Protocols and Components for Quantum Key Distribution

Dissertation

zur Erlangung des akademischen Grades
doctor rerum naturalium
(Dr. rer. nat.)
im Fach Physik
eingereicht an der
Mathematisch-Naturwissenschaftlichen Fakultät der
Humboldt-Universität zu Berlin

von

M. Sc. Matthias Leifgen
geb. am 03.08.1978 in Brühl

Präsident der Humboldt-Universität zu Berlin:
Prof. Dr. Jan-Hendrik Olbertz

Dekan der Mathematisch-Naturwissenschaftlichen Fakultät:
Prof. Dr. Elmar Kulke

Gutachter/innen:
1. .....
2. .....
3. .....

Tag der mündlichen Prüfung: .....

Abstract

Quantum information processing (QIP), which deals with information transmission and processing under the regime of quantum mechanics, offers new and fundamentally groundbreaking resources to the domain of cryptography and computing: the inherent randomness of quantum mechanics as well as superposition states, which have no classical counterpart.

In this thesis, photonic quantum states are used for experimental realisations of two different concepts exploiting these resources. The concept of quantum key distribution (QKD) is revolutionary because it is the only cryptographic scheme offering unconditional security, which means that under demanding but realistic conditions, the information of an eavesdropper can be bounded to be arbitrarily low. Over the last two decades, many different QKD protocols have been investigated both theoretically and experimentally. Two major problems prevail: Firstly, matching the conditions for unconditional security under limited experimental resources is challenging, secondly, long distance communication beyond 200 km is very demanding because for longer distances, an increasingly attenuated quantum state starts to fail the competition with noise, which remains constant.

One experiment accomplished in this thesis is concerned with the first problem. The realisation of the actual quantum state used for transmission is critical. Single photon states from nitrogen and for the first time also silicon vacancy defect centres are used for a QKD transmission under the BB84 (Bennett and Brassard 1984) protocol with polarised photons. The deviation of the used single photon states from the ideal state is thoroughly investigated and the information an eavesdropper obtains due to this deviation is analysed. The QKD setup is very practical and can be used as a testbed for single photon emitters from different defect centres.

Transmitting quantum states via satellites is a potential solution to the limited achievable distances in QKD. A novel protocol particularly suited for this is implemented for the first time in this thesis, the frequency-time (FT) protocol. The protocol is thoroughly investigated by varying the experimental parameters over a wide range and by evaluating the impact on the performance and the security.

Finally, big steps towards a fully automated fibre-based BB84 QKD experiment in the time-bin implementation with autonomous sender and receiver units are accomplished.

Another important concept using quantum mechanical properties as a resource is a quantum random number generator (QRNG). Random numbers are used for various applications in computing and cryptography. Especially QKD itself relies on the usage of good random numbers. A QRNG supplying bits with high and quantifiable randomness at a record-breaking rate is reportetd and the statistical properties of the random output is thoroughly tested.

Zusammenfassung

Die Quanteninformationsverarbeitung, also die Übertragung und Prozessierung von Quantenzuständen, hat das Potential, die Informationstechnik völlig zu verändern.

In dieser Doktorarbeit werden zwei Konzepte der Quanteninformationsverarbeitung mithilfe von photonischen Quantenzuständen realisiert. Das erste Konzept, der Quantenschlüsselaustausch, ist revolutionär, weil es das einzige Kryptografiekonzept ist, welches perfekte Sicherheit gewährleistet. Das heißt in diesem Kontext, dass die Information eines potentiellen Lauschers unter bestimmten Annahmen auf beliebig kleine Werte begrenzt werden kann. Zahlreiche Quantenkryptografieprotokolle wurden schon untersucht. Zwei grundsätzliche Probleme bleiben bestehen. Zum einen ist es sehr schwer, unter begrenzten Ressourcen die Bedingungen herzustellen, die in den Annahmen für perfekte Sicherheit impliziert sind. Zum anderen sind die Reichweiten auf momentan etwa 200 km begrenzt, da irgendwann das abnehmende Signal des Quantenzustands schwächer wird als das konstante Rauschen.

Ein Experiment, welches im Rahmen dieser Doktorarbeit durchgeführt wurde, beschäftigt sich mit dem ersten Problem. Insbesondere die konkrete Realisierung des übertragenen Quantenzustands ist sehr kritisch für die Sicherheit des Verfahrens. Es werden Einzelphotonen von Stickstoff-Fehlstellen-Zentren und zum ersten Mal auch von Silizium-Fehlstellen-Zentren für einen Quantenschlüsselaustausch mit Hilfe des BB84-Protokolls mit polarisierten Photonen benutzt. Die Abweichung der benutzten Zustände von idealen Einzelphotonenzuständen sowie deren Bedeutung für die Sicherheit werden analysiert. Der experimentelle Aufbau kann als Testübertragungsstrecke für Einzelphotonen von verschiedensten Defektzentren benutzt werden.

Die Übertragung von Quantenzuständen via Satellit könnte das Problem der begrenzten Reichweite lösen. Ein neues Protokoll, das Frequenz-Zeit-Protokoll, eignet sich dafür besonders gut. Es wird während dieser Arbeit zum ersten Mal überhaupt implementiert. Umfangreiche Untersuchungen inklusive der Variation wesentlicher experimenteller Parameter geben Aufschluss über die Leistungsfähigkeit und Sicherheit des Protokolls.

Außerdem werden elementare Bestandteile eines vollautomatischen Experiments zum Quantenschlüsselaustausch über Glasfasern in der sogenannten Time-bin-Implementierung mit autonomem Sender und Empfänger realisiert.

Ein anderes wichtiges Konzept der Quanteninformationsverarbeitung ist die Nutzung des Quantenzufalls zur Herstellung zufälliger Bitfolgen. Zufällige Bitfolgen haben zahlreiche Anwendungsgebiete in der Kryptografie und der Informatik. Die Realisierung eines Quantenzufallszahlengenerators mit mathematisch beschreibbarer und getesteter Zufälligkeit und bisher unerreichter Bitrate wird ebenfalls in dieser Doktorarbeit beschrieben.

Contents

1 Introduction

Quantum mechanics started out in the beginning of the 20th century as a theory able to explain intriguing phenomena which could not be explained by classical physics. Back then, no one even dreamed of applications of this theory explaining the behaviour of typically very small systems.

Especially superposition states and entangled states existing in the quantum world brought about the interest of a small community of scientists but did not seem to lead to anything "useful" in the "real world". Quantum information processing (QIP) changed that in a radical manner. Quantum key distribution (QKD) and quantum computing promise solutions to real problems not at hand in the classical world.

QKD, a means to secretly communicate between two distant parties secured by the laws of quantum physics has its roots already in the seventies (although published only in the 80s) of the past century [1]. Once the idea was mature [2], a rapid development on the theoretical and experimental level took place. Nowadays the experimental status is far beyond the first proof-of-principle experiments and first commercialized QKD setups exist. Still, some fundamental limits remain and restrict it from a widespread application, making the ongoing research worthwhile.

First brought about by Feynman [3] and others, e.g. Deutsch [4] in the 80s, a higher interest in quantum computing was only sparkled by the publication of the Shor algorithm [5]. This is an algorithm using qubits (a quantum algorithm) able to factorize large primes much faster than any known classical algorithm. While activities were reinforced over the last 20 years, a fully functional quantum computer still seems out of reach.

The elementary building block of both concepts is the qubit, the quantum mechanical analogue to the classical bit. Starting point is a two level quantum system where each level, represented by the states $|0\rangle$ and $|1\rangle$, respectively, is associated with a bit. These states are vectors in a two-dimensional Hilbert space. Contrary to a classical system, this so called qubit can be in a superposition of the two levels or states:

$$|\Psi\rangle \;=\; \alpha\,|0\rangle + \beta\,|1\rangle \tag{1}$$

with

$$|\alpha|^2 + |\beta|^2 \;=\; 1\,. \tag{2}$$

α and β represent probability amplitudes in form of complex numbers and $|\alpha|^2$

and $|\beta|^2$ are the probabilities of the qubit to be in state $|0\rangle$ and $|1\rangle$, respectively. Qubit states can be visualized by the Bloch sphere, cf. Figure 1.

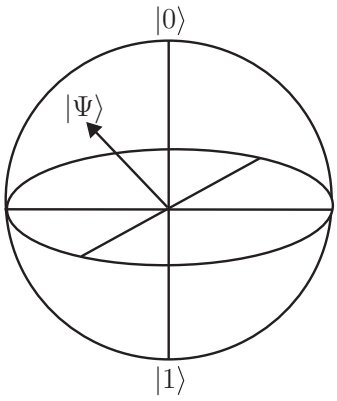


Figure 1: The Bloch sphere. The poles represent the $|0\rangle$ and the $|1\rangle$ state, respectively. All qubit states $|\Psi\rangle$ lie on the surface of the sphere.

The surface of the sphere represents all possible qubit states. A classical bit is represented by one of the two poles. States on the equator are qubits with equal probabilities of being in state $|0\rangle$ or $|1\rangle$, thus they can be written as $|\Psi\rangle = 1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}e^{i\phi}\,|1\rangle$. That is the most widely encountered form of a qubit in quantum information.

A realisation of such a qubit can come in different forms and depends on the application. For quantum computing, stationary qubits are mainly of interest as can be realised for example with the internal states of trapped ions [6]. For QKD, qubits should be transmitted from sender to receiver with as little interaction with the environment as possible. A natural realisation of such a so-called flying qubits is the photon, for example using two orthogonal polarisations to encode a qubit state. That is why efficient single photon generation is of great interest in QIP.

The qubit offers characteristics unknown in the classical world which are used in QKD and quantum computing. In QKD, the impossibility to get better than probabilistic results when not measuring the qubit in the computational basis guarantees that an eavesdropper ignorant of the proper measurement will introduce errors and thus will be perceived. For quantum computing, the probabilistic coexistence of the two classical bits in a single system at the same time enables a sort of parallel computing unknown in the classical world.

This thesis is dedicated to different QKD experiments and related components. QKD has come a long way since its first ideas and implementations. Nowadays it seems to approach its technological limits when it comes to transmission distances

and rates. The major problem is the sensible nature of the quantum system. It is also prone to loss and available detection schemes are noisy.

This thesis concentrates on different aspects of potentially stretching the existing limits. There are different strategies to this: there is an engineer's approach of making existing protocols and components better by using more advanced technology or by simple incremental improvement. At the same time, it is also worthwhile to concentrate on more fundamental research to develop new efficient sources of single photons or to explore new protocols. Both strategies are pursued here.

Before discussing the achievements of this thesis, some introductory chapters precede. In **Chapter 2**, QKD and its basic ideas as well as the state-of-the-art at the moment are introduced.

In **Chapter 3**, basic properties of quantum states of light relevant to this thesis are described.

The BB84 protocol is thoroughly explained in **Chapter 4**. This serves as a basis to understand the QKD experiments presented subsequently.

An efficient single photon source could be an important step towards higher transmission rates and distances. This has been experimentally investigated in this thesis with a QKD implementation using polarised single photons from nitrogen vacancy defect centres and for the first time from silicon vacancy centres in diamonds, cf. **Chapter 5**. The construction of the confocal setup used for the single photon source (SPS) [7] also concentrates on engineering aspects like compactness and practicability.

Another part of this dissertation is concentrated on the rather conceptual approach of implementing a new and practical protocol. The frequency-time (FT) protocol, experimentally realised for the first time, cf. **Chapter 6**, uses frequency and time as non-orthogonal bases to encode qubits. Additionally to having advantages for the implementation and to the robustness of these degrees of freedom in optical fibres, the potential of the FT protocol for satellite QKD and for transmitting several bits at a time makes it very interesting.

In the last part of this dissertation the focus is more on an engineer's approach to existing technologies. In **Chapter 7**, the strategy of implementing a state-of-the-art time-bin encoding scheme is depicted.

Chapter 8 finally reports the joint realisation with the company PicoQuant GmbH of a quantum random number generator (QRNG) with the highest random bit rate at the time using existing high-end timing resolution techniques. This chapter is also an example that quantum technology already found its way to real application.

2 Quantum key distribution

This chapter will introduce the basic ideas of quantum key distribution (QKD). In Section 2.1 existing classical cryptographic schemes will be introduced briefly. Then the basic idea of QKD will be established by means of the BB84 protocol in Section 2.2. After sketching the complete process of QKD beyond the transmission of qubits in Section 2.3, different qubit representations and protocols are discussed in Section 2.4. Section 2.5 deals with QKD with continuous variables. The frequency-time (FT) protocol which has been implemented in this thesis is treated in Section 2.6. QKD with entangled photons is introduced in Section 2.7. Major security threats such as eavesdropping in Section 2.8 or quantum hacking in Section 2.9 are presented then before giving an overview of the state-of-the-art in QKD research at the end of this chapter in Section 2.10.

2.1 From classical to quantum cryptography

There are basically two methods of modern cryptography, namely symmetric-key cryptography and asymmetric- or public-key cryptography [8]. The basic idea of symmetric key cryptography is that the sender and the receiver of a message use the same key to encrypt and decrypt the message. There are two different realisations of this, the stream cipher and the block cipher [8]. The simplest algorithm is the stream cipher, which encodes the message by forming the bitwise exclusive or (XOR) (the bitwise XOR is 1 if the two input bits differ and 0 otherwise) of the message and a random key of same size [8]. Due to its simplicity, the stream cipher is a fast algorithm [8]. One example of the stream cipher which is proven to be absolutely secure [9] is the one-time pad. In the one-time pad, the key is as long as the message, absolutely random and it is used only once. Since this is unpractical with conventional technology (see below), algorithms which work with shorter, cryptographically secure pseudo-random keys are usually used [8]. One widespread implementation of such an algorithm is RC4 [8].

A block cipher is a more sophisticated algorithm which encrypts and decrypts whole blocks of bits of a message in a manner determined by the symmetric key. Usually, several iterations of substitutions and permutations are applied on each block [8]. Typically, all blocks are randomized in a different way before the algorithm is applied to each of them, so that the same key can be used for several blocks of plaintext without compromising security [8]. Known examples of block ciphers are the Data Encryption Standard (DES), using block sizes of 64 bits and key sizes of 56 bits [8], and the Advanced Encryption Standard (AES), using block sizes of 128 bits and key sizes of up to 256 bits [8]. DES was shown to be breakable

in a reasonable amount of time simply by trying all possible keys, due to its short key length [8]. AES is still considered to be secure [8].

The main concern in symmetric-key exchange is to distribute the key secretly to the involved parties. For this, a trusted courier can be used. Also, the actual key can be exchanged using asymmetric key exchange (see below), as for example in the Diffie-Hellman key exchange protocol [8]. QKD for key distribution in combination with the one-time pad offers the highest possible security standard if implemented correctly, as will become clear in the next sections.

Asymmetric-key exchange circumvents the problem of key distribution by using two different keys, one public and one private, which are mathematically linked. If used for encryption, the public key is used to encrypt the message and the private one to decrypt it afterwards [8]. Security is brought about by the complexity of the mathematical link between the two keys. It is easy to create a public key and the corresponding private key, but computationally hard to calculate the private key for a given public key. The used algorithms security is e.g. based on the difficulty of factorization of large integers [8]. Asymmetric key exchange is widely used in Internet communication, for example in Transport Layer Security (TLS) in combination with symmetric keys [8]. A known and widely used algorithm is RSA (after its designers Rivest, Shamir and Adleman) [10, 8]. Asymmetric key exchange can also be used for the distribution of a symmetric key, as mentioned above. This can be of advantage since symmetric encryption is easier and faster [8]. The principle of asymmetric key exchange can not only be used for encryption but also as a digital signature. The main idea is here that a message or a hash of a message can be decrypted by everyone who is in possession of the public key but could have only be encrypted by the holder of the private key. This works because the cryptographic process is absolutely symmetric for both keys, both can be used to either encrypt or decrypt a message [8].

The security of the Internet is nowadays mainly based on asymmetric-key exchange. As already mentioned, the security relies on the fact that it is computationally very hard to calculate the private key from the public key. But this does not mean that it is impossible, unknown attacks able to break this scheme might already exist. And there is an algorithm known as Shor's algorithm, which in conjunction with a quantum computer would make the scheme based on factorization of large integers insecure [11].

2.2 The BB84 protocol

The one-time pad can offer absolute security, the problem is to secretly distribute the key. QKD can solve this problem by encoding the bits of the key into quantum states, the security is then guaranteed by the laws of quantum mechanics. The general scheme combining both ideas is depicted in Figure 2.

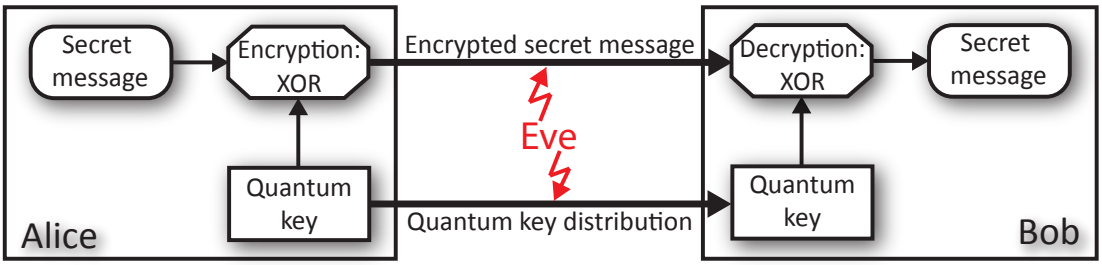


Figure 2: Scheme of the one-time pad in combination with quantum key distribution (QKD). The one-time pad is used for secure transmission of a secret message between Alice and Bob over a classical channel. The key, which is a random bit string of the same length as the message and used only once, is distributed securely guaranteed by the laws of quantum mechanics over the quantum channel. A possible eavesdropper (Eve) could attack both channels, but unsuccessfully.

Starting point is the qubit $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, introduced in Chapter 1. When transmitted from a sender, usually called Alice, to a receiver (Bob), it can be used to communicate secretly. An eavesdropper, typically called Eve, who tries to measure the state of the qubit will inevitably force the qubit to collapse onto either $|0\rangle$ or $|1\rangle$ with the given probabilities. Also, Eve is not able to make an exact copy of the qubit because of the no-cloning theorem [12], which is explained in Appendix A.

Hence, if Alice sends such a general qubit state in form of a photon to Bob via the so-called quantum channel, Eve cannot intercept the state without changing it and cannot copy it either. The complete scheme of the first and most important QKD protocol, the BB84 protocol [2] using polarised single photon states, goes as follows. Two orthogonal states are chosen to represent each a 0 and a 1 in two different bases, for example one in the horizontal-vertical ($|H\rangle$, $|V\rangle$) and one in the diagonal polarisation ($|{+45}\rangle$, $|{-45}\rangle$) basis (cf. Figure 3). Those two bases should have a maximal overlap, i.e. $|\langle{+45}|H\rangle|^2 = |\langle{-45}|H\rangle|^2 = |\langle{+45}|V\rangle|^2 = |\langle{-45}|V\rangle|^2 = \frac{1}{2}$. Alice chooses one of the two bases and then one of the two basis states at random and sends it to Bob. The transmission can be accomplished via optical fibres or through free space. Bob has two measurement instruments, one to measure

the H-V and one for the diagonal basis, and choses one of the two randomly. Each instrument typically consists of a filter device to separate both polarisations, e.g. a polarising beam splitter (PBS), and a single photon detector. If Bob chooses correctly, a deterministic bit measurement is accomplished. If not, the actual state is in the superposition state with $|\alpha|^2 = |\beta|^2 = \frac{1}{2}$ with respect to Bob's basis and the outcome is random. That is why after transmission Alice and Bob agree about photons which were processed in corresponding bases and discard the rest during a process called sifting. The scheme is schematically shown in Figure 3.

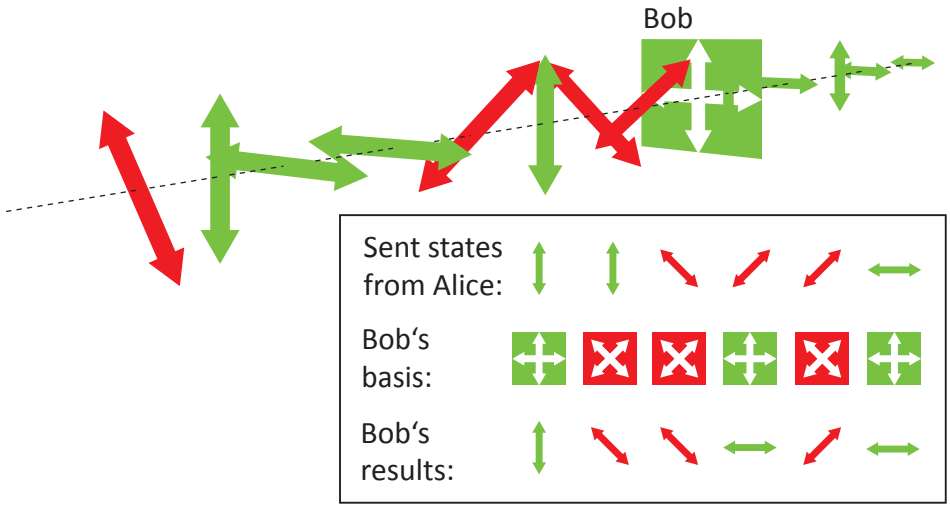


Figure 3: Flying qubits sent by Alice on the way to Bob. Bob measures in the H-V basis and hence all photons are projected on either horizontal or vertical polarisation. Normally, Bob would vary the basis randomly. In the inset, possible results are shown when Alice sends randomly one of four different polarisations states and Bob applies both bases.

If Eve tries to intercept the photon she has to decide for a measurement basis as well. Afterwards, if she resends the state she measures to Bob she will inevitably introduce errors. If she uses the same two bases as Alice and Bob, about half of the time she chooses the incompatible basis. Then, Eve has no information about the bit and the photon she sends to Bob will be projected onto the wrong state about half of the time. If she chooses the right basis, she will get full information and introduce no errors. If Eve intercepts every photon like that, she will thus get half of the information and introduce 25% errors. That is why Alice and Bob publicly compare a statistically relevant part of the transmitted key bits afterwards, which is not used for the key itself but only to estimate the quantum bit error rate (QBER). The QBER is defined as the number of wrongly

transmitted bits over the overall number of transmitted bits and is given in percent. The eavesdropping can be detected by estimation of it and a compromised key would not be used for secret communication. Eve could only attack a ratio of d of the transmitted photons. She will then gain information of $d/2$ of the whole key after sifting and will introduce a QBER of $d/4$. The presented attack is called intercept-resend attack and is just one of many possible attacks, cf. Section 2.8. However, it demonstrates well the principle of security of QKD. The BB84 protocol is described in more detail in Chapter 4.

2.3 The complete quantum key distribution process

The whole process of QKD is more complex than the basic principle explained above. It consists of the following steps [13]:

(1) quantum transmission, when qubits are exchanged between Alice and Bob,

(2) sifting,

(3) error estimation,

(4) error correction and

(5) privacy amplification.

The process of **quantum transmission** has already been explained. The bit string after the quantum transmission is called the raw key. It is important to add that beside the equipment to prepare and measure the degree of freedom of the photon which is used for transmission, Alice and Bob need a good source of randomness for this process. Alice has to choose the bits and the basis randomly and Bob his measurement basis. Inherently random quantum mechanical processes are an ideal source of randomness. QRNGs, i.e. generators of random numbers or bit strings exploiting quantum randomness are thus particularly well suited for this and an obvious choice for QKD. The working principle of QRNGs is explained in Chapter 8.

During **sifting** Bob publicly announces which photons he detected (transmission and detection efficiency are typically $\ll 1$) and in which basis he measured. Alice then tells him which measurements to discard because his basis choice was not corresponding to hers. Alice then also discards these bits as well as those not detected by Bob. In the absence of errors, Alice and Bob both possess the same string of bits now. This string is called the sifted key. During sifting no actual bit information is revealed to a possible eavesdropper. It should be noted that Alice

and Bob need to label their sent and measured bits identically to perform the sifting. For this purpose, typically a synchronisation scheme is applied between them. One such scheme, which has been realised as part of this dissertation is extensively discussed in Section 7.1.2.

The security of QKD relies on the fact that an eavesdropper inevitably introduces errors on the sifted key. That is why the **error estimation** is an essential part of the protocol. During this process, Alice and Bob publicly compare a randomly chosen subset of the sifted key to estimate their QBER. The number of compared bits should be large enough to estimate correctly. At the same time, it should be relatively small with respect to the raw key since these public bits cannot be used for a secret key anymore and have to be discarded. Once the QBER is known, Eve's information on the key can be estimated. How this is done will be explained in Section 2.8 and in Section 4.4. Even though the error can also result from experimental imperfections and not from Eve, all error will be attributed to her presence, as will be discussed in Section 2.8. Depending on her amount of information, the sifted key either has to be discarded or will be further processed. The first step of this so-called post-processing is the error correction.

The **error correction** aims at transforming an error afflicted sifted key into an error free key through public communication but without leaking any information about the concrete value of any single bit to an eavesdropper. This is typically done by comparing parities (parities are the result of XORs of two or more bits) of blocks of bits [14]. The block size is chosen such that there is maximally one error per block with high probability given the estimated QBER. If the parities match, the block is assumed to be error free. Otherwise, the block size is successively reduced until the faulty bit is identified. It can then be flipped or discarded. Several rounds of this process with random block compositions have to be made. The published information about the bits is only of probabilistic nature to Eve and no concrete value of a single bit is communicated. Still, Eve gains knowledge about the key but if the algorithm is efficient she will not learn any more than Bob does, who thus keeps his information advantage. All information Eve might have has to be considered in the following process of privacy amplification.

In **privacy amplification**, Alice and Bob agree on a specific processing of the key in order to lower Eve's knowledge about it down to an arbitrarily small amount. This can be done for example by taking parities of selected bits as constituting bits for a shorter key [13] or by processing the key with a well chosen hash function [15]. This way, Eve's information, which is generally only of probabilistic nature, will be reduced. At the same time, the key is shrunken. It has to be reduced by the supposed amount of information Eve possesses plus a well chosen safety margin [15]. The resulting key is naturally called secure key.

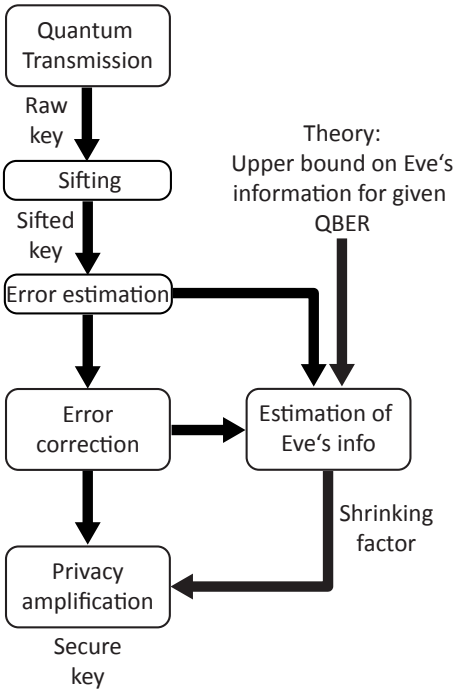


Figure 4: The algorithm of QKD. During quantum transmission, a raw key is generated. In the process of sifting Alice and Bob agree on qubits which were processed in the same basis, the others are discarded. From this results the sifted key, which is about half as long as the raw key. Then Alice and Bob compare a subset of their bits to get an approximation of the QBER. During error correction, additional information might be leaked to Eve. The key then has to be reduced by this information and the maximal information Eve already possesses given the estimated QBER. At the same time it is modified such that Eve has no more information on it. This process is called privacy amplification and results in the secure key.

The complete algorithm of QKD transmission is shown in Figure 4. The post-processing process and Bob's and Eve's resulting information on Alice's key is illustrated in Figure 5.

The whole classical communication process starting from the sifting has to be authenticated to guarantee that Alice and Bob talk to each other and not to Eve who could influence the communication to her advantage (man-in-the-middle attack). This authentication can be implemented by a shared secret, e.g. using a small part of an already transmitted secure key. That means that Alice and Bob have to share an initial secret before their first transmission.

A widely used post-processing protocol is CASCADE [14]. A version of this protocol has been implemented in C++ in the framework of this dissertation in the

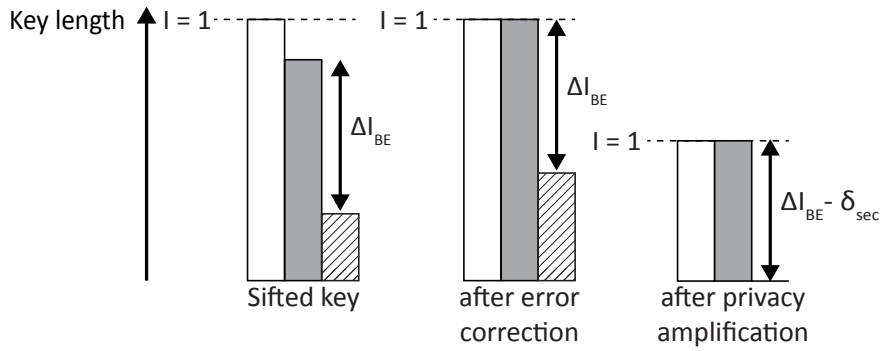


Figure 5: The effect of post-processing on the information of Bob (grey) and Eve (shaded) on Alice's key, shown for comparison in white. After sifting, Bob lacks some information due to the QBER. Also Eve might have learned something about the key during transmission, the difference between her and Bob's knowledge is labeled ΔI_{BE}. After error correction, Alice's and Bob's keys are identical. Eve has gained information as well, but the information gap between her and Bob ideally remains unchanged. After privacy amplification, Alice's and Bob's key shrinks, but Eve will be left without any information about the key. In the shrinking process, additionally to Eve's prior knowledge further bits δ_{sec} have to be sacrificed to create a safety margin.

master thesis of Robert Riemann [175], cf. Section 5.3.

2.4 Other qubit representations

Polarization is not the only photon feature used for encoding. Also, BB84 is not the only QKD protocol. Other implementations of BB84 as well as other QKD protocols will be introduced in the following four sections.

One reason to use other degrees of freedom than polarisation is that it is not very robust in optical fibres which are typically used for transmission. Of course, qubit states can be realised differently. For example, the phase between two possible paths a photon can take can also lead to superposition states. This was first proposed Charles Bennett [16] for a protocol using only two non-orthogonal states. Figure 6 shows a possible setup for a BB84 protocol with phase qubits [13]. With this, a state as described in Equation 1 of Chapter 1 can be produced where the two basis states $|0\rangle$ and $|1\rangle$ represent the two different arms of the interferometer. The coefficients of the equation then contain the coupling ratio of the first coupler, which is a fibre-based equivalent to a beam splitter, as well as the phase difference between the two paths of the interferometer. Thus, the phase difference between path A and B can be measured, just as in classical interferometry. If the phase

difference is 0, the photons end up in output 0, whereas if the phase difference is π the photon ends up in output 1. Alice can set those two phases in her phase modulator (PM Φ_A) to realise the first basis. A second basis can be realised if Bob sets his phase modulator (PM Φ_B) to $\pi/2$ and Alice chooses $\pi/2$ or $3/2\pi$. If the bases of Alice and Bob do not correspond, the output port is random.

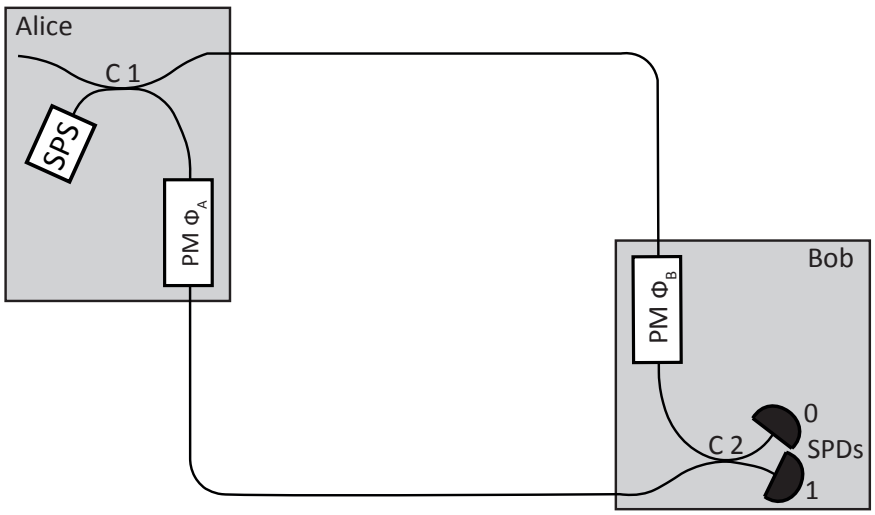


Figure 6: The setup for a BB84 QKD experiment where the information is coded in the phase. The single photon source (SPS) emits photons, which can take two arms of an interferometer. Alice controls the phase Φ_A in one arm through her phase modulator (PM), Bob controls the phase Φ_B in the other arm through his phase modulator. At the two output ports of the interferometer are two single photon detectors (SPDs), which are associated with bit 0 or bit 1.

A practical problem in this scheme is the phase stabilisation between two arms. That is why a similar but more phase stable scheme has been thought of, the time-bin encoding with two unbalanced Mach-Zehnder interferometers [16]. In general, a time-bin qubit refers to a photon which has passed through an unbalanced interferometer and is in a superposition of being in two different time-bins [17], see Figure 7. The basis states of Equation 1 then represent the two possible instances in time the photon could be in, the coefficients contain the coupling ratio of the beam splitters or couplers of the interferometer as well as the phase difference acquired when passing through the different arms. If the coupling ratios can actively be controlled, for example by an optical switch, this time-bin state can be used to realise one basis for the BB84 protocol. But typically, the two bases for BB84 are realised with different phases between the two time-bins, similar as above. These phases can be read out with a second, identical interferometer on Bob's side. This

scheme is introduced in detail in Section 4.2.

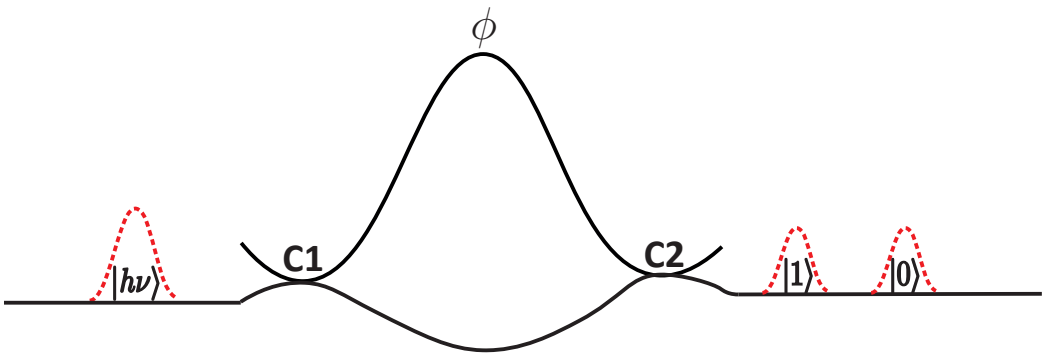


Figure 7: The generation of a time-bin qubit in a fibre-based setup is shown. By splitting up a single photon in an unbalanced interferometer one creates a superposition of two possible instances in time where the photon could be located. The exact form of the created state depends on the transmission and reflection of the two couplers C1 and C2 and the phase ϕ acquired in the interferometer.

There is another class of qubits which belongs to the so-called distributed phase reference protocols, namely the coherent one-way (COW) [18] and the differential phase shift keying (DPSK) [19] protocol, cf. Figure 8. For COW, the information is stored in the position of a nonempty signal pulse within a time bin of two successive pulses, of which one is a vacuum pulse and the other contains a signal with an intensity of $\mu < 1$. In DPSK the information is stored in the phase relation between two successive pulses of the same intensity μ. For both, the security relies on the coherence between all pulses, i.e. in this case the fixed phase relation between them. Basically, if an eavesdropper tries to measure the signal coming from Alice, he will destroy the coherence between the signals. This will be detected, in the case of DPSK directly by erroneous detections after Bob's interferometer. In the case of COW an additional interferometer serves as a second basis to survey the coherence from time to time.

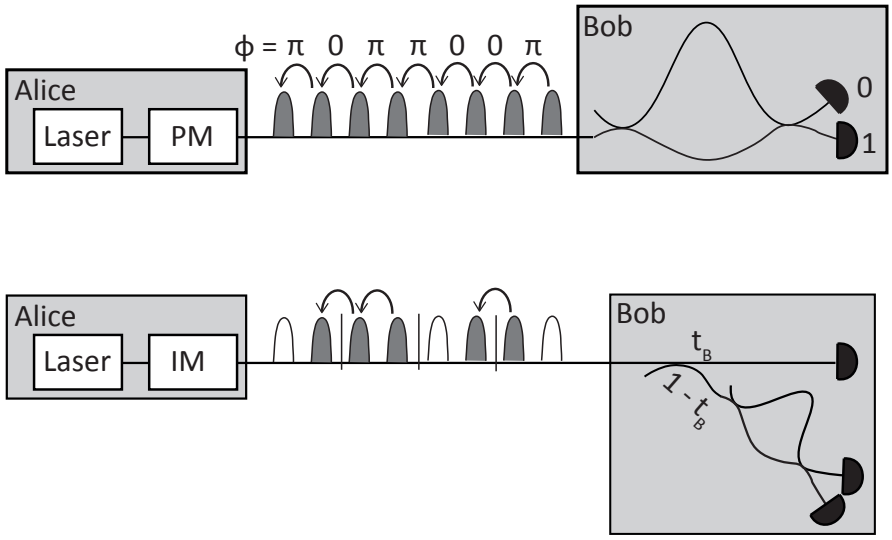


Figure 8: Two distributed phase reference QKD protocols. In the upper figure, the DPSK protocol [19] is depicted. Through the phase modulator (PM), the bit information is coded in the phase relation of different weak coherent pulses emitted by a pulsed laser. The coherence between the pulses, symbolized by the arrows, ensures interference of the pulses in the unbalanced interferometer and guarantees the security as well. An eavesdropper would break the coherence. In the lower figure, the COW protocol [18] is depicted. Here the information is encoded in the position of the nonempty weak coherent pulse within a sequence of two successive pulses of which the other one is a vacuum pulse. The pulses are formed by an intensity modulator (IM) behind a laser. Coherence is monitored from time to time with the help of an unbalanced interferometer coupled to the setup with a coupling ratio $(1 - t_B) \ll 1$. A sequence of two non-empty pulses has to be sent occasionally for reasons of security.

2.5 Continuous variables quantum key distribution

In addition to discrete QKD with qubits, there is continuous variable QKD [20], a scheme where measures generate results on a continuous scale. Typically, in continuous variable QKD the quantum states used are not single photon states and thus can be measured with standard PIN diodes, so that real amplitudes instead of discrete clicks as with single photon detectors are measured. In principle, continuous degrees of freedom instead of discrete ones can be used as well with single photons. But the binary nature of single photon detection, where threshold detectors either just click or not, is the reason that single photon schemes are typically described in a discrete variable picture. Most continuous variable schemes work with quadratures, so in- and out-of-phase components of coherent [21] or

squeezed states [22, 23], cf. Figure 9. The security of those protocols relies on the uncertainty principle. The uncertainty principle describes the fact that simultaneous high precision measurements of some pairs of physical quantities, for example both quadratures, are incompatible in quantum mechanics. Coherent states are minimal uncertainty states with the uncertainty equally distributed in both quadratures, whereas squeezed states have less uncertainty in one quadrature and more in the other [24]. Also, schemes with small variations in the polarisation of macroscopic coherent states exist [25]. There are many different realisations, schemes which encode and measure the information in just one degree of freedom [25] or in both degrees simultaneously [26], schemes with just two possible states and binary coding [25] or schemes which make use of the continuous degree of freedom [21].

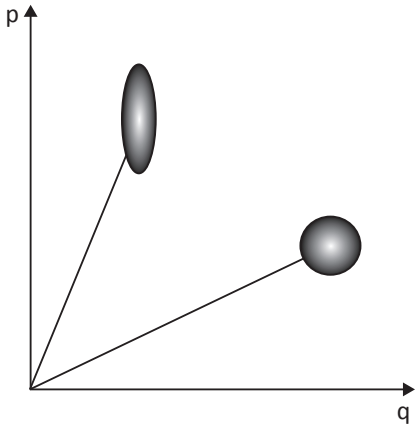


Figure 9: The optical phase or p-q space. Coherent states are characterized by an uncertainty represented by a circular disc. A squeezed state has less uncertainty in one, more in the other dimension.

They all have in common that if Eve tries to make a measurement of the sent states, the noise increases, in analogy to the QBER in single photon QKD schemes. First protocols where limited to transmission losses of less than 3 dB between Alice and Bob. To achieve transmission distances similar to single photon schemes, postselection of suitable measurements [27] or a suitable post-processing [21] (cf. Section 2.3) has to be applied. As mentioned, in principle also single or entangled (cf. below) photons can be used for continuous variables and some protocols have been devised which make use of the possibility of sending more than one bit at a time with single photons [28, 29, 30]. A protocol which can be classified in this domain and also has the potential to be used for a larger alphabet per signal is the FT protocol, introduced in the following.

2.6 The frequency-time protocol

This protocol encodes information in the frequency or arrival time of single photons. It is basically a continuous variables protocol whose security relies on the impossibility of measuring both frequency and time simultaneously due to the uncertainty relation. Time of arrival and frequency of a photon have the advantage that both are robust when transmitted in free space or optical fibres. Also, techniques to generate and measure theses quantities exist and are widely used also in classical telecommunication protocols. This protocol is implemented in this dissertation in analogy to the BB84 protocol, with binary coding and two states each in frequency and time of arrival. The protocol and the implemented experiment are discussed in more detail in Chapter 6.

2.7 Entangled photons

Entangled quantum states and their use for QKD shall also be briefly introduced here. An entangled state is a quantum state of two or more quantum systems which can only be expressed as whole and not as a simple product state of the individual quantum systems. The involved quantum systems can be located far away from each other. One example is the following state, one of the famous Bell states, an entangled state which consists of a pair of photons,

$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle\,|1\rangle - |1\rangle\,|0\rangle)\,. \tag{3}$$

$|0\rangle$ and $|1\rangle$ could for example represent two orthogonal polarisations of the individual photons of the photon pair. Such a state can be used for QKD, as proposed by [31]. Experimental realisations were achieved by several groups simultaneously [32, 33, 34]. It can be sent to Alice and to Bob who measure it in one of two random bases, analog to the BB84 protocol. The trick is that this state will give random but correlated results for both photons in any basis in which the entanglement can be described, as long as both Alice's and Bob's bases are the same. The protocol can be described in analogy to the BB84 protocol and this analogy is in fact paramount to prove the security of BB84, as will be described in 4.4.1.

Entanglement can also be used for continuous variable protocols [23].

2.8 Eavesdropping

As mentioned, eavesdropping causes errors in the sifted key and thus will be detected by Alice and Bob. In order to describe the security quantitatively, it is important to know which could be Eve's most effective eavesdropping strategy, how much information it yields to her and how much QBER it causes at Bob's side. The goal is to prove the security of QKD in a rigorous and mathematical way. This is no easy task, such a proof depends on the specific QKD protocol and its implementation as well as on the assumptions about the power Eve possesses. There are three different classes of attacks which assume different capabilities of Eve. Depending on the class of attacks one supposes, security is more or less easy to prove.

Individual attacks are the simplest kind of attacks. In these attacks, Eve is allowed to have a probe interacting with each transmitted qubit individually. The measurement of her probe can then be delayed until the sifting is conducted. The individual attack has been analysed thoroughly for BB84 and the security against it has been proven, for example in [35]. From a technological point of view, for this attack Eve might need some kind of quantum circuit acting on two qubits for the interaction of probe and qubit and a device to coherently store her probes (quantum memory) until the sifting process [35]. The intuitive intercept-resend attack illustrated in Section 2.2 is a very simple version of an individual attack.

The collective attack is more general. It has been analysed for BB84 and the security against it has been proven [36]. In this attack, Eve also lets interact each probe with each qubit individually. She also stores them in a quantum memory afterwards, but this time she waits until error correction and privacy amplification are over and then makes the optimal measurement giving her the maximum possible information about the final key. This measurement can be a measurement on many qubits at a time, which might be advantageous since also in the post-processing process several bits are combined to form a new key. Thus for this Eve would additionally need quantum circuits acting on an arbitrary number of qubits and thus a veritable quantum computer [4].

The most general attacks allowed by the laws of physics are coherent attacks. In these attacks, Eve's probe can be a n-dimensional quantum object interacting with the n quantum bits interchanged between Alice and Bob coherently. The probe can be stored in a quantum memory until post-processing is finished and can then be processed by Eve in any manner allowed by physics. Security against this most general attack has been proven for BB84 with single photons [37], cf. Section 4.4.1 and also with weak coherent pulse (WCP) [38].

To put these theoretical classifications into perspective, already a practical im-

plementation of some individual attacks seems very difficult given the technology available today [35]. Collective or even coherent attacks seem to be out of reach with today's technology. Nevertheless, it is the correct approach to assume an eavesdropper as powerful as possible if the claim of superior security of QKD should stand firm. That is also why in practical QKD, where QBERs due to experimental imperfections are typically in the order of several percent, this error has to be treated as if being a sign of Eve's presence. An almighty Eve might be able to compensate for imperfect equipment of Alice and Bob and exploit the error margin for eavesdropping.

An important concept in QKD is the notion of unconditional security. It means that security is guaranteed and an upper bound of Eve's information for a given QBER can be calculated for any kind of attack allowed by physics, as long as some supplementary requirements on the implementation are fulfilled [39]:

1. Eve cannot access Alice's and Bob's devices to check their settings.
2. Alice and Bob must trust their random number generators.
3. The classical channel is authenticated with unconditionally secure [8] authentication protocols, e.g. the one proposed by Carter and Wegman [40].
4. Eve is limited by the laws of physics.
5. The exchanged quantum states must match the theoretical description.

BB84 has been proven to be unconditionally secure for ideal SPSs [37] and WCPs [38]. There has also been a prove of unconditional security for distributed phase reference protocols [41]. To the author's knowledge, there are only security proofs against collective attacks for some classes of continuous variable protocols up to date [42, 43].

2.9 Quantum hacking

Despite the proven theoretical security of BB84 and other protocols, there are ways to hack real QKD schemes, meaning that eavesdropping causes only little or no significant error. But this hacking is only possible because the technical implementation is flawed and so at least one requirement of the unconditional security notion is not fulfilled. Two well known attacks on existing commercial QKD systems are described in [44, 45]. The field of quantum hacking is very important. By revealing vulnerabilities of real QKD implementations it advances their security.

2.10 State-of-the-art

QKD is a mature field of research. But to become a real world application up to its potential, unsolved issues remain. The major problem is the limited transmission distance and key rate. The weak quantum signal gets absorbed in optical fibres or through air. In fibres, transmission losses are minimally 0.16 dB/km at an optical wavelength of 1550 nm, cf. for example the supplemental material of [46]. Losses through air minimally amount to around 0.1 dB/km at a wavelength of around 1560 nm and for clear sky [47]. Inefficient and noisy detectors aggravate the problem. Furthermore, optical fibres used for regular Internet transmission cannot be used since this traffic causes excess noise and the frequently used amplifiers destroy the quantum signals.

Several experimental implementations mark the state-of-the-art in QKD in terms of rate, transmission distance and technical maturity. The latest COW implementation achieved a record breaking distance of 307 km over optical fibres with a key rate of approximately 3 bits/s [46]. A time-bin BB84 experiment achieves the highest reported key rates of up to 1.09 Mbit/s over 50 km [48]. A BB84 protocol with polarised photons over 200 km of optical fibre has been achieved at the dispense of using active compensation techniques [49] against the non-constant polarisation transformation in optical fibres. Continuous variables QKD, for which increasing noise at higher distances constitutes a bigger problem for the error correction schemes, has been realised up to a distance of 80 km with a secure key rate of 200 bits/s supposing collective attacks [50].

As mentioned before, there have also been several efforts to increase the capacity of a single photon to transmit more than one bit at a time with the goal of achieving higher key rates [28, 29, 30].

There have been experiments improving the compatibility between classical and quantum communication on a single fibre using wavelength-division multiplexing (WDM) techniques [51, 52].

There are even several commercial fibre-based QKD setups. Two, the ones from ID Quantique [53] and from MagiQ [54], work with the time-bin version of the BB84 protocol. There is one scheme based on continuous variables from SeQureNet [55].

Solutions to the limited transmission distance come from two different approaches. First of all, there is the idea of the quantum repeater [56], proposing to divide large distances into smaller segments. Entanglement transmitted over these segments can then successively be passed on by entanglement swapping [57] until the end points are reached. This interesting scheme still seems out of reach with today's technology. The idea of satellite QKD [58, 59], proposing that distant locations

can be connected via low earth orbit (LEO) satellites in a triangle configuration, seems more realistic at the present day [60]. This scheme benefits from the thinning atmosphere in the upward direction which offers relatively good transmission characteristics. That is why free space QKD, besides of being useful in metropolitan line-of-sight connections, is of great interest. The longest free space transmission distance achieved with polarisation based BB84 is 144 km [61]. There has also been an experiment achieving transmission between a fixed and a moving object, actually a plane [62], which is also interesting in this context.

3 Quantum states of light

In the previous chapter photons have been suggested as ideal transmitters of quantum information. This chapter now introduces some basics of photonic quantum states. At the beginning, in Section 3.1, the quantum theory of light is introduced as well as some basic formalism to describe it. Then the two most important quantum light states used in optical quantum information are introduced, namely Fock states in Section 3.2 and coherent states in Section 3.3. These states can not be fully appreciated without introducing some principal ideas of calculating and measuring statistical properties of light beams in Section 3.4.

3.1 From classical light to photons

Quantum mechanics came about because several experiments could not be described by existing theories. One example for this is the photoelectric effect, which was first observed by Heinrich Hertz in 1887 [63] but not yet understood at that time. It was Einstein in 1905 who gave an explanation to the effect by describing light as consisting of discrete particles which each possess an amount of energy given by its frequency multiplied with a constant [64], thus postulating the existence of photons. Hence, only photons above a certain frequency carry enough energy to release an electron from the metal surface. Another example is blackbody radiation and the prediction of classical physics that it would contain an infinite energy, which is known as the ultraviolet catastrophe. Only Planck's law [65] solved this problem. It required that the oscillators in the wall which in thermal equilibrium equally absorb and emit radiation can only do so in terms of indivisible quanta of energy which depend on the oscillator's frequency. This, together with the introduction of light quanta or photons by Einstein ultimately led to the introduction of quantum theory, which is able to describe this and other quantum phenomena.

When formally introducing photons one must start with the classical Maxwell equations. For a free electromagnetic field in free space with $\mathbf{E}$ describing the

electric and $\mathbf{B}$ the magnetic field they are

$$\begin{aligned} \nabla \cdot \mathbf{E} &= 0\,, & (4)\\ \nabla \cdot \mathbf{B} &= 0\,, & (5)\\ \nabla \times \mathbf{E} &= -\frac{\partial \mathbf{B}}{\partial t}\,, & (6)\\ \nabla \times \mathbf{B} &= \frac{1}{c^2}\frac{\partial \mathbf{E}}{\partial t}\,, & (7)\\ \text{with } c &= \frac{1}{\sqrt{\varepsilon_0 \mu_0}}\,, & (8) \end{aligned}$$

where c is the speed of light in free space, ε_0 is the electric vacuum permittivity and μ_0 the magnetic vacuum permittivity. When applying the curl to 6 and 7, one gets the wave equations for the electric field and magnetic field,

$$\begin{aligned} \nabla^2 \mathbf{E} - \frac{1}{c^2}\frac{\partial^2 \mathbf{E}}{\partial t^2} &= 0\,, & (9)\\ \nabla^2 \mathbf{B} - \frac{1}{c^2}\frac{\partial^2 \mathbf{B}}{\partial t^2} &= 0\,. & (10) \end{aligned}$$

An electric field in a cavity, linearly polarised in x-direction and satisfying Equation 9, when summed over over all possible cavity modes will take the form [66]

$$\mathbf{E}(\mathbf{r}, t) = \mathrm{E}_x(z, t) = \sum_j A_j q_j(t) \sin(k_j \cdot z)\,, \qquad (11)$$

where

$$A_j = \left(\frac{2\omega_j^2\, m_j}{V \varepsilon_0}\right)^2\,, \qquad (12)$$

with m_j being a constant with the dimension of a mass and q_j being an amplitude with the dimension of a length. Both are introduced to visualize the analogy of a single optical mode with that of the harmonic oscillator in the Hamilton mechanics formulation (see below), as in [66]. $\omega_j = j \cdot \pi \cdot c/L$ is the frequency of the cavity mode j, where $j = 1, 2, 3, ...$, $k_j = j \cdot \pi / L$, and V is the mode volume in the cavity. In its general form it is given by $V = \left(\int_{V'} d\mathbf{r} \varepsilon(\mathbf{r}) \left|\mathbf{E}(\mathbf{r})\right|^2\right) / \left(\max\left\{\varepsilon(\mathbf{r}) \left|\mathbf{E}(\mathbf{r})\right|^2\right\}\right)$, where ε is the permittivity and the integral is over all space (V') [67]. Following from Equation 11, the magnetic field has the form

$$\mathbf{B}(\mathbf{r}, t) = \mathrm{B}_y(z, t) = \sum_j \mu_0 A_j \left(\frac{\dot{q}_j(t)\, \varepsilon_0}{k_j}\right) \cos(k_j \cdot z)\,. \qquad (13)$$

Writing down the classical Hamiltonian of the field in the present form calculated for the volume of the cavity, one gets

$$\mathcal{H} = \frac{1}{2}\int_V \left(\varepsilon_0 \mathbf{E}_x^2 + \frac{1}{\mu_0}\mathbf{B}_y^2\right) dV\,. \tag{14}$$

Substituting the expressions 11 and 13 for $\mathbf{E}_x$ and $\mathbf{B}_y$, respectively, Equation 14 becomes

$$\mathcal{H} = \frac{1}{2}\sum_j \left(m_j\omega_j q_j + m_j\dot{q}^2\right) \tag{15}$$

$$= \frac{1}{2}\sum_j \left(m_j\omega_j q_j + \frac{p_j^2}{m_j}\right)\,, \tag{16}$$

with the momentum $p_j = m_j\dot{q}_j$. This shows the equivalence to the Hamiltonian for different modes of the harmonic oscillator. The quantization of functions in the Hamilton mechanics formulation is accomplished by replacing the observables with quantum mechanical operators. In this way, a single optical mode, which is a associated with a single mode of an harmonic oscillator is quantized in complete analogy to it by associating the variables q_j and p_j with the quantum mechanical operators $\hat{q}_j$ and $\hat{p}_j$. A fundamental difference between classical and quantum mechanics is the fact that many operators do not commute. This is expressed by the commutator relations, which are for $\hat{q}_j$ and $\hat{p}_j$

$$[\hat{q}_i, \hat{p}_j] = \hat{q}_i\hat{p}_j - \hat{p}_j\hat{q}_i = i\hbar\delta_{ij}\,, \tag{17}$$

$$[\hat{q}_i, \hat{q}_j] = 0\,, \tag{18}$$

$$[\hat{p}_i, \hat{p}_j] = 0\,. \tag{19}$$

It is useful to replace the operators $\hat{q}_j$ and $\hat{p}_j$ with the annihilation and creation operators $\hat{a}_j$ and $\hat{a}_j^\dagger$, whose meaning will become apparent soon,

$$\hat{q}_j = \sqrt{\frac{\hbar}{2m\omega_j}}(\hat{a}_j^\dagger + \hat{a}_j)\,, \tag{20}$$

$$\hat{p}_j = i\sqrt{\frac{m\hbar\omega_j}{2}}(\hat{a}_j^\dagger - \hat{a}_j)\,. \tag{21}$$

With these the quantum mechanical Hamilton operator becomes

$$\hat{\mathcal{H}} = \hbar\sum_j \omega_j \left(\hat{a}_j^\dagger\hat{a}_j + \frac{1}{2}\right)\,. \tag{22}$$

The annihilation and creation operators obey the commutator relations

$$[\hat{a}_i, \hat{a}_j^\dagger] = \delta_{ij}\,, \tag{23}$$
$$[\hat{a}_i, \hat{a}_j] = 0\,, \tag{24}$$
$$[\hat{a}_i^\dagger, \hat{a}_j^\dagger] = 0\,. \tag{25}$$

With these operators, the electric and magnetic fields take the form

$$\mathrm{E}_x(z,t) = \sum_j \xi_j \left(\hat{a}_j e^{-i\omega_j t} + \hat{a}_j^\dagger e^{i\omega_j t}\right) sin(k_j \cdot z)\,, \tag{26}$$
$$\mathrm{B}_y(z,t) = -i\mu_0\varepsilon_0 c \sum_j \xi_j \left(\hat{a}_j e^{-i\omega_j t} - \hat{a}_j^\dagger e^{i\omega_j t}\right) cos(k_j \cdot z)\,, \tag{27}$$
$$\text{with } \xi_j = \sqrt{\left(\frac{\hbar\omega_j}{\varepsilon_0 V}\right)}\,, \tag{28}$$

which has the dimensions of an electric field. This result can be generalized to a field in free space in which case the volume V represents a volume for which periodic boundary conditions are established [66],

$$\mathbf{E}(\mathbf{r},t) = \sum_{\mathbf{k}} \epsilon_{\mathbf{k}} \xi_{\mathbf{k}} \hat{a}_{\mathbf{k}} e^{-i(\omega_{\mathbf{k}} t - \mathbf{k}\cdot\mathbf{r})} + H.c.\,, \tag{29}$$
$$\mathbf{B}(\mathbf{r},t) = \sum_{\mathbf{k}} \frac{\mathbf{k}\times\epsilon_{\mathbf{k}}}{\omega_{\mathbf{k}}} \xi_{\mathbf{k}} \hat{a}_{\mathbf{k}} e^{-i(\omega_{\mathbf{k}} t - \mathbf{k}\cdot\mathbf{r})} + H.c.\,, \tag{30}$$

where $\epsilon_{\mathbf{k}}$ is an unit polarisation and *H.c.* stands for Hermitian conjugate.

3.2 Fock states

To introduce Fock states, only a single mode of the optical field will be considered for simplicity and without loss of insight, the index j will thus be omitted in what follows. It is useful to introduce the eigenvectors $|n\rangle$ to the Hamilton operator $\hat{\mathcal{H}}$ together with the corresponding eigenvalues E_n,

$$\hat{\mathcal{H}}\,|n\rangle = \hbar\omega \left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)|n\rangle = E_n\,|n\rangle\ . \tag{31}$$

$\hat{a}^\dagger\hat{a}$ can be expressed by the number operator $\hat{n} = \hat{a}^\dagger\hat{a}$, which has the eigenvalue equation [66]

$$\hat{n}\,|n\rangle = n\,|n\rangle \tag{32}$$

and thus the corresponding energy eigenvalue of $|n\rangle$,

$$E_n = \left(n + \frac{1}{2}\right)\hbar\omega\,. \tag{33}$$

It can also be shown that

$$\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle\ , \tag{34}$$
$$\hat{a}^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle\ . \tag{35}$$

It is now very intuitive that the state $|n\rangle$ represents a light mode consisting of exactly n photons of frequency ω, each carrying an energy of $\hbar\omega$. These states are called photon-number or Fock states.

