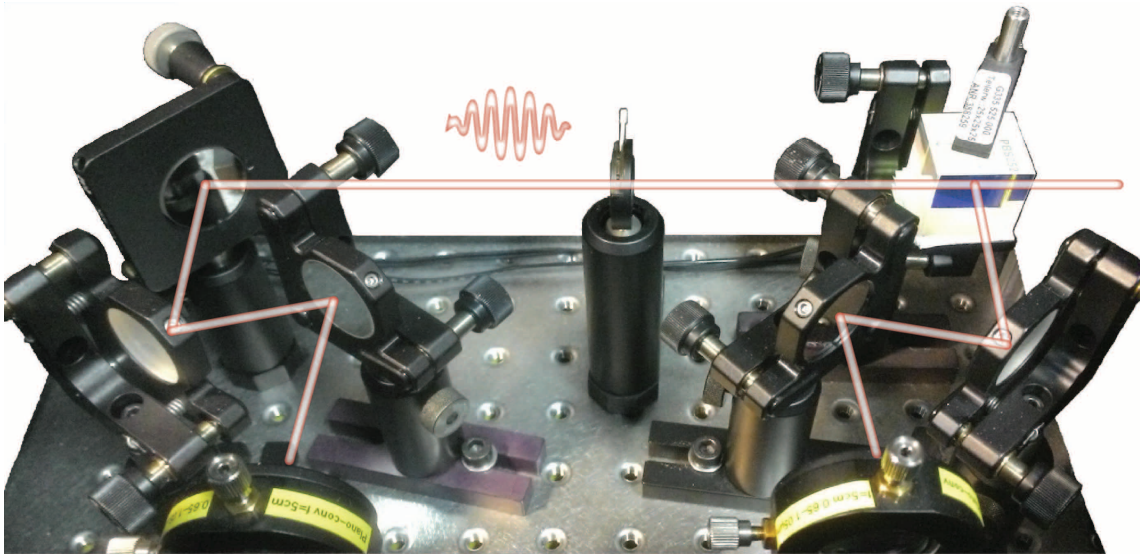
Humboldt Universität zu Berlin
Mathematisch-Naturwissenschaftliche Fakultät
Institut für Physik

Anleitung zum Versuch

Quantenkryptographie mit einzelnen Photonen – QKD via BB84

Fortgeschrittenen-Praktikum

Stand: Dezember 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 von Forschenden in einem außeruniversitären Institut oder einer Firma, die ein Gerät zur QKD nach BB84 entwickeln. Beurteilen Sie aus dieser Sicht die Eignung der im vorliegenden Aufbau verwendeten Geräte für eine sichere Kommunikation.
Zum Vortestat sollen Sie einer vorgesetzten Person erklären, wie mit Hilfe der Quantenphysik Information sicher übertragen werden kann, welche Bedingungen dazu erfüllt sein müssen, und was Sie messen wollen, um dies am vorliegenden Aufbau zu überprüfen.

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). Welche Eigenschaften der im Aufbau verwendeten Geräte haben einen Einfluss auf die Sicherheit der Übertragung?

Für Ihre Recherche können Sie neben den unter Literatur genannten möglichen Quellen natürlich auch eigene verwenden.

3. Die Hauptaufgabe in der Vorbereitung besteht darin, auf Grundlage von Aufgabe 1 und 2 festzulegen, welche Messungen Sie zur Beurteilung der Geräte durchführen sollten. Sie entscheiden selbstständig, was und in welchem Umfang Sie messen wollen. Dabei können Sie sich an den in Kap. 5 beschriebenen Schritten orientieren. Details dazu, wie die einzelnen Messungen genau durchgeführt werden, können Sie mit dem Versuchsbetreuenden im Vortestat festlegen. Fertigen Sie eine Liste mit den nötigen Messungen an, um die Sicherheit der Schlüsselübertragung beurteilen zu können, und bringen Sie diese zum Vortestat mit.

Durchführung

4. Bereiten Sie den Aufbau für die Übertragung eines Schlüssels mittels Laser 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 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.
    - Mit welcher Lichtquelle ist die Schlüsselübertragung sicher?
    - Gehen Sie auf Grenzen und mögliche Alternativen ein.

