann. Sicherheitsaspekte, die dabei unbedingt beachtet werden müssen, um eine Beschädigung der Geräte zu vermeiden, wurden dabei fett hervorgehoben.

Anhang

Im Anhang der Versuchsanleitung befindet sich eine Anlage zur Lasersicherheit, die von den Studierenden unterzeichnet werden muss. Dies gewährleistet eine Sensibilisierung der Studierenden für die Sicherheitsaspekte des Versuchs und gibt darüber hinaus auch eine Absicherung, dass die Belehrung erfolgt ist. Die Idee dazu stammt von Mandel (2014), auch wurden die dort verwendeten Formulierungen weitgehend übernommen.

Kapitel 5

Zusammenfassung und Ausblick

In dieser Bachelorarbeit wurde ein Versuch zum Quantenschlüsselaustausch (QKD) hinsichtlich physikalischer und didaktischer Gesichtspunkte untersucht. Ein Aufbau zur QKD mittels BB84 wurde rekonstruiert, in Betrieb genommen und verbessert. Auch wurden sich die theoretischen Grundlagen der Quantenkryptographie, der Quanteninformationsverarbeitung und des BB84-Protokolls sowie der Erzeugung und des Nachweises von einzelnen Photonen erarbeitet.
Die volle Funktionsfähigkeit des Aufbaus konnte durch exemplarische Messungen nachgewiesen werden. Diese reproduzieren zwar nicht die in den vorhergehenden Dissertationen an dem Aufbau ermittelten Werte, weisen aber dennoch die Möglichkeit einer Schlüsselübertragung nach. Die größte Herausforderung besteht dabei in der Gewährleistung der bedingungslosen Sicherheit der Übertragung. Dafür muss unter anderem sichergestellt werden, dass für jedes Schlüssel-Bit nicht mehr als ein Photon übertragen wird. Davon kann selbst bei der Einzelphotonenquelle nicht a priori ausgegangen werden.
Der didaktische Anteil der Arbeit bestand in der Formulierung konkreter Lehrziele für den QKD-Versuch, anhand derer die Durchführung des Praktikums ausgerichtet werden kann, und der Erstellung der Versuchsanleitung.
Da es leider zeitlich nicht mehr möglich war, den Versuch innerhalb dieser Arbeit zu erproben, muss offen bleiben, inwieweit die angestrebten Ziele erreicht werden und an welchen Stellen Verbesserungsbedarf besteht. Aus diesem Grund werden die Studierenden in der Versuchsanleitung explizit aufgefordert, konstruktiv Kritik an dem Versuch und der Anleitung zu äußern. Anhand dieser Kritik kann der Versuch zum einen evaluiert, zum anderen kontinuierlich verbessert werden. Eine kleine technische Erweiterung könnte dabei schon darin bestehen, einen gepulsten Laser zur Anregung der NV-Zentren zu verwenden.

Diese Bachelorarbeit endet damit, dass der Versuch zur QKD vollständig und funktionsfähig einschließlich einer Versuchsanleitung bereitsteht. Der erneute Einsatz des Aufbaus als F-Praktikum-Versuch hat an dieser Stelle allerdings gerade erst begonnen. Quantenkryptographie ist ein Thema, dass unter Studierenden auf reges Interesse stößt, weshalb auch der ehemalige F-Praktikum-Versuch zur QKD sehr beliebt war. Auch unter diesem Aspekt ist es schön, das Thema nun wiederum anbieten zu können. Der Aufbau ist dabei um wesentliche Elemente ergänzt worden und beinhaltet durch die Verwendung der Einzelphotonenquelle einen völlig neuen Aspekt, der auch unabhängig von der QKD eine hohe Aktualität und physikalische Relevanz besitzt.

Literaturverzeichnis

Aharonovich, I., Castelletto, S., Simpson, D. A., Su, C.-H., Greentree, A. D. & Prawer S. (2011). Diamond-based single-photon emitters. *Reports on Progress in Physics*, *74* (7), 1–28. Zugriff am 03.08.2016 auf `http://stacks.iop.org/0034-4885/74/i=7/a=076501`

Bennett, C. H. & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, *560*, 7–11. doi: 10.1016/j.tcs.2014.05.025

Benson, O. (2016). *Ist der Mond auch da, wenn keiner hinsieht? Wissen und Information in der Quantenphysik.* Berlin. Zugriff am 27.07.2016 auf `https://www.physik.hu-berlin.de/de/nano/folien-urania.pdf`

Bruchmüller, H.-G. & Haug, A. (2001). *Labordidaktik für Hochschulen: Eine Hinführung zum praxisorientierten Projekt-Labor* (Bd. 40). Alsbach/Bergstraße: Leuchtturm-Verlag.

Demtröder, W. (2006). *Experimentalphysik 2: Elektrizität und Optik* (4., überarb. und erw. Aufl.). Berlin: Springer.

Humboldt-Universität zu Berlin. (2014). *Amtliches Mitteilungsblatt Nr. 57/2014: Fachspezifische Studien- und Prüfungsordnung für das Bachelorstudium im Fach Physik. Monostudiengang.*

Humboldt-Universität zu Berlin. (2015). *Amtliches Mitteilungsblatt Nr. 63/2015: Fachspezifische Studien- und Prüfungsordnung für das lehramtsbezogene Masterstudium im Fach Physik (Schwerpunkt Gymnasium). Erstes und Zweites Fach.*

Jelezko, F. & Wrachtrup, J. (2006). Single defect centres in diamond: A review. *physica status solidi (a)*, *203* (13), 3207–3225. doi: 10.1002/pssa.200671403

Kewitsch, G. (2013). *Entwicklung einer FPGA-basierten Steuereinheit für Quantenkryptographieexperimente* (Masterarbeit zur Erlangung des akademischen Grades Master of Engineering). Beuth Hochschule für Technik Berlin.

Kroh, T. (2012). *Charakterisierung von Quantenpunkt-Einzelphotonen für Quantenrepeater-Anwendungen* (Masterarbeit zur Erlangung des akademischen Grades Master of Science (M. Sc.) im Fach Physik). Humboldt-Universität zu Berlin.

Leifgen, M. (2016). *Protocols and Components for Quantum Key Distribution* (Dissertation zur Erlangung des akademischen Grades doctor rerum naturalium (Dr. rer. nat.) im Fach Physik, Humboldt-Universität zu Berlin). Zugriff am 03.07.2016 auf `http://edoc.hu-berlin.de/dissertationen/leifgen-matthias-2016-03-15/PDF/leifgen.pdf`

Leifgen, M., Wahl, M., Berlin, M., Röhlicke, T., Rahn, H.-J. & Benson, O. (2011). An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. *Applied Physics Letters*, *98* (17). doi: 10.1063/1.3578456

Mandel, M. M. (2014). *Implementierung des Versuchs "Magneto-optische Falle" für das Fortgeschrittenenpraktikum* (Bachelorarbeit zur Erlangung des akademischen Grades Bachelor of Science (B. Sc.) im Lehramtsstudium (Kernfach: Physik; Zweitfach: Mathematik)). Humboldt-Universität zu Berlin.

Nielsen, M. A. & Chuang, I. L. (2005). *Quantum computation and quantum information* (8. Aufl.). Cambridge: Cambridge Univ. Press.

Riemann, R. (2013). *Implementierung einer Steuerung für ein Quantum Key Distribution (QKD) Experiment inklusive Postprocessing.* (Masterarbeit zur Erlangung des akademischen Grades Master of Science (M. Sc.) im Fach Physik). Humboldt-Universität zu Berlin.

Schröder, T. (2012). *Integrated photonic systems for single photon generation and quantum applications: Assembly of fluorescent diamond nanocrystals by novel nano-manipulation techniques* (Dissertation zur Erlangung des akademischen Grades doctor rerum naturalium (Dr. rer. nat.) im Fach Physik, Humboldt-Universität zu Berlin). Zugriff am 03.07.2016 auf `http://edoc.hu-berlin.de/dissertationen/schroeder-tim-2012-08-30/PDF/schroeder.pdf`

Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, *28* (4), 656–715. doi: 10.1002/j.1538-7305.1949.tb00928.x

Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, *26* (5), 1484–1509. doi: 10.1137/S0097539795293172

Shor, W. & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. *Physical review letters*, *85* (2), 441–444. doi: 10.1103/PhysRevLett.85.441

Singh, S. (2001). *Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet* (1. Aufl.). München: Hanser.

Vernam, G. S. (1919). *Secret signaling system* (Nr. US 1310719 A).

Vernam, G. S. (1926). Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the A.I.E.E.*, *45* (2), 109–115. doi: 10.1109/JAIEE.1926.6534724

Walls, D. F. & Milburn, G. J. (Hrsg.). (2008). *Quantum Optics*. Berlin, Heidelberg: Springer-Verlag. doi: 10.1007/978-3-540-28574-8

WhatsApp (Hrsg.). (2016). *WhatsApp Encryption Overview: Technical white paper.* Zugriff am 02.07.2016 auf `https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf`

Wootters, W. K. & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, *299* (5886), 802–803. doi: 10.1038/299802a0

Abkürzungen

Fachliche Abkürzungen

APD avalanche photodiode (Lawinenphotodiode)

ASCII American Standard Code for Information Interchange

BB84 BB84-Protokoll zum Quantenschlüsselaustausch

BKA Bundeskriminalamt

DAC digital analog converter (Digital-Analog-Wandler)

EOM Elektrooptischer Modulator

F-Praktikum Fortgeschrittenenpraktikum

FPGA field programmable gate array

HBT Hanbury Brown & Twiss Aufbau

HV-Basis rektilineare Basis mit Basiszuständen $|\updownarrow\rangle$ und $|\leftrightarrow\rangle$

NSA National Security Agency

NV nitrogen-vacancy center (Stickstoff-Fehlstellen-Zentrum)

OTP One Time Pad

PBS polarising beam splitter (Polarisations-Strahlteilerwürfel)

Qubit Quantenbit

QBER quantum bit error rate

QKD Quantum Key Distribution (Quantenschlüsselaustausch)

RL-Basis zirkulare Basis mit Basiszuständen $|\circlearrowleft\rangle$ und $|\circlearrowright\rangle$

SIL solid immersion lens (Öl-Immersionslinse)

S/MIME Secure / Multipurpose Internet Mail Extensions

SPS single photon source (Einzelphotonenquelle)

SSL Secure Sockets Layer

TAN Transaktionsnummer

TLS Transport Layer Security

Weitere Abkürzungen

Abb. Abbildung

bzw. beziehungsweise

d.h. das heißt

f. und folgende Seite

ff. und folgende Seiten

ggf. gegebenenfalls

s. siehe

S. Seite

sog. sogenannt

Tab. Tabelle

vgl. vergleiche

z.B. zum Beispiel

Abbildungsverzeichnis

Tabellenverzeichnis

Anhang A

Versuchsanleitung

Auf den folgenden Seiten findet sich die in dieser Arbeit erstellte Versuchsanleitung im Wortlaut. Die Nummerierung der Seiten folgt dabei der Nummerierung innerhalb der Versuchsanleitung.

Humboldt Universität zu Berlin
Mathematisch-Naturwissenschaftliche Fakultät
Institut für Physik

Anleitung zum Versuch

Quantenkryptographie mit einzelnen Photonen – QKD via BB84

Fortgeschrittenen-Praktikum

Stand: Oktober 2016

Inhaltsverzeichnis

1 Einleitung

Es gehört zu den ältesten Bestrebungen des Menschen, Wissen geheim zu halten und nur dem beabsichtigten Adressaten zugänglich machen zu wollen. Heutzutage werden ausgeklügelte mathematische Verfahren in Verbindung mit leistungsstarker Technik eingesetzt, um Informationen zu schützen – oder um gerade diesen Schutz auszuhebeln [Sin01, S. 353 ff. und S. 383 ff.]. Kennzeichnend für viele Verschlüsselungen ist, dass ein **Schlüssel** zur Umwandlung des sogenannten **Klartextes** (d.h. der geheim zu haltenden Nachricht) in den sogenannten **Geheimtext** benutzt wird. Im Cäsar-Chiffre wird z.B. jeder Buchstabe um drei Stellen verschoben [Sin01, S. 26], somit ergibt sich aus dem Klartext H U B der Geheimtext K X E unter Verwendung des Schlüssels 3.
Das *One Time Pad*-Verfahren (OTP) kann absolute Sicherheit der Verschlüsselung ermöglichen, wenn der Schlüssel bestimmte Voraussetzungen erfüllt [Sin01, S. 152]. Damit ist das Hauptproblem der Kryptographie die sichere Schlüsselübertragung. Derzeit am verbreitetsten sind dafür sogenannte asymmetrische Verfahren [Sin01, S. 372]. Diese Verfahren beruhen auf mathematischen Problemen wie der Faktorisierung großer Zahlen [Sin01, S. 329 ff.], welche bisher nicht durch effiziente Algorithmen gelöst werden konnten. Eine entsprechende Erhöhung der Rechenleistung von Computern macht diese Verfahren also potentiell angreifbar. Gefährlich wäre in diesem Zusammenhang auch ein funktionierender Quantencomputer, für den bereits Algorithmen (z.B. der Shor-Algorithmus zum Faktorisieren einer Zahl, siehe [Sho97]) entwickelt wurden, welche die zur Zeit hauptsächlich eingesetzte asymmetrische Verschlüsselung wertlos machen würde [Sin01, S. 386].
Durch einen Quantenschlüsselaustausch (*Quantum Key Distribution*, QKD) kann dagegen bedingungslose Sicherheit (meist als *unconditional security* bezeichnet) durch Ausnutzung fundamentaler physikalischer Gesetze erreicht werden. Dabei kann zwar nicht ausgeschlossen werden, dass auch hier die Schlüsselübertragung abgehört wird, jedoch kann das nie unbemerkt geschehen. Der Lauscher fällt schon auf, während der Schlüssel ausgetauscht wird, bevor also die eigentliche Nachricht gesendet wird. Aus diesem Grund kann er zwar im schlimmsten Fall die Kommunikation unterbinden, aber nicht einmal ansatzweise Informationen über den Inhalt der Nachricht erhalten. Die Quantenkryptographie schützt damit nicht nur den Inhalt der Nachricht, sondern erlaubt es auch, einen Lauscher sofort zu entdecken [Sin01, S. 411 ff.].

