Humboldt-Universität zu Berlin
Mathematisch-Naturwissenschaftliche Fakultät
Institut für Physik

Anleitung zum Versuch

Quantenkryptographie mit einzelnen Photonen – QKD via BB84

Fortgeschrittenen-Praktikum

Stand: November 2019

Inhaltsverzeichnis

1 Introduction

It is one of man's oldest endeavours to keep knowledge secret and to make it accessible only to the intended addressee. Nowadays, sophisticated mathematical methods are used in connection with powerful technology to protect information – or to cancel this protection [Sin01, S. 353 ff. and S. 383 ff.]. Characteristic for many encryptions is that a **Key** for the conversion of the so-called **cleartext** (i.e. the message to be kept secret) is used in the so-called **secret text**. In the Caesar cipher, for example, each letter is shifted by three digits [Sin01, p. 26], so the plaintext results in H U B the ciphertext K X E using the key 3.
The *One Time Pad* method (OTP) can provide absolute encryption security if the key meets certain requirements [Sin01, p. 152]. Thus the main problem of cryptography is secure key transmission. Currently, the most common methods are the so-called asymmetric methods [Sin01, p. 372]. These methods are based on mathematical problems like the factorization of large numbers [Sin01, p. 329 ff.], which could not be solved so far by efficient algorithms. A corresponding increase of the computing power of computers makes these methods potentially vulnerable. A functioning quantum computer would also be dangerous in this context, for which algorithms have already been developed (e.g. the SShorälgorithm for factorizing a number, see [Sho97]), which would render worthless the currently mainly used asymmetric encryption [Sin01, p. 386].
By a quantum key exchange (*Quantum Key Distribution*, QKD) unconditional security can be achieved by exploiting fundamental physical laws. Although it cannot be ruled out that the key transmission is also intercepted here, this can never happen unnoticed. The eavesdropper is already noticeable while the key is exchanged, before the actual message is sent. For this reason it can, in the worst case, prevent communication, but cannot even begin to receive information about the content of the message. Quantum cryptography does not only protect the content of the message, but also allows an eavesdropper to be detected immediately [Sin01, S. 411 ff.].

In this advanced internship experiment a QKD construction is worked on, which follows the BB84-Protokoll (BB84) developed by Charles Bennett and Gilles Brassard. The aim is to transfer a key according to BB84 and to assess the suitability of the devices used in the setup for this quantum cryptography method.

We are happy about any comments on the experiment and the instructions. Please give us a feedback at the end of the experiment!

2 Assignments

Put yourself in the position of a researcher at a university or in a company who wants to develop a device to QKD according to BB84. From this point of view, evaluate the suitability of the devices used in the present structure.

Preparation

1. Use this tutorial and your own sources to familiarize yourself with quantum information processing, quantum cryptography, and the BB84 protocol. Get also an overview of the used setup and the execution of the possible measurements.

2. Inform yourself about characteristic data and mode of action of the devices used in the setup, especially lasers, electro-optic modulator (EOM), avalanche photodiodes (APD), polarizers and retardation plates ($\frac{\lambda}{2}$ and $\frac{\lambda}{4}$ plates, respectively).

For your preparation, you can use your own sources in addition to those listed below too:

- data sheets of the devices used as well as additional documents for preparation (available from the supervisor)

- W. (2013). *Experimental Physics 2: Electricity and Optics.* Berlin: Springer. Available online at:
  `https://link.springer.com/book/10.1007/978-3-540-33795-9`
  – Chapter 8.6 Generation and application of polarized light

- Schiffner, G. (2005). *Optical communications engineering: physical foundations, development, modern elements and systems.* Wiesbaden: Vieweg+Teubner publishing house.
  Available online at:
  `http://link.springer.com/book/10.1007%2F978-3-322-80061-9`
  – 9.6 Avalanche photodiode and 10.3 Electro-optical modulator designs

In particular, prepare for the following questions:

- Why QKD? What are the benefits of the QKD?

- How does the BB84 protocol work?

- Why is the laser a bad quantum source (keyword statistics)?

- How can the single photon character of a source be determined?

- What is a NV center? What are its properties?

Execution

3. Determine which measurements you want to perform to evaluate the equipment. You can refer to the information given in Chap. 5 and define details with the supervisor.

4. Prepare the setup for the transfer of a key using the laser.

5. Use the laser in pulsed and continuous wave mode as well as the single photon source to perform transmissions. Measure the transmission rate per attenuation at least 10 times to get a good average value (don't forget the error calculation!).

6. Determine the autocorrelation curve for the NV-centers you use to generate the photons. Measure different NVs and start a data transfer for the NV with the best single photon character. Repeat the measurements on your best NV (autocorrelation, data transmission) for different excitation powers.

Evaluation

7. Write a report (protocol) about your results. Orientate yourself on the applicable standards in the advanced internship and refer to the context mentioned at the beginning of this discussion. Discuss the suitability of the devices used for a commercial application, discuss limits and possible alternatives, and in particular compare the two photon sources used. Graphically display the different measured quantities so that they can be easily compared. Choose a meaningful physical quantity. Interpret the results! Only recognizing a trend, without being able to explain it, is insufficient.

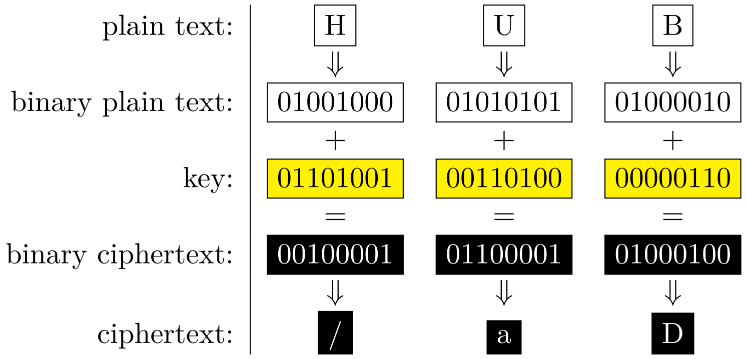
3 Theoretical Description

3.1 *One-Time-Pad* for classic encryption

The *One-Time-Pad* method can be used to encrypt the actual message using the block of keys transmitted via the QKD (the so-called *Pad*). Since only binary data is considered for quantum cryptography, it is assumed in the following that both plaintext and keys are present in this form. To encrypt a text, for example, the plaintext can first be converted into a binary form using a ASCII-table (or a comparable method).

Execution of a Cipher

In order to encrypt, each bit of the plaintext is binary added to one bit of the key, so the result is taken modulo 2, resulting in the sum $1 + 1 = 0$. The bits obtained in this way then form the binary ciphertext, which may be translated back into characters. This is shown in Fig. 1 is shown in an example.
The recipient of the message decrypts like the sender and also adds the key binary and bit by bit to the ciphertext to get the plaintext. This is possible because the bit-values 0 and 1 are additive inverse to each other (modulo 2). This is because the subtraction of two bits results in the same result as the addition.



plain text:	H	U	B
	⇓	⇓	⇓
binary plain text:	01001000	01010101	01000010
	+	+	+
key:	01101001	00110100	00000110
	=	=	=
binary ciphertext:	00100001	01100001	01000100
	⇓	⇓	⇓
ciphertext:	/	a	D

Abbildung 1 – Example of a binary cipher according to the OTP-method.

The plaintext H U B is converted into a binary form via a ASCII-table and added to the previously transmitted key in binary form. The resulting ciphertext can be binary or as a string / a D.

Requirements for this Procedure

The inventor of the OTP-procedure is usually G. Vernam, who filed the first patent application for it.
He describes in [Ver26] as prerequisites for the security of the procedure:

1. The key is, without repeating itself, as long as the plaintext.
2. The key (or parts of it) is inserted only once.
3. The key is composed of unpredictable random characters.

Under these conditions it can be proved within the framework of communication theory that plaintext cannot be determined without knowledge of the key [Sha49, S. 682].

3.2 Single photons as the Basis of Quantum Cryptography

The security of quantum cryptography is based on the use of the OTP- method on the one hand, and on the detection of every eavesdropping attack on the key transfer on the other. For the latter, it is essential in most cases to use single photons for key transfer. Because even if only two photons carry the same information, it is in principle possible to get an unnoticed copy of the information via a so-called *photon number splitting*-attack.
In the following a single photon source (*single photon source*, SPS) based on defect centers in nanodiamonds is presented and the method of autocorrelation measurement is described as proof of single photons.

Defect Centers in Nanodiamonds

A promising candidate for a SPS are defect centers in diamonds [ACS+11]. The spatial extent of the diamonds is often in the order of nanometers, which is why they are called nanodiamonds. A defect center is a structure created by the entry of foreign atoms or defects in the crystal lattice of carbon.
The SPS used here contains nitrogen -defects-centers (*nitrogen-vacancy center*, NV) in which a carbon atom of the diamond is replaced by a nitrogen atom and a gap (*vacancy*) in the crystal lattice occurs adjacent to it (see Fig. 2a). This NV-centre is excited by green laser light (532 nm) and emits photons in the visible red and infrared ranges. In model terms, the simplest structure to be considered for a SPS would be a two-level-system of a reason- and an excited state. This system emits photons with defined properties if the optical excitation is appropriate. In practice, however, these are usually three- or more-level-systems which contain metastable states between ground- and excited state (cf. Fig. 2b).
The outstanding advantage of using NV-centers as SPS is their ease of use. So the source does not have to be cooled and can be realized in a compact design [Sch12, p. 15].