3 Theoretische Beschreibung

3.1 *One Time Pad* zur klassischen Verschlüsselung

Das *One-Time-Pad*-Verfahren kann eingesetzt werden, um mit einem übertragenen Block aus Schlüsseln (dem sogenannten *Pad*) die Chiffrierung der eigentlichen Nachricht durchzuführen. Die Quantenkryptographie bietet dann eine Möglichkeit, einen OTP-Schlüssel sicher zwischen zwei Parteien auszutauschen. Da für die hier verwendete QKD-Anwendung 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.

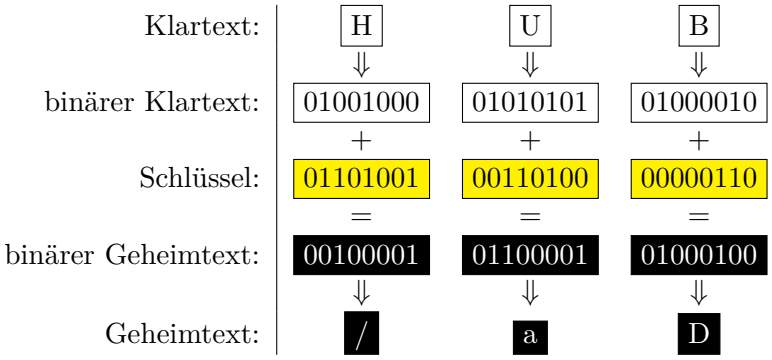


Abbildung 1 – Beispiel einer Chiffrierung in binärer Form nach dem OTP-Verfahren.
Der Klartext H U B wird über eine ASCII-Tabelle in eine binäre Form gebracht und mit dem vorher übermittelten Schlüssel binär addiert. Der so entstandene Geheimtext kann binär oder als Zeichenfolge / a D dargestellt werden.

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].

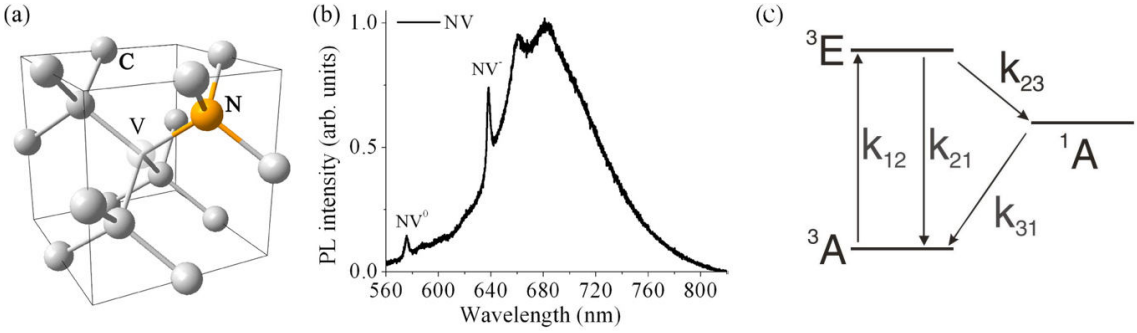


Abbildung 2 – Kristallographisches Modell, Spektrum und Drei-Niveau-Schema zur Beschreibung eines NV-Zentrums aus [ACS+11, JW06, S. 5 bzw. S. 3211].
a) Ein Stickstoffatom (mit N bezeichnet) ersetzt ein Kohlenstoffatom im Kristallgitter des Diamants, benachbart dazu tritt eine Lücke (mit V bezeichnet) 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 $K = \frac{k_- + k_{31} - k_{12} \cdot \frac{k_{23}}{k_{31}}}{k_+ - k_-}$.

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.