In diesem F-Praktikumsversuch wird an einem Aufbau für eine QKD gearbeitet, welcher dem von Charles Bennett und Gilles Brassard entwickelten BB84-Protokoll (BB84) folgt. Ziel ist es, die Übertragung eines Schlüssels nach BB84 durchzuführen und dabei die Eignung der im Aufbau verwendeten Geräte für dieses Quantenkryptographieverfahren zu beurteilen.

Wir freuen uns über jede Kritik am Versuch und an der Anleitung. Bitte geben Sie uns daher zum Versuchsende ein Feedback!

2 Aufgaben

Versetzen Sie sich in die Situation eines Forschenden an einer Hochschule oder in einer Firma, die oder der ein Gerät zur QKD nach BB84 entwickeln möchte. Beurteilen Sie aus dieser Sicht die Eignung der im vorliegenden Aufbau verwendeten Geräte.

Vorbereitung

1. Machen Sie sich anhand dieser Versuchsanleitung und eigener Quellen mit den Themen Quanteninformationsverarbeitung, Quantenkryptographie und dem Ablauf des BB84-Protokolls vertraut. Verschaffen Sie sich dabei auch einen Überblick über den verwendeten Aufbau und die Durchführung der daran möglichen Messungen.

2. Informieren Sie sich über Kenndaten und Wirkungsweise der im Aufbau verwendeten Geräte, vor allem Laser, Elektrooptischer Modulator (EOM), Lawinenphotodiode (APD), Polarisatoren und Verzögerungsplatten ($\frac{\lambda}{2}$- bzw. $\frac{\lambda}{4}$-Plättchen).

Für Ihre Recherche können Sie neben den im Folgenden genannten Quellen natürlich auch eigene verwenden:

- Datenblätter der verwendeten Geräte (beim Betreuenden erhältlich)
- Demtröder, W. (2013). *Experimentalphysik 2: Elektrizität und Optik.* Berlin: Springer. Online verfügbar unter: `http://www.springer.com/de/book/9783642299438` – Kapitel 8.6 Erzeugung und Anwendung von polarisiertem Licht
- Schiffner, G. (2005). *Optische Nachrichtentechnik: Physikalische Grundlagen, Entwicklung, moderne Elemente und Systeme.* Wiesbaden: Vieweg+Teubner Verlag. Online verfügbar unter: `http://link.springer.com/book/10.1007%2F978-3-322-80061-9` – Kapitel 7.1 Polarisatoren, 7.2 Verzögerungsplatten, 9 Photodioden und optische Empfänger (insbesondere 9.6 Ausführungsformen von Lawinenphotodioden) und 10.3 Elektrooptische Modulatoren

Durchführung

3. Legen Sie fest, welche Messungen Sie für die Beurteilung der Geräte durchführen möchten. Dabei können Sie sich an den in Kap. 5 beschriebenen Schritten orientieren und Details mit dem Versuchsbetreuenden festlegen. Sie entscheiden dabei selbstständig, was und in welchem Umfang Sie messen wollen und dokumentieren Ihre Ergebnisse eigenständig.

4. Bereiten Sie den Aufbau für die Übertragung eines Schlüssels mittels des Lasers vor.

5. Verwenden Sie sowohl den Laser im gepulsten und im Dauerstrichbetrieb als auch die Einzelphotonenquelle um Übertragungen durchzuführen.

6. Bestimmen Sie den Verlauf der Autokorrelation für die von Ihnen zur Erzeugung der Photonen verwendeten NV-Zentren.

Auswertung

7. Verfassen Sie einen Bericht (Protokoll) über Ihre Ergebnisse. Orientieren Sie sich dabei an den geltenden Standards im F-Praktikum und beziehen Sie sich in der Diskussion auf den eingangs genannten Kontext. Erörtern Sie dazu die Eignung der verwendeten Geräte für eine kommerzielle Anwendung, gehen Sie auf Grenzen und mögliche Alternativen ein und vergleichen Sie insbesondere die beiden verwendeten Photonenquellen.

3 Theoretische Beschreibung

3.1 *One Time Pad* zur klassischen Verschlüsselung

Das *One-Time-Pad*-Verfahren kann eingesetzt werden, um mit dem über die QKD übertragenen Block aus Schlüsseln (dem sogenannten *Pad*) die Chiffrierung der eigentlichen Nachricht durchzuführen. Da für die Quantenkryptographie nur binäre Daten betrachtet werden, wird auch im folgenden davon ausgegangen, dass sowohl Klartext als auch Schlüssel in dieser Form vorliegen. Um z.B. einen Text zu chiffrieren, kann der Klartext zuerst über eine ASCII-Tabelle (oder ein vergleichbares Verfahren) in eine binäre Form gebracht werden.

Durchführung einer Chiffrierung

Um zu verschlüsseln, wird jedes Bit des Klartextes mit einem Bit des Schlüssels binär addiert, das Ergebnis also modulo 2 genommen, wodurch sich insbesondere die Summe $1 + 1 = 0$ ergibt. Die so erhaltenen Bits bilden dann den binären Geheimtext, der ggf. wiederum in Zeichen zurückübersetzt wird. Dies ist in Abb. 1 an einem Beispiel dargestellt. Der Empfänger der Nachricht geht zum Entschlüsseln wie der Sender vor und addiert ebenfalls den Schlüssel binär und bitweise zu dem Geheimtext, um den Klartext zu erhalten. Möglich ist das, weil die Bit-Werte 0 und 1 additiv invers zu einander (modulo 2) sind. Denn damit ergibt die Subtraktion zweier Bits das gleiche Ergebnis wie die Addition.

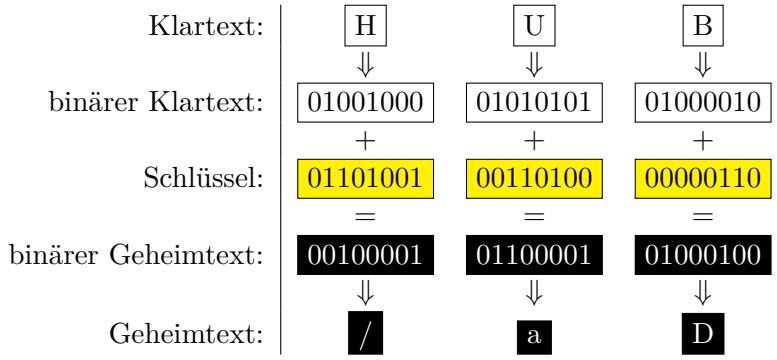


Abbildung 1 – Beispiel einer Chiffrierung in binärer Form nach dem OTP-Verfahren.
Der Klartext H U B wird über eine ASCII-Tabelle in eine binäre Form gebracht und mit dem vorher übermittelten Schlüssel binär addiert. Der so entstandene Geheimtext kann binär oder als Zeichenfolge / a D dargestellt werden.

Voraussetzungen des Verfahrens

Als Erfinder des OTP-Verfahrens wird meist G. Vernam gesehen, der es erstmalig zum Patent anmeldete.
Er beschreibt in [Ver26] als Voraussetzungen für die Sicherheit des Verfahrens:

1. Der Schlüssel ist, ohne sich zu wiederholen, so lang wie der Klartext.
2. Der Schlüssel (bzw. Teile daraus) wird nur einmal eingesetzt.
3. Der Schlüssel ist aus unvorhersagbar zufälligen Zeichen zusammengesetzt.

Unter diesen Voraussetzungen ist im Rahmen der Kommunikationstheorie beweisbar, dass der Klartext ohne Kenntnis des Schlüssels nicht ermittelt werden kann [Sha49, S. 682].

3.2 Einzelphotonen als Grundlage der Quantenkryptographie

Die Sicherheit der Quantenkryptographie beruht zum einen auf der Verwendung des OTP-Verfahrens, zum anderen darauf, jeden Lauschangriff auf die Schlüsselübertragung zu bemerken. Für Letzteres ist es in den meisten Fällen unerlässlich, einzelne Photonen zur Schlüsselübertragung zu verwenden. Denn wenn auch nur zwei Photonen dieselbe Information tragen, ist es prinzipiell möglich über einen sogenannten *photon number splitting*-Angriff unbemerkt an eine Kopie der Information zu gelangen.
Nachfolgend wird darum einerseits eine Einzelphotonenquelle (*single photon source*, SPS) auf Basis von Defektzentren in Nanodiamanten vorgestellt und andererseits das Verfahren der Autokorrelationsmessung als Nachweis von einzelnen Photonen beschrieben.

Defektzentren in Nanodiamanten

Ein vielversprechender Kandidat für eine SPS sind Defektzentren in Diamanten [ACS+11]. Die räumliche Ausdehnung der Diamanten liegt dabei oft in der Größenordnung von Nanometern, weshalb sie als Nanodiamanten bezeichnet werden. Ein Defektzentrum ist eine durch den Eintrag von Fremdatomen oder Fehlstellen im Kristallgitter des Kohlenstoffs erzeugte Struktur.
Die hier verwendete SPS enthält Stickstoff-Fehlstellen-Zentren (*nitrogen-vacancy center*, NV), bei denen ein Kohlenstoffatom des Diamants durch ein Stickstoffatom ersetzt wird und dazu benachbart eine Lücke (englisch *vacancy*) im Kristallgitter auftritt (vgl. Abb. 2a). Dieses NV-Zentrum wird durch grünes Laserlicht (532 nm) angeregt und sendet Photonen im sichtbaren roten und infraroten Bereich aus. Modellhaft gesehen wäre die einfachste Struktur, die für eine SPS in Frage kommt, ein Zwei-Niveau-System aus einem Grund- und einem angeregten Zustand. Diese sendet bei entsprechender optischer Anregung Photonen mit definierten Eigenschaften aus. Meist handelt es sich in der Praxis jedoch um Drei- oder Mehr-Niveau-Systeme, die metastabile Zustände zwischen Grund- und angeregtem Zustand enthalten (vgl. Abb. 2b).
Der herausragende Vorteil in der Verwendung von NV-Zentren als SPS liegt in der einfachen Handhabung. So muss die Quelle nicht gekühlt werden und kann in kompakter Bauform realisiert werden [Sch12, S. 15].

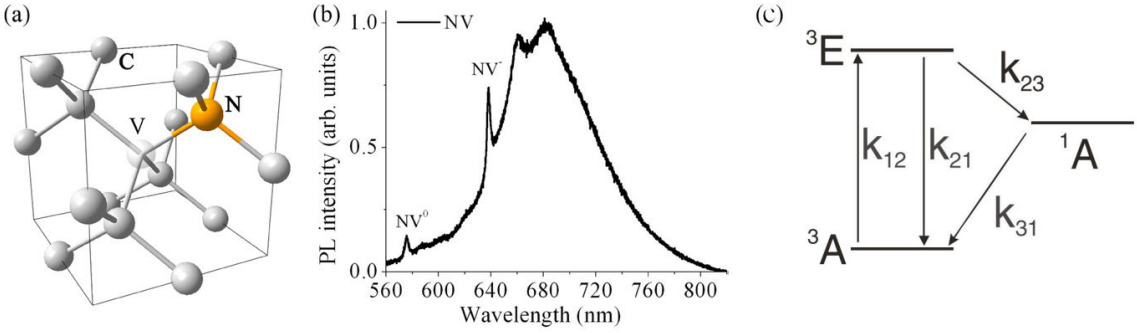


Abbildung 2 – Kristallographisches Modell, Spektrum und Drei-Niveau-Schema zur Beschreibung eines NV-Zentrums aus [ACS+11, JW06, S. 5 bzw. S. 3211].
a) Ein Stickstoffatom (mit N bezeichnet) ersetzt ein Kohlenstoffatom im Kristallgitter des Diamants, benachbart dazu tritt eine Lücke (mit V bezeichnet) auf.
b) Das Spektrum bei Raumtemperatur weist zwei charakteristische Spitzen bei 575 nm (neutrales NV-Zentrum) und 637 nm (negativ geladenes NV-Zentrum) auf.
c) Aus dem Grundzustand ${}^3A$ werden Elektronen mit einer Rate von k_{12} in den angeregten Zustand ${}^3E$ gehoben, aus dem sie mit k_{21} wieder nach ${}^3A$ zurück oder mit k_{23} in einen metastabilen Zustand ${}^1A$ übergehen können. k_{31} bezeichnet die Rate des Übergangs von dem metastabilen Zustand ${}^1A$ in den Grundzustand ${}^3A$.