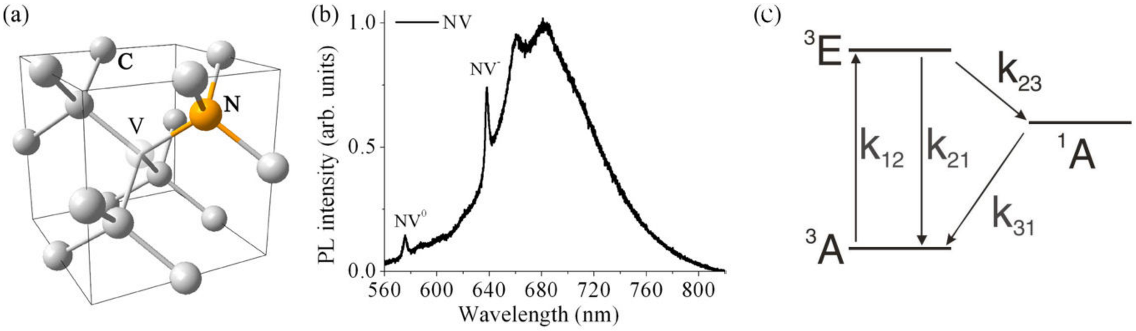


Abbildung 2 – Aharonovich.2011, Jelezko.2006.
a) A nitrogen atom (marked N) replaces a carbon atom in the crystal lattice of the diamond, adjacent to it a gap (marked V) occurs.
b) The spectrum at room temperature has two characteristic peaks at 575 nm (neutral NV center) and 637 nm (negatively charged NV center).
c) From the ground state ^3A electrons are lifted at a rate of k_{12} to the excited state ^3E, from which they can return to ^3A with k_{21} or to a metastable state ^1A with k_{23}. k_{31} indicates the rate of transition from the metastable state ^1A to the ground state ^3A.

Autocorrelation of Photons

The number of photons generated by a source at a time interval of τ can be described by the normalized second order correlation function [WM08, S. 39]:

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

Where I is the intensity operator, $: \cdots :$ corresponds to the normal order and $\langle \ldots \rangle$ indicates that it is a mean value. If one considers this function at $\tau = 0$, i.e. photons detected at the same time, then $|n\rangle$ results for photon number states (or Fock-states) from n photons in the same state [WM08, S. 41]:

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

If only one photon was generated, $g^{(2)}(0) = 0$, two $g^{(2)}(0) = \frac{1}{2}$ and so on. Since in practice effects occur that are neglected in the model, the ideal value $g^{(2)}(0) = 0$ is not always reached even for single photon sources. However, as long as $g^{(2)}(0) < \frac{1}{2}$, it can be assumed that the detected light contains a dominant proportion of single photons.
In the case of a three-level-system with transition rates k_{ij} from the i-ten to the j-ten state (cf. Fig. 2b), the autocorrelation can be described in good approximation by a function of the following form [JW06, p. 3213]:

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

With $k_\pm = -\frac{1}{2}P \pm \sqrt{\frac{1}{4}P^2 - Q}$ with $P = k_{21} + k_{12} + k_{23} + k_{31}$ and $Q = k_{31} \cdot (k_{21} + k_{12}) + k_{23} \cdot (k_{31} + k_{12})$, as well $K = \frac{k_2 + k_{31} - \frac{k_{23}}{k_{31}}}{k_+ - k_-}$.

3.3 Quantum Information Processing

Theoretical Description of Quantumbits

Following the binary system from classical information processing the units in quantum information processing are called Qubits (QBs).
Just as a classic bit has a state – either 0 or 1 –, a QB also has a state, which is conventionally expressed in Dirac- notation as follows [NC05, S. 13]:

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

This state is described as a unit vector in a two-dimensional, complex vector space (Hilbert space) whose orthonormal basis is formed by the states $|0\rangle$ and $|1\rangle$. When measured in this base, the state of the QBs collapses into one of the base states, where the amounts of α and β correspond to the probability density of obtaining 0 and 1, respectively: $|\langle 0||Psi\rangle|^2 = |\alpha|^2$ and $|\langle 1|\Psi\rangle|^2 = |\beta|^2$.
The collapse of the wave function causes, in particular, that a further measurement in this base will certainly result in the same state as the previous one. Any information about the original state is therefore lost during the first measurement.
Furthermore, another pair of states, $|+\rangle$ and $|-\rangle$, is interesting. They form an orthonormal base of the same vector space which is conjugated with the base of the states $|0\rangle$ and $|1\rangle$. This means that the measurement of a base state of one base yields with equal probability one of the two base states of the other base.

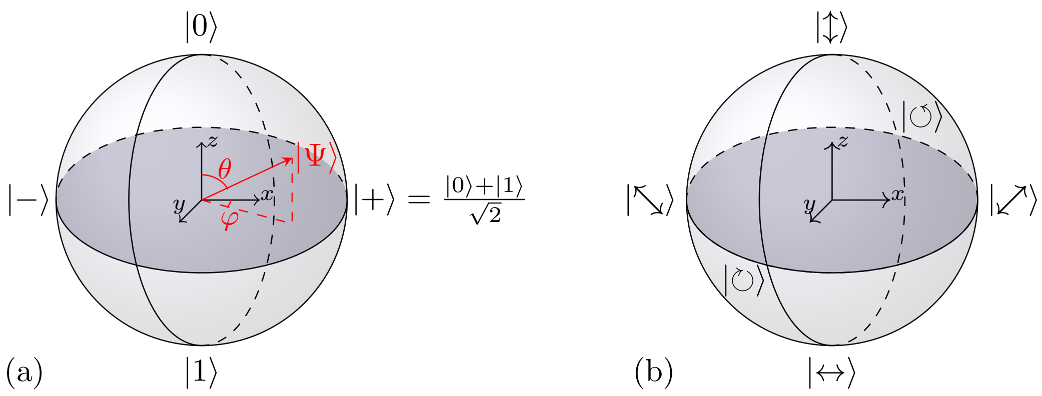


Abbildung 3 – Bloch- and Poincaré-sphere.
a) Bloch- Sphere to illustrate the vector space in which the QB in the state $|\Psi\rangle$ is in a superposition of the basic states $|0\rangle$ and States located on opposite sides of the sphere are orthogonal to each other. States on the equator collapse with equal probability into one of the base states $|0\rangle$ or $|1\rangle$.
b) Poincaré- Sphere to illustrate the conjugated bases of polarized light. It can be used like the Blochßphere to represent polarized photons as QB.

Formally the states $|+\rangle$ and $|-\rangle$ can be defined as follows [NC05, S. 22]:

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right) \cdot |0\rangle + e^{i\cdot\varphi} \cdot \sin\left(\frac{\theta}{2}\right) \cdot |1\rangle\,, \qquad \text{mit } \theta \in [0,\pi]\,, \varphi \in [0,2\pi]\,. \tag{5}$$

This leads to a vivid representation as points in polar coordinates on the surface of a unit sphere, the so-called Bloch-ball (s. Abb. 3a).

Polarized Photons as Quantumbits

To put these states of QB into practice, polarized photons can be used. A possible basis are linear horizontally and vertically polarized photons, of which conventionally horizontally polarized photons in the state $|\leftrightarrow\rangle$ are assigned the value 0 and vertically polarized photons in the state $|\updownarrow\rangle$ are assigned the value 1. This base is also called Basis (HV-base).
Another choice of base states is given by circularly polarized photons in the base states |↻⟩ (corresponds to value 0) and |↺⟩ (corresponds to value 1). This circular basis (RL-base) is conjugated with the HV-base, the states $|\leftrightarrow\rangle$,$|\updownarrow\rangle$ and |↻⟩,|↺⟩ are thus related to each other like $|0\rangle\,,|1\rangle$ and $|+\rangle\,,|-\rangle$. A third possibility would be to use diagonally polarized photons, since the diagonal base is conjugated with both HV- and RL-base.
Analogous to the Bloch-sphere, this fact can also be represented on a sphere surface, the so-called Poincaré-sphere (s. Abb. 3b). This has the advantage that polarization manipulations can be represented as rotation in the Poincaré-sphere.