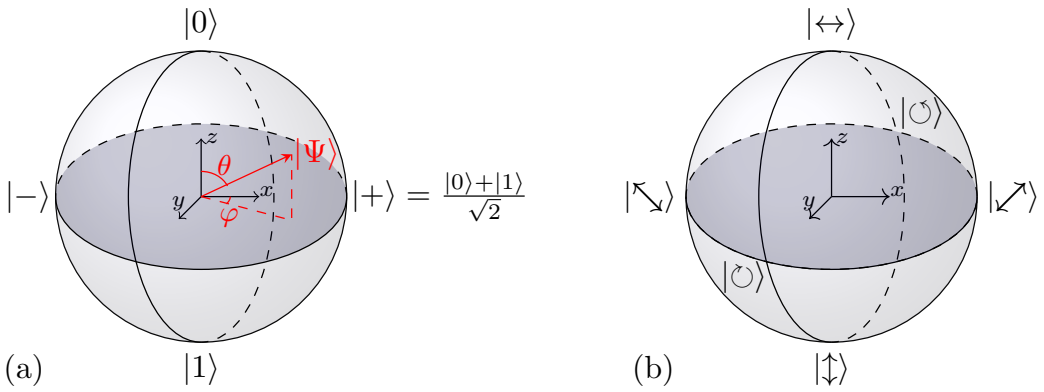


Abbildung 3 – Bloch- und Poincaré-Kugel.
a) Bloch-Kugel zur Veranschaulichung des Vektorraumes, in dem das Qubit im Zustand $|\Psi\rangle$ sich in einer Überlagerung der Basiszustände $|0\rangle$ und $|1\rangle$ befindet. Zustände, die auf gegenüberliegenden Seiten der Kugel liegen, sind orthogonal zueinander. 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.

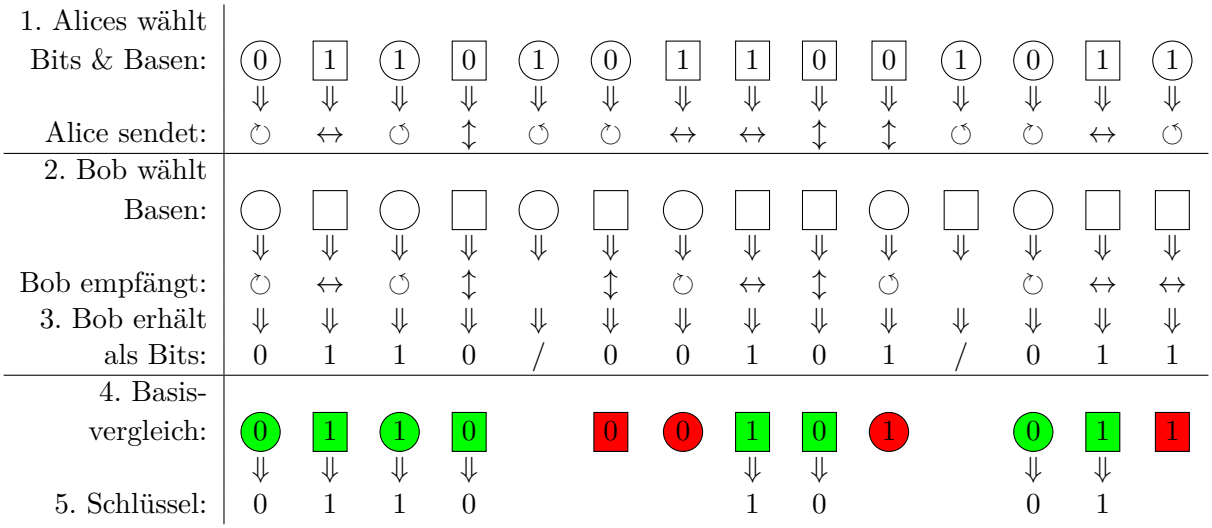


Abbildung 4 – Ablauf des BB84-Protokolls in 5 Schritten innerhalb von drei Phasen: Der Sender (Alice) übermittelt dem Empfänger (Bob) über einen Quantenkanal eine zufällige Folge von Bits in zufällig gewählten Basen (□ steht dabei für die rektilineare Basis, ◯ für die zirkulare) und sendet Bob eine Kette 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 (Eve nach englisch *eavesdropping*) 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.
Entstehen bei der Übertragung weniger als 12 % Fehler (*Quantum Bit Error Rate* QBER $<$ 12 %), kann der Schlüssel durch anschließende Prozesse (wie *error correction* und *privacy amplification*) soweit verbessert werden, dass sichere Übertragung dennoch möglich ist [SP00]. Dann 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).