Autokorrelation von Photonen

Die Anzahl von Photonen, die mit einem zeitlichen Abstand von τ von einer Quelle erzeugt werden, lässt sich über die normierte Korrelationsfunktion zweiter Ordnung beschreiben [WM08, S. 39]:

$$g^{(2)}(\tau) = \frac{\langle : I(0)I(\tau) : \rangle}{|\langle I \rangle|^2} \tag{1}$$

Dabei ist I der Intensitätsoperator, $: \cdots :$ entspricht der Normalordnung und $\langle \ldots \rangle$ gibt an, dass es sich um einen Mittelwert handelt. Betrachtet man diese Funktion zu $\tau = 0$, also Photonen, die zur gleichen Zeit detektiert werden, so ergibt sich für Photonenzahlzustände (bzw. Fockzustände) $|n\rangle$ aus n Photonen im selben Zustand [WM08, S. 41]:

$$g^{(2)}(0) = 1 - \frac{1}{n} \tag{2}$$

Wurde also nur ein Photon erzeugt, ist $g^{(2)}(0) = 0$, bei zweien $g^{(2)}(0) = \frac{1}{2}$ usw. Da in der Praxis noch Effekte auftreten, die im Modell vernachlässigt werden, wird der ideale Wert $g^{(2)}(0) = 0$ allerdings auch für Einzelphotonenquellen nicht immer erreicht. Solange jedoch $g^{(2)}(0) < \frac{1}{2}$ ist, kann davon ausgegangen werden, dass das detektierte Licht einen dominierenden Anteil von Einzelphotonen enthält.
Im Fall eines Drei-Niveau-Systems mit Übergangsraten k_{ij} von dem i-ten in den j-ten Zustand (vgl. Abb. 2b), kann die Autokorrelation in guter Näherung von einer Funktion der folgenden Form beschrieben werden [JW06, S. 3213]:

$$g^{(2)}(\tau) = 1 - (K+1)\, e^{k_+ \tau} + K e^{k_- \tau} \tag{3}$$

Dabei ist $k_\pm = -\frac{1}{2}P \pm \sqrt{\frac{1}{4}P^2 - Q}$ mit $P = k_{21} + k_{12} + k_{23} + k_{31}$ und $Q = k_{31} \cdot (k_{21} + k_{12}) + k_{23} \cdot (k_{31} + k_{12})$, sowie $K = \frac{k_- + k_{31} - k_{12}\frac{k_{23}}{k_{31}}}{k_+ - k_-}$.

3.3 Quanteninformationsverarbeitung

Theoretische Beschreibung von Quantenbits

In Anlehnung an das binäre System aus der klassischen Informationsverarbeitung werden die Einheiten in der Quanteninformationsverarbeitung Quantenbits (Qubits) genannt. So wie ein klassisches Bit einen Zustand – entweder 0 oder 1 – besitzt, hat auch ein Qubit einen Zustand, der konventionell jedoch in Dirac-Notation wie folgt ausgedrückt wird [NC05, S. 13]:

$$|\Psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle \qquad \text{mit} \qquad \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1. \tag{4}$$

Dieser Zustand wird als Einheitsvektor in einem zweidimensionalen, komplexen Vektorraum (Hilbertraum) beschrieben, dessen Orthonormalbasis durch die Zustände $|0\rangle$ und $|1\rangle$ gebildet wird. Bei einer Messung in dieser Basis kollabiert der Zustand des Qubits in einen der Basiszustände, wobei die Beträge von α und β der Wahrscheinlichkeitsdichte entsprechen, den Wert 0 bzw. 1 zu erhalten: $|\langle 0|\Psi\rangle|^2 = |\alpha|^2$ und $|\langle 1|\Psi\rangle|^2 = |\beta|^2$. Der Kollaps der Wellenfunktion bewirkt insbesondere, dass eine weitere Messung in dieser Basis mit Sicherheit den gleichen Zustand wie die vorhergehende ergibt. Jegliche Information über den ursprünglichen Zustand geht somit durch die erste Messung verloren.
Darüber hinaus ist ein weiters Paar von Zuständen, $|+\rangle$ und $|-\rangle$, interessant. Sie bilden eine Orthonormalbasis des gleichen Vektorraumes, die mit der Basis aus den Zuständen $|0\rangle$ und $|1\rangle$ konjugiert ist. Das bedeutet, dass die Messung eines Basiszustands der einen Basis mit gleicher Wahrscheinlichkeit einen der beiden Basiszustände der anderen Basis ergibt.

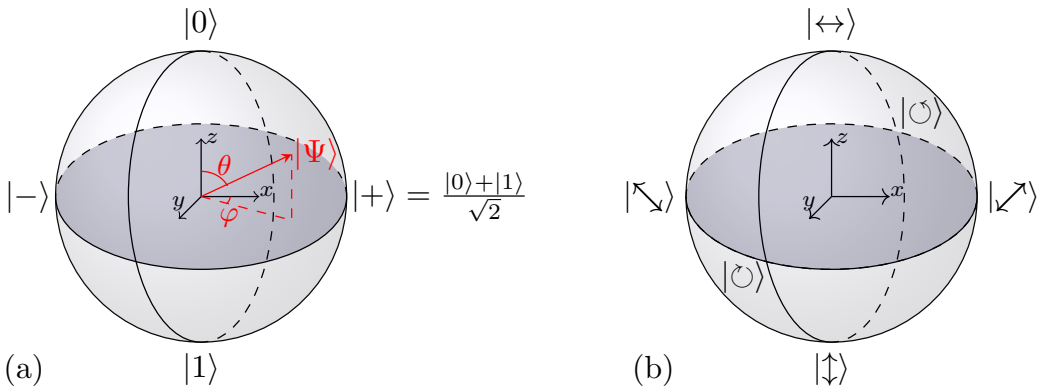


Abbildung 3 – Bloch- und Poincaré-Kugel.
a) Bloch-Kugel zur Veranschaulichung des Vektorraumes, in dem das Qubit im Zustand $|\Psi\rangle$ sich in einer Überlagerung der Basiszustände $|0\rangle$ und $|1\rangle$ befindet. Zustände, die auf gegenüberliegenden Seiten der Kugel liegen, sind orthogonal zueinander. Zustände auf dem Äquator kollabieren mit gleicher Wahrscheinlichkeit in einen der Basiszustände $|0\rangle$ oder $|1\rangle$.
b) Poincaré-Kugel zur Veranschaulichung der konjugierten Basen des polarisierten Lichts. Sie kann wie die Bloch-Kugel verwendet werden, um polarisierte Photonen als Qubit darzustellen.

Formal lassen sich die Zustände $|+\rangle$ und $|-\rangle$ wie folgt definieren [NC05, S. 22]:

$$|+\rangle = \frac{|0\rangle + e^{i\kappa}\,|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle + e^{i(\kappa+\pi)}\,|1\rangle}{\sqrt{2}}, \qquad \text{mit } \kappa \in [0,\pi]\,. \tag{5}$$

Unter den in Gleichung (4) genannten Bedingungen lässt sich der den Zustand des Qubits beschreibende Einheitsvektor auch über den Winkel φ zur x- bzw. θ zur z-Achse ausdrücken:

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)\cdot|0\rangle + e^{i\cdot\varphi}\cdot\sin\left(\frac{\theta}{2}\right)\cdot|1\rangle\,, \qquad \text{mit } \theta \in [0,\pi]\,, \varphi \in [0,2\pi]\,. \tag{6}$$

Dies führt zu einer anschaulichen Darstellung als Punkte in Polarkoordinaten auf der Oberfläche einer Einheitskugel, der sogenannten Bloch-Kugel (s. Abb. 3a).

Polarisierte Photonen als Quantenbits

Um diese Zustände von Qubit in der Praxis umzusetzen, können polarisierte Photonen eingesetzt werden. Eine mögliche Basis bilden dabei linear horizontal und vertikal polarisierte Photonen, wovon konventionell horizontal polarisierten Photonen im Zustand $|\leftrightarrow\rangle$ der Wert 0 und vertikal polarisierten Photonen im Zustand $|\updownarrow\rangle$ der Wert 1 zugeordnet werden. Diese Basis wird auch als rektilineare Basis (HV-Basis) bezeichnet.
Eine andere Wahl von Basiszuständen ist durch zirkular polarisierte Photonen in den Basiszuständen $|\circlearrowright\rangle$ (entspricht Wert 0) und $|\circlearrowleft\rangle$ (Wert 1) gegeben. Diese zirkulare Basis (RL-Basis) ist mit der HV-Basis konjugiert, die Zustände $|\leftrightarrow\rangle$,$|\updownarrow\rangle$ und $|\circlearrowright\rangle$,$|\circlearrowleft\rangle$ verhalten sich also zueinander so wie $|0\rangle\,, |1\rangle$ und $|+\rangle\,, |-\rangle$. Eine dritte Möglichkeit wäre die Verwendung von diagonal polarisierten Photonen, da die Diagonalbasis sowohl mit der HV- als auch der RL-Basis konjugiert ist.
Analog zur Bloch-Kugel kann auch dieser Sachverhalt auf einer Kugeloberfläche dargestellt werden, der sogenannten Poincaré-Kugel (s. Abb. 3b). Dies hat den Vorteil, dass Polarisationsmanipulationen als Rotation in der Poincaré-Kugel dargestellt werden können.

3.4 Ablauf des BB84-Protokolls

Das erste kryptographische Verfahren auf Basis der Quantenmechanik wurde 1984 von Charles Bennett und Gilles Brassard präsentiert [BB84]. Werden Sender und Empfänger der geheimen Nachricht als Alice und Bob bezeichnet, kann eine Übertragung mittels des BB84-Protokolls in fünf Schritten beschrieben werden, die in Abb. 4 illustriert sind.

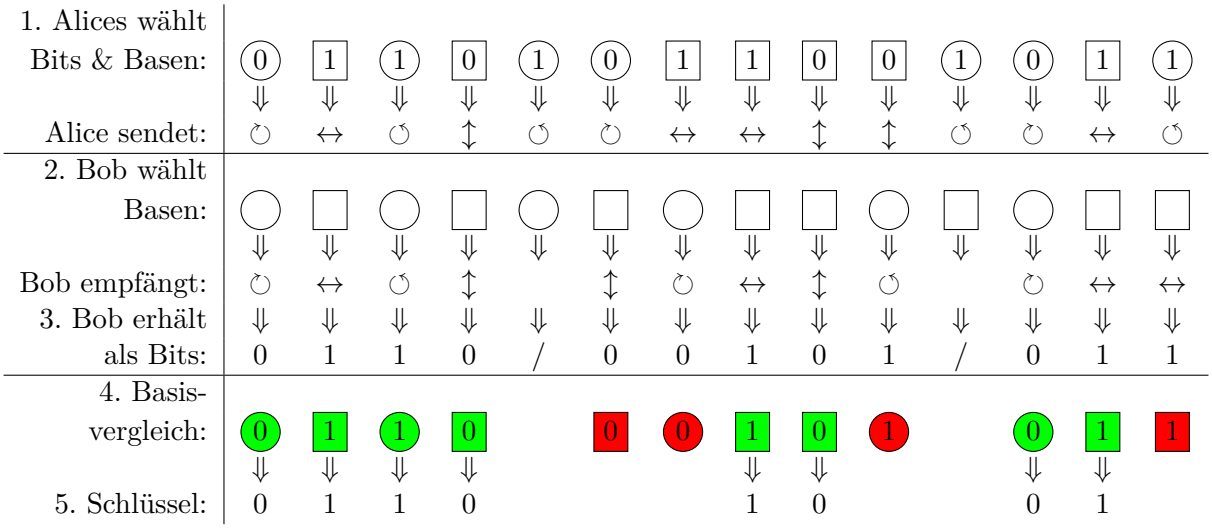


Abbildung 4 – Ablauf des BB84-Protokolls in 5 Schritten innerhalb von drei Phasen: Der Sender (Alice) übermittelt dem Empfänger (Bob) über einen Quantenkanal eine zufällige Folge von Bits in zufällig gewählten Basen (□ steht dabei für die rektilineare Basis, ◯ für die zirkulare) und sendet Bob eine Kette aus Photonen. Jedes Photon repräsentiert dabei 1 Bit der Folge in der für dieses Bit gewählten Basis. Wenn Bob diese Photonen empfängt (wobei es zu Übertragungsverlusten kommen kann, die mit / markiert wurden), entscheidet er für jedes davon zufällig und unabhängig von Alice, in welcher der beiden Basen er die Polarisation misst. Das Resultat der Messung interpretiert Bob als binäre 0 oder 1. Im Anschluss vergleichen Alice und Bob die korrekt übertragenen Bits (grün markiert) über einen öffentlichen Kanal und bestimmen daraus den Schlüssel.

Wie im letzten Kapitel erläutert, entsteht bei der Messung ein zufälliges Ergebnis, bei dem jede Information verlorengeht, wenn Bob die Polarisation nicht in der gleichen Basis wie Alice misst. Somit erhält Bob nur von im Mittel der Hälfte der detektierten Photonen brauchbare Daten. Da eine potentielle Lauscherin, meist Eve (nach englisch *eavesdropping*) genannt, vor dem gleichen Problem steht, birgt ein *intercept-resend*-Angriff das Risiko in sich, die Übertragung so zu verändern, dass die Übereinstimmung solcher Bits verringert wird, die nach Bobs Basiswahl eigentlich identisch zu Alice' Bits sein sollten. Darüber hinaus kann Eve nicht einen beliebigen unbekannten Quantenzustand des Photons kopieren [WZ82]. Wird für jedes Schlüsselbit nur ein Photon übertragen (wie in Kap. 3.2 beschrieben), kann sie das Signal auch nicht teilen, um unbemerkt Messungen durchzuführen.
Wurde die Übertragung nicht abgehört, sollten die in Schritt 4 verglichenen Bits idealerweise zu 100% übereinstimmen. Dieser Wert kann jedoch bei realen Übertragungen nie erreicht werden, da immer Verluste bei der Übertragung oder Detektion auftreten können. Wurde die Übertragung vollständig abgehört, sollten immer noch im Mittel 75% der verglichenen Bits übereinstimmen, da Eve bei im Mittel 50% von diesen Bits die korrekte Basis gewählt, bei den anderen aber dennoch zu 50% das richtige Qubit erhalten hat.
Wurden mehr als 88% richtig übertragen, kann der Schlüssel durch anschließende Prozesse (wie *error correction* und *privacy amplification*) soweit verbessert werden, dass eine sichere Übertragung dennoch möglich ist [SP00]. In diesem Fall können die übertragenen Bits als Schlüsselblock für anschließende geheime Kommunikation per OTP-Verfahren über einen öffentlichen Kanal verwendet werden.

