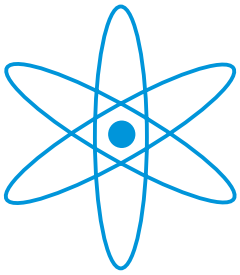
PHYSIK-DEPARTMENT



Experimental Quantum Cryptography

Diplomarbeit von
Henning Weier

angefertigt unter der Anleitung von
Prof. Dr. Harald Weinfurter und
Prof. Dr. Alfred Laubereau

TECHNISCHE UNIVERSITÄT
MÜNCHEN

Contents

1 Introduction

Whenever information is conveyed or processed, physical systems are involved. If information processing devices continue to get scaled down in size as they have been in the past, they will soon reach dimensions at which classical physics ceases to describe the systems correctly and quantum mechanics comes into play. Since classical systems are usually regarded as simpler, the fact that quantum effects cannot be neglected anymore seems to be disturbing at first glance. Yet, during the last few decades it was discovered that the combination of classical information theory and quantum physics offers amazing possibilities.

The most prominent member of the new field of quantum information is quantum computation, employing fundamental concepts of quantum physics as an advantage over classical computers. Some tasks have already been identified that can be implemented much more efficiently on a quantum computer, such as the famous problem of finding the prime factors of a large integer. But not only could a quantum computer help calculating classical problems, it furthermore allows for tests of predictions on multi-particle quantum systems, because what could be better suited for simulating quantum systems than a controllable quantum system. While some theoretical proposals have been made some time ago, experiments with quantum computers are still in a rather early stage, although there is a lot of progress. Different implementations fight against their specific limitations like restrictions on the numbers of qubits or decoherence effects. Despite all the problems it is almost certain that the mere effort to solve them will advance physics in general.

As well as focusing on possible applications, many quantum information experiments are testing foundations of quantum mechanics: For instance, experiments involving entangled states like quantum teleportation or quantum cloning are regularly obtaining values beyond classical limits, supporting the theory that physical systems cannot be described by models incorporating local realism. Still, so-called "loopholes" are claimed to remain in the realised experiments, leaving enough space for local hidden variable models to step in.

The perhaps most developed method of quantum information processing today is quantum cryptography or quantum key distribution (QKD). Since in the usual schemes only keys are distributed using a quantum channel, the latter term is more precise, but for historical reasons the two names are used synonymously. Although the first proposal was published less than 20 years ago, already two companies have been founded (to my knowledge), one in the United States and one in Switzerland, willing and able to sell quantum cryptography

systems. While these systems are not (yet?) regarded as a necessity for every household, the demand could arise, paving the way for other quantum information devices to soon find a place in high security communication between institutions like banks, insurance companies or public authorities.

The need for secure communication has generally increased tremendously during the last decade, since more and more sensitive information is transported and more and more people are concerned. Applications like home-banking make everyday life more comfortable, but they also bear additional risks. When the development continues as it has done lately, the demand for information security will rise and could well lead to a situation urging some institutions to think about a level of security that can only be reached with the help of quantum mechanics. Commercial investors as well as military organisations show increasing interest in quantum key distribution systems since they have evolved from laboratory experiments on big tables towards compact, handy devices. Whereas optical fibre based systems are already commercially available, free space implementations are a small step behind, but a first prototype for real-world application is not too far away.

The present work has brought this next step a little closer by contributing to the development of a continuously working free space quantum cryptography system for secure urban communication. Starting from the experience that was gained in this group during the successful free space key exchange over 23 km, the next tasks were identified: Telescopes had to be designed to meet the requirements of urban optical links and a method of permanent alignment was desired. New timing interfaces and synchronisation routines were found to be necessary and had to be developed and implemented. The following chapters will give a detailed description of the progress that has been made so far.

2 Classical Cryptography

Contents

2.1 Overview

Cryptography, the art of encrypting messages so that only legitimate addressees can read its content, has been invented more than 6000 years ago. For a long time, it was mainly military institutions who saw the need for secret communication. Examples date back to the ancient Egyptians, the Spartans and the Romans. Cryptographic systems and their defeat have influenced international conflicts like World War II. In the early 1940s British specialists managed to decrypt messages encoded by the German ENIGMA, gaining sensitive information about the positions of German troops.
Rapid development and wide deployment of computers have changed the possibilities of cryptography and cryptanalysis dramatically. While strong ciphers had been impractical because of their time consumption before, some of them became feasible immediately. On the other hand, attacks could now be performed in only a fraction of the time they took before.
Therefore, today cryptography is not anymore a playground for military forces only, but has become a part of everybody's life. Whenever sensitive data like PINs, credit card numbers etc. are being sent through networks, they usually get encrypted. In this chapter I will introduce some basic cryptographic algorithms to give an overview over classical cryptography and the motivation for the need of quantum cryptography.

2.2 Terminology

The usual situation is this: Party A (usually called Alice) wants to send a message to party B (named Bob) in a secure way. An eavesdropper (Eve) who gets hold of the message should not be able to gain any information about its contents.

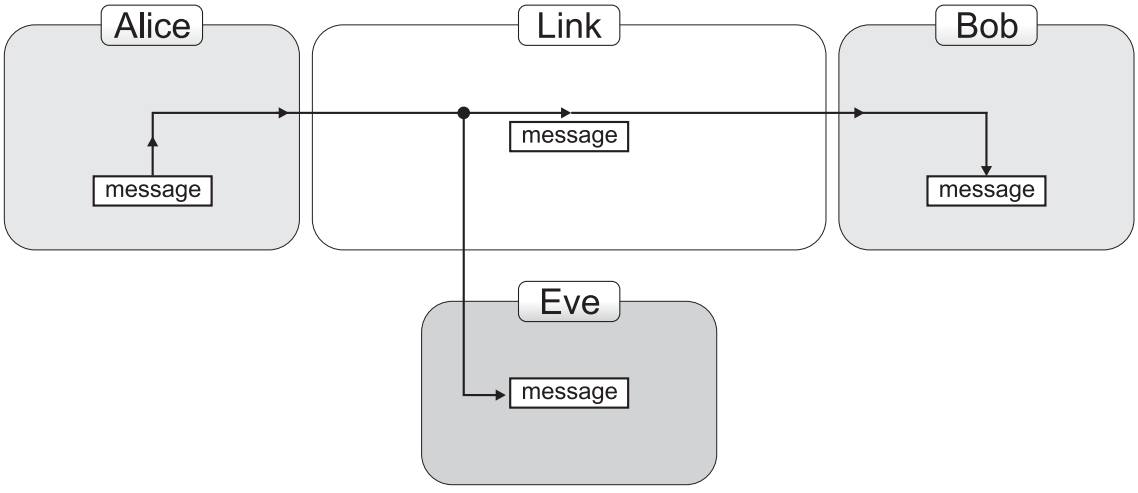


Figure 1: Alice sends a plaintext message to Bob with an eavesdropper (Eve) present.

Since Alice cannot send the plaintext message to Bob in a normal letter, she has two possibilities: She could either hide her message, so that a potential adversary would not recognise it as one, or transform her text into something which is illegible to anybody else than the legitimate recipient. The former method is called **stenography**, the latter **cryptography**, which will be the topic of this chapter.
Cryptography is one of the two fields covered by **cryptology** (from the Greek *kryptós*, "hidden" and *lógos* "word"), the science of secure or generally secret communications [1]. It also includes **cryptanalysis** (from the Greek *kryptós*, "hidden" and *analýein* "to loosen" or "to untie"), the art of recovering information from ciphertexts without knowing the key.

2.2.1 Encryption and Decryption

Alice writes her message in **plaintext** or clear text; the process of disguising the message so that the information is hidden, is called **encryption**. The encrypted message is referred to as **ciphertext**. When Bob performs the reversal of the encryption process, this is called **decryption**. The terms "encipher" and "decipher" are synonymously used for "encrypt" and "decrypt".

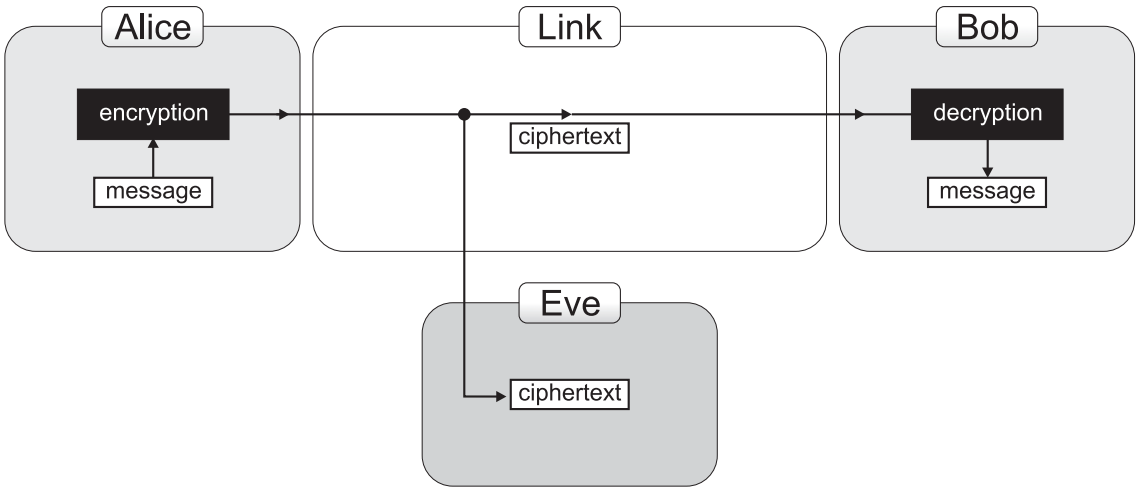


Figure 2: Alice encrypts her message and sends the ciphertext to Bob. While he can decrypt it and read the message, the eavesdropper should not be able to do so.

2.2.2 Algorithms and Keys

The actual procedure used by Alice to encrypt the message is a **cryptographic algorithm** or **cipher**. Generally there are two algorithms, one for the encryption and one for

decryption. The security of **restricted** algorithm is based on the fact that the algorithm itself is kept secret.

Historically, these restricted algorithms played an important role. In 1883 Auguste Kerckhoffs van Nieuwenhof proposed in his book *La Cryptographie militaire* that cryptographic methods should be divided into algorithms and **keys**, while only the key has to be kept secret. The key usually is a string of characters or a large number. It serves as a second input to the encryption and decryption process, to make the ciphertext depend strongly on the key itself. When such a keyed algorithm is used, the algorithm itself may be publicly known, but the security of the cipher depends on the key. This requirement is called **Kerckhoffs' principle**. There are practical advantages, too, as in the following situation: Alice wants to communicate privately with two parties, Bob and Charlie, Charlie should not be able to read what Alice has sent to Bob. Alice could develop two different cryptographic algorithms or she just develops one that needs a key. Then she can give different keys to Bob and Charlie and to every party with which she might want to communicate in future. And although they all know how the algorithm works, they still cannot decrypt those ciphertexts, which are not intended for them, as they do not have all keys.

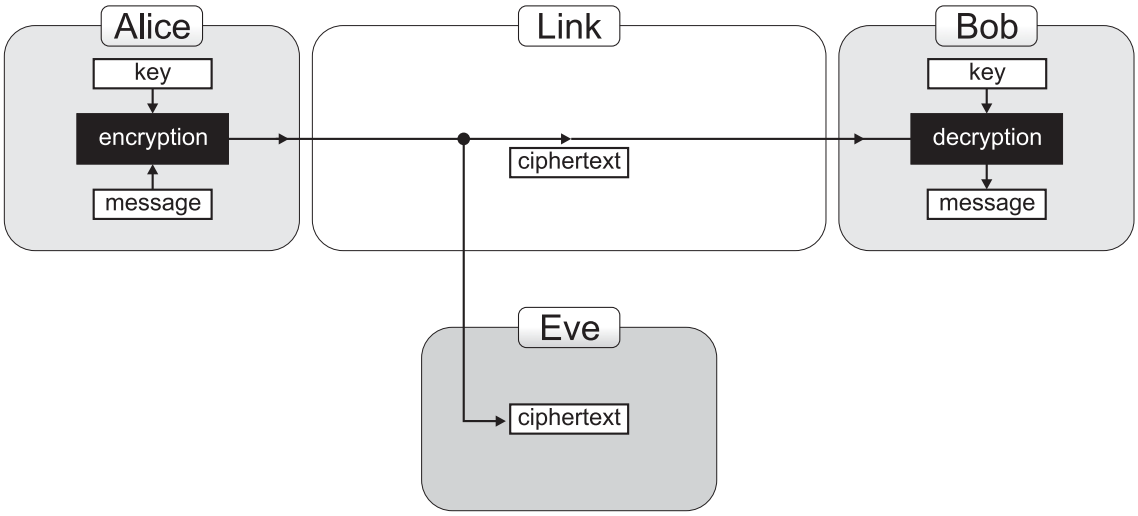


Figure 3: The encryption algorithm and the decryption algorithm have two inputs: Message or ciphertext and additionally a key, which both parties share. The employed algorithm may be publicly known, only the key has to be kept secret.

In fact, the discrimination between restricted and keyed algorithms may seem a little artificial. One could always look at the same algorithm with two different keys as two independent algorithms. Nevertheless it makes sense, because most properties of algorithms can be discussed independently of keys.

Symmetric and Asymmetric Algorithms

Keyed algorithms can be divided into two subgroups, symmetric and asymmetric ones. While **symmetric** algorithms use the same key for encryption and decryption, **asymmetric** ciphers work with one key for encryption and a different key for decryption. The most important examples of asymmetric ciphers are the so-called **public-key** algorithms, where messages get encrypted using the public key and decrypted only with the matching private key.

2.2.3 Security of Ciphers

An algorithm is called **unconditionally secure** if an adversary with unbounded computational power cannot gain enough information from the ciphertext to reconstruct the message, regardless of how much of the encrypted message he could obtain. Unconditional security is certainly the ultimate goal of cryptography and one algorithm is known that withstands the attack of an eavesdropper with infinite resources: The one-time pad (see section 2.5).
Because of the technical difficulties of that algorithm (key distribution, see section 2.5.3), classical cryptography is more concerned with ciphers that give **computational security**. Algorithms are said to be computationally secure if the level of computation required to break the cipher is sufficiently higher than what is available at the moment. Some of the involved problems are proven to be hard to compute, while others are only assumed to be difficult, since so far nobody has been able to solve them efficiently. Examples of supposedly difficult problems are the factorisation of large integers and the computation of discrete logarithms.
Since the latter class of algorithms is usually more practical to use, most of the currently used ciphers are only computationally secure.

2.3 Transposition Ciphers

Before computers were commonly used, cryptographic algorithms were mainly character-based, whereas today they are usually dealing with bits. Nevertheless, the principles are similar, since one can assign a number to each character or think of bits in terms of an alphabet containing only two letters.
The transposition cipher is one of the prominent algorithms originally designed for characters.