3.4 Procedure of the BB84-protocoll

The first cryptographic method based on quantum mechanics was presented in 1984 by Charles Bennett and Gilles Brassard [BB84]. If the sender and receiver of the secret message are referred to as Alice and Bob, a transmission using the BB84 protocol can be described in five steps, which are shown in Fig. 4.
As explained in the last chapter, the measurement produces a random result where any information is lost if Bob does not measure the polarization in the same base as Alice. This means that Bob only receives useful data from an average of half of the photons detected. Since a potential eavesdropper, usually called Eve (*eavesdropping*), faces the same problem, a *intercept-resend* attack involves the risk of altering the transmission in such a way as

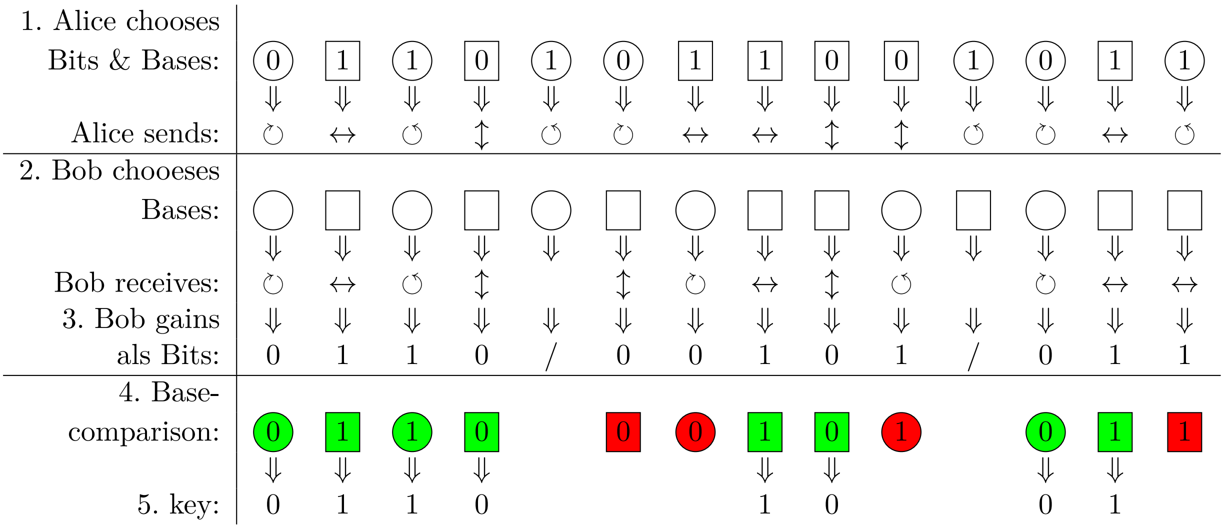


Abbildung 4 – Procedure of the BB84-protocol in 5 steps within three phases: The transmitter (Alice) transmits a random sequence of bits in randomly selected bases (□ stands for the retilinear base, ○ for the circular) to the receiver (Bob) via a quantum channel and sends Bob a chain of photons. Each photon represents 1 Bit of the sequence in the base selected for that bit. When Bob receives these photons (which may result in transmission losses marked with /), he randomly decides for each of them, independently of Alice, in which of the two bases he measures the polarization. Bob interprets the result of the measurement as binary 0 or 1. Alice and Bob then compare the correctly transmitted bits (marked green) over a public channel and determine the key..

to reduce the concordance of bits which, according to Bob's basic choice, should actually be identical to Alice's bits. Furthermore, Eve cannot copy any unknown quantum state of the photon [WZ82]. If only one photon is transmitted for each key bit (as described in chapter 3.2), she cannot divide the signal to perform measurements unnoticed.
If the transmission was not intercepted, the bits compared in step 4 should ideally match 100%. However, this value can never be reached with real transmissions, since losses can always occur during transmission or detection. If the transmission was completely intercepted, an average of 75% of the compared bits should still match, since Eve chose the correct base for an average of 50% of these bits, but still received the correct QB for 50% of the others.
If more than 88% were transmitted correctly, the key can be improved by subsequent processes (such as *error correction* and *privacy amplification*) so that a secure transmission is still possible [SP00]. In this case, the transmitted bits can be used as a key block for subsequent secret communication via OTP procedure over a public channel.

4 Build-Up

The entire experimental realization is compactly designed so that the optical setup can be accommodated in a box measuring $122 \times 60 \times 30\,\mathrm{cm}^3$ and arranged together with the other devices on a single table. This results in a free beam distance of about half a meter between the devices of the sender and the receiver (in the following again called Alice and Bob).

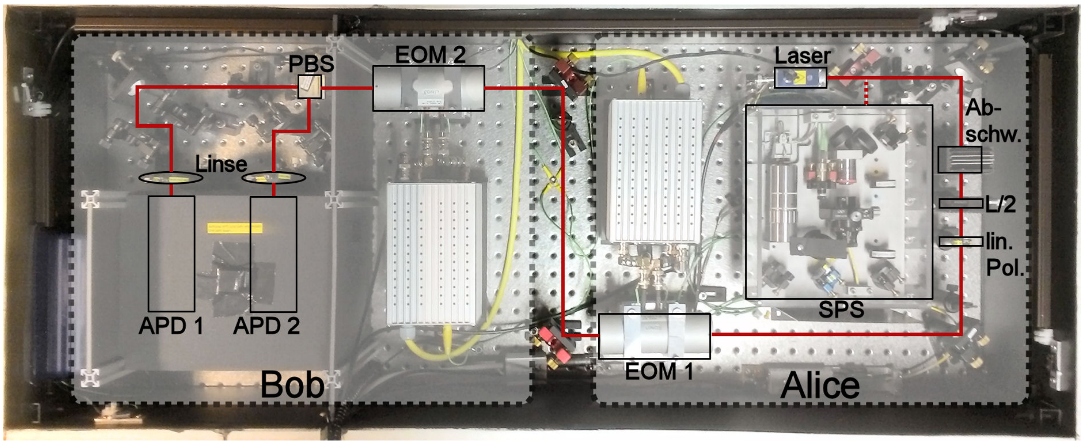


Abbildung 5 – Photographic representation of the QKD setup.
Photons are generated by an attenuated laser or a single photon source (*single photon source*, SPS). Alice provides photons with defined polarization using $\frac{\lambda}{2}-plate(L/2)$ and linear polarizer (linear pole). With the electro-optical modulator (EOM 1) it can set base and bit. Bob detects the number of bits over another EOM (EOM 2) and a polarization beam splitter cube (polarising beam splitter (PBS)) separated photons according to the transmitted bit value by two avalanche photodiodes (avalanche photodiodes (APDs)).
If the EOMs are set so that the photons are circularly polarized according to EOM 2, the ensemble of PBS and APDs functions as Hanbury Brown & Twiss Aufbau (Hanbury Brown & Twiss Aufbau (HBT)).

An overview of the current setup is shown in Fig. **??** and is explained in more detail below. Photons are generated either by a laser diode (QL65D6SA, Roithner, driver: iC-NZN EVAL, ic-Haus) with a wavelength of 650 nm or by a compact single photon source (SPS) based on NV-centers. The laser can either emit continuous photons in continuous wave mode or single pulses every 2,5 µs. With a $\frac{\lambda}{2}$-plate the polarization of these photons is then adjusted to the vertical polarization direction of a linear polarizer.
Since all photons now have the same polarization, all bit-values selectable by Alice in the corresponding polarization bases can be realized by using $\frac{\lambda}{2}$- and $\pm\frac{\lambda}{4}$-plates in the 45°-angle to the vertical polarization. In order to be able to change this setting within as short a time as possible, an electro-optical modulator (EOM, hereinafter as EOM 1) based on potassium dideuterium phosphate crystals (LM0202 P VIS, Linos), which acts like a $\frac{\lambda}{2}$- ,$+\frac{\lambda}{4}$- or $-\frac{\lambda}{4}$- plate, depending on the voltage applied.
Now the photons leave Alice's setup to reach Bob after about half a meter of free jet. With this the basic choice is also made via a EOM (hereinafter EOM 2) in conjunction with a polarization beam splitter cube (PBS). The EOM leaves the incoming photons in their polarization base or interchanges linear and circular polarization depending on Bob's measurement base. The PBS then registers linearly polarized photons with certainty at one of two detectors, whereas circularly polarized photons are unpredictably registered at one of the two detectors. To detect the photons, avalanche photodiodes (*avalanche photodiode*, APD) based on silicon (SPCM-AQRH-33, Excelitas) are used, which are focused on with a lens. Since the power emitted by the laser is far too high for it and would overload it, attenuators are used to reduce the laser power.