4 Aufbau

Die gesamte experimentelle Realisierung ist kompakt gestaltet, sodass der optische Aufbau in einem Kasten mit den Maßen $122 \times 60 \times 30\,\mathrm{cm}^3$ Platz findet und zusammen mit den weiteren Geräten auf einem einzigen Tisch angeordnet werden kann. Daraus ergibt sich eine Freistahlstrecke von etwa einem halben Meter zwischen den Apparaten von Senderin und Empfänger (im Folgenden wieder als Alice und Bob bezeichnet).

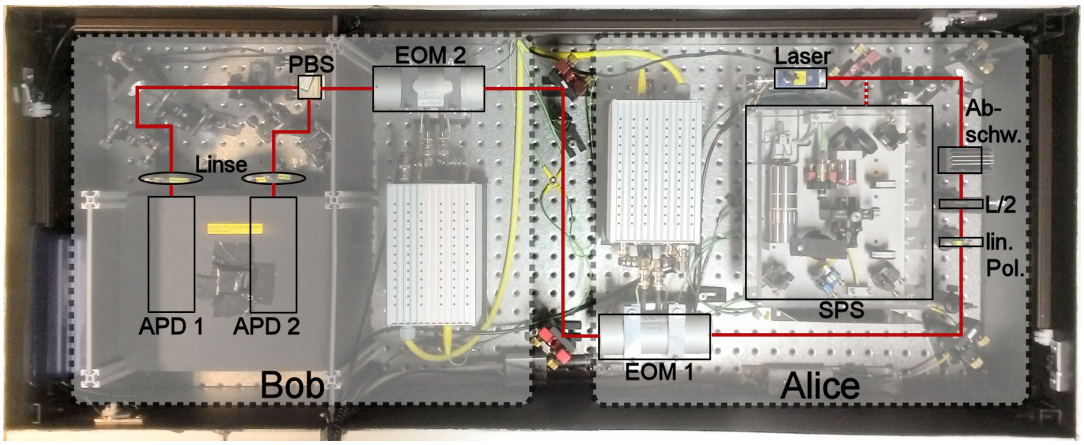


Abbildung 5 – Fotografische Darstellung des QKD-Aufbaus.
Photonen werden durch einen abgeschwächten Laser oder eine Einzelphotonenquelle (*single photon source*, SPS) erzeugt. Alice stellt mit Hilfe von $\frac{\lambda}{2}$-Plättchen (L/2) und linearem Polarisator (lin. Pol.) Photonen mit definierter Polarisation bereit. Mit dem Elektrooptischen Modulator (EOM 1) kann sie Basis und Bit einstellen. Bob detektiert die über einen weiteren EOM (EOM 2) und einen Polarisations-Strahlteilerwürfel (PBS) je nach übermitteltem Bit-Wert getrennten Photonen mittels zwei Lawinenphotodioden (APDs).
Werden die EOMs so eingestellt, dass die Photonen nach EOM 2 zirkular polarisiert sind, fungiert das Ensemble von PBS und APDs als Hanbury Brown & Twiss Aufbau (HBT).

Eine Übersicht über den aktuellen Aufbau ist in Abb. 5 dargestellt und wird im Folgenden näher erläutert. Photonen werden entweder mittels einer Laserdiode (QL65D6SA, Roithner, Treiber: iC-NZN EVAL, ic-Haus) mit einer Wellenlänge von 650 nm oder einer kompakten Einzelphotonenquelle (SPS) auf Basis von NV-Zentren erzeugt. Der Laser kann dabei entweder durchgehend Photonen im sogenannten Dauerstrichbetrieb aussenden oder alle 2,5 µs einzelne Pulse. Mit einem $\frac{\lambda}{2}$-Plättchen (PRM1/M, ThorLabs) wird die Polarisation dieser Photonen anschließend auf die vertikale Polarisationsrichtung eines linearen Polarisators (RSP05/M, ThorLabs) eingestellt.
Da alle Photonen nun die selbe Polarisation aufweisen, können sämtliche von Alice wählbaren Bit-Werte in den zugehörigen Polarisationsbasen durch den Einsatz von $\frac{\lambda}{2}$- und $\pm\frac{\lambda}{4}$-Plättchen im 45°-Winkel zur vertikalen Polarisation realisiert werden. Um diese Einstellung innerhalb einer möglichst kurzen Zeitspanne wechseln zu können, kommt dafür ein Elektrooptischer Modulator (EOM, im Folgenden EOM 1) auf Basis von Kaliumdideuteriumphosphat-Kristallen (LM0202 P VIS, Linos) zum Einsatz, der je nach angelegter Spannung wie ein $\frac{\lambda}{2}$- ,$+\frac{\lambda}{4}$- oder $-\frac{\lambda}{4}$-Plättchen wirkt.
Nun verlassen die Photonen Alice's Aufbau um nach etwa einem halben Meter Freistrahlstrecke bei Bob anzukommen. Bei diesem erfolgt die Basiswahl ebenfalls über ein EOM (im Folgenden EOM 2) in Verbindung mit einem Polarisations-Strahlteilerwürfel (PBS). Der EOM lässt dabei je nach Bobs Messbasis die ankommenden Photonen in ihrer Polarisationsbasis oder vertauscht lineare und zirkulare Polarisation miteinander. Durch den PBS werden daraufhin linear polarisierte Photonen mit Sicherheit an einem von zwei Detektoren registriert, zirkular polarisierte dagegen unvorhersagbar an einem der beiden

Detektoren. Zur Detektion der Photonen werden Lawinenphotodioden (*avalanche photodiode*, APD) auf Siliziumbasis (SPCM-AQRH-33, Excelitas) verwendet, auf die mit einer Linse fokussiert wird. Da die vom Laser ausgestrahlte Leistung für diese viel zu hoch ist und sie überlasten würde, kommen Abschwächer zur Reduktion der Laserleistung zum Einsatz.

4.1 Geräte

Kompakte Einzelphotonenquelle

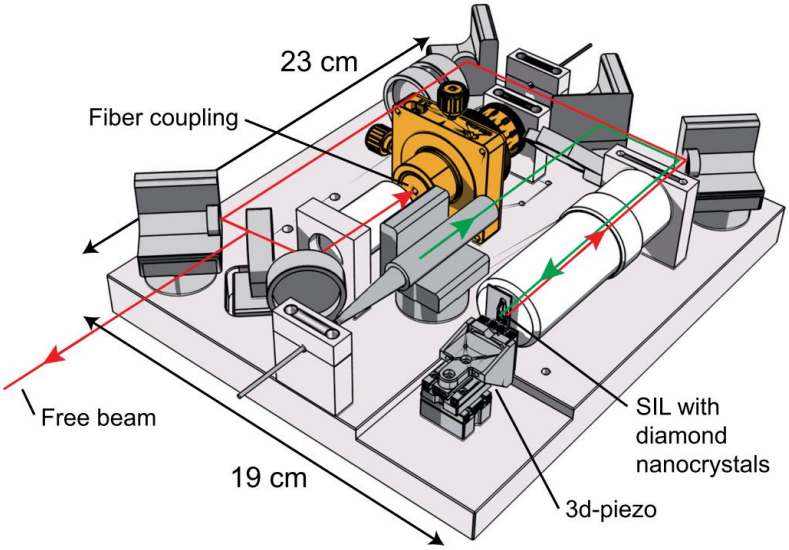


Abbildung 6 – Darstellung der verwendeten Einzelphotonenquelle [Sch12, S. 148].
Unten im Bild befindet sich die Probe mit den Naondiamanten zusammen mit der Öl-Immersionslinse (SIL) auf einem 3D-Piezo-Tisch. Der grüne Anregungslaser (532 nm) wird über eine Faser eingekoppelt, über einen dichroitischen Spiegel (nicht im Bild) durch das Objektiv auf die SIL gelenkt und regt dort ein NV-Zentrum zur Aussendung von einzelnen Photonen an. Diese können den dichroitischen Spiegel im Gegensatz zu den reflektierten Photonen des Anregungslasers ungehindert passieren und werden per Freistrahlkopplung zu Alice' Aufbau gelenkt.

Eine Übersicht über den Aufbau der kompakten Einzelphotonenquelle ist in Abb. 6 dargestellt. Die Erzeugung der Photonen geschieht in Nanodiamanten mit NV-Defektzentren, die auf einer Öl-Immersionslinse (*solid immersion lens*, SIL) aufgebracht sind. Diese sorgt zusammen mit einem Objektiv durch einen höheren Brechungsindex zwischen Objekt und Linse für eine effizientere Aufsammlung der Photonen. Die dreidimensionale Positionierung der Probe erfolgt dabei mittels eines Piezo-Tisches (SLC-1720-S-HV, SmarAct, Treiber: MCS-3D, SmarAct). Ein 532 nm-Laser (etwa 100 µW) regt die NV-Defektzentren bei Raumtemperatur an. Um die emittierten Photonen von dem reflektierten 532 nm-Laser zu trennen, wird ein dichroitischer Spiegel verwendet. Ein Kurzpassfilter (785 nm, im Bild nicht zu sehen) und zwei Langpassfilter (620 nm, im Bild nicht zu sehen) filtern verbleibendes Licht aus. Die Photonen der SPS können nun entweder in eine Faser eingekoppelt oder per Freistrahl weitergeleitet werden, wobei in diesem Versuch Letzteres eingesetzt wird.

Hanbury Brown & Twiss Aufbau

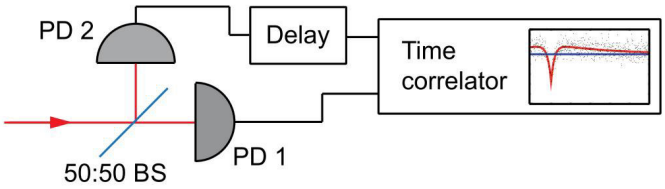


Abbildung 7 – Darstellung des Hanbury Brown & Twiss Aufbaus zur Bestimmung der Autokorrelation [Sch12, S. 11].
Die eingestrahlten Photonen werden durch einen 50:50-Strahlteiler (in der Abb. 50:50-BS) mit gleicher Wahrscheinlichkeit an einem von zwei Photodetektoren (in der Abb. PD) registriert, die eine Zeitmessung starten bzw. stoppen (in der Abb. am „Time correlator“). Einer der beiden Kanäle wird dabei gegenüber dem anderen verzögert (in der Abb. am „delay“), um eine Verschiebung des zeitlichen Nullpunktes zu erreichen.

Um eine Autokorrelationsmessung durchzuführen, kann der vorhandene Aufbau als sogenannter Hanbury Brown & Twiss Aufbau verwendet werden. Der Aufbau ist schematisch in Abb. 7 dargestellt. Er besteht aus einem Gerät zur Zeitmessung im Nanosekundenbereich (*TimeHarp*), einem 50:50-Strahlteiler, und zwei Einzelphotonendetektoren, von denen der eine als Start-, der andere als Stop-Signalgeber für die Zeitmessung fungiert. Die am Strahlteiler ankommenden Photonen werden zu gleicher Wahrscheinlichkeit an einem der beiden Detektoren registriert. Wird die Anzahl an Koinzidenzen zwischen beiden Detektoren über der zeitlichen Verzögerung τ zwischen zwei Ereignissen aufgetragen, ergibt sich ein charakteristischer Verlauf. Dieser kann als Maß für die Korrelationsfunktion zweiter Ordnung $g^{(2)}(\tau)$ genommen werden, wenn er entsprechend normiert wird.
Da in dem für die QKD verwendeten Aufbau zwei APDs als Detektoren und ein PBS zur Verfügung stehen, müssen lediglich beide EOMs so eingestellt werden, dass sie zusammen wie ein $\frac{\lambda}{4}$-Plättchen wirken und so am PBS einfallende Photonen mit gleicher Wahrscheinlichkeit an einer der beiden APDs registriert werden.

Polarisationsmanipulation mittels EOMs

Die eingangs durch den linearen Polarisator auf vertikal eingestellte Polarisation der Photonen wird bei Alice mithilfe von EOM 1 so manipuliert, dass sie dem zu dem Bit gehörenden Basiszustand in der gewählten Basis entspricht: Will Alice Bit 0 in Basis 0 senden, belässt sie die vertikale Polarisation unverändert, für Bit 1 in Basis 0 lässt sie EOM 1 wie ein $\frac{\lambda}{2}$-Plättchen wirken, um die Polarisation um 90° zu drehen. In Basis 1 dagegen muss Alice das Photon zirkular polarisieren. Dafür stellt sie ihr EOM je nach Bit-Wert als $+\frac{\lambda}{4}$- (Bit 0) oder $-\frac{\lambda}{4}$-Plättchen (Bit 1) ein.
Bei Bob wird EOM 2 zur Basiswahl verwendet. Will Bob in der HV-Basis (Basis 0) messen, lässt er EOM 2 als $\frac{\lambda}{2}$-Plättchen wirken, was die Polarisationsbasis des Photons bestehen lässt. Will er dagegen in der RL-Basis (Basis 1) messen, wirkt sein EOM als $+\frac{\lambda}{4}$-Plättchen und wandelt zirkulare in lineare Polarisation und umgekehrt. Durch einen PBS hinter EOM 2 wird das Photon dann entsprechend seiner Polarisation an einer von zwei APDs registriert, sofern es linear polarisiert ist. Ist es dagegen zirkular polarisiert, wird es mit gleicher Wahrscheinlichkeit an einem der beiden Detektoren registriert. Da horizontal polarisierte Photonen dabei an APD 1 registriert werden, wird der Bit-Wert 0 dieser APD zugewiesen.