2.3.1 Principle

Given a plaintext message, the transposition algorithm shuffles the characters around, rearranging their positions in the string. The ciphertext consists of the same characters,

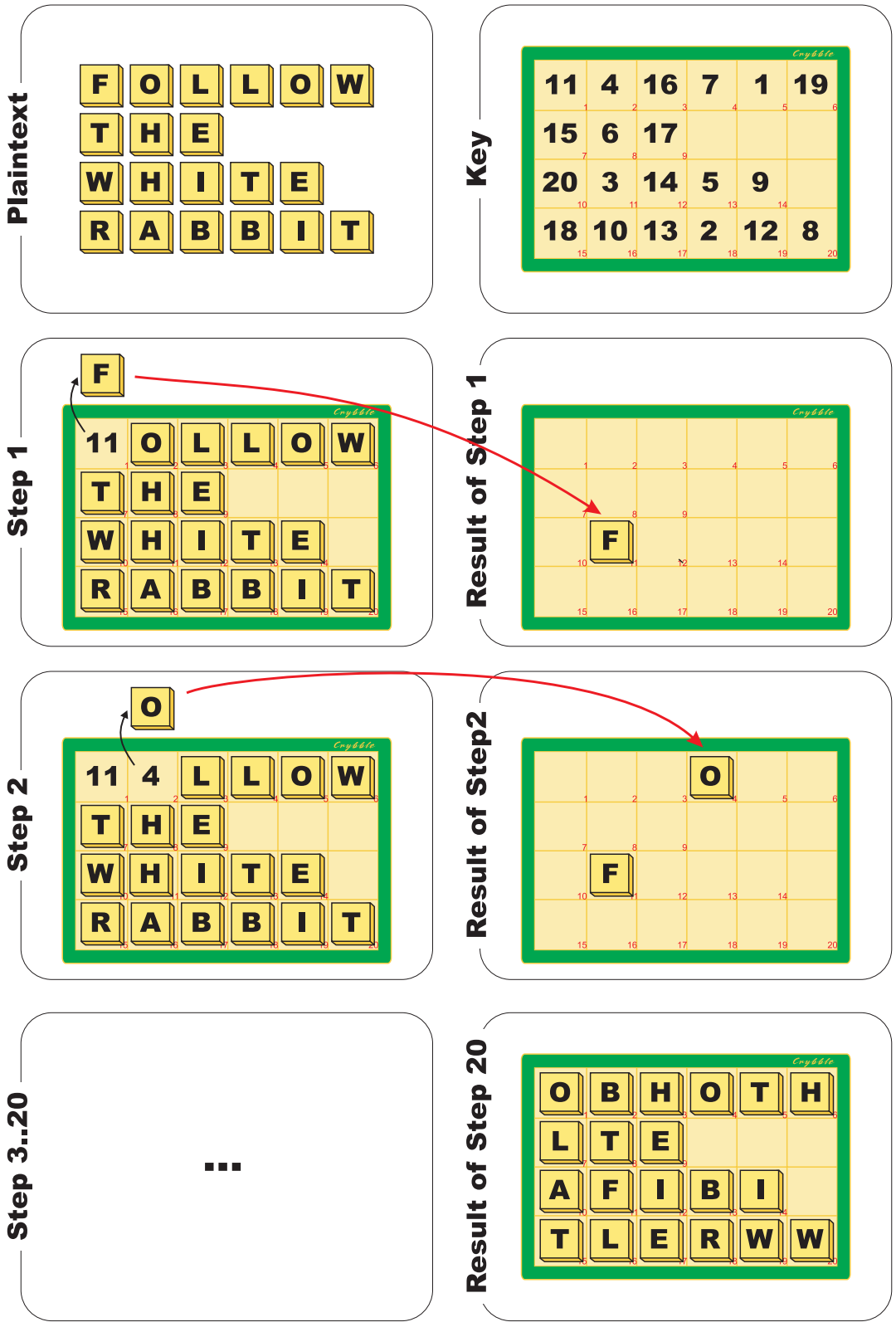


Figure 4: Transposition Cipher. The key determines, how the characters are reordered.

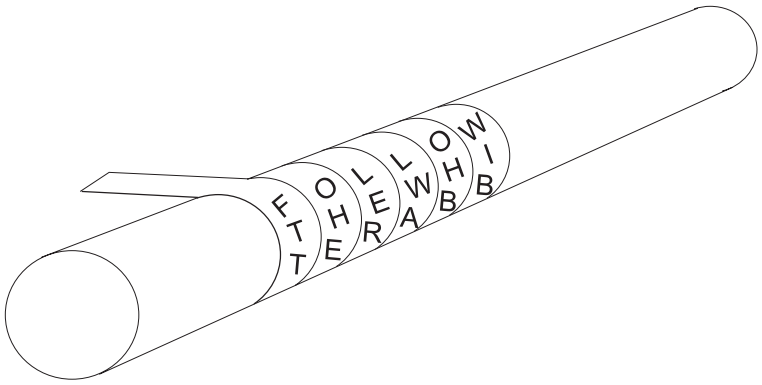


Figure 5: Scytale

they have just been put into different positions. The precise way how this is done can be thought of as the key.
To illustrate this, one can think of a Scrabble® set consisting of a board and some tiles with the needed characters (see figure 4). The key could be imprinted on the board, giving the exact position in the ciphertext. Working through the plaintext and placing each tile on its position in the ciphertext as the board tells, one ends up with a string of the original characters in a different order. This is rather easy and quick to do manually. The decryption is done the other way around.

2.3.2 Example: Scytale

The Spartans introduced military cryptography in Europe using a device called **Scytale** (see figure 5) around 400 BC [2]. It was a (possibly irregularly shaped) wooden staff with a piece of parchment wound around it. The message was written lengthwise along the device so that the characters appeared shuffled after unwrapping.
The receiver had an identical copy of the Scytale and could easily reveal the message by wrapping the piece of parchment around his device. In this scheme, the staff itself serves as the symmetric key for the transposition cipher.

2.3.3 Security Considerations

Depending on the complexity of the special algorithm, the security of transposition ciphers can range from very weak to very strong. This complexity is introduced by the properties of the key that determines exactly in which way the characters are reordered. Strong ciphers need keys which are long, random and only used once, so that an adversary cannot gain any knowledge about them. Keys with these properties are difficult to exchange in a secure way, which will also be discussed in section 2.5.3.

2.4 Substitution Ciphers

2.4.1 Principle

A substitution cipher is one in which every character of the plaintext is replaced by another character in the ciphertext. This class can be divided into four groups [3]:

Monoalphabetic Substitution Ciphers

To produce the ciphertext one uses two alphabets. The plaintext alphabet (the usual alphabet) and a cipher alphabet, which consists of the same number of symbols as the normal one. Now one has to exchange every character of the plaintext by the corresponding symbol of the cipher alphabet. To decrypt the message, the reverse procedure is applied.
A very easy example of this type is the Caesar Cipher, described below.

Polyalphabetic Substitution Ciphers

The same principle as in the monoalphabetic substitution is used in a polyalphabetic substitution, only now there are two or more cipher alphabets. Of course, both parties have to agree on a common scheme of when to use which cipher alphabet. The increase in complexity has led to a higher level of security.
The Vigenère Cipher is a powerful example of this subgroup using 26 different cipher alphabets.

Homophonic Substitution Ciphers

A homophonic substitution cipher is an enhancement of a monoalphabetic or polyalphabetic substitution. Here, every character of the plaintext alphabet can be mapped to more than one character of the cipher alphabet, for example “a” could be coded as “12”, “31” and “67”. This can be especially effective against so-called frequency analysis attacks, which exploit the fact that some characters are used more often than others.

Polygram Substitution Ciphers

This scheme replaces blocks of characters in the plaintext with blocks of characters in the ciphertext. It is rather complicated to execute, so that it has not become very popular.

2.4.2 Examples: The Caesar Cipher and the Vigenère Cipher

The Caesar Cipher

One of the earliest known substitution algorithms is the one used by Julius Caesar (100 to 44 BC). He exchanged every character with the third entry of the alphabet to its right.

So the used alphabets look like this:

plaintext alphabet:	a b c d e f g h i j k l m n o p q r s t u v w x y z
secret alphabet:	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
message:	`alea iacta est`
ciphertext:	`DOHD LDFWD HVW`

This method is very simple to use, but it is also easy to break. As soon as the cryptanalyst expects it to be a substitution cipher with the cipher alphabet being a shifted plaintext alphabet, he can simply try out the 25 possibilities.

The Vigenère Cipher

One example for the polyalphabetic schemes was published by Blaise de Vigenère in 1586, combining ideas from Leon Battista Alberti, Johannes Trithemius and Giovanni Porta. The idea is to use 26 different alphabets, shown in table 1. A key is used to determine which ciphertext alphabet is used for which position of the plaintext.
Each alphabet is shifted as in the Caesar Cipher one more character to the left than the previous one. If the key is shorter than the plaintext, the total key has to be concatenated, repeating itself until it is as long as the plaintext. Here is an example of this scheme using the key *hwkqe*.

plaintext:	`follow the white rabbit`
key:	`hwkqeh wkq ehwkq ehwkqe`
ciphertext:	`NLWCTE QSV BPFEV WIYMZY`

2.4.3 Security

A monoalphabetic substitution algorithm with a randomly ordered cipher alphabet seems to give already quite good security since there are $26! \approx 4 \cdot 10^{26}$ possible permutations. But methods such as the analysis of frequencies at which the characters occur, make monoalphabetic and simple polyalphabetic versions of substitution ciphers rather easy to overcome. To increase the security of polyalphabetic substitution ciphers, one needs to increase their complexity. This can be easily done by choosing a more complicated key, i.e. increase its randomness. Hence, repeating a short key to build a longer one is a significant security risk.

2.5 One-time Pad

2.5.1 Principle

The cryptographic algorithm itself is the so-called **Vernam cipher**: Given an alphabet $\mathcal{A} = \{0, 1, \ldots, n-1\}$, a message $m = m_1 m_2 \cdots m_L$, $m_i \in \mathcal{A}$ and a key string of the same

plaintext alphabet :	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
cipher alphabet *a* :	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
cipher alphabet *b* :	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
cipher alphabet *c* :	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
cipher alphabet *d* :	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
cipher alphabet *e* :	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
cipher alphabet *f* :	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
cipher alphabet *g* :	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
cipher alphabet *h* :	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
cipher alphabet *i* :	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
cipher alphabet *j* :	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
cipher alphabet *k* :	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
cipher alphabet *l* :	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
cipher alphabet *m* :	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
cipher alphabet *n* :	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
cipher alphabet *o* :	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
cipher alphabet *p* :	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
cipher alphabet *q* :	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
cipher alphabet *r* :	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
cipher alphabet *s* :	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
cipher alphabet *t* :	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
cipher alphabet *u* :	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
cipher alphabet *v* :	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
cipher alphabet *w* :	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
cipher alphabet *x* :	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
cipher alphabet *y* :	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
cipher alphabet *z* :	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Table 1: The Vigenère Square

length $k = k_1 k_2 \cdots k_L$, $k_i \in \mathcal{A}$, the Vernam cipher produces the ciphertext $c = c_1 c_2 \cdots c_L$ as follows:

$$c_i = m_i \oplus k_i \,, \qquad 1 \leq i \leq L \tag{1}$$

Here, $\oplus$ denotes addition modulo n. In most applications n will be 2, so all the text will be represented in binary. As long as the key string is random and only used once, this method is called the **one-time pad**.

Connection to Polyalphabetic Substitutions

In fact, this Vernam cipher has already been mentioned before, because it (see section 2.4.2) is in principle nothing else but a Vernam cipher, when every Latin character is assigned the position in the alphabet (a=1, b=2, etc.). Equipped with a random key that is only used once, this is already sufficient to provide unconditional security.

2.5.2 Security

As already stated, it can be shown that a message encrypted with the one-time pad contains no information. A random key string added to a non-random plaintext message results in a completely random ciphertext to anybody who doesn't know the key. In this case there is no possibility of breaking the cipher, even with unlimited computational power, because even a brute force attack will not find a criteria to discriminate the correct plaintext from all other possibilities of the same length. There simply is no information in the ciphertext (apart from the length of the text, which can be hidden by compressing it).
It can also be shown that the one-time pad is optimal in the sense that its security would suffer if a shorter key would be used. So this seems to be a perfect cipher, but in fact, it is only rarely used.

2.5.3 Problem: Key Distribution

Despite the very high level of security, there are some major drawbacks of the one-time pad which have prevented it from becoming a widely used encryption scheme. The main problem is key distribution. Since the security of the one-time pad is only dependent on the secrecy of the key, one has to be absolutely sure, that a potential eavesdropper has no information at all about the key. So the key distribution method has to be at least as secure as the one-time pad itself. There is no efficient classical method to fulfil this requirement.
At this point quantum mechanics has provided a completely new opportunity. Quantum cryptography enables us to distribute a random key between two spatially separated parties in a secure way. This key can then be used in a one-time pad to come as close to unconditional security as possible (see chapter 3).

2.6 Modern Algorithms

When human beings are the ones that have to carry out cryptographic algorithms, these algorithms have to be chosen rather carefully with respect to the complexity. Though the basic steps usually are easy, there is a huge number of them to be performed with high precision. Depending on the cipher, one mistake in an early stage of the encryption process could lead to a total loss of information. To circumvent those restrictions, scientists invented machines, capable of computing some algorithms much faster and much more reliable. A very famous example is the ENIGMA, a mechanical machine used by the German forces during World War II. It was a rather sophisticated device with a relatively complicated algorithm implemented into it, but nevertheless English specialists led by Alan Turing were able to break the ciphers, enhancing an idea from a Polish cryptanalyst [2].

Nowadays, the availability of computers has revolutionised the field of cryptography and cryptanalysis. Simple ciphers can easily be broken by brute force methods because of the speed with which modern computers can carry out operations. On the other hand, more and more complex cryptographic algorithms can be used, which help to keep the balance. Furthermore, the Internet has created a great need for cryptography. Sensitive information like credit card numbers and access codes for bank accounts are constantly flowing through the web, putting ordinary people in a position where they have to rely on the fact that only the legitimate addressee will be able to use it. Fifty years ago, strong cryptography was hardly an issue for private citizens. Today most of us are using it on an everyday basis more or less consciously.
Most algorithms that are currently used are block ciphers. In contrast to stream ciphers, which process each character separately, block ciphers divide the message into parts of fixed length and do some manipulations on these blocks. This is usually done in many iterations, so that a slight change of the plaintext can result in a completely different ciphertext. This leads to a big advantage over some eavesdropping strategies, like the known-plaintext-attack, an attack where the eavesdropper tries to deduce the key and therefore the full plaintext from a fragment of known plaintext.

2.6.1 Symmetric Block Ciphers: DES and Triple DES

DES

When computer based cryptography became more and more important, people had to agree on which cipher to use. In July 1977, the U.S. National Bureau of Standards (NBS) proclaimed the so-called Data Encryption Standard (DES or DEA, Data Encryption Algorithm). It was reviewed in 1983, 1988 and 1993 and remained the standard symmetric cipher until October 1999, when Triple DES was announced to be the "FIPS approved symmetric encryption algorithm of choice" by the National Institute of Standards and Technology (NIST), the successor of the NBS [4].
DES is an implementation of the Lucipher cipher (or Feistel cipher) with an effective key length of 56 bits, developed by Horst Feistel for IBM [2]. More precisely, the key is specified as a 64 bit string, but 8 bits are used as parity bits and therefore not relevant for security. The plaintext is divided into blocks of 64 bits, and each of these blocks is then encrypted by the algorithm described below.
The DES algorithm can be divided into five stages (see figure 6):

1. **Round key generation**
   The algorithm calculates 16 keys $(K_1, ..., K_{16})$, each of 48 bits length, from the 56 bit long input key.

2. **Initial permutation**
   The 64 input bits are permuted in a fixed way and then split into two blocks of 32 bits L_0 and R_0.