Fock states have the following characteristics. First of all, they form a complete set of states, i.e

$$\sum_n^\infty |n\rangle\langle n| = 1\,. \tag{36}$$

They form an orthonormal basis,

$$\langle n|m\rangle = \delta_{nm}\,. \tag{37}$$

An arbitrary state can thus be represented by Fock states,

$$|\psi\rangle = \sum_n c_n\,|n\rangle\ , \tag{38}$$

with

$$c_n = \langle n|\psi\rangle\ . \tag{39}$$

Arbitrary Fock states can be created by repeated application of the creation operator on the vacuum state,

$$|n\rangle = \frac{\left(\hat{a}^\dagger\right)^n}{\sqrt{n!}}\,|0\rangle\ . \tag{40}$$

The mean photon number or expected value of a state $|n\rangle$ is naturally

$$\langle n\rangle = \langle n|\hat{n}|n\rangle = n\,. \tag{41}$$

The variance is

$$(\Delta n)^2 = \left\langle n|\hat{n}^2|n\right\rangle - \langle n|\hat{n}|n\rangle^2 = 0\,. \tag{42}$$

Of particular interest in quantum optics is of course the single photon state $|1\rangle$, produced by a single photon source (SPS).

3.3 Coherent states

For the introduction of coherent states only single mode optical fields will be considered as well.

Coherent states are eigenstates of the annihilation operator,

$$\hat{a}\,|\alpha\rangle \;=\; \alpha\,|\alpha\rangle\;, \tag{43}$$

with α being a complex amplitude. Calculating the mean photon number with the number operator $\hat{n}$, one gets

$$\langle n\rangle = \left\langle \alpha\left|\hat{a}^\dagger\hat{a}\right|\alpha\right\rangle = |\alpha|^2\;. \tag{44}$$

Using Equations 40, 43, the orthogonality of the Fock states and requiring $|\alpha\rangle$ to be normalized, the representation of coherent states in the Fock state basis looks as

$$|\alpha\rangle \;=\; e^{-\frac{|\alpha|^2}{2}}\sum_n \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\;. \tag{45}$$

The probability p_n to find n photons in the coherent state $|\alpha\rangle$ is

$$p_n = |\langle n|\alpha\rangle|^2 = e^{-\langle n\rangle}\frac{\langle n\rangle^n}{n!}\,. \tag{46}$$

This is a Poissonian distribution. Figure 10 shows the photon number distribution for coherent states and for comparison for a Fock state.

The variance of a coherent state is

$$(\Delta n)^2 = \langle n\rangle = |\alpha|^2\;, \tag{47}$$

as can be easily shown by properly rearranging the creation and annihilation operators [24].

Coherent states are important in quantum optics because they are the best approximation to classical light states, for example the states generated by lasers. Weak coherent pulses (WCPs) are used to approximate single photon states in many experiments, despite their fundamentally different statistical features, as will be discussed in the next section.

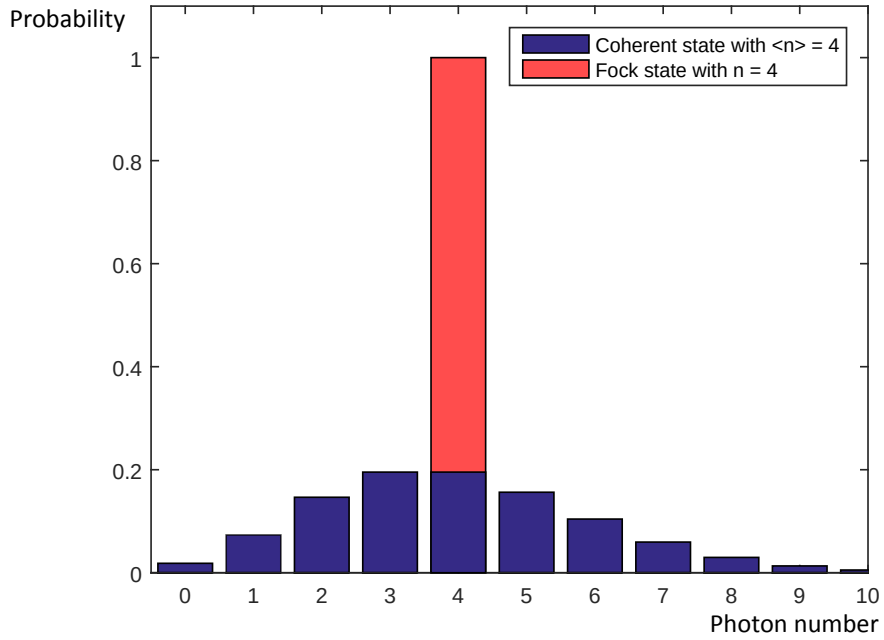


Figure 10: The probabilities for coherent and Fock states to contain a certain amount of photons are shown. Both have a mean photon number of $\langle n \rangle = 4$. Whereas the photon number of the Fock state is determined, the coherent states' photon number obeys a Poissonian distribution.

3.4 Characterizing light sources

3.4.1 Autocorrelation functions

Now the field and intensity correlation functions of a single light beam are introduced, the autocorrelation functions. Starting point are the classical expressions, then a transition to the quantum mechanical expressions is made. They have an important meaning in interference experiments. In addition, the quantum mechanical intensity autocorrelation function leads to expressions which enable to fully appreciate the nature of non-classical light sources such as single photon source (SPS).

3.4.1.1 Spectral properties of light - the degree of first order coherence

The degree of first order coherence is a normalized version of the first-order auto-correlation function and is for a plane wave light beam [24]

$$g^{(1)}\left(z_1,t_1;z_2,t_2\right) \;=\; \frac{\left\langle E^{*}\left(z_1,t_1\right)E\left(z_2,t_2\right)\right\rangle}{\left[\left\langle\left|E\left(z_1,t_1\right)\right|^2\right\rangle\left\langle\left|E\left(z_2,t_2\right)\right|^2\right\rangle\right]^{1/2}}\,, \tag{48}$$

with $E(z_i,t_i)$ being the complex field amplitude of the light beam at point z_i and time t_i and the $\langle\rangle$ brackets stand for the average over a time much longer than one period of oscillation of the light. This function relates the field of a single plane wave light beam at two different points in space z_1 and z_2 and at two different instances in time t_1 and t_2. The degree of first order coherence plays a role in interference experiments such as in a Mach-Zehnder interferometer, cf. Figure 11.

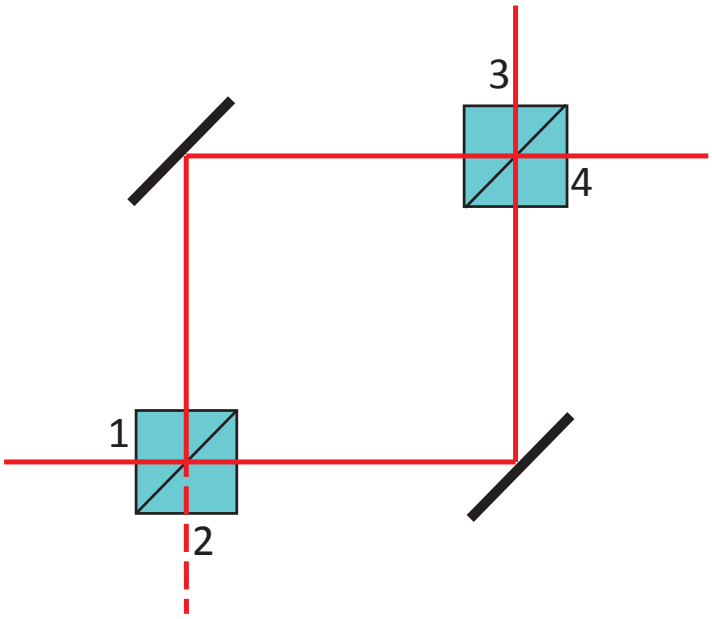


Figure 11: The scheme of a Mach-Zehnder interferometer. Light from input 1 or input 2 is split by a beam splitter (BS). The light then is reunited on a second BS where it interferes, which affects the intensities at output 3 and 4

Looking at the averaged intensity at output 4 for an incoming light beam at output 1, one gets the expression [24]

$$\bar{I}_4(t) \;=\; \frac{1}{2}\varepsilon_0 c\left|\mathcal{R}\right|^2\left|\mathcal{T}\right|^2\left\{\left\langle\left|E(t_1)\right|^2\right\rangle+\left\langle\left|E(t_2)\right|^2\right\rangle+2\Re\left[E^{\star}(t_1)E(t_2)\right]\right\}\,, \tag{49}$$

where $\bar{I}$ is the averaged intensity over one period of field oscillation, $\mathcal{T}$ and $\mathcal{R}$ are the transmission and reflection coefficient of the involved beam splitters and t_1 and t_2 are the acquired delays of the light traveling through the two different arms. If the light is stationary, meaning that its statistical characteristics over time do not change, one can drop the indices 1 and 2 marking specific instances in time and only $\tau = t_2 - t_1$ is relevant. With this, expression Equation 49 can be written as [24]

$$\begin{aligned} \left\langle \bar{I}_4(t) \right\rangle &= 2\left|\mathcal{R}\right|^2\left|\mathcal{T}\right|^2\left\langle \bar{I}(t)\right\rangle\left\{1+\Re\left[g^{(1)}(\tau)\right]\right\} && (50)\\ &= 2\left|\mathcal{R}\right|^2\left|\mathcal{T}\right|^2\left\langle \bar{I}(t)\right\rangle\left\{1+\left|g^{(1)}(\tau)\right|\cos\left(\arg\left[g^{(1)}(\tau)\right]\right)\right\} && (51)\\ &= 2\left|\mathcal{R}\right|^2\left|\mathcal{T}\right|^2\left\langle \bar{I}(t)\right\rangle\left\{1+\left|g^{(1)}(\tau)\right|\cos\,\varphi\right\}\,, && (52)\\ \text{with } \left\langle \bar{I}(t)\right\rangle &= \frac{1}{2}\varepsilon_0 c\left\langle\left|E(t)\right|^2\right\rangle\,. && (53) \end{aligned}$$

Here $g^{(1)}(\tau)$ is a simplified version of Equation 48 for stationary light and the intensity measured at a single point. $\Re[g^{(1)}(\tau)]$ is the term introducing the interference effects. The absolute value of the $g^{(1)}(\tau)$ function depends on the spectral properties of the light beam and can be used to define its coherence time $\tau_c = \int_{-\infty}^{\infty}\left|g^{(1)}(\tau)\right|^2 d\tau$. It can also be used to calculate the normalized spectral distribution function by use of the Wiener-Khintchine theorem [24],

$$F(\omega) = \frac{1}{\pi}\Re\left[\int_0^\infty g^{(1)}(\tau)e^{i\omega\tau}d\tau\right]\,. \qquad (54)$$

$g^{(1)}(0)$ is always 1. Light is said to be first-order coherent if $|g^{(1)}(\tau)| = 1$ for all τ.

In this context it is interesting to introduce the visibility V, which is a measure of the contrast in interference experiments when observing interference fringes [66], for example by slightly varying the path length difference in the interferometer of Figure 11,

$$V = \frac{\langle I\rangle_{max} - \langle I\rangle_{min}}{\langle I\rangle_{max} + \langle I\rangle_{min}}\,, \qquad (55)$$

where $\langle I\rangle_{max}$ and $\langle I\rangle_{min}$ are the maximal and minimal observed intensities when slightly varying the path length difference around a temporal difference of τ. Looking at Equation 52 one can appreciate that the maximal and minimal intensities result when the cosine equals $+1$ and -1 and V can actually be expressed as

$$V = \left|g^{(1)}(\tau)\right|\,. \qquad (56)$$

As pointed out, the degree of first order coherence gives information about the spectral properties of a light beam. Very often in quantum optics one is interested in the statistical properties of the intensity of a light source, which can be identified by measuring the degree of second order coherence. Particularly the characteristics of a SPS can only be appreciated like that.

3.4.1.2 Intensity fluctuations of light - the degree of second order coherence

The degree of second order coherence is the normalized second order autocorrelation function, for plane polarised parallel beams it is [24]

$$g^{(2)}(z_1,t_1;z_2,t_2) = \frac{\langle E^*(z_1,t_1)\,E^*(z_2,t_2)\,E(z_2,t_2)\,E(z_1,t_1)\rangle}{\left\langle |E(z_1,t_1)|^2\right\rangle \left\langle |E(z_2,t_2)|^2\right\rangle}. \tag{57}$$

If the light is stationary and if the degree of second order coherence is evaluated at a single point in space, only the relative difference in time $\tau = t_2 - t_1$ matters. With this Equation 57 becomes

$$g^{(2)}(\tau) = \frac{\langle E^*(t)\,E^*(t+\tau)\,E(t+\tau)\,E(t)\rangle}{\langle E^*(t)\,E(t)\rangle^2}, \tag{58}$$

where $\tau = t_2 - t_1$. If the light beam is classical, inequalities describing the properties of $g^{(2)}(\tau)$ at different τ can be established [24],

$$1 \leq g^{(2)}(0) \leq \infty, \tag{59}$$

$$0 \leq g^{(2)}(\tau) \leq \infty \quad \tau \neq 0, \tag{60}$$

$$g^{(2)}(\tau) \leq g^{(2)}(0). \tag{61}$$

Inequality 61 means that for classical light, $g^{(2)}(0)$ can never be smaller than $g^{(2)}(\tau)$ for $\tau \neq 0$. This is not true for some fields which are described by quantum mechanics, as will be seen below. Two different kinds of classical light sources are interesting in this context. A stable electromagnetic wave of monochromatic light, meaning that no amplitude or phase fluctuations are present and the τ_c is infinitely long, gives a $g^{(2)}(\tau) = 1$ for all τ. A thermal light source can be shown to have a $g^{(2)}(0) = 2$ and a $g^{(2)}(\tau) \to 1$ for $\tau \gg \tau_c$.

3.4.1.3 Quantum mechanical degrees of coherence

In order to evaluate the degrees of coherence for quantum fields, quantum mechanical operators are used instead of the classical complex field amplitudes,

$$g^{(1)}\left(z_1,t_1;z_2,t_2\right) = \frac{\left\langle \hat{E}^-\left(z_1,t_1\right)\hat{E}^+\left(z_2,t_2\right)\right\rangle}{\left[\left\langle \hat{E}^-\left(z_1,t_1\right)\hat{E}^+\left(z_1,t_1\right)\right\rangle\left\langle \hat{E}^-\left(z_2,t_2\right)\hat{E}^+\left(z_2,t_2\right)\right\rangle\right]^{1/2}} \tag{62}$$

for plane parallel beams. If a stationary field is observed at a single point in space, then

$$g^{(1)}\left(\tau\right) = \frac{\left\langle \hat{E}^-\left(t\right)\hat{E}^+\left(t+\tau\right)\right\rangle}{\left\langle \hat{E}^-\left(t\right)\hat{E}^+\left(t\right)\right\rangle}. \tag{63}$$

$\hat{E}^-\left(z,t\right)$ and $\hat{E}^+\left(z,t\right)$, respectively, denote the negative or positive frequency part of the electric field operator of Equation 26 or more generally of Equation 29 which contain the creation and annihilation operators, respectively. Differently to the classical expressions, the quantum mechanical operators do not generally commute. The order in which they appear here, with annihilation operators lying to the right of creation operators, is the so-called normal ordering. It is important to use this normal ordering to account for measured intensities [24].

A quantum mechanical treatment does not give any different results for $g^{(1)}(\tau)$ than a classical one. For the second order coherence and a plane parallel light beam the quantum mechanical version is

$$g^{(2)}\left(z_1,t_1;z_2,t_2\right) = \frac{\left\langle \hat{E}^-\left(z_1,t_1\right)\hat{E}^-\left(z_2,t_2\right)\hat{E}^+\left(z_2,t_2\right)\hat{E}^+\left(z_1,t_1\right)\right\rangle}{\left\langle \hat{E}^-\left(z_1,t_1\right)\hat{E}^+\left(z_1,t_1\right)\right\rangle\left\langle \hat{E}^-\left(z_2,t_2\right)\hat{E}^+\left(z_2,t_2\right)\right\rangle} \tag{64}$$

and

$$g^{(2)}\left(\tau\right) = \frac{\left\langle \hat{E}^-\left(t\right)\hat{E}^-\left(t+\tau\right)\hat{E}^+\left(t+\tau\right)\hat{E}^+\left(t\right)\right\rangle}{\left\langle \hat{E}^-\left(t\right)\hat{E}^+\left(t\right)\right\rangle^2}, \tag{65}$$

respectively. If a single mode light beam is considered, $g^{(2)}(\tau)$ becomes a time-

independent function [24],

$$g^{(2)}(\tau) = \frac{\left\langle \hat{a}^\dagger \hat{a}^\dagger \hat{a}\hat{a} \right\rangle}{\left\langle \hat{a}^\dagger \hat{a} \right\rangle^2} \tag{66}$$

$$= 1 + \frac{(\Delta n)^2 - \langle n \rangle}{\langle n \rangle^2}. \tag{67}$$

For Fock states this results together with Equation 41 and Equation 42 in

$$g^{(2)}(\tau) = 1 - \frac{1}{n}. \tag{68}$$

This is a surprising result, since it clearly violates that $g^{(2)}(0) \geq 1$ (see Equation 59) for $n \ll \infty$. This result can only be achieved by fields which can exclusively be described by quantum mechanics. It has been confirmed experimentally many times. Light having the second order temporal degree of coherence < 1 at $\tau = 0$ has sub-Poissonian statistics. For a coherent state Equation 67 results in $g^{(2)}(\tau) = 1 = g^{(2)}(0)$. This coincides with the classical result of a stable monochromatic wave, which is thus very well approximated by coherent light. Light beams with $g^{(2)}(\tau) = 1$ are called Poissonian.

If more realistic multimode coherent or Fock states are treated, the results are the same. Additionally, thermal light treated this way gives results like in the classical case, with $g^{(2)}(0) = 2$ and $g^{(2)}(\tau) = 1$ for $\tau \gg \tau_c$. Light with a $g^{(2)}(\tau) > 1$ is called super-Poissonian.

There is no time dependence of $g^{(2)}(\tau)$ in Equation 68. If the light described by a Fock state is described more rigorously with respect to its source, for example when describing fluorescence from a two-level system in a good approximation to an actual SPS, a time dependence of $g^{(2)}(\tau)$ is found. This gives rise to another phenomenon only observed in the quantum world, which is antibunching [24]. Antibunching takes place when $g^{(2)}(0) < g^{(2)}(\tau)$. It expresses the fact that photons from such a light source are less likely to be emitted at the same time than at different times, which is naturally the signature of a single photon source. Thermal sources are more likely to emit more than one photons at a time, this is called bunching. The emission of photons from a coherent light source is completely random without any time correlation. These characteristics are illustrated in Figure 12 for different light sources.

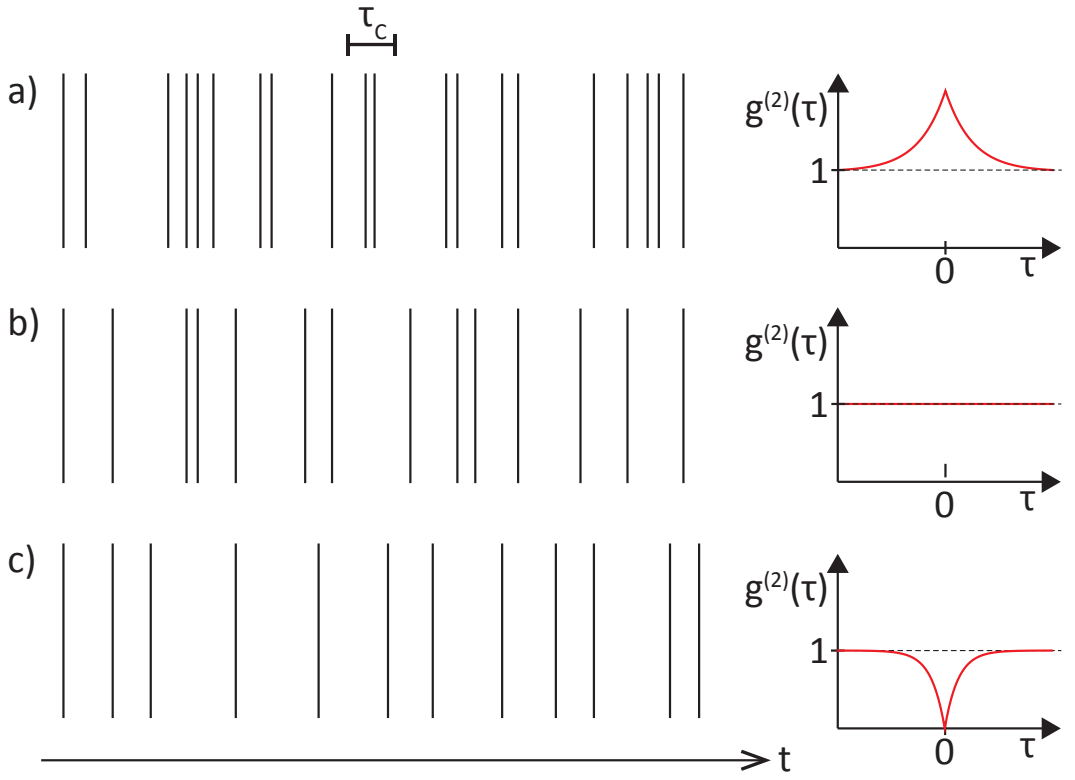


Figure 12: To the left: representation of the time-series of photocounts for a) a thermal light source with bunching, b) a coherent light source with Poissonian distributed photon emission and c) an anti-bunched light source as for example a single photon source (SPS). To the right, the corresponding $g^{(2)}(\tau)$ are shown.

Single photon sources (SPSs) have two statistical properties only explainable by a quantum mechanical description: they have a sub-Poissonian statistics and they show antibunching. Both . Often, these two characteristics of a light source are observed at the same time, but this does not have to be the case [68].

3.4.2 The Hanburry Brown and Twiss effect

It was shown how the first order degree of coherence is connected to the visibility in an interferometer. However it has not yet been explained how the second order degree of coherence is actually measured. The measurement setup is actually simple, as shown in Figure 13.

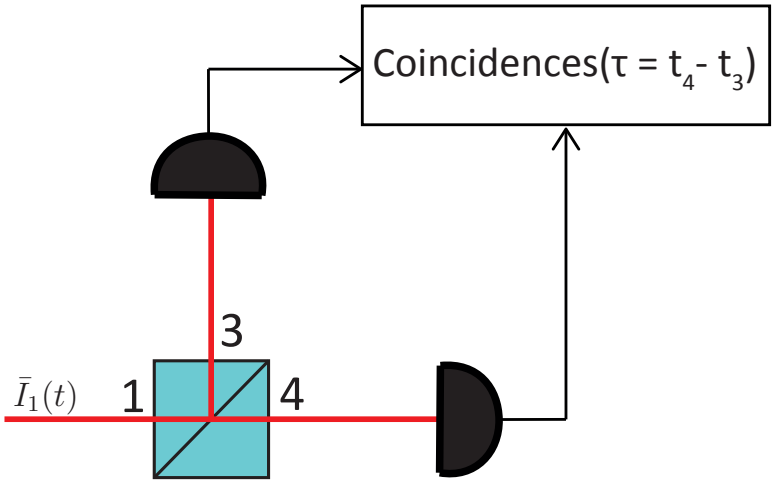


Figure 13: The typical setup to measure the Hanbury Brown and Twiss (HBT) effect. An incoming beam is equally divided by a 50/50 beam splitter (BS) before each output is measured by a detector. The detector signals are analysed in a coincidence counter. The result can be used to calculate $g^{(2)}(\tau)$.

The light beam to be measured is simply divided into two equal beams by a 50/50 BS. The light beam is then measured with two single photon detectors which output a stream of clicks proportional to the number of impinging photons. The coincidences between the two detectors at time intervals of synchronous detections are counted by an electronic coincidence counter. The recorded signal can be converted into a histogram of time differences between correlated detections which is directly proportional to $g^{(2)}(\tau)$ and only has to be normalized. Theoretically only a single detector without a beam splitter would suffice to make this measurement, as was shown also experimentally in [69]. The setup with a beam splitter and two detectors is necessary when trying to measure beams with only few photons because detectors sensitive to single photons are typically not able to resolve the detected number of photons and have a significant dead time after detection. This setup, also called intensity interferometer, was originally invented to measure angular sizes of astronomical objects [70] and the measured correlation of intensities is called the HBT effect after its discoverers.

4 The BB84 protocol

The importance of the BB84 protocol for quantum key distribution (QKD) has already been mentioned. It was the first and is today still the most implemented protocol, with state-of-the-art and even commercial realisations. It has also been the first QKD protocol for which unconditional security has been established. In this chapter the most important aspects are examined, starting with the two most frequent realisations in Section 4.1, the one using polarised photons and the time-bin implementation. Then key components such as light sources, electro-optic modulators and detectors are discussed in detail in Section 4.3. Especially light sources play a crucial role when it comes to the security of the protocol. Finally the security is discussed in more depth and the calculation of secure key rates is established in Section 4.4. This is used in later chapters to describe the three different QKD experiments reported on in this dissertation.

4.1 The standard protocol - BB84 with polarisation

In Figure 14 a basic scheme for a BB84 experiment with polarised photons is shown. In this very simple realisation, four different pulsed laser diodes (LD) emit the horizontally, vertically, $+45°$ and $-45°$ polarised photons needed. The beams are combined by beam splitters (BSs) and attenuated by a neutral density filter (ND) to approximate single photons before being transmitted to Bob. On Bob's side, a BS serves as a passive device to randomly choose a basis. This is an implementation of a passive basis choice. If in contrast an active device is used for the basis choice, which has to be fed with random numbers, it is called active basis choice. In both outputs of the beam splitter BS, there is a polarising beam splitter (PBS) and two avalanche photodiodes (APDs), in one output there is an additional $\lambda/2$ plate in front of the PBS which turns an incoming linear polarisation by $45°$. In this way, the horizontally and the vertically and diagonally polarised photons, respectively, can be distinguished. A photon measured in the wrong basis gives a random result through a random projection on one of the two output states of the PBS.

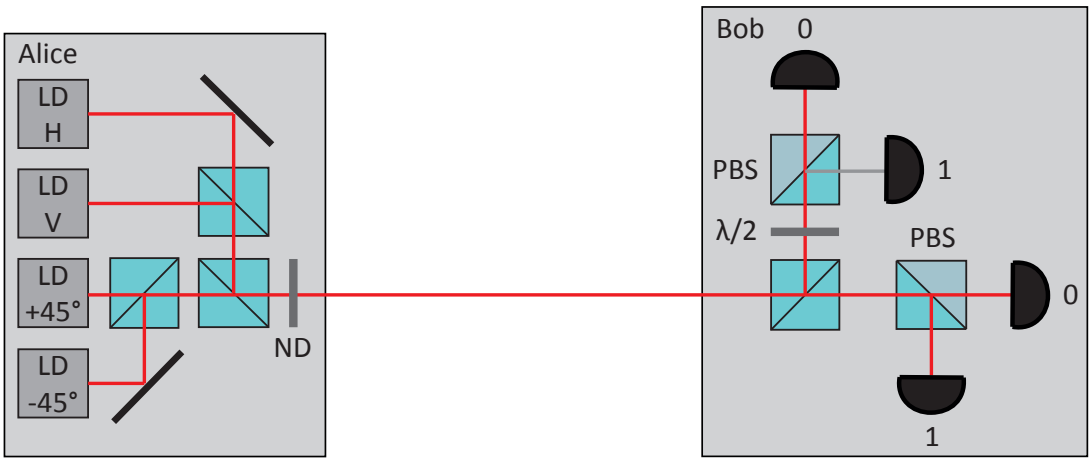


Figure 14: A basic scheme for an experimental realisation of the BB84 protocol with polarised photons, here coming from pulsed laser diodes (LD). There is one diode for each polarisation used, horizontal (H), vertical (V), and the two diagonal ones (+45°, −45°). A neutral density filter (ND) attenuates the laser pulses to approximately single photon level. On Bob's side, a first beam splitter (BS) realises Bob's random basis choice. In one basis, a polarizing beam splitter (PBS) distinguishes between horizontally and vertically polarised photons. In the other basis the photons are first rotated by 45° such that the two diagonally polarised photons can be faithfully distinguished by a PBS as well. The detection is realised with four APDs.

If transmission is performed via an optical fibre instead of free-space, the polarisation will most likely be transformed and the transformation will usually not remain stable over time (cf. Section 4.3.3 in this chapter). Then, additional waveplates can be used in front of Bob's measurement apparatus to compensate for this effect.

An alternative setup with less light sources and less detectors and thus reduced cost can be realised using active optical components such as electro-optic modulators (EOMs), see Figure 15. An EOM is a device which acts as an electrically modulatable waveplate when a voltage is applied. It will be described in more detail in 4.3.2. With this EOM, vertically polarised light from a laser diode or a real SPS is either left unmodified or turned by 90° to become horizontally polarised light when the EOM acts as $\lambda/2$ plate. The EOM can also act as $\pm\lambda/4$ plate to transform the vertically polarised light into left- or right-handed circular polarisation.

Figure 15: A basic scheme for an experimental realisation of the BB84 protocol with polarised photons, here with only one pulsed laser diode (LD), two APDs and active base choice. The diode emits vertically polarised photons. An EOM is used to either not modify the polarisation, turning it by 90° or transforming the linear into left- or right-handed circular polarisation. A neutral density filter (ND) attenuates the laser pulses to approximately single photon level. On Bob's side, a second EOM either leaves the polarisation unmodified or acts as a $\lambda/4$ plate to transform circular light into linear one. Linear light can then be deterministically discriminated by a polarizing beam splitter (PBS) before the light is detected in one of its two outputs with an APD. Circular light gives random detection events.

When represented in the linear polarisation base,

$$|L\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + i\,|V\rangle\right), \tag{69}$$

$$|R\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle - i\,|V\rangle\right). \tag{70}$$

It can be seen that the overlap between this two bases is the same as between the horizontal/vertical and the diagonal basis introduced before. On Bob's side, instead of the BS, an EOM can be used to either leave the light unmodified or to turn circular polarisation into linear one or vice versa. Linear polarisation can then be faithfully discriminated with a PBS and two APDs whereas circular light gives random results. This is thus a realisation of an active base choice.

4.2 The time-bin implementation

The time-bin scheme has already been briefly introduced in 2.4. Now it will be presented in more detail. It is especially well suited for transmission via optical fibres where polarisation is not very robust. A scheme is shown in Figure 16.

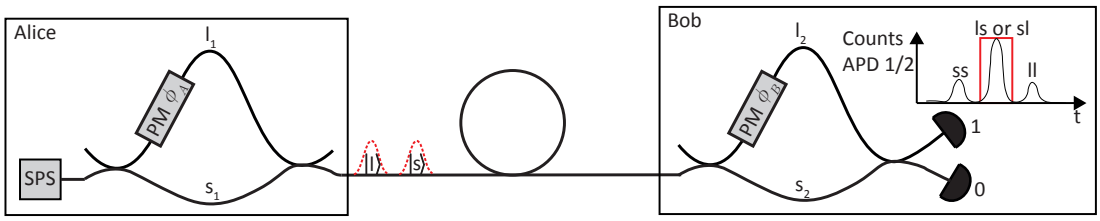


Figure 16: The fibre-based time bin scheme. A photon is in a superposition state of two different time-bins l or s after passing through an unbalanced Mach-Zehnder-interferometer with a short arm s_1 and a long arm l_1. In this interferometer, Alice can modify the phase Φ_A in one arm with her phase modulator (PM). When the photon passes through an identical interferometer at Bob's side with short arm s_2 and long arm l_2, detection with two APDs can take place in three different time slots (see on top on the right): a first one, corresponding to the photon having taken the short arm in both interferometers, a last one, corresponding to a photon which went through the long arms of both interferometers and an intermediate one (red rectangle). Photons being detected in this intermediate time slot can have passed either through the long arm l_1 in the first and the short arm s_2 in the second interferometer or the short arm s_1 in the first and the long arm l_2 in the second interferometer. These two possibilities are indistinguishable and thus interfere at the last coupler of Bob's interferometer. Bob can influence the phase Φ_B in one arm of this interferometer by a phase modulator and applies his basis choice by this.

In a first unbalanced interferometer controlled by Alice, a time-bin qubit is created. The photon will have either passed through the short arm, denoted by s_1 or the long arm, l_1, the path length difference being Δl. Alice can influence the phase Φ_A in the long arm by a phase modulator (PM). This is basically an EOM with an index of refraction depending on the applied voltage. On Bob's side the superposition state passes through a second, identical interferometer. In this interferometer, Bob can influence the phase Φ_B in the long arm by a phase modulator. The photon can take again the short arm, denoted by s_2 or the long arm, l_2. Then detection occurs in one of two APDs at either of the output arms of the interferometer in three different possible time-slots, as shown in Figure 16. These correspond to four different photon path combinations: s_1s_2, l_1l_2, l_1s_2 and s_1l_2. The two latter possibilities are temporally indistinguishable and thus interfere according to the phase set by Alice and Bob. Temporally filtering only those events yields the

following superposition state:

$$|\psi\rangle = e^{i\Phi_A}|l_1 s_2\rangle + e^{i\Phi_B}|s_1 l_2\rangle \quad (71)$$
$$= |l_1 s_2\rangle + e^{i(\Phi_B - \Phi_A)}|s_1 l_2\rangle \quad (72)$$

Alice will choose between four different phases: 0, π, $\pi/2$ and $\frac{3}{2}\pi$. Bob will choose his basis by setting his phase to either 0 or $\pi/2$. A truth table (Table 1) associates the different phases with clicks in APD 0 or 1 (see Figure 16).

Φ_A	**Bit sent**	Φ_B	**Click APD no.**	**Bit received**
0	0	0	0	0
π	1	0	1	1
$\pi/2$	0	0	0 or 1	?
$\frac{3}{2}\pi$	1	0	0 or 1	?
0	0	$\pi/2$	0 or 1	?
π	1	$\pi/2$	0 or 1	?
$\pi/2$	0	$\pi/2$	0	0
$\frac{3}{2}\pi$	1	$\pi/2$	1	1

Table 1: Truth table for the time-bin BB84 protocol

There are some practical issues which have to be considered when implementing this scheme. First of all, the arm length difference Δl has to be such that the three different possible arrival times can be temporarily resolved, so it has to be larger than the pulse length and the minimal temporal resolution of the detectors. With typical experimental equipment it should be in the order of nanoseconds [13]. This corresponds to roughly 10 cm of arm length difference.

Secondly, as was seen in Equation 56, the interference contrast or visibility depends on the coherence time in relation to the temporal difference between the two paths. In reality the two interferometers will never be exactly identical, but their path differences δl should only be within a fraction of the coherence time. Typically, this means that they must be matched within a difference in the order of mm [13]. Also, to keep the phase relation between them stable, they have to be stabilised, for example by keeping them at a stable temperature in isolated boxes. Active compensation techniques, e.g. fibre stretchers [48], are typically necessary as well.

Additionally, for interference to take place, the polarisation of states which have been transmitted over different, interfering paths have to be the same. The transmission path in between Alice and Bob should induce the same polarisation transformation on the two time-bin states. The different arms of the interferometers are more critical in this respect. Fortunately, the polarisation in temperature stable,

isolated boxes is rather stable. There are also special techniques to circumvent this problem, such as the use of Faraday mirrors [71] employed in a Michelson interferometer.

These practical issues will be addressed in more detail in Chapter 7.

4.3 Essential components for the BB84 protocol

4.3.1 Light sources

In this section the focus is on components for QKD. The discussed components are typically used in experimental setups for the BB84 protocol but are also relevant for implementations of other protocols. They are key components in the different experiments presented in this thesis. This first section deals with possible light sources for QKD. There are two different possibilities: a real single photon source (SPS) or an approximation of single photons through weak coherent pulse (WCP) coming from a laser. Specific aspects of these two possibilities are discussed in the following.

4.3.1.1 Single photon sources

Only a single photon source has a sub-Poissonian statistic and features anti-bunching, as has been discussed in Section 3.4. Thus only a true single photon source emits one photon at a time. This is an important issue for the security of QKD as will be seen in Section 4.4.3. Different realisations exist so far, with specific drawbacks and advantages as well as a typical wavelength regions of emission. Typically, some kind of two-level system is used or approximated whose fluorescence after excitation exhibits the typical statistical signature of a SPS. The most common systems are semiconductor quantum dots [72], single molecules [73], single ions [74] or defect centres such as the Nitrogen-vacancy (NV) centre in diamonds [75]. Excitation of the system can be either by optical pumping or through electrical excitation. In this thesis, QKD with two types of defect centres in diamonds, the NV centre and the silicon vacancy centre (SiV) will be further discussed in Chapter 5. Some two-level systems, which are of interest not only as single photon emitters but also as localized quantum bits for storage or processing, couple to wavelengths which are not suited for long distance photon transmission. This is why schemes for the conversion of single photon wavelengths are of interest [76, 77]. A different approach to SPSs are heralded single photons generated from photon pairs in spontaneous parametric down-conversion (SPDC) [78]. In this scheme, two photons of a pair are separated in two different spatial modes. A high

conditional probability of the existence of a single photon state in one mode then results from a detection of one photon in the other mode.

All available SPS have different practical issues which limit their applicability presently. An ideal single photon source should be efficient, meaning that a single photon is emitted into a well defined spatial and spectral mode with near unity probability each time a trigger signal is applied. This aspect concerns the quantum efficiency, the collection efficiency and the spectral bandwidth of the emission. The quantum efficiency is the emission probability per excitation and is in principle an inherent property of the quantum emitter. It can be enhanced by enhancing the radiative rate using the Purcell effect through coupling of the emitter to resonant structures. The collection efficiency can be influenced as well by the design of photonic structures in the environment of the emitter. Improving both quantum and coupling efficiency of single photon emitters is an active area of research at the moment and different approaches with different quantum emitters have been sought, e.g. terrylene molecules coupled to dielectric plannar antennas [79], NV centres in diamond coupled to fibre-based microcavities [80], defect centres integrated in diamond nanowires [81], the coupling of quantum dots to nanoantennas [82] or plasmon-enhanced single photon emission of NV centres [83] have been successfully demonstrated. Of interest for long distance quantum communication is of course the coupling into a single mode of an optical fibre (see Section 4.3.3). Concerning the spectral mode, it is desirable to have a narrow bandwidth emission for most experiments. The SPS should also yield a high and stable emission rate without blinking or bleaching and be practical, meaning that it can be built in a robust and compact way and can be operated ideally at room temperature. Some of the aforementioned realisations are promising, but further fundamental research and extensive testing is necessary to reach this goal.

4.3.1.2 Attenuated lasers

Due to their practicability, very often attenuated laser pulses are used to approximate single photons. Compact and easy-to-use pulsed laser diodes in combination with precise attenuators are typically used to produced the weak coherent pulses (WCPs). Even though very low intensities with a mean photon number μ of typically $\sim$0.1 is used, the statistical properties of the emitted coherent light, which are Poissonian, do not change, see Sections 3.3 and 3.4. This means that there is always a finite probability that a pulse contains more than one photon. Since all photons within a pulse are coded in the same way, this could be exploited by Eve (see photon number splitting (PNS) attacks, 4.4.3). Because of that, μ has to scale linearly with the transmission coefficient t between Alice and Bob, (Section

4.4.3), meaning that the key rate scales with t^2. This is a problem when using WCPs if no sophisticated additional protocols are used as for example the decoy state method [84], see Section 4.4.3.

4.3.2 Electro-optic modulators

Electro-optic modulators (EOMs) are used in many different experiments discussed in this thesis. Mainly they are used to accomplish four different tasks: polarisation modulation, intensity modulation, switching, and phase modulation.

The modulators are based on the linear electro-optic effect. This means that (additional) birefringence is induced in a crystal through a change in the index of refraction n along an axis by application of an electric field. The change is linear to the applied field. The axis shall be called optical axis as in uniaxial birefringent material from now on. By the change of n, the phase of light polarised along this axis can be modulated. The effect is caused by a redistribution of bond charges at an atomic level as well as a possibly slight deformation of the lattice under the application of an electric field [85]. Typically, a crystal transparent at the desired wavelength and offering a high electro-optic coefficient r is sandwiched between two electrodes to apply the electric field. There are two possible configurations, longitudinal or transverse. Longitudinal modulators apply the electric field parallel to the light beams propagation direction, transverse modulators apply it orthogonally to the propagation direction. Transverse modulators usually allow lower voltages to be applied for the same effect and all modulators used in this thesis are of the transverse type. The phase along the optical axis is modified according to [85]:

$$\Delta\phi = \frac{2\pi}{\lambda} L \Delta n \tag{73}$$

with L being thy crystal's length and

$$\Delta n \approx \frac{1}{2} n^3 r \cdot E \tag{74}$$

E being the applied electric field. So to use an EOM as a phase modulator, one uses light polarised linearly along the optical axis and applies an appropriate voltage.

For a controlled modulation of a linear polarisation, light should be entering with an angle of 45° with respect to the optical axis of the modulator. This polarisation is equally projected on a plane containing the optical axis and onto an orthogonal plane. In this manner, one projection is shifted with respect to the other, and arbitrary waveplates like a $\lambda/2$ plate with a resulting rotation of the polarisation of 90° or a $\lambda/4$ plate resulting in circular polarisation can be realised.

One way to modulate the intensity is to modulate the polarisation in combination with a linear polarisation filter at the output of the modulator. All modulators used in this thesis are however so-called Mach-Zehnder modulators (MZMs). They actually consist of a small Mach-Zehnder interferometer whose phase between the two arms is modulated by the electro-optic effect. The modulator output consists of only one interferometer output and the intensity results from the degree of constructive and destructive interference, respectively, controllable by the applied voltage. Typically, a so-called push-pull constellation is used [85], with phase modulators of opposite phase in each interferometer arm. This constellation needs lower voltages and pulse deformation caused by chirp can be avoided [86]. The same device can also be used as a switch when both outputs are used for a so-called double output Mach-Zehnder modulator (DOMZM).

The crystal materials depend on the wavelength of the application. Typical materials are potassium dihydrogen phosphate (KDP) for visible light and lithium niobate ($LiNbO_3$) for the infrared.

For high-frequency modulation, a so-called traveling wave constellation is used, where the applied voltage travels along with the light. This way, the light will see the same index of refraction all the way along the crystal. This is realised by designing the electrodes such that they are part of the driving transmission line [85].

Another practical issue is that many modulators are intrinsically polarizing since they guide only a single linear polarisation.

4.3.3 Transmission channels

There are two channels for transmission of quantum signals in QKD: optical fibres or free-space. Optical fibres are made of silicon dioxide (SiO_2) and possess an index of refraction profile which results in axial guidance of light through total internal reflection of the light in radial direction. Standard single mode optical fibres for telecommunication purposes, which are usually used, have low losses at $1.3\,\mu$m and $1.5\,\mu$m (0.35 dB/km [13]; 0.16 dB/km [46]) and preserve the coherence of most quantum states, even though active compensation might be necessary, for example when using polarisation states [13]. They naturally offer perfect overlap of the spatial mode when coupling between different devices or beams. Free-space or air also offers good transmission at some visible and infrared wavelengths (0.19 dB/km at 780 nm and 852 nm, respectively [87], 0.1 dB/km at around 1560 nm [47]). Losses scale typically exponential with the transmission distance but can progress significantly more favourable when transmitting between the earth and low earth orbit (LEO) satellites. Transmission through free-space also preserves the coherence of

most quantum states, for polarisation no compensation as for fibres is needed. One problem is the unavoidable divergence of light beams and beam path fluctuations due to turbulence. Also, the spatial mode of the light is not well defined as it is in the case of optical fibres.

4.3.4 Single photon detectors

One difficulty in working with single photons is to detect them. There are no ideal, noise-free single photon detectors available, ultimately since quantum fluctuations represent a fundamental limit. There are basically two widely used methods to detect single photons: either with avalanche photodiodes (APDs) or with superconducting single photon detectors (SSPDs). Both techniques have its advantages and its drawbacks which are discussed in the following. The characteristics of the less frequently used photomultiplier tube (PMT) are also introduced since it has properties which are interesting for some applications and one is used for the implementation of the QRNG reported in Chapter 8. APDs, which are used mostly for the experiments in this thesis, are photodiodes which are operated in the so-called Geiger-mode, where the voltage applied to the diode exceeds the breakdown voltage such that a single electron-hole pair created from a photon can lead to a detectable avalanche of electrons [13]. To stop the avalanche, once it is detected, there are different methods: in passive quenching, a resistor in series with the diode quenches the avalanche once it occurs. In active quenching, this is done by an electronic circuit once the avalanche is detected. In gated mode, the voltage is brought above the breakdown voltage only during certain gates of variable width. For this mode, the instance in time when the photon arrives should be known [13].

There are different materials for the diode material of the APDs, basically there is silicon (Si) for the wavelength range from the visible up to $1\,\mu$m and there is indium gallium arsenide (InGaAs) covering the telecom wavelength range between $1.3\,\mu$m and $1.5\,\mu$m.

A second class of detectors are SSPDs [88, 89]. They consist of a superconducting nanowire which is arranged in a pattern of meanders to cover large areas. The nanowire is kept well below critical temperature and just below but close to the critical current. Incoming photons create a localized non-superconducting region, called hotspot, eventually causing the current density to exceed its critical value. The superconductance is disrupted and a measurable voltage pulse is created [90]. SSPDs are typically made of niobium nitride (NbN) or of tungsten silicide (WSi) [91].

PMTs are less frequently used in quantum information processing (QIP), but they do have characteristics which make them competitive to the other types for some

applications. A PMT exploits the photoelectric effect to create electrons out of single photons on a photocathode. A detectable avalanche of electrons is created by a series of dynodes in a vacuum tube with an increasing acceleration voltage between each pair of dynodes [92]. Materials are gallium arsenide phosphide (GaAsP) for visible wavelengths and InGaAs/indium phosphite (InP) for the near infrared. There are variants like the hybrid detector, a photocathode combined with an avalanche diode, [93], which offers very good timing resolution of about 50 ps and the ability to resolve photon numbers. There is also the microchannel plate PMT, built of glass capillaries whose walls act as dynode with a continuously increasing acceleration voltage, [94]. It offers good timing resolution of 80 ps [95].

There are different figures of merit when it comes to single photon detection. Some of them are related to problems intrinsic to devices sensitive enough to detect single photons. The quantum efficiency η gives the probability that a single photon results in an electronic output signal. For APDs it varies from 10-25% typical for InGaAs/InP models to over 70% for Si APDs. Recently there has been a report of η up to 55% at a wavelength of 1.5 μm [96]. For SSPDs an η of around 10-25% [97] for light from the visible to the infrared without the use of external cavities is reported for NbN models. It should be noted that higher efficiencies are typically achieved by a resonator structure around the detector which prevents detection over a wide wavelength range. Recently a SSPD made of WSi showed an η of over 90% [91]. PMTs typically have lower quantum efficiencies in all wavelength ranges than APDs.

Dark counts are counts which are not due to photons but due to thermal or electronic noise. They impair the signal to noise ratio and ultimately limit possible transmission distances (see Section 4.4.1). The dark count rates of Si APDs and of SSPDs are much better than those of InGaAs APDs. The dark count rates of PMTs is usually worse than those of APDs.

The so-called afterpulses are a phenomenon typical to APDs when trapped charges produced after a detection cause an avalanche which mimic a detected photon [13]. Also PMTs typically produce afterpulses. They can be dealt with by introducing a dead time after detection, giving the charges time to relax unnoticed in the meantime. This comes at the price of reducing the maximal detection rate. Also a higher detector temperature helps decreasing afterpulses, but this increases the thermal noise.

Then there is the timing jitter which is the uncertainty in the time between a detected photon and the corresponding electronic output signal. Typically APDs possess jitter in the order of 100 ps whereas SSPDs are an order of magnitude better. PMTs can possess lower jitter than APDs of 50 to 80 ps [95, 93].

The maximum count rate of all these devices can vary from MHz to GHz [96] and depends on dead times and the electronic circuitry used. Typically the maximum count rate of the detectors imposes the limit to repetition frequencies of modern QKD experiments.

It is worth mentioning that while most detectors do not have the ability to resolve the number of photons in a given pulse and just have a digital output signal indicating that either a detection was registered or not, there are detectors with the ability to resolve the number of photons [98, 99, 93]

Last but not least, practicability deals with the question if bulky and unpractical cryogenic cooling with liquid helium is used, which has to be frequently exchanged. This is the case for some SSPDs implementations, but often closed cycle cooling is available.

Table 2 summarises the figures of merit for different types of available commercial single photon detectors as well as a state-of-the-art research prototype (Toshiba). The data of the commercial products was taken from the companies' websites [100, 101, 102, 103, 53, 104].

	SSPDs			**APDs**			**PMTs**	
	Scontel	**Photon Spot**	**Single Quantum**	**Excelitas SPCM**	**ID Q id210**	**Toshiba [96]**	**Hamamatsu 7421/7422**	**H10330A**
λ [μm]	0.5-1.7	∼1.5	0.2 - 2.0	0.4 - 1.0	0.9 - 1.7	∼1.5	0.3-0.72	0.95-1.7
Material	NbN	WSi?	?	Si	InGaAs/ InP	InGaAs/ InP	GaAsP	InP/ InGaAs
η	10-25%	>90%	>75%	>70% (700 nm)	10-25%	55%	40% (580 nm)	2%
DC [Hz]	<10	?	<300	25	∼20 k	?	100	250 k
AP	0	0	0	0.5%	?	10%	?	?
Δt [ps]	<45 ps	30-50 ps	<40 ps	350 ps	200 ps	<100 ps	300 ps [92]	400 ps
Max. count rate/ dead time	>100 MHz	3-30 ns	20 ns	40 MHz	typ. 10 μs	500 MHz	>1.5 MHz	?
Cooling type	closed cycle	?	closed cycle	Peltier	Peltier	$\sim T_{room}$	Peltier	Peltier
PNR	n	y	n	n	n	n	y [92]	?

Table 2: A table comparing the performance of different single photon detectors. DC stands for dark counts, AP for afterpulses, Δt stands for the timing jitter between incoming photon and output signal. When a maximal count rate is not available, the dead time can give an indication about maximal rates. PNR stands for the ability to resolve the number of detected photons. When a field is marked with a"?", more specific data was not available.

4.4 The security of BB84

In this section, the secret key rate, which is the magnitude of interest in QKD, will be analysed in more detail for the well studied example of the BB84 protocol. At first, a security proof of a perfectly implemented BB84 protocol will be sketched and a secure key rate will be deduced. Then, after a short introduction to experimental sifted key rates and QBERs, practical flawed implementations will be analysed, with the focus on light sources which do not emit true single photons. The deterioration of the secret key rate due to a photon number splitting (PNS) attack of Eve is calculated. Finally, the recovery of satisfactory secure key rates when using weak coherent pulses (WCPs) through the decoy state method is introduced.

4.4.1 Unconditional security

The notion of unconditional security has already been discussed in Section 2.8. It has been briefly explained that if Eve's information on a sifted key can be bounded and if it is low enough, error correction and privacy amplification can be applied to generate a secret key which is secure.

Now it shall be sketched how this unconditional security can be proven and how Eve's information can be bounded for the BB84 protocol following the security proof from Shor and Preskill [37].

It starts with entangled EPR pairs (named after Einstein, Podolsky and Rosen) distributed between Alice and Bob, meaning that one photon each is received. EPR pairs are states of entangled qubits of the following form:

$$|\beta_{00}\rangle \quad = \quad \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{75}$$

The states, which might have been changed due to noise on the channel or eavesdropping, are locally measured by Alice and Bob to extract a key. It can be shown that the fidelity of the states shared between Alice and Bob with respect to the original EPR states can bound the information an eavesdropper might possibly have about the key [105]. The fidelity between two states described by the density matrices ρ and σ is defined by the following expression:

$$F(\rho, \sigma) \quad \equiv \quad tr\sqrt{\rho^{1/2}\sigma\rho^{1/2}} \tag{76}$$

It gives a measure of the similarity of the two states. If they are identical $F = 1$, otherwise smaller. The fidelity can be measured by random sampling of some of the distributed states and by applying a specific measurement to them

[105]. The information of Eve is then bounded and can be removed by privacy amplification if it is low enough. Alternatively, and this is in the line of proving the security for the BB84 protocol, one can apply so-called entanglement distillation protocols until the fidelity comes arbitrarily close to 1. Entanglement distillation is a process using n-states of fidelity $F < 1$ to produce m-states of fidelity $F = 1$, where $m < n$. If a measurement of the state is effected only afterwards, a secure key can be distributed. This entanglement distillation can be accomplished using so-called quantum error correction (QEC) codes correcting t errors and working on quantum states. They typically need complex quantum operations which require a quantum computer and quantum memories. Random sampling of Alice and Bob must guarantee that no more than t errors have been transmitted for this to work. This is the so-called modified Lo-Chau protocol [105]. Such QEC which correct up to t errors of m states using n states exist with certainty as long as the following equation, known as the quantum Gilbert-Varshamov bound is satisfied:

$$m/n \;\geq\; 1 - 2H\left(\frac{2t}{n}\right) \tag{77}$$

where H is the binary Shannon entropy, $H(x) = -x \cdot log_2(x) - (1-x) \cdot log_2(1-x)$. So for m states with fidelity close to one, one needs at least n states where n is given by Equation 77 or the other way around if n states are used to obtain m secure states, the error on the n states should be maximally t. This scheme is still far from BB84, as entangled photon pairs, quantum computers and quantum memories are needed. The need for entangled pairs can be relaxed by showing the equivalence of all the required operations for entangled pairs and qubit states prepared by Alice and measured by Bob, as long as Alice and Bob use the so-called Calderbank-Shor-Steane (CSS) codes [106] as QEC [105]. These codes are based on classical error correction codes but rely on quantum mechanical operations.

CSS codes correct both bit and phase errors of a quantum state, but in a decoupled manner. Because in the version with qubits instead of EPR pairs, Bob only cares about bit values of the final key and not about phase errors [37], the phase error correction information normally necessary to implement the QEC can be dropped. This allows Alice and Bob to work with the two classical codes on which CSS codes are based, so no quantum computers are needed. Now introducing a random basis choice for Bob's measurement instead of Bob storing the received states in a quantum memory and waiting for Alice to announce the correct measurement basis as required in the initial proposition actually results in the BB84 protocol [105]. The classical codes which are used actually implement error correction and privacy amplification in this. This scheme works with certainty for maximally t errors on n bits producing m secure bits as expressed by Equation 77. This bound can be relaxed if one only demands the codes working with high probability for

random errors $\leq t$ [37]. The bound then becomes

$$m/n \;\geq\; 1 - 2H\left(\frac{t}{n}\right). \tag{78}$$

The right side of this equation becomes 0 for t/n (the QBER) equal to 11%. It should be noted that this bound is true only for ideal error correction and also only for qubits encoded in single photon states.

4.4.2 Theoretical rates

Now equations to theoretically estimate secret key rates for experimental realisations of the BB84 protocol are introduced. The secret key rate can be calculated as a product of two factors, the sifted key rate R_{sifted} and the secret key fraction r. The secure key rate is then given by $S = R_{sifted} \cdot r$.

Before turning to the sifted key rate, which possibly counts events which are not generated by photons, the sifted photon key rate is defined, which only contains bits caused by the detection of photons. The sifted photon key rate $R_{sifted\ photon}$ for the BB84 protocol depends on the repetition frequency of the light source f_{rep}, the mean intensity or mean photon number per signal μ, the transmission between Alice and Bob t, the transmission in Bob's apparatus t_B, the detection efficiency η and a factor q which is typically 1 but is 1/2 for example in the time-bin implementation, where only half of the sent signal ends up in the right time window,

$$R_{sifted\ photon} \;=\; \frac{1}{2} \cdot q \cdot f_{rep} \cdot \mu \cdot t \cdot t_B \cdot \eta\,. \tag{79}$$

The pre-factor $\frac{1}{2}$ accounts for the fact that in only half of the cases Alice and Bob will have chosen corresponding bases.

The QBER is defined as the number of wrong counts over the number of overall counts,

$$\begin{aligned} QBER &= \frac{N_{wrong}}{N_{sifted}} \\ &= \frac{R_{wrong}}{R_{sifted}}\,. \end{aligned} \tag{80}$$

The experimental QBER, which is not caused by eavesdropping, consists of two different contributions to R_{wrong}: R^Q_{opt} and R^Q_{det}. The rate of erroneous bits of

purely optical origin, R^Q_{opt}, which comes from an imperfectly prepared or measured state and has a probability to occur of p_{opt} for every sent state,

$$R^Q_{opt} = \frac{1}{2} q \cdot f_{rep} \cdot \mu \cdot t \cdot \eta \cdot p_{opt} \,. \tag{81}$$

This error is thus part of $R_{sifted\ photon}$, which can be divided into an error free and a flawed part, $R_{sifted\ photon} = (1 - p_{opt}) \cdot R_{sifted\ photon} + p_{opt} \cdot R_{sifted\ photon}$. Then there is the QBER which accounts for noise, typically from dark counts from the detector, the corresponding rate is

$$R^Q_{det} = \frac{1}{2} \cdot \frac{1}{2} f_{rep} \cdot n_{det} \cdot p_{det} \,. \tag{82}$$

The first pre factor $\frac{1}{2}$ comes from dark counts which occur while Alice and Bob chose different bases, the second comes from the probability that dark counts accidentally occur in the right detector, thus not causing errors. This error rate is thus not proportional to the transmission and thus grows relatively to $R_{sifted\ photon}$ with increasing loss. That is why eventually the transmission distance is limited because the QBER becomes too big. The complete sifted key rate including erroneous bits is thus

$$R_{sifted} = R_{sifted\ photon} + R^Q_{det} \,. \tag{83}$$

The secret key fraction is of course a function of the QBER and in the case of ideal post-processing it is given by Equation 78, so that the secret key rate becomes

$$S = R_{sifted} \cdot (1 - 2H(Q)) \,, \tag{84}$$

where Q stands for QBER. As most error correction codes are not as effective in reality, there is some function $f(Q)$ that gives its effectiveness, with $f \geq 1$, a typical value is 1.2. Then Equation 84 becomes

$$S = R_{sifted} \cdot (1 - f(Q) \cdot H(Q) - H(Q)) \,. \tag{85}$$

4.4.3 The photon number splitting attack

When weak coherent pulse (WCP) from attenuated lasers are used, there is a finite probability to generate and prepare more than one photon per pulse and thus per state. This can be exploited by Eve in the so-called photon number splitting (PNS) attack [107]. It goes as follows: Eve performs a so-called quantum non-demolition measurement (QND) on the WCP sent by Alice to measure the number of photons in the pulse without disturbing the qubit itself. Such a quantum

non-demolition measurement can be quite complicated experimentally, but is not impossible. When more than one photon is present, she can keep one, for example put it in a quantum memory and measure it only after the sifting. She can thus gain full information on the qubit without introducing errors. The situation is bad when significant losses on the line exist. If the transmission t is as small or smaller than the probability of having more than one photon in a pulse $p_{n\geq 2}$, Eve can replace the transmission channel between her and Bob with a (theoretically possible) lossless channel and block all pulses with just one photon. She could then gain full information on the key without being detected since the key rate would be as expected. This attack is illustrated also in Figure 17.

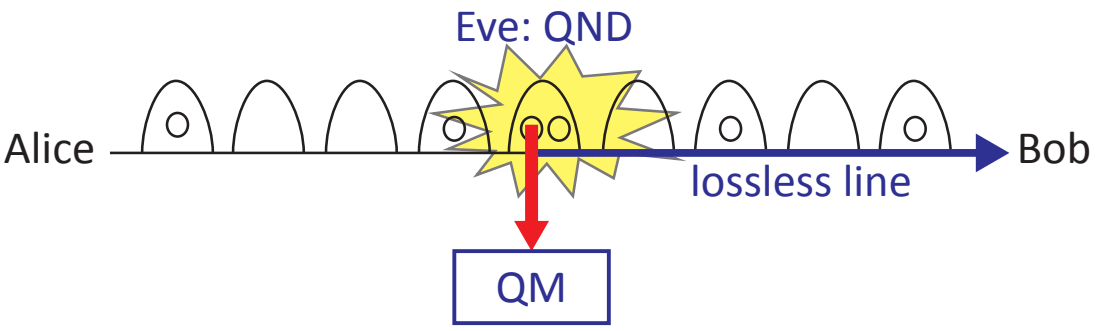


Figure 17: The photon number splitting (PNS) attack. Alices sends WCP with typical intensities μ to Bob. These contain very often no photon at all, from time to time one photon and with a probability of $\sim \mu^2/2$ two photons (more photons are even less probable). Eve performs quantum non-demolition measurements (QND) on each pulse and in case of two or more photons contained, she puts one in her quantum memory where she stores it until sifting, only then she measures, then in the correct basis. She sends the remaining photon(s) to Bob via a lossless line, making her intervention unnoticeable.