Diese Einstellungen und Zuordnungen ermöglichen eine Übertragung nach den Prinzipien des BB84-Protokolls, denn:

- Sendet Alice Bit 0 in Basis 0, so bleibt das Photon hinter EOM 1 im Zustand $|\updownarrow\rangle$. EOM 2 wandelt diesen in $|\leftrightarrow\rangle$, sofern Bob sich ebenfalls für Basis 0 entscheidet, und in $|\circlearrowright\rangle$, falls er Basis 1 wählt. Durch Verwendung des PBS wird der Zustand $|\leftrightarrow\rangle$ mit Sicherheit an APD 1 (Bit 0) registriert, $|\circlearrowright\rangle$ dagegen zu je 50% an einer der beiden APDs.
- Sendet Alice dagegen Bit 1 in Basis 0 und misst Bob in derselben Basis, wirken beide EOMs als $\frac{\lambda}{2}$-Plättchen, wodurch das Photon im Zustand $|\updownarrow\rangle$ an APD 2 (Bit 1) registriert werden kann. Wählt Bob die falsche Basis, erhält er ein Photon im Zustand $|\circlearrowleft\rangle$, welcher durch den PBS ebenfalls zu je 50% an einer der beiden APDs registriert wird.
- Entscheidet sich Alice für Basis 1, ergibt sich an EOM 1 je nach Bit-Wert der Zustand $|\circlearrowright\rangle$ (Bit 0) oder $|\circlearrowleft\rangle$ (Bit 1). Misst Bob in Basis 0, ist das Resultat wiederum nicht vorhersagbar, bei Basis 1 misst er dagegen mit Sicherheit Alice' Bit 0 an APD 1 (da EOM 2 $|\circlearrowright\rangle$ in $|\leftrightarrow\rangle$ wandelt) bzw. Bit 1 an APD 2 (indem $|\circlearrowleft\rangle$ in $|\updownarrow\rangle$ gewandelt wird).

4.2 Ansteuerung

Der gesamte Versuchsaufbau wird mittels einem *field programmable gate array* (FPGA) (NI-R7813, National Instruments) gesteuert, deren Programmierung mittels *LabView* (Version 2011, National Instruments) erfolgt. Zur Interaktion stehen ebenfalls zwei *LabView*-Programme zur Verfügung.

Programm „fpga3.vi“ zur Steuerung des Versuchsaufbaus und Durchführung der Übertragung

Die Programmierung des FPGA erfolgt über *LabView*, wofür das im Hintergrund laufende Programm „fpga3.vi“ zum Einsatz kommt.
Die Übertragung eines Bits nimmt dabei 100 Takte des FPGA in Anspruch. Bei einer Taktrate von 40 MHz können also maximal (bei voller Effizienz der Photonenerzeugung und -detektion, sowie ohne Verluste innerhalb der Übertragungsstrecke) 400 kBit pro Sekunde übertragen werden. Die Dauer eines Taktes liegt entsprechend bei 25 ns.

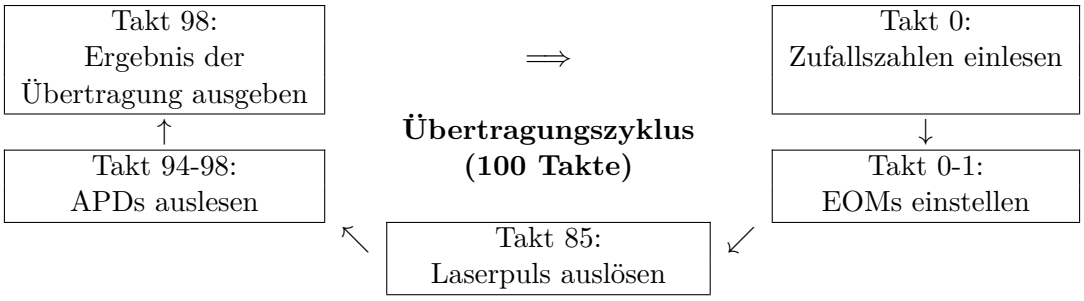


Abbildung 8 – Ablauf eines FPGA-Zyklus von 100 Takten.
In jeder Übertragung werden zuerst in Takt 0 Zufallszahlen, die von dem steuernden Programm „GUI.vi“ bereitgestellt werden, in das FPGA eingelesen und anhand dieser Werte die EOM-Spannungen eingestellt. In Takt 85 wird dann der Laserpuls ausgelöst und somit die optische Übertragung gestartet. Die erzeugten Photonen passieren beide EOMs, wobei sie entsprechend der gewählten EOM-Spannungen polarisiert werden. Von Takt 94 bis 98 werden die an den APDs ankommenden Photonen registriert und zuletzt in Takt 98 an das steuernde Programm ausgegeben, von dem sie gespeichert werden.

Innerhalb eines Übertragungszyklus von 100 Takten werden zu Beginn (Takt 0, vgl. auch Abb. 8) 4 Bit an Zufallsdaten aus dem Programm „GUI.vi“ eingelesen und die entsprechenden Spannungen für beide EOMs (als binärer Wert zwischen 0 und 1024) aus einer Liste ausgewählt, die im Vorfeld ebenfalls mit „GUI.vi“ erstellt werden muss. Diese Werte werden dann über einen Digital-Analog-Wandler in Spannungen umgewandelt und über einen Verstärker auf die EOMs gegeben. Da diese einige Zeit für die Umstellung brauchen, wartet das Programm etwa 2 µs bis Takt 85, bevor ein Signal an den Laser gesendet wird, das im gepulsten Betrieb den Puls auslöst.
9 Takte (also 225 ns) später werden 4 Takte (also 100 ns) lang die APD-Signale aufgezeichnet. Dabei wird binär für jede APD getrennt gespeichert, ob (mindestens) ein Photon detektiert wurde (Bit 1) oder nicht (Bit 0). Auch wird innerhalb des Zeitraums von Takt 85 bis 99 in jedem Takt gezählt, wie viele Photonen innerhalb von 10.000 Durchläufen (also 25 ms) an jeder APD registriert wurden. Diese Werte werden in „GUI.vi“ als Histogramm dargestellt. Abschließend wird in Takt 98 ein 6 Bit langer Wert an das Programm „GUI.vi“ übergeben und von diesem zur späteren Analyse gespeichert, der Folgendes beinhaltet:

Basis & Bit Alice (2 Bits) | Basis Bob (2 Bits) | Detektion APD 1 & 2 (2 Bits)

Programm „GUI.vi“ zur Einrichtung der EOMs und Steuerung der QKD-Übertragung

Das Programm „GUI.vi“ erlaubt den Wechsel zwischen Dauerstrichbetrieb und gepulstem Betrieb am Laser, die Steuerung der EOMs und zeigt die APD-Zählraten in Echtzeit an. Die Benutzeroberfläche ist in Abb. 9 dargestellt.
An den EOMs können über eine Skale in ganzzahligen Schritten von 0 bis 1024 Spannungen im Bereich von ±250 V angelegt werden. Die detektierten Photonen werden getrennt nach den APDs in zwei Histogrammen in der Form Zählrate pro Takt aufgetragen (in der Abb. gelb markiert).
Das Programm erlaubt darüber hinaus auch Scans über den gesamten möglichen Bereich von Spannungen der EOMs (Steuerung in der Abb. grün markiert). Die Dauer eines Scans ist dabei von der eingestellten Schrittweite abhängig und beträgt zum Beispiel bei einer Schrittweite von 30 etwa eine Minute, bei einer Schrittweite von 10 dagegen schon über zehn Minuten. Bei einem Scan werden für jede APD die Zählraten in Abhängigkeit von beiden EOM-Spannungen als Intensitätsverteilung dargestellt (in der Abb. rot markiert). Die EOM-Spannungen werden wiederum als ganzzahliger Wert zwischen 0 und 1024 ausgedrückt. Weiße Bereiche deuten dabei auf eine hohe, schwarze auf eine niedrige und blaue auf eine mittelhohe Zählrate hin.
Daneben wird im dritten Bild auch der Kontrast K der APD-Zählraten R_i:

$$K = \frac{|R_{\text{APD 1}} - R_{\text{APD 2}}|}{R_{\text{APD 1}} + R_{\text{APD 2}}} \tag{7}$$

dargestellt (in der Abb. ebenfalls rot markiert). In diesem Diagramm stehen weiße Bereiche für einen Kontrast $K \geq 90\%$ und schwarze für $K \leq 10\%$. Zur Basiswahl von Alice und Bob werden für die EOMs sowohl Spannungspaare mit möglichst hohem Kontrast (Paare gleicher Basen) als auch mit möglichst niedrigem Kontrast (Paare verschiedener Basen) benötigt, wozu diese Darstellung herangezogen werden kann (siehe dazu auch die Darstellung in Kap. 4.1).
Während der Übertragung stellt das Programm „GUI.vi“ die von dem FPGA benötigten Zufallszahlen bereit, die über einen Dateidialog ausgewählt werden. Echte Zufallszahlen können dabei über die Webseite der Arbeitsgruppe Nanooptik bezogen werden. Alternativ kann die Datei „sampledata-600MB.bin“ im Ausführungsverzeichnis des Programms verwendet werden. Ebenfalls speichert das Programm die durch die „fpga3.vi“ aufgenommenen Daten in einer Datei „key.bin“ zur späteren oder zeitgleichen Analyse durch „analyser_ qkd.exe“ im Ausführungsverzeichnis ab.

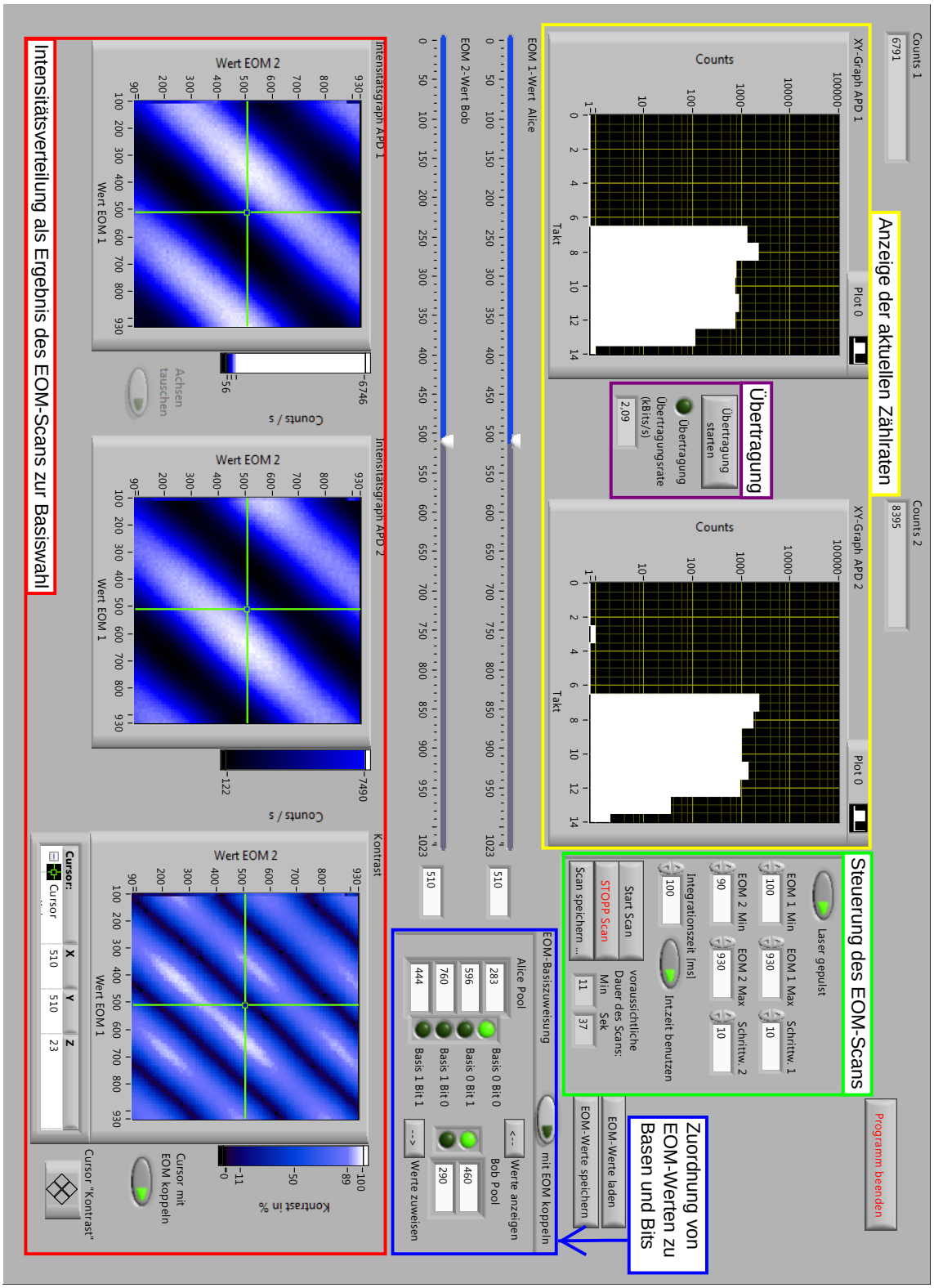


Abbildung 9 – Benutzeroberfläche des *LabView*-Programms „GUI.vi“.
Gelb markiert: Echtzeitanzeige der APD-Zählraten, darin (violett markiert) Steuerung der QKD-Übertragung.
Rot markiert: Darstellung der APD-Zählraten und des Kontrastes K in Abhängigkeit der EOM-Werte von EOM 1 und 2 als Ergebnis eines EOM-Scans (Steuerung dazu grün markiert). Zur manuellen Feineinstellung der EOM-Werte gibt es zwei Regler, die sich in der Mitte der Benutzeroberfläche befinden (nicht markiert). Die anschließende Zuweisung zu den Basen und Bits befindet sich ebenfalls hier (blau markiert).