3. **16 keyed substitution rounds**
   This is the heart of the DES algorithm. The following steps are applied 16 times ($i = 1, ..., 16$):

   a) $$L_i = R_{i-1} \tag{2}$$

   b) $$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \tag{3}$$

   This means that R_{i-1} is first encrypted using the round key K_i. R_{i-1} is expanded to a 48 bit string by using some bits twice, then it is added to K_i modulo 2 and afterwards shrunk to 32 bits in a way that is complicated for humans, but not for machines.

   The result is added to the left half of the outcome of the previous stage L_{i-1} modulo 2.

4. L_{16} and R_{16} are swapped to make the decryption process easier.

5. The inverse of the initial permutation is performed.

The decryption works exactly like the encryption with the round keys in reverse order. This can be easily seen:

1. The round keys are generated as in the encryption process, but they will be applied from K_{16} to K_1.

2. The initial permutation IP is the inverse of the final permutation IP^{-1}, so that after applying IP, the string will be $R_{16}L_{16}$.

3. The 16 keyed substitution rounds are processed as above (with reversed key order). To keep the notation consistent, i has to be decreased from $i = 16$ to $i = 1$:

   a) $$R_{i-1} = L_i \tag{4}$$

   This is exactly the reversal of assignment (2).

   b) $$L_{i-1} = R_i \oplus f(L_i, K_i) \tag{5}$$

   It can be shown, that this is the inverse of the encryption process. The right half of equation (5) can be evaluated using equations (2) and (3):

$$\begin{aligned} R_i \oplus f(L_i, K_i) &\overset{(2)}{=} R_i \oplus f(R_{i-1}, K_i) && \text{(6a)} \\ &\overset{(3)}{=} L_{i-1} \oplus \underbrace{f(R_{i-1}, K_i) \oplus f(R_{i-1}, K_i)}_{=0} && \text{(6b)} \\ &= L_{i-1} && \text{(6c)} \end{aligned}$$

The fact, that this can be shown without knowledge of the special form of $f(R_{i-1}, K_i)$ implies that the choice of f is not important for the successful operation of encryption and decryption. Hence it can be chosen with respect to optimal security.

4. R_0 and L_0 are swapped, so that one ends up with L_0R_0.

5. The reverse of the initial permutation will give the original plaintext block $m = m_1 \dots m_{64}$.

Triple DES

Triple DES or TDEA (Triple Data Encryption Algorithm) replaced the single DES as a U.S. standard. It basically uses the DES algorithm three times. If $E_K(I)$ and $D_K(I)$ are encryption and decryption of I using (single) DES with the key K, then TDEA encryption with the outcome O is defined as

$$O = E_{K_3}(D_{K_2}(E_{K_1}(I))) \quad .$$

So TDEA encryption first encrypts the message with a key K_1, then decrypts the result with key K_2 and after that encrypts this with key K_3. The decryption works the other way round, of course.
The standard allows three keying options: Either all keys are different ($K_1 \neq K_2 \neq K_3$), or $K_1 = K_3 \neq K_2$, or all keys are the same ($K_1 = K_2 = K_3$). The last case is equivalent to only one single DES encryption process with key K_1. Thus, it doesn't yield any additional security compared to single DES. Nevertheless it is allowed in order to maintain backward compatibility.
It is important to note that the encryption of DES does not form a group, which would mean that subsequently encrypting a message with two different keys can always be achieved by only encrypting the message once with a third key. If this were the case, multiple encryption using DES would not lead to enhanced security [5].

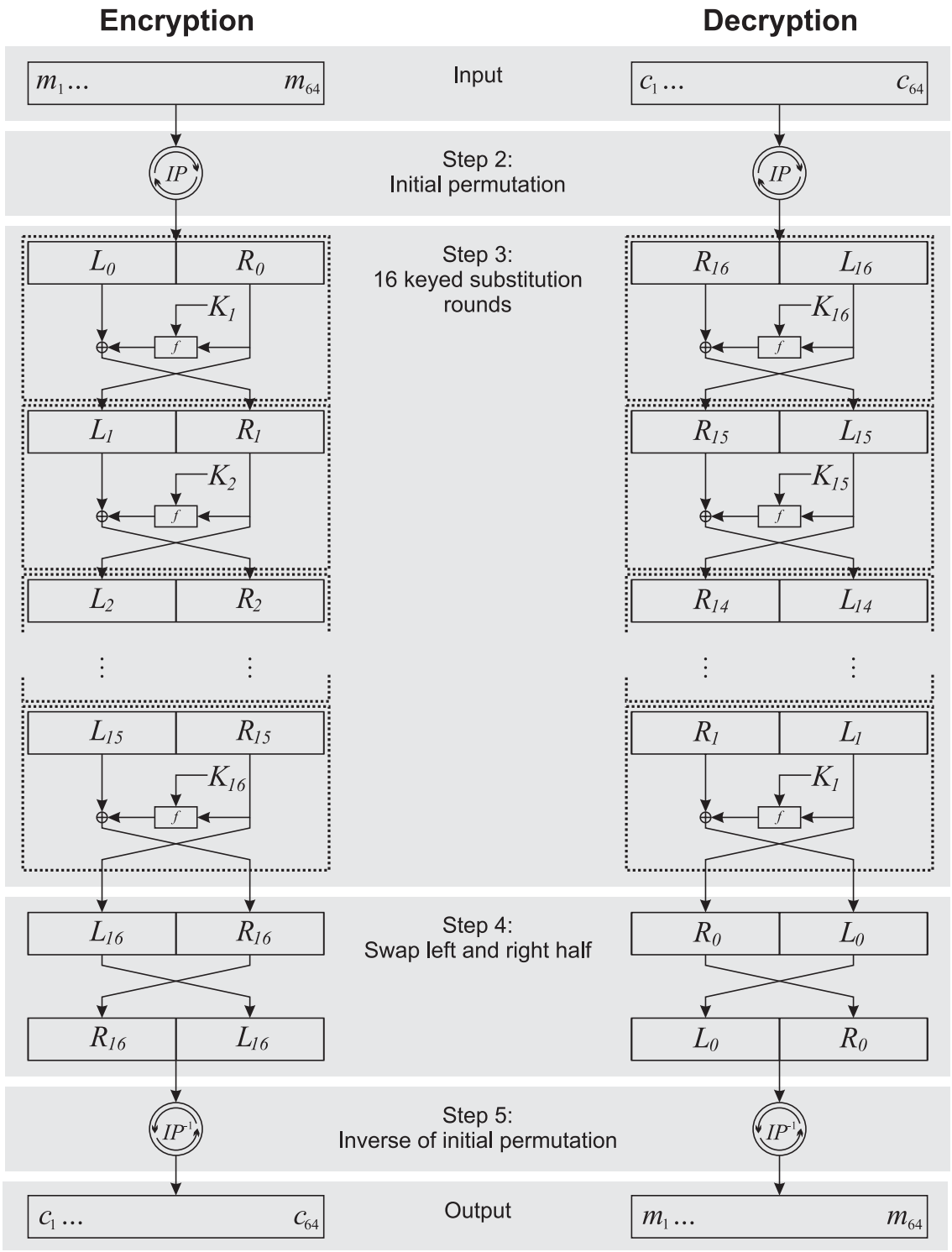


Figure 6: Encryption and decryption in the DES algorithm. 64 bits of the plaintext message are processed to 64 bits of the ciphertext in the encryption process and vice versa in the decryption process. Step 1, the round key computation generation is not shown.

2.6.2 Asymmetric Cryptography: RSA

So far, I have only considered symmetric algorithms, where both parties have to share the same key. This key has to be kept secret, which imposes the problem of secure key distribution from one party to the other.
In 1976 Whitfield Diffie and Martin Hellman published their ideas to use a cryptosystem with two different keys: One for encryption (the public key) and a different one for decryption (the private key). The great advantage is, that the public key doesn't have to be kept secret, only its authenticity needs to be assured.
The basic idea is that there are problems which are easily solved in one direction, but hard to solve inversely. A famous example is the integer factorisation problem: It is quite easy to multiply some prime numbers and obtain a big integer, but it is much more difficult to find out the prime factors, given a large integer.
Although Diffie and Hellman first published their idea of public-key cryptography, it is likely that it had been invented before, but kept secret by employees of the Government Communications Headquarters (GCHQ) in Cheltenham, UK. In 1969, James Ellis found an existence theorem for asymmetric cryptography and Clifford Cocks invented an algorithm equivalent to RSA in 1973. One year later, Malcolm Williamson presented the Diffie-Hellman-Merkle key exchange algorithm.

RSA

The RSA cryptosystem, invented by R. Rivest, A. Shamir and L. Adleman, is the most important asymmetric cryptosystem. It relies on the intractability of the integer factorisation problem and can be used for secret communication as well as for digital signatures. The RSA algorithm is rather simple and consists of three parts:

1. **Key generation**

   a) Select two large primes p and q randomly, ensuring that both are roughly the same size.

   b) Calculate $n = p \cdot q$ and $\phi = (p-1)(q-1)$.

   c) Select a random integer e, $1 < e < \phi$, under the restriction that the greatest common divisor of e and ϕ is 1.

   d) Compute the unique integer d, $1 < d < \phi$ with the property $ed = 1 (\mathrm{mod}\, \phi)$. This can be accomplished using the so-called Euclidean algorithm.

   The public key consists of (n, e) and the private key is d.

2. **Encryption of the message**
   This is what Alice has to do

   a) Get Bob's public key and ensure its authenticity.

b) Represent the message as an integer m, with $0 \leq m < n$. This can for example be done by translating every character of the plaintext into an 8-bit binary number (e.g. using the ASCII standard), concatenate all bits and calculate the corresponding integer.

c) Calculate $c = m^e \bmod n$.

c is the encrypted message that can be sent to Bob.

3. **Decryption of the ciphertext**
   When Bob receives the encrypted message, all he has to do is calculate one function to reconstruct the original message: $m = c^d \bmod n$.

Applications of RSA

Even when all known acceleration techniques are employed, the RSA encryption and decryption is considerably slower than popular symmetric ciphers. Hence, the RSA scheme is mostly used to exchange a secret key, which can then be used for a symmetric cipher. This combination is implemented in applications and protocols like "Pretty Good Privacy" (PGP), "Secure Sockets Layer" (SSL) and "Secure Shell" (SSH).
As already mentioned, a variant of RSA provides the opportunity of digital signatures. It allows the receiver of a message to verify that it really came from the correct sender and rules out that it was forged. This is possible, because the RSA keys allow Alice to encrypt a message using her private key. The ciphertext can be decrypted only with the matching public key only. If Bob is sure that the public key belongs to Alice, he can determine whether the message came from Alice or not.

Security of RSA

The only known way how to decrypt the message is to calculate d by factoring n. There are no efficient algorithms known to achieve that, but there might be an alternative way to break the cipher: Until now, it hasn't been proven that there aren't methods of deducing m from c, e and n. But if this alternative procedure allowed calculating d, then this would obviously be a way of factoring large integers. There are more problems one has to keep in mind while working with RSA cryptosystems. These impose constraints on the choices of the parameters and prohibit some actions like signing documents one doesn't know the content of.
The biggest threat to the RSA algorithm is, of course, that it could become possible to factorise large integers efficiently. So far, nobody has published a method that achieves this goal on a classical computer. Still it seems rather dangerous to rely on this. As unlikely as it may seem, someone might come up with an efficient algorithm in the near future or, even worse, somebody might already have thought of such an algorithm. Furthermore, there already exists an algorithm to factor big integers efficiently on a quantum computer, although the realisation is very difficult from today's point of view.

3 Quantum Cryptography - Theory

Contents

3.1 Introduction

In the previous chapter a variety of encryption algorithms have been introduced, providing different levels of security. Apart from one, they all have in common that in principle they can be cracked. For example, the RSA cryptosystem, one of the widely used algorithms (e.g. in SSL, SSH), relies on the fact that it is difficult to find the factors of large integers. There are two threats to this method: The first is that more computational power will help to make time-consuming attacks (like brute-force attacks) more convenient. Moreover, someone might even think of an efficient algorithm for factoring integers. The second problem is, that quantum computers are in fact already capable of executing the factorisation efficiently (see e.g. [6, 7]). Until now, it cannot be done with large integers (so far, 15 has been factorised into 5 and 3 with high probability on an NMR quantum

computer) and it will probably take some time for it to become practical, but for crucial applications "probably secure" isn't enough.
On the other hand, there exists a classical, unconditionally secure cryptographic algorithm, but it has a big problem: It requires a random key, which has to be as long as the message itself and this has to be transported securely from one party to the other. This cannot be done classically.
Here, an amazing idea comes into play: Quantum mechanics has the property of hiding some information from us, as expressed in Heisenberg's uncertainty relation. Could this inherent ignorance be used as an advantage over a potential eavesdropper? It turns out, that this is indeed possible and after discussing the essential quantum mechanical properties, I will introduce a method of establishing a secret key between two parties, which is provably secure. This security is a direct consequence of the fundamental axioms of quantum mechanics. As long as we do not find that we can gain more information on quantum states than described by quantum mechanics, this scheme has to be regarded secure.
Really interesting about this method is that a usually unfavourable property of quantum mechanics is actually employed to achieve something that can't be done outside the quantum world. The fact that two non-commuting observables can only be measured with limited precision allows unconditionally secure key distribution.
The whole idea has been named **quantum cryptography** or **quantum key distribution** (QKD). I will use these expressions synonymously. A broad introduction into the field of quantum cryptography can be found in [8].

A Quantum Cryptography System

Before reviewing general properties of quantum particles, it might be instructive to sketch very briefly how a quantum cryptography system could be used to transmit binary data from Alice to Bob.

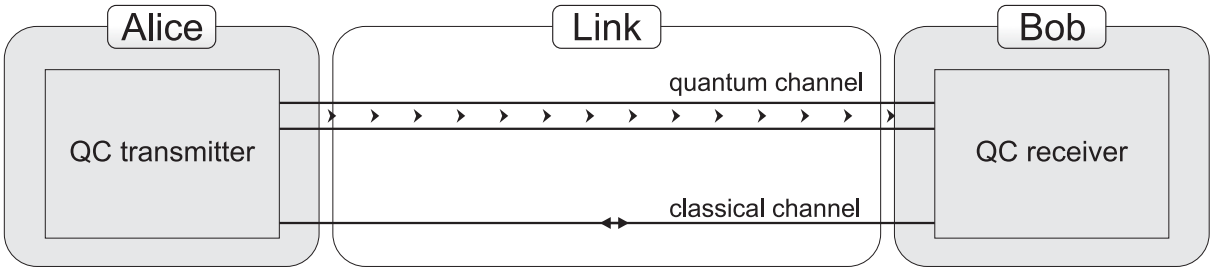


Figure 7: The basic quantum cryptography system. Alice can send qubits into a quantum channel, at which Bob listens. Both have bidirectional access to an authentic classical channel.

First, Alice and Bob need to establish a secret key between them, using quantum key

distribution. This requires a quantum channel, into which Alice can send and Bob can listen to. Furthermore, they will need an authentic classical communications channel. This means that while their messages are not secure against eavesdropping, they still cannot be forged by an eavesdropper[1]. As soon as they both share the secret key, they can use it to encrypt a message with a classical algorithm. For the highest possible security, they should use the one-time pad, but if other restrictions (like low key rates) make that impossible, they can use algorithms like Triple-DES and still have the advantage over classical methods, that at least the key distribution was unconditionally secure.