This attack can be prevented while using weak coherent pulse (WCP), but at the price of a strongly reduced rate. To see this, one can make an estimate of the maximal secure key rate. When a single photon source (SPS) is used, μ is fixed. But when attenuated lasers are used, it has to be optimised, giving a good compromise between a maximal sifted key rate and and a probability $p_{n\geq 2}$ being not to high [39]. R_{sifted} is proportional to μ and t, the information given to Alice unnoticed is proportional to $\sim \mu^2/2$ if just the two-photon probability (see Equation 46 in Section 3.3) is considered. So the secret key rate is proportional to $\mu \cdot t - \mu^2/2$ which is maximised for $\mu \approx t$. The secret key rate thus scales with $t^2/2$ instead of just t as one might expect, which is very unfavorable.

There is another, more efficient way in terms of secret key rates to deal with

PNS attacks, the decoy state method [108, 84]. Before presenting the idea and achievable rates, some terms have to be introduced with a nomenclature as in [39]. First of all R_{sifted} can be split into separate rates caused by different numbers n of photons actually emitted,

$$R_{sifted} = \sum_n R_n \,. \tag{86}$$

The yield $Y_n = \frac{R_n}{R}$, with $\sum_n Y_n = 1$ is the probability of an emitted signal with n photons being detected. Also the errors can be split into parts associated with different numbers of emitted photons,

$$\varepsilon_n = \frac{R^n_{wrong}}{R} \,, \tag{87}$$

with the QBER

$$Q = \sum_n Y_n \varepsilon_n \,. \tag{88}$$

The same expression can be formulated for the information of Eve I_E,

$$I_E = \sum_n Y_n I^E_n \,. \tag{89}$$

Recapitulating the PNS attack, the worst case scenario is that $\varepsilon_{n>1} = 0$ and $I^E_{n>1} = 1$. Eve will try to keep Y_1 as low as possible. All the parameters directly accessible to Alice and Bob are R_{sifted} and the QBER. Y_1 can be calculated in principle for the worst case assumption that all pulses emitted with more than one photon will be detected and with $p_{n>1}$ which can be calculated from μ. The secret key rate from Equation 85 for BB84 implemented with WCP then becomes [109]

$$S = R_{sifted} \cdot \{Y^\star_1 (1 - H \cdot (Q/Y^\star_1)) - f(Q) \cdot H(Q)\} \,, \tag{90}$$

where $Y^\star_1$ is the worst case assumption as described above. If a more optimistic estimation of a lower bound of Y_1 and thus of the error $\varepsilon_1 = Q/Y_1$ could be made, higher key rates would be possible. That is the trick of the decoy state method. Imagine Alice chooses between different intensities μ_1, μ_2, ..., μ_m: only after transmission she will publicly announce which intensity she used when. Bob will thus have different results for the rates $R^{\mu_1}_{sifted}$, $R^{\mu_2}_{sifted}$, ..., $R^{\mu_m}_{sifted}$ as well as for the QBER Q_{μ_1}, Q_{μ_2}, ..., Q_{μ_m}. But the different Y_ns and ε_ns will not have changed since Eve can only measure the photon number but knows nothing about

the intensity Alice applied and thus cannot change her strategy according to it. Since

$$R^{\mu_i}_{sifted} = \sum_n R^{\mu_i}_n \,, \tag{91}$$

$$Y_n = R^{\mu_i}_n / R^{\mu_i}_{sifted} \tag{92}$$

and

$$Q_{\mu_i} = \sum_n Y_n \varepsilon_n \tag{93}$$

the yields and errors can be exactly calculated for $m \to \infty$. In practice it can be shown that with only three different intensities used a good approximation can be made [110]. So not only can Eve be detected when trying to apply the PNS attack because a deviation from the expected yields and errors will be noticed, also the secret key rate is much more favourable with the better lower bounds on Y_1 and ε_1,

$$S = R_{sifted} \cdot \{Y_1 (1 - H \cdot (\varepsilon_1)) - f(Q) \cdot H(Q)\} \,. \tag{94}$$

Also, the decoy state method allows Alice to use substantially higher mean intensities than is the case when using WCP without it [110].

5 BB84 with single photons

When quantum key distribution (QKD) is implemented with an attenuated laser as signal source, the security can be compromised, cf. Section 4.4.3 and the intensity of weak coherent pulses (WCPs) has to be significantly reduced to circumvent the problem, resulting in a low key rate. One effective solution is to use the decoy state method [108, 84]. However, if a practical and efficient single photon source (SPS) is at hand, it will be a natural choice for most QKD protocols and also for linear optical quantum computing (LOQC) [111] and some quantum repeater protocols [112]. Efficiency means here that it emits a single photon into a well-defined spectral and spatial mode with a probability near unity each time a trigger is applied. To be practical, the SPS should also have a stable emission rate, be easy-to-use, it should operate at room temperature and at high repetition frequencies which are comparable to those of pulsed lasers. A promising candidate for such a SPS are defect centres in diamonds [75, 113, 114]. They operate at room temperature and show bright and mostly stable emission.

In order to evaluate the applicability of defect centres in diamonds as reliable sources for QKD, a test-bed that allows for long-term measurements and integration of different defect centres in diamonds is implemented. It consists of a short free-space transmission line combined with a compact SPS based on diamond-based defect centres for polarisation based BB84. The source relies on a confocal setup for stable optical excitation and efficient collection of single photons from nanodiamonds containing defect centres. Furthermore, it is designed in a way that facilitates the replacement of one kind of nanodiamond single photon source by another. A QKD experiment is performed with nitrogen vacancy (NV) centres and for the first time also with silicon vacancy (SiV) centres. This chapter is organized as follows: First of all, in Section 5.1, defect centres as single photon source are introduced more thoroughly. Afterwards, the setup is introduced in Section 5.2, consisting of the three main parts, the confocal setup, the QKD testbed and the control and data acquisition unit. Before presenting and discussing the results in Section 5.4, the CASCADE protocol used for post-processing of the raw key is presented in Section 5.3.

The results presented in this chapter have been published in [171].

5.1 Defect centres in diamonds as single photon sources

Diamonds consist of carbon (C) atoms in a double face centred cubic crystalline structure. Diamonds have interesting optical properties. Their wide band gap makes them transparent over a wide range of wavelengths and they have a high index of refraction of $n \approx 2.4$.

Interesting in this context is their ability to host impurities such as nitrogen (N) atoms. The impurities have electronic properties which can result in optical activity. Only some impurities are known for emission of single photons. Here, NV and SiV centres, named after the dominant impurities and the coexisting vacancy of a carbon atom in the lattice, are used as single photon source.

5.1.1 The nitrogen vacancy centre

The NV centre modifies the crystalline diamond structure by a nitrogen atom replacing a carbon atom and a neighbouring vacancy, as can be seen in Figure 18 a).

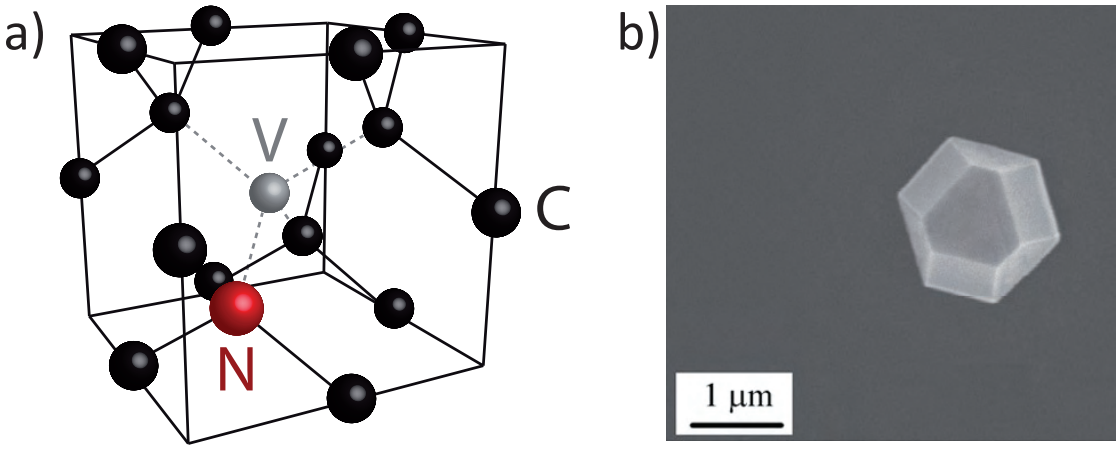


Figure 18: In a) the atomic structure of the nitrogen vacancy (NV) centre. It is constituted of a substitutional nitrogen atom (N) replacing a carbon atom (C) together with a nearest neighbour vacancy (V) is shown, taken from [7]. In b), an image taken with a scanning electron microscope (SEM) of a diamond nanocrystal is shown. Taken from [115].

Due to additional electrons which can be bound or missing, there exist several charged states of the NV centre in addition to the neutral state. In this dissertation, so-called nanodiamonds, thus diamonds with a size of 20-100 nm [7], cf. Figure 18 b), are used due to their practicability and good photon extraction

properties. All of them had one bound electron, only NV^- centres will be discussed in the following.

Responsible for the single photon emission is an electronic structure which can be described as a three-level structure with one ground, one excited and a metastable state (see Figure 19). Single photon emission, indicated by $g^{(2)}(0) < 0.5$ (see Equation 68), is observed, see inset of Figure 19 for an exemplary measurement [7]. At the same time, close in time to the antibunching-dip, bunching can be observed, see also inset of Figure 19. The bunching structure can be explained with the existence of the metastable state. The metastable state has a relatively long lifetime and can only be reached via the excited state. When it is excited, photon emission is not possible for a while until it decays to the ground state which can then be excited again, so no photon detection will take place for long time. But when a photon has been detected and one knows that the system is in the ground state, another detection can take place because the excited state can be reached again. This makes the conditional probability of detecting a photon when another one has just been detected higher than the average probability to detect a photon.

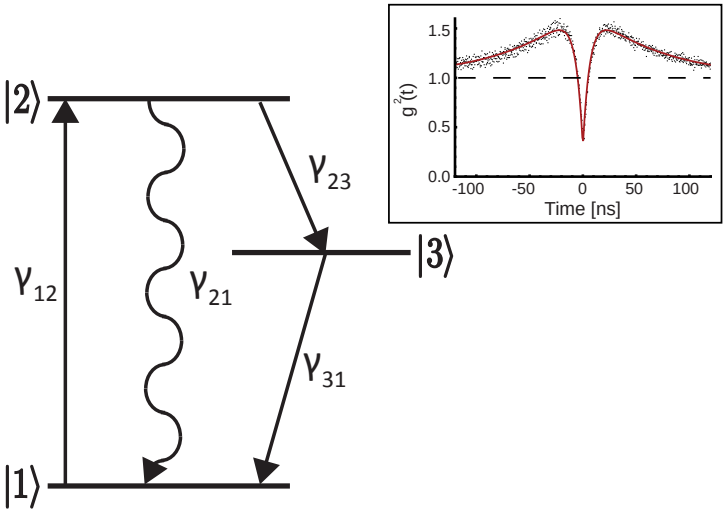


Figure 19: The simplified energy level structure of both a SiV and a NV centre and the different associated transition rates. The 3-level structure allows to explain the observed emission behaviour of the defect centres, especially when measuring $g^{(2)}(\tau)$ (see inset for measurement of a typical NV^- centre, taken from [7]). The observed values of $g^{(2)}(0) < 1$ are accompanied by a pronounced bunching.

Fluorescence emission is around 637 nm, that is where the phonon-free transition lies (zero phonon line (ZPL)). The NV^- centre shows emission strongly coupled

to phonons, making its spectrum very broad (100 nm full width at half-maximum (FWHM) at room temperature), see Figure 20. The Debye-Waller factor (DWF), indicating the ratio of emission into the ZPL to the overall emission is only about 3% at a temperature of 5 K [7].

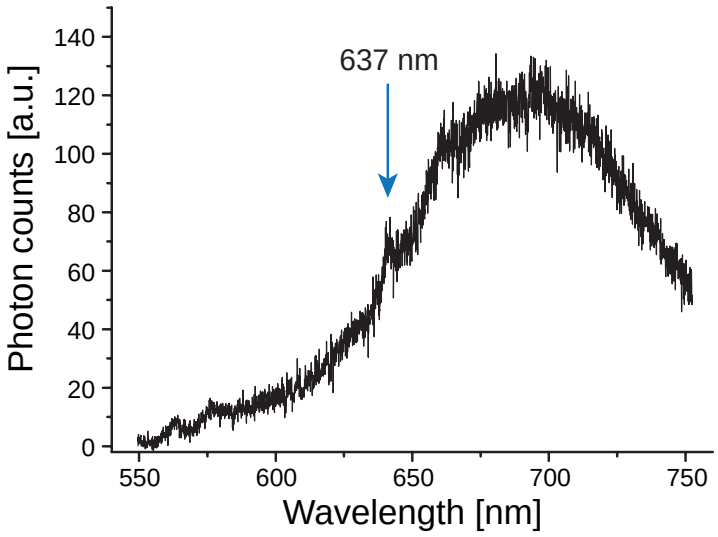


Figure 20: Spectrum at room temperature of a NV^- centre under 532 nm excitation. The ZPL at 637 nm can be seen. Taken from [7].

NV^- centres occur both in bulk and in diamond nanocrystals. In such nanodiamonds NV^- centres have radiative lifetimes τ_{rad} of $\sim 20\,ns$.

The quantum yield of the NV^- centre was shown to be upper bounded to 0.7 [116]. High count rates of up to 2.4 Mcts/s under continuous wave (CW) excitation have been reported [117].

The emission of the NV^- centre can be described by two optical transitions from two perpendicular dipole moments [118]. This limits the polarisation contrast of NV^- centres. That is a drawback when implementing the polarisation based BB84 protocol, as a linear polariser before state preparation blocks about 40-50 % of the overall emission.

5.1.2 The silicon vacancy centre

The SiV centre consists of a Si atom and a lattice vacancy in a so-called split-vacancy configuration (see Figure 21), where the substitutional Si atom relaxes its position in the direction of the lattice vacancy next to it [7].

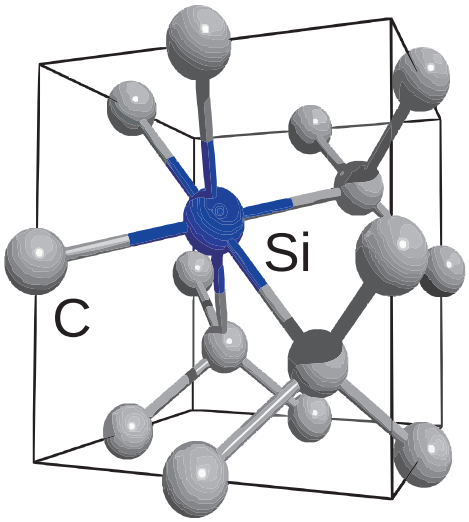


Figure 21: The atomic structure of the silicon vacancy (SiV) centre consisting of a substitutional silicon (Si) atom and a vacancy in the usual lattice of carbon atoms (C). Taken from [113].

The electronic structure can be approximated by a three level system as well and shows similar behaviour of the second order degree of coherence as the NV^- centre, see Figure 19.

The spectral emission for different centres is distributed around 738 nm with a typical linewidth smaller than 4.9 nm [7].

The radiative lifetime τ_{rad} of 0.2 to 2 ns is much shorter than for the NV^- centre, allowing a maximal theoretical emission rate larger than 5 GHz. However, the quantum yield in nanodiamonds was estimated to be only 0.01-0.09 % [119]. Nevertheless, high count rates up to 6 Mcts/s under CW excitation have been reported [113].

The SiV centre exhibits favourable linear polarisation visibilities up to 91 % [7].

Many SiVs centres in nanodiamonds show blinking and bleaching behaviour [7], limiting their suitability as stable SPS. However, SiVs centres with stable emission have been observed.

5.2 The experimental setup

The experimental setup consists of three parts, which are described in the following sections. The compact and versatile SPS will be introduced in the next section. The free-space testbed for BB84 QKD with polarised photons, which is usable over a broad wavelength range is presented subsequently. Finally, the control and data acquisition unit consisting of a field programmable gate array (FPGA) in conjunction with a personal computer (PC) is presented.

5.2.1 Compact and versatile design of a single photon source

The design of the SPS relies on a compact, portable and ready to use confocal microscope setup [7]. A hemispherical zirconium dioxide (ZrO_2) solid immmersion lens (SIL) can be utilized to enhance the collection efficiency of single photons emitted from defect centres in nanodiamonds spin-coated directly on the flat side of the SIL. Details of the fabrication of SILs with NV centres are provided in [117] or [7]. Figure 22 shows a schematic (a) and a photograph (b) of the source which fits completely on an aluminum plate and has dimensions of only $22.5\,cm \times 19\,cm \times 9\,cm$. Thus the SPS is mobile and can easily be integrated in different experimental setups. The setup is robust against mechanical vibrations and thermal drifts due to its small size and compact mounting of all optical components. The generated single photon beam can either be free-space or fibre coupled by removal/addition of a single mirror which is equipped with a magnetic base. The sample unit holding the defect centres can either be a SIL with spin-coated defect centres or another substrate due to a removable sample holder. The setup is equipped with broadband optics and thus suitable for various defect centres, provided their emission wavelength is in the range of 600 nm to 800 nm. Only the exchangeable dichroic mirror has to be adapted together with the suitable excitation source. The sample holder is mounted on a 3-axes piezo stage. In order to keep track of the absolute position of the stage, sensors capable of detecting changes down to a nanometre are used (SmarAct System). In combination with a numerical aperture (NA) = 0.9 objective it is possible to focus on a well defined position on the sample with very high accuracy and stability, enabling high, constant single photon rates.

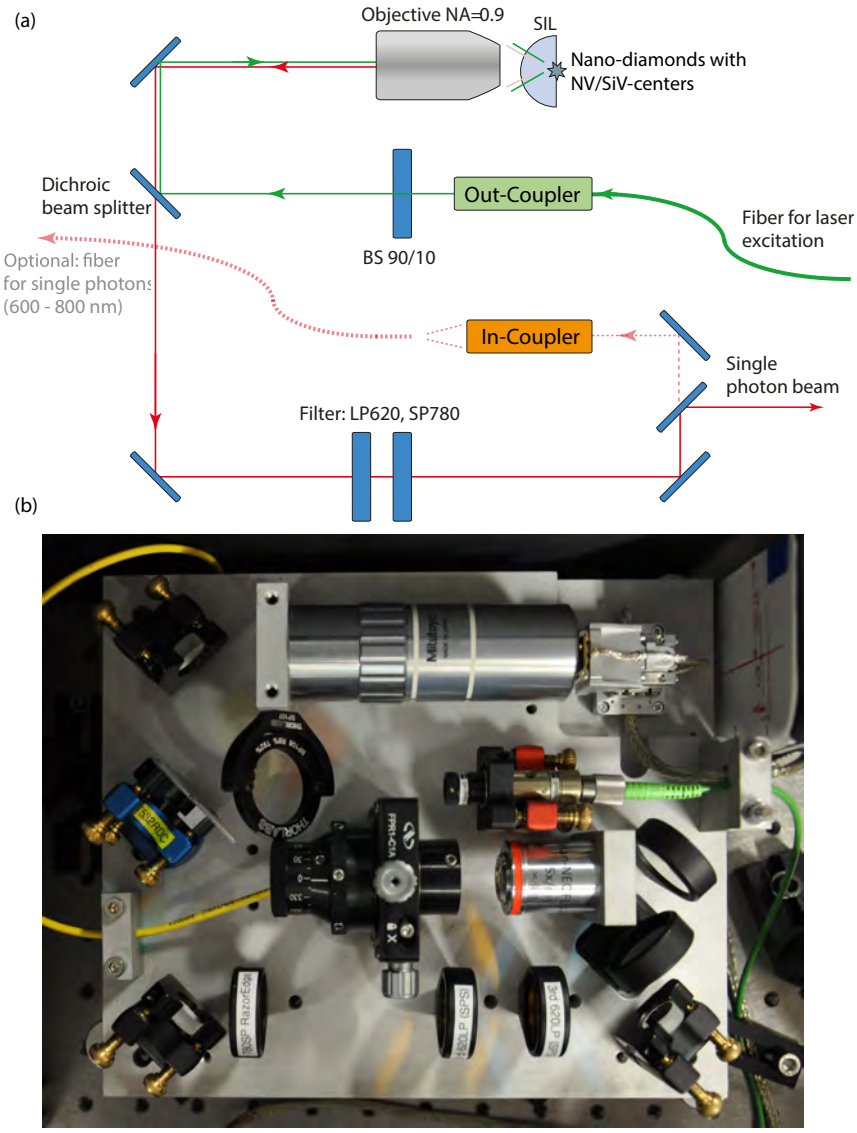


Figure 22: (a) Scheme and (b) photo of the compact confocal microscope setup. The excitation laser is focused with a high numerical aperture (NA) objective onto the sample. The sample contains nanocrystals that contain either NV or SiV defect centres. In the case of NVs centre, a SIL serves as the sample holder, enabling a higher NA for increased photon collection. The emission is collected by the same objective and then filtered by a dichroic beam splitter (exchangeable) and longpass (LP) and shortpass (SP) filters to clean it from residual laser light or fluorescence of the SIL or the substrate. The 90/10 beam splitter (BS) behind the out-coupler of the excitation laser is used to monitor the excitation power. Taken from [171].

In QKD it is favourable to use photons at a well defined instant of time, thus pulsed excitation of the defect centres is used. For the QKD experiment, the maximal excitation rate is limited to frequencies up to 1 MHz by the modulation rate of the EOMs (see below).

Alice uses a green diode laser (PicoQuant LDH-P-FA-530, 531 nm, pulse width <100 ps) for excitation at a rate of 1 MHz. This yields detected count rates at Bob's side for an NV^- centre in a nanodiamond which was spin coated on a SIL of about 8900 cps. That corresponds to an overall photon yield of 0.89 % and a source efficiency of 2.9 %. The latter is defined as the ratio of excitation pulses resulting in a single photon without background in the desired optical mode, here the free-space beam of the QKD experiment. It is determined, for a given overall photon yield, by taking the overall transmission t_{setup} of 0.31 of the setup, including the quantum efficiency of $\sim$ 65 % of the APDs (Perkin Elmer AQR), into account. A $g^{(2)}(0)$ value under pulsed excitation of 0.09, indicating high purity single photon emission, is determined (Fig. 23a) using high resolution time-correlation electronics (PicoHarp 300, from PicoQuant). A lifetime of 28.5±1.5 ns is estimated from the exponential decay of the fluorescence in time.

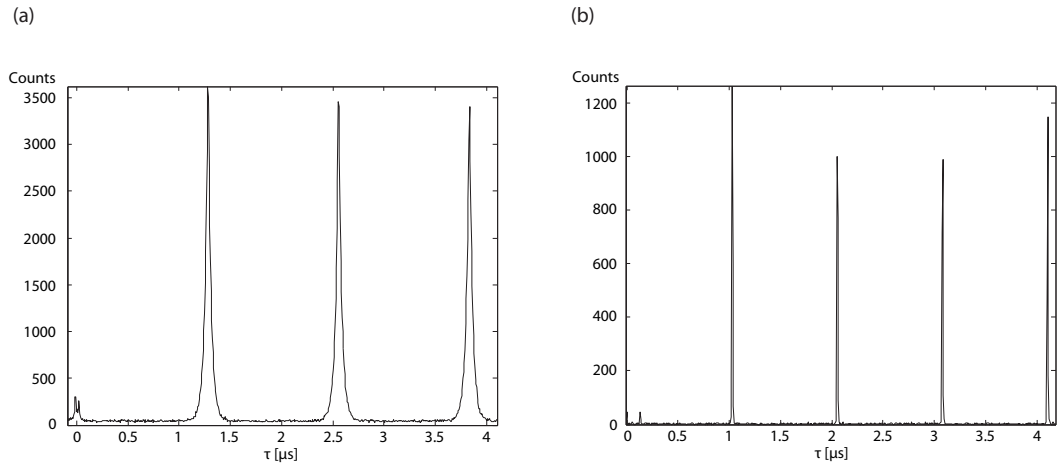


Figure 23: Measured intensities as a function of time for NV (a) and SiV (b) emission under pulsed excitation to calculate $g^{(2)}(\tau)$. The excitation rates are 800 kHz and 1 MHz, respectively. The missing peak at $\tau = 0$ indicates single photon emission. From the pulse shape, a lifetime of the excited state of 28.5±1.5 ns for the NV centre and 3±2 ns for the SiV centre is calculated. Taken from [171].

The single SiV centres used here are created during chemical vapour deposition (CVD) growth of randomly oriented nanodiamonds on Iridium (Ir) films [113] and have been supplied by the research group of Christoph Becher from the University

of Saarbrücken. During the growth process, Si atoms in the gas phase of the CVD chamber are incorporated into the diamond lattice. Subsequent annealing yields SiV centres. Excitation of the SiV centre is performed with laser pulses from a red diode laser (PicoQuant diode laser LDH-D-C-690, 687 nm, pulse width <100 ps) also at an excitation frequency of 1 MHz. For the brightest SiV centre a photon count rate of 3700 cps and a $g^{(2)}(0)$ value of 0.04 is achieved, see fig. 23b. From the exponential decay of the fluorescence peak, a lifetime of 3±2 ns is estimated. The overall photon yield is 0.37 % and the plain source efficiency is thus 1.2 %. The achieved count rate per excitation pulse is lower for the SiV centre compared to the NV centre. Knowing that the collection efficiency of emitted photons from SiV centres in nanodiamonds grown on Ir-substrate can be very high [119], this hints at a lower quantum efficiency. In [119], a quantum efficiency between 1-9 % is estimated. However, compared to the NV centre, the excitation frequency could in principle be chosen to be much higher for the SiV centre due to the shorter lifetime, which could compensate for the lower quantum efficiency.

5.2.2 Setup of the quantum key distribution testbed

The QKD setup is illustrated in Figure 24. The emitted free-space photons from the SPS are initially prepared in a linear polarisation state by passing through a linear polarisation filter after a $\lambda/2$ plate which is adjusted to maximise the transmission through the polariser. After passing through a pinhole for further spatial mode cleaning, the photons impinge on the first EOM which is controlled by Alice. The EOM can act as a half-wave ($\lambda/2$) or quarter-wave ($\lambda/4$) plate, respectively, depending on the applied voltage. In this way two orthogonal linearly polarised photon states as well as two orthogonal circular polarisation states can be generated, compliant to the BB84 protocol with polarised photons as described in Section 4.1. After a lens system for recollimation, the photons pass through a second EOM which is controlled by Bob. The transmission distance is in the order of meters. Bob randomly chooses a measurement basis by setting the EOM voltage such that it either does not modify the photons or acts as a $\lambda/4$ plate. A circular polarisation is thus transformed into a linear one or vice versa. The linear polarisation states can then be deterministically analysed in a system consisting of a polarising beam splitter (PBS), a linear polarisation filter, compensating the non-perfect contrast of the PBS in reflection, and two APDs. For the random bit and basis choice of Alice and Bob, quantum random numbers from the online random number service of Humboldt-Universität zu Berlin (HU Berlin) and PicoQuant GmbH (http:// qrng.physik.hu-berlin.de/, see also Chapter 8 and [172]) are used.

All used components are broadband. The EOM is constructed in a way that it

acts as a zero order waveplate. This minimises its wavelength dependency during the modulation of different polarisation states. Even so, especially when using the broadband NV centre as light source, possible dependencies between wavelength and transmitted polarisation state could open the door to side-channel attacks which would have to be analysed in way similar to the analysis of multiphotons (cf. 4.4.3). However, a thorough analysis of this problem is beyond the scope of this work.

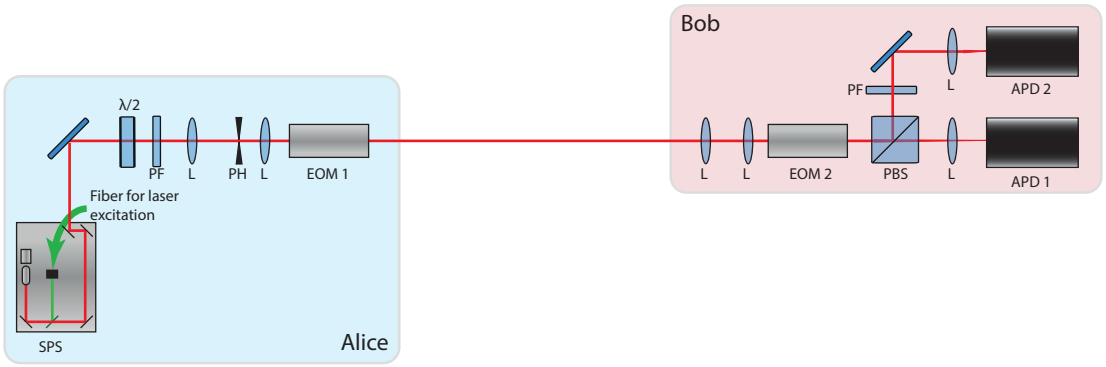


Figure 24: Schematics of the QKD testbed. Single photons are emitted from the source (SPS) and prepared in a well defined polarisation state by the $\lambda/2$ plate and a polarisation filter (PF). After collimation and spatial mode cleaning by two lenses (L) and a pinhole (PH), they pass through EOM 1. On Bob's side, the beam is recollimated by two lenses and then passes through a second modulator EOM 2). Then, the polarisation is analysed by a PBS and a polarisation filter in the reflected mode of the PBS. Its slightly reduced contrast compared to the transmitted mode with that linear polariser. After passing through a lens in each path for focusing, the photons are detected by one of two APDs. Taken from [171].

It should be noted that the QKD implementation is directly usable as a Hanbury Brown and Twiss (HBT) interferometer setup to measure the $g^{(2)}(\tau)$ of the SPS in use. For this, a constant polarisation with equal probability of projection onto horizontal and vertical polarisation states, i.e. any circular polarisation is set by means of the EOMs. In this way, the PBS in front of the APDs acts like a regular BS on incoming photons, implementing a setup as introduced in Section 3.4.2. The APDs have to be connected to fast time-tagging electronics in this case (PicoHarp 300 from PicoQuant).

5.2.3 Control and data acquisition

The whole experiment is controlled by a single field programmable gate array (FPGA) control unit (National instruments NI PCI 7813R) interfaced with a host PC via Peripheral Component Interconnect (PCI) Bus [175]. A FPGA is programmable hardware specifically useful to accomplish time critical tasks in parallel (cf. Section 7.1.3 for more information on FPGAs). For this purpose, the FPGA is equipped with many input/outputs (I/Os) to interface it with the device or setup which is controlled. The output signal logic is transistor-transistor logic (TTL) (see Section 7.1.2). The clock frequency of the FPGA is 40 MHz. The control algorithms are designed with a subset of the usual LabVIEW Code suitable for FPGA specific tasks. It is translated into low-level hardware description language used for actually programming the FPGA by a supplied software tool.

The control process of the FPGA consists of the several steps, see Figure 25. The process is started by acquiring random data from the PC, received from the quantum random number generator (QRNG) reported on in Section 8. The EOMs are set according to these random numbers which determine the used basis for Alice and Bob, respectively, as well as the sent state for Alice. This is accomplished by a 10 bit value which is output in parallel for each EOM. These values are transformed to analogue voltages by two homemade digital-to-analogue converters (DACs), see Section 7.1.3. The DACs need a trigger signal to read in the bits from the FPGA. The signals from the DACs are amplified to high voltages of up to ± 250 V by homemade EOM drivers. It is those drivers which currently limit the repetition frequency to 1 MHz. Once enough time is elapsed that the EOMs are set, the excitation laser of the SPS is triggered. The data acquisition is started by reading the outputs of the free-running APDs at a well defined instant in time after the laser trigger has been applied. The measured data together with the random bits and bases associated with it are transferred back to the host PC, where they are analysed to determine the sifted key rate and the QBER. It is also on the host PC that the post-processing is applied to the data (see next section).

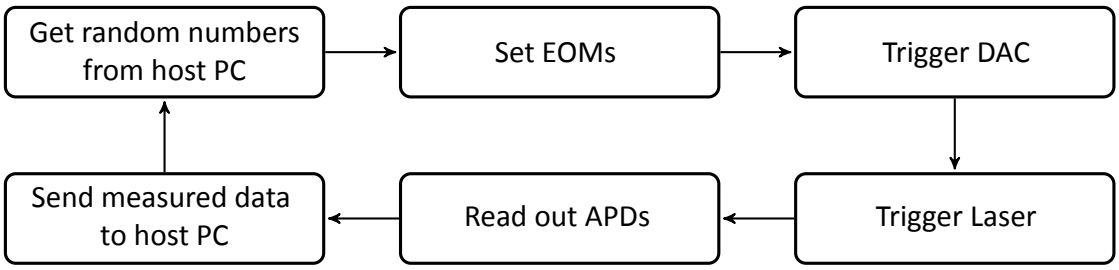


Figure 25: Flow chart of the processes the field programmable gate array (FPGA) controls during a typical cycle of the experiment. Taken from [175].

The principal parameters of the experiment can be set via a graphical user interface (GUI) programmed in LabVIEW and running on the host PC, see Figure 26. Those parameters comprise for example the bit values between 0 and 1023 (10 bit) for the EOMs of Alice and Bob (Alice Pool and Bob Pool in Figure 26). These values have to be determined experimentally beforehand. The repetition frequency is set by f_ratio (see figure) to $f = 40\,\mathrm{MHz}/\mathrm{f\_ratio}$. f_ratio thus determines the number of basic FPGA clock cycles per clock cycle of the QKD experiment. f_laser and f_read (see Figure 26) determine the FPGA clock cycle in which the laser is triggered and the APDs are read out, respectively. f_read is counted as number of FPGA clock cycles after the laser trigger has been applied, the actual cycle for the read-out of the APDs is given by f_laser+f_read. These and other parameters are communicated to the FPGA via the PCI Bus.

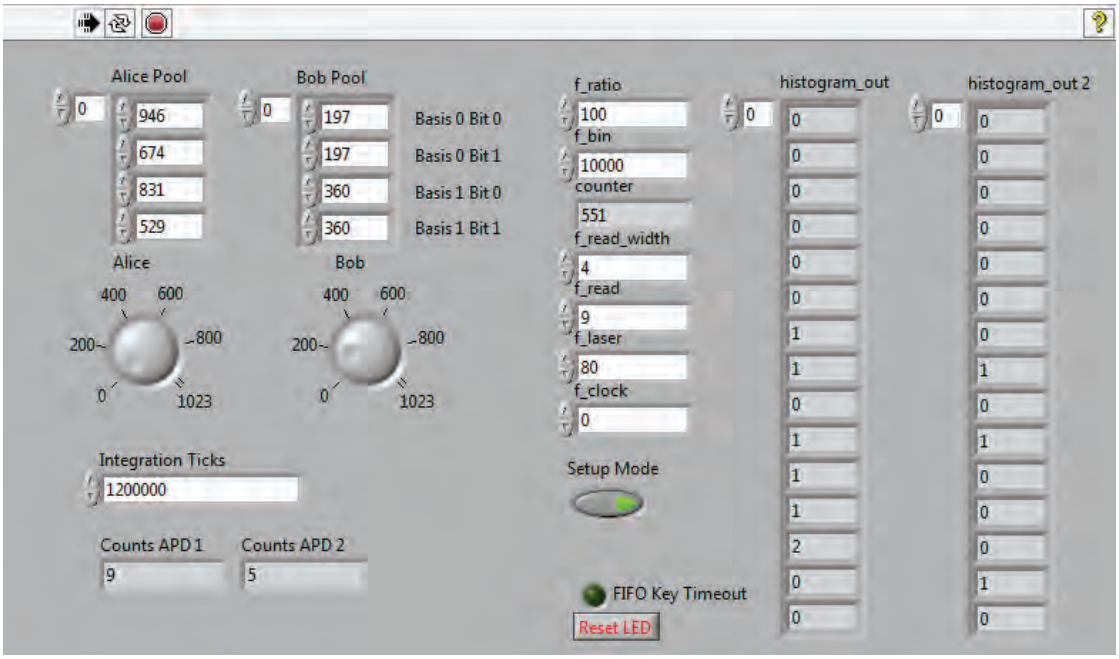


Figure 26: Graphical user interface (GUI) of the LabVIEW field programmable gate array (FPGA) module. Taken from [175].

5.3 CASCADE: the post-processing algorithm

As discussed in Section 2.3 before, a post-processing algorithm based on CASCADE [14] has been realised as part of this thesis. Details as well as the source code can be found in the master thesis of Robert Riemann [175] and can also be publicly downloaded (www.physik.hu-berlin.de/de/nano). Here, a brief summary of the most important ideas and their implementation shall be given.

5.3.1 Error correction

For error correction codes, there are three different important characteristics [14]. An error correction code can be (i) robust, (ii) optimal and (iii) efficient.

(i) An error correction code R being ϵ-robust with $\epsilon \in [0,1]$ expresses its probability of successfully conciliating to strings A and B of length n, thus producing a secret message S while exchanging information E. The process is described as $R(\mathrm{A},\mathrm{B}) = (S,E)$. An ϵ-robust code fulfills the following:

$$(\exists N_0(\epsilon))(\forall n \geq N_0(\epsilon)) \sum_{\alpha,\beta\in\{0,1\}^n} \mathrm{prob}(\mathrm{A}=\alpha,\mathrm{B}=\beta)\cdot \mathrm{prob}(\mathrm{R}(\alpha,\beta)=[\perp,\cdot]) \leq \epsilon$$

where $\perp$ indicates a failed run to generate a secret key.

(ii) An optimal code is an ϵ-robust code that does not exchange more information than necessary given an error probability p of each bit in B with respect to the original A:

$$\lim_{n\to\infty} \frac{I_E(S|E)}{nh(p)} \quad = \quad 1+\zeta \tag{95}$$

with $I_E(S|E)$ being the information Eve has on S given E. If a code is optimal, then $\zeta = 0$.

(iii) The efficiency of an error correction code is concerned with its run time: If there exists a polynomial $t(n)$ such that $\bar{T}(n) < t(n)$ for n sufficiently large, where $\bar{T}(n)$ is the expected run time of R acting on messages of length n, the code R is said to be efficient.

An ideal code is a code which is both optimal and efficient. There are unfortunately no known suited ideal codes for QKD. The resort are so-called almost ideal codes. Those are ϵ-robust and efficient codes with a $\zeta > 0$.

Such a code is realised in the CASCADE protocol. The realisation presented here works with parities of blocks of bits. A parity of block of bits is found by the sum of the bits modulo 2 or the XOR of these bits. In CASCADE, it works in the following way: first of all, an error estimation is done by taking 2% of the final key and comparing it publicly. By this, a suitable initial block size k_1 for comparing parities between Alice and Bob can be chosen such that there is on average maximally one error per block. The reason for that is that a parity check does not find an even number of errors. Of course, Alice's parity is the reference to which Bob's should agree. If the parity check on the block shows a disagreement, an error finding code called *Binary* is started. It subdivides the block successively

into blocks of half the length than the previous one and compares parities until the erroneous bit is found and flipped. Then, the block size is doubled, as is done right away if the parities of the initial block match. To detect an even number of errors undetected before, the bit order is randomized every time a block size is doubled. If for the larger block an error is found and corrected, the original block is checked again so that a previously even number of errors in it can now be detected. The same is done with the block of doubled size for the same reason. Every time the parities of two blocks match, their size is doubled until a final predetermined block size is reached. Then the error correction is terminated. The scheme of the algorithm is shown in Figure 27.

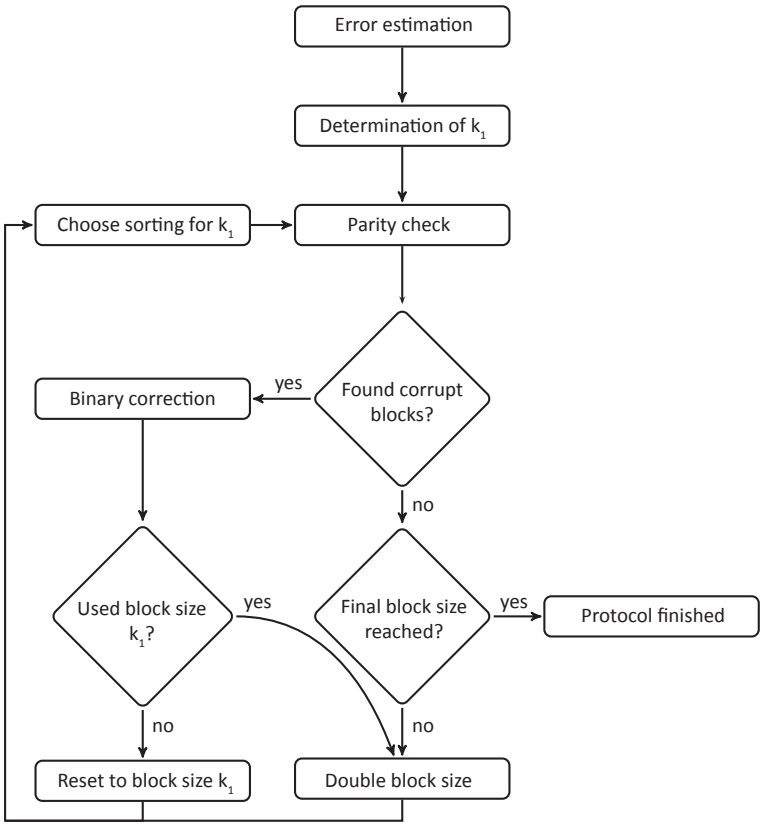


Figure 27: The error correction code based on CASCADE. Taken from [175]

5.3.2 Privacy amplification

The privacy amplification is supposed to vanish the information Eve has on the key from eavesdropping on the quantum channel and from the information distributed during error correction. This info I_E can be quantified (supposing single photon BB84) as $t = f(Q) \cdot n \cdot h(Q) - n \cdot h(Q)$, (cf. Equation 85) and has to be subtracted from the sifted key. This is accomplished by using compression functions g chosen at random from a set of functions $\mathcal{G}$:

$$g : \{0,1\}^n \rightarrow \{0,1\}^r, r = n - t - s \tag{96}$$

where n is the sifted key length (see Section 2.3 for the concept of sifting) and s is a security parameter. It can be shown [15] that Eve's knowledge of the resulting bit string K is bounded by $\frac{2^{-s}}{ln2}$ even if Eve knows the compression function (after the quantum transmission) if g belongs to a so-called universal$_2$ class of hash functions [40].

A possible set of functions fulfilling this requirement is the following:

$$\mathcal{H} \quad = \quad \{g_x : x \rightarrow [(c \cdot x) \mathrm{mod} 2^r] \in \{0,1\}^r | x, c \in \{0,1\}^r, c \text{ odd}\} \tag{97}$$

This set of functions is practical to implement in soft- and hardware and has another advantage: the odd random number c can be taken to be Alice's and Bob's basis choice, which is absolutely random and communicated only after the quantum transmission [15].

5.3.3 Authentication

All of the public communication steps beginning with sifting have to be authenticated. The underlying principle is to build checksums, or tokens, out of the message to be authenticated and a private random key as a digital signature. If the same private random key is possessed by the receiver, he can verify the checksum. It is very important to use an efficient algorithm for authentication which consumes as few bits as possible of the private key. This is fulfilled by a scheme proposed by Wegman and Carter [120] in which universal$_2$ hash functions are used. The scheme is depicted in Figure 28. The function itself used in every step of the scheme for compression is the same as for privacy amplification above, only adapted for the length of the message to be compressed and the resulting token. It could be shown that the scheme only consumes $\mathcal{O}(\log\ a)$ private key bits for authenticating a message of a bits opposed to $\mathcal{O}(a)$ for other schemes.

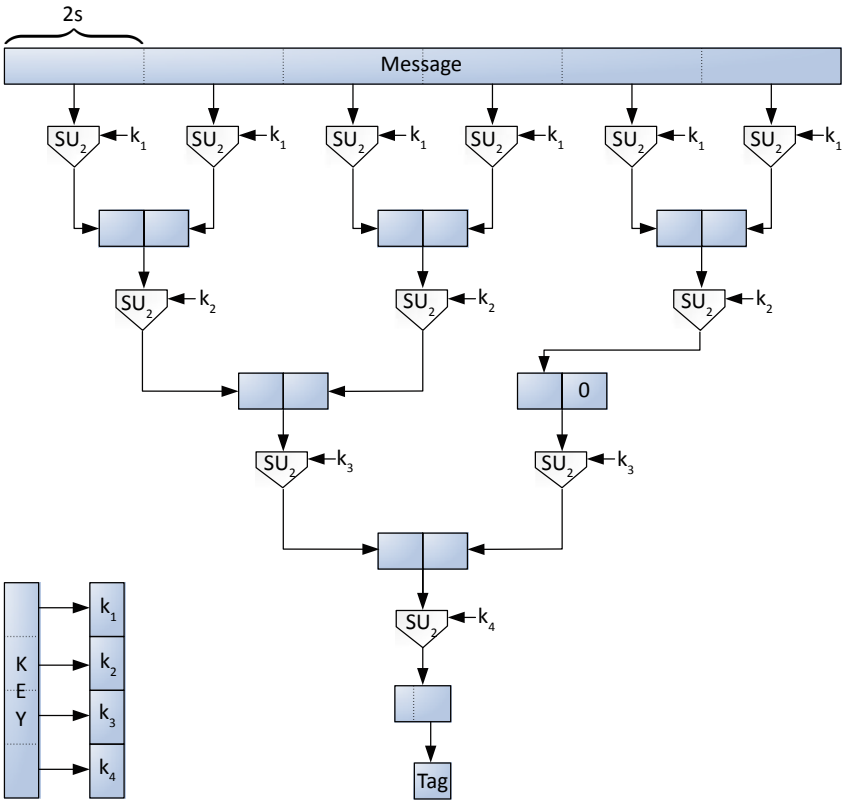


Figure 28: The authentication scheme. The message to be authenticated is split into parts of lengths $2s$ with $s = b + \log_2 \log_2 a$, where b is the length of the authentication token and a the length of the message. If necessary, zero-padding is added. The blocks of length $2s$ are then all compressed to length s using the appropriate function defined by the secret key k_1. Two resulting blocks are then concatenated and again compressed using a new key k_2. This is continued until a block of length s remains. The authentication tag is then simply the lower order b bits of this block. Taken from [15].

A typical scenario could be that an adversary has intercepted one message and the corresponding token and now tries to slip his own message to the designated receiver with a corresponding token guessed from his knowledge. It can be shown that the probability p_{guess} for the adversary to guess the token of size b correctly is [120]

$$p_{guess} < \frac{2}{2^b} = \frac{1}{2^{b-1}}. \tag{98}$$

The software is implemented using C++ and the cross-platform application framework Qt 4.7.4 provided by the Qt Project (http://qt-project.org). It is thus applicable on all major desktop platforms. Even though this experiment is controlled

by a single FPGA and thus there are no separated senders and receivers, the whole program is realised as two separate units for Alice and Bob which could be run on different platforms and which could communicate via TCP/IP. More details can be found in [175].

5.4 Results

The BB84 protocol is experimentally implemented with the two different SPSs, a NV^- and a SiV centre.

The results are summarised in Table 3. With the brightest NV^- centre with a detected count rate of 8.9 kcps, a sifted key rate of 4.0 kbit/s at a QBER of 3.0 % is achieved. The raw key is then further processed using the CASCADE protocol, resulting in a secure key rate of 2.6 kbit/s. The observed QBER can be attributed to the limited contrast of the polarisation optics and the EOMs.
Using the brightest stable SiV centre with a detected count rate of 3.7 kcps, a sifted key rate of 1.5 kbit/s, a QBER of 3.2 % and a resulting secure key rate of 1.0 kbit/s is demonstrated. The keys are transmitted at an experimental clock rate of 1 MHz.

Both NV and SiV centres are showing a stable emission rate over several hours. This indicates the long-term stability of the setup and the defect centres.

	NV	**SiV**
Repetition rate	1 MHz	1 MHz
Count rate	8.9±0.1 kbit/s	3.70±0.04 kbit/s
Sifted key rate	3.99±0.05 kbit/s	1.51±0.02 kbit/s
QBER	3.0±0.2 %	3.2±0.2 %
Secured key rate	2.6 kbit/s	1 kbit/s

Table 3: Results of the QKD experiments with NVs and SiVs centres, each executed for 300 seconds.

The single photon sources (SPSs) implemented here do occasionally emit more than one photon at a time and thus make the QKD vulnerable to photon number splitting (PNS) attacks (see Section 4.4.3). It is thus interesting to have a look at the source efficiencies and the $g^{(2)}(0)$ values of the SPSs and their consequences on the security concerning multiphoton events.

An upper bound on the probability p_m to have multiphoton events in pulses emitted from a sub-Poisson light sources is given by [121],

$$p_\mathrm{m} \leq \frac{\mu^2 g^{(2)}(0)}{2}, \tag{99}$$

where μ is the mean photon number per pulse which is identical to the source efficiency. This upper bound can then be used to calculate a lower bound on the secure key rate R, which takes the insecurity of having multiphoton events into account. In fact, Equation 90 from Section 4.4.3 describes this with a $Y_1^\star$ given by

$$Y_1^\star = 1 - \frac{p_\mathrm{m}}{p_\mathrm{click}} \tag{100}$$

with the detection probability of a signal $p_\mathrm{click} \approx \mu \cdot t_\mathrm{total} + p_\mathrm{dc}$ [121]. t_total contains, besides the setup transmission t_setup (cf. Section 5.2.1), the transmission of the quantum channel. The dark count probability p_dc is 2.4×10^{-5}. Figure 29 shows secure key rates as a function of the channel loss.

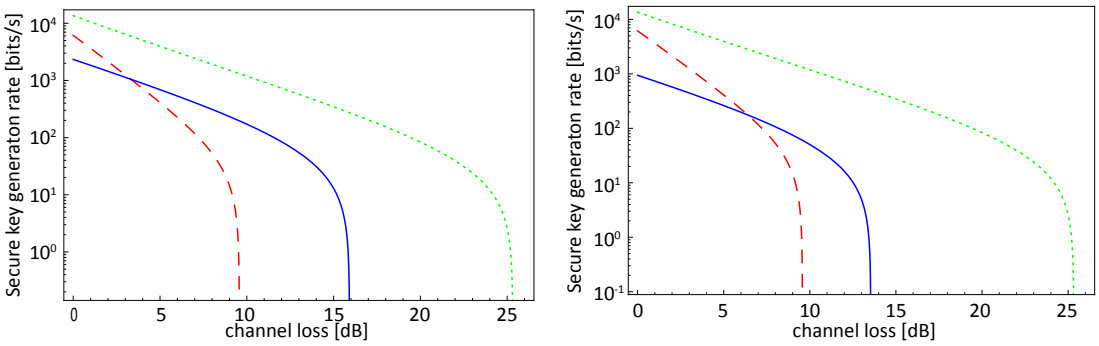


Figure 29: Secure key rates as a function of channel loss achieved with the BB84 protocol utilizing a SPS with an NV centre (a) and a SiV centre (b) in blue considering also possible multiphoton events. For comparison, the key rate when using an attenuated laser without the decoy state protocol at the optimised mean photon number $\mu \sim t_{total}$, where t_{total} is the overall transmission of the setup, is shown in red and dashed. Also shown in green and dotted is the secure key rate when using weak coherent pulse (WCP) together with the decoy state protocol with a mean photon number of 0.5.

The secure key generation rate at 0 dB roughly reproduces the measured secure key rate after post-processing. For comparison, the secure key rate of a potential experiment with identical parameters, but with an attenuated laser instead of a single photon source with a mean photon number of $\mu \sim t_\mathrm{total}$ (cf. Section 4.4.3) is also plotted. The key rate is calculated as in Equation 90, taking the multiphoton probability of a Poissonian light source into account. Also, the key rate of an identical experiment with an attenuated laser source together with the decoy state protocol (the used mean photon number of 0.5 is calculated as in [110]) is shown, calculated with Equation 94. At low loss, attenuated laser pulses without the decoy state protocol have relatively high signal intensities and thus outperform the SPS. At a channel loss of > 3.3 dB for the NV centre and > 6.4 dB for the SiV

centre, cf. Figure 29, translating into distances $> 8\,\mathrm{km}$ and $> 16\,\mathrm{km}$ using a typical transmission of light through air in sea level of $0.4\,\mathrm{dB/km}$ [122] the SPS provides higher secure key rates and longer achievable transmission distances. However, for the parameters achieved here, an attenuated laser together with the decoy state protocol is still favourable over the SPS regarding maximum key rates and achievable distances. This is because the obtained efficiencies of the SPS is not high enough and at the same time the $g^{(2)}(0)$ value not low enough.

Finally, following this analysis, requirements on nearly ideal but still realistic SPSs are explored and their performance is compared with WCPs using decoy states. For this, the different parameters characterizing a SPS, like the quantum efficiency, the photon yield and the value of $g^{(2)}(0)$ are varied towards more favourable values. This could be achieved by integrating the defect centres in photon extracting architectures like three dimensional light guiding micro structures [123] and using narrow-band emitting defect centres which could be easily filtered against background fluorescence. A prerequisite would be to use emitters with quantum yields ~ 1. In Figure 30 the resulting rates are shown for different parameter choices. It can be seen that building a SPS which generates superior key rates than WCP with decoy states is challenging, but could be possible in the future.

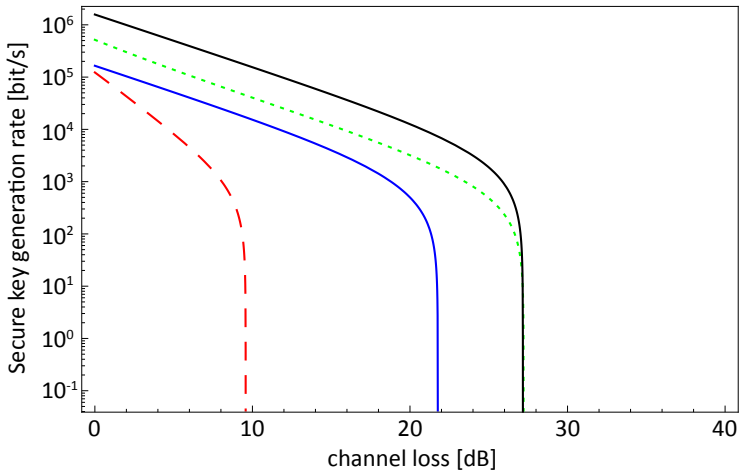


Figure 30: Secure key rates as a function of the channel losses of QKD experiments with defect centres with ideal but realistic features. For these sources, quantum efficiencies of 95 % and photon yields of 10 % (blue curve) and 95 % (black curve) are assumed. The $g^2(0)$ value is 0.005 (blue curve) and 0.0005 (black curve). For comparison, an attenuated laser without (dashed red curve) and with (dotted green curve) decoy state protocol is depicted as well. The repetition rate is assumed to be 20 MHz for all sources.

5.5 Summary

In summary, a QKD experiment including post-processing with a compact SPS using defect centres in diamonds has been implemented. The source is designed to be easily deployed in various QIP experiments. NV and SiV centres are used and can readily be interchanged within the experiment. SiV centres are potentially interesting for QIP applications due to their narrow spectral emission bandwidth but still suffer from drawbacks concerning their internal quantum efficiency and photostability, which have to be overcome in the future. Together with a thorough security analysis of the QKD experiment, taking into account the source efficiency as well as its $g^{(2)}(0)$ value, the requirement to test quantum light sources in realistic architectures has been discussed.

6 The frequency-time protocol

For fibre based quantum key distribution (QKD) linear polarisation is not ideal as a coding technique, because of its low robustness. Similarly, using the phase is also not ideal and typically complex alignment or stabilisation schemes have to be deployed. This motivates the use of different coding techniques as for example the time of arrival or the frequency of photons. In satellite communication, where the transmission channel is free-space, polarisation coding seems a good choice for QKD and has already been used in feasibility tests [124]. In this context it might however be problematic that classical optical satellite links generally use circular polarisation for duplexing communication [125, 126]. This would prevent using the same terminals for sender and receiver for classical and quantum communication. Also, the relative rotation of the coordinate systems of sender and receiver would demand complex alignment schemes once again [62]. This makes the use of frequency and time of arrival an interesting alternative for satellite QKD as well. These reasons motivate practical studies of QKD with photons in the FT protocol [127, 128, 129, 130], see also Section 2.6. From a technological point of view the FT protocol is advantageous since mature time and frequency-resolving measurement techniques are at hand, although there might be challenging demands concerning the timing jitter of photon detectors and the resolution of employed spectrometers. But these challenges can be dealt with well, as will be shown in this chapter reporting the first implementation of the FT protocol ever [173]. It is organized as follows: at first, in Section 6.1, the FT protocol is introduced. In the following Section 6.2, the conceptual peculiarities are highlighted by introducing three different intercept-resend attacks which do not exist in this form for the BB84 protocol. Then, in Section 6.3, the experimental setup of the implementation is introduced in depth. In the following Section 6.4, results are presented, including a security analysis on the aforementioned attacks. The chapter is closed with a summary and outlook in Section 6.5.

6.1 The protocol

The security of the BB84 protocol relies on encoding qubits in single quantum states in different bases which should be mutually unbiased. This maximises the sensitivity to eavesdropping attacks. Actually, each state of one basis can always be constructed as a superposition of the two states of the complementary basis with equal squared amplitudes each. The BB84 protocol is typically introduced in an implementation using polarisation, for example with the states $|H\rangle$, $|V\rangle$ in the rectilinear and $|+45\rangle$, $|-45\rangle$ in the diagonal basis or similarly with four different possible phases of a photon which are acquired and read out with two

unbalanced interferometers, see Section 4.2 and Chapter 7. The FT protocol encodes states which are seemingly very similar to those of BB84, but defined in time and frequency.

In the time basis, Alice creates one of two states $|0\rangle$ and $|1\rangle$ by temporally well-defined single photon pulses at two different possible instances in time, t_{0j} and t_{1j}, where j stands for the j-th bit sent. Each has a full width at half-maximum (FWHM) of δt, and $\delta t < \Delta t$, where Δt stands for the temporal separation of the two states, $\Delta t = t_{1j}$ - t_{0j}.

The frequency basis is represented, in analogy to the time basis, by a photon state with FWHM of δf at one of two possible frequencies f_0 or f_1. Here as well $\delta f < \Delta f = f_1$ - f_0. For his measurement, Bob chooses a basis at random and analyses either the frequency or the arrival time of the photon to find out which state has been sent.