4.1 Equipment

Compact Single-Photon Source

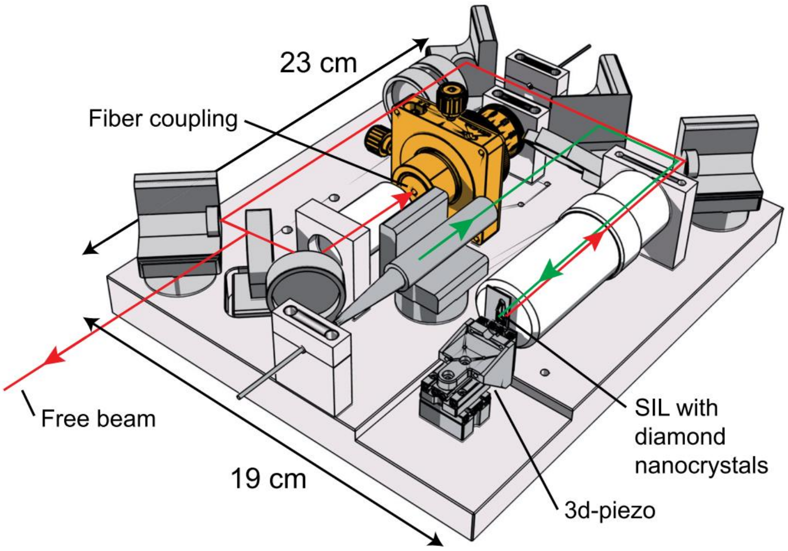


Abbildung 6 – Presentation of the single photon source used [Sch12, S. 148].
At the bottom of the image, the sample with the nanodiamonds and the oil immersion lens (solid immersion lens (SIL)) are on a 3D piezo table. The green excitation laser (532 nm) is coupled in through a fiber, directed through a dichroic mirror (not in the image) through the lens to the SIL, where it excites a NV-center to emit single photons. In contrast to the reflected photons of the excitation laser, these can pass unhindered through the dichroic mirror and are directed to Alice's structure by free beam coupling.

An overview of the structure of the compact single photon source is shown in Fig. 6. The photons are generated in nanodiamonds with NV-defect centers applied to an oil-immersion lens (*solid immersion lens*, SIL). Together with a lens, this provides a higher refractive index between object and lens for a more efficient collection of photons. The three-dimensional positioning of the sample is done by a piezo-table
(SLC-1720-S-HV, SmarAct, driver: MCS-3D, SmarAct). A 532 nm-laser (about 100 µW) excites the NV-defect centers at room temperature. A dichroic mirror is used to separate the emitted photons from the reflected 532 nm-laser. A short pass filter (785 nm, not shown in the image) and a long pass filter (620 nm, not shown in the image) filter out remaining light. The photons of the SPS can now either be coupled into a fiber or transmitted via a free beam, the latter being used in this experiment.

Hanbury Brown & Twiss Setup

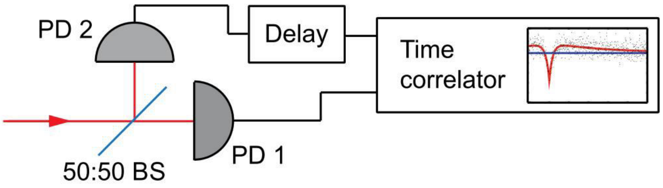


Abbildung 7 – Illustration of the Hanbury Brown & Twiss construction to determine the autocorrelation [Sch12, p. 11].
The irradiated photons are registered by a 50:50-beam splitter (in Fig. 50:50-BS) with equal probability at one of two photodetectors (in Fig. PD), which start or stop a time measurement (in Fig. „Time correlator"). One of the two channels is delayed relative to the other (in the figure at the "delay") in order to achieve a shift of the time zero point.

To perform an autocorrelation measurement, the existing setup can be used as a so-called Hanbury Brown & Twiss Aufbau. The structure is schematically shown in Fig. 7. It consists of a 50:50-beam splitter, two single photon detectors, one of which acts as a start-, and the other as a stop-signal generator for time measurement, and a device for time measurement in the nanosecond range (*TimeHarp*). The photons arriving at the beam splitter are registered with equal probability at one of the two detectors. The time correlator determines the time difference τ between the two measured photons. If the number of coincidences between both detectors is plotted over the time difference τ between two events, a characteristic curve is obtained. This can be used as a measure for the second order correlation function $g^{(2)}(\tau)$ if it is normalized accordingly. The typical course of such a measurement is shown in Fig. 8.

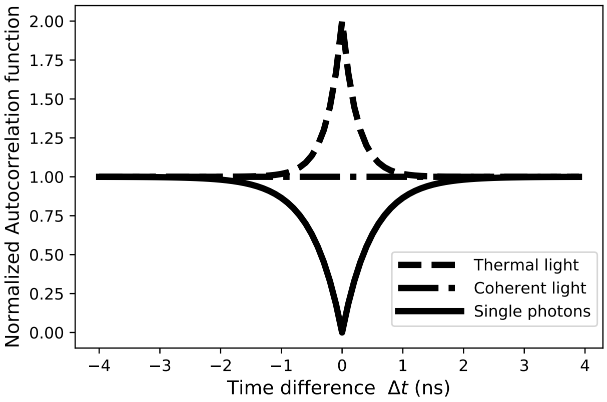


Abbildung 8 – representation of the second order correlation function $g^{(2)}$ for different light sources.
For a thermal source (e.g. a light bulb) there is an increased chance to find several photons at once, which can be measured by a peak in the correlation function. A coherent light source (e.g. a laser) does not correlate the single photons with each other, so the correlation function is constant. For a single photon source, only one photon can be detected at a time. This is for a dip in the correlation function.

Since two APDs and one PBS are available as detectors in the structure used for the QKD, only both EOMs have to be set in such a way that they act together like a $\frac{\lambda}{4}$- plate and so photons incident on the PBS are registered with the same probability on one of the two APDs.

Polarization Manipulation by using EOMs

The input polarization of the photons set vertically by the linear polarizer is manipulated by Alice with the help of EOM 1 in such a way that it corresponds to the base state belonging to the bit in the selected base: If Alice wants to send bit 0 in base 0, she leaves the vertical polarization unchanged, for bit 1 in base 0, she lets EOM 1 act like a $\frac{\lambda}{2}$-plate to rotate the polarization 90°. In base 1, Alice must circularly polarize the photon. She sets her EOM as $+\frac{\lambda}{4}$- (Bit 0) or $-\frac{\lambda}{4}$-plate (Bit 1) depending on the bit value.
Bob uses EOM 2 for basic dialing. Will Bob in the HV-base (base 0), it lets EOM 2 act as $\frac{\lambda}{2}$-platelets, which leaves the polarization base of the photon intact. If, on the other hand, he wants to be in the RL-base (base 1), his EOM acts as $+\frac{\lambda}{4}$-plate and converts circular to linear polarization and vice versa. A PBS behind EOM 2 registers the photon according to its polarization at one of two APDs if it is linearly polarized. If, on the other hand, it is circularly polarized, it is registered with the same probability at one of the two detectors. Since horizontally polarized photons are registered at APD 1, the bit-value 0 is assigned to this APD.

These settings and assignments allow a transmission according to the principles of the BB84-protocol, because:

- Sends Alice bit 0 in base 0, so the photon remains behind EOM 1 in the state $|\updownarrow\rangle$. EOM 2 converts it to $|\leftrightarrow\rangle$if Bob also chooses base 0, and to $|\circlearrowright\rangle$if he chooses base 1. By using the PBS the state $|\leftrightarrow\rangle$ is definitely registered at APD 1 (bit 0), $|\circlearrowright\rangle$ is registered at 50% each at one of the two APDs.

- If Alice sends bit 1 in base 0 and measures Bob in the same base, both EOMs act as $\frac{\lambda}{2}$-plates, whereby the photon in the state $|\updownarrow\rangle$ can be registered at APD 2 (bit 1). If Bob chooses the wrong base, he receives a photon in the state $|\circlearrowleft\rangle$, which is also registered by the PBS to 50% each at one of the two APDs.

- If Alice decides for base 1, the state $|\circlearrowright\rangle$ (bit 0) or $|\circlearrowleft\rangle$ (bit 1) results at EOM 1 depending on the bit-value. If Bob measures in base 0, the result is again unpredictable, but at base 1 he measures with certainty Alice' bit 0 at APD 1 (since EOM 2 $|\circlearrowright\rangle$ converts to $|\leftrightarrow\rangle$) or bit 1 at APD 2 (by converting $|\circlearrowleft\rangle$ to $|\updownarrow\rangle$).

4.2 Communicating

The entire experimental setup is constructed using a *field programmable gate array* (FPGA) (NI-R7813, National Instruments), which is programmed using *LabView* (Version 2011, National Instruments). Two *LabView*-programs are also available for interaction.
, von denen eines allerdings fast ausschließlich für die SPS relevant ist.

Program „fpga3.vi“ for the control of the setup and execution of the transfer

The FPGA is programmed via *LabView*, for which the program „fpga3.vi"running in the background is used.
The transmission of one bit uses 100 clocks of the FPGA. At a clock rate of 40 MHz, a maximum of 400 kBit per second can be transmitted (with full efficiency of photon generation and detection, and without losses within the transmission path). The duration of a clock is correspondingly with 25 ns.