3.2 Quantum Mechanical Background

3.2.1 Qubits

In classical information theory the basic unit of transmitted information is the **bit** (binary digit), it can have the two values 0 and 1.
The quantum analogue of the bit is the so-called **qubit** (quantum bit). It is represented by a state $|\psi\rangle$ in a two-dimensional Hilbert space, whose orthogonal basis vectors are denoted $|0\rangle$ and $|1\rangle$ and called computational basis states. The big difference between bits and qubits is that a bit can only be in state 0 or 1, whereas a qubit can be in a **superposition** state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $\alpha, \beta \in \mathbb{C}$ and $\langle\psi|\psi\rangle = 1$, so that $|\alpha|^2 + |\beta|^2 = 1$. Neglecting global phases, as they have no measurable effect, any such state (i.e. any pure qubit state) can be written as

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{\mathrm{i}\phi}\sin\frac{\theta}{2}|1\rangle \quad . \tag{7}$$

This is called the Bloch representation and can be visualised on the **Bloch sphere** (figure 8). The vector $(\cos\phi\sin\theta, \sin\phi\sin\theta, \cos\theta)$ is called the Bloch vector. Since unitary transformations do not alter the length of a state, every unitary transformation can be represented by a rotation of the Bloch vector.

Physical Realisation of Qubits

A qubit can be physically realised with any 2-level-system, for example two electronic levels of an atom could be used. A different well known realisation is a spin 1/2 particle, where $|0\rangle = |\uparrow\rangle$ and $|1\rangle = |\downarrow\rangle$ are the eigenfunctions of σ_z. In every 2-dimensional Hilbert

[1] An arbitrary channel can be made authentic only if Alice and Bob initially share a short secret key. Without that, it is impossible for Bob to tell, whether Alice is not being impersonated by Eve etc., the so-called man-in-the-middle attack. The quantum secret growing protocol (see [9]) starts with a short secret key and extends this to a useful length. A short part is then being kept for authentication of the next key distribution and the rest can be used to encrypt the message.

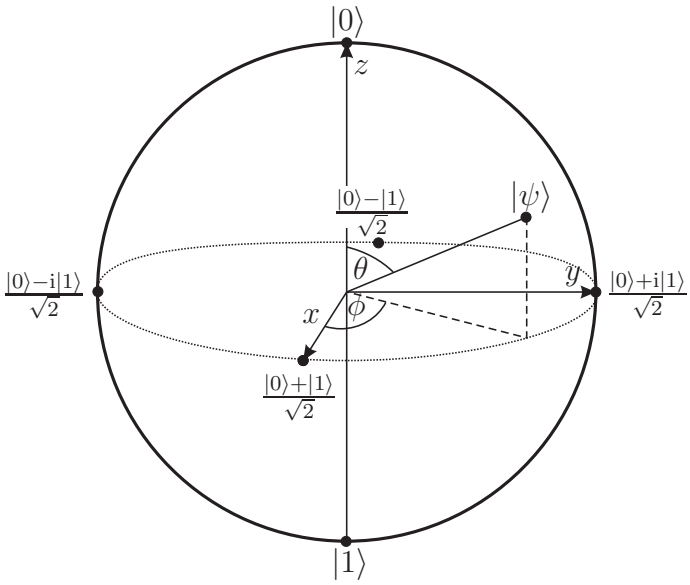


Figure 8: The Bloch sphere. Every state on it can be expressed by $|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\,\sin(\theta/2)|1\rangle$.

space, there exist three conjugate bases[2], in this special case they can be chosen as the eigenfunctions of the σ_z, σ_x and σ_y operators. These three sets of basis vectors are shown as dots in figure 8. The states $\frac{|0\rangle\pm|1\rangle}{\sqrt{2}}$ are the eigenvectors of σ_x and the remaining ones are eigenvectors of σ_y.

The polarisation of a single photon can be treated analogously to the spin 1/2 formalism. Here, a possible combination of bases is horizontal/vertical (H/V), $+45°/-45°$ diagonal (+/−) and left/right circular (L/R) corresponding to the eigenvectors of σ_z, σ_x and σ_y.

In the following sections, the notation of polarisation will be used, because this is needed for the experiment. In this special case, the analogue to the Bloch sphere is called the **Poincaré sphere** (figure 9).

3.2.2 General Properties of Qubits

Before introducing quantum cryptography itself, some characteristics of quantum states have to be discussed, since they will be needed later to understand the security of the used methods.

[2]Two bases of a 2-dimensional Hilbert space are said to be conjugate if both basis vectors of one basis projected onto each basis vector of the other basis have length 1/2. This means that a measurement in one basis will completely randomise the result of a measurement in the other basis.

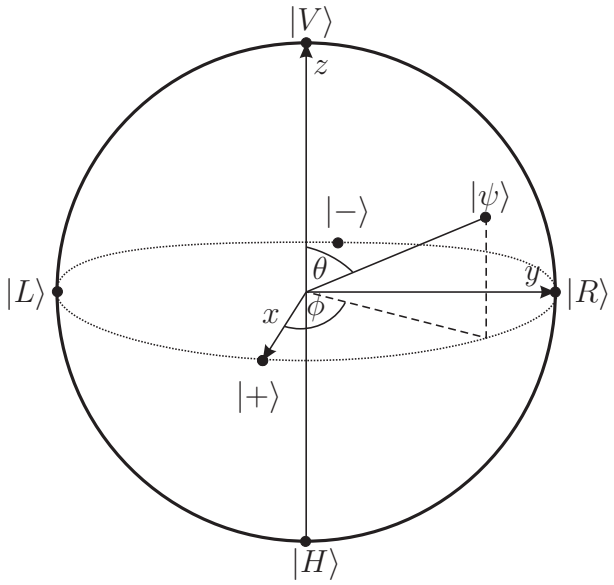


Figure 9: The Poincaré sphere. $|H\rangle$ ($|V\rangle$), $|+\rangle$ ($|-\rangle$) and $|L\rangle$ ($|R\rangle$) denote horizontal (vertical), $+45°$ ($-45°$) and left (right) circular polarisation of a photon.

Distinguishing Non-Orthogonal States

An important property of the quantum world is the impossibility to discriminate two non-orthogonal states reliably. This can be generally shown (see [6, p. 87]), but it's easier to prove under the assumption, that only projective measurents are used:
Let $|\psi\rangle$ and $|\phi\rangle$ be non-orthogonal states, which means

$$\langle\psi|\phi\rangle \neq 0 \quad . \tag{8}$$

A projective measurement is defined as follows [6]:

Definition: Projective measurement A projective measurement is described by an observable M, a Hermitian operator on the state space of the system being observed. The observable has a spectral decomposition

$$M = \sum_m m P_m \quad , \tag{9}$$

where P_m is the projector onto the eigenspace of M with eigenvalue m. The possible outcomes of the measurement correspond to the eigenvalues m of the observable. Upon measuring the state $|\psi\rangle$, the probability of getting result m is given by

$$p(m) = \langle\psi|P_m|\psi\rangle \quad . \tag{10}$$

Given that the outcome m occured, the state of the quantum system immediately after the measurement is

$$|\psi'\rangle = \frac{P_m|\psi\rangle}{\sqrt{p(m)}} \quad . \tag{11}$$

Let there be four different states $|H\rangle$, $|V\rangle$, $|+\rangle$ and $|-\rangle$, denoting four linear polarisations (horizontal, vertical, $+45°$ and $-45°$), building two orthonormal bases $\{|H\rangle, |V\rangle\}$ and $\{|+\rangle, |-\rangle\}$. One can construct two observables

$$M_R = |V\rangle\langle V| - |H\rangle\langle H| \tag{12a}$$
$$M_D = |+\rangle\langle +| - |-\rangle\langle -| \quad , \tag{12b}$$

representing a measurement of the polarisation in the H/V basis (R for rectilinear) and in the diagonal basis $+/-$ (D).
To see more easily, how the projectors work in the different bases, one can decompose the base states into the rotated basis:

$$|V\rangle = (|+\rangle + |-\rangle)/\sqrt{2} \tag{13a}$$
$$|H\rangle = (|+\rangle - |-\rangle)/\sqrt{2} \tag{13b}$$
$$|+\rangle = (|V\rangle + |H\rangle)/\sqrt{2} \tag{13c}$$
$$|-\rangle = (|V\rangle - |H\rangle)/\sqrt{2} \tag{13d}$$

This means that for example letting act M_R on a state $|+\rangle$, one will get equal probabilities of having the outcome $+1$ (corresponding to V) and -1 (corresponding to H):

$$p_R^{|\pm\rangle}(+1) = \langle \pm|V\rangle\langle V|\pm\rangle \tag{14a}$$
$$= (\langle H| \pm \langle V|)\,|V\rangle\langle V|\,(|H\rangle \pm |V\rangle)/2 \tag{14b}$$
$$= 1/2 \tag{14c}$$

In the same way, the other measurements are equally unsignificant:

$$p_R^{|\pm\rangle}(-1) = p_D^{|H\rangle}(\pm 1) = p_D^{|V\rangle}(\pm 1) = 1/2 \tag{15}$$

This proves, that there is no possibility to distinguish reliably between the four different states, when a projective measurement is used and the basis is unknown. If basis vectors of two bases have this property, they belong to conjugate bases. These basis vectors are located on perpendicular axes of the Poincaré or Bloch sphere.
One could think that it might help to measure in the other basis after the first measurement and repeat these measurements a lot of times, but it can be shown, that this does not help to solve the problem:

Measurements Disturb States

Not only is the measurement potentially incorrect, furthermore it can also change the state of the qubit after the measurement. This can be concluded from equation (11).
In the case of the four states $|V\rangle$, $|H\rangle$, $|+\rangle$ and $|-\rangle$, this leads to the fact, that if one measures in the wrong basis, the state which leaves the measurement device will be different from the one that entered it. Applied to the first example above (measuring a $|\pm\rangle$ in an H/V basis), this leads to:

$$|\psi'\rangle = \begin{cases} |V\rangle\langle V|\pm\rangle/\sqrt{p_R(+1)^{|\pm\rangle}} & \text{if outcome } +1 \\ |H\rangle\langle H|\pm\rangle/\sqrt{p_R(-1)^{|\pm\rangle}} & \text{if outcome } -1 \end{cases} \tag{16a}$$

$$= \begin{cases} |H\rangle\langle H|\left(|H\rangle \pm |V\rangle\right) = |H\rangle & \text{if outcome } +1 \\ |V\rangle\langle V|\left(|H\rangle \pm |V\rangle\right) = \pm|V\rangle & \text{if outcome } -1 \end{cases} \tag{16b}$$

Thus, if the result of the measurement leads to the conclusion that there has been e.g. a horizontally polarised photon, after the measurement it will be a horizontally polarised photon. Having acknowledged this, it becomes unnecessary to try and measure the system again to learn more about the state before the measurement.
Again, this has only been shown here for projective measurements, but in can be proven more generally (see [6, 7, 10]), that any attempt to distinguish between non-orthogonal states will disturb the state itself.

Quantum Cloning

To bypass the indistinguishability, the following idea could arise: If it is impossible to measure in two bases at once, why not duplicate the qubit and measure one of the clones in the H/V basis and the other one in the +/− basis.
One might already have the impression that this cannot work, because it would violate the principle that it is not possible to determine in which of two non-orthogonal states a system exists without introducing some disturbance. And indeed, this is easy to show.
Let $|\psi\rangle$ and $|\varphi\rangle$ be two non-orthogonal states, so that $\langle\psi|\varphi\rangle \neq 0$. Suppose that there exists a quantum mechanical machine, which accomplishes cloning the two states:

$$|\psi\rangle|\text{blank}\rangle|\text{machine}\rangle \longrightarrow |\psi\rangle|\psi\rangle|\text{machine}'\rangle \tag{17a}$$

$$|\varphi\rangle|\text{blank}\rangle|\text{machine}\rangle \longrightarrow |\varphi\rangle|\varphi\rangle|\text{machine}''\rangle \tag{17b}$$

The evolution of systems in quantum mechanics can always be described by unitary transformation (possibly in a Hilbert space of higher dimension), which leave scalar products unchanged. So the scalar product of the input states should be equal to that of the output states:

$$\langle \text{machine}|\langle \text{blank}|\langle\varphi||\psi\rangle|\text{blank}\rangle|\text{machine}\rangle = \langle\varphi|\psi\rangle \tag{18a}$$

$$\stackrel{!}{=} \langle \text{machine}''|\langle\varphi|\langle\varphi||\psi\rangle|\psi\rangle|\text{machine}'\rangle = \langle \text{machine}''|\text{machine}'\rangle\langle\varphi|\psi\rangle^2 \tag{18b}$$

This can only be fulfilled if either all factors are equal to 1 or both sides are equal to 0 (since every scalar product of normalised vectors holds $0 \leq |\langle\psi_1|\psi_2\rangle| \leq 1$). This means that one can only clone a state which is known to be one of two orthogonal states. That is contradictory to the assumption that the two states are non-orthogonal, which means that one cannot clone quantum states.
Although the existence of such a no-go theorem is very attractive, it doesn't say anything about the possible quality that can be achieved when one tries to duplicate a quantum state. This has been examined for example in [11, 12].
Gisin and Massar [11] have generalised an idea of Bužek and Hillery [12] to find a state independent optimal quantum cloning machine, which takes N identical input states and produces $M > N$ identical output states. It is optimal with regard to the fidelity

$$\mathcal{F} = \int \mathrm{d}\Omega \ \langle\psi|\rho_{\text{out}}|\psi\rangle \quad , \tag{19}$$

where ρ_{out} is the reduced density matrix of the output states and the input state is considered to be uniformly distributed over the the Poincaré sphere: $|\psi\rangle = \cos(\theta/2)|H\rangle + e^{i\phi}\sin(\theta/2)|V\rangle$. Therefore, the integration is carried out over the whole sphere $\mathrm{d}\Omega = \int_0^{2\pi}\mathrm{d}\phi \ \int_0^{\pi}\mathrm{d}\theta\sin\theta/4\pi$.
The fidelity is a measure for the overlap or distance between one of the input states with one of the output states and can be considered as the quality of the cloning process.
Gisin and Massar find a theoretical limit for the fidelity of creating M clones from N input states:

$$\mathcal{F}_{N,M} = \frac{M(N+1)+N}{M(N+2)} \tag{20}$$

From this equation, one can immediately see that trying to create two qubits from one original, the fidelity becomes $\mathcal{F}_{1,2} = 5/6$. The implications of this result on an eavesdropping attack will be mentioned in section 3.3.2.

3.3 BB84: A Simple Quantum Cryptography Protocol

In 1984, the first protocol for quantum cryptography was proposed by Charles Bennett and Gilles Brassard [13]. Though several more protocols have been invented, the so-called **BB84 protocol** is still the most popular one. It is easy to understand and can be physically realised using different implementations of the qubits.