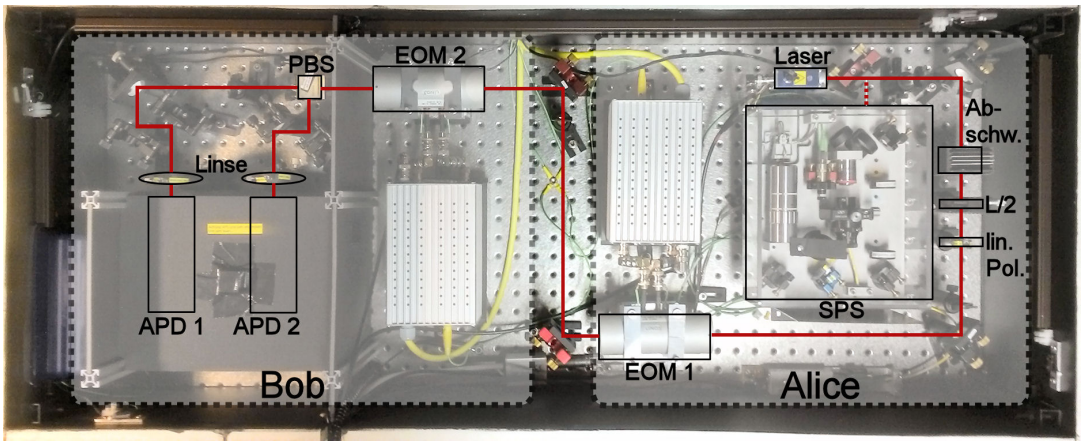


Abbildung 5 – Fotografische Darstellung des QKD-Aufbaus.
Photonen werden durch einen abgeschwächten Laser oder eine Einzelphotonenquelle (*single photon source*, SPS) erzeugt. Alice stellt mit Hilfe von $\frac{\lambda}{2}$-Plättchen (L/2) und linearem Polarisator (lin. Pol.) Photonen mit definierter 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

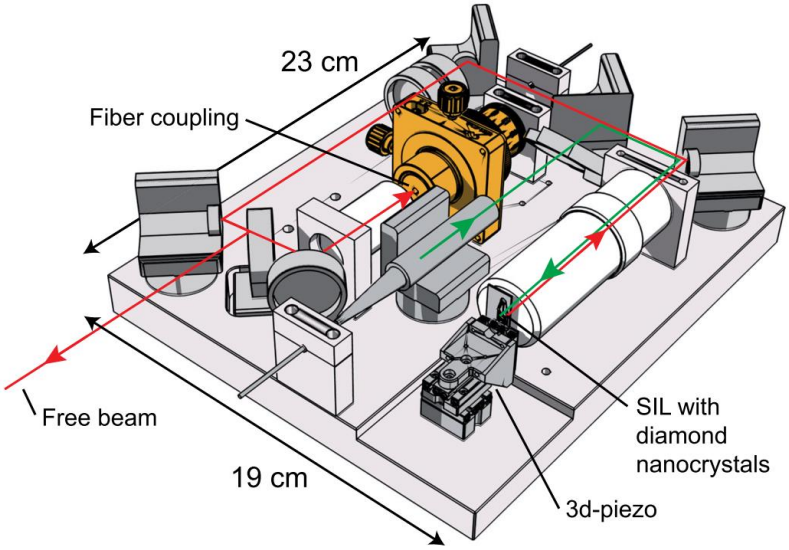


Abbildung 6 – Darstellung der verwendeten Einzelphotonenquelle [Sch12, S. 148].
Unten im Bild befindet sich die Probe mit den Naondiamanten zusammen mit der Öl-Immersionslinse (SIL) auf einem 3D-Piezo-Tisch. Der grüne Anregungslaser (532 nm) wird über eine Faser eingekoppelt, über einen dichroitischen 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

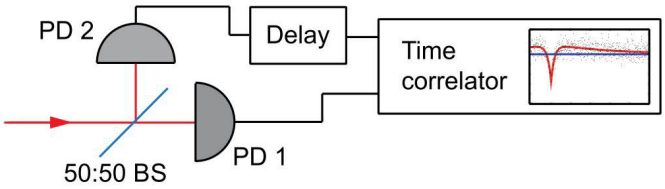


Abbildung 7 – Darstellung des Hanbury Brown & Twiss Aufbaus zur Bestimmung der Autokorrelation [Sch12, S. 11].
Die eingestrahlten Photonen werden durch einen 50:50-Strahlteiler (in der Abb. 50:50-BS) mit gleicher Wahrscheinlichkeit an einem von zwei Photodetektoren (in der Abb. PD) registriert, die eine 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.