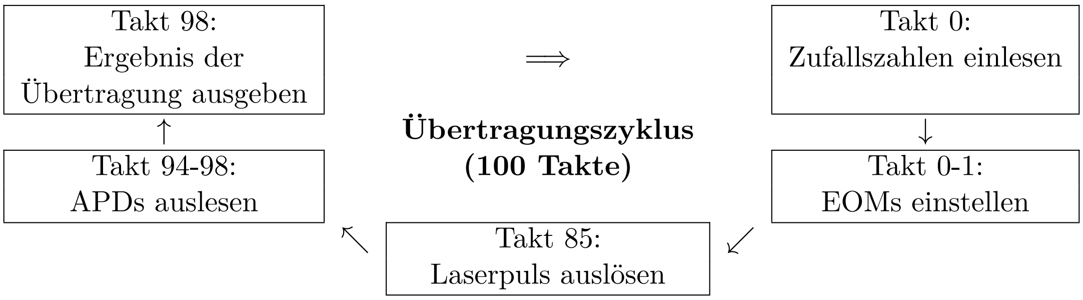


Abbildung 9 – Ablauf eines FPGA-Zyklus von 100 Takten.
In each transmission, random numbers provided by the controlling program „GUI.vi“ are first read into the FPGA in clock 0, and the EOM-voltages are set on the basis of these values. In clock 85 the laser pulse is triggered and the optical transmission is started. The generated photons pass both EOMs, where they are polarized according to the chosen EOM-voltages. From clock 94 to 98, the photons arriving at the APDs are registered and last output in clock 98 to the controlling program from which they are stored.

Within a transmission cycle of 100 clock pulses, 4 Bit of random data from the program „GUI.vi“ are read in at the beginning (clock pulse 0, see also Fig. 9) and the corresponding voltages for both EOMs (as a binary value between 0 and 1024) from a list that must also

be created in advance with „GUI.vi“. These values are then converted into voltages by a digital-to-analog converter and passed to the EOMs via an amplifier. Since these need some time for the conversion, the program waits about 2 µs until clock 85 before sending a signal to the laser that triggers the pulse in pulsed mode.
9 bars (225 ns) later 4 bars (100 ns) long the APD signals are recorded. For each APD it is stored binary separately whether (at least) one photon was detected (bit 1) or not (bit 0). Also within the time period from clock 85 to 99 in each clock it is counted how many photons were registered within 10.000 passes (i.e. 25 ms) at each APD. These values are represented in „GUI.vi“ as a histogram. Finally, a 6 Bit long value is passed to the program „GUI.vi“ in bar 98 and stored by it for later analysis, which contains the following:

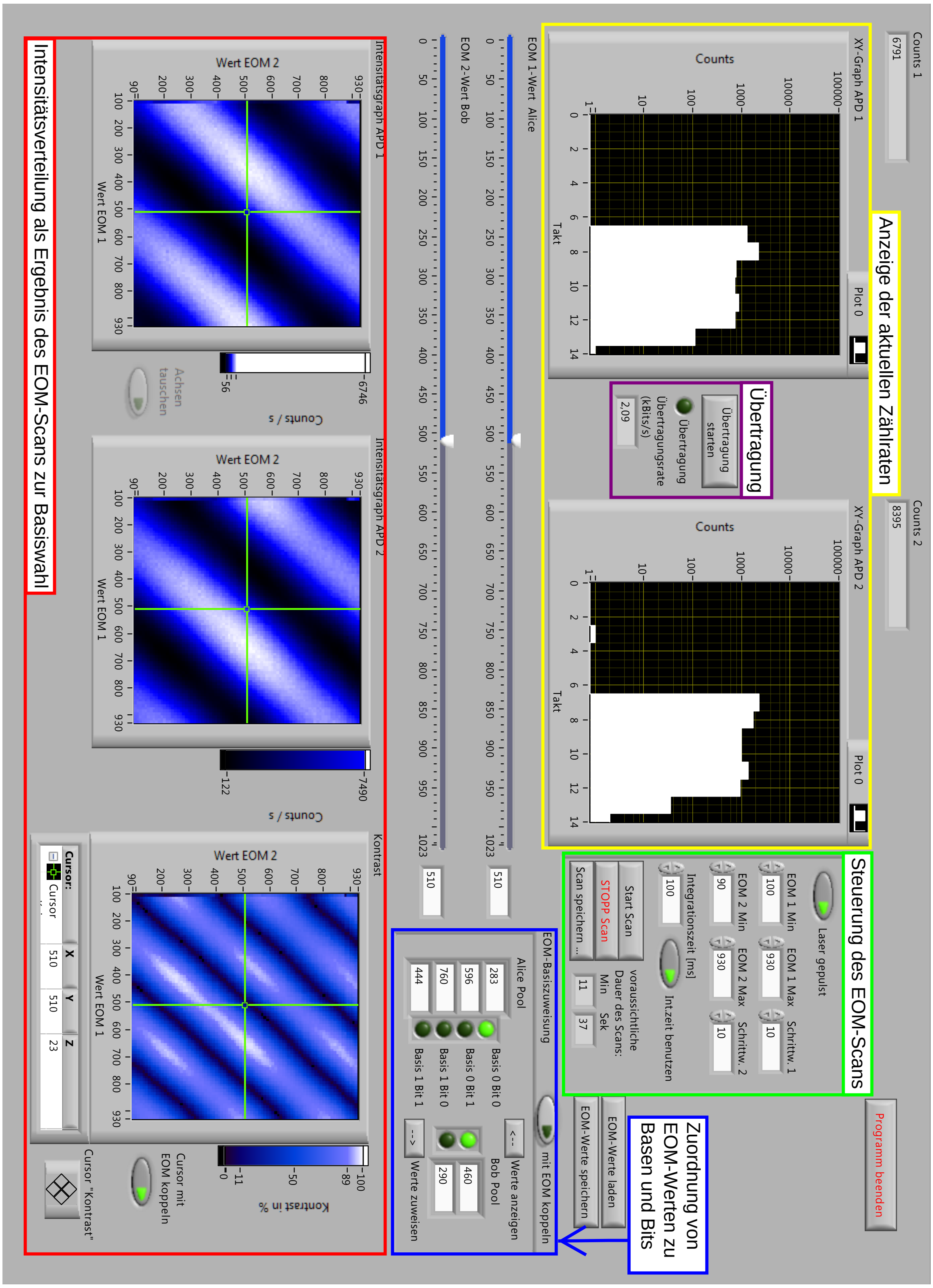
Base & Bit Alice (2 Bits) | Base Bob (2 Bits) | detection APD 1 & 2 (2 Bits)

Program „GUI.vi“ for setting-up the EOMs and communication of the QKD-transmission

The program „GUI.vi“ allows the change between continuous wave operation and pulsed operation at the laser, the control of the EOMs and displays the APD-count rates in real time. The user interface is shown in Fig. 10.
Voltages in the range of ±250 V can be applied to the EOMs via a scale in integer steps from 0 to 1024. The detected photons are plotted separately according to the APDs in two histograms in the form counting rate per clock (marked yellow in the figure).
The program also allows scans over the entire possible range of voltages of the EOMs (Control marked green in the figure). The duration of a scan depends on the set step size and is, for example, with a step size of 30 about one minute, with a step size of 10 already over ten minutes. For each APD of a scan, the count rates are displayed as an intensity distribution depending on both EOM-voltages (marked red in the figure). The EOM-voltages are expressed as integer values between 0 and 1024. White areas indicate a high count rate, black areas a low count rate and blue areas a medium count rate.
The contrast K of the APD count rates R_i is also shown in the third image:

$$K = \frac{|R_{\text{APD }1} - R_{\text{APD }2}|}{R_{\text{APD }1} + R_{\text{APD }2}} \tag{6}$$

(also marked red in the figure). In this diagram, white areas represent a contrast of $K \geq 90\%$ and black areas $K \leq 10\%$. For the basic selection of Alice and Bob, both voltage pairs with the highest possible contrast (pairs of identical bases) and with the lowest possible contrast (pairs of different bases) are required for the EOMs, for which this representation can be used (see also the representation in chapter **??**).
During the transmission, the program „GUI.vi“ provides the random numbers required by the FPGA, which are selected via a file dialog. Genuine random numbers can be obtained via the Nanooptics working group’s website. Alternatively, the file „sampledata-600MB.bin“ can be used in the execution directory of the program. The program also saves the data recorded by „fpga3.vi“ in a file „key.bin“ for later or simultaneous analysis by „analyser_ qkd.exe“ in the execution directory.