3.3.1 Principle

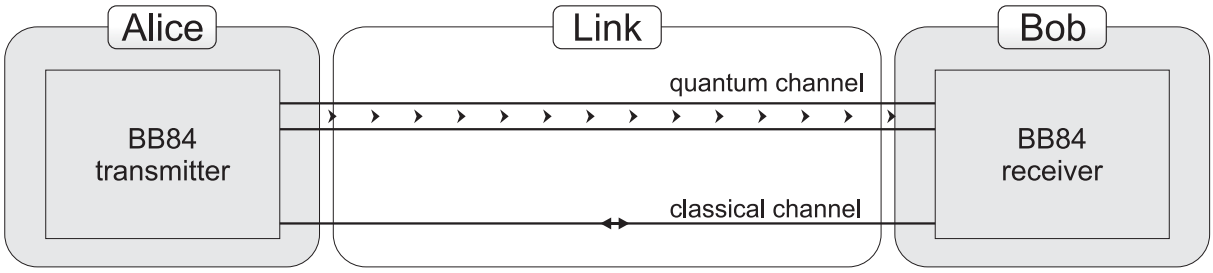


Figure 10: A BB84 quantum cryptography system: Alice has connected a BB84 transmitter to her end of the quantum channel, Bob needs a BB84 receiver. Both have access to an authentic classical channel, which can later also be used to transmit the encoded message.

During the following pages, the BB84 protocol with polarisation encoded photons will be discussed. Since this method will later be used in the experiment, a detailed explanation is given.

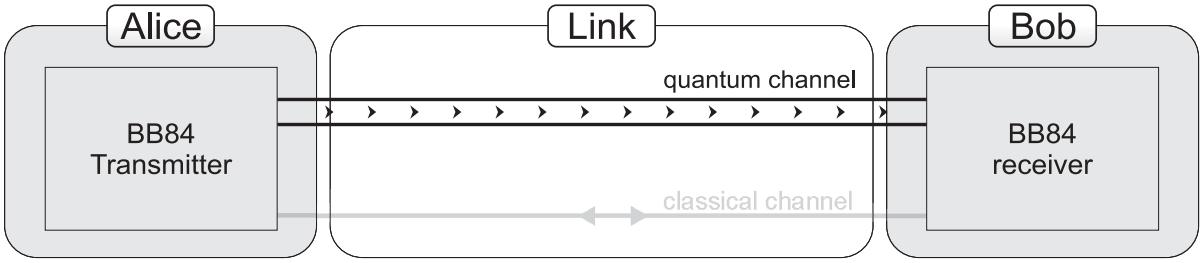
Random bit strings		Polarisation
b_m	d_m	
0	0	V
0	1	H
1	0	$+45°$
1	1	$-45°$

Table 2: The values of the random bit strings b and d are mapped to the polarisation of the photon stream in accordance with this table.

1. Alice chooses two equally long, independent random strings $b = b_1 b_2 \cdots b_M$ and $d = d_1 d_2 \cdots d_M$ with $b_m, d_m \in \{0, 1\}$, $m \in \{1, 2, \ldots, M\}$. For every $m \in \{1, 2, \ldots, M\}$, the following procedure is performed:

2. The value of (b_m, d_m) is mapped to basis and polarisation in that basis according to table 2. Alice prepares the photon in the chosen state and sends it to Bob.

3. Every time Bob expects a photon to come, he also chooses a basis $\{|H\rangle, |V\rangle\}$ or $\{|+\rangle, |-\rangle\}$ randomly, independent from Alice's choices. He then tries to measure the polarisation of the photon with respect to his chosen basis.



Alice

b	*d*	Basis	Pol.
1	1	+/-	+45
0	1	H/V	H
1	0	+/-	-45
0	0	H/V	V
0	1	H/V	H
1	0	+/-	-45
0	0	H/V	V
1	1	+/-	+45
1	0	+/-	-45
0	1	H/V	H
0	1	H/V	H
1	1	+/-	+45
0	0	H/V	V
1	1	+/-	+45
.	.	.	.
.	.	.	.
.	.	.	.
1	0	+/-	-45
0	0	H/V	V
1	1	+/-	+45
1	0	+/-	-45
0	0	H/V	V
0	1	H/V	H
1	1	+/-	+45
0	1	H/V	H
1	0	+/-	-45

① Alice choses random bit strings b and d

② Alice sends polarised photons to Bob →

③ Bob analyses polarisation of photons in randomly chosen basis

④ ← Bob tells Alice, which photons he has not detected. She deletes them from her list.

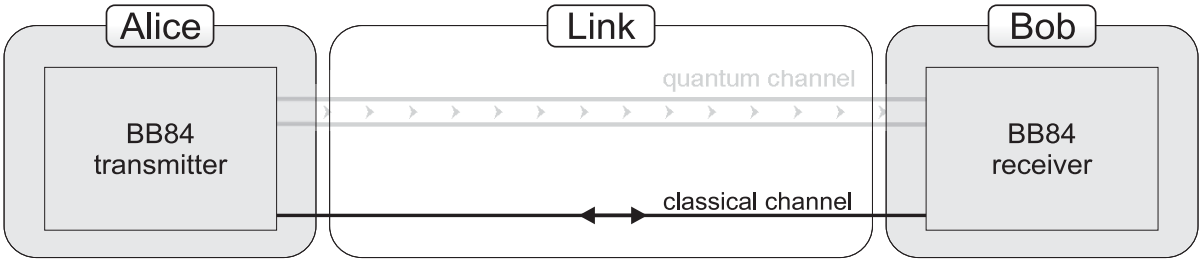
⑤ ↔ Both parties announce their bases publicly and only keep entries where they conicide.

Bob

Click	Basis	Pol.	s_B
x	+/-	+45	
x	+/-	+45	
x	H/V	H	
x	H/V	H	
x	H/V	H	
x	+/-	-45	
x	H/V	V	
.	.	.	
.	.	.	
.	.	.	
x	H/V	V	
x	H/V	H	
x	+/-	-45	
x	H/V	V	

4. Bob tells Alice, which photons he has detected. She discards every entry, where Bob did not see the photon. In any real system, the link will be lossy and the detectors will have an efficiency less than unity, hence not every sent photon will be detected by Bob.

   In theory, the total loss does not impose a problem on the security, but in real systems it can, depending on the actual implementation. This will be the topic of section 3.3.2.



Alice

b	*d*	Basis	Pol.
1	1	+/-	+45
0	1	H/V	H
1	0	+/-	-45
0	0	H/V	V
0	1	H/V	H
1	0	+/-	-45
0	0	H/V	V
1	1	+/-	+45
1	0	+/-	-45
0	1	H/V	H
0	1	H/V	H
1	1	+/-	+45
0	0	H/V	V
1	1	+/-	+45
.	.	.	.
.	.	.	.
.	.	.	.
1	0	+/-	-45
0	0	H/V	V
1	1	+/-	+45
1	0	+/-	-45
0	0	H/V	V
0	1	H/V	H
1	1	+/-	+45
0	1	H/V	H
1	0	+/-	-45

① Alice choses random bit strings b and d

② Alice sends polarised photons to Bob

③ Bob analyses polarisation of photons in randomly chosen basis

④ Bob tells Alice, which photons he has not detected. She deletes them from her list.

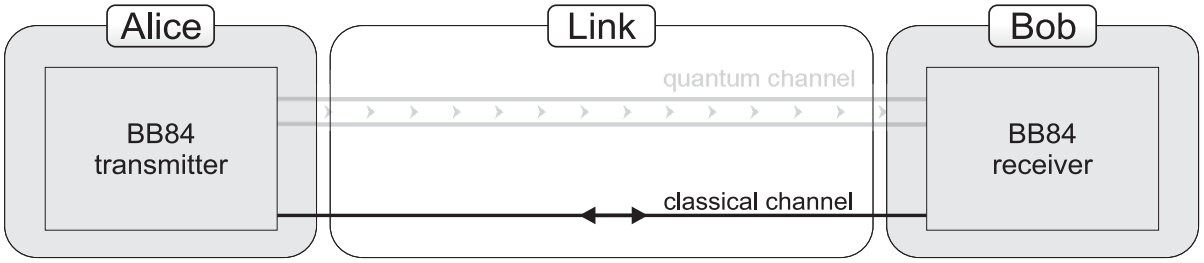
⑤ Both parties announce their bases publicly and only keep entries where they conicide.

Bob

Click	Basis	Pol.	s_B
x	+/-	+45	
x	+/-	+45	
x	H/V	H	
x	H/V	H	
x	H/V	H	
x	+/-	-45	
x	H/V	V	
.	.	.	
.	.	.	
.	.	.	
x	H/V	V	
x	H/V	H	
x	+/-	-45	
x	H/V	V	

5. The sifting procedure: Alice and Bob tell each other, when they used which bases. In those cases, where the bases coincide, both should ideally have the same values, if Bob maps the polarisation to a bit value as Alice has done. Both parties form a bit string out of the remaining entries, these strings are called the **sifted keys** s_A and s_B. (s_A is formed by the remaining entries of Alice's string d.)

   The red circle shows an error in Bob's sifted key s_B, which will have to be corrected in a later stage of the process.



Alice

b	*d*	Basis	Pol.
1	1	+/-	+45
0	1	H/V	H
1	0	+/-	-45
0	0	H/V	V
0	1	H/V	H
1	0	+/-	-45
0	0	H/V	V
1	1	+/-	+45
1	0	+/-	-45
0	1	H/V	H
0	1	H/V	H
1	1	+/-	+45
0	0	H/V	V
1	1	+/-	+45
.	.	.	.
.	.	.	.
.	.	.	.
1	0	+/-	-45
0	0	H/V	V
1	1	+/-	+45
1	0	+/-	-45
0	0	H/V	V
0	1	H/V	H
1	1	+/-	+45
0	1	H/V	H
1	0	+/-	-45

① Alice choses random bit strings b and d

② Alice sends polarised photons to Bob

③ Bob analyses polarisation of photons in randomly chosen basis

④ Bob tells Alice, which photons he has not detected. She deletes them from her list.

⑤ Both parties announce their bases publicly and only keep entries where they conicide.

Bob

Click	Basis	Pol.	s_B
x	+/-	+45	1
x	+/-	+45	0
x	H/V	H	1
x	H/V	H	
x	H/V	H	1
x	+/-	-45	
x	H/V	V	0
.	.	.	.
.	.	.	.
.	.	.	.
x	H/V	V	0
x	H/V	H	
x	H/V	H	
x	H/V	V	

6. Alice and Bob both hold a string now, which would ideally be equal. But they have to check whether there was an eavesdropper present. This can be determined by the error rate, i.e. the difference between Alice's and Bob's key. Alice and Bob can calculate the error rate (named quantum bit error rate, QBER) by comparing some randomly chosen bits. This is the great advantage of this protocol: Before the key is actually used to encrypt the message, it can be determined whether it is save to use or not, because the maximal amount of information an eavesdropper could have got can be calculated from the QBER. (More details will be given in section 3.3.2. Information on error correction is given in section 3.5.1.)

7. If the error rate is too high (values will be discussed in section 3.3.2), they will have to discard the key and try again. In case the error rate is tolerable, there are means to gain a secret, flawless key (see section 3.5) starting from the remaining key strings s_A and s_B, leaving them with a shared secret key string K_{final}. This can be used for classical symmetric crypto algorithms like the one-time pad (section 2.5) or DES (section 2.6.1).

3.3.2 Security

The novelty of this protocol and hence its huge advantage over classical ones is, that quantum mechanical principles allow sender and receiver to find out whether an eavesdropper was present or not. They can even calculate an upper bound of the amount of information an eavesdropper could have gained. The reasons for this are the principles introduced earlier in this chapter: The no-cloning theorem forbids to create a perfect copy of the photon. Eve cannot measure the polarisation of the photon precisely, since the used states are non-orthogonal. Moreover, Alice and Bob will be able to spot Eve trying to do that, because she will cause errors. Lo and Chau [14] presented a security proof for the principle of quantum key distribution, considering ideal systems.

Attacks

As already mentioned, no-go theorems are not enough. Alice and Bob need to have some criteria to determine, whether the key transmission was secure or not. One way to find those is to imagine eavesdropping strategies on the BB84 protocol in order to reveal security limits of the system. The spectrum of attacks ranges from the simple intercept-resend attack to more advanced methods like photon number splitting (PNS) attacks.

Intercept-Resend Attack

The easiest eavesdropping strategy one can think of is the so-called intercept-resend attack (figure 11). An eavesdropper simply interrupts the quantum channel, measures each

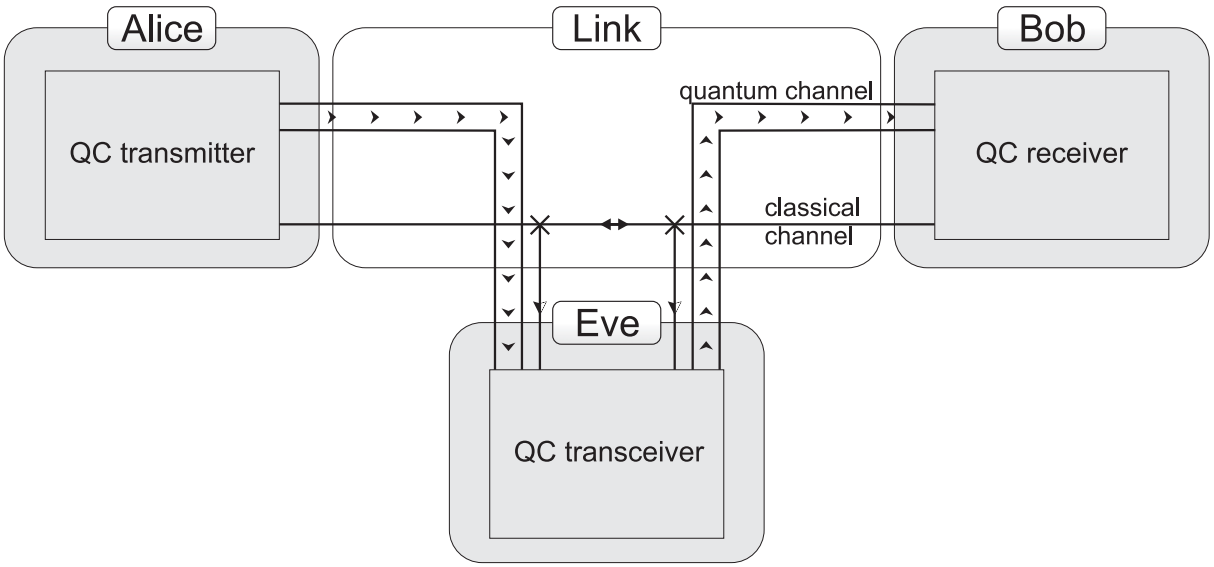


Figure 11: The intercept-resend attack: Eve tries to measure every qubit and sends out the state which corresponds to the outcome of her measurement.

incoming photon from Alice in a fixed or random basis[3] and afterwards sends the state which she has measured to Bob.

	Alice		Eve		Bob		Comment
	Basis	State	Basis	State	Basis	State	
1	H/V	H	?	?	+/-	?	discarded
2	H/V	H	H/V	H	H/V	H	Eve remains unrecognised
3	H/V	H	+/-	+	H/V	H	Eve remains unrecognised
4	H/V	H	+/-	+	H/V	V	Error hinting at eavesdropper

Table 3: Possible events in an intercept-resend attack. The "?" denotes that in that case it doesn't matter, which basis Eve chooses or what Bob's measurement outcome is.

Example: Alice sends an H polarised photon into the quantum channel. Eve intercepts the transmission and measures its polarisation fortunately for her in the H/V basis. If Bob decides to use the $+/-$ basis, this entry will be discarded in the sifting procedure anyway (table 3, case 1). In case Bob also chooses the H/V basis for his measurement, Alice, Eve and Bob will have the same information.

[3]It has also been considered that Eve might measure in an intermediate basis, e.g. the so-called Breidbart basis. In that case, Eve's chance to guess each bit correctly decreases, but her (very small) chance of guessing the entire key correctly is higher [9].