Programm „ScanSoft_ SmarAct_ 2011.vi“ zur Steuerung des Piezo-Treibers

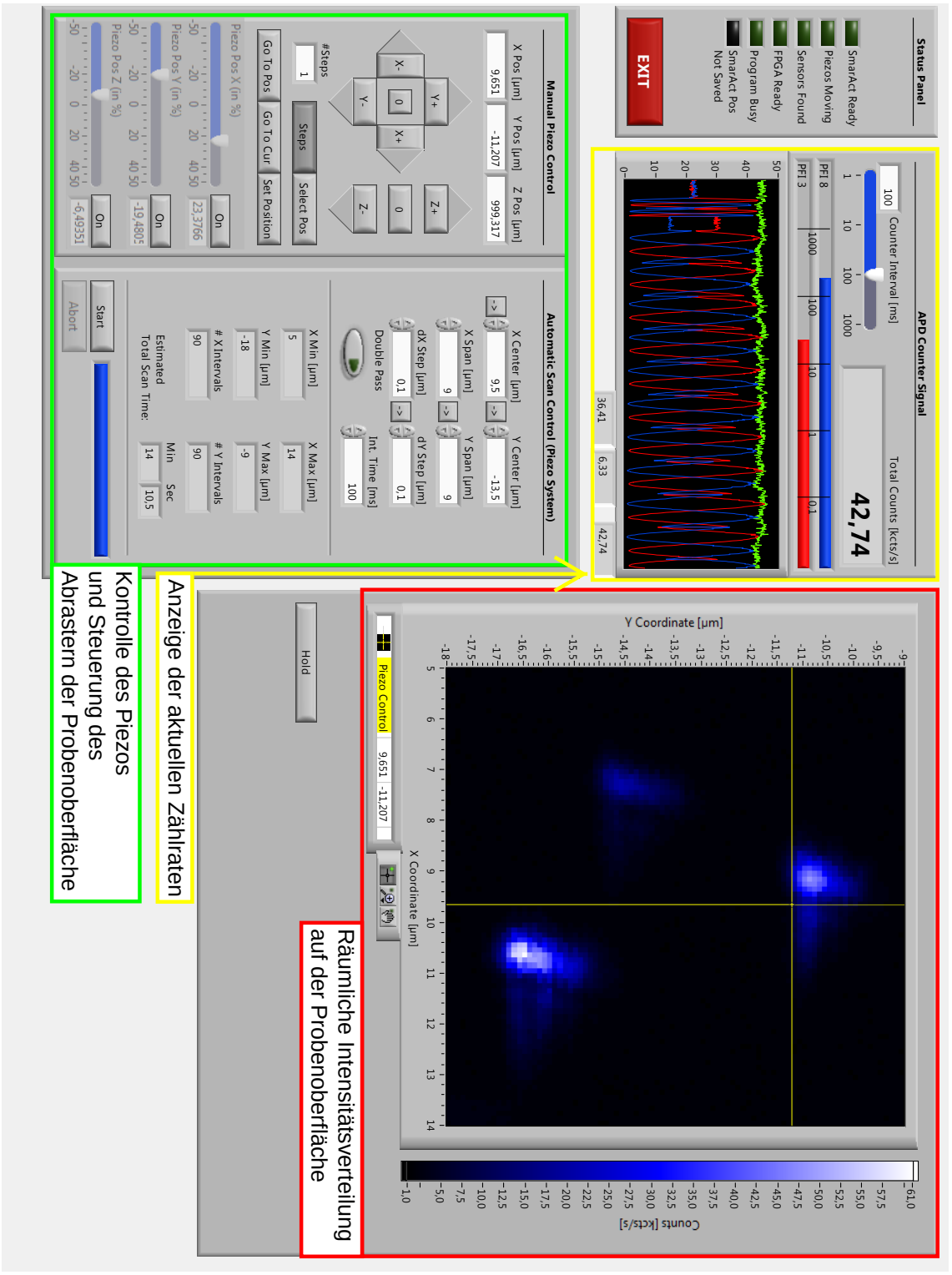


Abbildung 10 – Benutzeroberfläche des Programms „ScanSoft_ SmarAct_ 2011.vi“.
Gelb markiert: Echtzeitanzeige der APD-Zählraten.
Rot markiert: Darstellung der summierten Zählrate in Abhängigkeit von der räumlichen Position des Piezo-Tisches als Ergebnis eines Scans der Probenoberfläche.
Grün markiert: Positionierung des Piezo-Tisches und Steuerung des Scans.

Zur Steuerung des Piezo-Treibers steht das Programm „ScanSoft_ SmarAct_ 2011.vi“ zur Verfügung. Die Benutzeroberfläche ist in Abb. 10 dargestellt.
Das Programm stellt ebenfalls die Zählrate der APDs (in der Abb. gelb markiert) einzeln und unter der Bezeichnung „Total Counts“, im Folgenden kurz C_T, in Summe dar. Neben dieser auch für eine Darstellung des Verlaufs während eines EOM-Scans nützlichen Funktion wird das Programm zur Positionierung des Piezo-Tisches mit den Nanodiamanten in allen drei Raumrichtungen x, y und z verwendet und ermöglicht auch automatische Scans (in der Abb. grün markiert). Als Ergebnis eines solchen Scans wird eine Intensitätsverteilung angezeigt, die die gemessene summierte Zählrate in Abhängigkeit von der räumlichen Position anzeigt (in der Abb. rot markiert). Weiße Bereiche deuten dabei auf ein oder mehrere NV-Zentren hin. Nach einem Scan kann die Position des Piezo-Tisches dann so eingestellt werden, dass die Photonen eines der gefundenen NV-Zentren für weitere Messungen und Übertragungen verwendet werden können.

Programm „analyser_ qkd.exe“

Während der Übertragung der Bits wird auf dem zur Steuerung verwendeten Computer eine Datei angelegt, die pro übertragenem Bit folgendes (in der dargestellten Reihenfolge) enthält: Basis & Bit Alice (2 Bits) | Basis Bob (2 Bits)| Detektion APD 1 & 2 (2 Bits).
Die Auswertung dieser Daten erfolgt mittels des Programms „analyser_ qkd.exe“. Dieses bestimmt in Echtzeit, bei wie vielen Übertragungen (jeweils absolut und relativ)

1. an genau einer APD Photonen detektiert wurden,
2. die gleiche Basis von Alice und Bob gewählt wurde,
3. das korrekte Bit von Bob registriert wurde.

Letzteres wird dabei in Relation zu den in gleicher Basis übertragenen Bits angegeben und führt auf die Fehlerrate (*quantum bit error rate*, quantum bit error rate (QBER)) der Übertragung. Dabei wird der vollständige Schlüssel verglichen und steht somit nicht anschließend für eine geheime Kommunikation zur Verfügung. Da für den Versuch aber ein Nachweis der Funktionalität eines Schlüsselaustauschs nach BB84 im Vordergrund steht, stellt dieser Umstand kein Problem dar. Wie bei einer echten Übertragung, bei der nur etwa ein Drittel des Schlüssels verglichen wird [BB84], kann auch hierbei 11% als Obergrenze für einen noch akzeptablen QBER angenommen werden [SP00, S. 444].

TimeHarp

Für die Autokorrelationsmessung der SPS mittels des Hanbury Brown & Twiss Aufbaus kommt eine *TimeHarp*-Karte (TimeHarp200, PicoQuant) zum Einsatz, die über ein dazugehöriges Programm gesteuert wird.

Digital-Analog-Wandler

Für die EOMs werden analoge Signale im Bereich ±250 V benötigt. Dazu wird zuerst mittels eines Digital-Analog-Wandlers (*digital analog converter* , DAC) das digitale Signal zwischen 0 und 1024 in eine Spannung im Bereich ±5 V umgewandelt. Anschließend wird dieses Signal über je einen Treiber pro EOM auf ±250 V verstärkt. An dem DAC befinden sich darüber hinaus ein Anschluss zum Auslösen des Lasers im gepulsten Betrieb sowie die Eingänge für die APD-Signale.

SmarAct-Piezo-Treiber

Der Piezo-Tisch zur Positionierung der Nanodiamanten wird über einen Piezo-Treiber (MCS-3D, SmarAct) gesteuert, der über einen USB-Anschluss mit dem Computer verbunden werden oder manuell bedient werden kann.

5 Durchführung der Messungen

5.1 Durchführung der Messungen unter Verwendung des Lasers

Inbetriebnahme der Geräte und Ausrichtung des Strahlenganges

Es empfiehlt sich, eine Weile vor Beginn der Messungen (0,5 bis 1 h) den Laser im Dauerstrichbetrieb einzuschalten, da in der ersten Zeit Schwankungen in der Intensität auftreten, welche die Messungen sonst verfälschen könnten. Dazu muss neben der Spannungsversorgung auch am Auslöser-Eingang (dem sog. *Trigger*) des Lasers ein Signal anliegen, dass in diesem Fall über den DAC bereitgestellt wird. Somit muss auch die Spannungsversorgung des DAC eingeschaltet und das *LabView*-Programm „GUI.vi“ gestartet werden.

Bevor mit dem eigentlichen Einrichten des Aufbaus für die Übertragung begonnen werden kann, müssen die Spiegel nachjustiert werden, um sicherzustellen, dass die EOMs gerade durchquert und die APDs mittig getroffen werden. Um die Justage zu erleichern, wurden vier Irisblenden fest montiert, auf die nacheinander eingestellt wird. Dabei empfiehlt es sich, die Abschwächer zu entfernen, da dann der Laserpunkt auf einem Schirm (z.B. einem Stück Papier) mit bloßem Auge gut wahrnehmbar ist. **Unbedingt sind jedoch die Abschwächer vor Einschalten der APDs wieder einzusetzen, um eine Beschädigung zu vermeiden.**

Jetzt kann der Deckel zur Abdunklung aufgelegt und die EOM-Verstärker und APD-Spannungsversorgung angeschaltet werden. Eine Sicherheitsschaltung direkt am Kasten verhindert dabei den Betrieb der APDs bei geöffnetem Deckel. Als Resultat sollte eine Zählrate in den beiden Histogrammen von „GUI.vi“ registriert werden und auch in „ScanSoft_ SmarAct_ 2011.vi“ sollten die Zählraten der einzelnen APDs angezeigt werden (s. Kap. 4.2). **Generell darf die Zählrate jeder APD den Wert 1000 kcts/s nicht überschreiten, um die APDs nicht zu überlasten.**

Überprüfung von Strahlengang und linearem Polarisator

Um sicherzustellen, dass die APDs korrekt getroffen werden und der lineare Polarisator optimal eingestellt ist, sollte zuerst ein grober Scan der EOMs (als Schrittweite in „GUI.vi“ sollte je 30 gewählt werden) erfolgen und der Verlauf des gesamten Scans im ScanSoft-Programm betrachtet werden.

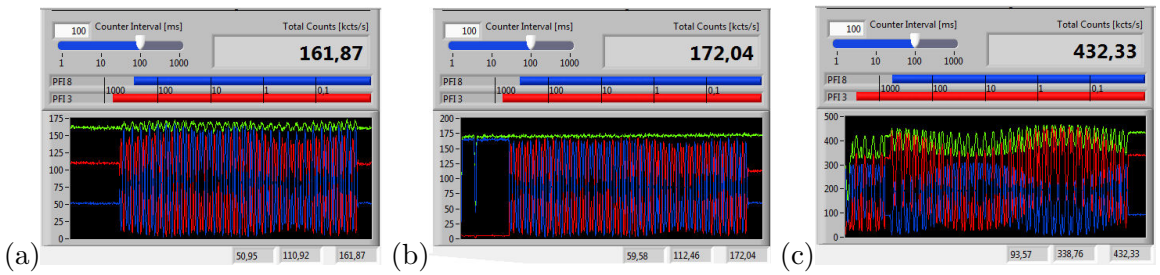


Abbildung 11 – APD-Signal vor und nach der Justage des Strahlenganges.
a) Der grobe Scan über den EOMs zeigt, dass die Maxima von APD 1 (blau) durchgehend über denen von APD 2 (rot) liegen. Dies deutet darauf hin, dass APD 2 noch nicht mittig getroffen wird.
b) Nach der Justage des Strahlenganges liegen beide Signale annähernd gleich auf. Ihre Summe ist im Rahmen der zu erwartenden Schwankungen konstant.
c) Die Schwankungen innerhalb der Maxima und Minima einer APD sind extrem stark. Der lineare Polarisator sollte auf jeden Fall nachjustiert werden.

Liegen dabei die Maxima von APD 2 deutlich unter denen von APD 1 (vgl. Abb. 11a), ist der Strahlengang noch nicht optimal und muss nachjustiert werden (vgl. Abb. 11b). Liegen die einzelnen Minima und Maxima einer APD während des Scans nicht auf (etwa) gleicher Höhe, muss erst am linearen Polarisator, dann am $\frac{\lambda}{2}$-Plättchen nachjustiert werden. Das Ergebnis sollte mit einem weiteren Scan überprüft werden (vgl. Abb. 11c). Bei nur geringfügig höheren Maxima auf APD 2 muss der Strahlengang nicht nachgestellt werden.