Counts 1: 6791

Counts 2: 8395

Übertragungsrate (kBits/s): 2,09

EOM 1 Min: 100

EOM 1 Max: 930

Schrittw. 1: 10

EOM 2 Min: 90

EOM 2 Max: 930

Schrittw. 2: 10

Integrationszeit [ms]: 100

voraussichtliche Dauer des Scans: Min 11 Sek 37

Alice Pool: 283, 596, 760, 444

Bob Pool: 460, 290

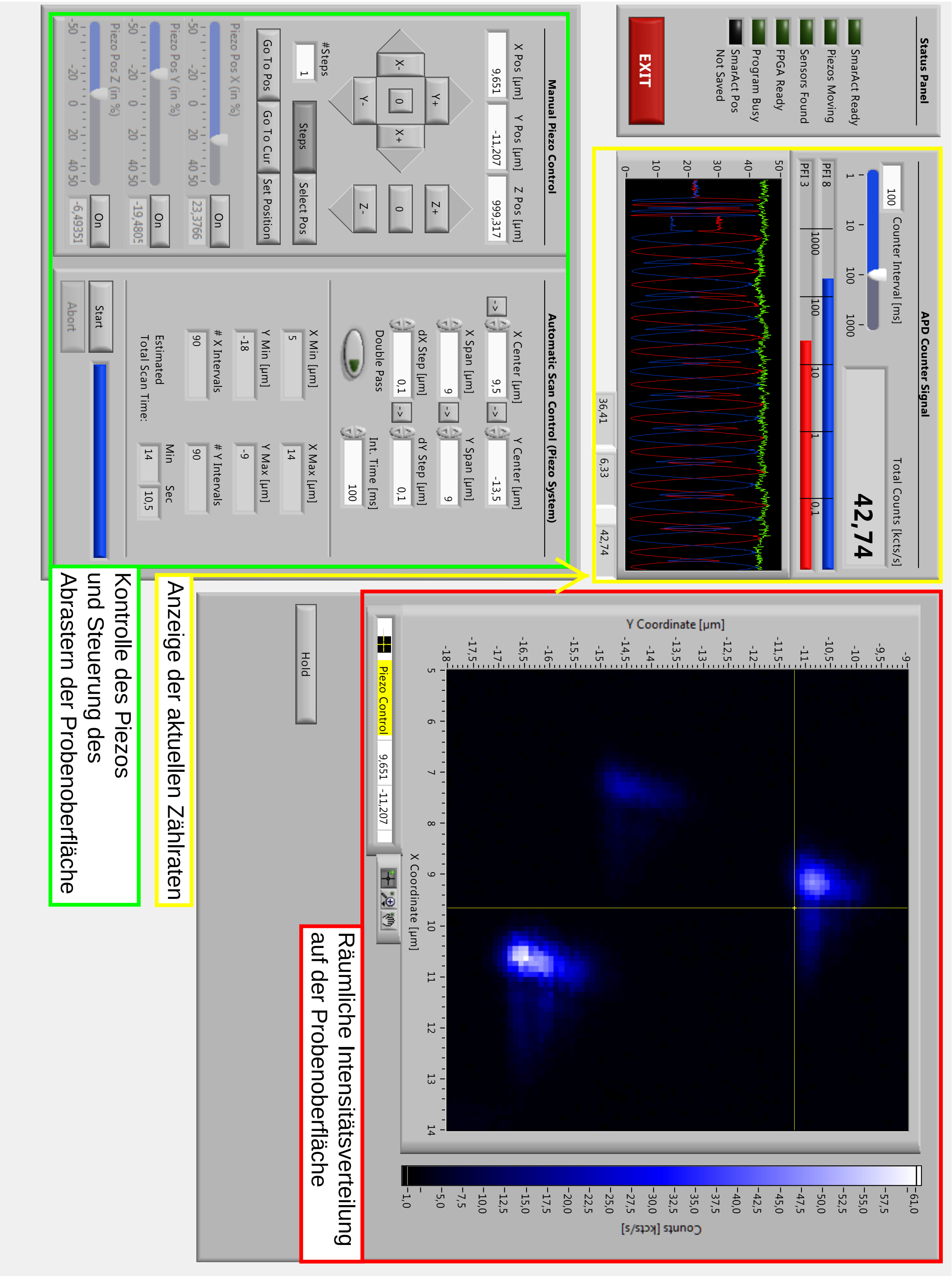
EOM 1-Wert Alice: 510

EOM 2-Wert Bob: 510

Cursor: X 510, Y 510, Z 23

Abbildung 10 – user interface of the *LabView*-Program „GUI.vi“.
yellow labeled: real time counting of the APD-count, darin (purple labeled) Steuerung der QKD-Übertragung.
Marked red: depiction of APD-count rates and contrast K depending on EOM-values EOM 1 and 2 as a result of an EOM-scan (Controlling is marked green). There are two controller for fine adjustment of the EOMvalues. The assignment of the bits and bases are shown here as well (marked blue).

Program „ScanSoft_ SmarAct_ 2011.vi“ for controlling the Piezo-driver



Status Panel

APD Counter Signal

Counter Interval [ms]: 100

Total Counts [kcts/s]: 42,74

Manual Piezo Control

X Pos [µm]: 9,651

Y Pos [µm]: -11,207

Z Pos [µm]: 999,317

#Steps: 1

Piezo Pos X (in %): 23,3766

Piezo Pos Y (in %): -19,4805

Piezo Pos Z (in %): -6,49351

Automatic Scan Control (Piezo System)

X Center [µm]: 9,5

Y Center [µm]: -13,5

X Span [µm]: 9

Y Span [µm]: 9

dX Step [µm]: 0,1

dY Step [µm]: 0,1

Int. Time [ms]: 100

X Min [µm]: 5

X Max [µm]: 14

Y Min [µm]: -18

Y Max [µm]: -9

# X Intervals: 90

Y Intervals: 90

Estimated Total Scan Time: Min 14 Sec 10,5

Piezo Control: 9,651 -11,207

Kontrolle des Piezos und Steuerung des Abrastern der Probenoberfläche

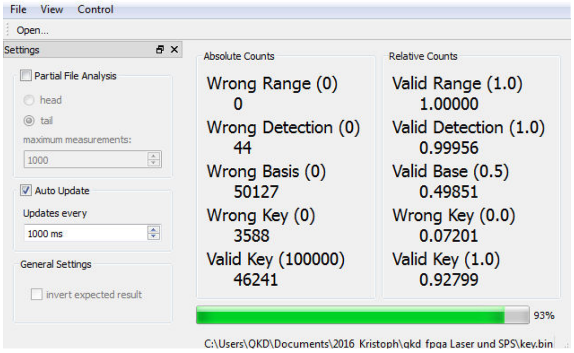
Anzeige der aktuellen Zählraten

Räumliche Intensitätsverteilung auf der Probenoberfläche

Abbildung 11 – user interface of the program „ScanSoft_ SmarAct_ 2011.vi“.
yellow marked: real-time display of APD-count rates.
red marked: Display of the summed counting rate as a function of the spatial position of the piezo-table as a result of a scan of the sample surface
green marked: positioning of the Piezo-table and control of the scan.

The program „ScanSoft_ SmarAct_ 2011.vi“ is available for controlling the piezo driver. The user interface is shown in Fig. 11.
The program also provides the counting rate of the APDs (marked yellow in the figure) individually and under the name „Total Counts“, in the following briefly C_T. In addition to this function, which is also useful for displaying the course during a EOM scan, the program is used to position the piezo stage with the nanodiamonds in all three spatial directions x, y and z and also enables automatic scans (marked green in the figure). As a result of such a scan an intensity distribution is displayed which shows the measured summed count rate depending on the spatial position (marked red in the figure). White areas indicate one or more NV- centers. After a scan, the position of the piezo stage can be adjusted so that the photons of one of the found NV-centers can be used for further measurements and transmissions.

Program „analyser_ qkd.exe“



□ Partial File Analysis

○ head

● tail

maximum measurements: 1000

☑ Auto Update

Updates every 1000 ms

General Settings

□ invert expected result

Absolute Counts

Wrong Range (0)
0
Wrong Detection (0)
44
Wrong Basis (0)
50127
Wrong Key (0)
3588
Valid Key (100000)
46241

Relative Counts

Valid Range (1.0)
1.00000
Valid Detection (1.0)
0.99956
Valid Base (0.5)
0.49851
Wrong Key (0.0)
0.07201
Valid Key (1.0)
0.92799

93%

C:\Users\QKD\Documents\2016 Kristoph\qkd fpga Laser und SPS\key.bin

Abbildung 12 – Benutzeroberfläche des Programms „analyser_ qkd.exe“

During the transfer of the bits, a file is created on the computer used for control, which contains the following (in the sequence shown) for each transferred bit: Base & Bit Alice (2 bits) | Base Bob (2 bits)| Detection APD 1 & 2 (2 bits).
This data is evaluated using the program „analyser_ qkd.exe. This program determines in real time how many transmissions (absolute and relative in each case) are required.

1. on exactly one APD photon, *’s the same base of Alice and Bob has been chosen,*
2. *the correct bit of Bob was registered.*

The latter is given in relation to the bits transmitted on the same basis and leads to the error rate (*quantum bit error rate*, quantum bit error rate (QBER)) of the transmission. The complete key is compared and is therefore not available for secret communication. Since, however, the attempt focuses on proving the functionality of a key exchange according to BB84, this circumstance poses no problem. As in a real transmission, where only about one third of the key is compared [BB84], 11% can be assumed as a still acceptable upper limit QBER [SP00, p. 444].

TimeHarp

For the autocorrelation measurement of the SPS by means of the Hanbury Brown & Twiss setup, a *TimeHarp* card (TimeHarp200, PicoQuant) is used, which is controlled by an associated program.