To ensure a random outcome when measuring in the wrong basis, the overlap between any two states of a different basis should be large. So the temporal width $\delta\tau$ of the frequency pulse should be larger than Δt and the pulse should be sent at time $t_{2j} = (t_{1j}$ - $t_{0j})/2$. In frequency, the spectral width $\delta\nu$ of the time pulse should also be larger than the frequency separation Δf between the two frequency states. In addition, the central frequency of the time pulse should be at $f_2 = (f_1$ - $f_0)/2$. If one supposes a Gaussian pulse shape in time and in frequency, a pulse of a temporal width of δt has a spectral width of $\delta\nu = 0.44/\delta t$ and a pulse of spectral width of δf has a temporal width of $\delta\tau$ =$0.44/\delta f$. This is given by the time-frequency uncertainty relation or simply by the pulses' Fourier transformation. The formulated requirements on the parameters describing the time and the frequency basis can be summarised by the relations

$$\begin{aligned} \delta\tau &= 0.44/\delta f \sim \Delta t, && (101)\\ \delta\nu &= 0.44/\delta t \sim \Delta f., && (102)\\ \delta f &< \Delta f, && (103)\\ \delta t &< \Delta t, && (104) \end{aligned}$$

as well as

$$t_{2j} = \frac{t_{1j} - t_{0j}}{2} \quad (105)$$

and

$$f_2 = \frac{f_1 - f_0}{2}\,. \quad (106)$$

Figure 31 shows a scheme of the described Gaussian pulses in time and in frequency.

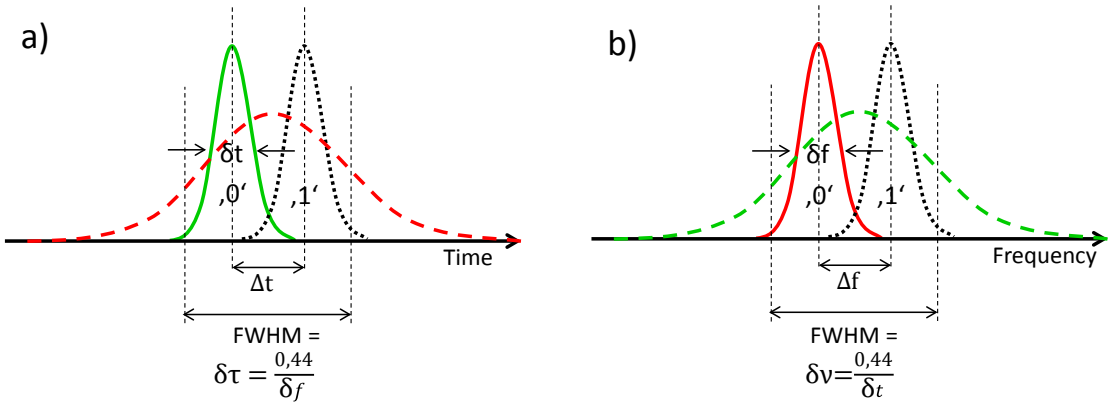


Figure 31: Scheme of the FT-protocol with Gaussian pulses in time (a) and frequency (b). The shape of the two possible states is shown as well as the shape of a state in its complementary basis (dashed). Taken from [173]

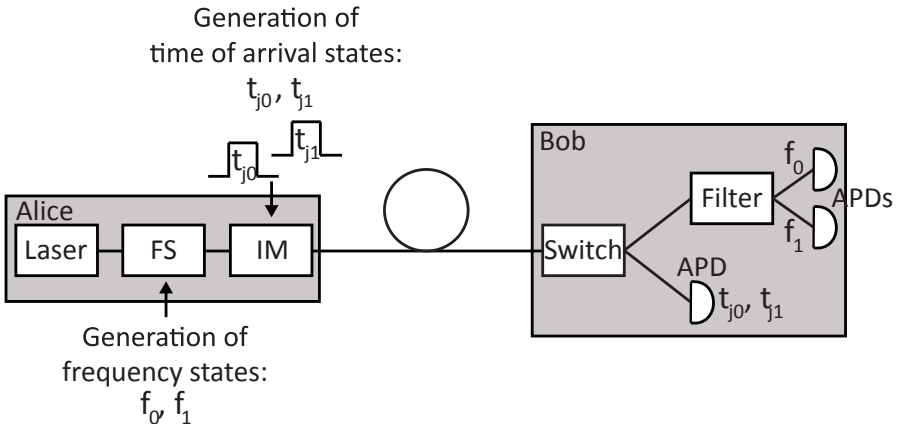


Figure 32: Schematic setup for the FT-protocol: A laser generates light at a given frequency, which can then be modified to generate frequencies f_0 or f_1. An intensity modulator carves short pulses at different instances in time to produce t_{0j} or t_{1j} or longer pulses to preserve the frequency information for the frequency basis. At the receiver, a switch is used for the basis choice. In one arm of the switch a fast avalanche photodiode (APD) measures arrival times for the time basis, whereas in the other arm the frequency is measured with a suitable filter. f_0 and f_1 are measured by APDs in each output of the filter. Taken from [173]

Figure 32 shows a possible setup to implement the FT protocol with an attenuated laser. A continuous wave (CW) light source emits light at frequency f_2 with a narrow spectral width. This frequency can be changed to f_0 or f_1 by a device to shift the frequency, generating two frequency states. An intensity modulator then

shapes pulses representing the different states. These can either be long with a spectral width of δf or short and at t_{0j} or t_{1j}, according to Equations 101-106. On the receiver side, a beam splitter (BS) (passive basis choice) or a switch (active basis choice) selects the basis. A fast single photon detector on one arm then measures the time basis. A suitable frequency filter on the other arm and one single photon detector on each filter output implements a measurement in the frequency basis.

The protocol then works as follows, in analogy to the BB84 protocol:

1. Alice chooses randomly and with uniform probability if she wants to send a state in the time or the frequency basis.

2. Alice chooses randomly and with uniform probability which bit she wants to send, thus if she wants to send a "0", corresponding to either t_{0j} or f_0, or a "1", corresponding to either t_{1j} or f_1.

3. Bob decides randomly with uniform probability in which basis he is going to measure.

4. Alice and Bob perform the sifting, thus they agree about the signals which have been received and which have been measured in the correct basis and discard the others.

5. Alice and Bob estimate the error by comparing a subset of the sifted key in order to bound Eve's information on it.

6. Alice and Bob perform error correction and privacy amplification.

This key can then be used to perform the one-time pad (see Section 2.1) over a classical channel.

6.2 Intercept-resend attacks: discussion of three different attacks

As described in Sections 2.8 and 4.4, the ultimate goal for any QKD protocol is an unconditional security proof. However, this can be complicated and for newly introduced QKD protocols it is a good starting point to think about individual attacks which are specific to it. This is the strategy adapted here. Having emphasized the similarities to the BB84 protocol before, the differences and their possible consequences on the security of the protocol are analysed in the following.

Two substantial differences to the BB84 protocol exist: first, two states within one basis are non-orthogonal, the exact overlap between the two depends on the parameter choice of δt, Δt, δf and Δf and on the pulse shape, which might not be Gaussian. This means that even in theory a measurement of a state sent by Alice in the correct basis might result in an error. In addition, if an eavesdropper for some reason sends an incorrect state to Bob albeit in the right basis, this state might not cause an error at Bob's side. This will play a role in the numerical calculations on the security presented in this and the following sections. Second, the actual Hilbert space describing the protocol is of infinite dimension as opposed to two dimensions, which is the case for BB84. So any possible state cannot be described as a superposition between two basis states and the overlap between two states of two different bases is not necessarily 50% as in BB84. Also the measurement cannot be described as a projection on one of only two possible states anymore, but the possibilities of projections are infinite and the appropriate measurement for a state is not anymore well defined. That has consequences on the security of the protocol. Without treating most general attacks, the treatment of three different individual attacks reveals those differences in the following.

The effectiveness of the intercept-resend attacks described in the following sections is analysed in a similar way here as it has been described in the intercept/resend eavesdropping section of [131]. The approach is as follows: first of all, one supposes that Eve attacks each bit individually without any knowledge about the basis which is used. In average, she makes a certain error measuring the state because of that, which results in a mutual information I_{AE} with Alice < 1 per sent bit, with $I_{AE} = H(A) - H(A|E)$ and H being the Shannon entropy (cf. Section 4.4.1). Eve will send a bit to Bob, which has a certain probability of causing an error at Bob and lessen his mutual information I_{AB} with Alice. To get a lower bound on the secure key rate, a well known relation of classical cryptography [132] is used (see also [13]),

$$\begin{aligned} S &= I_{AB} - I_{AE} && (107) \\ &= 1 - H(Q_{Bob}) - (1 - H(Q_{Eve}))\,, && (108) \end{aligned}$$

with S being the ratio of secured key bits which can be generated out of the sifted key bits. This basically states that a secure key can be generated as long as Bob has more information about the key Alice sent than Eve does. The second equality is valid in the case of individually attacked bits. Q_{Bob} and Q_{Eve}, respectively, are the average errors Bob and Eve encounter when measuring their individual bits. To calculate S, one needs to know the error Eve makes when applying a certain attack as well as the error this causes on Bob's side. The calculation is done here numerically using Matlab by simulating measurements of Eve and Bob and calculating their error. The exact approach is explained below in this section. The ultimate goal of the effected calculations is to consider different attacks, find the maximally tolerable QBER Q_{Bob}^{max} for which Alice and Bob can still generate a secure key given Equation 108 and compare it to the experimentally encountered error.

This is accomplished in two steps: first of all, different individual attacks, which are presented in the following sections, are simulated and the encountered errors of Eve Q_{Eve} and Bob Q_{Bob} are calculated. In a typical constellation, Eve cannot attack every bit since Bob's resulting error would be too high and no secret key would be generated. But Eve can attack a fraction d of the sent bits, resulting in an information of Eve on the key as well as an error of Bob proportional to d. That is why in a second step, the maximum fraction d_{max} which still enables Alice and Bob to generate a key is calculated. The corresponding error Q_{Bob}^{max} can then be compared to the experimental error. The results of these comparisons are presented together with the experimental results in Section 6.4.

For the numerical simulations of the attacks, first of all the time and frequency domains of interest are discretized by an appropriate number of points representing each. Signal pulses can then be described by amplitudes sampled at those points, filters by appropriate operations on the pulses over a range of points defining the filter width. Default Matlab functions, e.g. fft (fast Fourier transform) can then be used for the analysis. In the simulations, assumptions are made regarding the sent signals by Alice and Eve and regarding the time and frequency measurement techniques used. These assumptions are close to the experimental realisation. As will be discussed in Section 6.3.2.2, in the experiment the pulse shape in time and in frequency is determined in the time domain by Alice's intensity modulator. All pulses are more precisely described in time by rectangular pulses with half Gaussian-shaped edges than by Gaussian-shaped pulses. The spectral shape of the pulses is given by the Fourier transform of this shape in time, resulting in approximately sinc^2 shaped pulses.

The measurement process in both bases is approximated by a rectangular shaped filter in time and frequency, respectively. Bob has one such filter for each state of

both bases, which is centred around $t_{0j/1j}$ and $f_{0/1}$ and has a width of Δt and Δf, respectively.

Eve's measurement apparatus and her unit for sending pulses to Bob are specifically adapted to each of the presented attacks and are presented in the respective section below.

In the calculations, a signal which is measured outside of the filter associated with the correct state is counted as an error for Bob and Eve, respectively. With each pulse representing a state sent by Alice having an area normalised to one, the proportion of a signal ending up in one or the other filter directly gives the probability of this event and facilitates the calculation of errors. An example is shown in Figure 33 for illustration purposes. The simulated sent single photon pulse, a pulse representing the state $|t_{0j}\rangle$, has a pulse area equal to one. It is subject to a measurement effected by two filters, one centered at t_{0j} and the other one at t_{1j}, representing a measurement of the associated states. The part of the pulse area which lies outside of the correct filter is counted as an error, symbolised by the red areas as opposed to the green area representing a correct measurement. Since these areas describe the probability of the single photon pulse being measured at the associated times, the error is directly apparent.

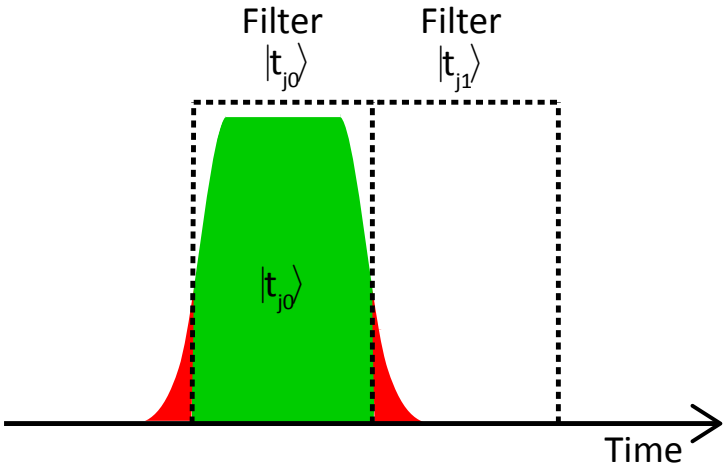


Figure 33: An illustration of the error calculations used in the numerical simulations. A pulse normalised to an area of one representing $|t_{0j}\rangle$ is measured by filters associated with both time states. The area of the pulse lying outside of the correct filter (red areas) directly gives the probability of an error for a single photon state.

The following sections present the three different individual attacks considered here.

6.2.1 The two bases attack

One such attack consists of Eve measuring a state in two bases consecutively, first in the time and then in the frequency basis or vice versa. Contrary to the BB84 protocol, in the FT-protocol not all information is erased by a measurement in the wrong basis. E.g. a measurement of a time pulse in the frequency basis broadens the pulse in the time domain, but it is still centred around a specific time t_{0j} or t_{1j} and contains information about the original qubit. The two different time states will have the same intensity profile in frequency, but their amplitudes differ and still contain the information about the state. So as long as Eve applies a frequency filter and then measures the intensity by detection, the two states will have the same probability for either frequency state and after detection, all information about the time is lost. But if Eve measures the frequency without measuring the intensity afterwards, the time information contained in the amplitudes might not be completely destroyed and a measurement in time afterwards might still extract some information about the original state.

A possible setup of Eve to exploit this is shown in Figure 34. In this exemplary setup, Eve measures first the frequency of an unknown state. Behind each output of the frequency filter, there is a second filter to implement a measurement in the time basis. Only after this second measurement, Eve detects in one of four outputs, each associated with a combination of information about frequency and time. Only when she learns about the actually sent basis in the sifting of Alice and Bob, she discards the information of the other basis. But first of all, before she has learned about the correct basis, she has to send a pulse to Bob. For this, she uses a special light source with which which she tries to convey both her measured time and frequency information, for example a pulse centred on t_{0j} in time and spectrally on f_1. Concerning the temporal and spectral width of the pulses, she has to make a trade-off such that they will cause the minimal average error when Bob makes a measurement.

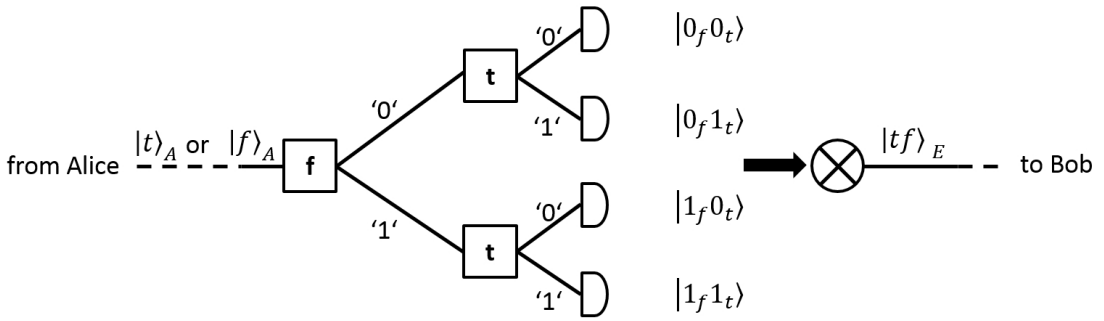


Figure 34: A possible setup for an intercept-resend two bases attack from Eve. Eve cascades the measurement in both bases of an unknown state and only detects after both measurements. She then sends a state that conveys both time and frequency information she measured.

This attack is simulated in Matlab by supposing that Eve uses two very broad rectangular filters both in time and frequency. This is assumed advantageous for her, because it modifies less the original pulse shape than the use of narrow filters. The two time filters are defined from t_{2j} (see Equation 105) over the whole time domain for $t < t_{2j}$ and $t > t_{2j}$ respectively. In the frequency domain, the filters are analogously defined. Both first a measurement in the time and first a measurement in the frequency basis are analysed separately to find out which one is more effective. This is of interest because in the simulation as well as in the actual experiment, there is no symmetry between the time and the frequency bases, e.g. the pulses have different pulse shapes. The specific pulse Eve sends, which conveys both time and frequency information she measured, is assumed to have a Gaussian shape. The pulse width in time and in frequency (both are related by $\delta f_{Eve} = 0.44/\delta t_{Eve}$) is optimised in the simulation by minimising Bob's averaged error for a pulse he measures half of the time in the time basis and half of the time in the frequency basis.

This is of course just exemplary and might not be the ideal realisation of this attack. The goal is rather to show the difference to the BB84 protocol and to see if the FT-protocol can still produce a secret key under the assumptions made here.

The comparison of the maximally tolerable QBER Q_{Bob}^{max} for this attack is presented together with the experimental results in Section 6.4.

6.2.2 The side filter attack

Another possible attack highlighting the differences between the FT and the BB84 protocol is the attempt to measure only parts of the time or frequency pulses, called the side filter attack. This attack exploits the fact that at e.g. $t/f \ll t_{0j}/f_0$ and $t/f \gg t_{1j}/f_1$, the probability to measure i) one state of the actual basis or ii) any state of the complementary basis might be much higher, depending on the exact parameter choice. As an example to illustrate both cases, Gaussian pulses sent by Alice are considered with parameters which are the same order of magnitude as in the experimental realisation. For case i), $\delta t = 50\,\text{ps}$ and $\Delta t = 2 \times \delta t = 100\,\text{ps}$, $\Delta f = 17.6\,\text{GHz} = 2 \times \delta\nu$, and $\delta f = 8{,}8\,\text{GHz}$. This parameter choice results in perfect symmetry between all states in time and in frequency, cf. Figure 35. It can also be seen in Figure 35a) that at $t < t^\star_{0j}$ and at $t > t^\star_{1j}$, the probability to find t_{0j} and t_{1j}, respectively, is much higher. So if Eve deploys special filters measuring only at $t < t^\star_{0j}$ and at $t > t^\star_{1j}$, she can directly determine the correct state with high probability. The situation is of course analogue in frequency, cf. part b) of the figure.

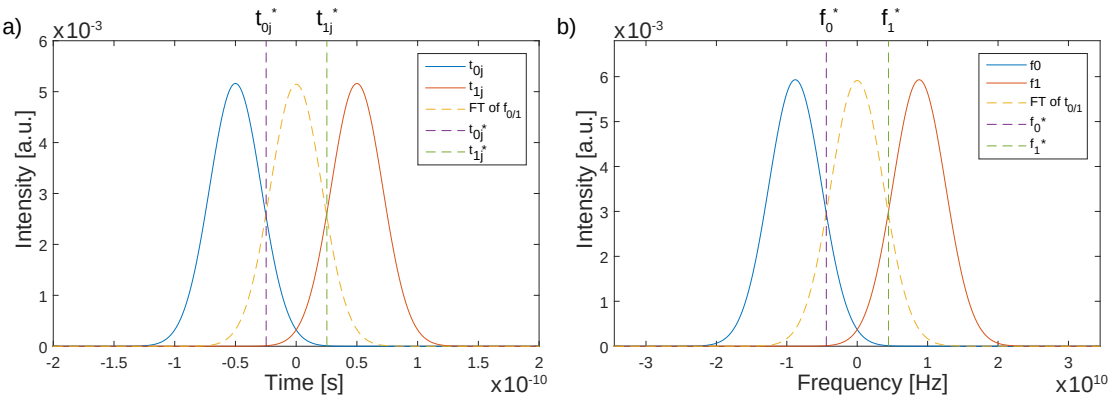


Figure 35: An example of a parameter choice which might be exploitable by Eve: a) the states $|t_{0j}\rangle$ (blue) and $|t_{1j}\rangle$ (red) are shown as well as any states of the frequency basis (orange, dashed). At $t < t^\star_{0j}$ and $t > t^\star_{1j}$, the probabilities of the respective states in the time basis are much larger than of any state in the frequency basis. b) the analogue is shown in frequency with the points of interest at $f < f^\star_0$ and $f > f^\star_1$.

Case ii) is encountered with the following parameter choice: $\delta t = 50\,\text{ps}$, $\Delta t = 100\,\text{ps}$, $\Delta f = 4.4\,\text{GHz} = 0.5 \times \delta\nu$, $\delta f = 2.2\,\text{GHz}$. This parameter choice results again in a symmetric arrangement of the states in time and in frequency, cf. Figure 36. It is also apparent in Figure 36a) that this time at $t < t^\star_{0j}$ and at $t > t^\star_{1j}$, the probability to measure a frequency pulse is higher than for a time pulse. The analogue in frequency is true at $f < f^\star_0$ and $f > f^\star_1$ as can be seen in Figure 36b).

So if e.g. in time Eve uses a filter analysing only the domains where a frequency pulse is more likely and then measures the resulting signal with frequency filters, she might gain an informational advantage, cf. the two bases attack of last section.

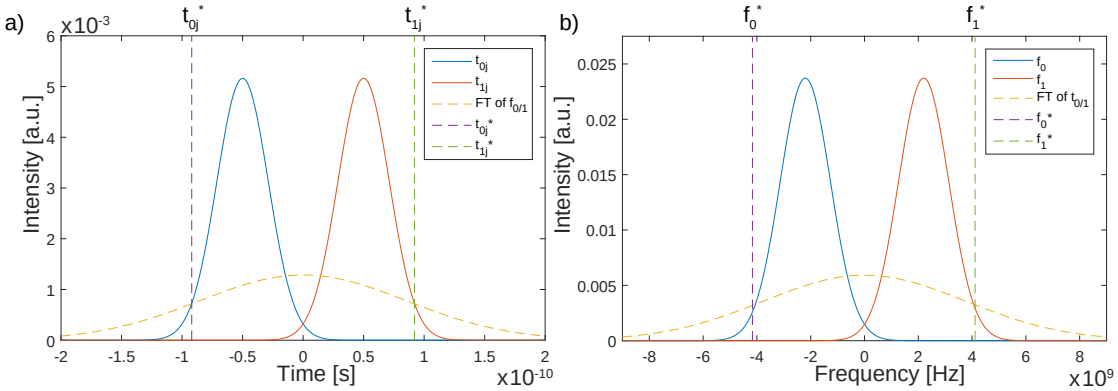


Figure 36: Another example of a parameter set which might be exploited in the side filter attack: a) this time, at $t < t^{\star}_{0j}$ and $t > t^{\star}_{1j}$ in the time domain and b) at $f < f^{\star}_{0}$ and $f > f^{\star}_{1}$ in the frequency domain, respectively, the probabilities for the states in the complementary basis become much larger.

This attack is simulated by first of all finding Eve's best measurement strategy. For this, the points $t^{\star}_{0j/1j}$ and $f^{\star}_{0/1}$, respectively, are calculated and Eve's filters are adapted. It is assumed that these points are the points where the probability for one state of the basis and its complementary basis are equal, just as in Figure 35 and 36. The position of these points with respect to the different states of both bases determines if strategy i) or strategy ii) is applied. It is assumed that Eve sends the same states as Alice but according to her measurement results.

Since the parameter choice is not necessarily symmetric, for example in the experiment implemented here (see Section 6.4), the strategy is evaluated in both bases individually. The overall efficiency of the strategy in terms of Eve's shared information I_{AE} with Alice and Bob in perspective to Alice's and Bob's information I_{AB} is calculated by averaging over both results. It is assumed that Eve must attack both bases with the same probability to keep a uniform probability for Bob to receive states in both bases.

It should be noted that the presented attacks do not represent all of Eve's possibilities. For example, when choosing different pulse shapes than Gaussian, as in this experimental implementation, the situation might be more complex and more complex filter shapes might grant Eve more information per error she causes at Bob's side. In addition, one can see in Figures 36 and 35 that in the middle between the two states of one basis there is also a higher probability to measure

a state of the complementary basis. This has not been taken into account here. Numerical tests suggest that this does not give a lot of advantage to Eve with the parameters chosen in the experiment, but in general it should be further examined in future security analyses of this protocol.

6.2.3 The classical intercept-resend attack

To conclude this section about specific individual attacks on the FT protocol, the basic intercept resend attack is treated, see Section 2.2 in the context of the BB84 protocol. The only difference here with respect to the BB84 protocol is that there is an intrinsic error when measuring in the right basis due to the non-orthogonality of states within a basis. This has to be taken into account when calculating the mutual information of Alice and Bob and Alice and Eve. It also plays a role when Eve measures in the correct basis and sends the measured state to Bob. It might be the correct state and still cause an error or might be the wrong state without causing an error. This has to be taken into account when calculating the efficiency of this attack. Due to the fact that the states within a basis are almost orthogonal with the parameter choice implemented here, the efficiency of the intercept-resend for the FT protocol attack is very similar to BB84.

6.3 Experimental setup

The goal of the experiment is to show the feasibility of the FT protocol with existing, mainly off-the-shelf telecom components. The use of mainly telecom components for the optical setup constrains the possibilities of using frequency filters with a very high frequency resolution. Here, an optical interleaver for dense wavelength division multiplexing (DWDM) with a resolution of 12.5 GHz is used. This determines the minimal timing resolution to about 35 ps assuming Gaussian pulses, see Equations 101 and 103, which cannot be achieved directly by using standard APDs. That is why the setup introduced above in Figure 32 has to be modified in the following way: the switch is used not only for the basis choice but also to implement the temporal resolution necessary to distinguish the two states of the time basis. This is accomplished by switching one time state to output 1 and the other state to output 2, cf. Figure 37. Fortunately, fast optical and electronic equipment to achieve this is at hand. The frequency shifting of the laser is accomplished by a direct modulation of the current which drives the laser, the intensity modulation to shape short time or longer frequency pulses is achieved by a Mach-Zehnder modulator (MZM), cf. Figure 37. The experiment is performed over a transmission distance in the order of 10 m which does not compromise the

intended feasibility test.

The truth Table 4 associates clicks of the APDs with possible sent and received states for this setup.

Alice			**Bob**		
Basis	**Bit**	**State sent**	**Basis**	**Click APD no.**	**Bit received**
f	0	$\|f_0\rangle$	f	1	0
f	1	$\|f_1\rangle$	f	2	1
f	0	$\|f_0\rangle$	t	1, 2 or 3	?
f	1	$\|f_1\rangle$	t	1, 2 or 3	?
t	0	$\|t_{0j}\rangle$	t	1 or 2	0
t	1	$\|t_{1j}\rangle$	t	3	1
t	0	$\|t_{0j}\rangle$	f	1 or 2	?
t	1	$\|t_{1j}\rangle$	f	1 or 2	?

Table 4: Truth table for the setup of the frequency-time (FT) protocol.

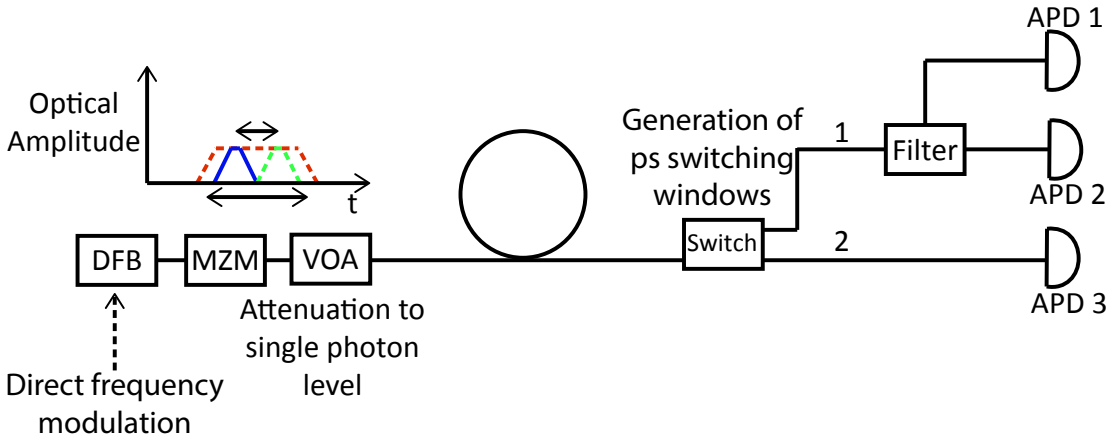


Figure 37: A modified setup for the FT protocol. A current modulated distributed feedback (DFB) laser emits continuous wave (CW) light which is modulated by a Mach-Zehnder modulator (MZM) and attenuated by a variable optical attenuator (VOA). On the receiver side, a switch directs all light to the frequency filter for a measurement in the frequency basis. For a measurement in the time basis, the state at t_{0j} is switched to output 1 whereas a state at t_{1j} is switched to output 2. Three avalanche photodiodes (APDs) are used for detection.

The complete setup is more complex. It is shown in Figure 38. It can be subdivided into different parts, described in the following sections. At the heart of the setup is the **bit pattern generator (BPG)**. This device provides the basic electronic signal controlling the experiment via a digital pattern of logical bits and supplies

the overall time frame. The **frequency-modulated laser** is the CW light source of the experiment. Two **intensity modulators** (MZMs) (intensity-mod and pulse carver) are used to shape short pulses for the time basis or longer pulses for the frequency basis. These are then attenuated to single photon level (Variable optical attenuator-VOA). On the receiver side there is a **switch** in form of a double output Mach-Zehnder modulator (DOMZM) which allows making a measurement in the time base by switching t_{0j} to one and t_{1j} to the other output or directs all the light to the **interleaver** which allows measuring the frequency of the optical signal for the frequency base. The measured signals are then **detected** by three APDs. Finally, **data analysis** is implemented with a real-time sampling scope and offline data processing.

As can be seen in Figure 38, the receiver outputs leading to the APDs can be coupled to a digital channel analyzer (DCA) via optional 3 dB couplers (dashed blue lines). This DCA is equipped with appropriate photodiodes to detect unattenuated classical signals. It has been used frequently to calibrate and characterize the system.

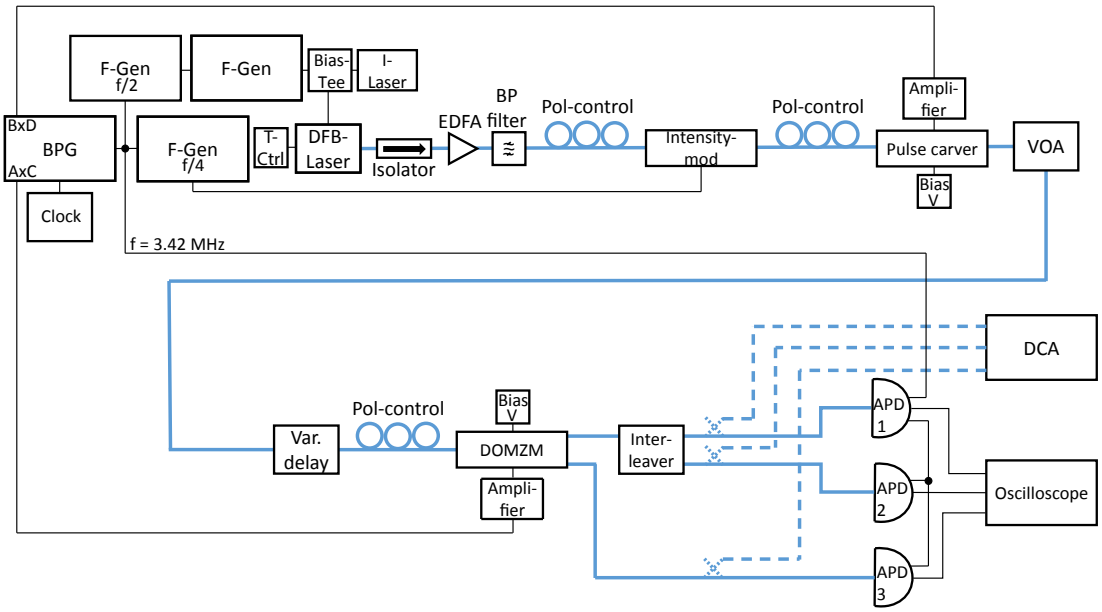


Figure 38: Detailed scheme of the experiment. Black fine lines represent electronic connections, blue thicker lines optical fibre links. Taken from [173].

6.3.1 The bit pattern generator

The SHF 12103 A BPG is able to generate sequences of electronic digital signals in form of pseudo-random or individually programmable bit patterns. It is usually employed to generate electronic signals which are used to test the performance of optical setups, typically for telecommunication purposes.

The BPG controls all basic processes of the experiment, all the non-grayed-out parts of Figure 39 are directly or indirectly driven or triggered by it.

It provides signals at a very high rate, which are used for controlling the pulse shaping on the sender and switching on the receiver side. Also the basic clock or repetition rate of the experiment, which has a lower frequency, is provided. For this purpose, various outputs of the BPG (see Figure 40) are used.

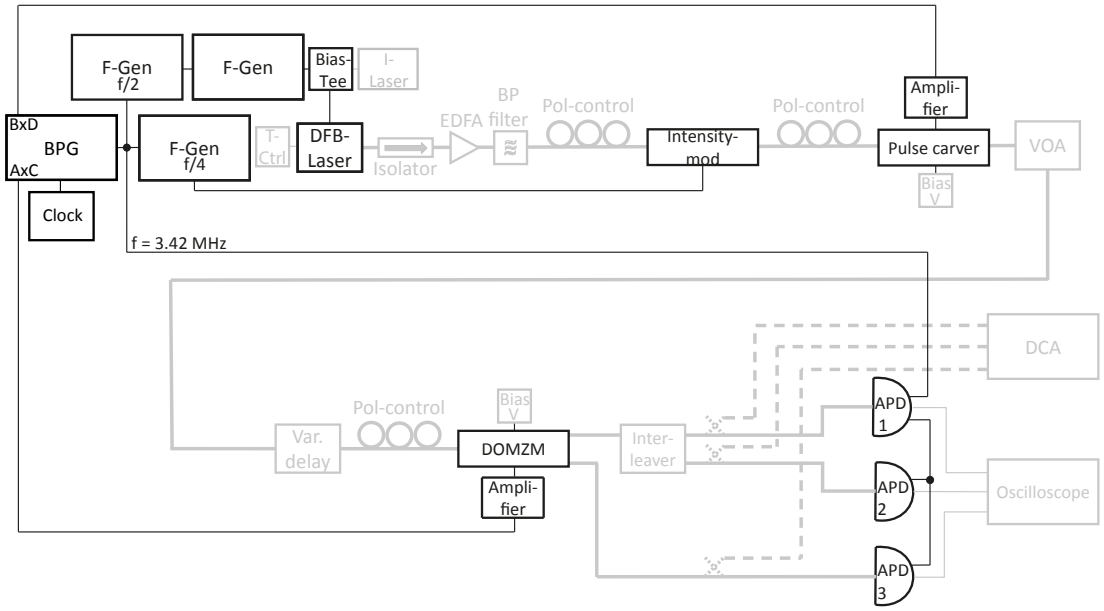


Figure 39: Non-grayed-out all parts which are directly controlled by the bit pattern generator (BPG).

Figure 40: The various outputs of the SHF 12103 A bit pattern generator (BPG). Taken from [133]

The pattern on which the output signals are based is a sequence of logical bits, thus zeroes and ones, which are individually programmable through a graphical interface, cf. Figure 41. The ensemble of blue and green lines in the figure, respectively, correspond to sub-patterns which are output at different outputs of the BPG, the $A \times C$ and $B \times D$ outputs. Each little line corresponds to an individual bit which can be set to "high" (0) or "low" (1) by a mouse click. The patterns can also be loaded from external files. The total length of the pattern can be chosen to be arbitrarily long up to the maximal memory capacity. The pattern is run through with a rate determined by an external clock. Once the whole pattern has been run through, it is repeated.

The output corresponding to a bit of value "0" or "low" is $-V$, for a "1" or "high" bit it is $+V$, where V is the adjustable voltage amplitude.

A separate output can provide a much slower trigger signal, the so-called frame out. Its frequency can be programmed by choosing an integer divisor of the clock frequency which can be chosen to be sufficiently large to output a trigger signal once per pattern period, for example.

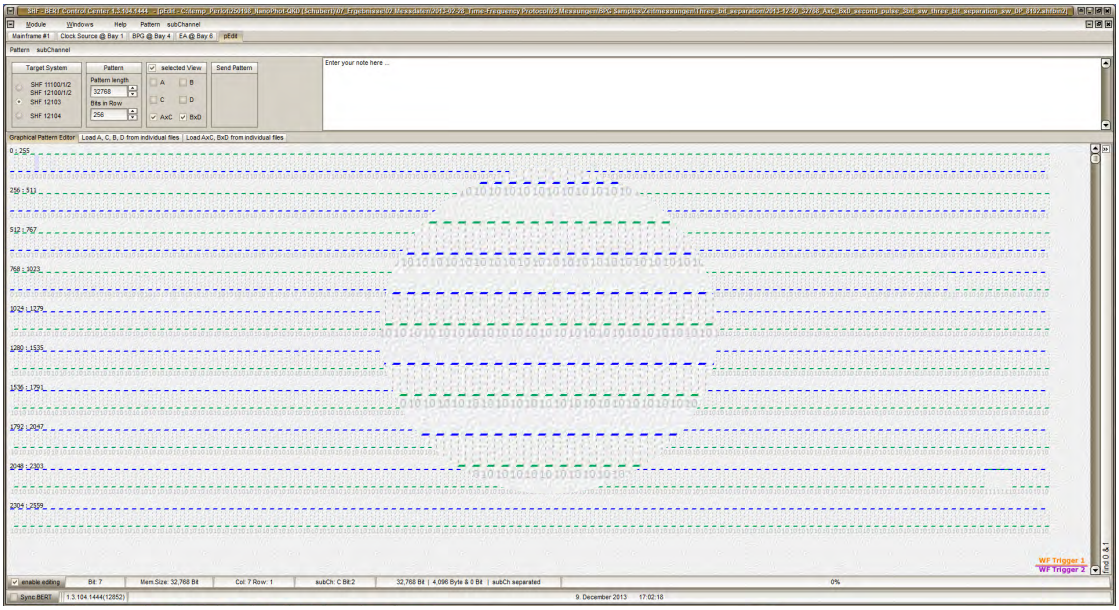


Figure 41: The graphical user interface (GUI) to control the pattern output by the bit pattern generator (BPG), the zoomed in part shows the two sub-patterns (blue and green) in more detail.

The maximal timing resolution of the BPG is given by its smallest programmable unit, the single bit. When used at its maximal bit rate of 56 GBps, this means

that the duration of the electronic output signal representing a single bit is 18 ps. To achieve this bit rate, an appropriate external clock has to be used. Here it is provided by the SHF 78210 B synthesized signal generator. It provides a 28 GHz signal which is internally doubled in frequency within the BPG.

The pattern used here has a length of 65536 bits. Given the clock frequency, this results in a pattern repetition frequency of 854 kHZ. Within one of the sub-patterns, there are two sequels of several bits each (6-20, see Section 6.4) which are set on "high" representing the temporally long pulses of the frequency basis. These bits on "high" level set the MZM for shaping of the pulses (pulse carver) on maximal transmittance, whereas a "low" bit minimises the transmitted intensity. Within each pattern, there are also two sequels of several bits each (typically two, see Section 6.4) set on "high", each representing of the two possible time states. All four bit-sequences representing signal states are evenly spaced within the pattern (save the Δt, typically 72 ps or 4 bit, between the two possible time states). The signal frequency is hence 3.42 MHz. The frame out providing the basic clock of the experiment is thus set to this frequency. In the other sub-pattern there are two sequels of severals bits (typically 4, see below) put on "high". They are used for switching the state $|t_{1j}\rangle$ to APD 3 by setting the DOMZM to maximal transmittance at the corresponding output. All other signals are to be transmitted towards its other output, which is achieved by applying "low" bits for the rest of the pattern. To facilitate the application of the switch bits at the right instant in time at the DOMZM, this sub-pattern can be shifted with respect to the other.

Because of the predetermined ever-repeating pattern, the order of different sent signal states is deterministic. Also, the switching is only applied for the time basis, all states are measured in their corresponding basis and no sifting is needed. This is acceptable in an experiment proving the feasibility of the protocol with available equipment. For the data processing used here, the deterministic results even present an advantage, cf. Subsection 6.3.4.

The relative long pattern length results in a relatively low repetition frequency of the QKD experiment of 3.42 MHz. This is practical due to two reasons. First of all, available function generators (F-Gen*s* in Figure 39) are used for further reducing this frequency by frequency division. They are needed for the generation of auxiliary signals necessary for the experiment. Those function generators do not support much higher frequencies. Second, the behaviour of the current modulated laser is not known for higher modulation frequencies and terminal damage of the laser could result.

The maximum amplitude of the BPG is too small to drive the MZMs and the DOMZMs directly. Hence, in front of each modulator, there is a fast electronic amplifier (SHF 806 E). Those amplifiers are alternating current (AC)-coupled and

need a zero-mean input signal to work properly. Since in the original pattern of 65536 bits, there are only very few ones representing the actual signals and thus predominantly only zeroes, the resulting signal does have a mean very close to $-V$. This is why large blocks of 512 bits each with "high" level are programmed throughout the pattern alternating with blocks of 512 bits each on "low". Within the latter, there are the actual signal bit sequences.

Three different outputs are used for the purpose of controlling the experiment, cf. Figure 40: there are the high-speed $B \times D$ and $A \times C$ outputs, which output the two sub-patterns. These outputs are a specialized variant of the SubMiniature version A (SMA) connectors apt for the high frequencies in use, the so called K-type. Semi-rigid high-quality coaxial cables are used to connect them to the final devices. The standard SMA *Frame out* output is used to provide the basic clock rate of the experiment of 3.42 MHz.

Some specific aspect of the BPG signal generation and application will be addressed in more detail in some of the following subsections.

6.3.2 Light generation and modulation

The sender can be divided into two parts: one part for the generation of the frequency modulated attenuated light signal and one part for the modulation of the light. They are described in the following two sections.

6.3.2.1 The frequency modulated light source

The light modulation scheme is shown in Figure 42. A temperature controlled (Profile TED 200 temperature controller, T-Ctrl in the figure) DFB laser emits coherent light in CW mode at a wavelength of 1582 nm. The frequency modulation is done by applying a pattern of appropriate voltage pulses added via a bias tee to the constant current supply of the laser (Digistant 6426, I-Laser in the figure). The injection current modulation from the voltage pulses leads to carrier density modulation and temperature change effects that induce the desired frequency modulation (cf. [134], p. 68). The voltage pulses are output from a function generator (Wavetek 164, F-Gen in the figure) and are adapted in shape and amplitude such that the desired frequency modulation amplitude is achieved. This is accomplished by a skewed sinusoidal signal. Figure 43 shows a screenshot of the intensities at the outputs of the used frequency filter for unattenuated frequency modulated cw light, measured by the DCA (in this demonstration measurement, the intensities seem different due to differently attenuating fibres used).

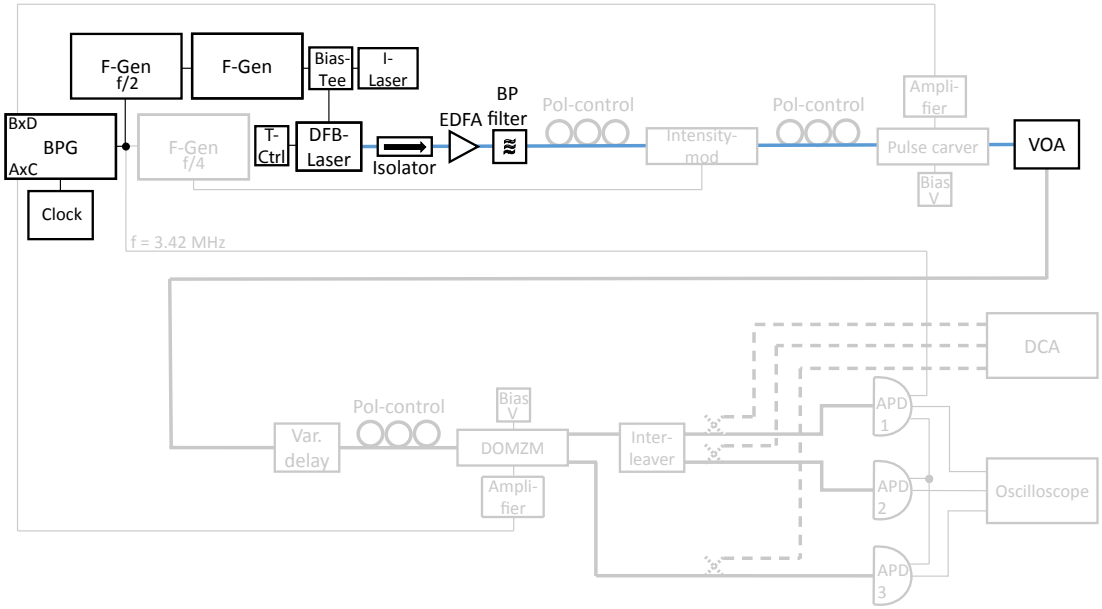


Figure 42: The non grayed-out parts show all components which compose the frequency modulated light source.

The two generated frequencies are separated by approximately 10 GHz, as is measured by a heterodyne spectral measurement. In this type of measurement, a laser with a precisely known frequency and the frequency modulated signal are mixed on a BS before detection by a photodiode. The resulting beat signal gives direct information about the difference frequency. It should be noted that for this measurement the frequency is statically changed between the two target frequencies states by applying the associated voltage amplitudes statically to the laser.

To assure that the pulse shaping of the signal states and the frequency modulation are in phase, the frequency modulation is synchronised to the rest of the experiment. This is achieved by dividing the basic clock rate by two with a function generator (F-Gen, HP 3314 A). The function generator used for the laser current modulation is synchronised to this one, see Figure 42. In this manner every second pulse is frequency modulated with respect to its predecessor, regardless if it is a signal in the time or the frequency basis. This differs from the original protocol (cf. Equation 106) but is necessary due to technical reasons. The exact phase of the modulation with respect to the clock frequency can be set with the HP 3314 A function generator such that the frequency modulation is applied at the right instant in time.

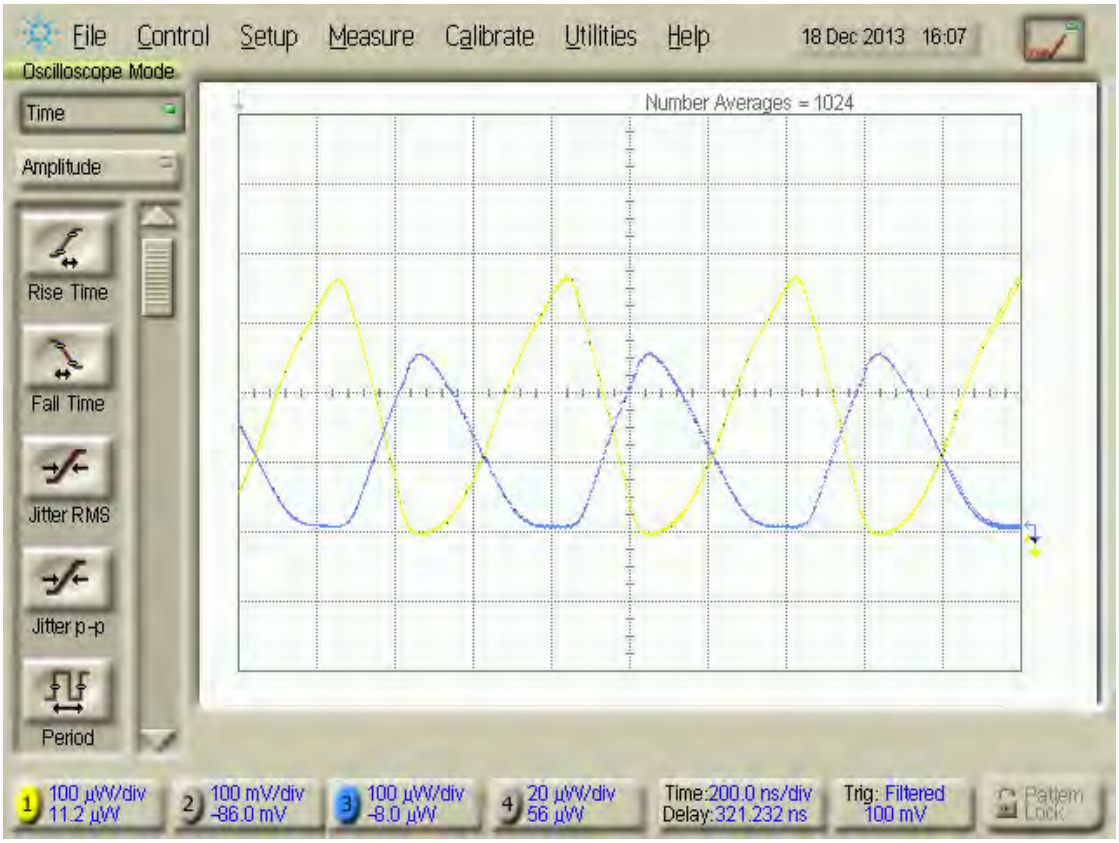


Figure 43: Shown are the intensities of unattenuated CW light behind the two outputs of the interleaver when the frequency modulation is applied. The different amplitudes are due to different attenuations of the optical fibres which are connected to the photodiodes.

Behind the laser and an isolator to prevent back reflections, the light is amplified by an Erbium doped fiber amplifier (EDFA) (Keopsys) which preserves the frequency of the input signal. The output light beam is filtered by a bandpass filter (BP-Filter) to suppress noise from the amplification. The amplifier is used for practical reasons, i.e. before working with quantum signals the system is characterized and calibrated with sufficiently strong classical light signals (see e.g. Figure 43). To change the intensity easily, a variable optical attenuator (VOA) is used.

6.3.2.2 The signal modulation

All non grayed-out parts in Figure 44 are involved in the light intensity modulation on the sender side. A high-speed MZM for 40 Gb/s data transmission (Oclaro SD), is used as pulse carver which serves to shape short time or longer frequency basis pulses. Its modulation is driven by an amplified (amplifier SHF 806 E) digital signal from the $B \times D$ output of the BPG, as reported in Section 6.3.1. The modulation contrast can be fine-tuned and temperature drifts compensated by an externally generated bias voltage (Bias V). The achievable modulation contrast is about 20 dB.

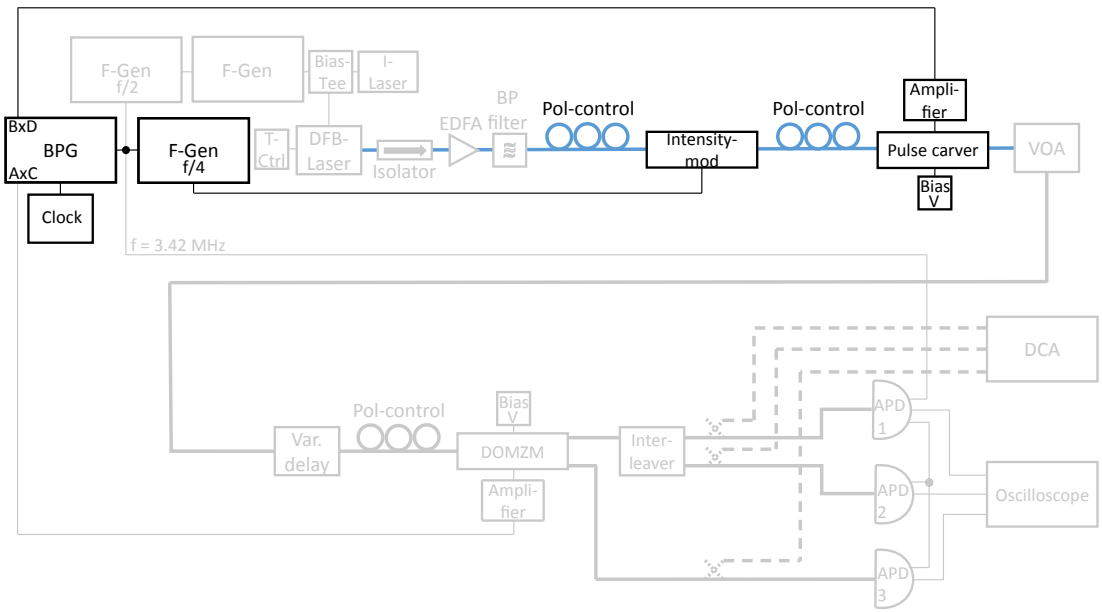


Figure 44: The non grayed-out parts show all components for the intensity modulation of the light on the sender side.

Both the temporal shape of the time and the frequency states is determined by the electronic signal driving the MZM. Due to the binary driving signal, rectangular pulses are formed instead of Gaussian pulses. The temporal shape of both the typical time and the frequency pulses is shown in Figure 45. The time pulse shown in Figure 45 a) results from to bits with of the bit pattern and has an approximate pulse width of 36 ps. The frequency pulses are varied in length and thus also in spectral width throughout the experiment, see Section 6.4. The smallest and thus spectrally broadest pulse used here is formed by six successive bits within the pattern, the longest and thus spectrally narrowest pulse consists of 20 bits. In

the figure, part b), a frequency pulse resulting from 10 bits is shown, which has an approximate pulse width of 180 ps. It should be noted that the time pulse in part a) is probably not shown in its full shape due to the limited bandwidth of the digital channel analyzer (DCA) and its integrated photodetectors. Nevertheless it can be seen that the temporal signal shape can be approximated by rectangular shaped pulses with edges given by half a Gaussian with a FWHM of about 18 ps. The spectral shape of the frequency states is given by the Fourier transformation of their temporal shape, resulting in approximately sinc^2 shaped pulses in frequency. The numerical simulations presented in Section 6.2 are adapted to this.

Due to the binary driving signal the transmission can only be switched between low and high. Another MZM (Fujitsu FRM7921ER, intensity mod in Figure 44), is needed to assure that the longer frequency pulses contain the same number of photons as the short time pulses. This modulator is driven by a binary signal from a function generator (F-Gen, HP E3610A). This generator divides the BPG trigger frequency by four. The signal amplitude and the duty cycle are adapted such that the intensity of two successive frequency pulses is attenuated with respect to two successive time pulses at a ratio resulting in the same intensity for both. It is simply given by the ratio of the length of the frequency pulse to the length of the time pulses. Fine tuning is achieved by a bias voltage (Bias V), which can be set by the function generator.

a) b)

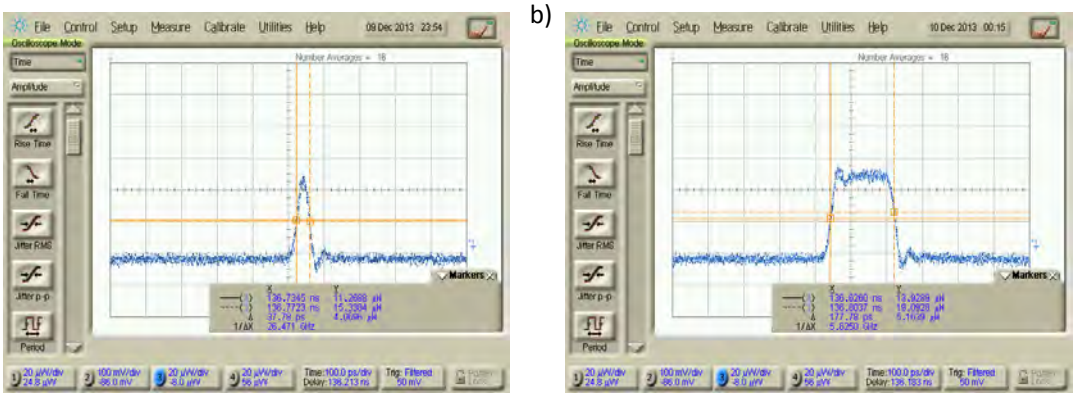


Figure 45: The temporal shape of a non-attenuated light pulse in the a) time basis and b) frequency basis as detected on the digital channel analyzer (DCA). The time pulse is generated by two successive bits on high level, the frequency pulses by 10 successive "high" bits.

The ensemble of electronic signals on the sender side, for both MZMs and the frequency modulation of the laser, are schematically shown in Figure 46 for one pattern cycle of the experiment.

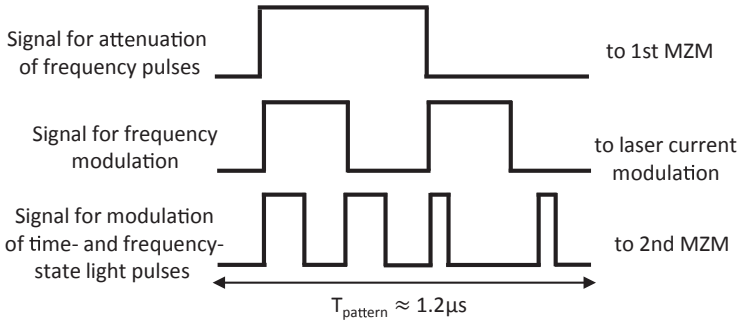


Figure 46: The different signals on the sender side which are generated during a period $T_{pattern}$ of the basic digital pattern. From top to bottom: the attenuation signal to adjust the pulse energy of the time and the frequency pulses; the signal which is used to modulate the laser frequency; the signal which is applied to the pulse-shaping modulator on Alice's side.

In front of both MZMs there is a manual polarisation controller (Pol-control in Figure 44) to maximise their polarisation dependent transmission

The expected modulation contrast of both MZMs is 20 dB.

6.3.3 Bobs measurement and detection scheme

The receiver can be divided into several parts as well, which will be reported on in the following sections: first of all, there is the DOMZM which serves to choose the basis as well as to implement the measurement in the time basis. Second, there is the implementation of the frequency basis measurement by using an interleaver. Behind these devices there are three APDs to determine the actual output the light state has taken an thus to complete the measurement.

6.3.3.1 Rapid switching to implement the time basis

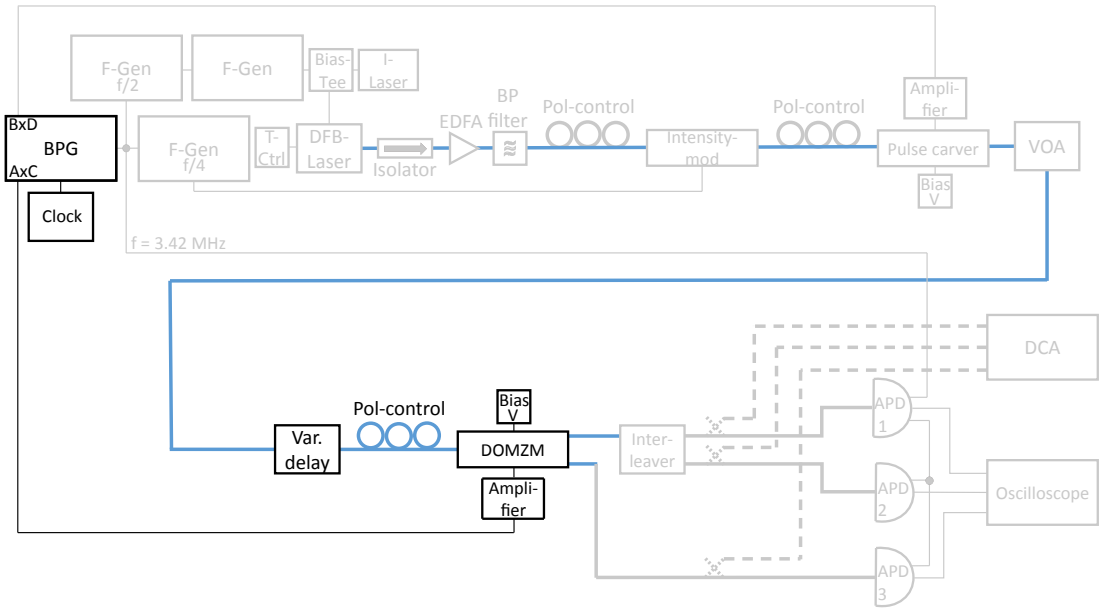


Figure 47: The non greyed-out components show all parts which implement the switch used for choosing the measurement basis and for the time basis.