Wahl der EOM-Spannungen für die Basen von Alice und Bob

Nach diesem groben EOM-Scan sollte ein feiner (Schrittweite für beide EOM je 10) erfolgen, um die Basiswahl für Alice und Bob zu ermöglichen. Dieser Scan dauert mit 12 min deutlich länger als der grobe (etwa 1 min), sollte also erst dann durchgeführt werden, wenn Strahlengang und linearer Polarisator mit Sicherheit gut eingestellt sind, um ein Wiederholen zu vermeiden.
Anschließend kann die Basiszuweisung erfolgen. Dabei sollten generell zuerst die Paare von EOM-Spannungen gewählt werden, in denen Alice und Bob die gleiche Basis verwenden und anschließend für verschiedene Basen bei Alice und Bob so nachjustiert werden, dass Bit 0 und 1 für Bob nicht zu unterscheiden sind. Auch ist zu beachten, dass Bob per Definition Bit 0 an APD 1 und Bit 1 an APD 2 misst. Diese Zuordnung sollte auch bei der Wahl der EOM-Spannungen beachtet werden, um Probleme in der Auswertung zu vermeiden.
Konkret kann zur Basiswahl folgendermaßen vorgegangen werden (s. auch Abb. 12):

1. Zwei Spannungspaare suchen, für die der Kontrast K (s. Kap. 4.2) von APD 1 und APD 2 maximal ist und den Basen mit entsprechendem Bit (0, wenn $R_{\text{APD 1}} > R_{\text{APD 2}}$, sonst 1) zuweisen (Punkte A01B0 und A11B1 in Abb. 12).

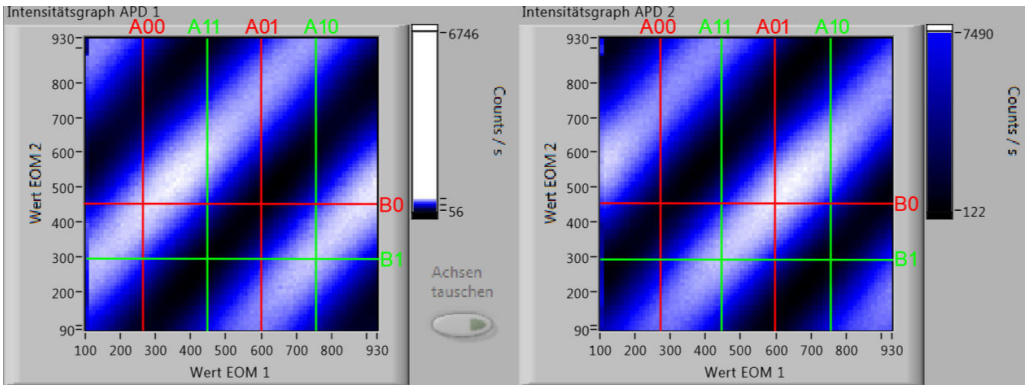
2. Eines der eben gewählten Bits von Alice in der falschen Basis bei Bob anzeigen (z.B. A01 und B1 auswählen) und so lange schrittweise diagonal wandern, bis die Signale von APD 1 und APD 2 etwa gleich sind (Punkt A01B1 in Abb. 12), dann diesen Wert für Alice und Bob übernehmen. Für das andere Bit (Punkt A11B0 in Abb. 12) analog.

3. Jetzt bei beiden Spannungen von Bob das jeweils andere Bit von Alice zuweisen. Dazu eine Stelle wählen, an der die jeweils andere APD als bei dem ersten Bit von Alice ein Maximum zeigt.

4. Diese Bits ebenfalls in der anderen Basis von Bob anzeigen lassen und so lange den Wert für Alice nachjustieren, bis beide APDs das gleiche Signal anzeigen.

Zur Kontrolle können zuerst für Basis 0 bei Alice und Bob beide Bits angezeigt werden (also A00B0 und A01B0), dann für Basis 1 (A10B1 und A11B1) und schließlich für Basis 1 bei Alice und 0 bei Bob (A10B0 und A11B0) und umgekehrt (A00B1 und A01B1). Die dabei erreichten Zählraten von APD 1 und APD 2 sollten für eine bessere Vergleichbarkeit tabellarisch notiert werden.
Die während des Scans erhobene Intensitätsverteilung wird für beide APDs automatisch in der Datei „Scan_ APD1.dat“ (bzw. „...APD2.dat“) gespeichert, die eingestellten EOM-Werte müssen dagegen manuell über das Programm „GUI.vi“ auf dem Computer gespeichert werden.

(a)



(b)

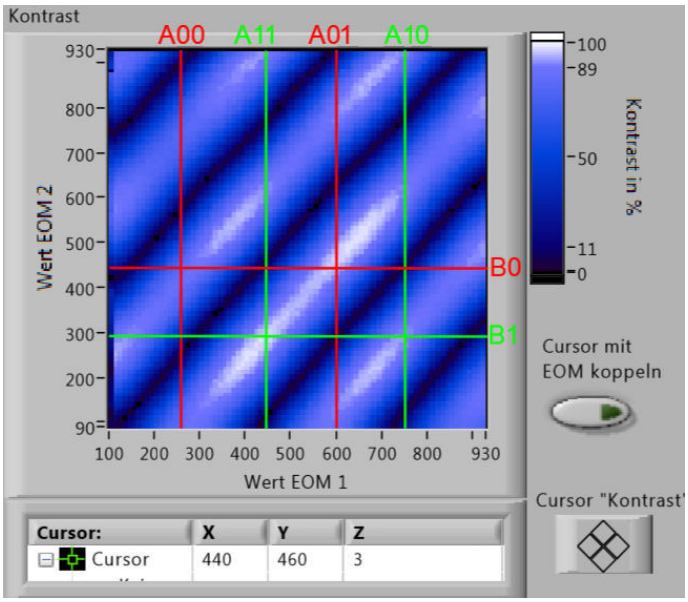


Abbildung 12 – EOM-Scan zur Basiswahl mit dem Laser.
Zu sehen ist das Ergebnis eines EOM-Scans. Dabei sind die Intensitätsgraphen der APDs (in der Abb. a) getrennt von dem sich daraus ergebenem Kontrast K (in der Abb. b) dargestellt. Darüber hinaus sind die Alice und Bob zugeordneten EOM-Werte in rot (Basis 0) und grün (Basis 1) eingezeichnet und entsprechend beschriftet („A“ für Alice, „B“ für Bob gefolgt von den Werten für Basis und (bei Alice) Bit.
An den Kreuzungspunkten, welche die gleiche Basis für Alice und Bob repräsentieren (A00B0, A01B0, A10B1 und A11B1), ist eines der beiden APD-Signale nahe seiner maximalen Zählrate (weiß in der Farbskala von a), während das andere nahe seiner minimalen Zählrate (schwarz in der Farbskala von a) befindet.
Die Kreuzungspunkte, die verschiedene Basen von Alice und Bob repräsentieren(A00B1, A01B1, A10B0 und A11B0), weisen dagegen etwa gleiche Zählraten für beide APD-Signale auf (blau in der Farbskala von a, schwarz in der Farbskala von b).

Übertragung im Dauerstrich- und im gepulsten Modus

Mit den so über die EOM-Werte eingestellten EOM-Spannungen kann nun ein Schlüssel übertragen werden, wobei der Laser zuerst wie bei den vorherigen Schritten im Dauerstrichbetrieb betrieben werden kann und anschließend im gepulsten Modus. Damit können beide Betriebmodi miteinander verglichen werden. Ebenfalls kann die Anzahl der Abschwächer variiert werden, um ihren Einfluss auf die Übertragung zu untersuchen. Als Parameter der Schlüsselübertragung können dabei die Übertragungsrate R und die Fehlerrate QBER bestimmt werden, letztere über das Programm „analyser_ qkd.exe“.

5.2 Durchführung der Messungen unter Verwendung der SPS

Inbetriebnahme der Einzelphotonenquelle und Ausrichtung des Strahlenganges

Es empfiehlt sich, vor einer Übertragung mit der Einzelphotonenquelle (SPS) zuerst alle Geräte mittels des roten Lasers zu kalibrieren, wie es im vorherigen Abschnitt beschrieben wurde, da sich Ausrichtung des Strahlenganges, die Überprüfung des linearen Polarisators und der Scan der EOM-Spannungen mit der höheren Leistung des Lasers einfacher gestaltet.
Nachdem dies geschehen ist, kann die SPS in den durch den roten Laser vorgegebenen Strahlengang eingekoppelt werden. Dafür müssen bei geöffnetem Deckel (also ausgeschalteten APDs) zuerst alle Abschwächer aus dem Strahlengang entfernt und der dafür bereitstehende variable Spiegel auf einen magnetischen Halter zwischen Laser und erster Irisblende gestellt werden. Anschließend sind die Abdeckung der Einzelphotonenquelle zu öffnen und die Langpassfilter zu entfernen. Nun kann der grüne Anregungslaser eingeschaltet und der Piezo-Treiber gestartet werden. Jetzt muss die z-Komponente des Piezo-Tisches vorsichtig auf etwa 1.000.000 nm gestellt werden (am besten zuerst mit einer Schrittweite von 9 bis etwa 900.000 nm gehen, dann die Schrittweite nach und nach verringern). **Den Piezo-Tisch am Ende nur noch sehr vorsichtig bewegen und auf keinen Fall in Berührung mit dem Objektiv bringen.**
Nachjustieren, bis ein kollimierter grüner Lichtpunkt auf einem in Höhe der ersten Irisblende in den Strahlengang gehaltenen Schirm zu sehen ist. Dieser Lichtpunkt kommt durch Reflexion des grünen Lasers auf der Oberfläche der SIL zustande und kann zur Justierung der Spiegel verwendet werden, da die Langpassfilter entfernt wurden.
Für diese Justierung kommt als Methode der sogenannte *beam walk* zum Einsatz, und zwar folgendermaßen:

1. Mit dem letzten Spiegel der Einzelphotonenquelle den Strahl auf die erste Irisblende richten;

2. dann die Irisblende weit öffnen und mittels des Spiegels auf dem Magnethalter die zweite Irisblende anpeilen, anschließend die erste Irisblende wieder weitgehend schließen;

3. mit dem ersten Spiegel bezüglich der ersten Irisblende nachjustieren, da sich die Position durch den vorherigen Schritt verschoben hat;

4. mit dem zweiten Spiegel bezüglich der zweiten Irisblende nachjustieren, da sich die Position durch den vorherigen Schritt verschoben hat.

Die Schritte 3 und 4 müssen dabei solange im Wechsel wiederholt werden, bis der Strahlengang beide Irisblenden mittig durchquert.
Falls möglich (je nach Sichtbarkeit des grünen Laserpunktes) kann anschließend auch noch die dritte Irisblende (vor dem zweiten EOM) angepeilt werden. Wenn der Strahlengang zuvor mit dem Laser gut ausgerichtet wurde, genügt dies um die APDs mittig zu treffen.
Abschließend werden erst die Langpassfilter wieder ein- und die Abdeckung der SPS wieder aufgesetzt. **Währenddessen den grünen Laser ausschalten, um Augenschäden zu vermeiden.** Nach dem Schließen des Kistendeckels können die APDs eingeschaltet werden. **Die APDs dürfen nur eingeschaltet werden, wenn alle Filter der SPS im Strahlengang stehen, da der grüne Laser zu einer Überlastung führen könnte.** Die Verwendung der Abschwächer ist hierbei dagegen nicht nötig, da die Zählraten der NV-Zentren in einem für die APDs unschädlichen Bereich liegen.
Obwohl die APDs eingeschaltet wurden, zeigen sie in den meisten Fällen höchstens ein schwaches Signal (je etwa 1 kcts/s), da die Position des Piezo-Tisches noch nachjustiert

werden muss. Es empfiehlt sich deshalb, einen groben Scan der Probe in der xy-Ebene durchzuführen. Als Mittelpunkt (im Programm „Center“) sollte dabei $(0\,\mu m, 0\,\mu m)$ gewählt werden, als Verfahrbereich (im Programm „Span“) je 5 µm und als Schrittweite (im Programm „Step“) je 1 µm. Dann muss der hellste Punkt (mit maximalem APD-Signal) angesteuert und dort das APD-Signal durch Justieren der z-Koordinate weiter optimiert werden.
Anschließend sollten die korrekte Einstellung von Strahlengang und linearem Polarisator sichergestellt werden, wozu wie bei der Übertragung mit dem Laser (s. vorherigen Abschnitt) vorgegangen werden kann.
Wurden diese Voreinstellungen getroffen, kann über Scans der Probe, die ein größeres Gebiet abdecken, sowie über Scans mit feinerer Schrittweite nach NV-Zentren gesucht werden. Die folgenden beiden Schritte können dann für verschiedene NV-Zentren vergleichend durchlaufen werden:

Wahl der EOM-Spannungen und Übertragung

Für eine Übertragung müssen nun noch die EOM-Spannungen richtig eingestellt werden. Diese stimmen allerdings meist mit den zuvor unter dem Laser gebrauchten weitgehend überein. Deshalb sollte hier nur ein kurzes Nachjustieren nötig sein. Dafür können für beide Basen von Alice beide Bits in der jeweils anderen Basis bei Bob angezeigt werden. Dann wird der Wert für EOM 1 so lange verändert, bis das Signal beider APD gleich ist. Dabei sollten für jede Wahl von Alice die Zählraten beider Basen von Bob tabellarisch notiert werden.
Mit den so nachjustierten Spannungen kann nun ein Schlüssel übertragen werden, wobei wieder Übertragungsrate R und Fehlerrate QBER bestimmt und notiert werden sollten.