Digital-to-Analog Converter

For the EOMs analog signals in the range ±250 V are required. First the digital signal between 0 and 1024 is converted into a voltage in the range ±5 V by means of a digital-to-analog converter (*digital analog converter*, DAC). This signal is then amplified via one driver per EOM to ±250 V. The DAC also has a connector for triggering the laser in pulsed mode and the inputs for the APD signals.

***SmarAct*-Piezo-driver**

The piezo table for positioning the nanodiamonds is controlled by a piezo driver (MCS-3D, SmarAct), which can be connected to the computer via a USB port or operated manually.

5 Executing the Measurements

5.1 performing the measurements using the laser

Commissioning of the Devices and Alignment of the Beam Path

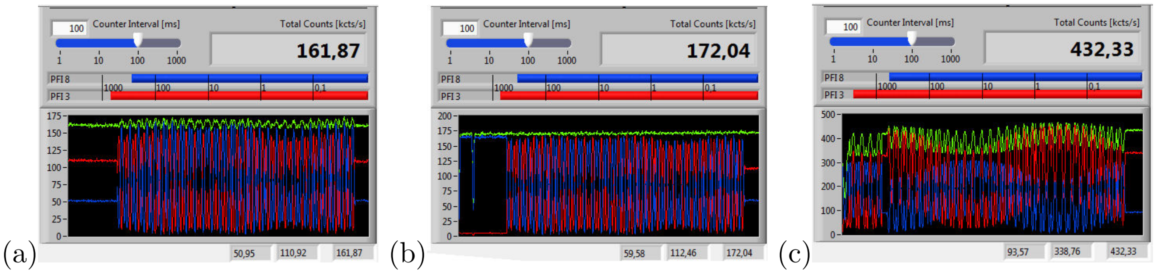
It is recommended to switch on the laser in continuous wave mode for a while before starting the measurements (0,5 to 1 h), as fluctuations in the intensity may occur during the first time, which could otherwise falsify the measurements. In addition to the power supply, a signal must also be present at the trigger input of the laser, which in this case is provided via the DAC. Thus the power supply of the DAC must also be switched on and the *LabView*-program „GUI.vi“ must be started.

Before the actual setup of the transmission setup can be started, the mirrors must be readjusted to ensure that the EOMs is just crossed and the APDs is centered. To facilitate the adjustment, four iris diaphragms have been fixed, which are adjusted one after the other. It is recommended to remove the attenuators, as the laser dot on a screen (e.g. a piece of paper) will be clearly visible to the naked eye. **However, the attenuators must be replaced before switching on the APDs in order to avoid any damage.**

Now the cover can be put on for darkening and the EOM-amplifier and APD-power supply can be switched on. A safety circuit directly on the box prevents the APDs from operating when the lid is open. As a result, a count rate should be registered in the two histograms of „GUI.viänd also in „ScanSoft_ SmarAct_ 2011.vi“ the count rates of the individual APDs should be displayed (see chapter 4.2). **In general, the count rate of each APD must not exceed the value 1000 kcts/s in order not to overload the APDs.**

Checking of Beam Path and linear Polarizer

To ensure that the APDs are hit correctly and the linear polarizer is optimally adjusted, a rough scan of the EOMs (the step size in „GUI.vi“ should be 30 each) and the course of the entire scan should be viewed in the ScanSoft program.


Counter Interval [ms] 100
Total Counts [kcts/s] 161,87

Counter Interval [ms] 100
Total Counts [kcts/s] 172,04

Counter Interval [ms] 100
Total Counts [kcts/s] 432,33

Abbildung 13 – APD signal before and after beam path adjustment.
a) The rough scan over the EOMs shows that the maxima of APD 1 (blue) are consistently higher than those of APD 2 (red). This indicates that APD 2 is not yet centered.
b) After adjusting the beam path, both signals are approximately equal. Their sum is constant within the expected fluctuations.
c) The fluctuations within the maxima and minima of a APD are extremely strong. The linear polarizer should be readjusted in any case.

If the maxima of APD 2 are clearly below those of APD 1 (cf. fig. 13a), the beam path is not yet optimal and must be readjusted (cf. fig. 13b). If the individual minima and maxima of a APD are not at (approximately) the same height during the scan, they must first be readjusted at the linear polarizer, then at the $\frac{\lambda}{2}$ plate. The result should be checked with another scan (see fig. 13c). With only slightly higher maxima on APD 2 the beam path does not have to be readjusted.

Choice of EOM-Voltages for the Bases of Alice and Bob

After this rough EOM-Scan a finer scan (step size for both EOM 10 each) should be done to allow the basic choice for Alice and Bob. This scan takes 12 min. Much longer than the coarse scan (about 1 min), so it should only be done when the beam path and linear polarizer are definitely well adjusted to avoid repetition.

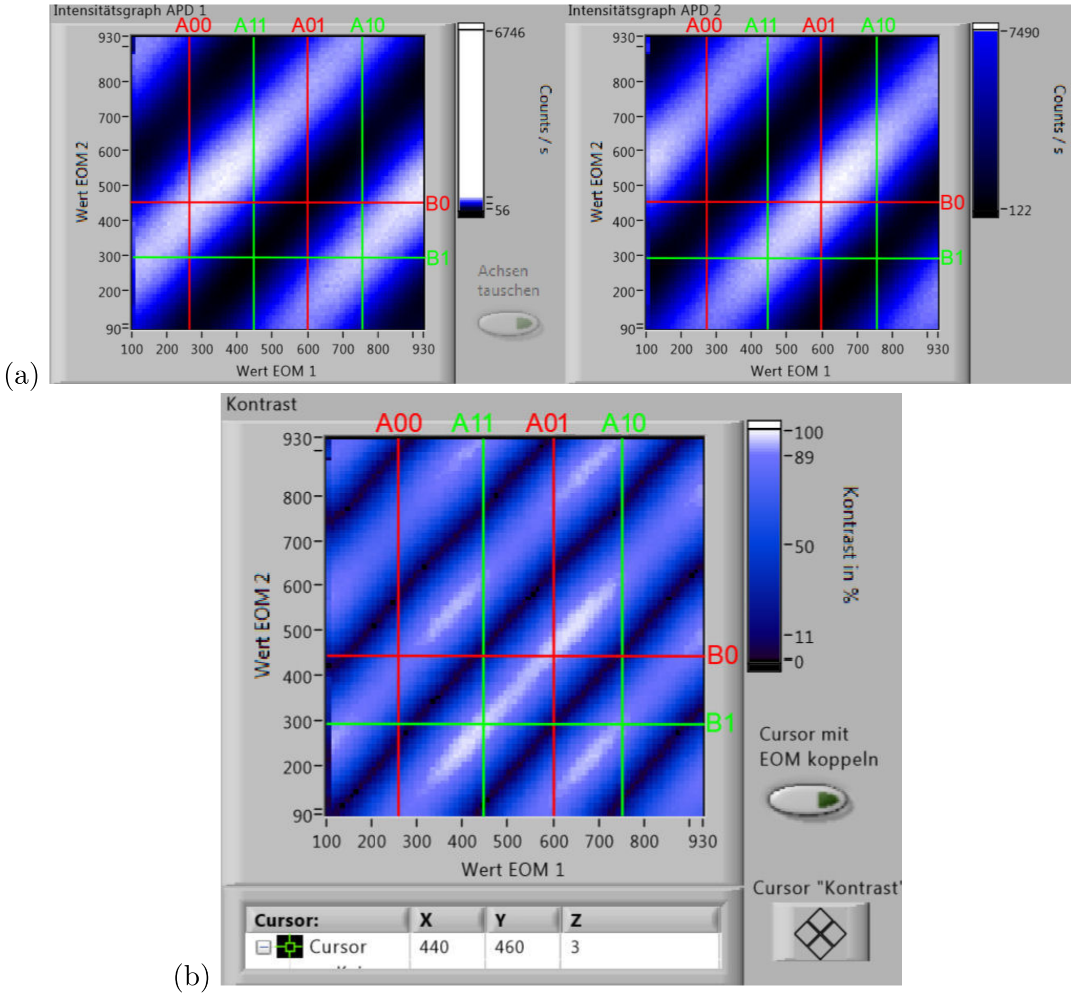
Then the base assignment can be done. In general, the pairs of EOM-voltages in which Alice and Bob use the same base should first be selected and then readjusted for different bases in Alice and Bob so that bits 0 and 1 cannot be distinguished for Bob. Also note that Bob by definition measures bit 0 at APD 1 and bit 1 at APD 2. This assignment should also be considered when selecting the EOM voltages in order to avoid problems in the evaluation.

In concrete terms, the basic selection can be proceeded as follows (see also Fig. 14):

1. Search for two voltage pairs for which the contrast is K (see Chap. 4.2) of APD 1 and APD 2 and assign the bases with corresponding bit (0 if $R_{\text{APD 1}} > R_{\text{APD 2}}$, otherwise 1) (points A01B0 and A11B1 in fig. 14).
2. Display one of the just selected bits of Alice in the wrong base at Bob (e.g. select A01 and B1) and move diagonally until the signals of APD 1 and APD 2 are approximately equal (point A01B1 in fig. 14), then use this value for Alice and Bob. For the other bit (point A11B0 in fig. 14) analog.
3. Now assign the other bit of Alice to both voltages of Bob. To do this, select a position at which the other APD than the first bit of Alice shows a maximum.
4. Those bits should also be displayed in the base by Bob and adjust the value for Alice until both APDs display the same signal.