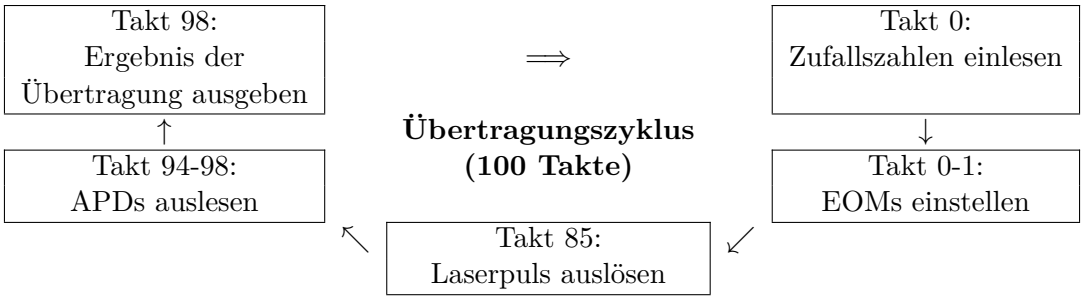


Abbildung 8 – Ablauf eines FPGA-Zyklus von 100 Takten.
In jeder Übertragung werden zuerst in Takt 0 Zufallszahlen, die von dem steuernden Programm „GUI.vi“ bereitgestellt werden, in das FPGA eingelesen und anhand dieser Werte die EOM-Spannungen eingestellt. In Takt 85 wird dann der Laserpuls ausgelöst 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.