The switching scheme on the receiver side is shown in Figure 47. The double output Mach-Zehnder modulator (DOMZM) is driven by an amplified signal (amplifier SHF 806 E) from the $A \times C$ output of the BPG as described in Section 6.3.1. Additional adjustment of the switching contrast and compensation for temperature drifts of the DOMZM comes from an external bias voltage. The maximally achievable switching contrast is 20 dB. The DOMZM is supposed to achieve two things: first of all, when Bob is measuring in the frequency basis, all light should be guided to the output connected to the interleaver. Second, when Bob is measuring in the time basis, a signal pulse centred at t_{0j} should be switched towards the interleaver as well (and thus towards APDs 1 or 2), whereas a signal pulse centred at t_{1j} should be switched toward APD 3, cf. Table 4. As explained in Subsection 6.3.1, a sequence of zeroes is programmed for a measurement in the frequency basis, making the DOMZM transparent towards the associated output. For a measurement in the time basis a small sequence of "ones" is programmed in the pattern, which is responsible for a fast intensity switching between the DOMZM's two outputs. To find the right instant in time for this switching of the $|t_{0j}\rangle$ state, the subpattern for the $A \times C$ output is shifted with respect to the $B \times D$ subpattern until optimal switching is accomplished. Fine tuning is achieved by a variable optical fibre delay

(Var. delay in Figure 47) in front of the DOMZM which can delay optical signals with a sub-ps resolution. A polarisation controller (Pol-control in the figure) in front of the DOMZM is used to maximise the transmission of this polarisation dependent device.

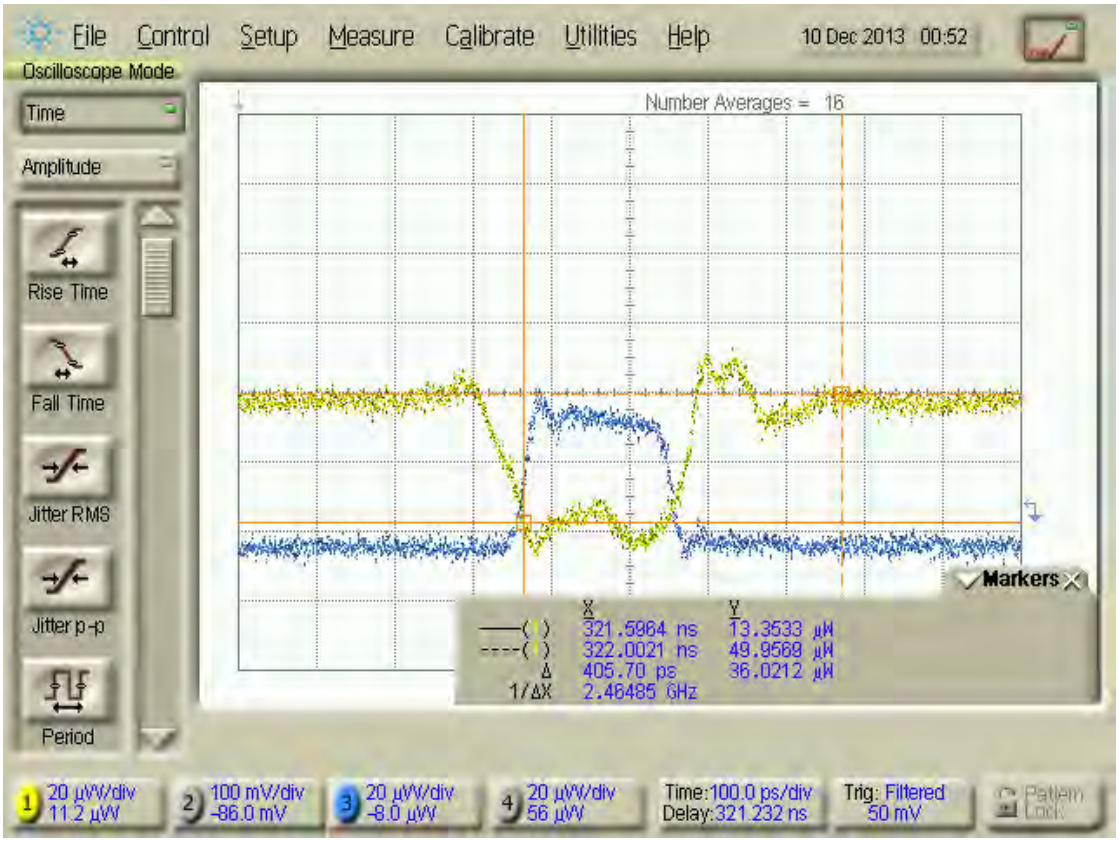


Figure 48: The intensities of switched continuous wave (CW) laser light at both outputs of the double output Mach-Zehnder modulator (DOMZM), detected by the digital channel analyzer (DCA).

A screenshot of classical, unattenuated CW light signal switched between both outputs of the DOMZM recorded by the DCA is shown in Figure 48. A 10 bit sequence brings about the shown switched signal.

In Figure 49, the complete schematic signal pattern used for controlling the experiment during one pattern period is shown.

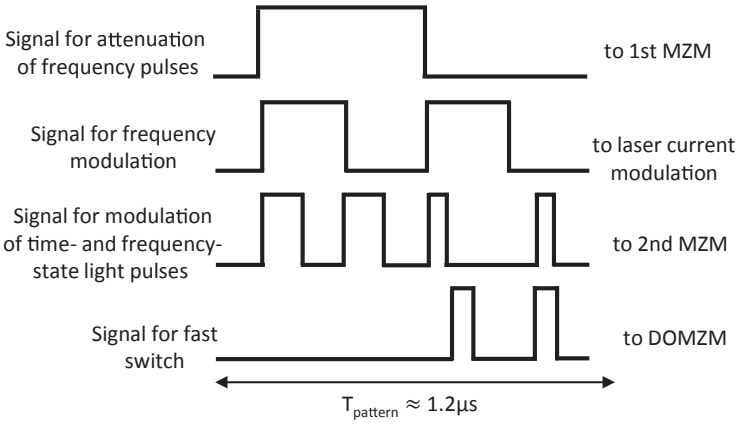


Figure 49: All different signals which are generated during a period $T_{pattern}$ of the basic digital pattern controlling the experiment. From top to bottom: the attenuation signal to adjust the pulse energy of the time and the frequency pulses; the signal which is used to modulate the laser frequency; the signal which is applied to the pulse-shaping modulator on Alice's side; the signal which is applied to the switch (DOMZM) on Bob's side. Taken from [173]

6.3.3.2 An interleaver to implement the frequency basis

Frequency filtering is supposed to separate the states $|f_0\rangle$ and $|f_1\rangle$ so they can be distinguished by single photon detection. The filter applied here is a so-called optical interleaver (Optoplex 12.5 GHz interleaver). This device is typically used in dense wavelength division multiplexing (DWDM) telecom applications to combine or separate signals with different frequencies. Its integration in the setup is shown in Figure 50.

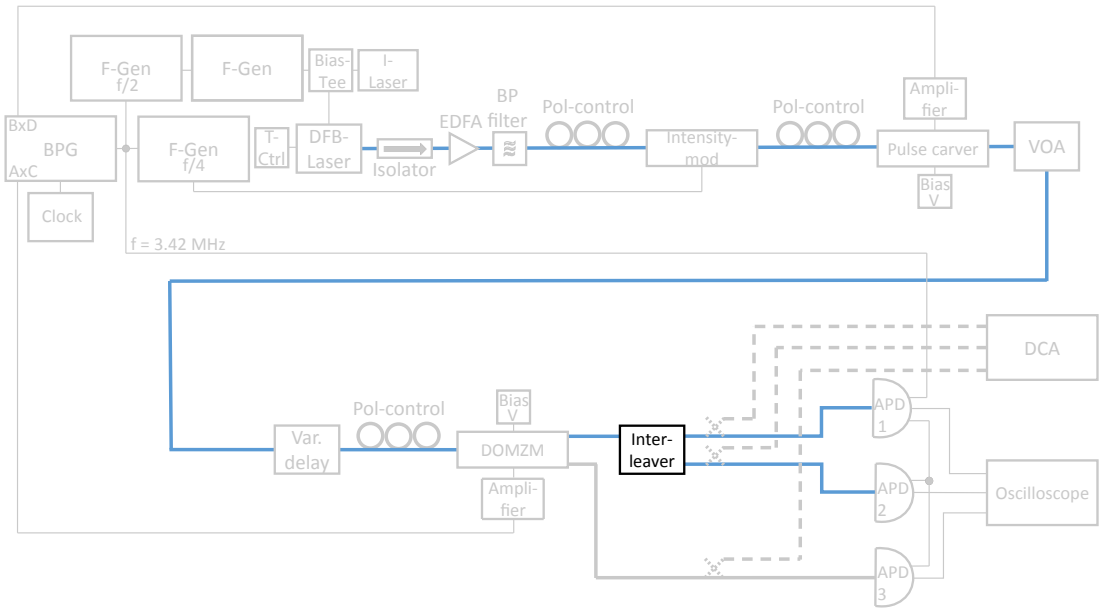


Figure 50: The non grayed-out parts show the interleaver and optical fibres used to implement the measurement in the frequency basis.

The interleaver works through multi-beam interference. It has the filtering characteristics with respect to the input wavelength as shown in Figure 51. As can be seen, the device is able to process signals over a broad spectral range. The free spectral range (FSR) of each output is 25 GHz. With the flat transmission profile of each output (see figure), the device is able to separate signals with a spectral difference of $7\,\text{GHz} < f_{Sep} < 18\,\text{GHz}$. The frequency separation between the centres of two neighbouring transmission windows of different outputs is 12.5 GHz. Ideal separation of two signals is achieved with this frequency separation.

The expected filtering contrast is greater than 20 dB.

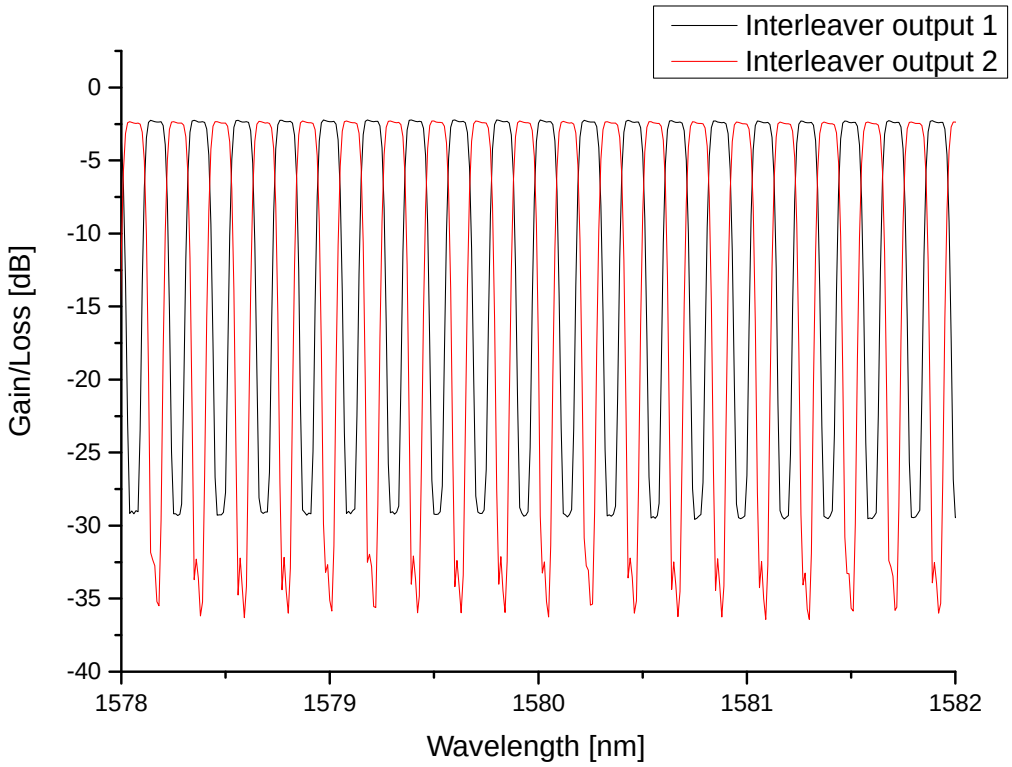


Figure 51: Filtering characteristics of the Optoplex 12.5 GHz interleaver as a function of wavelength. Measurement data by courtesy of the Heinrich Hertz Institute (HHI).

6.3.3.3 The signal detection

The complete detection scheme is shown in Figure 52. The detection is accomplished by three indium gallium arsenide (InGaAs) APDs (ID-Quantique ID210). These are employed in gated mode (see Section 4.3.4) and thus need an external trigger signal. The gate is a bias voltage of adjustable length and amplitude applied to the photodiode, which is only able to detect photons during this instant. Since the arrival times of the photons are known, this can be used to reduce noise not generated by signal photons. The trigger is taken from the frame out of the BPG, see Section 6.3.1. Not all three APDs can be triggered by it directly since the signal power is too weak to be split up further. It is used to trigger just one APD directly. The other two are synchronised to the gate-out output signal of the first APD, see figure. This output is synchronous to every applied gate.

The detection outputs of all three APDs are connected to a real-time sampling scope (Le Croy Wavepro 960).

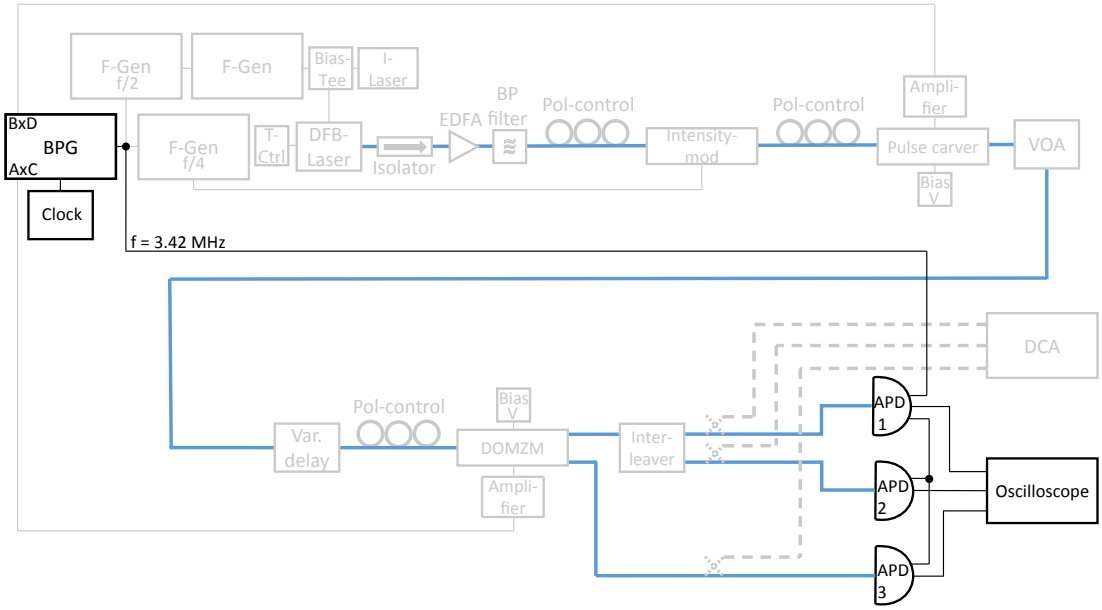


Figure 52: The non-grayed-out parts show the single photon detection and recording.

To find the right instant in time to apply the trigger is elaborate in this case. Normally, one could temporally scan the experimental clock cycle by adjusting the external trigger until a significant detection signal is found on the APDs. In contrast in this implementation, light is transmitted not only during transmission of the actual signal, but also by the impact of the blocks of 512 bits used to generate a zero-mean output of the BPG pattern, see Section 6.3.1. The correct trigger instant can be coarsely estimated by knowing the instant in time signal pulses are generated on the sender side as well as the length of the transmission channel. Adjusting the trigger instant is facilitated by the possibility to shift the frame out with respect to the pattern of the BPG. Fine tuning is achieved by shifting the gate with respect to its trigger by a small range via the user interface of the APDs.

The quantum efficiency can be individually set for each APD in the range between 5 and 25 %. It seems paradoxical to not choose the highest possible one, but actually a lower quantum efficiency comes together with a lower dark count rate, such that the actual signal-to-noise ratio might be improved. Here it has been set to 17.5 %.

The gate width can be set between 0.5 ns and 25 ns. If the signal arrival time is very well defined as it is here, it is useful to choose a gate as small as possible to reduce noise. The applied gate width is chosen between 2 and 3 ns. For such small gates, the exact gate width of each APD has an effect on the bias voltage amplitude

and thus on the quantum efficiency. This effect has been used to set the relation of count rates between the APDs as theoretically expected, counterbalancing different individual attenuations of the different receiver outputs. APDs 1 and 2 should have similar count rates, whereas the count rate of between the APD 3, which is used only to detect one time state, should be reduced by one third.

The dead time is set to $0.2\,\mu$s. A higher dead time reduces the probability of afterpulses but also reduces the maximally possible detection rate. The chosen value has been found to be sufficiently large in this case.

The signals of all three APDs are recorded by the real-time sampling scope. The sampling rate is 20 MS/s, the recorded period lasts 50 ms. Longer recording periods are not possible due to the maximum capacity of the internal scope memory. The recorded signal is read out by a PC which uses a Matlab script for data analysis, presented in the following section. The limited statistics which is collected during the short sampling period prohibits a reduction of the mean intensity below 0.5 photons per pulse.

6.3.4 The data analysis

The scheme of the data analysis is shown in Figure 53. At first, to reduce noise, the recorded digital signal from the scope passes through a low-pass filter. The oscilloscope is free-running, so afterwards the pulse rate has to be estimated. Once the pulse rate is known, the data is resampled such that an even number of samples per pulse results. During the clock recovery step, the theoretically optimal sampling instant is found. By interpolation, every signal pulse is then sampled at this instant. In the next step, the downsampling, only this one sample per pulse is kept. Then a threshold helps deciding which sample is kept as signal. The obtained signal sequence is then compared to the expected sequence and the errors are counted. This step is facilitated by the deterministic pattern used here. Also measuring exclusively in the correct basis (see Section 6.3.1) further reduces noise due to random outcomes within the relatively short recording of data.

Parts of the Matlab code for data analysis is proprietary and has been used by courtesy of the HHI. It can not be published in this work.

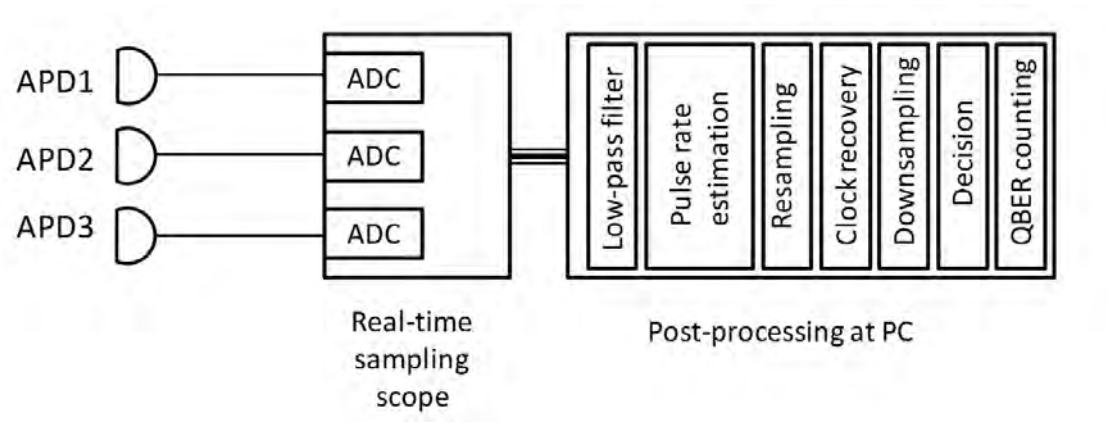


Figure 53: Receiver structure with digital signal processing. ADC stands for analog to digital converter.

6.4 Experimental results

During the experiment, different parameter settings are explored. A complete QKD experiment is performed with fixed δt, Δt and Δf and a δf which is varied by varying $\delta\tau$ through different programmed pulse lengths in the BPG. See Table 5 for the different chosen settings. δt, Δt and $\delta\tau$ are directly known through the programmed pattern, δf and $\delta\nu$ are calculated by the Fourier transformation of the given pulse width and shape. Δf has been measured by a heterodyne spectral measurement (see Section 42). All chosen parameters respect the Inequalities 101 -104

$\boldsymbol{\delta t}$	$\boldsymbol{\Delta t}$	$\boldsymbol{\delta f}$	$\boldsymbol{\Delta f}$	$\boldsymbol{\delta\nu}$	$\boldsymbol{\delta\tau}$
36 ps	72 ps	8.1 GHz	10 GHz	12.2 GHz	108 ps
36 ps	72 ps	6.1 GHz	10 GHz	12.2 GHz	144 ps
36 ps	72 ps	4.9 GHz	10 GHz	12.2 GHz	180 ps
36 ps	72 ps	4.1 GHz	10 GHz	12.2 GHz	216 ps
36 ps	72 ps	3.5 GHz	10 GHz	12.2 GHz	252 ps
36 ps	72 ps	3.1 GHz	10 GHz	12.2 GHz	288 ps
36 ps	72 ps	2.7 GHz	10 GHz	12.2 GHz	324 ps
36 ps	72 ps	2.4 GHz	10 GHz	12.2 GHz	360 ps

Table 5: Different chosen parameters during the experiment. Taken from [173].

In Table 6, the experimental QBERs in each basis, $Q^{exp}_{t/f}$, are shown as well as the average experimental QBER in both bases Q^{exp}_{both}. Also shown is the theoretical

QBER in each basis $Q^{th}_{t/f}$. Contrary to the BB84 protocol, it is not 0 % due to the overlap of both states of one basis. The numerical calculation of this theoretical error is done as described in Section 6.2 but without eavesdropping.

δf	Q^{th}_t	Q^{exp}_t	Q^{th}_f	Q^{exp}_f	Q^{exp}_{both}
8.1 GHz	0.02 %	9 %	9.4 %	15 %	12 %
6.1 GHz	0.02 %	9 %	5.3 %	9 %	9 %
4.9 GHz	0.02 %	7 %	5.6 %	7 %	7 %
4.1 GHz	0.02 %	6 %	5.7 %	6 %	6 %
3.5 GHz	0.02 %	7 %	4.9 %	7 %	7 %
3.1 GHz	0.02 %	9 %	3.8 %	5 %	7 %
2.7 GHz	0.02 %	8 %	3.0 %	5 %	7 %
2.4 GHz	0.02 %	8 %	2.9 %	5 %	7 %

Table 6: Set of δfs used in the experiment and the resulting theoretical ($Q^{th}_{t/f}$) and experimental ($Q^{exp}_{t/f}$) quantum bit error rates (QBERs) in each basis. Q^{exp}_{both} is the averaged experimental QBER in both bases. Taken from [173].

It can be seen that Q^{th}_f is not always monotonically decreasing with decreasing δf. This can be explained by the approximately sinc^2 shape of the pulses which possess side lobes and by Bob's measurement equipment. The side lobes can sometimes have higher portions in the wrong filter despite a smaller δf than for an increased value of δf.

The sifted key rate for all shown parameters was ∼12 kbit/s for a mean photon intensity of 0.5 photons per pulse (see Subsection 6.3.4) and a transmission distance in the order of 10 m.

The experimental QBERs differ from the theoretical ones, in some case significantly. Both can be explained by a reduced measurement contrast. For the time basis, the inherent intensity modulation and switching contrast of about 20 dB of the used modulator and DOMZM cannot be fully exploited due to several reasons: first of all, the modulator, the switch and the amplifiers used work at or even slightly beyond their electronic bandwidth limit, hence their optimal mode of operation cannot be reached. Also, the fact that both states in the time basis are frequency modulated is not ideal when it comes to the optimal adjustment of the modulator and switch which consist of interferometers sensitive to frequency changes. This applies to the pulse shaping of the frequency pulses as well. However, in frequency a non-optimal intensity extinction between two signal pulses does not contribute to the QBER but could open the door to a side-channel attack on the frequency information. The limited switching time of the DOMZM also contributes to the error in the time basis. An increased Δt should improve

the error rate. This will be analysed below. If in a future implementation, a smaller δf could be implemented through a filter with a higher frequency resolution, e.g. a fiber Bragg grating (FBG), these error sources could be further minimised by relaxing the constraints on the temporal resolution. Using a fast single photon detector with a high timing resolution for the time basis instead of the DOMZM, for example a superconducting single photon detector (SSPD), could further improve the results and simplify the setup.

For the frequency basis, the reduced contrast compared to the maximal interleaver contrast of minimally 20 dB might be explainable by a noisy frequency modulation. In addition, a non-optimal synchronisation with respect to the sent signals could contribute to the QBER. Compared to the possibilities of analyzing the temporal shape of the pulses, the analysis of the spectrum of the pulses has been rather limited with tools at hand. The exact impact of the scheme of the frequency modulation on the spectrum is not known. It can be seen in Table 6 that an increase of $\delta\tau$ beyond 180 ps and thus a decrease of δf below 4.9 GHz does not have a significant impact on Q_f^{exp}. This could mean that a further effective reduction of δf beyond this value is somehow prevented due to the noise in the frequency modulation. This might be improved by applying a smaller δf requiring a different filter. A trade-off between optimal performance and using standard telecom equipment should be found.

During the whole transmission, hardly any adjustment is needed. The frequency modulation and filtering is very stable. Only severe temperature changes acting on the equipment could derogate this. The polarisation is quite stable in the prevalent lab conditions with optical fibres which are fixed by scotch tape. It has to be adjusted about every 30 min. to every hour. The bias voltage of the modulators has to be readjusted in about the same cycles to compensate for temperature drifts. Both could be automated by a feedback loop. On the sender side, unattenuated classical signals could be used for such a feedback loop, also polarisation-maintaining fibres could be used here to avoid polarisation transformations. On the receiver side, if a fast single photon detector would be used instead of the DOMZM, no feedback at all would have to be applied , neither to control the polarisation nor the bias voltage. This would be very advantageous compared to many other QKD implementations which use feedback loops on the receiver side, where the statistic of the quantum signal used as feedback signal might be very low.

Under all supposed individual attacks (see Section 6.2) a secure key can be generated. For all chosen parameters, according to the simulations, the most effective attack turns out to be the attack in both bases. It should be noted that for δf = 8.1 GHz the error rate is above the 11 % introduced in Section 4.4.1 and [37], which is a lower bound for the maximum QBER of the BB84 protocol.

The stability of the scheme facilitates the testing of different parameter sets in the time basis. Different Δts and δts have been examined with respect to their impact on the QBER. The results are shown in Figure 54. For these measurements, the attenuation has always been adjusted such that count rates are similar for different δts. The switching sequence of the BPG pattern has a length of 6 bits for every measurement.

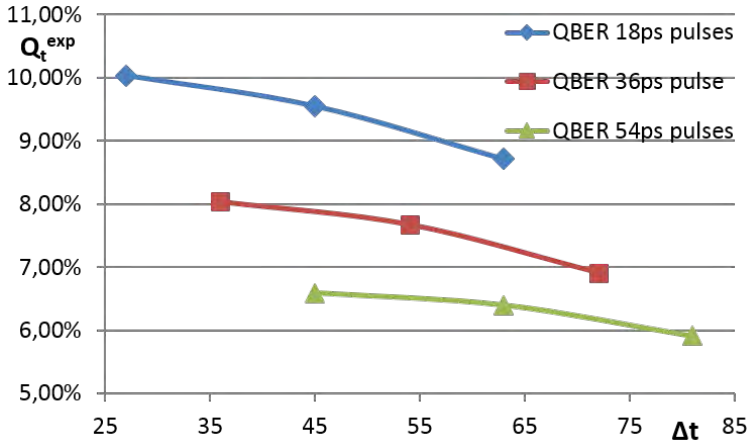


Figure 54: Measured QBER in the time basis Q_t^{exp}vs. pulse separation Δt for different temporal pulse widths δt (18 ps in blue with diamonds, 36 ps in red with squares and 54 ps in green with triangles). Taken from [173].

It can be seen that a larger Δt decreases the QBER as expected. Also, a larger δt lowers the QBER.

Last but not least it should be noted that when transmitting over larger distances, a compensation for chromatic dispersion might be necessary, for example by using dispersion shifted fibres. The effect of chromatic dispersion will be less if a smaller δf and a larger δt would be used.

6.5 Summary and outlook

In summary, a proof-of-principle implementation of the FT protocol with existing commercially available components has been shown for the first time. In fact, every component except the single photon detectors is off-the-shelf telecom equipment. A wide range of different parameters as well as their impact on the performance of the QKD transmission has been tested. This has been facilitated by the overall stability of the setup which needed little adjustment during longer periods of transmission time.

For the range of parameters tested, not only the experimental performance, but also the security under intercept-resend eavesdropping attacks specific to the FT protocol has been analysed by numerical simulations including a thorough investigation of the peculiarities of the FT protocol.

As a further development of this implementation, several modifications could be tested: with a different filter system, more advantageous parameters could be tested, which would allow for slower and less error-prone intensity modulation and switching. A fast single photon detector replacing the switch would simplify the setup considerably and dispense with the need for any polarisation and feedback dependency on the receiver side, which would be very advantageous compared to many other QKD schemes.

Besides the aforementioned modifications, it is planned to use the setup for free-space transmission to show the specific feasibility of the FT protocol for satellite transmission. Also, a larger alphabet, increasing the secure key rate per sent state is targeted. This could also increase the security of the protocol [135]. It should be noted that the FT protocol is well suited for this, since especially on the receiver side no major modifications would be needed.

Last but not least it is planned to further advance the security analysis of this protocol. For a full security proof, a collaboration with theoretical physicists experienced in this field should be sought.

7 Towards plug and play time-bin quantum key distribution

When implementing a QKD scheme with optical fibres, the BB84 time-bin implementation, see Section 4.2, is more practical than BB84 with polarised photons since polarisation is not robust in optical fibres. As part of this thesis, important steps towards a realisation of such an implementation have been accomplished. This implementation has been outlined to perform autonomously with two completely separate sender and receiver units representing Alice and Bob, which are only connected with an optical fibre representing the quantum channel and a standard Internet connection. In order to have a practical setup which is close to a real-world application, mainly standard telecom equipment is to be used for the realisation and the targeted repetition frequency is in the MHz range, for which available and cost-effective components can be used.

This chapter is organized as follows: at the beginning in Section 7.1, the proposed setup is introduced. Each succeeding section then addresses one main building block of this setup, stating the requirements which have to be met and reporting the current status including the results of performance tests. At the end in Section 7.2, the achievements are summarised and an outlook is given on the necessary steps to complete this work.

Two master theses and a bachelor thesis [176, 177, 178] have majorly contributed to this work. Also, preliminary works from two bachelor theses have been helpful [179, 180] for the realisation.

7.1 Setup

The whole setup consists of the basic optical setup introduced in 4.2 and additional equipment for synchronisation of Alice and Bob and overall process control, see Figure 55.

The setup shown in Figure 55 can be grouped into several parts on both Alice's and Bob's side. The optical setup is shown on top. On the sender side, a laser emits signal pulses at 1.5 μm into the fibre-based setup (red lines in Figure 55). An unbalanced interferometer with an electro-optic modulator (EOM) allows Alice to chose the sent state by controlling the phase. Before entering the actual transmission channel, the pulses are attenuated (Att.) to approximately single photon level. A second laser emits unattenuated pulses at 1.3 μm (blue line in Figure 55) at a predetermined time before the quantum signal. These pulses are used to synchronise Bob to Alice. They are added to the transmission channel with a

wavelength-division multiplexing (WDM) add-drop multiplexer. The two signals are again split on the receiver side by another WDM add-drop multiplexer. The synchronisation signal is detected by a fast photodiode (PD). The quantum signal passes through another unbalanced interferometer in which Bob control the phase by an EOM to set his basis choice. Additionally, in Bob's interferometer there is a device to adapt its length difference and the relative phase between both arms to Alice's interferometer in order to maximise the interferometric visibility. Signals are then detected on one of two avalanche photodiodes (APDs), each associated with a predetermined bit value. The APDs are enabled to detect a signal by application of an electronic trigger signal (APD trigger signal in Figure 62).

Below the optical setup in Figure 55, the field programmable gate arrays (FPGAs) and electronics part is shown. It is used to control the optical setup in order to execute the QKD. FPGAs are integrated circuits (ICs) which are (re-)programmable to accomplish custom tasks in parallel which are typically time-critical. They are described in more detail in Section 7.1.3. At the interface between each FPGA and the optical setup, signal adaption is necessary. This is e.g. accomplished by a digital-to-analogue converter (DAC), if bits are used to set one out of a range of possible values, as for example for the phase modulation by the EOMs. In addition, specialized homemade electronic printed circuit boards (PCBs) (Signal adaption and duplication in Figure 62) are used if digital signals have to translated to a different digital logic or duplicated. On both sender and receiver sides, the FPGA is equipped with a Universal Serial Bus (USB) module to facilitate communication with a personal computer (PC).

The PCs on sender and receiver side are at the next lower level in Figure 55. They are used for key data storage and the overall management of the experiment and offer a graphical user interface (GUI) to the user. In order to fulfill this task as well as the post-processing of the sifted key in a later stage of the experiment, they are connected to each other with an Internet connection (TCP/IP) and to the FPGAs via USB. They are also each connected to a quantum random number generator (QRNG) and acquire random numbers (Random no. acqu.) used for the bit and basis choice of the QKD. In an alternative implementation, the QRNGs could also be connected to the FPGAs directly.

In the following subsections, components of the presented setup will be summarised which are actually implemented together. The subsequent presentation is thus divided as follows: first of all, in Section 7.1.1, the interferometers as fundamental building blocks of the experiment are described. Next, in Section 7.1.2, the optical signal generation and its detection are presented together with the scheme to synchronise both. At the end in Section 7.1.3, the FPGAs controlling the experiment in conjunction with a PC are described. The homemade DACs are presented in

the same section. They are at the interface between the FPGAs and the EOMs used for phase modulation.

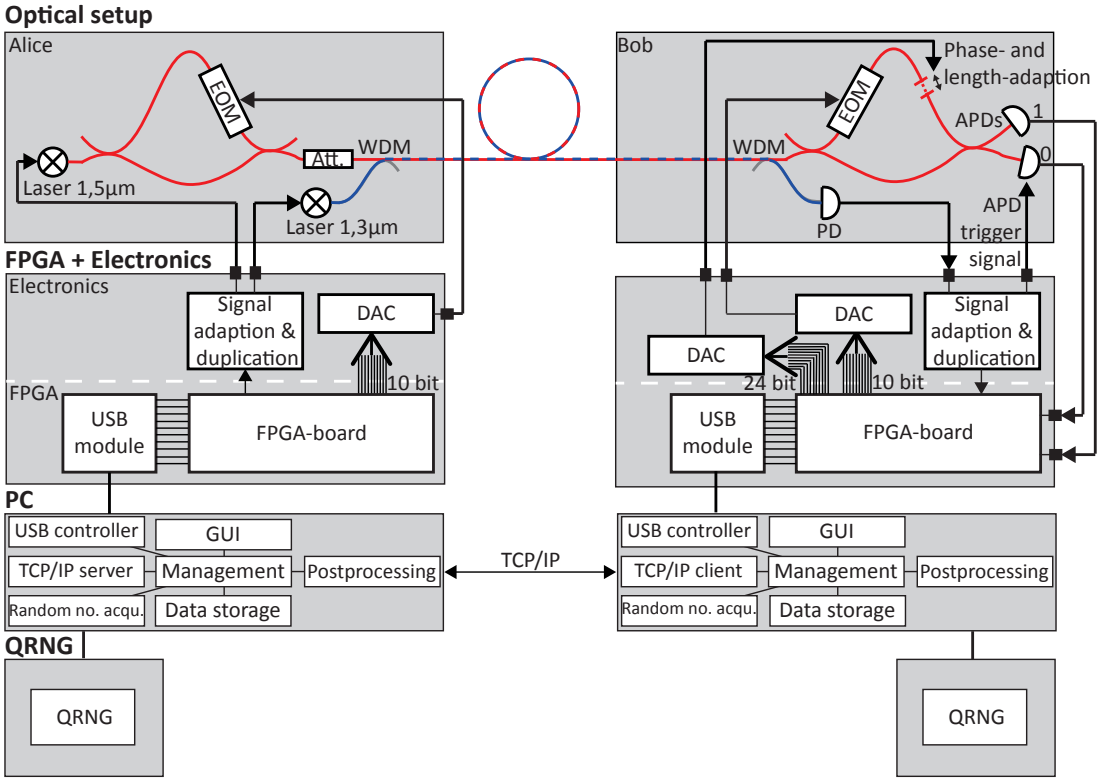


Figure 55: A scheme of the planned complete time-bin implementation. It can be grouped into several parts for each sender and receiver. The optical setup used for the actual transmission of the quantum signals is shown on top. For direct control of the experiment, field programmable gate arrays (FPGAs) and additional electronics are used, shown below the optical setup. The additional electronics is necessary to interface the FPGAs with the optical setup. Via an Universal Serial Bus (USB) module, each FPGA is connected to a personal computer (PC) which is shown graphically on the next lower level. It controls superordinate processes of the experiment. Each PC is connected to a quantum random number generator (QRNG) (shown at the bottom) to acquire random numbers (Random no. acqu.) for the bit and basis choice of Alice and Bob. The scheme is described in depth in Section 7.1 and throughout the whole chapter.

7.1.1 Two unbalanced interferometers for phase modulation and readout

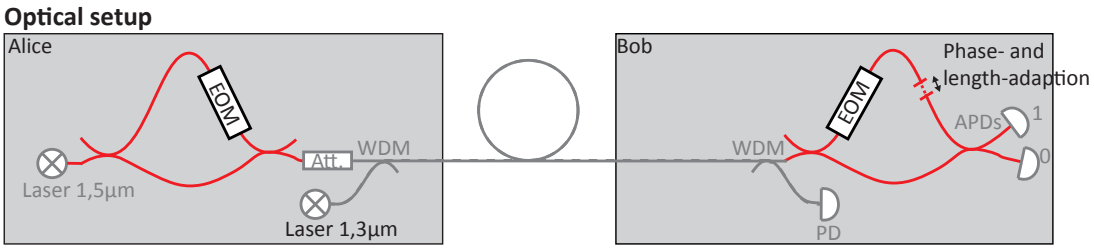


Figure 56: Shown are the interferometers (red) which constitute the fundamental building block of the BB84 time-bin quantum key distribution (QKD) implementation. Each interferometer includes an electro-optic modulator (EOM) for phase modulation. Additionally, the interferometer on Bob's side contains a device to adapt the length difference between both arms to Alice's interferometer. Also, the relative phase between the interfering paths can be stabilised with this device.

A fundamental building block of the optical setup of Figure 55 are the interferometers, see also red parts of Figure 56.

7.1.1.1 Requirements on the interferometers

As explained in Section 4.2, three commonly known practical issues play a role in implementing these interferometers. First of all, it is fundamental to build two interferometers with an identical path-length difference Δl between the short and the long arms. The path length difference mismatch $\delta l = |\Delta l_1 - \Delta l_2|$ between the two interferometers (indices 1 and 2) should be small with respect to the coherence length l_c ($l_c = c \cdot \tau_c$, with τ_c being the coherence time). At this point it should also be noted that in order to temporally distinguish interfering from non-interfering events in the time-bin implementation (see Section 4.2), Δl has to be large enough to be temporally resolvable by the involved measurement equipment. Second, the polarisation overlap between the two interfering paths at the last beam splitter (BS) should be as high as possible. The achievement of a high spatial overlap between both is satisfied without further intervention because the setup is fibre-based. Finally, the overall phase relations between the two paths should be kept constant over the whole transmission so a well-defined phase shift can be applied by Alice and Bob. These three factors play a fundamental role in achieving a high visibility V (see Equation 55 in Section 3.4.1 for the definition of visibility). The visibility itself has an important influence on the quantum bit error rate (QBER).

It is directly related to the optical error probability p_{opt} (cf. Equation 81 in Section 4.4.2) [13],

$$p_{opt} = \frac{1-V}{2} . \tag{109}$$

It is thus vital to know the influence of each of the aforementioned factors on the visibility. This shall be investigated in the following. Additionally, a fourth potentially influential factor is investigated here: the impact on unbalanced losses of the interfering paths on the visibility.

The resulting visibility can be described as a product of individual visibilities which are functions of these factors,

$$V = V_{\delta l} \cdot V_{pol} \cdot V_{\Delta\varphi} \cdot V_{loss} , \tag{110}$$

where $V_{\delta l}$ describes the visibility as a function of the path length mismatch δl and V_{pol} is the visibility as function of the polarisation overlap. $V_{\Delta\varphi}$ describes the visibility as function of the phase stability and V_{loss} describes it as function of individual losses in each of the interfering paths. Each can take values from 0 to 1.

At first, the intensity of an interfering light beam passing through two unbalanced interferometers as in Figure 55 has to be expressed mathematically. In principle, if continuous wave (CW) light is considered, the time average of the intensity at one of the two outputs of the second interferometer can be quite complicated, since there are contributions from all the different possible paths the light has taken. These contributions might all interfere with each other if l_c is long compared to the path difference Δl of the interferometers. In the experiment, pulsed light from a laser with a coherence length shorter than the path difference Δl is used. Also, in the time-bin scheme (see Section 4.2) only detections around the arrival time of a light pulse which has taken the long path in the first and the short path in the second interferometer or vice versa are considered. With this, the expression simplifies and for the output of the second interferometer of Figure 55 which is associated with the bit value "0", an expression very similar to Equation 52 of Section 3.4.1.1 can be found, only the higher number of transmissions and reflections in the couplers has to be taken into account,

$$\left\langle \bar{I}_4(t) \right\rangle = 2 \left|\mathcal{R}\right|^4 \left|\mathcal{T}\right|^4 \left\langle \bar{I}(t) \right\rangle \left\{ 1 + \left| g^{(1)}(\tau) \right| \cos \varphi \right\} . \tag{111}$$

This expression has been derived from Equation 52 which describes classical light. It could however also be expressed with quantized field operators, resulting in the same expression, where $\left\langle \bar{I}(t) \right\rangle$ would be the quantum mechanical expectation value of the intensity and $\left| g^{(1)}(\tau) \right|$ would be formed with quantum mechanical operators,

see Section 3.4.1.3. It thus remains valid if single photons are used as is the case in this QKD experiment.

To begin with, the impact of the spectral bandwidth and the mismatch δl on the visibility is discussed. For this, the assumption is made that the laser emits Fourier-limited Gaussian shaped pulses. Their spectral bandwidth is thus given by a Gaussian distribution with full width at half-maximum (FWHM) δf given by $\delta f = 0.44/\delta t$, where δt is the FWHM temporal width of the pulses. With this, using the Wiener-Khintchine theorem in the form of the Fourier transformation of Equation 54 as well as Equation 56, the visibility of such a pulse interfering with itself has a Gaussian shape as well, resulting in

$$V_{\delta l} \;=\; \exp\left\{-\frac{1}{2}\left(\frac{\pi\cdot 0.44}{c\cdot\sqrt{2ln2}}\right)^2\left(\frac{\delta l}{\delta t}\right)^2\right\}. \tag{112}$$

So for a given temporal pulse width of δt in the order of 100 ps as will be used here, the mismatch δl should be smaller than 2.6 mm to have an optical error contribution below 1%, cf. Equation 110. It should be noted that in reality the situation is worse since the real pulses are typically not Fourier-limited. Thus, ideally, interferometer offering ultra-fine adjustment of δl with a range covering $\delta l \approx 0$ should be implemented.

Next, the effect of the polarisation overlap on V is treated. Since arbitrary polarisation transformations are possible in the fibres, the final polarisations can be elliptical. The overlap is defined as $\mathcal{O} = |\langle\mathcal{P}_1|\mathcal{P}_2\rangle|^2$, with $\mathcal{P}_1$ and $\mathcal{P}_2$ being the polarisation states of the light passing through the two interfering optical paths. Supposing perfect visibility for the overlapping fraction and zero visibility for the non overlapping fraction,

$$V_{pol} \;=\; \mathcal{O}\,. \tag{113}$$

The influence of missing phase stability on the visibility will be discussed now. An applied erroneous phase of $\Delta\varphi$, added to the ideal phase difference $\varphi = \phi_B - \phi_A$ between Alice and Bob (cf. Equation 72) can be estimated in the following way: Taylor-series for $\langle I\rangle_{max}$ and $\langle I\rangle_{min}$ as functions of φ using Equation 111 are developed up to second order at 0 and π, respectively. The resulting expressions are put into Equation 55, and thus for small $\Delta\varphi$

$$V_{\Delta\varphi} \;\approx\; \frac{2-(\Delta\varphi)^2}{2}\,. \tag{114}$$

So with this and Equation 110, if a contribution to the optical QBER smaller than 1% is targeted, $\Delta\varphi$ should be smaller than 0.2 rad or 11° over the whole transmission period.

Finally, the influence of different losses in the interfering paths on V shall be estimated. Losses can occur e.g. through bad splices (see next section) at fibre-to-fibre connections. Also, components such as EOMs can have nonuniform losses. Starting point of the estimation is Equation 49, only the higher number of transmissions and reflections taking place have to be accounted for. Also, to account for possible losses, the fields from the interfering paths are each multiplied with a (real) transmission factor f_1 and f_2, respectively, which yields

$$\bar{I}_4(t) = |\mathcal{R}|^4 |\mathcal{T}|^4 \left\langle \bar{I}(t) \right\rangle \left\{ f_1^2 + f_2^2 + 2 f_1 f_2 \Re \left[g^{(1)}(\tau) \right] \right\} . \tag{115}$$

Of interest is the relation between the transmission of the two paths and its effect on the visibility. Assuming $\Re \left[g^{(1)}(\tau) \right]$ is only an argument of the phase φ, one gets

$$\bar{I}_4(t) = |\mathcal{R}|^4 |\mathcal{T}|^4 \left\langle \bar{I}(t) \right\rangle f_1^2 \left\{ 1 + \left(\frac{f_2}{f_1} \right)^2 + 2 \cdot \frac{f_2}{f_1} \cdot \cos(\varphi) \right\} . \tag{116}$$

Evaluating this expression at $\varphi = 0$ and π for $\langle I \rangle_{max}$ and $\langle I \rangle_{min}$, respectively, and substituting the acquired expressions into Equation 55, one gets

$$V_{losses} = \frac{2}{\frac{f_1}{f_2} + \frac{f_2}{f_1}} . \tag{117}$$

If again a QBER below 1% is desired, the relative transmission of one path with respect to the other, f_i^2 / f_j^2, with $i, j = 1, 2$ and $i \neq j$, should not be lower than 0.67. This expresses a relative robustness with respect to losses, nevertheless, fibre-splices should be performed as careful as possible to keep the transmission high and similar in both arms.

The presented issues have to be addressed when implementing the interferometers. The following section presents techniques used in this thesis to realise two interferometers with high visibility in the time-bin implementation.

7.1.1.2 Experimental implementation of the interferometers

Experimentally, each of these issues will contribute to the total optical QBER of the experiment and thus has to be addressed carefully when building the interferometers. Different strategies are possible for each. Now the experimental strategies seized in this thesis are presented.

In general, the interferometers are built of fibre optic components, such as couplers or EOMs. Each component is delivered with a certain length of optical fibre,

which usually cannot be further specified when buying the product. To connect the individual components, there are two different alternatives. First of all, there are different types of standard connectors, such as E-2000, FC and SC, to name a few, which have typical insertion losses of up to 0.3 dB. Secondly, bare fibres can be spliced together in a process called fusion splicing, where an electric arc produces heat which melts the tips of the two fibres before joining them together. Typical losses are below 0.1 dB. Since the fibres of the components of the interferometers have to be custom cut anyway to have matched interferometers, the second method has been chosen.

Fibres are cut by the so-called cleaving, which results in a very clean and flat surface. It is done by a cleaver which first introduces a crack into the fibre by a blade, for example of diamond, and then breaking it by applying a tension. With modern cleavers, a cutting precision in the order of millimetres can be achieved, which is not sufficient here to reach the targeted δl. Additionally, two techniques have been used: first of all, one interferometer is equipped with a simple fibre-coupled variable optical delay (OZ Optics ODL-700, see Figure 57) which can be controlled over a range of 4 mm by turning one part of the two-part element which is threaded. As the light passes through the device twice on its round trip through the interferometer (see Figure 58 below), up to 8 mm of path difference can be adapted. As a second technique, a voltage controlled fibre-wrapped piezo ring is used, which will be reported on below in this section.

Figure 57: The fibre-coupled mechanical variable delay line which is able to adjust the optical path lengths of the interferometers by turning the threaded brass-coloured element, taken from [136].

Next, the method used to ensure the polarisation overlap is presented. It has been first thought of by Mario Martinelli [71]. The idea is to use Michelson- instead of Mach-Zehnder interferometers, which have each arm terminated by a Faraday mirror (FM) (see Figure 58). A Faraday mirror is a combination of a mirror and a $\lambda/4$ Faraday rotator. The overall effect of the Faraday mirror is the inversion of the polarisation vector, an incoming polarisation state at the input of an interferometer is transformed into its orthogonal state at the output of the

interferometer regardless of the polarisation transformation induced by the fibre before and after reflection at the Faraday mirror. Like this, the polarisation overlap is maximal.

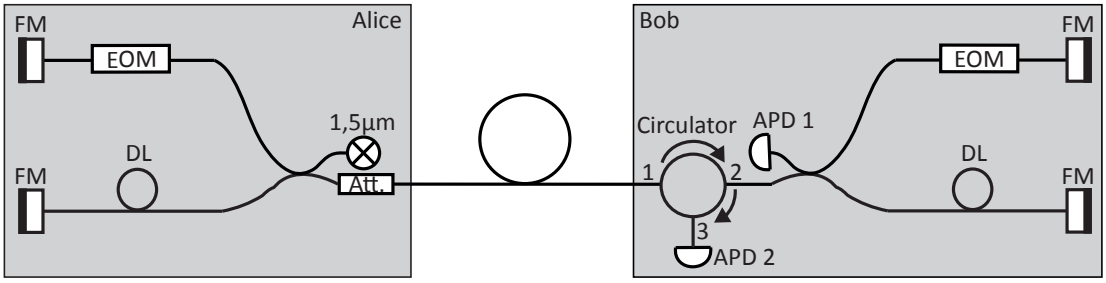


Figure 58: Simplified scheme of the BB84 time-bin implementation with Michelson- instead of Mach-Zehnder interferometers. Both arms of each interferometer are terminated with Faraday mirrors (FM). One arm of each interferometer is extended by a delay line (DL) of optical fibre. Since for Michelson interferometers, input and output ports are identical, the use of a circulator becomes necessary on Bob's side. It is a device based on Faraday rotators which guides light from port 1 strictly to port 2 and from port 2 strictly to port 3, as indicated by arrows in the figure.

There is another advantage using Faraday mirrors: the EOMs used for phase modulation have a polarisation dependent modulation depth, the modulation affects almost only the TM mode, while the TE mode passes unmodulated. The Faraday mirrors ensure that the mode which has been TE before reflection becomes TM mode on the way back and thus gets modulated as well.

Next, the approach for the phase stabilisation of the interferometers is addressed. It is approached by two different strategies: first of all, the phase is passively stabilised by a temperature stabilisation scheme. In addition, there is an active stabilisation by a voltage driven piezo ring wrapped in several meters of fibre. Both strategies have been pursued during a master thesis [176] in the framework of this dissertation.

The passive stabilisation is concerned with creating a temperature stable environment for the optical fibre. The change in optical path length under temperature changes can be estimated to be $10^{-5}\,\mathrm{K}^{-1}$ (empirical value, by courtesy of the GAP-Optique of the University of Geneva). This means a fibre optical path in the order of metres as in the interferometers will exhibit phase changes of multiples of 2π for temperature variations in the order of K. To minimise temperature changes, the interferometers are heated to well above room temperature with heating foils (Telemeter Electronics) in conjunction with a temperature sensor and a homemade proportional-integral-derivative controller (PID controller) as feedback

loop. The PID controller relies on existing technology within the research group and will not be presented in detail here. The housing of all fibre optical elements forming the interferometers is built of copper (Cu) packed in thermo-boxes made from polystyrene. The copper content as well as the targeted heating temperature are optimised to maximise thermal inertia of the housing. The homemade PID controller is able to control the temperature of the heating foil with a resolution in the range of mK. The exact stability of the feedback-controlled temperature under the given conditions is not known, but a minimal temperature stability of 0.1 K should be expected. This translates into a minimal phase stability in the order of π. It is also important to fix the optical fibre with adhesive tape into the housing, otherwise a type of fibre optic microphone [137] very sensitive to acoustic vibrations is built.

Now the active phase stabilisation with the piezo ring is presented. The ring is actually used for two different tasks: length adaption of the fibre and phase stabilisation.

It works by implementing a piezo ring with optical fibre which is tightly wrapped around the ring in one interfering path, see Figure 59. By expanding or contracting the ring through application of a voltage, rapid changes of the fibre length an thus of the optical path length can be induced [138]. The ring has a circumference of 74 mm. Its maximal contraction under application of one kV is 5 μm. With 64 windings of optical fibre on the ring, the index of refraction of the fibre of about 1.45 and given that the light travels through the ring twice, the achieved optical path length variation is of about 3 mm. To regulate the phase at a precision of better than 0.2 rad (see $V_{\Delta\varphi}$ in Equation 114), an adjustment precision of the piezo in the order of nanometres is required. Comparing this precision to the maximal path length variation, it is apparent that at least 22 bit resolution of the DAC involved in the feedback loop and an overall very noise free amplification and electronic circuitry are needed. These requirements are also very demanding for the feedback loop itself. Due to finite resources, a first implementation with an 8 bit DAC and a PC-controlled feedback loop has been sought. This is to be replaced by an appropriate DAC and a FPGA controlled feedback loop in the future (see Figure 55). Also, a classical photodiode and strong classical light is used for the feedback here. In a final implementation, the quantum signal and the APDs could be used for this if the count rate is high enough so that the statistical uncertainty acquired over a feedback loop cycle allows to regulate at the targeted precision.

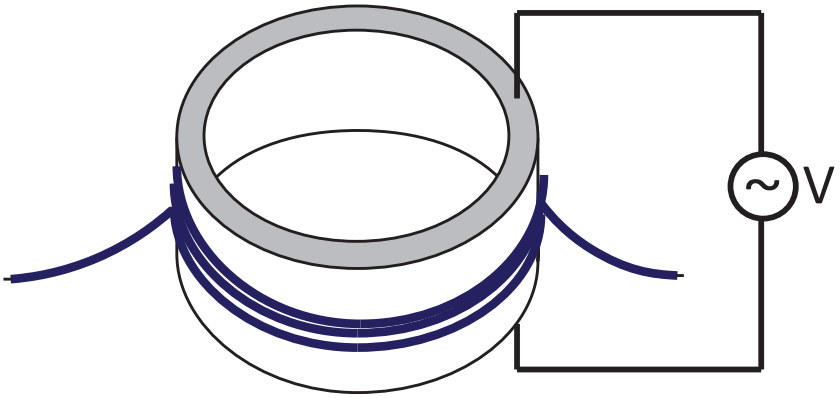


Figure 59: A piezo ring is shown whose diameter can be changed by applying a voltage. In blue the optical fibre which is tightly wrapped around the ring in order to modulate the optical path length of the transmitted light.

As voltage supply capable of delivering the required kV, a Hamamatsu power supply for phototubes (Type C9619-51) is used. One encountered experimental subtlety concerns the process of winding the fibre round the piezo ring. Since the ring contracts under applied voltage, the fibre has to be wrapped around the ring when the maximal voltage is applied. This is not trivial not only due to the high voltage but also because the fibre should be wrapped with a constant but not to high mechanical tension on it (risk of breakage). It is accomplished by a small homemade machine turning the ring with an electric motor while the fibre is kept under constant but weak tension manually. At the same time, the voltage is applied through the rotation axis by a cable mounted such that it turns together with the ring without tangling up. To achieve this, a high-voltage Bayonet NeillConcelman (BNC) connection is used as bearing, with the plug serving as fixed axle whereas the jack is rotating with the piezo ring. At the end of the process, the fibre is fixed on the piezo with instant glue. Only after the drying process the voltage is eventually lowered to zero. Several ramps of low to high voltage are applied to even out the mechanical tension throughout the wrapped fibre.

The piezo is installed in one arm of Bob's interferometer. The $\sim$15 m of fibre are compensated for in the other arm by the same amount of fibre wrapped around a ring of the same material and thus the same thermal characteristics.

The scheme of the feedback loop is shown in Figure 60. On the left-hand input side, the desired value is available to the feedback control software in form of a bit value. At the same time, the given voltage on the piezo ring results in a certain phase between the two arms of the interferometer and thus a certain detected intensity. This intensity is transformed to a bit value by an analog-to-digital converter (ADC), which is fed back to the PC and compared to the desired value. The feedback mech-

anism then adapts the bit fed to the DAC controlling the piezo ring. It should be noted that the resolution of the ADC is less critical since it is only used for the phase stabilisation and not for the length adaption. It thus only needs to be able to resolve the intensity increment equivalent to a phase change in the order of 0.2 rad.

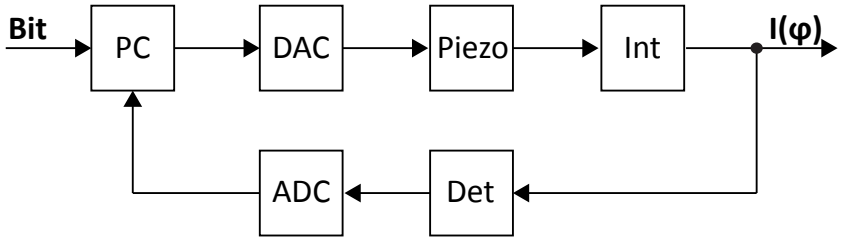


Figure 60: Schematics of the feedback loop used for the phase stabilisation scheme with the piezo ring. The controller is implemented in software on a PC. A digital-to-analogue converter (DAC) controls the piezo ring wrapped in fibre which serves to stabilise the phase in an interferometer (Int). The intensity I(φ) resulting from the relative phase is detected (Det), the detection signal is converted to a bit value by an analog-to-digital converter (ADC).

The regulative element of the feedback mechanism is a simple integrative element which is implemented in software (FreeBASIC) [176]. The integration interval as well as the time constant of the controller are found experimentally.

Due to a broken variable optical delay (OZ Optics), the length adaption could not be tested. Because of this, there is no conclusive result for the maximally achievable visibility of the interferometers. The effect of the phase stabilisation with an optimally adjusted feedback loop and 8 bit digital resolution of the used DAC is shown in Figure 61. A signal from the photodiode shows the fluctuations of the intensity after two unbalanced interferometers, which depends on the phase due to interference. It should be noted that no complete constructive or destructive interference can be observed because a CW laser instead of a pulsed laser is used here.

From time $t = 0\,\mathrm{s}$ until $t \approx 18\,\mathrm{s}$ (identified by the red arrow in Figure 61), the feedback is turned off. Large intensity fluctuations from relative minimum to maximum can be observed. When the feedback mechanism is switched on, these fluctuations are significantly reduced. If the required phase stability had been achieved, the fluctuations would have been hardly noticeable in Figure 61. However, the resolution of the 8 bit DAC is not sufficient to reduce them to a tolerable level for long term QKD transmission. The feasibility of the usage of the piezo ring for stabilising the phase can nevertheless be shown. It should be noted as well that

the temperature stabilisation has been switched off during the measurement.