As a check, both bits can be displayed first for base 0 for Alice and Bob (A00B0 and A01B0), then for base 1 (A10B1 and A11B1) and finally for base 1 for Alice and 0 for Bob (A10B0 and A11B0) and vice versa (A00B1 and A01B1). The achieved count rates of APD 1 and APD 2 should be noted in tabular form for better comparability.

The intensity distribution collected during the scan is automatically stored for both APDs in the file „Scan_ APD1.dat“ (or „...APD2.dat“), the set EOM values, on the other hand, must be stored manually on the computer via the program „GUI.vi.



Cursor:	X	Y	Z
Cursor	440	460	3

Abbildung 14 – EOM scan for base selection with the laser.
You can see the result of a EOM scan. Here the intensity graphs of the APDs (in fig. a) separately from the resulting contrast K (in fig. b). In addition, the EOM-values assigned to Alice and Bob are drawn in red (base 0) and green (base 1) and labeled accordingly („A“ for Alice, „B“ for Bob followed by the values for base and (for Alice) bit.
At the intersection points representing the same base for Alice and Bob (A00B0, A01B0, A10B1 and A11B1), one of the two APD signals is near its maximum count rate (white in the color scale of a), while the other is near its minimum count rate (black in the color scale of a). The intersection points representing different bases of Alice and Bob (A00B1, A01B1, A10B0 and A11B0), on the other hand, have approximately equal count rates for both APD signals (blue in the color scale of a, black in the color scale of b).

Transmission in continuous Wave and pulsed Mode

With the EOM-voltages set via the EOM--values, a key can now be transmitted, whereby the laser can first be operated in continuous wave mode as in the previous steps and then in pulsed mode. This allows both operating modes to be compared with each other. The number of attenuators can also be varied to examine their influence on the transmission. The transfer rate R and the error rate QBER can be determined as parameters of the key transmission, the latter via the program „analyser_ qkd.exe".

5.2 performing the measurements using the SPS

Commissioning the Single-Photon Source and Alignment of the Beam Path

It is recommended to first calibrate all devices with the red laser as described in the previous section before transmitting with the single photon source (SPS), since alignment of the beam path, checking the linear polarizer and scanning the EOM voltages with the higher power of the laser is easier.
After this has been done, the SPS can be coupled into the beam path specified by the red laser. Therefore all attenuators have to be removed from the beam path and the variable mirror has to be placed on a magnetic holder between the laser and the first iris diaphragm. Then open the cover of the single photon source and remove the long pass filters. Now the green excitation laser can be switched on and the piezo driver can be started. Now carefully set the z component of the piezo stage to about 1.000.000 nm (best to go with a step size from 9 to about 900.000 nm first, then decrease the step size bit by bit). **Only move the piezo stage very carefully at the end and never bring it into contact with the lens.**
Readjust until a collimated green light spot is visible on a screen held at the level of the first iris diaphragm in the beam path. This light spot is caused by reflection of the green laser on the surface of the SIL and can be used to adjust the mirrors because the long pass filters have been removed.
For this adjustment the so-called *beam walk* is used as a method, as follows:

1. With the last mirror of the single photon source, direct the beam onto the first iris diaphragm;

2. then open the iris diaphragm wide and aim for the second iris diaphragm by means of the mirror on the magnetic holder, then close the first iris diaphragm again to a large extent;

3. with the first mirror with respect to the first iris diaphragm, since the position has shifted due to the previous step;

4. with the second mirror with respect to the second iris diaphragm, since the position has shifted by the previous step.

Steps 3 and 4 must be repeated alternately until the light path crosses both iris diaphragms in the middle.
If possible (depending on the visibility of the green laser dot), the third iris diaphragm (before the second EOM) can also be located. If the beam path has previously been well aligned with the laser, this is sufficient to hit the APDs in the middle. Finally, the long pass filters are put on again and the cover of the SPS is put on again. During this time: turn off the green laser to avoid eye damage. After closing the box lid, the APDs can be switched on. **The APDs must only be switched on when all filters of the SPS are in the beam path, because the green laser could lead to an overload.** The use of the attenuators is not necessary because the counting rates of the NV-centers are in a range which is not harmful for the APDs.
Although the APDs has been switched on, in most cases they show only a weak signal (about $1 each$ kcts/s), because the position of the piezo stage still has to be readjusted. It is therefore recommended to perform a rough scan of the sample in the xy plane. The center (in the „Center"program) should be $(0\,\mu\text{m}, 0\,\mu\text{m})$, the traverse range (in the SSpan"program) 5 µm, and the step size (in the SStep"program) 1 µm. Then the brightest point (with maximum APD-signal) must be controlled and the APD signal further optimized by adjusting the z-coordinate.

Afterwards, the correct setting of the beam path and linear polarizer should be ensured, which can be done in the same way as with laser transmission (see previous section).
Once these presets have been made, scans of the sample covering a larger area and scans with finer increments can be used to search for NV centers. The following two steps can then be performed for different NV centers:

Choice of EOM Voltages and Transmission

For a transmission, the EOM voltages must now be set correctly. These voltages, however, are mostly the same as those previously used under the laser. Therefore only a short readjustment should be necessary. For both bases of Alice both bits can be displayed in the other base at Bob. Then the value for EOM 1 is changed until the signal of both APD is equal. For each choice of Alice, Bob should note the count rates of both bases in a table. With the voltages readjusted in this way, a key can now be transmitted, where again transmission rate R and error rate QBER should be determined and noted.

Verification of Autocorrelation

To check the autocorrelation, the APDs are separated from the digital-to-analog converter and connected directly to the *TimeHarp* card. Before a measurement the settings „Level“ for the „Sync“-channel and „ZeroCr.“ and „Discr.“ for the „CFD’-channel in the "TimeHarp Control Panel"must be adjusted. The displayed count rate should be similar to that of ScanSoft. If necessary, the EOM voltages must also be readjusted until both channels in the *TimeHarp*- program show about the same number of counts.
To approximate the measured course of the autocorrelation $g^{(2)}(\tau)$ via a fit function, equation (3) from Chap. 3.2 in slightly modified form:

$$f(x) = C_1 \cdot \left(g^{(2)}\left(|x - x_0|\right) + C_0 \right) = C_1 \cdot \left(1 - (K+1)\, e^{k_1|x-x_0|} + K e^{k_2|x-x_0|} + C_0 \right) \tag{7}$$

The constant C_0 indicates the uncorrelated background, because in the measurement the coincidences in the zero point x_0 do not drop to zero. Since this zero point is shifted during the measurement, it is necessary to use the distance $|x-x_0|$ to this point as argument of the $g^{(2)}$- function. The constant C_1 takes into account the fact that the measurement results are unnormalized. This constant can be specified during the adjustment and can be calculated via the count rates R_i at APD i, the temporal resolution t_{bin} and the measurement duration t_{int}, which can be set in the *TimeHarp*- program, using the following formula:

$$C_1 = R_1 \cdot R_2 \cdot t_{bin} \cdot t_{int} \tag{8}$$

The value $g^{(2)}(0)$ can then be calculated as follows using the parameter C_0 determined from the adjustment:

$$g^{(2)}(0) = \frac{C_0}{1 + C_0} \tag{9}$$

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.

Abbreviations

APD avalanche photodiode

ASCII American Standard Code for Information Interchange

BB84 BB84-Protokoll for quantum key exchange

DAC digital analog converter

EOM electro-optic modulator

FPGA field programmable gate array

HBT Hanbury Brown & Twiss Aufbau

HV-base Basis with states $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$

NV nitrogen-vacancy center

OTP One Time Pad

PBS polarising beam splitter

QB Qubit

QBER quantum bit error rate

QKD Quantum Key Distribution

RL-base circular basis with states $|\circlearrowright\rangle$ and $|\circlearrowleft\rangle$

SIL solid immersion lens

SPS single photon source

A Laser safety attachement

The following points to protect the eyes from laser radiation should be considered throughout the experiment. Class 2 lasers with a light output of up to 1 mW are used in the experiment.

- Never keep your head at beam level!
- Remove reflective objects (e.g. watches, jewellery, ...) before starting the test!
- Block the laser beam before replacing optical elements!
- Never handle reflective tools in the beam path!
- Check the beam path before releasing or switching on the laser!
- Note that the polarization beam splitter cube has two outputs!
- The single photon detectors must be closed before room light and may only be used with strongly attenuated laser light!
- Switch on the laser protection lamp during laser operation!
- Pay attention to other persons!

I hereby declare that I have read and understood the points on laser safety listed above. Furthermore, I confirm that I have received an introduction to the use of lasers and an instruction on the laboratory workplace.

____________________ ____________________

Name of advisor Name of experiment performer

____________________ ____________________

place, date sign of experiment performer