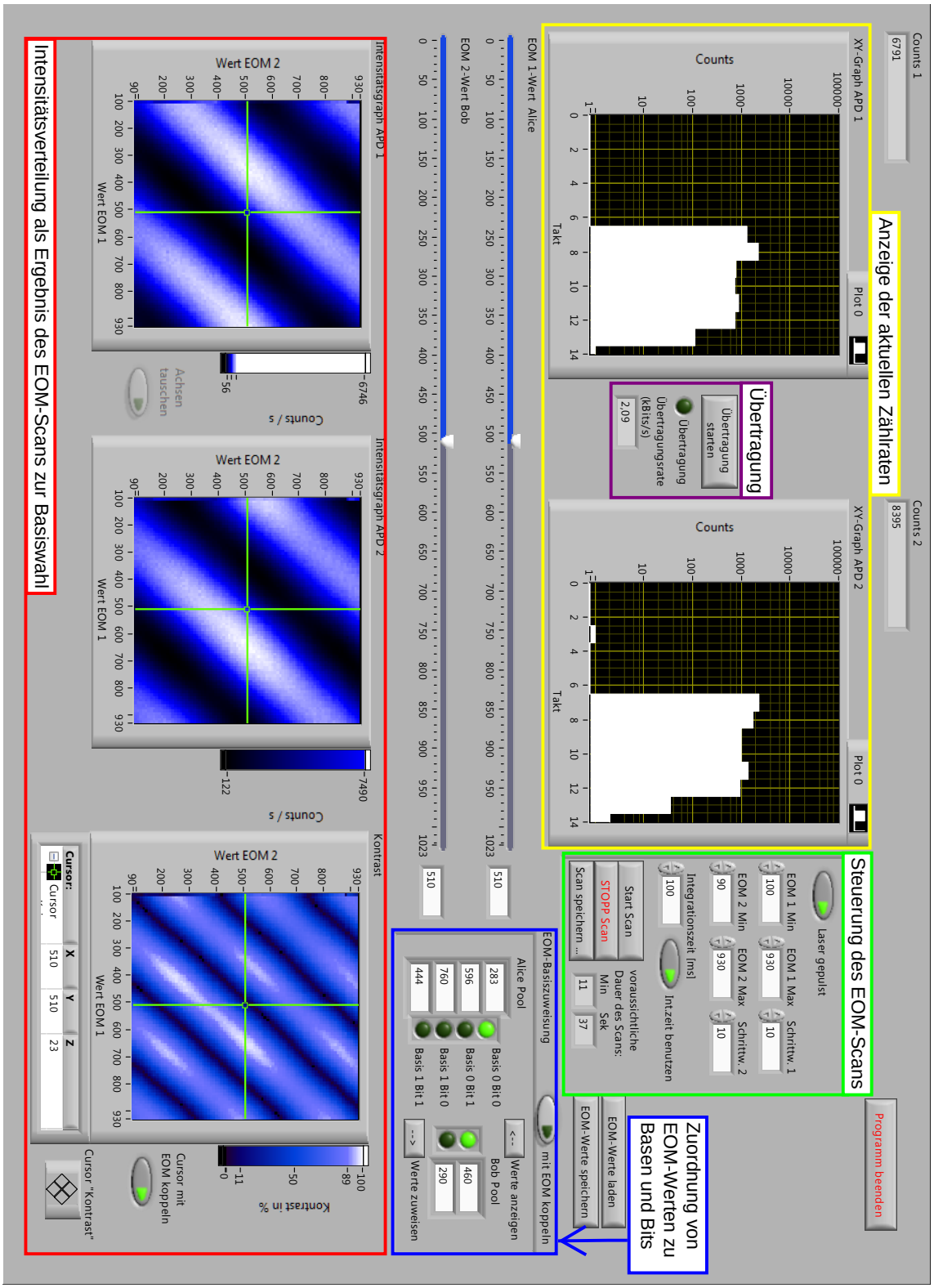


Abbildung 9 – Benutzeroberfläche des *LabView*-Programms „GUI.vi“.
Gelb markiert: Echtzeitanzeige der APD-Zählraten, darin (violett markiert) Steuerung der QKD-Übertragung.
Rot markiert: Darstellung der APD-Zählraten und des Kontrastes K in Abhängigkeit der EOM-Werte von EOM 1 und 2 als Ergebnis eines 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