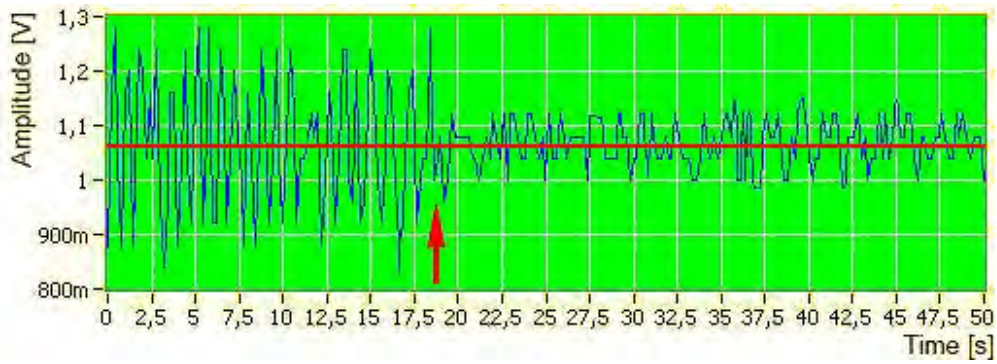


Figure 61: The detected signal behind the interferometer before and after the feedback loop is turned on. Taken from [176]

7.1.2 Signal generation, detection and synchronisation between Alice and Bob

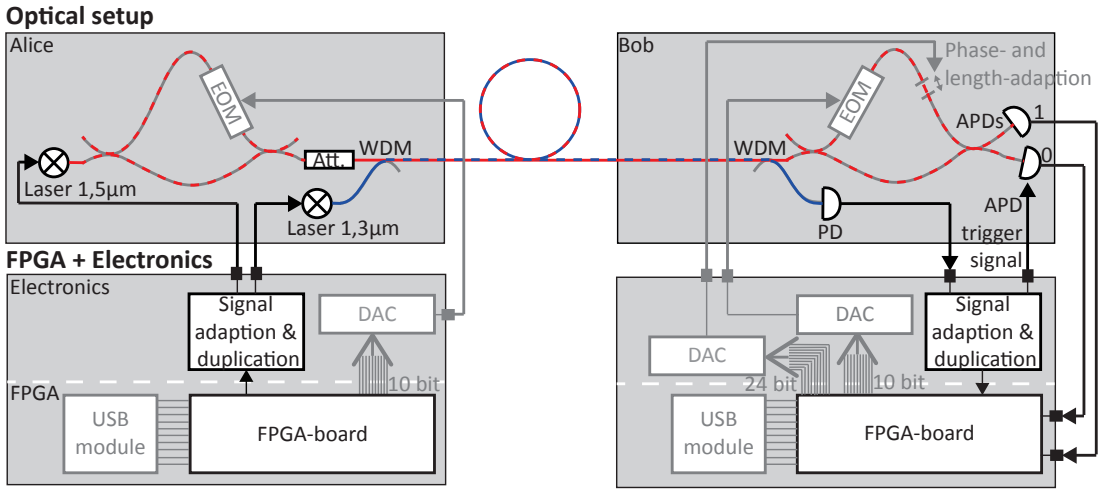


Figure 62: Shown are all components (non-greyed out) which are used for the optical signal generation and detection as well as the synchronisation between Alice and Bob. On top the optical components are shown, below the electronic control unit consisting of FPGAs and additional electronics. The scheme is described throughout Section 7.1.2.

The components necessary to generate and detect the quantum signals and to synchronise sender and receiver are shown in Figure 62. It involves parts of the optical setup and the FPGA and electronics modules. The quantum signal (its

signal path is symbolised by red lines) is generated by a 1.55 μm pulsed distributed feedback (DFB) diode laser (ID Quantique ID300) in combination with an appropriate attenuator (Att.). Each pulse has a duration of 300 ps, the pulse repetition frequency depends on the frequency of an applied electronic trigger signal generated by Alice and is variable over a wide range. The attenuation is variable and can be set according to the transmission losses (see Section 4.4.3). The intensity will be anyhow less than one photon per pulse in average. On Bob's side, the quantum signal is detected by one of two indium gallium arsenide (InGaAs) APDs (ID Quantique ID210 and ID201). They only work in the so-called gated mode, which means that they are only able to detect photons upon application of a gate of increased bias voltage (cf. Section 4.3.4) of variable length. This gate is generated synchronous to an electronic trigger signal which is provided either by an internal oscillator of the APDs or externally. Here it is provided by Bob (APD trigger signal in Figure 62). In order to detect the sent quantum signal with high probability, this trigger should be applied at a fixed instant in time before the quantum signal impinges on the detectors and synchronous to the pulse repetition frequency of Alice. This requires a precise synchronisation between sender and receiver, see next section. A detected signal from one of the APDs is indicated by an electronic pulse at its output. These pulses are read in by the FPGA on Bob's side, see Figure 62.

On the sender side, additionally to the quantum signal, an optical signal used for the synchronisation is generated by a pulsed laser. Both the signal and the synchronisation laser need an input electronic trigger signal, provided by the FPGA and homemade electronics (signal adaption and duplication). The laser is the same type than the one used for the quantum signal (ID Quantique ID300), but emitting at a different wavelength of 1.3 μm (a blue line in Figure 62 highlights its signal path), facilitating the spectral separation of both. For this purpose, two WDM add-drop multiplexers are used. The first one on Alice's side adds the unattenuated synchronisation signal to the transmission channel. The second one, at the entrance of Bob's optical setup, separates the quantum and the synchronisation signal again. The synchronisation signal is detected with a fast photodiode (PD, New Focus 1592), which generates an electronic pulse proportional to the detected intensity. This electronic pulse than has to be further processed electronically in order to synchronise Bob to Alice. For this purpose, homemade electronics is used (Signal adaption and duplication in the figure), see Section 7.1.2.3. The synchronisation pulse is generated well ahead of the quantum signal in time, so there is enough time for the electronic trigger signal to reach the APDs before the quantum state arrives. This temporal separation also helps to reduce noise from spurious light of the synchronisation pulse due to imperfect filtering of the WDM device on the receiver side.

7.1.2.1 Requirements on the synchronisation

There are two ostensible reasons why Alice and Bob need to be synchronised. First of all, they have to agree on the index of each bit they sent and measured, respectively. Especially, since in QKD many transmitted signals become subject to losses during transmission, Bob cannot number and list every measured signal and directly compare his list to the numbered list of Alice's sent signals. Instead, when Alice and Bob are synchronised, Bob can count every experimental cycle and number each measured signal accordingly. It is then easy for both to identify the signals which can be used to form a quantum key. Second, as has been mentioned in the last section, the used InGaAs APDs require an electronic trigger signal synchronous to the pulse repetition frequency of Alice.

Additionally, the time-bin implementation uses temporal filtering to sort out the the quantum signals which have been subject to interference. There are three different time-slots a signal can arrive at Bob's side due to the different path combinations it can take in the interferometers (see Section 4.2). A sufficient temporal resolution is thus paramount to filter out the interesting events originating from a light pulse which has taken either the short arm on Alice's side and the long arm on Bob's side or vice-versa.

The overall timing resolution depends on several factors: it is first and foremost limited by the pulse width of the signal pulse and the timing jitter of the employed APDs. Additionally, the timing jitter of the synchronisation comes into play. The convolution of these three factors yield the overall temporal resolution. It should be as high as possible for different reasons: it is possible to adapt the path length difference Δl of the interferometers to the temporal resolution, but eventually this is unfavourable because a greater Δl makes the phase stabilisation of the interferometers more difficult. Also, for large Δl, the repetition rate becomes constrained. Finally, the better the temporal resolution of the setup, the shorter the detection gate on the APDs can be chosen, which reduces detection noise. Due to this reasons, a timing resolution of minimally one nanosecond has been considered advisable and is demanding yet achievable with available components.

At first, the minimal timing resolution due to the used equipment for the generation and detection of the quantum signal is calculated, starting with the contribution of the signal laser. The pulse-width of the signal laser cannot be chosen too small because this results in a large spectral bandwidth which puts severe constraints on the interferometer unbalance mismatch δl, see Equation 112. Also, due to chromatic dispersion in the fibre, the small pulse width could not be sustained over larger transmission distances. The pulse width of the signal laser used here is about 300 ps. The additional jitter of the output light pulse of the laser with respect to

the input electronic trigger signal is 43 ps, as has been measured by the manufacturer. The timing jitter of the employed APDs is typically around 200-600 ps. A convolution of these values gives a minimal timing resolution of the equipment between 364 ps and 672 ps. The additional contribution of the synchronisation to this jitter should thus maximally have the same order of magnitude. Starting with the involved optical components, the requirements on the additional electronics (signal adaption and duplication in Figure 62) can be evaluated. The synchronisation laser has a low jitter contribution of 43 ps for the time between the input electronic trigger and the output pulse, just as the signal laser. The jitter of the photodiode on Bob's side presumably has the same order of magnitude than the laser. The resulting overall jitter thus mainly depends on the additional jitter of the electronics. If for the electronic circuitry involved in the synchronisation, standard transistor-transistor logic (TTL) (see next section) was used, a minimum jitter of several nanoseconds would be inevitable [139]. Thus, the components and the digital logic used for procession and transmission of electronic signals have to be chosen well and high-end electronic circuits have to be designed. A report on this is included in the next three sections. The following section introduces the light signal generation on the sender side. In the subsequent section, the light detection scheme on the receiver side is presented. The report on signal generation and detection is completed by the results of a performance test of the ensemble of sender and receiver.

It should be noted that an additional requirement on the synchronisation scheme is a stable detection rate throughout the whole transmission period of a quantum key distribution, regardless of variations of fibre length due to temperature changes or mechanical changes. This is accomplished by the presented scheme since both the quantum and the synchronisation signal are constantly transmitted through the same fibre.

7.1.2.2 Generating light signals

The generation of the quantum and the synchronisation signal is started with a digital signal originating from Alice's FPGA, see Figure 63, which triggers both lasers. Instead of taking separate signals from the FPGA for each laser, it has been decided to take a single signal and duplicate it with a separate electronic module (Signal adaption and duplication in the figure). The reason for this method is that the FPGA itself emits TTL signals (see below in this section) with a relatively high jitter. By appropriate electronic circuitry, the crucial relative jitter between both trigger signals after duplication can be kept much lower. This is realised by a specifically designed electronic circuit. This circuit also has the possibility to set

an adaptable delay between the two output trigger signals. Like this, the temporal distance between quantum and synchronisation signals is variable within a certain range. The circuit has been realised as a final project of a bachelor thesis [178] in the framework of this dissertation. The logic of the circuit as well as the design of the printed board is described in detail in the following. It serves as an example for other homemade electronic circuits described below.

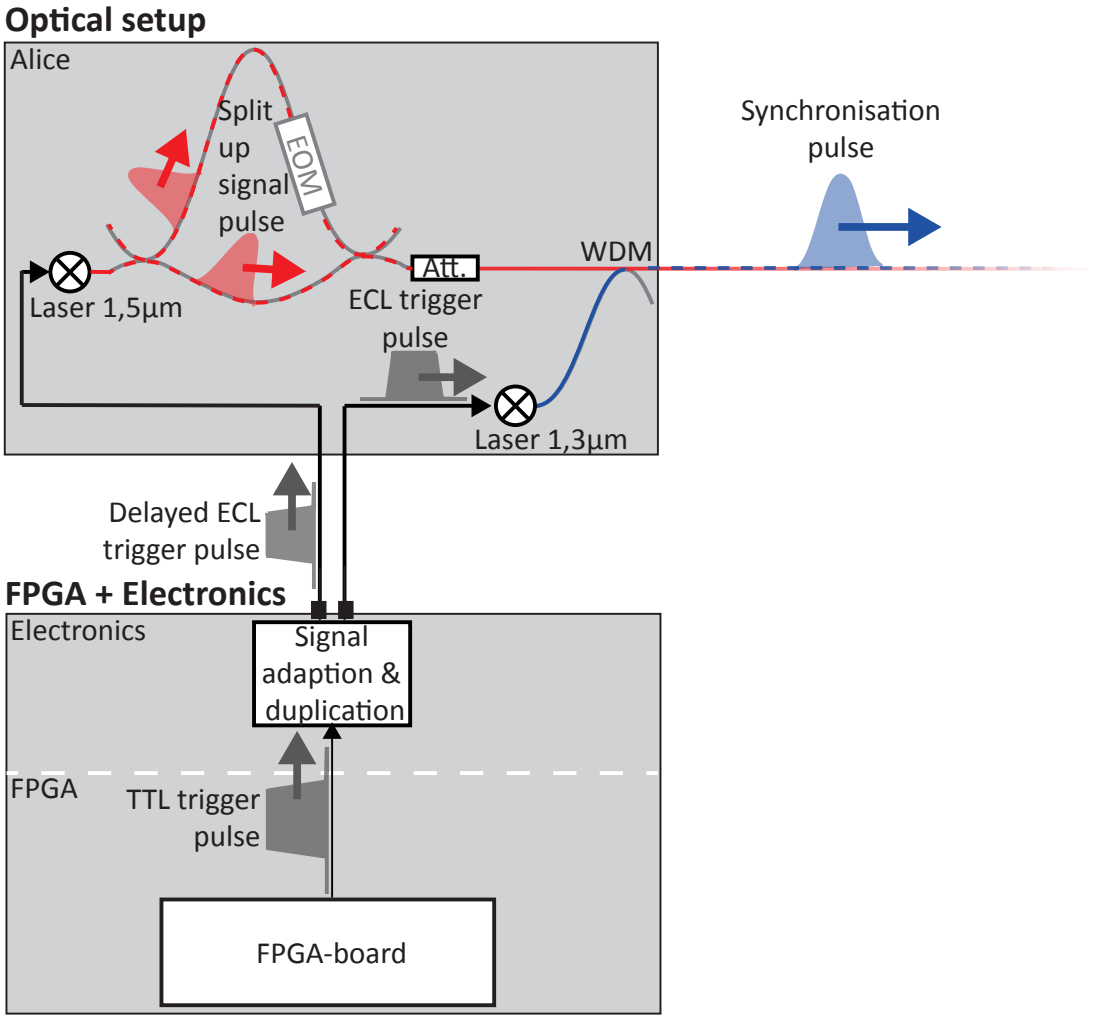


Figure 63: This scheme of the optical signal generation focuses on the paths of the involved electronic and optical signals on the sender side. A transistor-transistor logic (TTL) pulse from the field programmable gate array (FPGA) is converted by a specialised printed circuit board (PCB) (Signal adaption and duplication) to two emitter coupled logic (ECL) pulses of which one is delayed with respect to the other. They trigger the lasers emitting optical pulses serving as synchronisation (blue) and quantum signals (red), respectively.

Beforehand, a short introduction into digital logic families is made: three important logic families shall be presented here, TTL, ECL and complementary metal-oxide-semiconductor (CMOS) [140]. TTL is a standard electronic logic. It is robust, easy to implement with electronic boards, but not very fast, with typical switching times in the order of 10 ns and considerable electronic jitter in the order of ns [139]. ECL is a very fast digital logic family operating with negative voltages, with possible switching times below 1 ns and very low jitter. With its inputs and outputs which are typically differential, it is very well suited for noise resistant differential signal transmission with two complementary signals (see for example [141]). Disadvantageous are the more complex circuitry for differential high frequency signals, the obligatory negative power supply and the high power dissipation. There is also a variant using smaller amplitudes to achieve faster switching, called reduced swing ECL and a version using a positive power supply, positive emitter-coupled logic (PECL). Finally, CMOS is nowadays the most widely used digital logic. It is relatively simple, compact, consumes low power except in high frequency applications and is relatively fast, although not as fast as ECL. Due to its very low jitter, ECL has been chosen for the involved electronic circuitry here.

In Figure 63, the course of both quantum and synchronisation signals on the sender side is explicitly shown, involving the electronic trigger signals. A single trigger signal is emitted by the FPGA. This trigger signal is a digital TTL pulse with a pulse width of 25 ns. The designed PCB (Signal adaption and duplication) converts this pulse into two pulses in ECL format. One is output directly to trigger the emission of a light pulse of pulse width 300 ps at 1.3 μm used for synchronisation (blue pulse). The other electronic pulse is subject to a variable delay and thus the emission of the light pulse of 300 ps at a wavelength of 1.5 μm is triggered at a later instant in time. This light pulse becomes the actual quantum signal after being split up in Alice's unbalanced interferometer (red pulses) and being attenuated to approximately single photon level.

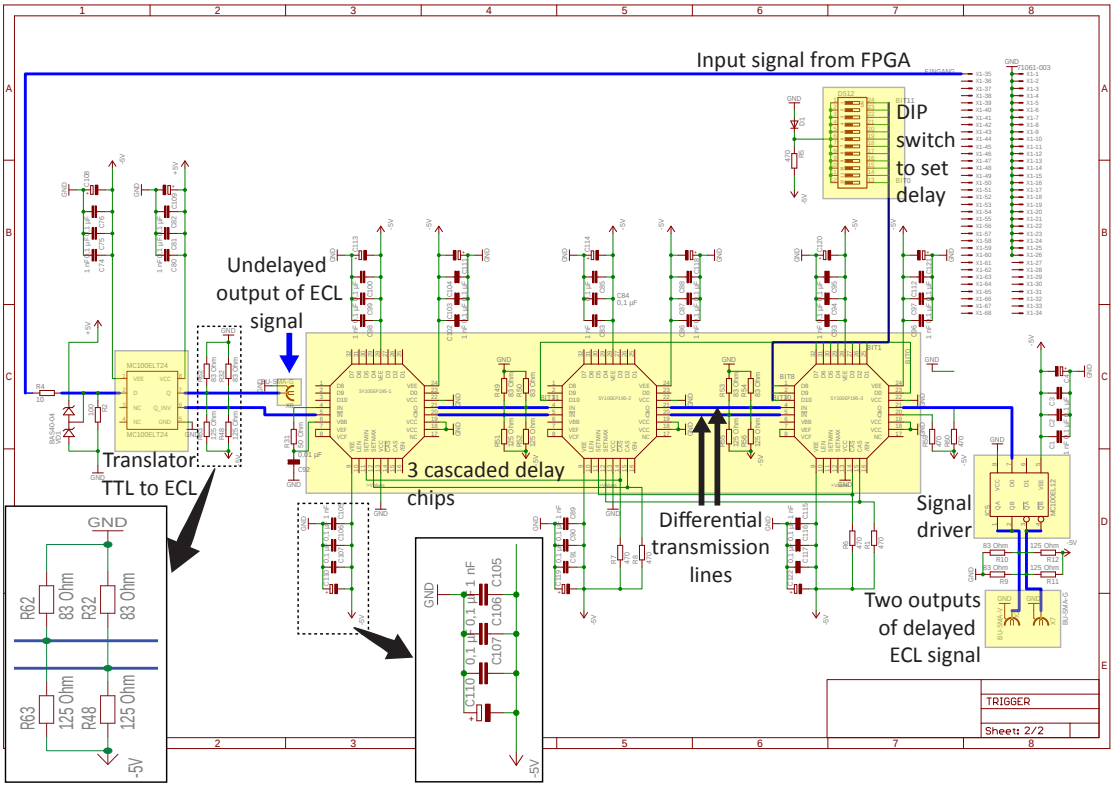


Figure 64: The trigger circuit is shown. The signal paths are highlighted by blue lines. Integrated circuits (ICs) or circuitry of interest, which are described in the text, are either highlighted by yellow rectangles and labeled or magnified. Electrical wiring is green, all components as ICs or e.g. resistances are red. The inset on the bottom left is a magnified image of the wiring for the Thevenin equivalent parallel termination. The inset on the bottom is a zoomed in cascade of capacitors to buffer the power supply of an IC. The ICs for power supply are not shown.

The circuit of the designed electronic board (printed circuit board (PCB)) for signal adaption and duplication is shown in Figure 64. The circuit and the printed board which describes the physical realisation of the circuit (see Figure 65) have been designed with the software Einfach Anzuwendender Grafischer Layout Editor (EAGLE). In Figure 64, the path of the trigger signal on the board is highlighted by a thick blue line. The signal from the FPGA is transmitted to the PCB with a specialised shielded conductor cable for parallel multi signal transmission of up to 68 signals. It is connected with a very-high-density cable interconnect (VHDCI) connector (see Figure 65). The TTL signal is converted to a differential ECL signal by a translator chip (MC100ELT24, ON Semiconductor), highlighted in Figure 64 (Translator TTL to ECL), with a very low inherent jitter of typically 2.5 ps. The signal output of this integrated circuit (IC) is differential, thus two comple-

mentary output signals are actually generated. One is directly used to trigger the synchronisation laser via a SubMiniature version A (SMA) coaxial output (undelayed output of ECL signal in Figure 64, see also Figure 65). The other output drives one of the differential inputs of a cascade of three specialised delay chips (SY100EP195V from Micrel, highlighted in Figure 64) interconnected with differential transmission lines. With this the delay of the output signal is adjustable between 6.6-37.3 ns [142]. It can be set manually with a 12 bit static ECL signal through a 12 bit dual in-line package (DIP) switch, see Figure 64. Behind the last delay chip, there is a driver module (MC100EL12 from ON Semicondutcor, Signal driver in the figure). This chip has a single input and two differential outputs and is able to drive ECL signals via long low impedance transmission lines. In addition, it protects the sensitive and expensive delay chips from strong currents caused by short circuits. One output of the driver IC is used to trigger the signal laser, the other one can be used for testing purposes. Both are output via SMA outputs, as can be seen in Figure 65 (SMA output of delayed signal and vertical SMA output for testing purposes, respectively).

For proper functioning, it is very important that every IC chip has a supply voltage which is buffered against voltage variations with several capacitors ranging from 1 nF to 1 μF. One of such typical capacitor cascades is shown in one inset of Figure 64.

The layout of the PCB is shown in Figure 65. Signal transmission lines are highlighted in light red. The PCB has Eurocard dimensions of 100 mm$\times$160 mm, suited to fit in standardised 19-inch racks. All electronic chips are surface-mount devices (SMDs). For the design of the board some basic rules have been respected to guarantee a high signal quality of the trigger signal: first of all, all the chips have been placed as close as possible to each other, keeping signal transmission lines as short and straight as possible. The signal transmission lines should not be crossed by other insignificant lines such as for the voltage supplies. If a straight line is not possible, it should be curved as smoothly as possible, see inset on top of Figure 65 for an example. All lines should have well defined impedances of 50 Ohm to avoid reflections. This is achieved by choosing a width determined by the material and the thickness of the dielectric layer of the board and the thickness of the line itself. Tools to calculate the appropriate width are available online, for example [143]. The board is constructed with four layers, beside the top layer with the principal ICs (ICs highlighted in yellow along the signal transmission line in Figure 65) and the bottom layer where the voltage controllers are situated, there are two inner layers: one ground layer and one which represents the negative voltage supply needed for the ECL. This assures a low-induction low-noise power supply. TTL is less sensitive to noise from its positive power supply and therefore it does not have a separate layer.

It is also advised to put the smallest of the cascade of buffer capacitors, which has a value of 1 nF, as close to the supply voltage pins of the ICs as possible, see inset on the bottom of Figure 65 for an example.

The electrical termination of the transmission lines between the ECL chips is guided by two principles: first of all, power has to be supplied to keep the transistors of the ECL devices at their operating point. Second, the effective impedance should be 50 Ohm. This can be achieved by the Thevenin equivalent parallel termination (see inset of Figure 64) [144]. It consists of a connection of the conduction strip to the -5V power supply via a 125 Ohm resistance. A second resistance of 83 Ohm connects the strip to ground.

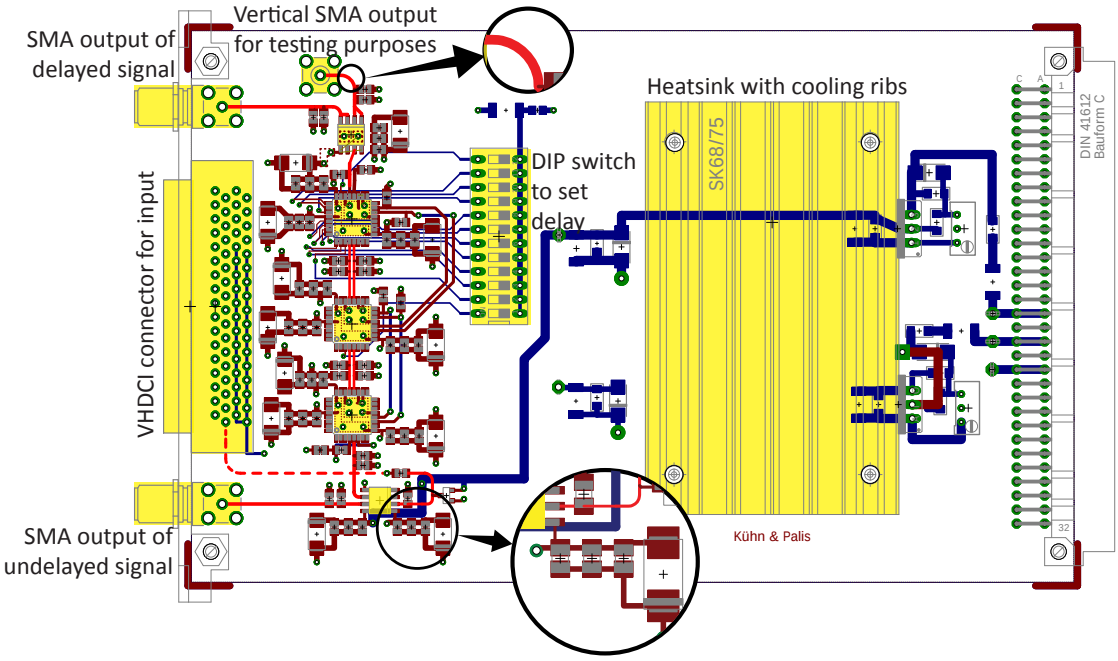


Figure 65: Shown is the layout of the trigger board in a top view. All lines and surface-mount device (SMD) parts which are on the top side of the board are dark red, those which are on the bottom are dark blue. The signal transmission line is light red (dashed if it is situated on the bottom of the board). All main components which are described in this section are highlighted in yellow. The inset on the top is a magnification of a curved transmission line. The inset on the bottom zooms in on a cascade of four capacitors with the smallest one being as close as possible to the power supply pin of the integrated circuit (IC).

A large heatsink with cooling ribs installed close to ICs for the power supply on the board, cf. Figure 65. It is necessary to dissipate the amount of heat generated by those ICs. Also, each logic chip should be subject to constant airflow for cooling.

To have an idea of the achievable jitter with the presented electronic equipment on the sender side, a TTL trigger signal is used as input of the PCB while the two outputs to are connected to a measurement device. Both with a fast digital sample oscilloscope (Tektronix DPO7104) and a time-to-digital converter (TDC), a coincidence counting instrument with very high timing resolution (PicoHarp 300 from PicoQuant), the maximal jitter between the two ECL outputs of the board is determined to be smaller than 28 ps [178]. This result shows that the sender equipment is suitable to achieve the targeted timing resolution.

7.1.2.3 Detecting light signals

Figure 66 shows explicitly all optical and electronic signals involved in the detection and synchronisation on the receiver side. The optical synchronisation signal (blue) and the quantum signal (red) are separated by a WDM add-drop multiplexer. The synchronisation signal is detected by a photodiode (PD). The resulting electronic signal is used to synchronise Bob's FPGA to Alice and to trigger the APDs. The analogue signal from the photodiode is proportional to the intensity of the synchronisation pulse, typically a pulse with a peak amplitude in the order of 100 mV and a width in the order of 100 ps is generated. This signal cannot be used directly as input for the APDs and the FPGA since it is to small and short. It has to be transformed to a broader digital logic signal. Again, homemade electronics is used for this task (Signal adaption and duplication in the Figure). A broad TTL signal is used to synchronise the FPGA, since it needs a positive voltage input signal and since the exact timing is not critical. However, as has been explained in Section 7.1.2.1, the exact timing of the APD trigger signal is crucial, hence ECL is used for this. The trigger input of the APDs is variable and the threshold voltage to detect the trigger can be set manually. If a quantum signal is detected by one of the APDs after a trigger has been applied, a TTL signal is generated which is read in directly by the FPGA.

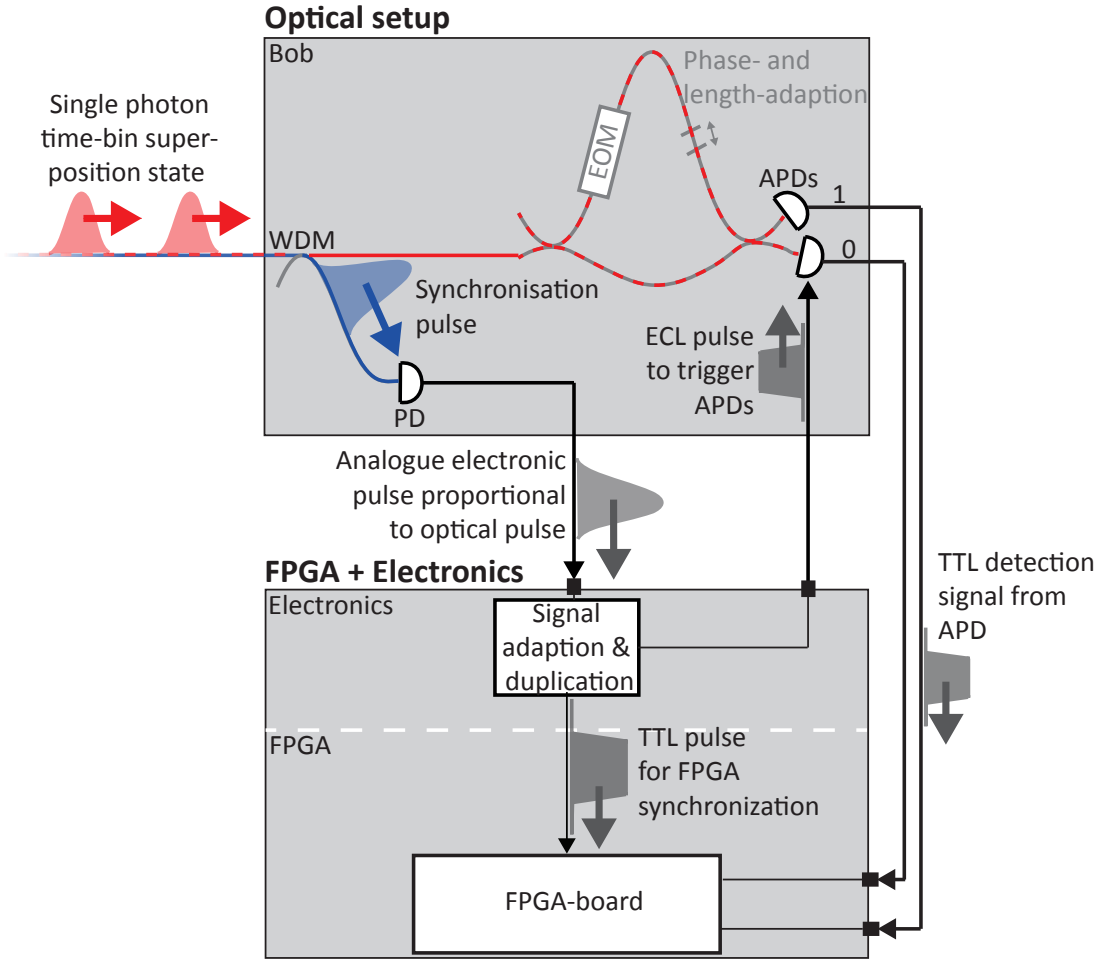


Figure 66: This scheme focuses on the optical and electronic signals on the receiver side. The synchronisation signal pulse (blue) arrives prior to the quantum signal (red). It is detected by a photodiode (PD), which transforms it to an analogue electronic pulse proportional to the optical one. It is converted into a transistor-transistor logic (TTL) signal which synchronises Bob's field programmable gate array (FPGA) and an emitter coupled logic (ECL) signal which triggers the avalanche photodiodes (APDs). The APDs emit TTL pulses upon detection which are read in by the FPGA.

Converting the analogue electronic pulse of the photodiode into a digital logic signal is demanding because of its low amplitude and small width. As shown in Figure 67, a very fast comparator IC (ADCMP581 from Analog Devices) is used to transform it into a reduced swing ECL signal. The comparator has two signal inputs: the actual signal V_{sig} and a reference voltage V_{ref}. If $V_{sig} > V_{ref}$, the output is switched to a high level, otherwise it is on low level. Since the amplitude of the analogue synchronisation signal V_{sig} depends on the losses of

the optical transmission channel between Alice and Bob, it is useful to have an adjustable reference voltage V_{ref}. It can be set by a DAC (AD9740 from Analog Devices) whose output is controlled by a 10 bit signal which can be set manually or by the FPGA. An external PCB can be used for this, see Appendix B.2. The reduced swing signal is then broadened by two two capacitors connected to ground which act as low pass filter. A second, fast comparator (ADCMP566 from Analog Devices) transforms the signal to regular ECL.

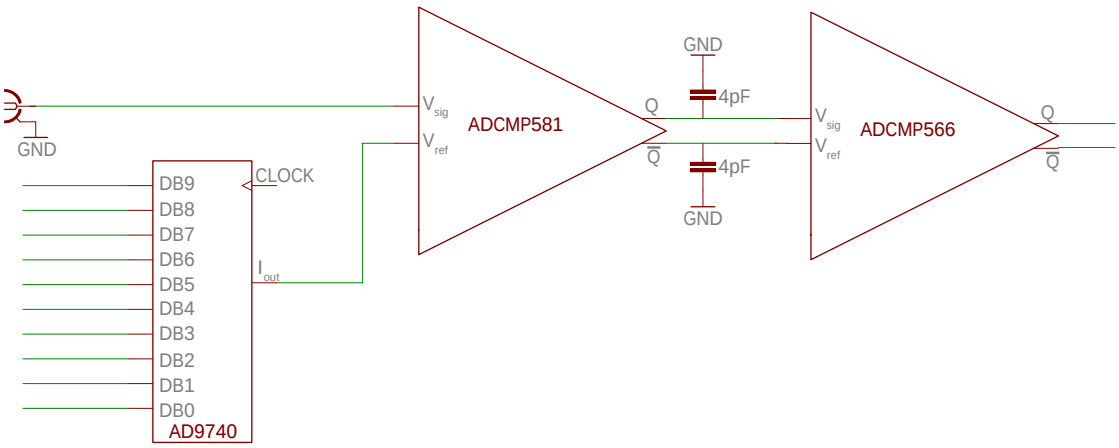


Figure 67: A simplified scheme of the first part of the the signal adaption electronics which converts the analogue output of the photodiode to a digital emitter coupled logic (ECL) signal. The input (on top on the left side) is transformed to a reduced swing ECL signal by a fast comparator (ADCMP581). The reference voltage V_{ref} defines the switching point of this comparator. It is set by a digital-to-analogue converter (DAC) (AD9740) which is controlled by a 10 bit input word. The DAC additionally needs a periodic clock signal to read the control bits. This clock is provided by a voltage-controlled oscillator (VCO) and a Schmitt-Trigger which create a clock signal at approximately 7 MHz (not shown). The output of the comparator is differential as is typical in ECL. Q is the reduced swing ECL signal, $\bar{Q}$ the complementary signal. Both outputs are first broadened by two capacitors connected to ground before a second fast comparator (ADCMP 566) transforms them to a regular ECL signal.

The temporal shape of the signal is then still very narrow and has to be broadened so that it can be used as a trigger signal. This is achieved by using a scheme consisting of delay ICs and a flip-flop IC, shown in a simplified version in 68. In this scheme, the output of the second fast comparator is split up. One part is connected to the S (Set) input of a flip-flop IC (MC100EL31), while the other part is delayed with respect to it by a delay IC with an adjustable delay of up to 4.3 ns, controlled by a 9 bit input. This input can either be set manually or by Bob's FPGA through an external PCB, see Appendix B.2. The delayed signal is

connected to the R (Reset) input of the flip-flop chip.

The scheme of the pulse-width modulation with the flip-flop IC is shown in Figure 69. A signal on the S input sets the output (Q) of the flip-flop to high. A delayed signal on the R input then sets it to low again after the time Δt *delay*. Like this, the output pulse width Δt PWM is set by Δt *delay*.

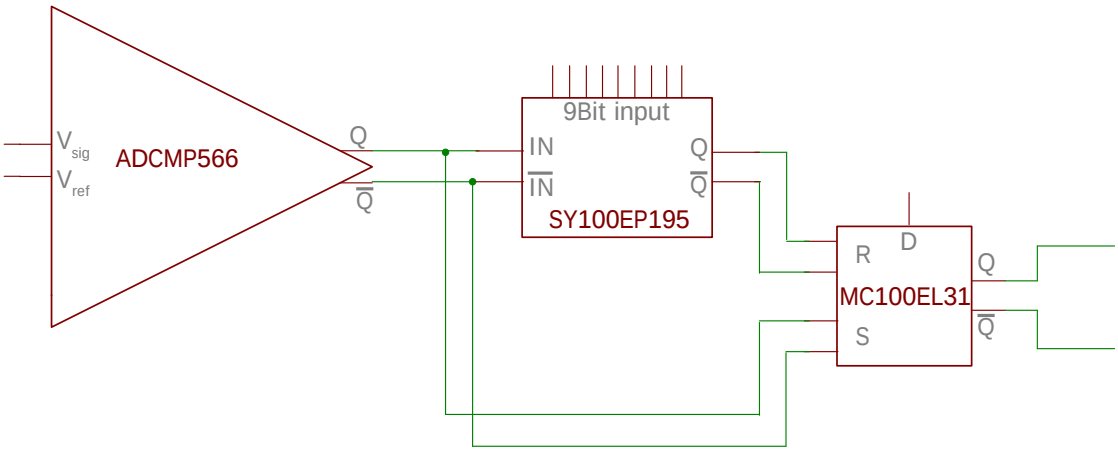


Figure 68: A simplified scheme of the second part of the the signal adaption electronics which converts the short digital emitter coupled logic (ECL) pulse into a longer pulse. The short ECL signal of the output of the second comparator (ADCMP566) on the left is split up. One transmission signal pair is connected to the S input of a flip-flop integrated circuit (IC) (MC100EL31). The other one is subject to an adjustable delay set by a delay IC (SY100EP195V). The delay time is controlled by a 9 bit input word. The output of this IC is connected to the R input of the flip-flop chip. The D input of the flip-flop is set to a logic low level at all times.

Two things have to be respected in order for this scheme to work: first of all, the S and the R input of the flip-flop IC should never be on high level at the same time, otherwise an undefined output state results. This can be achieved by setting a minimum delay Δt *delay* larger than the pulse-width of the input pulses. Second, the D input of the flip-flop IC has to be kept on a logic low level at all times.

Appendix B.1 shows the complete circuit and board layout of the PCB. Behind the flip-flop in Figure 68 there is actually a dual differential output driver to multiply the available outputs and to protect the preceding ICs from short circuits. The output can be directly used to trigger the APDs.

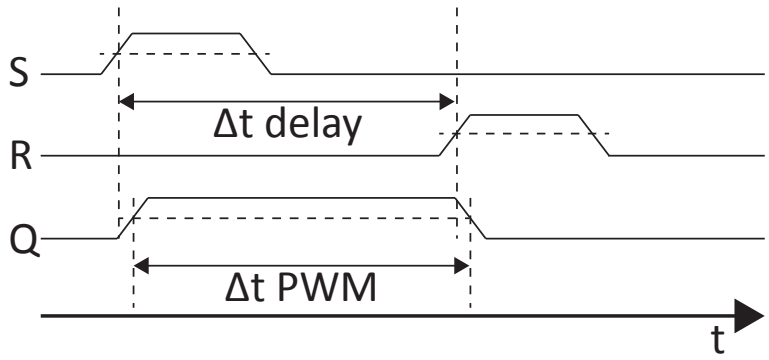


Figure 69: The signal scheme of the inputs and the output of the flip-flop integrated circuit (IC) over time is shown. A signal input exceeding a threshold voltage (dashed horizontal line) at the S input sets the output Q to high. A low to high transition of the R input at a time Δt *delay* later sets Q to low again. The output of Q is thus a pulse of pulse-width Δt PWM controlled by Δt *delay*.

To synchronise Bob's FPGA, an ECL signal not used for triggering the APDs is converted to TTL. At the same time, the pulse width is further broadened to about 20 ns in order to be readable by the FPGA. For this purpose, another PCB is used. It uses the same principle of pulse width modulation as has been reported. For the conversion of ECL to TTL, a translator IC is used. The circuit logic and the layout of the corresponding PCB is shown in Appendix B.3.

The operation of the receiver unit con only be tested in conjunction with the light generation scheme of the sender. The testing is reported on in the next section.

7.1.2.4 Testing the synchronisation

The whole synchronisation setup has been tested over a short transmission of ∼5 m in the quantum channel, cf. Figure 70. Only a single National Instruments FPGA (NI PCI 7813R, see Section 5.2.3) controlling both Alice and Bob has been used for this purpose with a PC as user interface. The optical setup has been kept very basic, without the interferometers and only with a single APD. This suffices to test the functionality of the light generation and detection scheme and the timing resolution of the synchronisation.

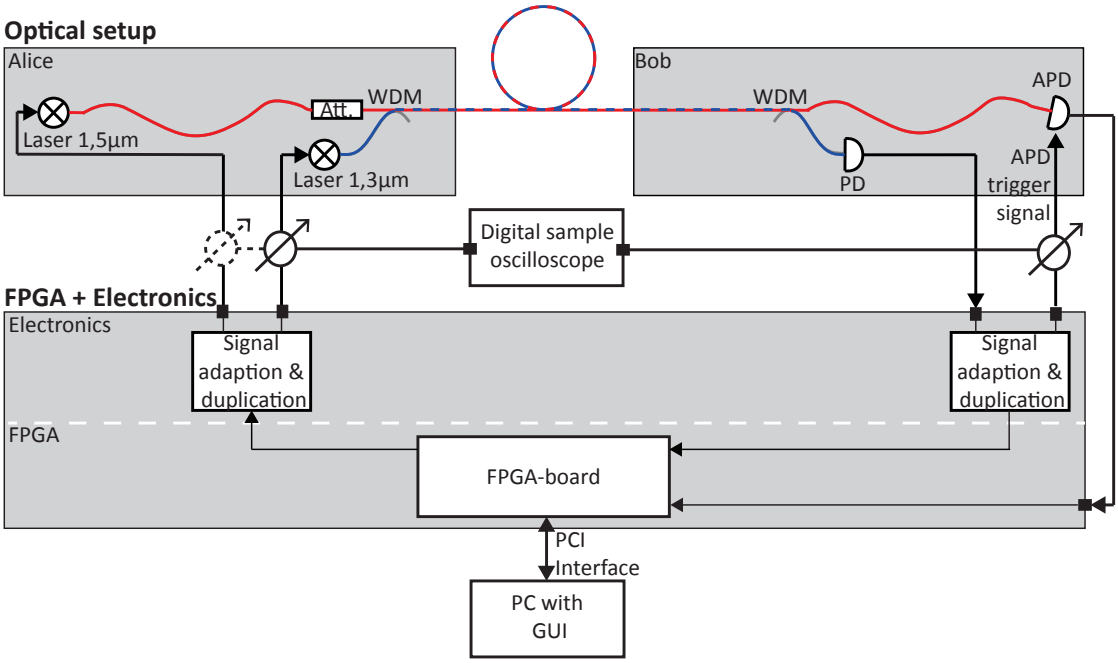


Figure 70: A scheme to test the light generation and detection of the setup as well as the synchronisation between sender and receiver. A measurement cycle is started with a laser trigger signal emitted by the field programmable gate array (FPGA). It ends on Bob's side with a single photon detection on the avalanche photodiode (APD), which has been triggered by a synchronisation signal emitted by Alice. This detection event is then indicated by a signal read in by the FPGA. If this cycle is completed and if the temporal resolution of the synchronisation is within the requirements, the scheme can be used for the quantum key distribution (QKD) experiment. The temporal resolution is measured with a fast digital sample oscilloscope probing the laser trigger signals on Alice's side and the APD trigger signal on Bob's side.

Starting point of the test is a 25 ns long TTL pulse as trigger signal. It is generated at 100 kHz from the FPGA. Both the optical synchronisation signal (blue in Figure 70) and after a time delay of about 32 ns the quantum signal (red in the figure) are transmitted. When the appropriate voltage discrimination level and the maximum delay for the pulse width modulation are set, the detected synchronisation signal from the photodiode (PD) is converted to an ECL pulse with 5 ns pulse-width. This signal successfully triggers the APD. Adapting the timing of the trigger signal by choosing appropriate lengths for the electric cables and the optical fibres as well as fine-tuning with an electronic delay directly adjustable at the APD enables single photon detection at a rate of approximately 7 kcts/s. This is the expected rate for pulses with mean photon number of 1 emitted at 100 kHz, a detection efficiency of 10% and the typical loss of the WDM devices and the transmission channel.

When th signal laser is turned off, the dark count rate is below 1 Hz, which shows that no additional noise is generated by the synchronisation pulses. The detection signal of the APD is successfully read by the FPGA. The signal for synchronising the FPGA is a TTL pulse of 20 ns pulse-width and is also read in by the FPGA. A PC connected to the FPGA via PCI runs a GUI. This GUI features counters which display the count rate of the APD detections as well as the synchronisation signal counts.

The jitter between the trigger signal on the sender side and the trigger signal for the APD on the receiver side is measured by a fast digital sample oscilloscope (Tektronix DPO 7104) by probes connected to each signal path (see Figure 70). It is measured to be 41 ps on average, thus clearly fulfilling the requirements on the temporal resolution. Figure 71 shows a screenshot of the oscilloscope during the measurement.

Figure 71: A screenshot of the oscilloscope during a performance test of the synchronisation. The yellow trace is the emitter coupled logic (ECL) laser trigger on the sender side, the blue trace the ECL trigger signal for the avalanche photodiodes (APDs) on the receiver side, which has been transmitted optically. Encircled in red at the bottom is the standard deviation of 38.15 ps of the time delay between the rising edges of both signals.

Increasing the attenuation in the quantum channel and thus simulating larger transmission distances quickly brings the synchronisation scheme to its limit. The output signal of the photodiode and its narrow pulse width then render the transformation to a digital signal extremely difficult. This represents a limit for this

scheme. Using a laser with a larger pulse width for the synchronisation would be an improvement.

The reference level of the discrimination voltage of the comparator which converts the analogue pulses from the photodiode (see Figure 67) is set manually via a DIP switch on a separate PCB (see Appendix B.2) for the test reported here. The PCB also offers the possibility to control it by the FPGA. This would enable an automatic adjustment to adapt to the actual transmission losses in a final implementation.

7.1.3 The control unit: field programmable gate arrays, software and digital-to-analogue converters

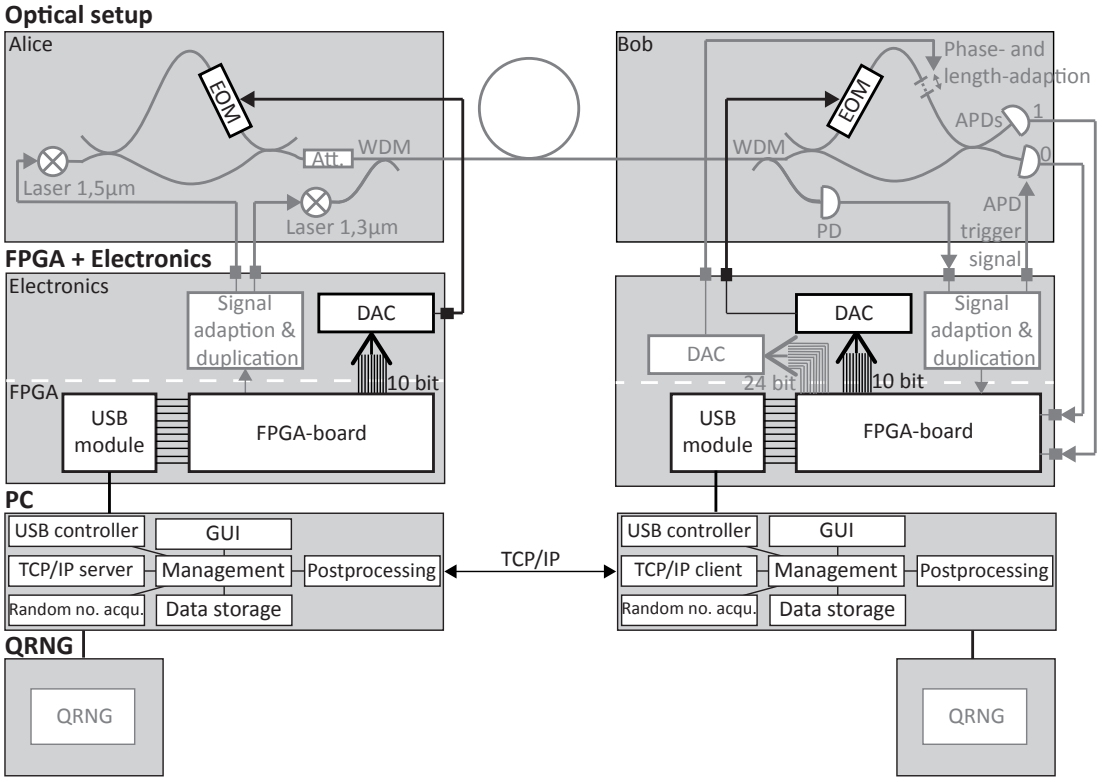


Figure 72: Shown are all components which are used to control the execution of the quantum key distribution (QKD) experiment (non-greyed out). This comprises field programmable gate arrays (FPGAs) both on sender and receiver side, each connected to a PC via USB for the execution of superordinate tasks and two digital-to-analogue converters (DACs) used to interface the FPGAs to the electro-optic modulators (EOMs).

Finally, the control and data acquisition unit of the experiment is reported on. At the heart of it lie two FPGAs, one each for sender and receiver, see Figure 72. It interfaces the optical setup. As has been presented, additional homemade electronics is needed for this. Part of this electronics are the DACs needed for the phase modulation by the EOMs (see figure), which are described in this section. The FPGAs also interface PCs via USB used for superordinate actions, as for example overall management processes like the initialisation of the experiment and key data storage. Also user control by GUIs is enabled, random numbers are acquired (Random no. acqu. in the figure) and an Internet connection between Alice and Bob is established. This is necessary not only for initialisation processes but also for the post-processing of the quantum key.

Since a complete time-bin BB84 setup for testing has not yet been available (see Section 7.1.1.2), the control unit is implemented and tested with the existing setup for QKD with single photons, see Chapter 5 and cf. Figure 73. Using this setup, the control and execution of mostly all interesting tasks can be tested. The QKD transmission management is executed by two PCs. When the transmission is started, at first an Internet connection is established between Alice and Bob. Also, random bits are obtained from a server connected to a QRNG ([172], see Chapter 8) which is located within the local network. A connection to the respective FPGA is established via USB. Once all connections are established and enough random numbers are obtained, the actual transmission is started. It is controlled by the FPGAs of Alice and Bob. First of all, the EOMs are set according to the random bits via DACs which transform the output bits of the FPGAs to an analogue voltage amplitude compliant with the predefined settings (entered via the GUI). The laser exciting the single photon source (SPS) is triggered at a predefined moment on the sender side and the APDs are read out the by Bob's FPGA the moment the photon should arrive. The obtained raw key is transmitted to the PC via USB. After transmission, sifting, error correction and privacy amplification are conducted.

There are only few differences with respect to the outlined time-bin setup: the Si APDs used here are free-running and do not need a trigger. The synchronisation is established with an electronic signal instead of an optical one. The free-space setup working with polarised photons does not need a phase stabilisation and length adaption nor any other feedback mechanism. Finally, only a single QRNG is used, connected to Alice and Bob via the local network.

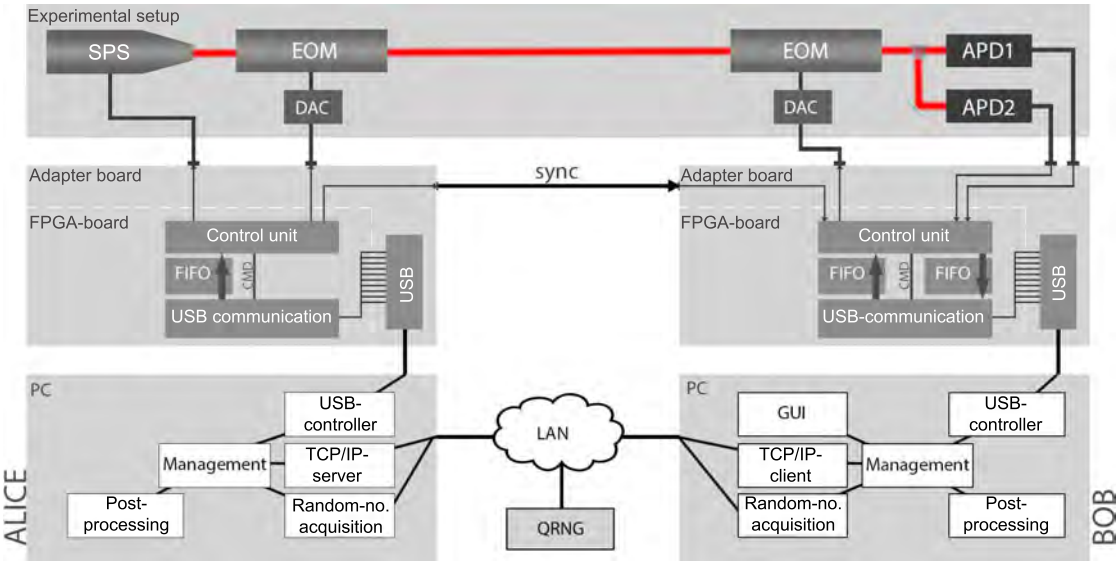


Figure 73: Scheme of the complete quantum key distribution (QKD) setup to test the control unit consisting of PCs, field programmable gate arrays (FPGAs) and digital-to-analogue converters (DACs). The QKD setup for this test consists of a single photon source (SPS) emitting single photons in free-space which are polarisation modulated by an electro-optic modulator (EOM) on Alice's side. Another EOM on Bob's side implements his basis choice. Two avalanche photodiodes (APDs) are used for detection. Contrary to the setup of Figure 72, the First In, First Out (FIFO) integrated circuits (ICs) used as intermediary between the USB modules and the FPGAs (control unit) are shown. Also, only one quantum random number generator (QRNG) is used which is connected to Alice's and Bob's PCs via Internet connection. Taken from [177]

Major parts of the presented work have been realised during a master thesis [177] in the framework of this dissertation. The work is based on results accomplished in an earlier master thesis [175], which were presented in Chapter 5. A major difference between both implementations is the type of FPGA which has been used. In the first project, a National Instruments FPGA (NI 7813R) programmable with LabVIEW has been tested. The FPGA has been interfaced via Peripheral Component Interconnect (PCI) with a PC for data storage and to realise a GUI (cf. Section 5.2.3). Additionally, a post-processing algorithm has been established by a separate software on this PC (cf. Section 5.3). This work has served as a blue print for the control and data acquisition unit presented now. In this recent implementation, GUI, experimental process management and post-processing are integrated within a single software. Also, two autonomous FPGAs for sender and receiver are used. Due to lower cost and higher flexibility, FPGAs directly programmable with Very High Speed Integrated Circuit Hardware Description Language (VHDL) are used instead of modules programmable in LabVIEW. Starting with a single FPGA

for both Alice and Bob, the concept is then expanded to separate units. Using large parts of code developed previously helps to save up resources.

7.1.3.1 The field programmable gate arrays

FPGAs are programmable logic similar to a programmable digital logic circuit [177]. They consist of an array of configurable basic modules, in-/output blocks for the in- and output of digital signals as well as specialised modules such as phase-locked loop (PLL) modules, block-random-access memory (RAM) and non-configurable modules realising specialised mathematical functions. All these modules are connected by a wiring system. A schematic setup of such a FPGA is shown in Figure 74. For Xilinx FPGAs, as used here, the basic modules are called configurable logic block (CLB) and consist of lookup tables (LUTs) realising the desired functionality and a Flash memory for the storage of this functionality.

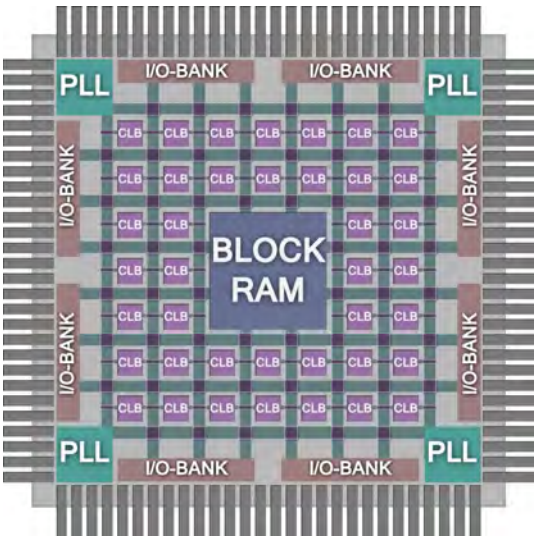


Figure 74: Schematical structure of a field programmable gate array (FPGA), taken from [177]

A FPGA is typically configured by loading relevant files from an external memory when powering up. The FPGAs used here are programmable with a development environment called Integrated Software Environment (ISE) design suite. It offers two different possibilities for programming the FPGA: with circuit diagrams combining different predetermined logic elements in a circuit or via the hardware description language VHDL which describes the hardware processes on an abstract level. Translating the programmed functions into the internal logic of the FPGA

is accomplished by a software module which is supplied by the producer for each type of FPGA individually.

Both FPGAs are used in the form of an evaluation board which additionally supplies the electronic environment including power supply, I/Os in the FPGA Mezzanine Card (FMC) standard, possibilities for Internet connections etc. Also available is a Joint Test Action Group (JTAG) port with which the FPGAs can be configured. One evaluation board, the Xilinx SP605, is used as both sender and receiver in a first test and later exclusively as sender. It uses a Spartan 6 FPGA. The receiver counterpart is a Zedboard Zynq-7000 development board, which uses a different programmable logic and an Advanced RISC Machine (ARM) microprocessor allowing for the implementation of a system on a chip (SoC). With this, an operating system independently of a PC could in principle be run, making the latter unnecessary. Despite some differences, the boards are similar enough to be described by a similar algorithm. The design of the electronic periphery is also very similar [177]. Like this, further resources are saved up.

The FPGAs have to accomplish several tasks. First and foremost, the quantum transmission has to be controlled as described above. Some processes involve communication with a PC via USB. Since no direct USB connection from the FPGA is foreseen, an external USB module is used (FTDI UM232H), which uses the serial synchronous FIFO format, which can handle data rates up to 40 MB/s.

The USB communication between FPGA and PC has to be configured. On the side of the PC, a driver provided together with the USB module can be used. Additionally, it has an interface for the configuration of the communication of the module with the FPGA. The serial synchronous FIFO format used here calls for FIFOs as communication buffers between the module and the FPGA. The FIFO adapts the module to FPGA communication, executed at 60 MHz, to the internal FPGA frequency which is derived by integer division of its clock frequency of 64 MHz. Not only the physical communication between module and FPGA has to be configured, but also the communication between PC and FPGA on a higher level of abstraction. All communication is supervised by the use of checksums.

14 of the FPGAs I/Os are used for this USB communication. All other I/O can be used to connect to the experiment. A specialized shielded cable with a VHDCI connector is used for this. As physical interface, a homemade PCB is used [177], which fits the FPGAs I/Os format (FMC) on one side and features a double VHDCI connector on the other side, as well as three BNC connectors and a layout for integration of the USB module, see Figure 75. The PCB also uses level shifters to adjust signal voltage levels of the FPGA of maximally 2.5 V to the electronic equipment of the experiment which needs 3.3 V.