So, if they all by chance choose the same basis, Eve will gain full information of the key bit and will introduce no disturbance. But this will be different if Eve has chosen the wrong basis: Let Alice send an H polarised photon again and Bob later analyse it in the H/V basis. Eve has opted for the +/− basis, so her measurement outcome is purely random according to equation (15). The first thing to note is, that she doesn't gain any information as there is no correlation between her result obtained in the +/− bases and the qubit originally defined in the H/V basis. Now she wants to send the correct state to Bob. Since she doesn't know, whether she has measured in the correct basis or not, the best thing she can do is send out the polarisation, which was the result of her measurement. Let it be a +45° polarised photon.
Now, Bob analyses this photon in the H/V basis, so his result will be purely random, too. If he sees an H, he won't be able to tell that Eve has measured the qubit before. Yet, if his analysis shows that it had vertical polarisation, he will have a different value for the sifted key bit than Alice (figure 12).

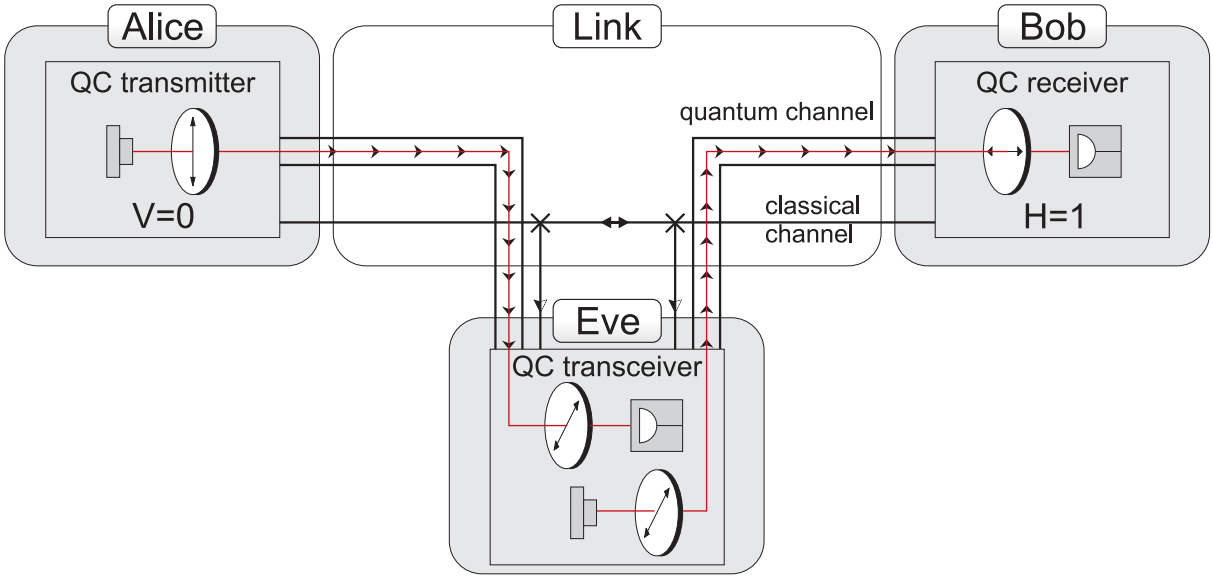


Figure 12: In the shown case, Eve introduces an error by measuring the polarisation in the wrong basis, causing Bob's measurement outcome to be random. Here, the result of his measurement contradicts the state Alice has sent.

The question is, how many errors will Eve induce, if she uses such a intercept-resend attack. This is rather simple. Only those cases have to be considered, where Alice and Bob choose the same basis. Now, Eve has a probability of 0.5 to measure in that basis. If she chooses the wrong one, Bob will see a wrong result in 50% of these events.

$\Longrightarrow$ **An intercept-resend attack on all qubit causes an error rate of $\epsilon_{\mathbf{ir}} = \mathbf{0.25}$.**

If Eve employs more advanced methods of measuring, like positive operator-valued measures (POVM), she can increase her gathered amount of information per introduced disturbance. This is beyond the scope of this work, but an analysis by Norbert Lütkenhaus can be found in [15]. A result is that the introduced error rate at which the key transmission is insecure, is reduced to $\epsilon_{\text{ir}}^{\text{POVM}} = 0.15$.

Quantum Cloning Attack

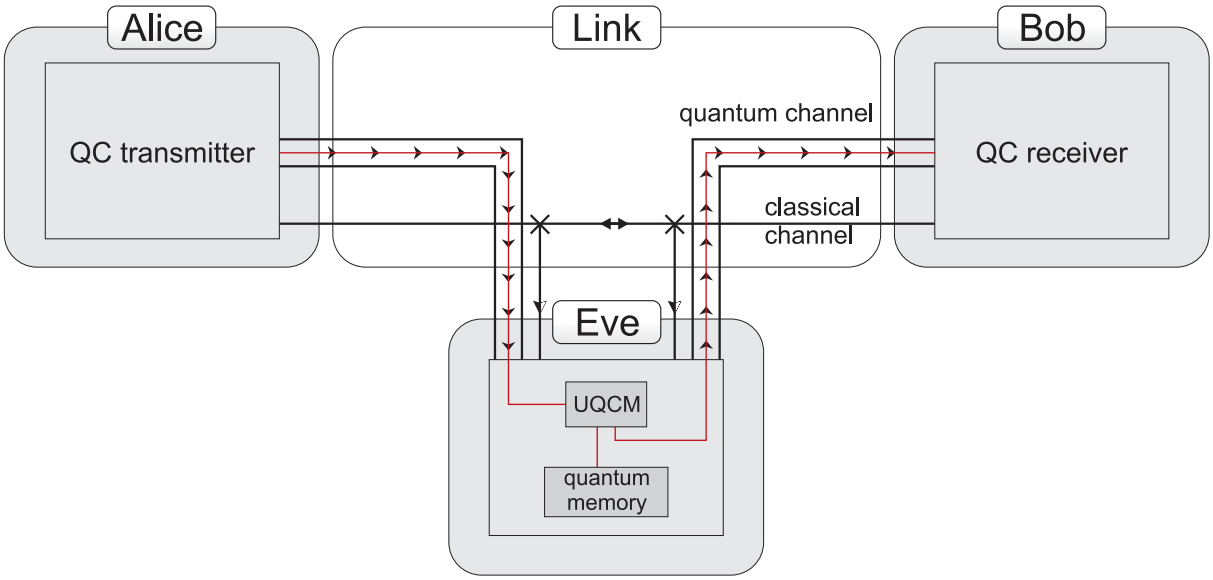


Figure 13: A quantum cloning attack: Eve uses a universal quantum cloning machine to "copy" Alice's qubit. She keeps one of the copies in her quantum memory and sends the other one to Bob. When Alice and Bob discuss their choice of the bases, she can measure her qubit in the correct basis.

A more sophisticated eavesdropping strategy tries to make use of quantum cloning machines. This method was proposed for eavesdropping purposes by Gisin and Huttner [16]. They suggested using either a machine that they named "pretty good quantum copying machine" (PGQCM) or the universal quantum cloning machine (UQCM) that has already been discussed in section 3.2.2.
The attack would look like this: Eve intercepts every photon, which Alice sends out and uses a cloning machine to end up with two photons. These have a certain fidelity $\mathcal{F}$ with respect to the photon, which Alice had sent. Eve keeps one of the photons in a so-called quantum memory and sends the other one to Bob. When the bases are announced during the sifting procedure, Eve can take her photons from the quantum memory and measure in the correct basis (see figure 13).

Of course, she will have introduced errors. The probability that Bob will see an incorrect bit value is $\epsilon_{\mathrm{QCA}} = 1-\mathcal{F}$. The fidelity of the PGQCM and the UQCM are $\mathcal{F}_{\mathrm{PGQCM}} \approx 0.825$ and $\mathcal{F}_{\mathrm{UQCM}} \overset{(20)}{=} 5/6 \approx 0.833$ respectively.

$\Longrightarrow$ **A quantum cloning attack with a universal quantum cloning machine introduces a QBER of $\epsilon_{\mathbf{QCA}} = 0.167$.**

The introduced error is lower than that of an intercept-resend strategy, but a universal quantum cloning machine is a difficult device and a quantum memory with a suitable capacity is also a problem. Eve's information on the key is also lower than in the intercept-resend attack. Nevertheless, if Alice and Bob want to be secure against such an attack, they should discard the key if the error is ϵ_{QCA}.

Optimal Attacks

Finally, optimal eavesdropping attacks have been studied [17], which lead to a limit of the error rate, at which a key transmission can no longer be assumed to be secure:

$\Longrightarrow$ **When optimal individual attacks are taken into account, the key exchange has to be regarded as insecure at a QBER of $\epsilon_{\mathbf{opt}} \geq 0.146$.**

The idea of this attack is that Eve lets a four-dimensional probe (i.e. two qubits) interact unitarily with the photon Alice has sent. She then waits until Alice and Bob announce the used basis, so that she can perform an optimised measurement on the stored probe, depending on the basis. A quantum circuit was proposed in [18], consisting of only two C-NOT gates.

In all previous considerations, experimental imperfections have not been accounted for. The next important eavesdropping strategy is not an attack against the fundamental BB84 protocol, but rather against the physical realisation with weak coherent pulses.

Photon Number Splitting Attack

Weak coherent pulses. The security of the BB84 scheme is based on the fact that single quantum particles are used to transmit information. Unfortunately, the existing single photon sources are not in a state where it seems practical to use them for quantum cryptography systems which are supposed to be close to an application. However, a lot of progress is made in this field and some groups have recently demonstrated quantum cryptography with real single photon sources [19, 20].

One way to bypass the problem of a missing practical single photon source is the use of weak coherent pulses instead of genuine single photon sources: The number of photons n in pulses of a pulsed laser beam is distributed according to Poissonian statistics (see e.g. [21]):

$$p(n) = \frac{\mu^n}{n!}\, e^{-\mu}\,, \qquad \text{with} \quad \mu := \langle n \rangle \qquad \text{(mean photon number)} \tag{21}$$

Here, $p(n)$ denotes the probability of finding n photons in a pulse of a coherent beam described by a mean photon number μ.

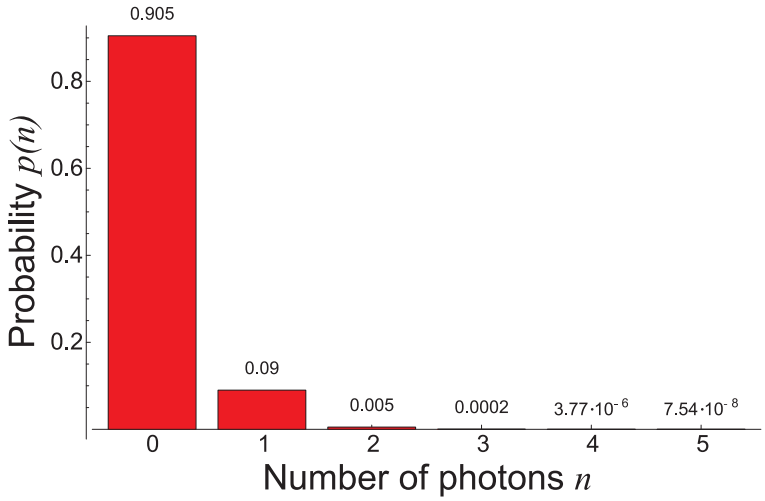


Figure 14: Poisson distribution for $\mu = 0.1$. It shows the probability that a pulse of a coherent beam contains n photons.

If weak coherent pulses are to be used in a protocol similar to BB84, it is vital to choose the mean photon number carefully, a popular value is $\mu = 0.1$. The implications of this method will be shown in the following paragraph. Details on how we produce a weak coherent beam with a defined mean photon number will be given in section 4.2.1.

Security risk. The fact, that there is a non-vanishing probability to have two or more photons in one pulse, gives rise to new eavesdropping strategies. The so-called photon number splitting attack (PNS attack, see figure 15) exploits this weakness in the following way: Eve is near Alice's end of the quantum channel and checks the number of photons in each pulse, without disturbing the polarisation, a so-called quantum non-demolition measurement (QND). Depending on the measured number of photons in the pulse, she takes one of the following actions:

- The pulses that contain no photons are not interesting to her.
- If there is exactly one photon in a pulse, she simply blocks it, so Bob doesn't get it.
- Whenever there are two or more photons in one pulse, Eve keeps one of them in her quantum memory to analyse it after the bases have been announced. She sends the remaining photon(s) of the pulse to Bob, causing no errors. Furthermore Eve is believed to be able to overcome the attenuation of the quantum channel by teleporting the qubit to Bob. This is especially important when the transmission of

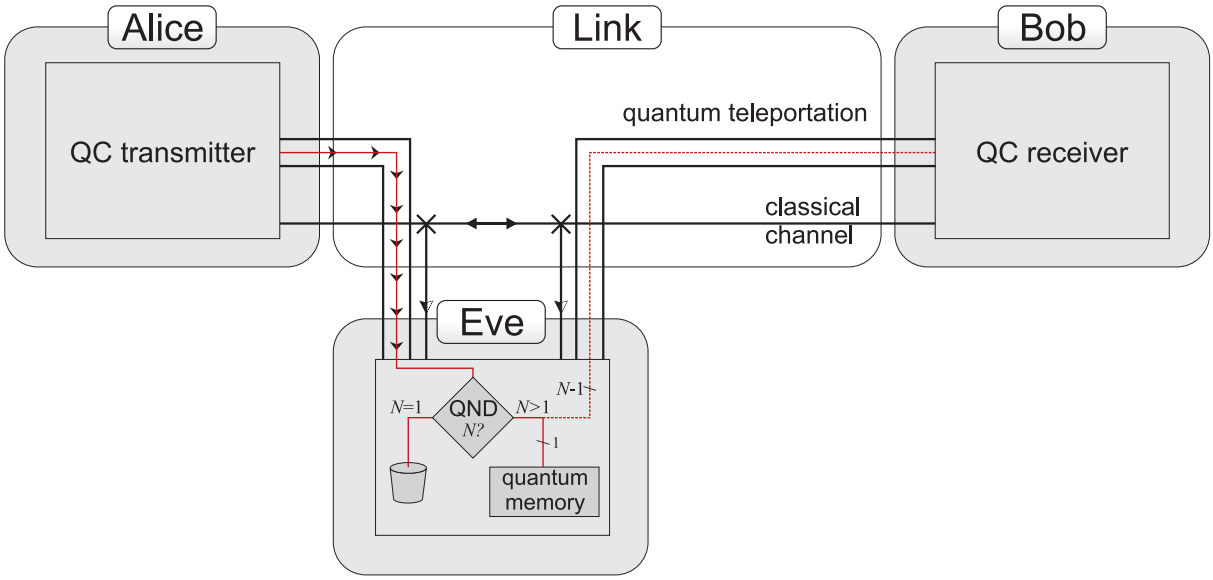


Figure 15: A photon number splitting attack: Eve performs a quantum non-demolition measurement (QND) to determine the number of photons in the pulse. In case it contains only one photon, she blocks it, but if there are more than one, she keeps one in her quantum memory and teleports the remaining ones to Bob.

a quantum channel is so low that it can be mimicked by Eve taking one photon out of each pulse and sending the remaining ones through a lossless channel.