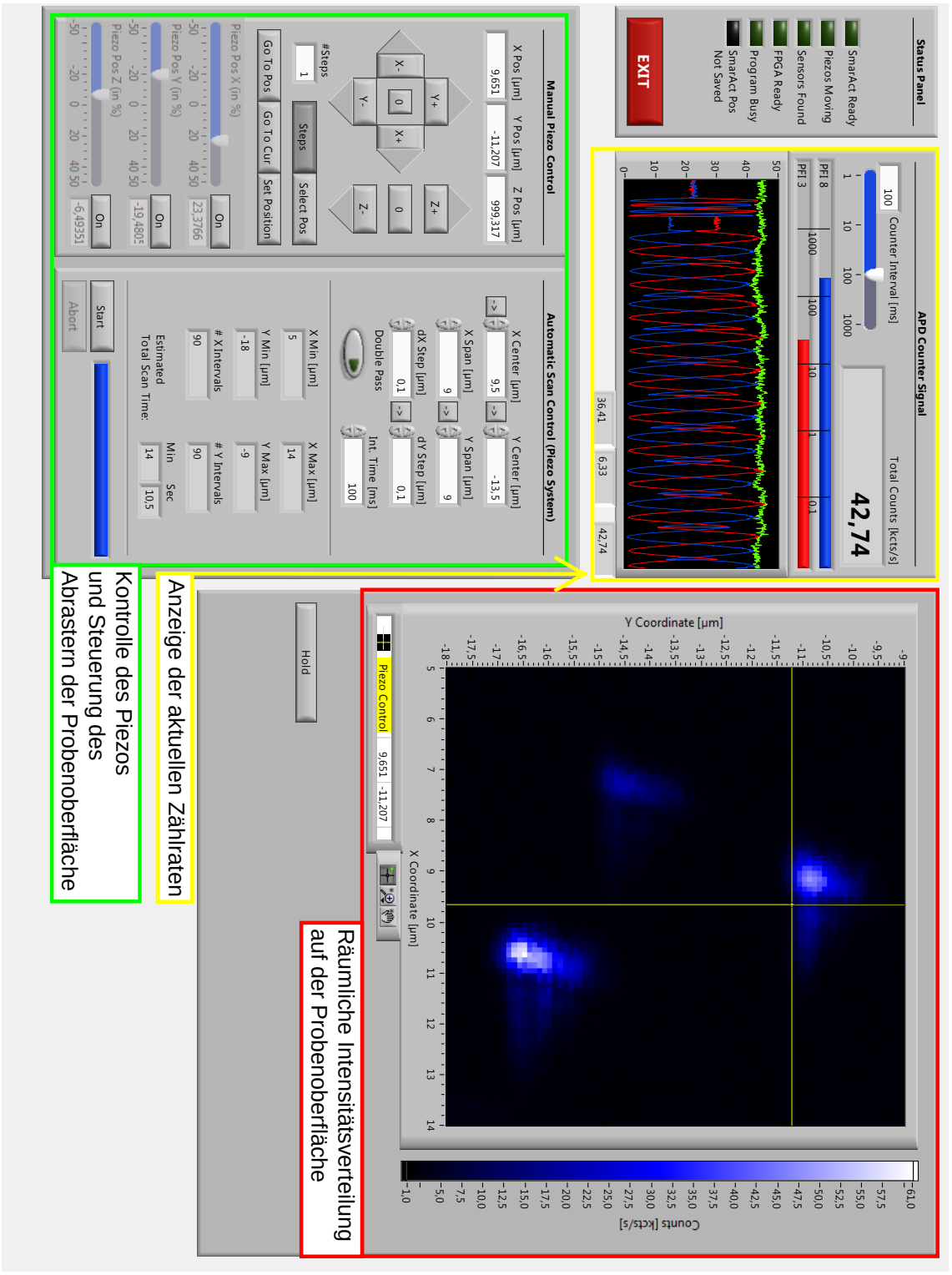


Abbildung 10 – Benutzeroberfläche des Programms „ScanSoft_ SmarAct_ 2011.vi“.
Gelb markiert: Echtzeitanzeige der APD-Zählraten.
Rot markiert: Darstellung der summierten Zählrate in Abhängigkeit von der räumlichen Position des Piezo-Tisches als Ergebnis eines Scans der Probenoberfläche.
Grün markiert: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

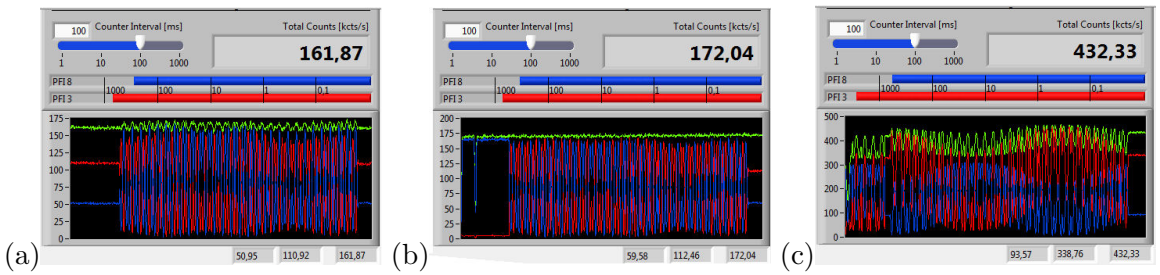


Abbildung 11 – APD-Signal vor und nach der Justage des Strahlenganges.
a) Der grobe Scan über den EOMs zeigt, dass die Maxima von APD 1 (blau) durchgehend über denen von APD 2 (rot) liegen. Dies deutet darauf hin, dass APD 2 noch nicht mittig getroffen wird.
b) Nach der Justage des Strahlenganges liegen 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).