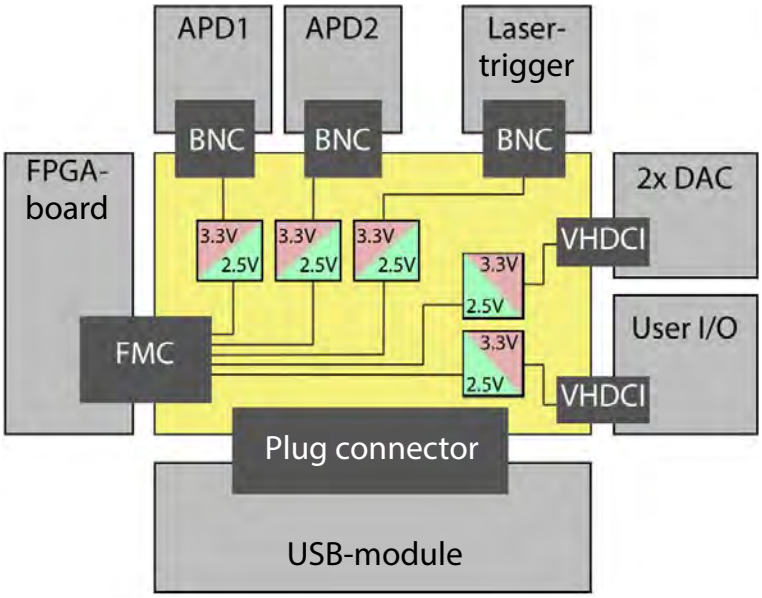


Figure 75: Schematics of the printed circuit board (PCB) used for interfacing the field programmable gate array (FPGA) with the experiment via very-high-density cable interconnect (VHDCI) and Bayonet NeillConcelman (BNC) connectors and the PC via USB. The FPGA itself is connected to the board with a FPGA Mezzanine Card (FMC) standard connection. Also shown are the level shifters from 2.5 V to 3.3 V. Taken from [177]

7.1.3.2 The control software

The software used for Alice and Bob are structurally similar. Both contain a software module for Internet communication to exchange data as well as a software module for USB communication with the FPGA. When both programmes are started, procedures as described in the beginning of Section 7.1.3 have to be performed, starting with the Internet connection between Alice and Bob. It is established from Bob to Alice by using her predetermined Internet Protocol (IP) address. Random numbers are acquired through an Internet connection to a QRNG server in the local network. In a future implementation, the random numbers should be acquired locally from two separate QRNGs for Alice and Bob in order to guarantee the secrecy of the random numbers. The FPGAs are configured via the USB connection. When all connections are established and the FPGAs are configured, the software representing Bob, which contains the GUI for user interaction, waits for input. In this GUI (see Figure 76), the user can enter experimental parameters in the *run* tab such as the key size to be sent by Alice, the repetition frequency and the exact timing of the laser trigger as well as the instance the APDs are read out,

which depends on the transmission distance. In the *config* tab of the GUI, e.g. the specific voltages to be applied to the modulators for the different bits and basis choices are entered in form of a number between 0 and 1023 each, corresponding to 10 bit. These numbers have to be determined by a pre-measurement.

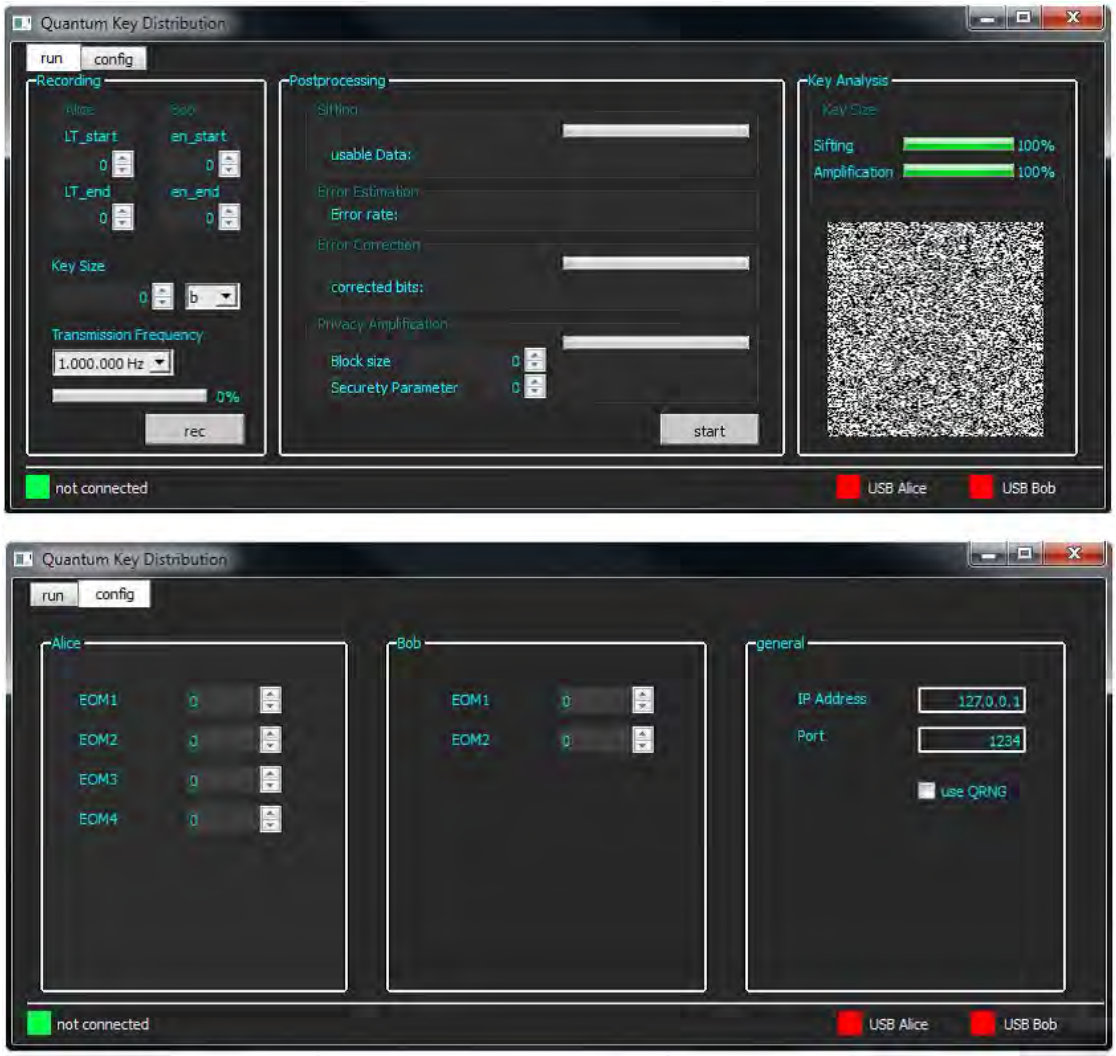


Figure 76: The *run* tab (above) and the *config* tab (below) of Bob's graphical user interface (GUI) to control the QKD experiment. Taken from [177].

Once the configuration is terminated and all entered parameters are transmitted, the transmission is initiated by both Alice and Bob downloading and saving the appropriate size of random numbers so no bottlenecks due to a bad Internet connection occur during transmission. When both FPGAs are synchronised, the

quantum transmission is started. After the transmission is completed, the processing of the raw key, which includes sifting as well as post-processing, can be started. For this, some parameters like the security parameter s (cf. Section 5.3) can be chosen via the GUI. After a secure key has been generated, statistics about the process, as sifted and secure key rate, are displayed as well as a binary picture of the secured key which should show no structure for a random key, see on top in Figure 76.

For building the software functionalities, the C++ library Qt is used, which contains ready-made modules for building GUIs as well as for Internet and USB communication. For the post-processing, existing software (see Section 5.3 and [175]) has been integrated.

7.1.3.3 The digital-to-analogue converters

Two DACs are used to translate the 10 bit signals of Alice's and Bob's FPGAs into analogue voltage signals for the EOMs. They are integrated on a single homemade PCB realised as part of this thesis. The complete circuit and the corresponding board are shown in Appendix B.4. A simplified circuit with a single DAC is shown in Figure 77. A DAC IC from Analog Devices (AD9740) puts out a current I_{DAC} proportional to the applied 10 bit value and a complementary current $\bar{I}_{DAC} = I_{DAC}^{max} - I_{DAC}$. The 10 bit in parallel (DB0-DB9) as well as a signal indicating a new bit value at the inputs is supplied by the FPGA (clock). The maximal output current of the DAC is 20 mA. With the termination of the output with 15 Ohm to ground, the differential input of the following differential amplifier (Analog Devices AD8129AR) is maximally 0.3 V. The gain of the amplifier is set by the feedback pin (FB). With the chosen resistances, a gain of $(1 + R_F/R_G) = 10$ is set, resulting in a maximal/minimal output voltage of ± 3 V. The last stage of amplification comes from a conventional operational amplifier (op-amp) (Linear Technology LT1363) in an inverting configuration with a gain of $R_F/R_G = 1.\bar{6}$. Like this an output voltage range of ± 5 V is produced. Also, the maximal current of the op-amp is large enough to directly drive the fibre-coupled EOM which is terminated with 50 Ohm. All components are high frequency components which work in the MHz regime. For the free-space polarisation-based BB84 scheme used here, existing high-voltage amplifiers designed in the Nano-optics research group precede the EOMs.

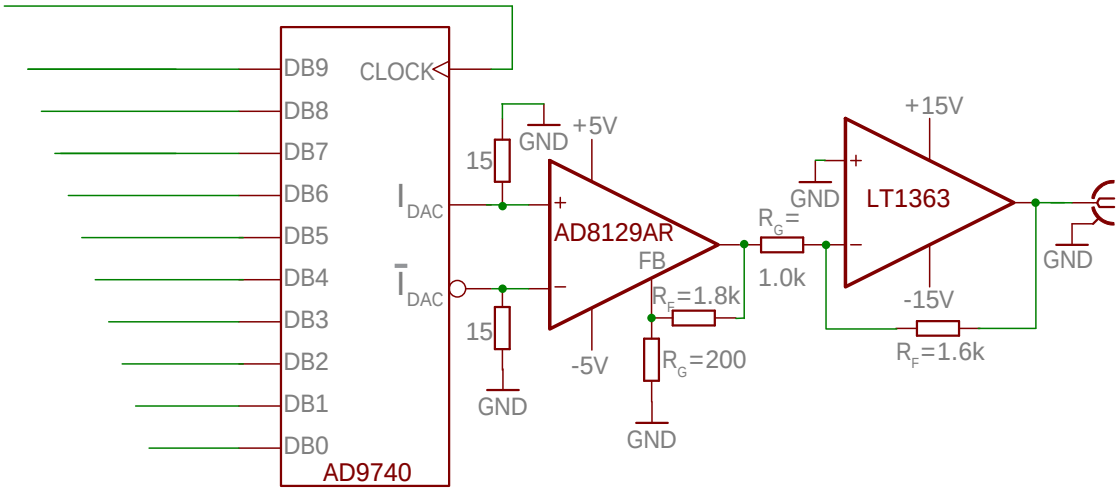


Figure 77: A simplified scheme of a single digital-to-analogue converter (DAC) used to drive an electro-optic modulator (EOM), consisting of a DAC integrated circuit (IC) (AD9740), a differential amplifier (AD8129AR) and an operational amplifier (op-amp) (LT1363).

7.1.3.4 Testing of the complete control unit

In a first test implementation, the Xilinx SP605 is used successfully as control unit for both sender and receiver. The control software for sender and receiver are run separately on a single PC and communicate via Internet within the local network of the research group. In a final test, the Zedboard Zynq-7000 is used as separate receiver control unit, synchronised to the sender via electronic signals. Also in this case, a secure quantum key has been successfully transmitted.

Only few steps are left to complete this control module: first of all, instead of an electronic signal, the optical synchronisation scheme of Section 7.1.2 shall be used. In addition, sender and receiver control software should operate on separate PCs and use separate QRNGs connected locally for their random number supply.

7.2 Summary and outlook

Major components of the time-bin plug & play scheme have been realised: the interferometers have been built with a compensation scheme for uncontrolled transformations of the polarisation in the interferometer arms. Strategies for length adaption of one interferometer to the other and active/passive phase stabilisation have been integrated by use of temperature stabilisation, a mechanically adjustable

optical delay line and a fibre-wrapped piezo ring. A first test has shown the principal feasibility of the phase stabilisation scheme. A DAC with a higher resolution and a feedback loop integrated in the FPGA control unit would be the next step towards robust high visibility interferometers for the realisation of an autonomously running time-bin BB84 QKD scheme.

In addition, a suitable optical synchronisation scheme between Alice and Bob with high temporal resolution has been successfully realised. In a future scheme, the current synchronisation laser could be replaced by a specimen with longer pulse length and/or higher intensity to make the transmission scheme suitable for longer distances.

An automated control unit for sender and receiver has been realised. It governs the complete experiment including the post-processing. In the future, it should be operated on two separate PCs and with random numbers from two local QRNGs, one each at Alice's and Bob's position.

Each module needs only few steps for completion. Integrating the modules into a complete time-bin BB84 setup will accomplish the implementation.

8 Realization of a quantum random number generator

Quantum randomness plays a principal role in quantum information processing (QIP). It manifests itself in quantum key distribution (QKD) when Eve measures in the wrong basis and cannot measure the qubit Alice sends to Bob deterministically. It also serves as a reliable and cryptographically safe source of randomness for the bit and basis choice of Alice and Bob in this context. In addition, good sources of randomness are indispensable for more practical or even mundane applications: they are an essential resource for classical cryptography and for Monte-Carlo simulations. Furthermore gambling and lotteries require good random numbers. For any of these applications, if the used random numbers are of low quality (see Section 8.1), because they do not occupy each possible random outcome with the same probability or because they are predictable, this can be fatal to the respective application. Thus, a generator of "good" random numbers, a random number generator (RNG), is of wide interest. If additionally the inherent randomness of quantum mechanics is exploited as in a quantum random number generator (QRNG) and if this device is practical and puts out random numbers at a high rate, then this device steps out of the niche other devices that apply quantum information processing still occupy.

A QRNG with an extremely high output rate of random bits of 152 Mbit/s has been realised in cooperation with PicoQuant GmbH and will be described in this chapter. PicoQuant GmbH has designed and manufactured the device while the testing and general analysis of the device was realised within this dissertation. This effort has led to a joint publication [172] and a public online service providing random numbers from the QRNG [145]. The QRNG has even reached the status of a commercial product [146].

This chapter is structured as follows: Section 8.1 introduces the general notion and scientific interpretation of randomness, how it can be produced and quantified. In particular randomness generated by random quantum processes is discussed.

The subsequent Section 8.2 presents the design and technical implementation of the QRNG and the deployed methods to guarantee the randomness of the output.

Finally, Section 8.3 analyses the resulting randomness of the output before and after post-processing. Randomness is tested by the application of an exhaustive randomness test on a large amount of random output sequences.

8.1 Random numbers

The need for random numbers has been motivated by a variety of straight forward examples. However, the definition and recognition of true randomness is a challenging task, as will be discussed in the following. Before regarding random numbers from a quantum perspective, the concept of randomness is introduced. A positive integer random number in binary format, a sequence of N random bits, can be described as $\mathcal{X} = \{x_0, x_1, ..., x_{N-1} | x_i \epsilon \{0, 1\}\}$. For a true random number, $P(x_i = 0) = P(x_i = 1) = \frac{1}{2}$, independently of all the other bits in the sequence. This is the same as saying that every possible $\mathcal{X}$ has equal probability of appearance of $P(\mathcal{X}) = 2^{-N}$ or that all 2^N integer numbers representable by the sequence are equally likely. Looking at a single number generated by a RNG does not give any information about its randomness. For this purpose, it is advantageous to look at the binary representation of this number, in which the probability of each bit and a possible bit interdependence might be revealed by statistical tests if the tested sequence is long enough. But the underlying probability distribution of the physical process used for the random number generation is not revealed by a statistical test of the output. Hence, in addition to statistical testing, this distribution should be analysed well to quantify the degree of randomness of a RNG.

Before this aspect is further formalized, different concepts of random number generation shall be introduced. First of all, an important distinction is to be made between pseudo random number generators (PRNGs) and true random number generators (TRNGs).

A PRNG uses a deterministic algorithm to produce a number with seemingly random properties out of a smaller seed consisting of a number or sequence which may be random. Beside the obvious deterministic relation between seed and output, even the output of a PRNG is often limited in its randomness , as can be revealed in statistical tests.

A TRNG utilizes a physical process such as thermal noise or quantum processes (see below) that is known or believed to be random. The process should be well understood in order to remove eventual residual deviations from an ideal random process by an adequate post-processing algorithm.

Quantum randomness has already been described in this thesis, for example when introducing the BB84 protocol in Section 2.2. The prototype of a random process is the single photon impinging on a 50:50 beam splitter (BS), with two single photon detectors, one at each output port of the BS (see Figure 78).

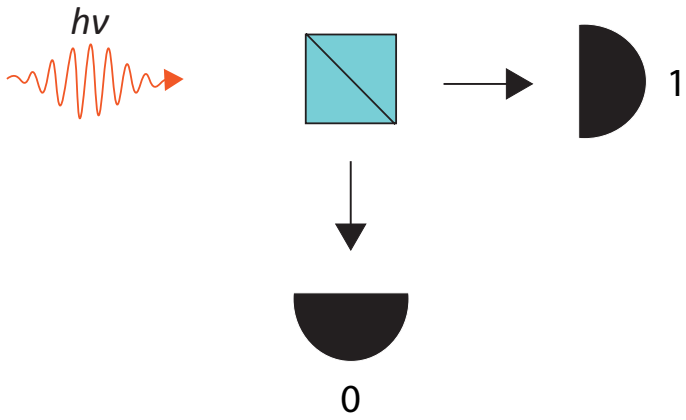


Figure 78: A simple scheme of a quantum random number generator (QRNG): a photon impinging on a beam splitter with two output ports. Each detector is associated with a different bit value.

In an ideal implementation of this experiment, with a perfect BS and perfect (or perfectly equal) detectors, the generated sequence of "0s" and "1s" each associated with a click of one of the two detectors is perfectly random. In reality, the beam splitter will most likely be imperfect, creating a little bias towards one bit value in the random sequence. Also, single photon detectors typically have a dead time, i.e. a time after a detection when the detector is not able to register another photon. If the period between two single photons is shorter than the dead time, correlated bits might be produced. In addition, with each photon only creating a single bit per detection, the overall bit rate is limited. Nevertheless, if carefully designed, this is a valid approach for a QRNG [147].

Alternatively, Poisson processes which have exponential waiting times like radioactive decays or the detection of a single photon from an attenuated Poissonian light source can be used [148, 149, 150]. The latter approach is implemented here, cf. Figure 79. The light of a light emitting diode (LED) is attenuated to single photon level with respect to the average period between two detection events in a photomultiplier tube (PMT). The waiting times between two detection events are registered by a time-to-digital converter (TDC). The particle-like nature of the single photons leads to waiting times between two detection events with a Poissonian distribution. This exponential waiting time can than be translated into a binary sequence by simply expressing the time in binary representation. In this manner, many bits can be created by only two successive events.

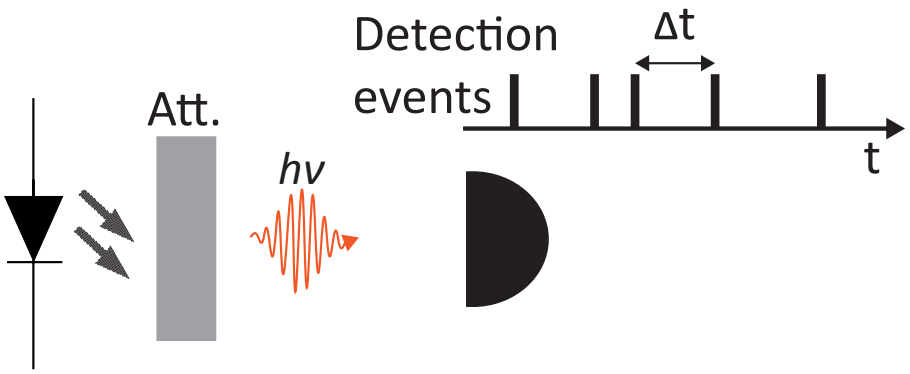


Figure 79: A different scheme of a QRNG compared to the BS solution in Figure 78: an attenuated light source emits single photons with a Poisson distribution. The random arrival times of the photons are exploited to create random numbers.

Because the waiting time distribution is exponential, it is not free of bias. But with an appropriate post-processing, this bias can be removed.

The randomness of a number can be quantified by the Shannon entropy, cf. Section 4.4.1. If some number or sequence $\mathcal{X}_k$ out of 2^N possibilities has a probability of appearance of $p(\mathcal{X}_k)$, the Shannon Entropy is

$$H(\mathcal{X}) \quad = \quad -\sum_{k=1}^{2^N} p(\mathcal{X}_k) \cdot \log_2(p(\mathcal{X}_k)) \,. \tag{118}$$

It gives a measure of the average information contained in the number in units of bits. If every number out of the set is equally probable, than one needs just as many bits as necessary to represent that same number, i.e. N. If the probabilities are not equally distributed, if there is e.g. a repetitive pattern in each binary sequence representing a number, then the Shannon entropy results in less than N bits. Hence it should be as close as possible to N for a random number generator.

A more rigorous way to measure the randomness of a number or bit sequence is the min-entropy H_∞,

$$H_\infty(\mathcal{X}) \quad = \quad -\log_2 \max_{\mathrm{k}} p(\mathcal{X}_k) \,. \tag{119}$$

The min-entropy gives a measure of the largest bit sequence such that all possible sequences have a probability of maximally 2^{-H_∞}.

To quantify either entropy, one needs to know the underlying probability distribution. If one is just confronted with a number or sequence claimed to be random, it is not obvious if it is really random. That is why tests for random numbers

have been established. Tests on a binary sequence calculate the probability of the actual test statistics of the tested characteristic under the assumption of perfect randomness. Only if this probability is above an agreed value, the randomness of the sequence is accepted. Since it is improbable but possible that a random sequence takes a highly unlikely form, a single failed test is not meaningful. Only a repetitive failure of many different sequences of a random bit string in a given test could confirm that the string is actually not random.

8.2 Design of the quantum random number generator

The quantum random number generator (QRNG) presented here is based on attenuated light from a LED which is detected by a PMT. The average photon detection rate is 40 MHz based on the detector capabilities. The time period between two detection events is recorded by ultrafast time-tagging electronics with a timing resolution of 1 ps [151]. With this ultra-high timing resolution, the measured waiting times can be measured with very high precision, resulting in many bits per measurement. This and the real-time post-processing provide extremely high output random bit rates.

One could argue that the photon statistics of the thermal light source (see Section 3.4.1) lead to correlations between successive waiting times. However, the according bunching effects would only be observed on timescales unaccessible to the detector due to its considerable dead time of 80 ns, hence they do not have any impact on the observed photon distribution.

Each waiting time event is registered by a 19 bit sequence which represents the waiting time measured in picoseconds. Taking the minimal time-bin Δt and the given photon rate λ, the probability mass function of a waiting time x_i between two detection events is

$$p(x_i) \;=\; e^{-\lambda i \Delta t}(1 - e^{-\lambda \Delta t}) \simeq \lambda \Delta t \cdot e^{-\lambda i \Delta t}\,, \tag{120}$$

where i denotes the i-th time-bin. This function is obtained by integrating the exponential waiting time distribution for the given rate over the width of a single time-bin.

With this, the Shannon entropy becomes

$$S \;=\; \frac{1 - \ln(\lambda \Delta t)}{\ln(2)}\,, \tag{121}$$

where the approximation of Equation 120 as well as an identity for the geometric series has been used.

The entropy is thus 16.05 bits, the min-entropy is 14.61 bits.

With the given dead time of the PMT, the effective detection rate λ' is reduced with respect to the raw rate to

$$\lambda' = \frac{\lambda}{1+\lambda\tau}, \tag{122}$$

with τ being the dead time. This formula can be found in the literature [152] and is obtained by calculating the expected time between two measurements supposing a Poissonian process and a dead time which is unchanged by detection events during the dead time. The effective rate is thus $\lambda' = 9.52\,\mathrm{MHz}$ with each detection event resulting in 19 bits.

The bias due to the exponential waiting time distribution can be removed by using an appropriate function for post-processing. For similar QRNGs, a secure hash algorithm (SHA)-256 function has been used for this purpose. However, there have been successful attacks on these functions [153, 154] which raise doubts about their usage for sensible applications. In addition, they are hard to implement efficiently.

Here, so-called (n, m, k)-resilient functions are used for the post-processing. A (n, m, k)-resilient function is a function f: $\mathrm{F}_2^n \to \mathrm{F}_2^m$, which produces a perfectly random output bit string (as defined at the beginning of Section 8.1) of length m for k fixed input bits and the other $n-k$ input bits perfectly random. They have the advantageous property that they can be used as resilient correctors [155] and as such have a quantifiable output bias for a known input bias. The input bias is the deviation of the probability of each bit of the input bit string from a perfectly random probability distribution. For a (n, m, k)-resilient corrector, the output bias is a polynomial of the input bias of minimally $k+1$th degree [155, 156].

In order for these resilient functions to work, it is important that the input bits are independent [156]. This is in general the case for an exponential waiting time distribution [157]. However, one has to take care that is is also true for the specific experimental implementation. This will be investigated in the next section for the QRNG realised here.

In order to produce real time random data, the post-processing is implemented directly into the field programmable gate array (FPGA) logic (see Section 7.1.3 for more information on FPGAs) of the timing electronics. The output is delivered via USB 2.0.

8.3 Results

When random data is successfully generated, it is important to know its properties well to quantify the quality of the produced randomness. This comprises an understanding of the underlying physical random process and testing of the statistical properties of the output data. That is why both a theoretical and experimental analysis of the resulting random data from the QRNG is carried out and presented here. In order to provide high statistically accuracy, 10 million photon waiting times have been collected to analyse the randomness of the raw data before post-processing. Also, 30 files of 1.3 TB each of post processed binary random data output from the QRNG have been tested with a statistical test tool specifically designed to test RNGs. This tool evaluates the randomness of output data by submitting it to different statistical tests and by comparing the distribution of the test results to the expected distribution of results when perfectly random data is assumed. The tested amount of data corresponds to several weeks of constantly generated random data of the QRNG.

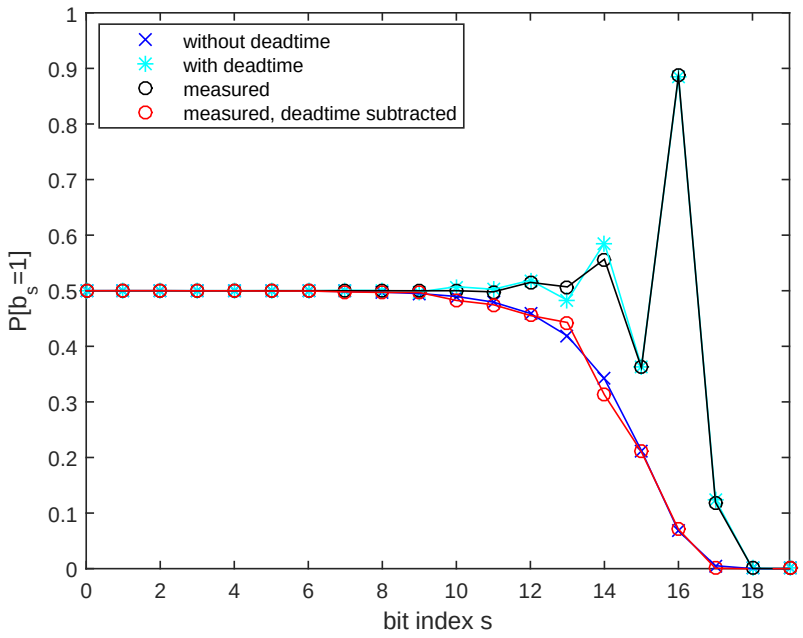


Figure 80: The bit value probability $P[b_s]$ as a function of the bit index s, without taking into account the detector's dead time (blue curve with crosses), with dead time theoretically (cyan curve with crosses), measured (black curve with circles) and measured with subtracted dead time (red curve with circles).

It was shown in [157] that sampling with n bits from an exponential distribution like the given one (cf. Equation 120) results in independent but biased random bits s with $0 \leq s < n$ with probability

$$P(b_s = 1) \quad = \quad \frac{1}{1 + e^{(-\lambda \Delta t 2^s)}}\,, \tag{123}$$

where $P(b_s = 1)$ is the probability of bit s being one. This probability is shown in Figure 80 (blue curve with crosses). It can be seen that the first eight to nine bits are almost free of bias. For more significant bits, thus bits representing higher powers of 2, a significant derivation from $P(b_s = 1) = 0.5$ can be observed.

In the case of the implemented QRNG, the dead time of the detector further influences the individual bit probability. The dead time can be interpreted as a temporal region with constant detection probability of zero,

$$f(t, \lambda, \tau) = \begin{cases} 0 \text{ for t} \leq \tau \\ \lambda \cdot e^{-(t-\tau)} \text{ for t} > \tau\,. \end{cases} \tag{124}$$

With this probability distribution, Equation 123 becomes

$$P[b_s = 1] = \frac{\int_{t=0}^{t=2^n} f(t, \lambda, \tau) \cdot (\lfloor \frac{t}{2^s} \rfloor \bmod 2) dt}{\int_{t=0}^{t=2^n} f(t, \lambda, \tau) dt}\,, \tag{125}$$

where t is in picoseconds and the probability is selectively integrated over all times where bit s is one. This probability is also shown in Figure 80 (cyan curve with stars), together with the measured data (black curve with circles), which shows good agreement.

During the dead time, detection events are impossible. This constant minimal waiting time does not have an effect on the least significant bits which are unbiased. For the most significant bits, which are biased, this constant minimal time is perceivable (cf. figure) and actually results in correlations between bits. This correlation is unwanted and also prevents the resilient function to work properly. This problem is solved easily by subtracting the constant dead time from the measured waiting times. By doing this, one recovers the original independent distribution from the measured data (cf. Figure 80, red curve with circles). The least significant bits could be used directly as a random output. Since this implementation targets a high random bit rate, no bits should be neglected. To make use of the more significant but biased bits, a resilient function is used to remove the bias of the raw bits.

(n, m, k)-resilient functions can be constructed from $(n, m, k+1)$ linear codes by the following scheme [158]: Let G be a generator matrix for an

$(n, m, k+1)$ linear code C. Define a function $f\colon \{0,1\}^n \to \{0,1\}^m$ by the rule $f(x) = x\,G^T$. Then f is an (n, m, k)-resilient function. Here, a Bose-Chaudhuri-Hocquenghem (BCH) code [159] is used to generate the resilient function. Starting point for the creation of the code is the generator polynomial. The polynomial used here is actually from a (255,231)-BCH code. Such a polynomial can be generated for example by a function integrated by default into Matlab. From this, a shortened (152,128,7)-BCH code is generated as described in the literature [160, 161] to form a (152,128,6)-resilient function. This function is also easily implementable in hardware [162].

An advantage of this implementation which used resilient functions for post-processing is that the maximal output bias of the generated random numbers can be calculated. This is done here following the example of Theorem 15 of [156]. Using the given theoretical and experimental input bias, respectively, as well as the generator matrix used, the maximal output bias is 10^{-22} for the theoretical input bias and 10^{-21} for the measured input bias.

In the experimental realisation, the input of the function is constructed by concatenating eight waiting times with 19 bits each. The number of resulting output bits after post-processing per sampled waiting time is 16 bits, in agreement with the Shannon entropy of the input distribution. With the given effective rate of detection, the output bit rate is about 152 MBit/s, which is to the knowledge of the author the highest reported at the time of the publication. For very sensitive applications, a resilient function with a higher compression rate could be considered to match the min-entropy of $\sim$14 bits per detection event. However, it should be pointed out that the performed analysis and the very low output bias already without further compression reduces the necessity to make use of the min-entropy.

For statistical testing, the extremely rigorous big crush test from the TestU01 Suite [163] has been used. The results are shown in Table 7. Tests with a large amount of input bits have been performed. 30 random data strings of 1.3 TB each are used to realise 31 different tests on each of them. Since a random sequence can consist of an unlikely pattern with a small but finite probability, occasional failures are within expectations. Only repetitive tests, as executed here, can give a reliable prediction about the randomness of the input bits.

Test	Passed	Test	Passed
SerialOver	30/30	SumCollector	30/30
CollisionOver	28/30	MatrixRank	30/30
BirthdaySpacings	30/30	Savir2	29/30
ClosePairs	29/30	GCD	30/30
SimpPoker	29/30	RandomWalk1	29/30
CouponCollector	30/30	LinearComp	30/30
Gap	30/30	LempelZiv	30/30
Run of U01	30/30	Fourier3	30/30
Permutation	30/30	LongestHeadRun	30/30
CollisionPermut	30/30	PeriodsInStrings	30/30
MaxOft	30/30	HammingWeight2	30/30
SampleProd	30/30	HammingCorr	30/30
SampleMean	30/30	HammingIndep	30/30
SampleCorr	30/30	Run of Bits	30/30
AppearanceSpacings	30/30	AutoCorr	30/30
WeightDistrib	30/30		

Table 7: Results of the 31 different tests of the big crush battery of the TestU01 Suite [163], tested on 30 files of 1.3 TB each. The occasional failures ($< 0.2\%$) of individual tests are within statistical expectations.

To illustrate how the randomness is actually tested, two specific tests out of the 31 tests are described qualitatively, *LempelZiv* and *Run of Bits*. *LempelZiv* counts the number of distinct patterns W in the bit string as proposed in the compression scheme by Ziv and Lempel [164]. Under the assumption of randomness and for large bit strings of length n, W is approximately normally distributed with a mean and a variance which are functions of n [165].

Each binary sequence consists of a run of ones followed by a run of zeroes and so on or vice-versa. For *Run of Bits*, the length of the runs of ones and of zeroes is collected until there is a number of n runs for each [165]. The number of runs of ones and zeroes of length j each are counted for $j = 1, \ldots k$ for some k. Runs of length larger than k are grouped with the runs of length k. The expected number of runs of length j is simply given by 2^{-j}. A Chi-squared test is then applied on the $2k$ length counts of the tested sequence.

The introduced QRNG has become a commercial product, the PQRNG 150 [146]. One device is permanently connected to a server at the Department of Physics of the Humboldt-Universität zu Berlin (HU Berlin) and offers the possibility of

downloading unique random numbers for various applications [145] to the public. Random numbers from this generator have also been used for some of the performed experiments in this thesis.

After 20 months of continuous operation, the randomness of this specific QRNG has been re-tested by the same testing procedure as discussed above. The test results [174] show the long term stable operation of the QRNG and its uncompromised random output.

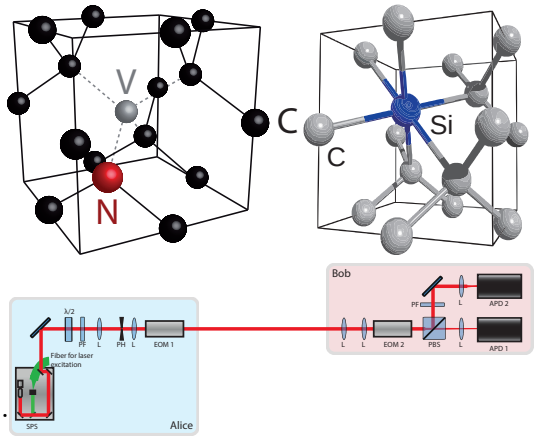
8.4 Summary

A practical and ready-to-use QRNG with an output rate of 152 Mbit/s has been implemented. The underlying randomness distribution has been thoroughly analysed and tested. To remove its residual bias, a resilient function is used, which provides a bound for the output bias of the random bits given the known input bias. The randomness of the output and the stable longterm operation of the device has been proven by repeated rigorous testing.

9 Summary and outlook

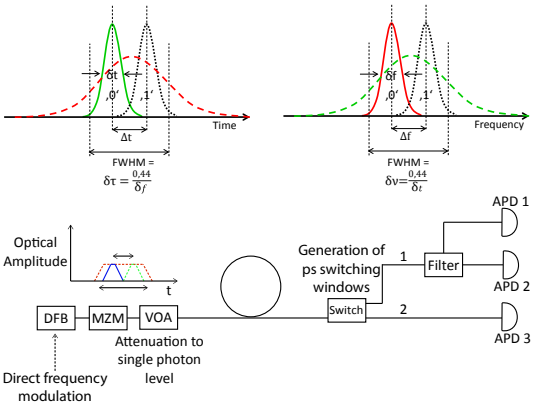
This thesis has given a thorough introduction to quantum key distribution (QKD), has implemented a new protocol for QKD, and has introduced a few QKD related aspects, such as QKD with compact mobile single photon sources (SPSs) and in particular the generation of random numbers from a quantum random number generator (QRNG). The first section of this chapter chronologically summarises the theoretical and experimental results of this thesis as well as important building blocks towards future experiments which were implemented. In the last section, an outlook is given on future experiments which will be enabled and motivated by the research conducted in this thesis.

9.1 Summary

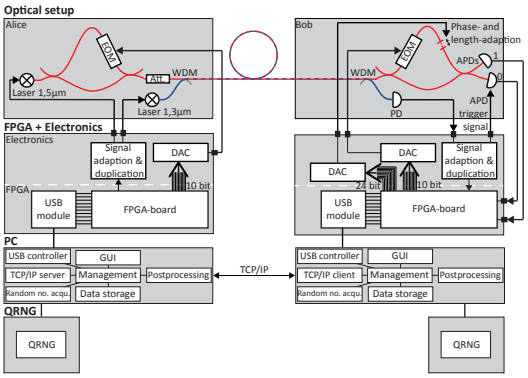


In **Chapter 5**, the implementation of a testbed for BB84 QKD experiments with single photons from single quantum emitters was reported. This testbed was used for quantum key transmission with single photons emitted from nitrogen vacancy (NV) and for the first time also silicon vacancy (SiV) centres in diamond. The transmitted key was post processed to a secure key by a CASCADE algorithm programmed in the framework of this thesis. A thorough security analysis for QKD with imperfect single photon sources (SPSs) was established and requirements on future SPSs were discussed which are able to compete with attenuated laser pulses using decoy states [84].

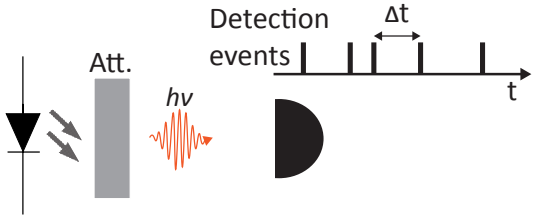
Chapter 6 reported on a protocol relying on the time-frequency uncertainty, the frequency-time (FT) protocol, which was implemented for the first time while using mainly off-the-shelve telecom components. Different parameter sets describing the time and frequency states were used for successful QKD. Numerical simulations have shown that a secure key can be generated using the FT protocol supposing individual eavesdropping attacks specific to the protocol.



Chapter 7 reports on the realisation and testing of fundamental building blocks of a fully automated fibre-based time-bin BB84 QKD scheme. Functional control units consisting of field programmable gate arrays (FPGAs) and a personal computer (PC) for sender and receiver were established as well as a synchronisation and detection unit enabling the autonomy of both. Large parts of temperature stabilised unbalanced interferometers with the capacity of automatic length adaption and phase stabilisation were implemented.



In **Chapter 8**, a high bitrate QRNG was reported. The device outputs a ready-to-use 152 MBit/s of random bits. The randomness of the underlying waiting time distribution was characterized theoretically and experimentally. Due to resilient functions which were used for maximizing the randomness of the output, the maximal bias of the output bits can be quantified for the known input bias. The long term stability after 20 months of operation of the device was shown.



9.2 Outlook

The presented **QKD experiment using defect centres as single photon source (SPS)**, could, by implementing a few technical improvements, reach much higher transmission rates. The key rate was mainly limited by non-optimised single

photon emitters and relatively slow electro-optic modulators (EOMs) drivers. Especially the SiV defect centres have not yet been used up to their full potential. Despite the relatively low probability of single photon emission per excitation pulse, much higher excitation rates are possible due to the short lifetime of the SiVs centre. In the research group of Christoph Becher in Saarbrücken, a SiV centre excited at 80 MHz delivered a count rate of 230 kcps with a $g^{(2)}(0) < 0.1$ [171], see Figure 81. Using a testbed with capabilities of faster polarisation modulation, as would be achievable with more advanced amplifiers for the EOMs used, this could be exploited to implement a high bit rate QKD experiment using single photons.

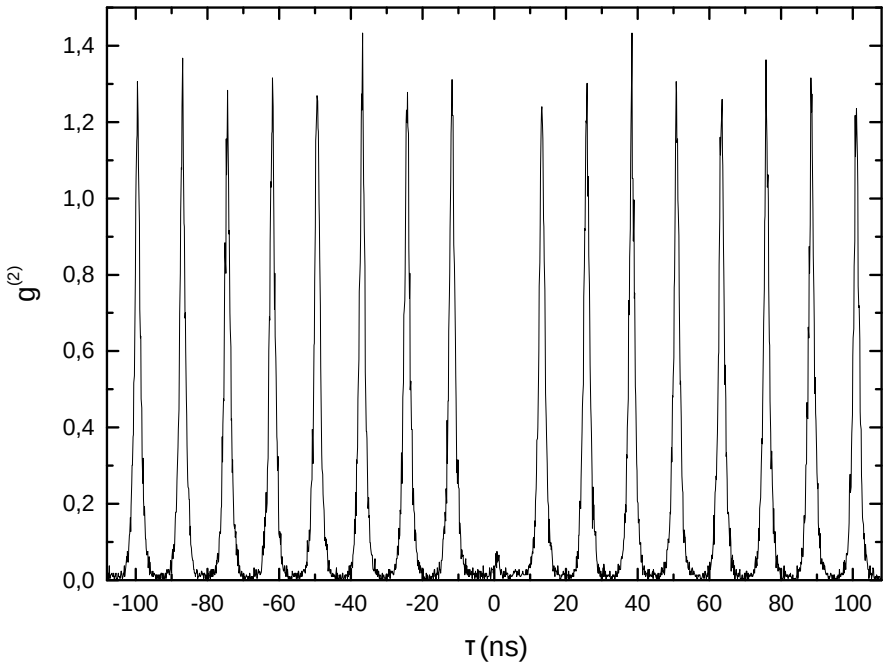


Figure 81: The figure shows the $g^{(2)}(\tau)$ value for a SiV centre for pulsed excitation at a repetition rate of 80 MHz. The count rate is 230 kcps with $g^{(2)}(0) < 0.1$. With courtesy of the research group of Christoph Becher from University of Saarbrücken.

A key message of the theoretical investigation of the suitability of SPSs for QKD in this thesis could be summarised as follows: for a SPS to be attractive for quantum information processing (QIP) and especially for QKD, a short lifetime, a quantum efficiency near unity, high coupling into a usable (preferably single) optical mode and a strong suppression of multi-photon events are mandatory requirements. Projections onto each of these requirements into the future are made now, showing the path to such high performance SPSs. Besides the SiV centre,

also chromium (Cr) based defect centres in nanodiamonds have shown very bright single photon emission [114] and short lifetimes.

Unfortunately, the quantum efficiency of the SiV and other defect centres can be quite low. However, it has been shown that the quantum efficiency may vary significantly within different nanodiamonds and that emitters with more than 90% efficiency can be selected [166, 167]. An approach to enhance the quantum efficiency requires enhancement of the radiative rate due to the Purcell effect [168, 169] which is technically more challenging for a room-temperature emitter [80] but has been demonstrated recently in [170].

Photonic structures to efficiently couple single photons from point-like SPS like defect centres in nanodiamonds to a usable output mode have been demonstrated [83, 79, 123] and show that collection efficiencies near unity might be possible in the near future.

To suppress multi-photon events, near resonant excitation might be useful. Also, using narrow band emitters, like SiV and Cr based defect centres would allow for better filtering of the emitted light to reduce background photons.

All these approaches, their advantages and drawbacks, as well as new and not yet known defect centres or other single photon emitters might be experimentally analysed in depth using the QKD testbed implementation with its flexible and easy-to-use confocal microscope setup. To test the performance limits of SPSs, as mentioned, higher repetition rates of the QKD experiment would be desirable, as would be readily achievable by the implementation of faster EOMs drivers.

Another interesting future application of the setup, in particular considering its robustness and practicability, is the possibility to use it as student experiment. These are an integral part of university studies in physics to enable the students to perform experiments that are very close to those in modern laboratories. The first hand experience of QIP with single photons could motivate students for a research career in the field. The use of the setup with students has already been successfully conducted several times.

For the **frequency-time (FT) protocol**, several paths shall be pursued in the future. First and foremost, the existing setup could be simplified by using a narrower frequency separation between the two states of the frequency basis to relax the requirements in the timing resolution of the setup and/or using superconducting single photon detectors (SSPDs) with a high timing resolution of about 30-50 ps for a direct measurement of the arrival times. With this method, no switching on Bob's side would be necessary, which would reduce the overall complexity and the error-proneness of the measurement in the time basis. Additionally, a complete independence of the setup on the polarisation would be achieved this way. If an

automated long term stable setup is striven for, no feedback mechanism on the receiver side would be required. This would be a huge experimental advantage compared to many other schemes.

Another important capacity of the scheme is the easy expansion to a higher number of possibles states per transmission in time and frequency, probably enhancing the security of the scheme. If the expansion in the dimensionality of states is accompanied by an expansion in the dimensionality of bits per transmitted state, the transmission rate could be dramatically increased. This expansion is currently pursued at the Heinrich Hertz Institute (HHI), cf. Figure 82.

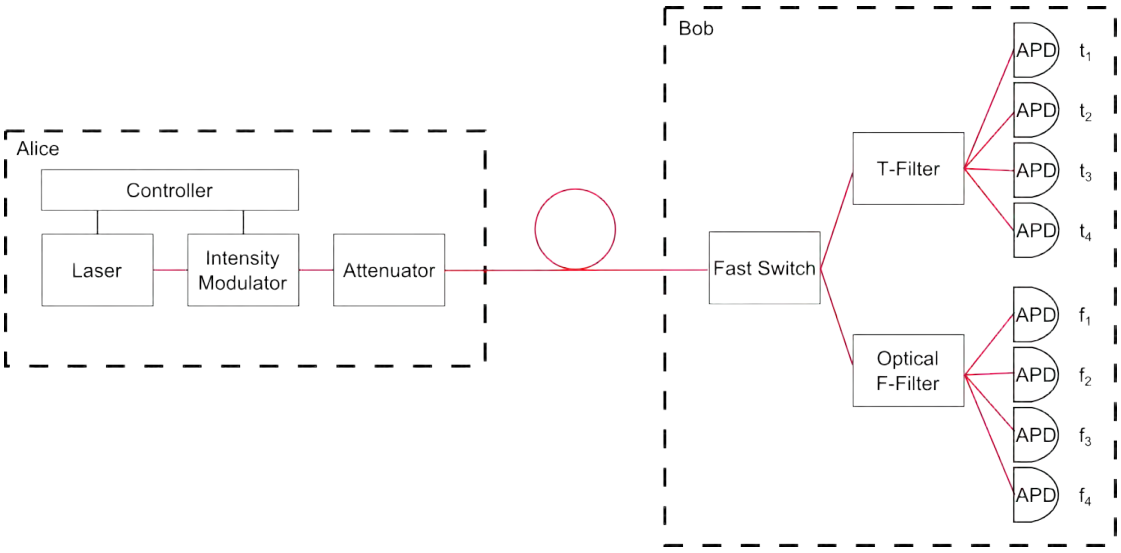


Figure 82: Planned setup of an experiment for the frequency-time (FT) protocol with two transmitted bits per signal. On the sender side, four instead of two frequency states are generated by a laser for the frequency basis. Pulses at one of four different instants in time are generated by the intensity modulator for the time basis. Correspondingly, on the receiver side, four different time and frequency states, respectively, have to be distinguished by appropriate filters and four different avalanche photodiodes (APDs) per basis. If very fast single photon detectors like superconducting single photon detectors (SSPDs) are used, a single detector suffices to implement the measurement in the time basis. With courtesy of the Heinrich Hertz Institute (HHI).

The FT protocol is very well suited for long distance satellite transmission. To make a step towards this long-term goal, line-of-sight automated free-space transmission over 500 m between Technische Universität Berlin (TUB) and HHI is currently planned using the expertise of free-space optical systems group of the HHI and their pre-installed free-space sender and receiver units, see Figure 83.

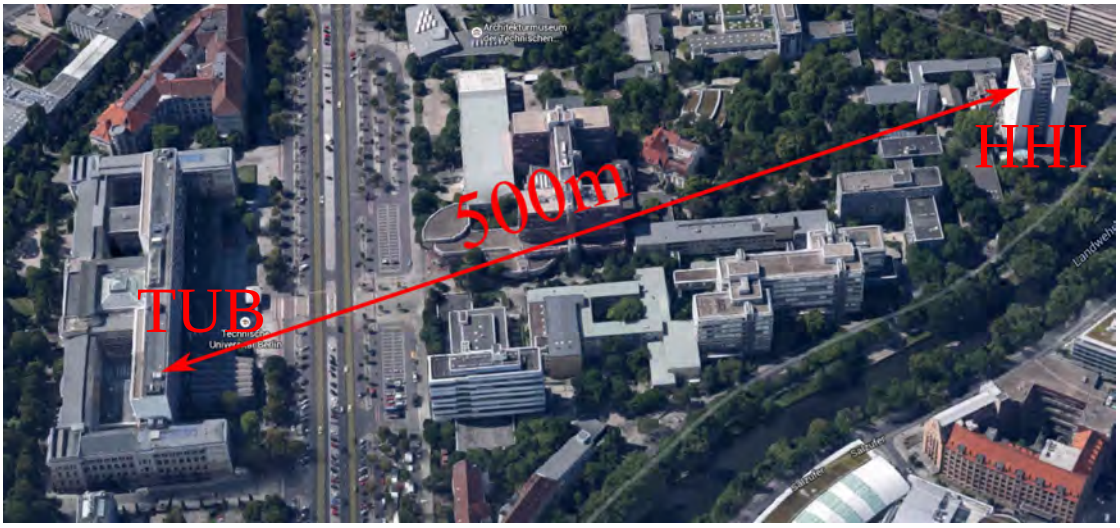


Figure 83: Planned line-of-sight free-space transmission between Technische Universität Berlin (TUB) and Heinrich Hertz Institute (HHI) using pre-installed sender and receiver units. With courtesy of the HHI.

Finally, collaborations with renowned quantum information theorists would enable a more thorough security analysis and could also establish a proof of unconditional security in the future.

For the fibre-based **time-bin BB84 QKD setup**, the future steps are quite clear: expanding the length adaption and phase-stabilisation capabilities of the interferometers, integrating its control loop into the existing FPGA control unit on the receiver side, enhancing the long distance synchronisation capabilities by using stronger and/or longer synchronisation pulses, and combine everything in a complete, automated setup. This setup could not only be used as a benchmark to other protocols and implementations, it could also be used as a testbed for new variations of the existing protocol and/or to test new eavesdropping attacks on their effectiveness.

In the future, the experiment could also be used as a very advanced student experiment representing the status quo of secure information transfer in QIP.

The **quantum random number generator (QRNG)** has already reached the status of a commercial product [146] offering higher random bit rates than any other comparable product on the market. In addition, on average 0.8 Gigabyte each day have been downloaded from the website of the Humboldt-Universität zu Berlin (HU Berlin) [145]. In the near future, quantum random numbers could also be delivered as an exclusive licensed service to companies or research groups in need of good and safe random numbers, possibly with extended cryptographic protection

when transmitted via the Internet or even with a locally installed QRNG. Also, higher rates through parallelization of several devices can be envisaged, which could be vital for some applications.

A No cloning theorem

A perfect quantum cloning machine could be represented by the following mechanism:

$$\hat{C}\,|0\rangle\,|\Psi\rangle \;=\; |0\rangle\,|0\rangle \tag{126}$$
$$\hat{C}\,|1\rangle\,|\Psi\rangle \;=\; |1\rangle\,|1\rangle \tag{127}$$

$|0\rangle$ and $|a\rangle$, respectively represent the state to be copied, $\hat{C}$ the copy-operator and $|\Psi\rangle$ represents the blank state of the "copy machine". By linearity of quantum mechanics, if $\hat{C}$ is to be applied to a superposition state, our copy machine would produce the following:

$$\hat{C}(\alpha\,|0\rangle + \beta\,|1\rangle)\,|\Psi\rangle \;=\; \alpha\,|0\rangle\,|0\rangle + \beta\,|1\rangle\,|1\rangle \tag{128}$$

This does not correspond to the desired cloned state, which is

$$(\alpha\,|0\rangle + \beta\,|1\rangle)(\alpha\,|0\rangle + \beta\,|1\rangle)\,. \tag{129}$$

B Circuits and Layouts of printed circuit boards

B.1 The analogue to broadened ECL converter

The full circuit (Figure 84) as well as the layout (Figure 85) of the printed circuit board (PCB) introduced in Section 7.1.2.3 (see especially Figure 68) is shown. It is used for the conversion of the analogue electronic signal coming from a photodiode into a digital emitter coupled logic (ECL) signal, whose pulse width is then broadened. The principal integrated circuits (ICs), shown as dark red rectangles, triangles and octagons with dark red labels, consist of the digital-to-analogue converter (DAC) (AD9740), the two fast comparators (ADCMP581 and 566), the delay chip (SY100EP195) and the flip-flop IC (MC100EL31) as described in Section 7.1.2.3. Additionally, a voltage-controlled oscillator (VCO) (LTC1799) and a Schmitt-trigger (NC7SZ14) provide a clock input to the DAC of about 7 MHz. Also shown is a second delay chip (SY100EP195V) in front of the S input of the flip-flop. This IC does not provide any noticeable delay, it is merely used to provide an input pulse comparable to the R input of the flip-flop which is also preceded by a delay chip. In front of the SubMiniature version A (SMA) outputs, a line driver (MC100EP11) provides sufficiently powerful signals and protects the sensitive circuitry from short circuits.

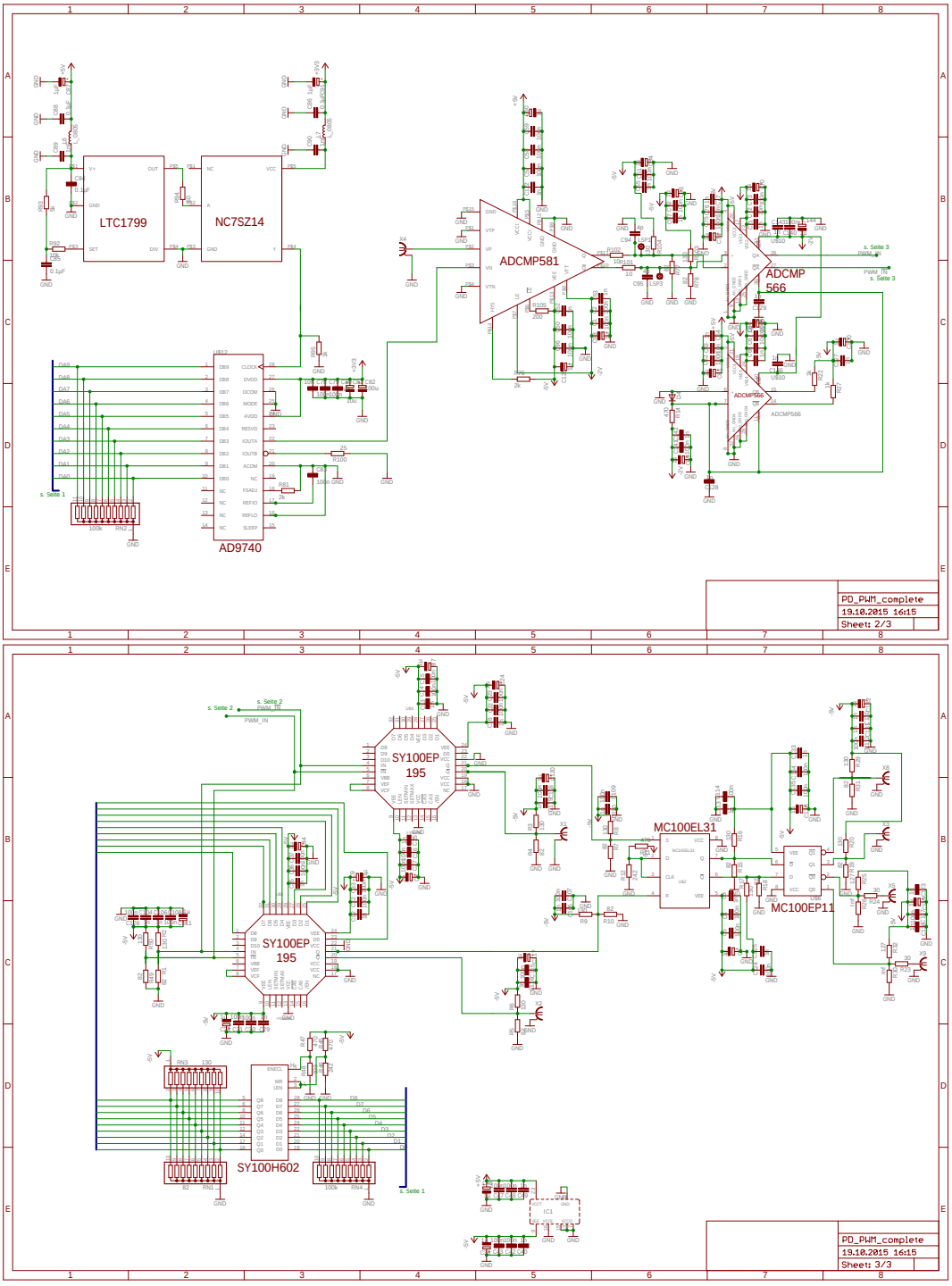


Figure 84: The complete circuit of the analogue to ECL converter with pulse width modulation (cf. Section 7.1.2.3). Shown on top is the first part of the circuit. All components, as the principal integrated circuits (ICs) and all resistances, capacitors etc. are dark red, the electrical wiring is green. Not shown are the ICs for power supply.

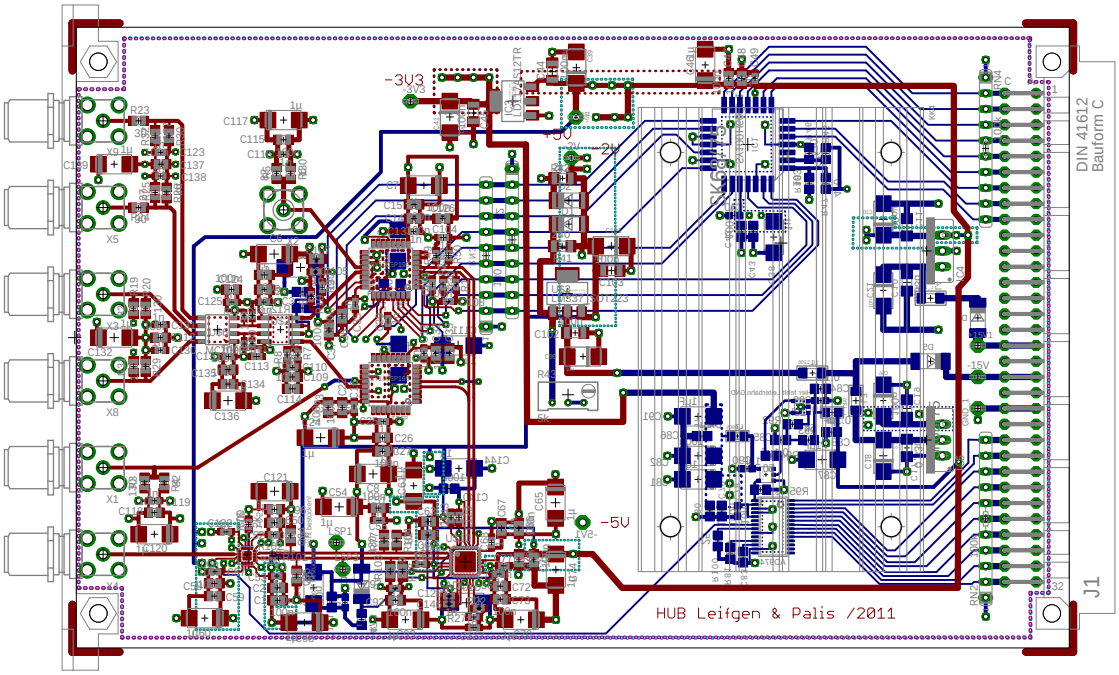


Figure 85: Top view of the layout of the printed circuit board (PCB). Components and wiring on top are shown in dark red, those on the bottom in blue. On the right side one can see five SubMiniature version A (SMA) outputs and one SMA input. On the left side an interface for controlling some of the boards functionalities.