This procedure has the following consequences: The eavesdropper doesn't cause any disturbance in the polarisation, so Bob cannot recognise him/her in the usual way. This is quite a severe problem, because especially when the secret key is distilled from the sifted key (this is called privacy amplification, see section 3.5), it is important to have a good estimate of the information Eve has gathered.
Still, it was shown in [22, 23] that the security of the BB84 can be proven for a realistic system, if certain restrictions for parameters are obeyed. One result is, that for a realistic transmission efficiency of the channel η_T and detector efficiency η_B, an optimal mean photon number

$$\mu_{\text{opt}} \approx \eta_B \eta_T \tag{22}$$

has to be used. This, however, is not valid for high loss situations, when errors and dark counts gain more importance. The security of realistic quantum cryptography solutions is also discussed in [24–26], taking into account experimental problems like imperfect sources and detectors.
So far, only individual attacks have been addressed, where all qubits are processed one after the other. Additionally, there also is a class of so-called collective attacks, but this is beyond the scope of this work.

3.4 Entangled State Quantum Cryptography

The BB84 is an example of single-quantum schemes, but there are also some protocols which use entangled multi-particle states to convey information. They usually are technically more challenging than weak coherent pulse experiments, but nevertheless introduce some properties which make them very interesting for specific applications.

3.4.1 Polarisation Entanglement

An entangled state cannot be written as a product of two single-qubit states:

$$|\psi\rangle_{1,2} \neq |\psi\rangle_1 \otimes |\psi\rangle_2 \tag{23}$$

Examples of maximally entangled states are the **Bell states**, which are described below, using the polarisation degree of freedom:

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_1|V\rangle_2 \pm |V\rangle_1|H\rangle_2\right) = \frac{1}{\sqrt{2}}\left(|HV\rangle \pm |VH\rangle\right) \tag{24a}$$

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2 \pm |V\rangle_1|V\rangle_2\right) = \frac{1}{\sqrt{2}}\left(|HH\rangle \pm |VV\rangle\right) \tag{24b}$$

These states can be produced in a process called spontaneous parametric down conversion (SPDC). It involves a nonlinear crystal (e.g. BBO) optically pumped by a laser, which in some configuration emits a polarisation-entangled photon-pair into two directions.

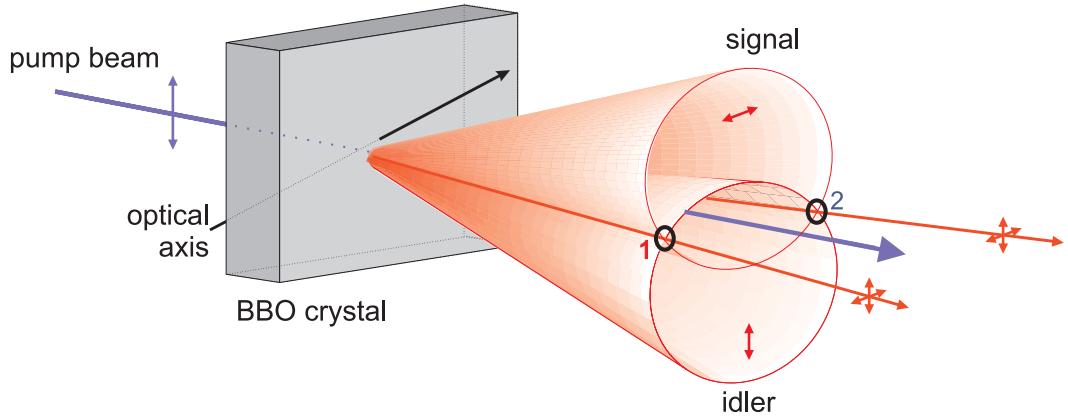


Figure 16: A spontaneous parametric down conversion source. The down-converted light is emitted into two cones, one is horizontally polarised, the other one vertically. If one picks up the photons at the intersection points 1 and 2 of the two cones, ideally every pair of emitted photons is maximally entangled.

3.4.2 Ekert or EPR Protocol

There is an astonishing property of entangled states, which was first predicted by Einstein, Podolsky and Rosen in their famous EPR paradox paper [27]: As soon as a measurement on the first particle has given a result, the state of the second particle is immediately known. This is an amazing effect, and it can be exploited as a resource of information for example in experiments like quantum teleportation, quantum cloning, quantum dense coding and quantum key distribution.

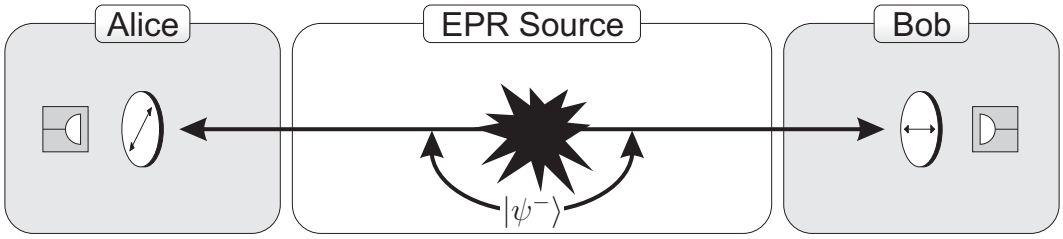


Figure 17: The configuration of the Ekert protocol. A source of entangled photons sends out pairs. One photon is directed towards Alice, the other one to Bob. They analyse the polarisation of their photon in randomly chosen bases.

The first quantum cryptography scheme using entanglement was proposed by Artur Ekert [28]: A source of entangled photon pairs is located between Alice and Bob, sending out entangled photon pairs in Bell state

$$|\psi^-\rangle = \frac{1}{\sqrt{2}} \left(|H_\mathrm{A} V_\mathrm{B}\rangle - |V_\mathrm{A} H_\mathrm{B}\rangle\right) = \frac{1}{\sqrt{2}} \left(|+_\mathrm{A} -_\mathrm{B}\rangle - |-_\mathrm{A} +_\mathrm{B}\rangle\right) \tag{25}$$

into opposite directions, A to Alice, B to Bob[4]. When Alice and Bob get their photon, they analyse its polarisation, again in a randomly and independently chosen basis (H/V or $+/-$).
Afterwards they tell each other, which bases they have used. They know, that in those cases, where they have chosen the same basis, they should have obtained completely correlated results, namely opposite ones. For example, if they have measured in the H/V basis and Alice's result indicates a horizontal polarisation, the wavefunction collapses into the product state $|H_\mathrm{A} V_\mathrm{B}\rangle$. She knows Bob must have measured V.
Using this method, they can distribute the key, but they still have to check for eavesdropping: For this purpose, they can use the events, in which they had chosen different bases. They announce the results of those measurements publicly, since they cannot be used for the key transmission, anyway. These numbers allow them to calculate, whether their experimental data violates the so-called Clauser-Horne-Shimony-Holt (CHSH) inequality [29]. This is an alternative form of Bell's inequality [30], who took up the idea

[4]This is also called singlet state, because in the spin 1/2-formalism it is the eigenstate of the S^2 operator with eigenvalue 0.

from the EPR paradox. The CHSH inequality gives a bound for classically correlated particles, which is maximally violated by quantum correlations in those cases of the Ekert protocol, where Alice and Bob measure in different bases.
Since these quantum correlations are the resource of information that is used to generate the key, Alice and Bob can be sure that no eavesdropper was present, by calculating the violation of the CHSH inequality.
The advantage of this protocol is that the source doesn't have to be trusted. Hence, one can dream about putting an EPR source on an untrusted satellite, enabling two distant parties on earth to establish a private key securely. The major drawback is, that EPR sources are much more complicated to operate than e.g. a weak coherent pulse source.

3.4.3 Other protocols

A different scheme based on entangled photon pairs was proposed by Bennett, Brassard and Mermin [31]. Although it employs the correlation of the maximally entangled state as a resource of information, it is equivalent to the BB84 protocol. It differs from the Ekert protocol in the way the presence of an eavesdropper is checked. Instead of calculating the CHSH inequality, the error rate of the sifted key is evaluated, as in the BB84.
Furthermore, there is a variety of different single-particle schemes, using more settings than the BB84 (e.g. the six-state protocol), less settings (B92) or Hilbert spaces of higher dimension [8]. They are in general more complicated. A fundamentally different approach is based on continuous quantum variables. In those schemes the information is coded into the position or momentum of so-called squeezed states, which means that the state was prepared either with well-defined position or with well-defined momentum [32]. The main advantage of continuous variable QKD is that high key transmission rates can be achieved. However, these protocols are very sensitive to losses, which limits their practical usability.

3.5 Error Correction and Privacy Amplification

The last section of the theoretical part will deal with the question, how a mutual and secret key can be produced from the two potentially different sifted key strings both parties have. These techniques are purely classical, but they are nevertheless vital for quantum cryptography.

3.5.1 Error Correction

In realistic setups, Alice's and Bob's sifted keys will not be perfectly correlated, whether or not an eavesdropper was present. What they have to do is to determine the error rate (QBER) and correct the errors, with as little information leaking out to an adversary as possible (this is called error correction or error reconciliation). Shannon's theorem says, that a minimum of bits have to be sent via the classical channel in order to be able to

correct the errors. Unfortunately, this theorem does not provide a solution how this can be done in such an optimal way. Brassard and Salvail have found a method, which is close to the optimum [33]. This method, called "`cascade`", can be briefly summarised as follows: Alice and Bob divide their sifted keys into blocks of a certain length. Then, they announce the parity of each of these blocks publicly. The parity is defined as the sum of all bits in that block modulo 2. If Alice's parity for a block differs from Bob's, they know that there must be an odd number of errors in that block. They search for these errors recursively, dividing the block into smaller ones, until only an even number (possibly 0) is contained in that block. When they have processed all blocks, they shuffle the bits and repeat the block parity procedure with a different block size, which can be optimised with respect to the required amount of conversation. This is done a number of times, so that the probability that the remaining key contains an error is very low. One major advantage of this method is, that the amount of information which leaks out to the public is close to the minimum.
This method is probabilistic, but the probability that they share an identical key string afterwards is close to unity.

3.5.2 Privacy Amplification

At this point, Alice and Bob share an identical key string $K_{\text{reconciled}}$, and they have evaluated the error rate of the sifted key ϵ_{sifted}. Furthermore they know, how much information might have slipped through to Eve during the error correction. They can calculate, how long the final key K_{final} may be. Now, Alice randomly picks one out of all hash functions that map a binary string of length $|K_{\text{reconciled}}|$ to a binary string of length $|K_{\text{final}}|$. She broadcasts this hash function to Bob, both of them apply the hash function to their reconciled key and end up with a private key which they can use to encrypt data and send it over the public channel.
A software package called QuCrypt, performing error correction on the basis of `cascade` and privacy amplification is described in [34] and can be downloaded via Internet.

4 Experiment

Contents

Some years after the proposal of the BB84 protocol, Bennett and co-workers successfully used it to distribute a key over a free space link [9]. The distance between Alice and Bob was less than half a meter, but nevertheless it was a feasibility proof of quantum cryptography. They used a pulsed green LED with a pinhole, an interference filter and a polariser to generate weak coherent pulses of polarised photons. The sender could rotate the polarisation of individual pulses with two Pockels cells. Alice and Bob were separated by about 32 cm of air. The receiver consisted of a further Pockels cell and a calcite Wollaston prism with a photomultiplier tube at each of the two outputs. The Wollaston prism was set so that it split the beam into a horizontally and vertically polarised part. The basis could be switched by applying a certain voltage at the Pockels cell.
Many more experiments followed this first one, some of them operating in free space (see section 4.3), others using optical fibres. While fibres have some advantages (e.g. for connections without a direct line of sight), they also bring along some problems like

stress induced birefringence and the need for wavelengths at which available detectors are less efficient. Because of this, fibre based and free space quantum cryptography have different possible applications. When no direct sight connection between two parties is available, perhaps a dedicated fibre could be used, but when a free space connection is possible, this might be the more convenient solution. Since fibres are generally not polarisation maintaining, different implementations of qubits have to be used. Successful key exchanges using fibres over distances of up to 67 km are reported in [35–37].
The following sections will be dealing with our effort of implementing a continuously working free space quantum cryptography system which might become the prototype of a commercial application in the near future. While this hasn't been completely demonstrated, progress has been made especially by automating the pointing alignment of the free space link and the synchronisation of sender and receiver.

4.1 Setup

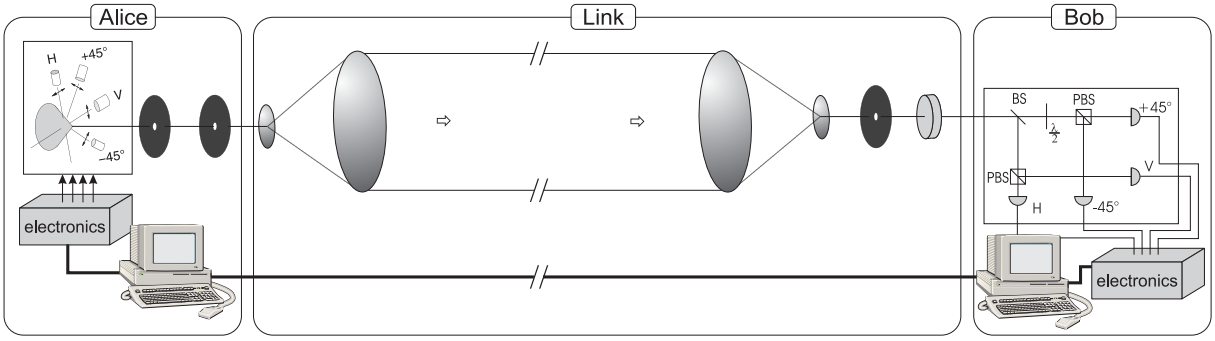
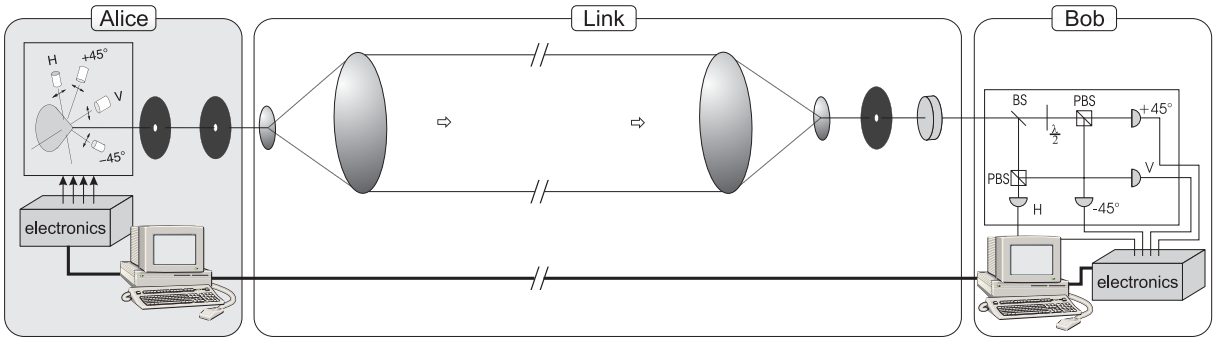


Figure 18: Sketch of the complete quantum cryptography system, divided into three parts: Sender unit (Alice), free space link and receiver unit (Bob).