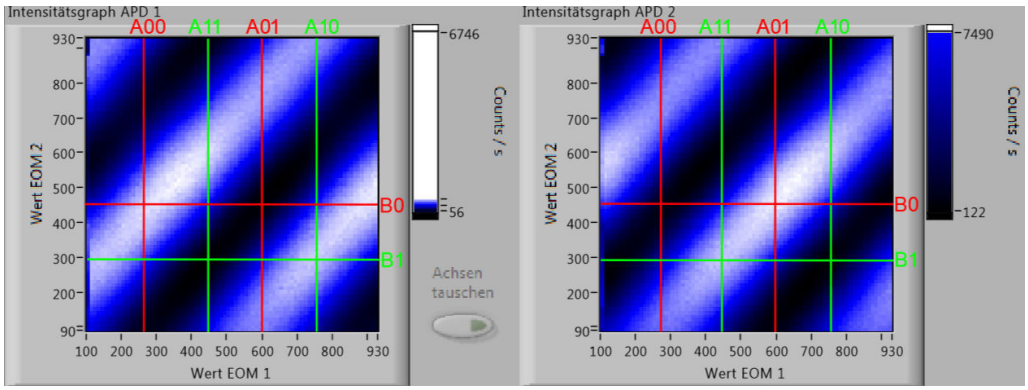
2. Eines der eben gewählten Bits von Alice in der falschen Basis bei Bob anzeigen (z.B. A01 und B1 auswählen) und so lange schrittweise diagonal wandern, bis die Signale von APD 1 und APD 2 etwa gleich sind (Punkt A01B1 in Abb. 12), dann diesen Wert für Alice und Bob übernehmen. Für das andere Bit (Punkt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

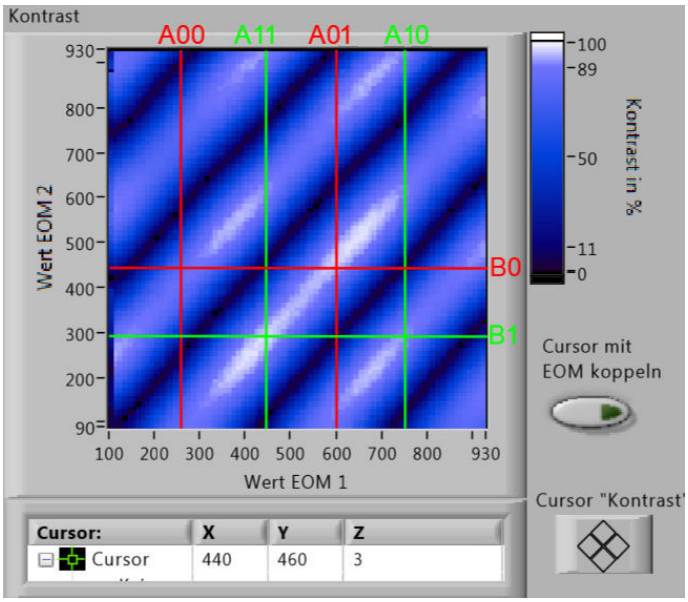


Abbildung 12 – EOM-Scan zur Basiswahl mit dem Laser.
Zu sehen ist das Ergebnis eines EOM-Scans. Dabei sind die Intensitätsgraphen der APDs (in der Abb. a) getrennt von dem sich daraus ergebenem Kontrast K (in der Abb. b) dargestellt. Darüber hinaus sind die Alice und Bob zugeordneten EOM-Werte in rot (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 SPS 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 SPS den Strahl auf die erste Irisblende richten;
2. 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 $(0\,\mu\text{m}, 0\,\mu\text{m})$ 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

$$f(x) = C_1 \cdot g^{(2)}\left(|x - x_0|\right) + C_0 = C_1 \cdot \left(1 - (K+1)\, e^{-k_1|x-x_0|} + K e^{-k_2|x-x_0|}\right) + C_0\,. \quad (8)$$

Die Konstante C_0 gibt dabei den unkorrelierten Untergrund an, da in einer Messung die Koinzidenzen im Nullpunkt x_0 oft nicht ideal auf Null abfallen. Da dieser Nullpunkt bei der Messung verschoben wird, 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. In dieser Darstellung sollten alle Anpassungsparameter positiv sein. 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}, die in dem *TimeHarp*-Programm eingestellt werden können, mittels folgender Formel berechnet werden

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

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

$$g^{(2)}(0) = \frac{C_0}{C_1 + C_0} = \frac{C_0}{C_1'}\,. \quad (10)$$

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.

- Datenblätter der verwendeten Geräte im Moodle zum Versuch.
- 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

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