B.2 The control board

The just presented printed circuit board (PCB) needs two adjustable parameters as input: the reference voltage V_{ref} (see Section 7.1.2.3) as well as the pulse width of the output emitter coupled logic (ECL) pulse by setting Δt *delay* (see Section 7.1.2.3). It therefore has an interface which is connected to another PCB with a broadband cable. This PCB offers the possibility to set these parameters either manually with two 10 bit DIP switches or with a connection to a field programmable gate array (FPGA) with a very-high-density cable interconnect (VHDCI) connector. The circuit is shown in Figure 86. It basically consists of the two DIP switches connected to the interface with the other PCB. The VHDCI connector for the FPGA is also linked to this interface. To avoid interference between manually set parameters and FPGA controlled parameters, there are two switches enabling the one or the other mode of control. The layout of the board is shown in Figure 87.

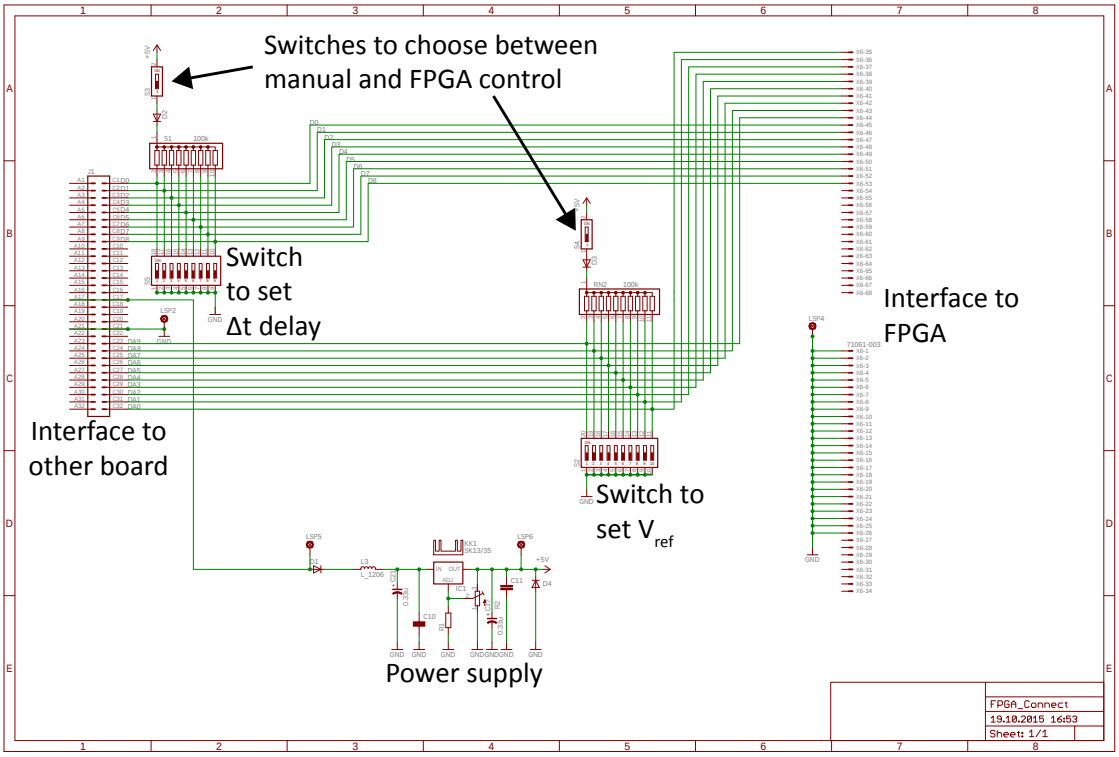


Figure 86: The circuit of the board used for setting the reference voltage as well as the pulse width of the printed circuit board (PCB) from Section 7.1.2.3 and Appendix B.1 above. Green lines represent electrical wiring, all dark red symbols represent components. The setting of V_{ref} and Δt *delay* can be done with dual in-line package (DIP) switches or externally via a signal coming from a field programmable gate array (FPGA).

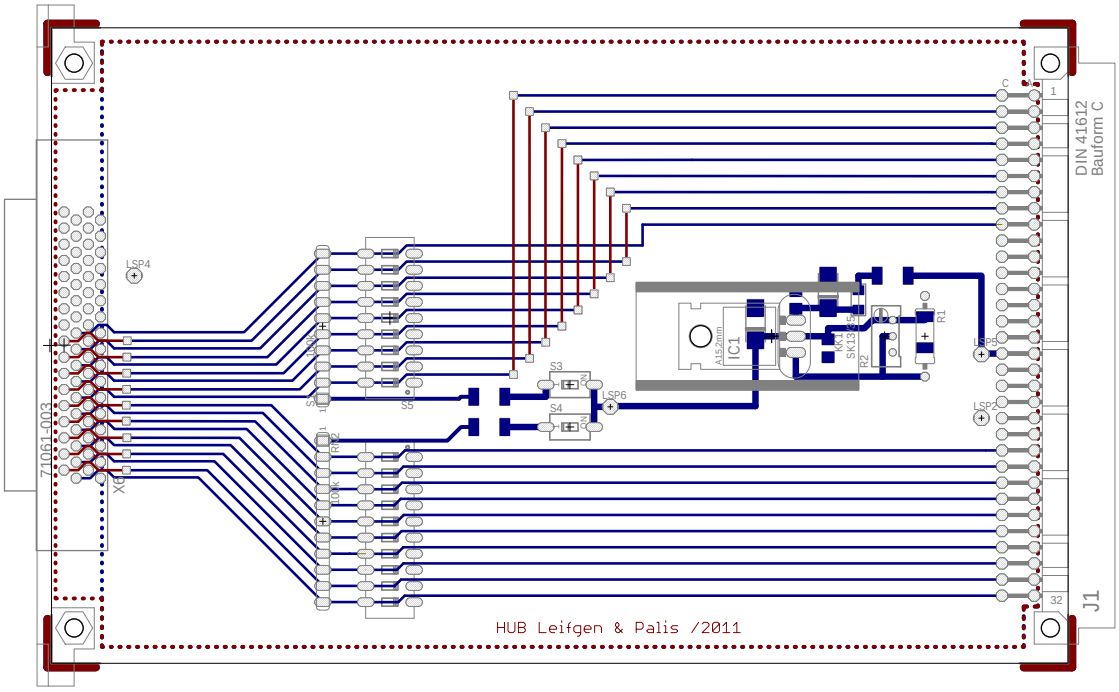


Figure 87: The top view of the layout of the described board is shown. All wiring and components on top of the board are symbolised by dark red colouring, on the bottom by blue colouring.

B.3 The board for ECL to TTL transformation and pulse-width modulation

The circuit in Figure 88 is used for further broadening the output emitter coupled logic (ECL) of the board presented in Section 7.1.2.3 and Appendix B.1. The pulses are then translated to transistor-transistor logic (TTL), so they can be used as synchronising input to Bob's field programmable gate array (FPGA). The incoming ECL pulse is first of all reshaped after its transmission by a driver integrated circuit (IC) (MC100EL12). Afterwards, a pulse broadening scheme similar to the one presented in Section 7.1.2.3 and Appendix B.1 is used, with two adjustable delay ICs (SY100EP195) and a flip-flop chip (MC100EL31). The delays and thus the resulting pulse width are adjustable by a DIP switch in a range between approximately 4 ns and 24 ns. The pulses are then transformed to TTL by a translator IC (MC100ELT25).

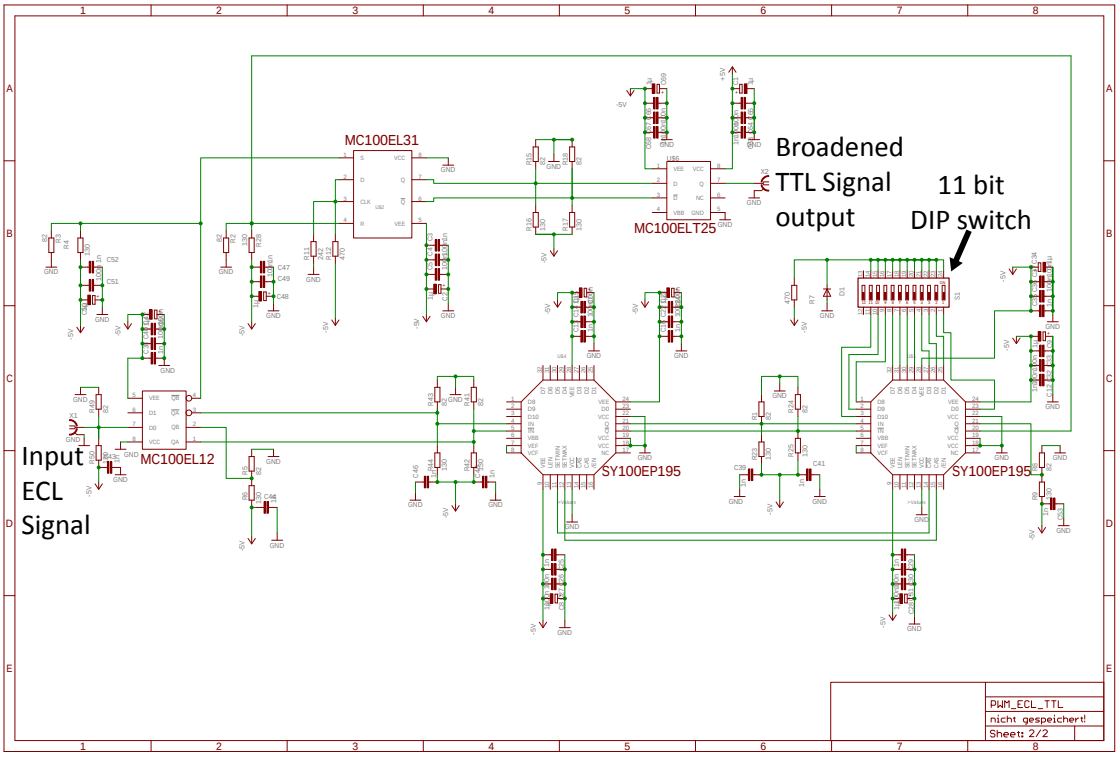


Figure 88: The printed circuit board (PCB) for emitter coupled logic (ECL) to transistor-transistor logic (TTL) transformation and pulse-width modulation. All principal integrated circuits (ICs) are symbolised by red rectangles or octagons. Small, basic components such as resistances and capacitors are also shown in red. The electric wiring of the circuit is represented by green lines. All ICs which are described in the text are labeled. Not shown are ICs for power supply.

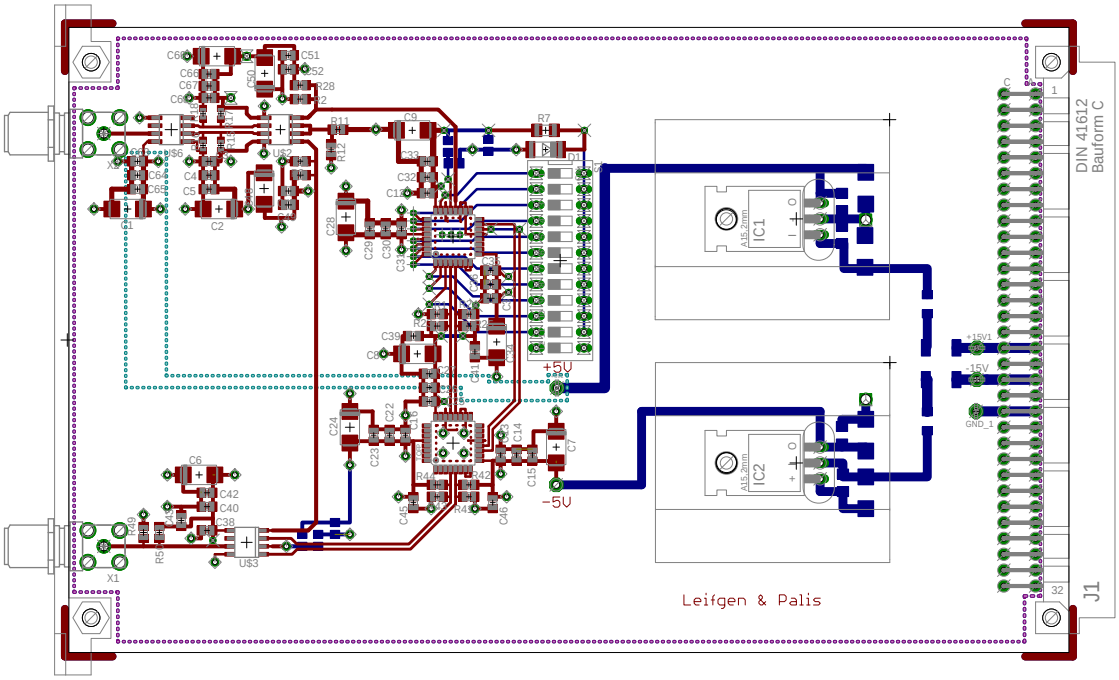


Figure 89: Top view of the board layout of the described circuit. All lines and components on top of the board are symbolised by dark red colour, the ones on the bottom in dark blue.

B.4 The digital-to-analogue converter

Figure 90 shows the full circuit of the digital-to-analogue converters (DACs) presented in Section 7.1.3.3, with both DACs integrated on a single PCB. It is originally equipped only with one VHDCI connector for use with a single FPGA for sender and receiver (cf. figure). It has been subsequently extended to feature a second connector, so it can be used with two separate FPGA platforms (not shown).

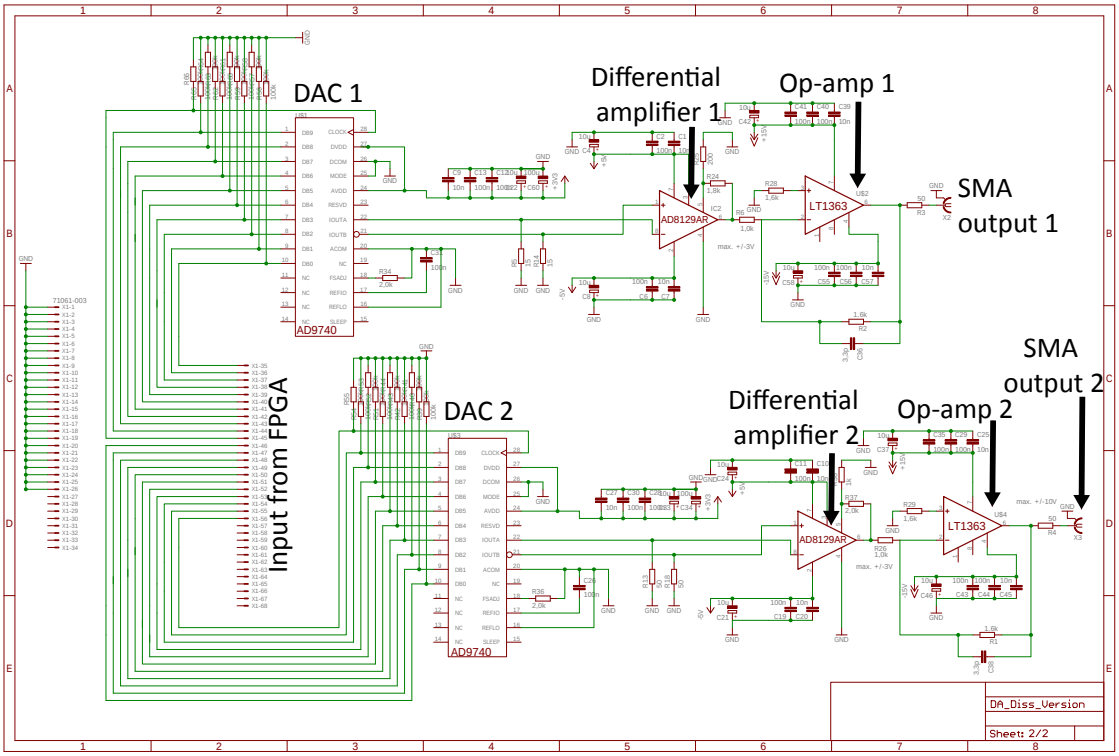


Figure 90: The circuit of the double 10 bit digital-to-analogue converter (DAC) as described in the text (shown without integrated circuits (ICs) for power supply).

The board layout is shown in Figure 91.

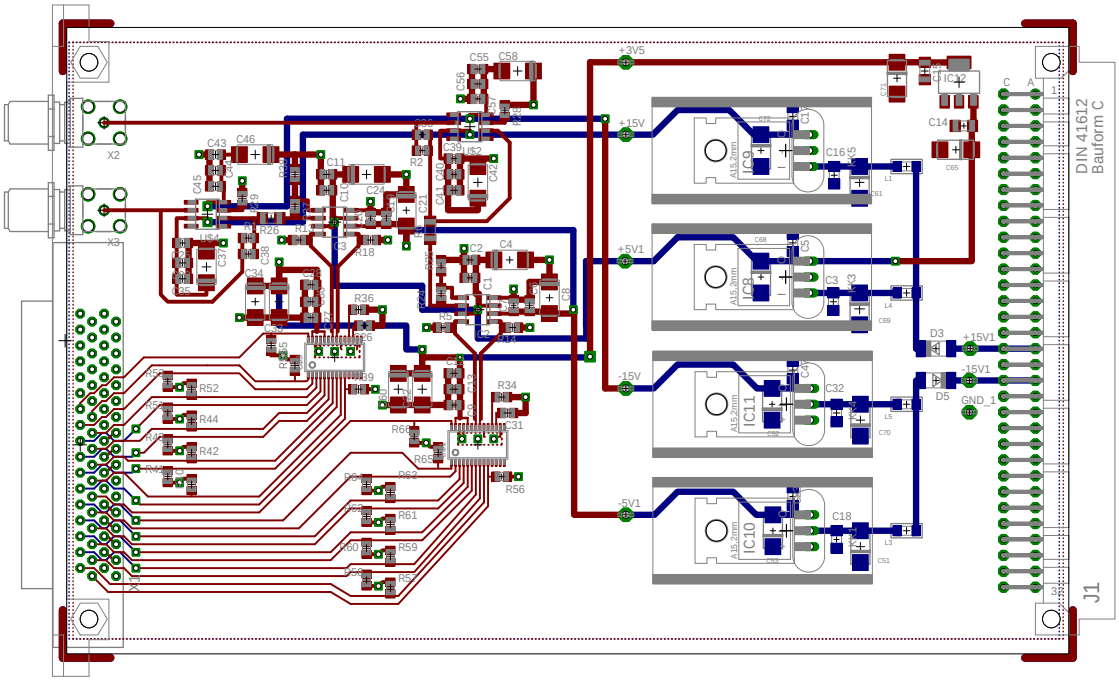


Figure 91: The top view of the board layout of the digital-to-analogue converters (DACs). Components and electric transmission lines on top are show in dark red, the ones on the bottom in blue. On the left side on the bottom one can see the very-high-density cable interconnect (VHDCI) input connector linked to the field programmable gate array (FPGA). The small red lines connected to it are the transmission lines for the two times 10 bit transmitted in parallel. On top of the VHDCI connector, the two SubMiniature version A (SMA) outputs of the analogue signal are shown.

Bibliography

[1] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, January 1983.

[2] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore*, page 175, 1984.

[3] RichardP. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6-7):467–488, 1982.

[4] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 400(1818):97–117, 1985.

[5] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 124–134, Nov 1994.

[6] Thomas Monz, Philipp Schindler, Julio T. Barreiro, Michael Chwalla, Daniel Nigg, William A. Coish, Maximilian Harlander, Wolfgang Hänsel, Markus Hennrich, and Rainer Blatt. 14-qubit entanglement: Creation and coherence. *Phys. Rev. Lett.*, 106:130506, Mar 2011.

[7] Tim Schröder. *Integrated photonic systems for single photon generation and quantum applications - assembly of fluorescent diamond nanocrystals by novel nano-manipulation techniques*. PhD thesis, 2013.

[8] Christof Paar and Jan Pelzl. *Understanding Cryptography - A Textbook for Students and Practitioners*. Springer-Verlag Berlin Heidelberg, 2010.

[9] C.E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal, The*, 28(4):656–715, Oct 1949.

[10] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978.

[11] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, October 1997.

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

[13] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74(1):145–195, Mar 2002.

[14] G. Brassard and L. Salvail. Secret key reconciliation by public discussion. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 410–423. Springer, 1994.

[15] Christian Kollmitzer and Mario Pivk. *Applied Quantum Cryptography*. Springer Berlin Heidelberg, 2010.

[16] Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121–3124, May 1992.

[17] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden. Pulsed energy-time entangled twin-photon source for quantum communication. *Phys. Rev. Lett.*, 82:2594–2597, Mar 1999.

[18] Damien Stucki, Nicolas Brunner, Nicolas Gisin, Valerio Scarani, and Hugo Zbinden. Fast and simple one-way quantum key distribution. *Applied Physics Letters*, 87(19):–, 2005.

[19] H Takesue, E Diamanti, T Honjo, C Langrock, M M Fejer, K Inoue, and Y Yamamoto. Differential phase shift quantum key distribution experiment over 105 km fibre. *New Journal of Physics*, 7(1):232, 2005.

[20] U.L. Andersen, G. Leuchs, and C. Silberhorn. Continuous-variable quantum information processing. *Laser & Photonics Reviews*, 4(3):337–354, 2010.

[21] Frederic Grosshans, Gilles Van Assche, Jerome Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421(6920):238–241, January 2003.

[22] Mark Hillery. Quantum cryptography with squeezed states. *Phys. Rev. A*, 61:022309, Jan 2000.

[23] Lars S. Madsen, Vladyslav C. Usenko, Mikael Lassen, Radim Filip, and Ulrik L. Andersen. Continuous variable quantum key distribution with modulated entangled states. *Nat Commun*, 3:1083–, September 2012.

[24] Rodney Loudon. *The Quantum Theory of Light*. Oxford University Press, third edition edition, 2006.

[25] S. Lorenz, N. Korolkova, and G. Leuchs. Continuous-variable quantum key distribution using polarization encoding and post selection. *Applied Physics B*, 79(3):273–277, 2004.

[26] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam. Quantum cryptography without switching. *Phys. Rev. Lett.*, 93:170504, Oct 2004.

[27] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs. Continuous variable quantum cryptography: Beating the 3 db loss limit. *Phys. Rev. Lett.*, 89:167901, Sep 2002.

[28] Malcolm N. O'Sullivan-Hale, Irfan Ali Khan, Robert W. Boyd, and John C. Howell. Pixel entanglement: Experimental realization of optically entangled $d = 3$ and $d = 6$ qudits. *Phys. Rev. Lett.*, 94:220501, Jun 2005.

[29] S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. Souto Ribeiro. Quantum key distribution with higher-order alphabets using spatially encoded qudits. *Phys. Rev. Lett.*, 96:090501, Mar 2006.

[30] Lijian Zhang, Christine Silberhorn, and Ian A. Walmsley. Secure quantum key distribution using continuous variables of single photons. *Phys. Rev. Lett.*, 100:110504, Mar 2008.

[31] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[32] Thomas Jennewein, Christoph Simon, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger. Quantum cryptography with entangled photons. *Phys. Rev. Lett.*, 84:4729–4732, May 2000.

[33] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat. Entangled state quantum cryptography: Eavesdropping on the ekert protocol. *Phys. Rev. Lett.*, 84:4733–4736, May 2000.

[34] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Quantum cryptography using entangled photons in energy-time bell states. *Phys. Rev. Lett.*, 84:4737–4740, May 2000.

[35] Christopher A. Fuchs, Nicolas Gisin, Robert B. Griffiths, Chi-Sheng Niu, and Asher Peres. Optimal eavesdropping in quantum cryptography. i. information bound and optimal strategy. *Phys. Rev. A*, 56:1163–1172, Aug 1997.

[36] Eli Biham and Tal Mor. Security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 78:2256–2259, Mar 1997.

[37] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.

[38] H. Inamori, N. Lütkenhaus, and D. Mayers. Unconditional security of practical quantum key distribution. *The European Physical Journal D*, 41(3):599–627, 2007.

[39] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.

[40] J.Lawrence Carter and Mark N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143 – 154, 1979.

[41] Tobias Moroder, Marcos Curty, Charles Ci Wen Lim, Le Phuc Thinh, Hugo Zbinden, and Nicolas Gisin. Security of distributed-phase-reference quantum key distribution. *Phys. Rev. Lett.*, 109:260501, Dec 2012.

[42] Raúl García-Patrón and Nicolas J. Cerf. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.*, 97:190503, Nov 2006.

[43] Miguel Navascués, Frédéric Grosshans, and Antonio Acín. Optimality of gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.*, 97:190502, Nov 2006.

[44] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat Photon*, 4(10):686–689, October 2010.

[45] Feihu Xu, Bing Qi, and Hoi-Kwong Lo. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New Journal of Physics*, 12(11):113026, 2010.

[46] Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew, and Hugo Zbinden. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat Photon*, 9(3):163–168, March 2015.

[47] D. Giggenbach, J. Poliak, R. Mata-Calvo, C. Fuchs, N. Perlot, R. Freund, and T. Richter. Preliminary results of Terabit-per-second long-range free-space optical transmission Experiment THRUST , 2015.

[48] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields. Efficient decoy-state quantum key distribution with quantified security. *Opt. Express*, 21(21):24550–24565, Oct 2013.

[49] Yang Liu, Teng-Yun Chen, Jian Wang, Wen-Qi Cai, Xu Wan, Luo-Kan Chen, Jin-Hong Wang, Shu-Bin Liu, Hao Liang, Lin Yang, Cheng-Zhi Peng, Kai Chen, Zeng-Bing Chen, and Jian-Wei Pan. Decoy-state quantum key distribution with polarized photons over 200 km. *Opt. Express*, 18(8):8587–8594, Apr 2010.

[50] Paul Jouguet, Sebastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat Photon*, 7(5):378–381, May 2013.

[51] P Eraerds, N Walenta, M Legré, N Gisin, and H Zbinden. Quantum key distribution and 1 gbps data encryption over a single fibre. *New Journal of Physics*, 12(6):063027, 2010.

[52] Iris Choi, Robert J. Young, and Paul D. Townsend. Quantum key distribution on a 10gb/s wdm-pon. *Opt. Express*, 18(9):9600–9612, Apr 2010.

[53] www.idquantique.com.

[54] www.magiqtech.com.

[55] www.sequrenet.com.

[56] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932–5935, Dec 1998.

[57] Matthaus Halder, Alexios Beveratos, Nicolas Gisin, Valerio Scarani, Christoph Simon, and Hugo Zbinden. Entangling independent photons by time measurement. *Nat Phys*, 3(10):692–695, October 2007.

[58] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons. Practical free-space quantum key distribution over 1 km. *Phys. Rev. Lett.*, 81:3283–3286, Oct 1998.

[59] J G Rarity, P R Tapster, P M Gorman, and P Knight. Ground to satellite secure key exchange using quantum cryptography. *New Journal of Physics*, 4(1):82, 2002.

[60] Giuseppe Vallone, Davide Bacco, Daniele Dequal, Simone Gaiarin, Vincenza Luceri, Giuseppe Bianco, and Paolo Villoresi. Experimental satellite quantum communications. *Phys. Rev. Lett.*, 115:040502, Jul 2015.

[61] Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G. Rarity, Anton Zeilinger, and Harald Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.*, 98:010504, Jan 2007.

[62] Sebastian Nauerth, Florian Moll, Markus Rau, Christian Fuchs, Joachim Horwath, Stefan Frick, and Harald Weinfurter. Air-to-ground quantum communication. *Nat Photon*, 7(5):382–386, May 2013.

[63] Heinrich Hertz. Ueber einen Einfluss des ultravioletten Lichtes auf die electrische Entladung. *Annalen der Physik*, 267(8):983–1000, 1887.

[64] Albert Einstein. ber einen die erzeugung und verwandlung des lichtes betreffenden heuristischen gesichtspunkt. *Annalen der Physik*, 322(6):132148, 1905.

[65] Max Planck. Ueber das gesetz der energieverteilung im normalspectrum. *Annalen der Physik*, 309(3):553–563, 1901.

[66] Marlan O. Scully and M. Suhail Zubairy. *Quantum Optics*. 1997.

[67] Tobias J. A. Kippenberg. *Nonlinear Optics in Ultra-high-Q Whispering-Gallery Optical Microcavities*. PhD thesis, California Institute of Technology, Pasadena, California, 2004.

[68] X. T. Zou and L. Mandel. Photon-antibunching and sub-poissonian photon statistics. *Phys. Rev. A*, 41:475–476, Jan 1990.

[69] Gesine A. Steudle, Stefan Schietinger, David Höckel, Sander N. Dorenbos, Iman E. Zadeh, Valery Zwiller, and Oliver Benson. Measuring the quantum

nature of light with a single source and a single detector. *Phys. Rev. A*, 86:053814, Nov 2012.

[70] R. Hanbury Brown and R. Q. Twiss. Correlation between photons in two coherent beams of light. *Nature*, 177(4497):27–29, January 1956.

[71] Mario Martinelli. Time reversal for the polarization state in optical systems. *Journal of Modern Optics*, 39(3):451–455, 1992.

[72] P. Michler, A. Kiraz, C. Becher, W. V. Schoenfeld, P. M. Petroff, Lidong Zhang, E. Hu, and A. Imamoglu. A quantum dot single-photon turnstile device. *Science*, 290(5500):2282–2285, 2000.

[73] M. Orrit and J. Bernard. Single pentacene molecules detected by fluorescence excitation in a p -terphenyl crystal. *Phys. Rev. Lett.*, 65:2716–2719, Nov 1990.

[74] Frank Diedrich and Herbert Walther. Nonclassical radiation of a single stored ion. *Phys. Rev. Lett.*, 58:203–206, Jan 1987.

[75] Christian Kurtsiefer, Sonja Mayer, Patrick Zarda, and Harald Weinfurter. Stable solid-state source of single photons. *Phys. Rev. Lett.*, 85:290–293, Jul 2000.

[76] Sebastian Zaske, Andreas Lenhard, Christian A. Keßler, Jan Kettler, Christian Hepp, Carsten Arend, Roland Albrecht, Wolfgang-Michael Schulz, Michael Jetter, Peter Michler, and Christoph Becher. Visible-to-telecom quantum frequency conversion of light from a single quantum emitter. *Phys. Rev. Lett.*, 109:147404, Oct 2012.

[77] Ping Jiang, Tim Schroeder, Michael Bath, Vladimir Lesnyak, Nikolai Gaponik, Alexander Eychmüller, and Oliver Benson. Incoherent photon conversion in selectively infiltrated hollow-core photonic crystal fibers for single photon generation in the near infrared. *Opt. Express*, 20(10):11536–11547, May 2012.

[78] C. K. Hong and L. Mandel. Experimental realization of a localized one-photon state. *Phys. Rev. Lett.*, 56:58–60, Jan 1986.

[79] K. G. Lee, X. W. Chen, H. Eghlidi, P. Kukura, R. Lettow, A. Renn, V. Sandoghdar, and S. Gtzinger. A planar dielectric antenna for directional single-photon emission and near-unity collection efficiency. *Nat Photon*, 5(3):166–169, March 2011.

[80] Roland Albrecht, Alexander Bommer, Christian Deutsch, Jakob Reichel, and Christoph Becher. Coupling of a single nitrogen-vacancy center in diamond to a fiber-based microcavity. *Phys. Rev. Lett.*, 110:243602, Jun 2013.

[81] Thomas M. Babinec, HausmannBirgit J. M., Mughees Khan, Yinan Zhang, Jeronimo R. Maze, Philip R. Hemmer, and Marko Loncar. A diamond nanowire single-photon source. *Nat Nano*, 5(3):195–199, March 2010.

[82] Alberto G. Curto, Giorgio Volpe, Tim H. Taminiau, Mark P. Kreuzer, Romain Quidant, and Niek F. van Hulst. Unidirectional emission of a quantum dot coupled to a nanoantenna. *Science*, 329(5994):930–933, 2010.

[83] Stefan Schietinger, Michael Barth, Thomas Aichele, and Oliver Benson. Plasmon-enhanced single photon emission from a nanoassembled metal-diamond hybrid structure at room temperature. *Nano Letters*, 9(4):1694–1698, 2009. PMID: 19301860.

[84] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005.

[85] Paul M. Amirtharaj, Rasheed M. A. Azzam, Leo Beiser, Jean M. Bennett, Ellis Betensky, Glenn D. Boreman, Robert P. Breault, Tom G. Brown, I. C. Chang, Russell A. Chipman, Katherine Creath, Mark Cronin-Golomb, Michael W. Farn, Norman Goldberg, P. Hariharin, Terry J. Harris, James E. Harvey, Brian Henderson, Lloyd Huff, Shinya Inoue, R. Barry Johnson, Lloyd Jones, Marvin Klein, Thomas L. Koch, M. Kreitzer, F. J. Leonberger, John D. Lytle, Daniel Malacara, Zacarias Malacara, Theresa A. Maldonado, Tom D. Milster, Duncan T. Moore, J. Moskovich, Rudolf Oldenbourg, James M. Palmer, Roger A. Paquin, Stephen M. Pompea, David G. Seiler, John C Stover, P. G. Suchoski, Chung L. Tang, Michael E. Thomas, William J. Tropf, Wilfrid B. Veldkamp, William B. Wetherell, William L. Wolfe, Shin-Tson Wu, James C. Wyant, Edward F. Zalewski, and George J. Zissis. *Handbook of Optics*, volume Volume II: Devices , Measurements , and Properties. McGraw-Hill, 1995.

[86] Christian-Alexander Bunge. "high-speed optical transmission systems". Lecture at Hochschule für Telekommunikation Leipzig, 2012.

[87] Isaac I. Kim, Ron Stieger, Joseph A. Koontz, Carter Moursund, Micah Barclay, Prasanna Adhikari, John Schuster, Eric Korevaar, Richard Ruigrok, and Casimer DeCusatis. Wireless optical transmission of fast ethernet, fddi, atm, and escon protocol data using the terralink laser communication system. *Optical Engineering*, 37(12):3143–3155, 1998.

[88] Alex D. Semenov, Gregory N. Golt́sman, and Alexander A. Korneev. Quantum detection by current carrying superconducting film. *Physica C: Superconductivity*, 351(4):349 – 356, 2001.

[89] G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and Roman Sobolewski. Picosecond superconducting single-photon optical detector. *Applied Physics Letters*, 79(6):705–707, 2001.

[90] Chandra M Natarajan, Michael G Tanner, and Robert H Hadfield. Superconducting nanowire single-photon detectors: physics and applications. *Superconductor Science and Technology*, 25(6):063001, 2012.

[91] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam. Detecting single infrared photons with 93% system efficiency. *Nat Photon*, 7(3):210–214, March 2013.

[92] Robert H. Hadfield. Single-photon detectors for optical quantum information applications. *Nat Photon*, 3(12):696–705, December 2009.

[93] A. Fukasawa, J. Haba, A. Kageyama, H. Nakazawa, and M. Suyama. High speed hpd for photon counting. *Nuclear Science, IEEE Transactions on*, 55(2):758–762, April 2008.

[94] Hamamatsu. Photomultiplier tubes - Basics and applications. Technical report, Hamatsu Photonics, 2007.

[95] Hamamatsu. Microchannel plate photomultiplier tube (MCP-PMT) R3809U-61/-63/-64. Technical report, Hamamatsu Photonics, 2015.

[96] L. C. Comandar, B. Fröhlich, J. F. Dynes, A. W. Sharpe, M. Lucamarini, Z. L. Yuan, R. V. Penty, and A. J. Shields. Gigahertz-gated ingaas/inp single-photon detector with detection efficiency exceeding 55% at 1550 nm. *Journal of Applied Physics*, 117(8):–, 2015.

[97] Alexander Korneev, Alexander Divochiy, Yury Vachtomin, Yulia Korneeva, Irina Florya, Michael Elezov, Nadezhda Manova, Michael Tarkhov, Pavel An, Anna Kardakova, Anastasiya Isupova, Galina Chulkova, Konstantin Smirnov, Natalya Kaurova, Vitaliy Seleznev, Boris Voronov, and Gregory Goltsman. Recent advances in superconducting nbn single-photon detector development, 2011.

[98] B. E. Kardynał, Z. L.. Yuan, and Shields A. J. An avalanche-photodiode-based photon-number-resolving detector. *Nat Photon*, 2(7):425–428, July 2008.

[99] Aleksander Divochiy, Francesco Marsili, David Bitauld, Alessandro Gaggero, Roberto Leoni, Francesco Mattioli, Alexander Korneev, Vitaliy Seleznev, Nataliya Kaurova, Olga Minaeva, Gregory Gol'tsman, Konstantinos G. Lagoudakis, Moushab Benkhaoul, Francis Levy, and Andrea Fiore. Superconducting nanowire photon-number-resolving detector at telecommunication wavelengths. *Nat Photon*, 2(5):302–306, May 2008.

[100] www.scontel.ru.

[101] www.photonspot.com.

[102] www.singlequantum.com.

[103] www.excelitas.com.

[104] www.hamamatsu.com.

[105] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[106] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996.

[107] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85:1330–1333, Aug 2000.

[108] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91:057901, Aug 2003.

[109] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. *Quantum Information & Computation*, 4(5):325–360, 2004.

[110] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72:012326, Jul 2005.

[111] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, January 2001.

[112] Nicolas Sangouard, Christoph Simon, Jiří Minář, Hugo Zbinden, Hugues de Riedmatten, and Nicolas Gisin. Long-distance entanglement distribution with single-photon sources. *Phys. Rev. A*, 76:050301, Nov 2007.

[113] Elke Neu, David Steinmetz, Janine Riedrich-Möller, Stefan Gsell, Martin Fischer, Matthias Schreck, and Christoph Becher. Single photon emission from silicon-vacancy colour centres in chemical vapour deposition nano-diamonds on iridium. *New Journal of Physics*, 13(2):025012, 2011.

[114] Igor Aharonovich, Stefania Castelletto, David A. Simpson, Alastair Stacey, Jeff McCallum, Andrew D. Greentree, and Steven Prawer. Two-level ultrabright single photon emission from diamond nanocrystals. *Nano Letters*, 9(9):3191–3195, 2009. PMID: 19670845.

[115] Alastair Stacey, Igor Aharonovich, Steven Prawer, and James E. Butler. Controlled synthesis of high quality micro/nano-diamonds by microwave plasma chemical vapor deposition. *Diamond and Related Materials*, 18(1):51 – 55, 2009.

[116] G. Waldherr, J. Beck, M. Steiner, P. Neumann, A. Gali, Th. Frauenheim, F. Jelezko, and J. Wrachtrup. Dark states of single nitrogen-vacancy centers in diamond unraveled by single shot nmr. *Phys. Rev. Lett.*, 106:157601, Apr 2011.

[117] Tim Schröder, Friedemann Gädeke, Moritz Julian Banholzer, and Oliver Benson. Ultrabright and efficient single-photon generation based on nitrogen-vacancy centres in nanodiamonds on a solid immersion lens. *New Journal of Physics*, 13(5):055017, 2011.

[118] Thiago P. Mayer Alegre, Charles Santori, Gilberto Medeiros-Ribeiro, and Raymond G. Beausoleil. Polarization-selective excitation of nitrogen vacancy centers in diamond. *Phys. Rev. B*, 76:165205, Oct 2007.

[119] Elke Neu, Mario Agio, and Christoph Becher. Photophysics of single silicon vacancy centers in diamond: implications for single photon emission. *Opt. Express*, 20(18):19956–19971, Aug 2012.

[120] Mark N. Wegman and J.Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265 – 279, 1981.

[121] Edo Waks, Charles Santori, and Yoshihisa Yamamoto. Security aspects of quantum key distribution with sub-poisson light. *Phys. Rev. A*, 66:042315, Oct 2002.

[122] Dirk Giggenbach. Optimierung der optischen Freiraumkommunikation durch die turbulente Atmosphäre - Focal Array Receiver. Dissertation, DLR Oberpfaffenhofen, Institut für Kommunikation und Navigation, Digitale Netze, 2005.

[123] Andreas W. Schell, Johannes Kaschke, Joachim Fischer, Rico Henze, Janik Wolters, Martin Wegener, and Oliver Benson. Three-dimensional quantum photonic elements based on single nitrogen vacancy-centres in laser-written microstructures. *Sci. Rep.*, 3:–, April 2013.

[124] Jian-Yu Wang, Bin Yang, Sheng-Kai Liao, Liang Zhang, Qi Shen, Xiao-Fang Hu, Jin-Cai Wu, Shi-Ji Yang, Hao Jiang, Yan-Lin Tang, Bo Zhong, Hao Liang, Wei-Yue Liu, Yi-Hua Hu, Yong-Mei Huang, Bo Qi, Ji-Gang Ren, Ge-Sheng Pan, Juan Yin, Jian-Jun Jia, Yu-Ao Chen, Kai Chen, Cheng-Zhi Peng, and Jian-Wei Pan. Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nat Photon*, 7(5):387–393, May 2013.

[125] Jose Romba, Zoran Sodnik, Marcos Reyes, Angel Alonso, and Aneurin Bird. Esa's bidirectional space-to-ground laser communication experiments. *Proc. SPIE*, 5550:287–298, 2004.

[126] G. Muehlnikel, H. Kämpfner, F. Heine, H. Zech, D. Troendle, and R. S. Philipp-May Meyer. The alphasat geo laser communication terminal flight acceptance tests. *Proc. International Conference on Space Optical Systems and Applications (ICSOS)*, 2012.

[127] S.F. Yelin and Bing C. Wang. Time-frequency bases for bb84 protocol. *arXiv:0309105 [quant-ph]*, 2003.

[128] Bing Qi. Single-photon continuous-variable quantum key distribution based on the energy-time uncertainty relation. *Opt. Lett.*, 31(18):2795–2797, Sep 2006.

[129] Zhu Chang-Hua, Pei Chang-Xing, Quan Dong-Xiao, Gao Jing-Liang, Chen Nan, and Yi Yun-Hui. A new quantum key distribution scheme based on frequency and time coding. *Chinese Physics Letters*, 27(9):090301, 2010.

[130] L. Olislager, J. Cussey, A. T. Nguyen, P. Emplit, S. Massar, J.-M. Merolla, and K. Phan Huy. Frequency-bin entangled photons. *Phys. Rev. A*, 82:013804, Jul 2010.

[131] H. Bechmann-Pasquinucci. Eavesdropping without quantum memory. *Phys. Rev. A*, 73:044305, Apr 2006.

[132] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *Information Theory, IEEE Transactions on*, 24(3):339–348, May 1978.

[133] SHF. Datasheet SHF 12103 A. Technical report, SHF Communication Technologies AG, 2012.

[134] David Höckel. *Narrow-Band Single Photons as Carriers of Quantum Information*. PhD thesis, 2010.

[135] J. Nunn, L. J. Wright, C. Söller, L. Zhang, I. A. Walmsley, and B. J. Smith. Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion. *Opt. Express*, 21(13):15959–15973, Jul 2013.

[136] Optical Delay Lines. Technical report, OZ Optics, 120.

[137] Alexander Paritsky and Alexander Kots. Fiber optic microphone as a realization of fiber optic positioning sensors. In *Proc. of International Society for Optical Engineering (SPIE)*, volume 3110, pages 408–414, 1997.

[138] William B. Spillman Jr. Eric Udd, editor. *Fiber Optic Sensors: An Introduction for Engineers and Scientists - Second Edition*. Wiley, Hoboken, NJ, 2011.

[139] J.M.Vogt. Transmission of Timing-critical Signals Using TTL Levels. Technical report, Canadian Light Source, 2000.

[140] P. Horowitz and W. Hill. *The Art of Electronics*. Cambridge University Press, New York, NY, USA, 1989.

[141] Ryan J. Pirkl. ECL Design Guide. Technical report, The Propagation Group-Georga Institute of Technology, 2005.

[142] Micrel. SY100EP195V. Technical report, Micrel, 2005.

[143] www.chemandy.com/calculators/microstrip_transmission_line_calculator_hartley27.htm.

[144] Paul Shockman. AND8020/D, Termination of ECL Devices with EF (Emitter Follower) OUTPUT Structure. Technical report, ON Semiconductor, 2007.

[145] http://qrng.physik.hu-berlin.de/.

[146] http://www.picoquant.com/products/category/quantum-random-number-generator/pqrng-150-quantum-random-number-generator.

[147] André Stefanov, Nicolas Gisin, Olivier Guinnard, Laurent Guinnard, and Hugo Zbinden. Optical quantum random number generator. *Journal of Modern Optics*, 47(4):595–598, 2000.

[148] Martin Fürst, Henning Weier, Sebastian Nauerth, Davide G. Marangon, Christian Kurtsiefer, and Harald Weinfurter. High speed optical quantum random number generation. *Opt. Express*, 18(12):13029–13037, Jun 2010.

[149] Michael A. Wayne, Evan R. Jeffrey, Gleb M. Akselrod, and Paul G. Kwiat. Photon arrival time quantum random number generation. *Journal of Modern Optics*, 56(4):516–522, 2009.

[150] Michael A. Wayne and Paul G. Kwiat. Low-bias high-speed quantum random number generator via shaped optical pulses. *Opt. Express*, 18(9):9351–9357, Apr 2010.

[151] Michael Wahl, Hans-Jürgen Rahn, Tino Röhlicke, Gerald Kell, Daniel Nettels, Frank Hillger, Ben Schuler, and Rainer Erdmann. Scalable time-correlated photon counting system with multiple independent input channels. *Review of Scientific Instruments*, 79(12):–, 2008.

[152] Glenn F. Knoll. *Radiation Detection and Measurement, Fourth Edition.* Wiley, Hoboken, NJ, 2010.

[153] Sebastiaan Indesteege, Florian Mendel, Bart Preneel, and Christian Rechberger. Collisions and Other Non-random Properties for Step-Reduced SHA-256. In Roberto Avanzi, Liam Keliher, and Francesco Sica, editors, *Selected Areas in Cryptography*, volume 5381 of *Lecture Notes in Computer Science*, pages 276–293. Springer Berlin / Heidelberg, 2009.

[154] Somitra Sanadhya and Palash Sarkar. Non-linear Reduced Round Attacks against SHA-2 Hash Family. In Yi Mu, Willy Susilo, and Jennifer Seberry, editors, *Information Security and Privacy*, volume 5107 of *Lecture Notes in Computer Science*, pages 254–266. Springer Berlin / Heidelberg, 2008.

[155] Patrick Lacharme. Post-processing functions for a biased physical random number generator. In *FSE*, pages 334–342, 2008.

[156] Patrick Lacharme. Analysis and construction of correctors. *IEEE Trans. Inf. Theor.*, 55:4742–4748, October 2009.

[157] David B. Thomas and Wayne Luk. Sampling from the exponential distribution using independent Bernoulli variates. In *In Proceedings of FPL*, 2008.

[158] Berk Sunar, William J. Martin, and Douglas R. Stinson. A provably secure true random number generator with built-in tolerance to active attacks. *IEEE Trans. Computers*, 56(1):109–119, 2007.

[159] R. C. Bose and D. K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Information and Control*, 3 (1):6879, 1960.

[160] Peter Mathys. Lecture Course ECEN 5682: Theory and Practice of Error Control Codes - Cyclic Codes. http://ecee.colorado.edu/ mathys/ecen5682/notes.html, 2007.

[161] Jonathan I. Hall. Notes on Coding Theory. http://users.math.msu.edu/users/jhall/classes/codenotes/coding-notes.html, September 2010.

[162] Dries Schellekens, Bart Preneel, and Ingrid Verbauwhede. FPGA vendor agnostic true random number generator. CiteSeer http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.86.5319, 2006.

[163] Testu01. www.iro.umontreal.ca/ simardr/testu01/tu01.html.

[164] J. Ziv and A. Lempel. Compression of individual sequences via variable-rate coding. *Information Theory, IEEE Transactions on*, 24(5):530–536, Sep 1978.

[165] Pierre L'Ecuyer and Richard Simard. TestU01: A C Library for Empirical Testing of Random Number Generators. *ACM Trans. Math. Softw.*, 33(4), August 2007.

[166] Andreas W. Schell, Philip Engel, Julia F. M. Werra, Christian Wolff, Kurt Busch, and Oliver Benson. Scanning single quantum emitter fluorescence lifetime imaging: Quantitative analysis of the local density of photonic states. *Nano Letters*, 14(5):2623–2627, 2014. PMID: 24694035.

[167] Martin Frimmer, Abbas Mohtashami, and A. Femius Koenderink. Nanomechanical method to gauge emission quantum yield applied to nitrogen-vacancy centers in nanodiamond. *Applied Physics Letters*, 102(12), 2013.

[168] Janik Wolters, Andreas W. Schell, Günter Kewes, Nils Nüsse, Max Schoengen, Henning Döscher, Thomas Hannappel, Bernd Löchel, Michael Barth, and Oliver Benson. Enhancement of the zero phonon line emission from a single nitrogen vacancy center in a nanodiamond via coupling to a photonic crystal cavity. *Applied Physics Letters*, 97(14), 2010.

[169] Janine Riedrich-Möller, Laura Kipfstuhl, Christian Hepp, Elke Neu, Christoph Pauly, Frank Mücklich, Armin Baur, Michael Wandt, Sandra Wolff, Martin Fischer, Stefan Gsell, Matthias Schreck, and Christoph Becher. One- and two-dimensional photonic crystal microcavities in single crystal diamond. *Nat Nano*, 7(1):69–74, January 2012.

[170] Janine Riedrich-Möller, Carsten Arend, Christoph Pauly, Frank Mücklich, Martin Fischer, Stefan Gsell, Matthias Schreck, and Christoph Becher. Deterministic coupling of a single silicon-vacancy color center to a photonic crystal cavity in diamond. *Nano Letters*, 14(9):5281–5287, 2014. PMID: 25111134.

List of own contributions

List of own publications

[171] Matthias Leifgen, Tim Schröder, Friedemann Gädeke, Robert Riemann, Valentin Métillon, Elke Neu, Christian Hepp, Carsten Arend, Christoph Becher, Kristian Lauritsen, and Oliver Benson. Evaluation of nitrogen- and silicon-vacancy defect centres as single photon sources in quantum key distribution. *New Journal of Physics*, 16(2):023021, 2014.

[172] Michael Wahl, Matthias Leifgen, Michael Berlin, Tino Röhlicke, Hans-Jürgen Rahn, and Oliver Benson. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. *Applied Physics Letters*, 98(17):171105, 2011.

[173] Matthias Leifgen, Robert Elschner, Nicolas Perlot, Carl Weinert, Colja Schubert, and Oliver Benson. Practical implementation and evaluation of a quantum-key-distribution scheme based on the time-frequency uncertainty. *Phys. Rev. A*, 92:042311, Oct 2015.

[174] Michael Wahl, Matthias Leifgen, Michael Berlin, Tino Röhlicke, Hans-Jürgen Rahn, and Oliver Benson. Addendum: "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements" [Appl. Phys. Lett. 98, 171105 (2011)]. *Applied Physics Letters*, 101(15):–, 2012.

Supervised bachelor and master theses

[175] Robert Riemann. Implementierung einer Steuerung für ein Quantum Key Distribution (QKD) Experiment inklusive Postprocessing. Master's thesis, 2013.

[176] Björnstjerne Zindler. Aufbau von faserbasierten Interferometern für die Quantenkryptografie. Master's thesis, 2011.

[177] Georg Kewitsch. Entwicklung einer FPGA-basierten Steuereinheit für Quantenkryptographieexperimente. Master's thesis, 2013.

[178] Danilo Kühn. Design eines Triggersystems für ein Quantenkryptographie Experiment
Bachelor thesis, 2010.

[179] Georg Hasselberg. Bau eines Interferometers zur Vermessung optischer Weglängen
Bachelor thesis, 2008.

[180] Paul Pflugradt. Untersuchungen zur Implementierung von Faser-basierter Quantenkryptografie
Bachelor thesis, 2010.

List of conference contributions

[1] Matthias Leifgen, Tim Schröder, Robert Riemann, and Friedemann Gädeke. Demonstration of QKD with a compact and mobile single photon source based on defect centers in diamond
DPG-Frühjahrstagung Stuttgart 2012.

[2] Matthias Leifgen, Robert Elschner, Oliver J. Benson, and Colja Schubert. Conference Paper Quantum Information and Measurement (QIM) 2012: The Implementation of a Quantum Key Distribution Scheme based on the Frequency-Time Uncertainty. In *Research in Optical Sciences*, page QW2A.2. Optical Society of America, 2012.

[3] Jasper Rödiger, Nicolas Perlot, Matthias Leifgen, Robert Elschner, Roberto Mottola, Oliver Benson, and Ronald Freund. Conference Poster: Large-Alphabet Time-Frequency Quantum Key Distribution
QCrypt 2015, 5th International Conference on Quantum Cryptography, Tokyo, Japan, 2015.

Abbreviations

AC alternating current

ADC analog-to-digital converter

AES Advanced Encryption Standard

APD avalanche photodiode

ARM Advanced RISC Machine

BB84 first QKD protocol after Bennett and Brassard, 1984

BCH Bose-Chaudhuri-Hocquenghem

BNC Bayonet NeillConcelman

BPG bit pattern generator

BS beam splitter

CLB configurable logic block

CMOS complementary metal-oxide-semiconductor

COW coherent one-way

Cr chromium

CSS Calderbank-Shor-Steane

Cu copper

CVD chemical vapour deposition

CW continuous wave

DAC digital-to-analogue converter

DCA digital channel analyzer

DES Data Encryption Standard

DFB distributed feedback

DIP dual in-line package

DOMZM double output Mach-Zehnder modulator

DPSK differential phase shift keying

DWDM dense wavelength division multiplexing

DWF Debye-Waller factor

EAGLE Einfach Anzuwendender Grafischer Layout Editor

ECL emitter coupled logic

EDFA Erbium doped fiber amplifier

EOM electro-optic modulator

FBG fiber Bragg grating

FIFO First In, First Out

FMC FPGA Mezzanine Card

FPGA field programmable gate array

FSR free spectral range

FT frequency-time

FWHM full width at half-maximum

GaAsP gallium arsenide phosphide

GUI graphical user interface

HBT Hanbury Brown and Twiss

HHI Heinrich Hertz Institute

HU Berlin Humboldt-Universität zu Berlin

I/O input/output

IC integrated circuit

InGaAs indium gallium arsenide

InP indium phosphite

IP Internet Protocol

Ir Iridium

ISE Integrated Software Environment

JTAG Joint Test Action Group

KDP potassium dihydrogen phosphate

LED light emitting diode

LEO low earth orbit

$LiNbO_3$ lithium niobate

LOQC linear optical quantum computing

LUT lookup table

MZM Mach-Zehnder modulator

NA numerical aperture

NbN niobium nitride

NV nitrogen vacancy

op-amp operational amplifier

PBS polarising beam splitter

PC personal computer

PCB printed circuit board

PCI Peripheral Component Interconnect

PECL positive emitter-coupled logic

PID controller proportional-integral-derivative controller

PLL phase-locked loop

PMT photomultiplier tube

PNS photon number splitting

PRNG pseudo random number generator

QBER quantum bit error rate

QEC quantum error correction

QIP quantum information processing

QKD quantum key distribution

QRNG quantum random number generator

RAM random-access memory

RNG random number generator

RSA public key algorithm by Ron Rivest, Adi Shamir and Leonard Adleman

SEM scanning electron microscope

SHA secure hash algorithm

Si silicon

SIL solid immmersion lens

SiO_2 silicon dioxide

SiV silicon vacancy

SMA SubMiniature version A

SMD surface-mount device

SoC system on a chip

SPDC spontaneous parametric down-conversion

SPS single photon source

SSPD superconducting single photon detector

TDC time-to-digital converter

TLS Transport Layer Security

TRNG true random number generator

TTL transistor-transistor logic

TUB Technische Universität Berlin

USB Universal Serial Bus

VCO voltage-controlled oscillator

VHDCI very-high-density cable interconnect

VHDL Very High Speed Integrated Circuit Hardware Description Language

WCP weak coherent pulse

WDM wavelength-division multiplexing

WSi tungsten silicide

XOR exclusive or

ZPL zero phonon line

ZrO_2 zirconium dioxide

List of Figures

List of Tables

Danksagung

Zunächst einmal danke ich Herrn Professor Oliver Benson, der einen großen Anteil am Gelingen dieser Dissertation hat. Seine fachliche Betreuung und sein entgegengebrachtes Vertrauen waren sehr wichtig für mich. Mit großem persönlichen Einsatz schafft er stets aufs Neue ideale Rahmenbedingungen zum Forschen.

Dazu gehört unter anderem die Schaffung einer sehr angenehmen Arbeitsatmosphäre mit verantwortungsbewußten, hilfsbereiten und netten Kollegen. Es ist ein großer Vorteil, wenn man sich alleine schon deswegen auf die Arbeit freut, weil man dort seine Kollegen trifft. Hierzu zähle ich im erweiterten Sinn auch die QOMs. Einigen dieser (Ex-) Kollegen möchte ich an dieser Stelle besonders danken, weil sie Teile dieser Arbeit Korrektur gelesen haben und mir sehr hilfreiche Ratschläge gegeben haben. Danke an Tim Kroh, Ben, Günter, Tim Schröder, Jasper und Katharina Möhle.

Ich bedanke mich natürlich auch bei meinen Master- und Bachelorstudenten für ihren sehr guten Beitrag zu dieser Arbeit.

Zu danken habe ich auch Hans Scholz von der Elektronikwerkstatt, einem ausgewiesenen Elektronikfachmann, sowie Dipl.-Ing. Klaus Palis. Beide waren mir beim Bau der elektronischen Schaltungen mit vielen Tipps behilflich. Klaus stand mir auch bei anderen Projekten stets mit Rat und Tat zur Seite.

Ich möchte mich auch bei Dr. Ing. Robert Elschner vom HHI bedanken. Sein akribischer Ansatz und seine ständige Reflektion bei der wissenschaftlichen Arbeit waren vorbildlich und wichtig für meine wissenschaftliche Entwicklung.

Ein Dank geht auch an alle meine Freunde. Es ist großartig, so tolle Menschen zu kennen, die an mich glauben und für mich da sind und das Leben aufregend machen. Besonders möchte ich Laura danken, für ihre Hilfe und Geduld.

Zum Abschluss danke ich meinen Eltern, dass sie mehr als alle anderen Menschen für mich da sind und mich unterstützen. Auch meiner Schwester und ihrer Familie danke ich sehr.

Selbstständigkeitserklärung

Ich erkläre, dass ich die Dissertation selbständig und nur unter Verwendung der von mir gemäß 7 Abs. 3 der Promotionsordnung der Mathematisch-Naturwissenschaftlichen Fakultät, veröffentlicht im Amtlichen Mitteilungsblatt der Humboldt-Universität zu Berlin Nr. 126/2014 am 18.11.2014 angegebenen Hilfsmittel angefertigt habe.

Berlin, den Matthias Leifgen