Überprüfung der Autokorrelation

Zur Überprüfung der Autokorrelation werden die APDs von dem Digital-Analog-Wandler getrennt und direkt an die *TimeHarp*-Karte angeschlossen. Vor einer Messung müssen dabei die Einstellungen „Level“ für den „Sync“-Kanal und „ZeroCr.“ sowie „Discr.“ für den „CFD“-Kanal im „TimeHarp Control Panel“ angepasst werden. Die angezeigte Zählrate sollte in etwa der von ScanSoft entsprechen. Ggf. müssen auch die EOM-Spannungen nachjustiert werden, bis beide Kanäle im *TimeHarp*-Programm etwa gleich viele Counts zeigen.
Um den gemessenen Verlauf der Autokorrelation $g^{(2)}(\tau)$ über eine Fitfunktion anzunähern, kann Gleichung (3) aus Kap. 3.2 in leicht abgewandelter Form verwendet werden:

$$f(x) = C_1 \cdot g^{(2)}\left(|x - x_0|\right) + C_0 = C_1 \cdot \left(1 - (K+1)\, e^{k_+|x-x_0|} + K e^{k_-|x-x_0|}\right) + C_0 \qquad (8)$$

Die Konstante C_0 gibt dabei den unkorrelierten Untergrund an, da in der Messung die Koinzidenzen im Nullpunkt x_0 nicht auf Null abfallen. Da dieser Nullpunkt bei der Messung verschoben wurde, ist es nötig, als Argument der $g^{(2)}$-Funktion den Abstand $|x - x_0|$ zu diesem Punkt zu verwenden. Die Konstante C_1 trägt der Tatsache Rechnung, dass die Messergebnisse unnormiert sind.
Die Summe $C_1 + C_0 = C_1'$ kann bei der Anpassung vorgegeben werden und dafür über die Zählraten R_i an APD i, der zeitlichen Auflösung t_{bin} und der Messdauer t_{int} mittels folgender Formel berechnet:

$$C_1' = R_1 \cdot R_2 \cdot t_{bin} \cdot t_{int} \qquad (9)$$

Der Wert $g^{(2)}(0)$ kann dann mit Hilfe der aus der Anpassung ermittelten Parameter C_0 und C_1 wie folgt berechnet werden:

$$g^{(2)}(0) = \frac{C_0}{C_1 + C_0} \qquad (10)$$

Literatur

[ACS+11] I. Aharonovich, S. Castelletto, D. A. Simpson, C.-H. Su, A. D. Greentree, and S. Prawer. Diamond-based single-photon emitters. *Reports on Progress in Physics*, 74(7):1–28, 2011.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 1984.

[JW06] F. Jelezko and J. Wrachtrup. Single defect centres in diamond: A review. *physica status solidi (a)*, 203(13):3207–3225, 2006.

[NC05] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge Univ. Press, Cambridge, 8. print edition, 2005.

[Sch12] T. Schröder. *Integrated photonic systems for single photon generation and quantum applications: Assembly of fluorescent diamond nanocrystals by novel nanomanipulation techniques*. Dissertation, Humboldt-Universität zu Berlin, 2012.

[Sha49] C. E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[Sho97] W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[Sin01] S. Singh. *Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*. Hanser, München, 2001.

[SP00] W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical review letters*, 85(2):441–444, 2000.

[Ver26] G. S. Vernam. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the A.I.E.E.*, 45(2):109–115, 1926.

[WM08] D. F. Walls and G. J. Milburn, editors. *Quantum Optics*. Springer-Verlag, Berlin, Heidelberg, 2008.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

Abbildungsverzeichnis

Abkürzungen

APD avalanche photodiode (Lawinenphotodiode)

ASCII American Standard Code for Information Interchange

BB84 BB84-Protokoll zum Quantenschlüsselaustausch

DAC digital analog converter (Digital-Analog-Wandler)

EOM Elektrooptischer Modulator

FPGA field programmable gate array

HBT Hanbury Brown & Twiss Aufbau

HV-Basis rektilineare Basis mit Basiszuständen $|\updownarrow\rangle$ und $|\leftrightarrow\rangle$

NV nitrogen-vacancy center (Stickstoff-Fehlstellen-Zentrum)

OTP One Time Pad

PBS polarising beam splitter (Polarisations-Strahlteilerwürfel)

Qubit Quantenbit

QBER quantum bit error rate

QKD Quantum Key Distribution (Quantenschlüsselaustausch)

RL-Basis zirkulare Basis mit Basiszuständen $|\circlearrowleft\rangle$ und $|\circlearrowright\rangle$

SIL solid immersion lens (Öl-Immersionslinse)

SPS single photon source (Einzelphotonenquelle)

A Anlage zur Lasersicherheit

Die folgenden Punkte zum Schutz der Augen vor Laserstrahlung sollten während der gesamten Versuchsdurchführung berücksichtigt werden. Im Versuch werden Laser der Klasse 2 mit einer Lichtleistung von bis zu 1 mW verwendet.

- Halten Sie Ihren Kopf niemals auf Strahlhöhe!
- Nehmen Sie reflektierende Gegenstände (z.B. Uhren, Schmuck, ...) vor Versuchsbeginn ab!
- Blockieren Sie den Laserstrahl vor dem Austausch von optischen Elementen!
- Hantieren Sie niemals mit reflektierenden Werkzeugen im Strahlengang!
- Kontrollieren Sie den Strahlengang, bevor Sie den Laser freigeben bzw. einschalten!
- Beachten Sie, dass der Polarisations-Strahlteilerwürfel zwei Ausgänge besitzt!
- Die Einzelphotonendetektoren sind vor Raumlicht zu schützen und dürfen nur mit stark abgeschwächtem Laserlicht verwendet werden!
- Schalten Sie bei Laserbetrieb die Laserschutzlampe ein!
- Achten Sie auf andere Personen!

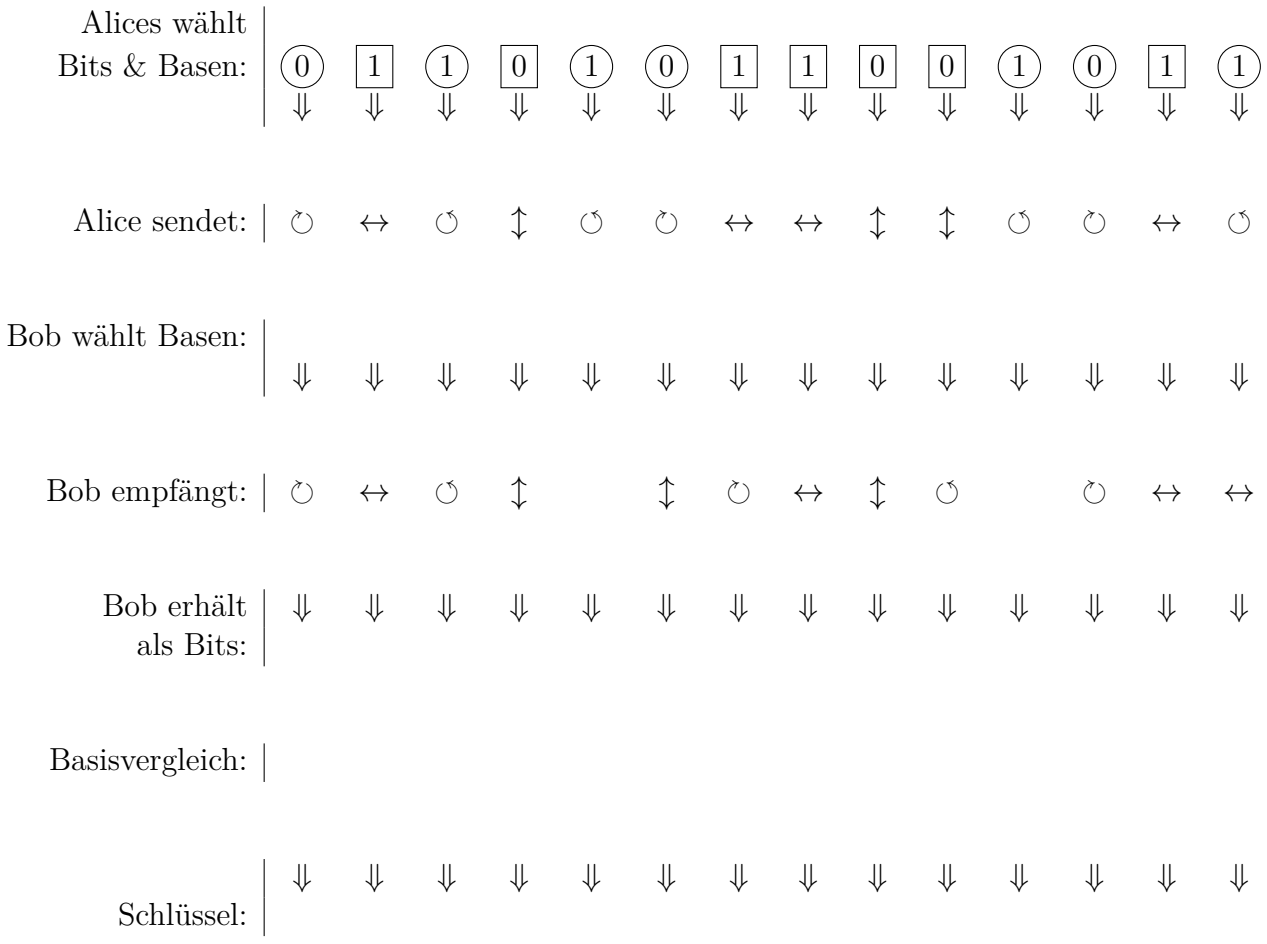
Ich erkläre hiermit, dass ich die zuvor aufgeführten Punkte zur Lasersicherheit gelesen und verstanden habe. Weiterhin bestätige ich, dass ich eine Einführung über den Umgang mit Lasern und eine Unterweisung zum Laborarbeitsplatz erhalten habe.

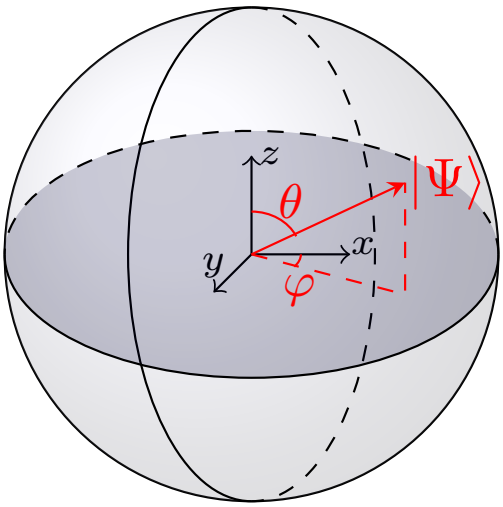
Name des Versuchsbetreuenden	Name des Versuchsdurchführenden
Ort, Datum	Unterschrift des Versuchsdurchführenden

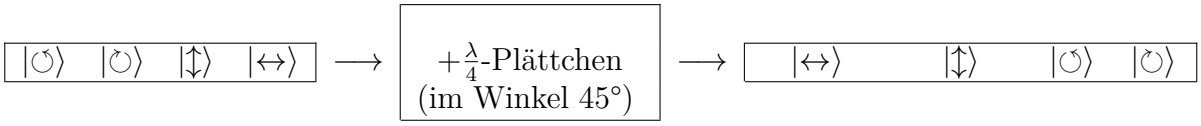
Anhang B

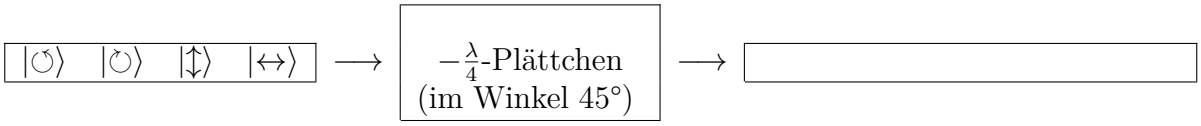
Materialien zum Versuch

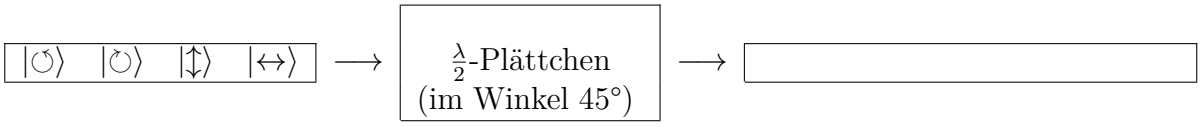
Im Anschluss befindet sich eine Kopiervorlage für den Versuchsbetreuenden, welche die in Kapitel 4.1.3 genannten Materialien enthält.

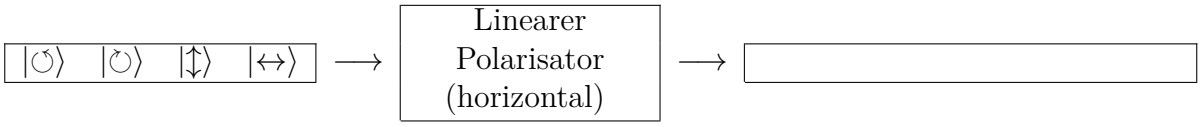


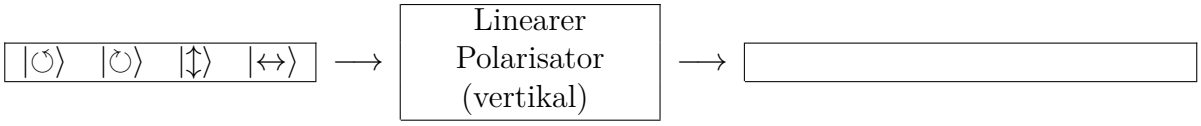

z
θ
|Ψ⟩
x
y
φ


|↺⟩ |↻⟩ |↕⟩ |↔⟩
+λ/4-Plättchen
(im Winkel 45°)
|↔⟩ |↕⟩ |↺⟩ |↻⟩


|↺⟩ |↻⟩ |↕⟩ |↔⟩
−λ/4-Plättchen
(im Winkel 45°)


|↺⟩ |↻⟩ |↕⟩ |↔⟩
λ/2-Plättchen
(im Winkel 45°)


|↺⟩ |↻⟩ |↕⟩ |↔⟩
Linearer
Polarisator
(horizontal)


|↺⟩ |↻⟩ |↕⟩ |↔⟩
Linearer
Polarisator
(vertikal)


|↺⟩ |↻⟩ |↕⟩ |↔⟩
PBS
+ + + +