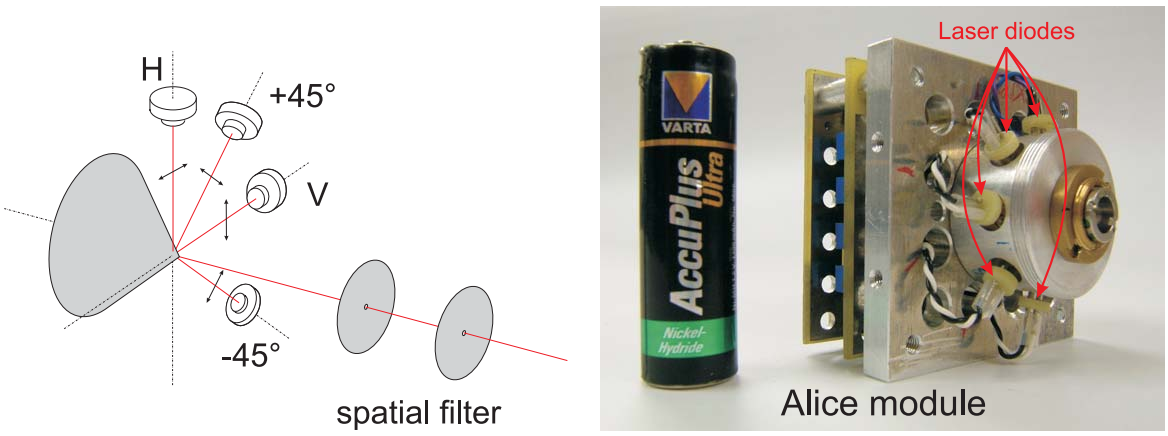
The complete setup can be divided into three parts (figure 18): The sender consists of the weak coherent pulse source, which sends out pulses of polarised light with a Poissonian distribution of mean photon number μ, and since the spatial filter contributes to this task, it is included here. The next part is the optical free space link which is formed by two telescopes and a spatial and a spectral filter on the receiver end. Finally, there is the receiver unit, which detects the single photons and analyses their polarisation. The three parts will be described in detail in the following sections.

4.2 Transmitter: Alice



4.2.1 Alice Module

The sender unit would ideally produce a stream of single polarised photons according to the choice of basis and bit value. Since currently no single photon source is competitive, we use weak coherent pulses with a mean photon number μ, which are produced as follows: Four laser diodes emitting at wavelength 850 nm, are arranged around a conical mirror (see figure 19) in such a way that the four beams are reflected and combined into one direction. The light of the laser diodes has a high intrinsic polarisation (better than 1:1000) and they are oriented so that there is one laser diode for sending out photons in each desired polarisation. The advantage of this method is that no active polarisation manipulations are needed. This makes the Alice module very small and cheap.
A fifth laser diode that is much brighter than the other four has been added to ease the alignment procedure. It is not used for the actual key exchange. After the beams have been reflected by the conical mirror, they have to pass a **spatial filter**, which consists of two 100 μm pinholes, 0.9 cm apart. It serves a vital purpose: Since the four beams are not combined perfectly on the conical mirror, it would still be possible to gather some information on the polarisation of a photon by measuring its direction or position. This is a serious security risk, so it has to be counteracted. The spatial filter is designed to let only one spatial mode pass through, so that the beams of the four laser diodes are indistinguishable with respect to the spatial degree of freedom. In order to get as much light as possible through the spatial filter, there is a lens with focal length $f = 2.75$ mm between the conical mirror and the pinholes, which focuses the beam between the two pinholes.
Because of the very strong spatial filtering, the alignment of the pinholes is crucial. If the alignment is not good enough, it won't be possible to achieve the desired mean photon number for all four polarisations.
When the spatial filter has been placed in an optimal position (using a small x-y translation stage), the mean photon numbers of all four beams have to be set to the required



(a) (b)

Figure 19: The Alice module: The beams of four laser diodes (one for each polarisation) are reflected by a conical mirror and overlapped into a spatial filter to ensure that no information on the polarisation of a photon can be gained by measuring its spatial mode.

value. We measured the mean photon number by collecting the photons on a calibrated single photon counter. At this wavelength, silicon avalanche photo diodes (SiAPDs) are commonly used and they are commercially available.
To get the desired value of μ, a potentiometer is used (see figure **??** in the appendix) to adjust the voltage levels at the laser diode. Whenever the diode is supposed to fire, the TTL signal at the input of the circuit is raised, resulting in an increase of the voltage level at the laser diode of 1 Volt. The potentiometer adjusts the offset level, so that the voltage at the laser diode is below the lasing threshold when the input signal is low and above the threshold when the input is high. Before, the input signal is combined with a reshaped clock signal by an AND gate. Thereby it is ensured that the photons will be sent out at a fixed repetition frequency. The duration of the pulse can be adjusted by a variable capacitor. Both, offset level and pulse duration of the voltage at the laser diodes can thus be set to fit the needs, i.e. to adjust the mean photon number μ behind the spatial filter.

4.2.2 Alice Driver Electronics and Software

As mentioned before, the Alice module has five important input channels, one clock channel and four TTL channels, determining which of the diodes is on or off during the next clock beat. These signals are produced by a different set of electronics, which

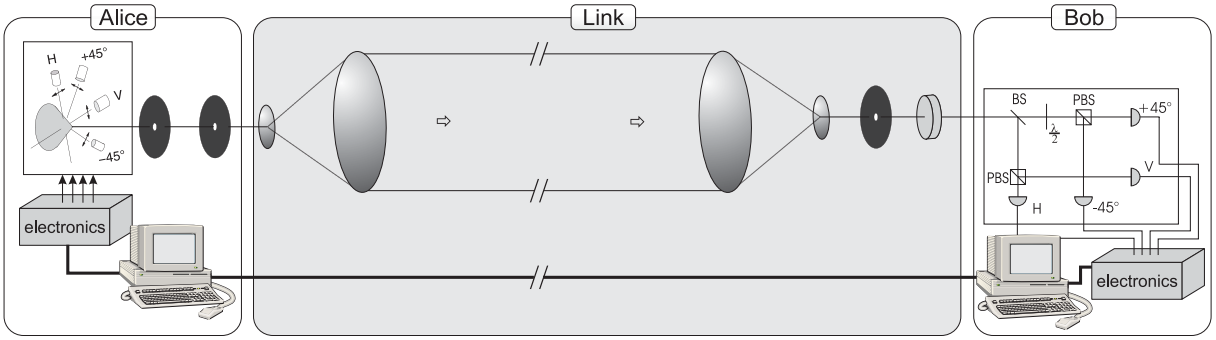
provides a 10 MHz clock signal and the four TTL signals depending on the output of a digital input/ output card (Nudaq PCI 7200) in Alice's computer. A FIFO (first in first out) memory on the electronics board is used to buffer the input to ensure that the correct laser diode is switched on at the respective clock pulse.
The digital I/O card itself is controlled by Alice's computer. The software reads in two strings of random bits b and d and translates these into the format needed by the card. Since Alice and Bob later need to talk about the same photons, some additional information has to be sent from Alice to Bob for synchronisation, as will be explained in more detail in section 4.4.2.

4.2.3 Generation of Random Numbers

Although it seems to be an easy task, the generation of truly random numbers has been a hardly solvable problem for decades. Computers[5] can only calculate so-called **pseudo-random numbers**, generated by a deterministic algorithm iteratively producing a bit stream from some initial starting parameter called "seed". Yet, once the seed is known to an adversary, the strings b and d can immediately be computed by the eavesdropper and the security of quantum cryptography is lost.
In order not to compromise the high security level of quantum cryptography, real random number generators are needed, which have to be based on well-known statistical processes with easily verifiable parameters, like the radiative decay of a nucleus. An optical method is described in [38], using an LED that shines onto a 50/50 beam splitter with a photo-multiplier tube at each of its outputs. The signals of both detectors are connected to a set/reset flipflop, one to the set and the other one to the reset input. Thus, the state of the flipflop depends on the truly random process, whether a photon was transmitted or reflected by the beam splitter. A quantum random number generator based on this principle is already commercially available [39].

[5] Although the behaviour of computers often seems to be completely unpredictable, in theory they work absolutely deterministic. Hence they cannot produce random numbers on their own.

4.3 Quantum Channel: Optical Free-space Link



When the stream of polarised photons is being sent out by Alice, it has to be assured that they arrive at Bob's detector with as little disturbance as possible along the way. As already mentioned, optical fibres are not a good medium in this respect, but free space links are a good alternative. Their further advantages are that they do not impose severe restrictions on the used wavelength, so that it can be chosen to allow for the use of practical detectors and minimal absorption in air. Moreover, free space links could one day be used to build a global quantum key exchange system based on the communication with satellites.

There have already been some free space experiments over relatively large distances, for example a 10 km link in the group of Richard Hughes [40] and a 23 km link from Karwendelspitze to Zugspitze in this group in collaboration with the group of John Rarity [41]. The experience which was gathered during this experiment was a good starting point for building a stable quantum cryptography system for urban areas.

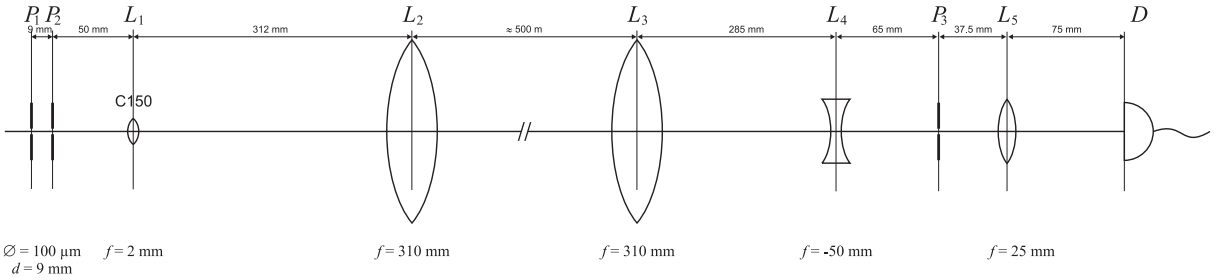
4.3.1 Telescopes and Tables

The principle of an optical free space link is simple: A direct line of sight between sender and receiver is needed and some kind of optical equipment to enable Bob to collect as many photons from Alice as possible. Furthermore, if the whole system is supposed to work during daylight, measures have to be taken to suppress stray light, because it will otherwise raise the error rate or even saturate the single photon counters.

The free space link can be optimised in this respect using different methods. One idea is to keep Bob's field of view as small as possible, so that only light from Alice's direction will enter his detectors. This is called spatial filtering. The next possibility is to look only at wavelengths, which are close to the one Alice sends out. This method is known as spectral filtering. Bob will do some more filtering on the software level based on the synchronisation information, which will be described in section 4.4.2.

Telescopes

To ensure that as many photons from Alice as possible are detected by Bob, two telescopes are employed, one at each end. Both telescopes have the same front lens ($f = 310$ mm, open aperture $a = 75$ mm), but the rest of the system is chosen to match the different requirements of sender and receiver.

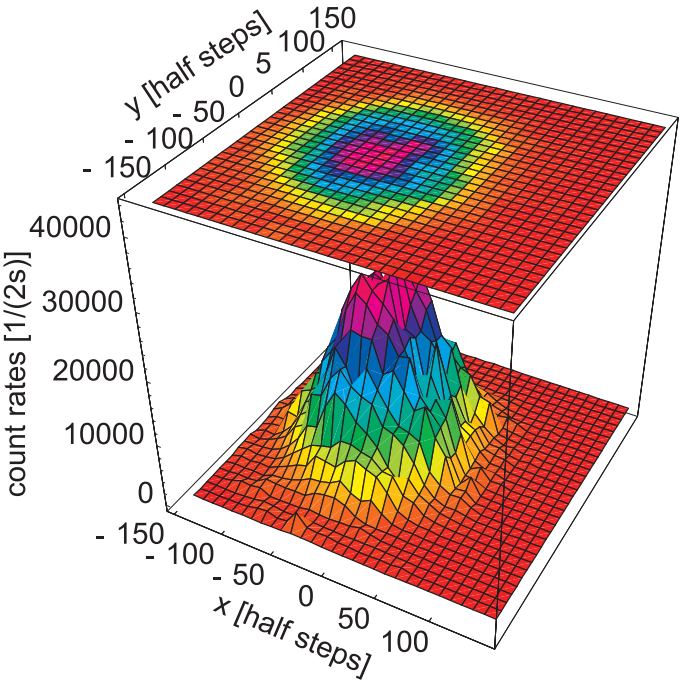


On the sender side, the two pinholes forming the spatial filter define the initial beam parameters. The focus of the beam is at the centre of the spatial filter with a measured minimal waist of $w_0 = 52$ μm. Lens L_1 is needed to adapt the small divergence angle of the beam to the numerical aperture of L_2 via an intermediate focus at the focal point of the latter. The beam is then focused at the centre between lenses L_2 and L_3 with a calculated minimal waist $w_0 = 1.55$ mm. L_4 is used to make the numerical aperture of L_3 fit with the 100 μm pinhole P_3. P_3 is intended to narrow Bob's field of view, so that as little stray light as possible is collected (spatial filtering). Its position was adjusted to maximise the transmission, which should mean that it is in the focal plane of the lens system L_3 and L_4. The function of the remaining lens L_5 is to image P_3 onto Bob's detector. All lenses are anti-reflex coated for 850 nm wavelength.

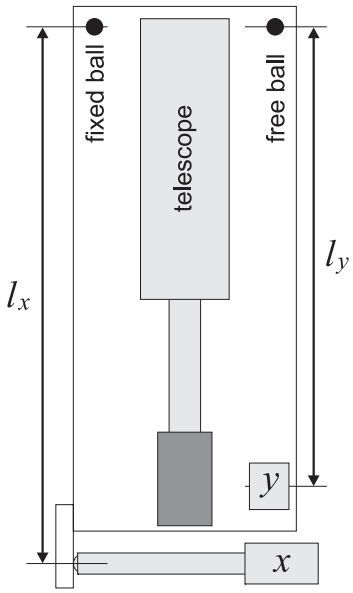
Tip-Tilt Stages

Because of their narrow field of view (the receiver sees a region of approximately 14 cm $\times$ 17 cm at a distance of 500 m, see figure 20(a)), the orientation of the telescopes has to be aligned very precisely. Thus, stable mounts are necessary which permit the required pointing accuracy. For reasons described below, each tip-tilt stage is equipped with two stepper motors, which drive micrometer screws to adjust the two possible angles (see table 4 and figure 20(b) for more details).

Figure 20:



(a) Intensity profile obtained by scanning the orientation of the receiver looking at the static sender.



(b) Sketch of the tip-tilt stage on the receiver side. The one on the sender side is similar.

	Alice	Bob
Leverage in x direction: l_x	270 mm	543 mm
Leverage in y direction: l_y	270 mm	445 mm
Stepper motor: half steps per revolution	400	400
Micrometer screw: travel per revolution	0.5 mm	0.5 mm
Travel per half step:	1.25 μm	1.25 μm
Angular displacement x per half step:	$4.6 \cdot 10^{-3}$ mrad	$2.3 \cdot 10^{-3}$ mrad
Angular displacement y per half step:	$4.6 \cdot 10^{-3}$ mrad	$2.8 \cdot 10^{-3}$ mrad

Table 4: Technical data of the tip-tilt stages and their additional components.

Figure 21: Alice and Bob on the roof tops.

4.3.2 Location

This experiment takes place in downtown Munich, sender and receiver are located on the roof tops of two buildings (figure 22) belonging to the university. There are no solid obstacles obstructing the line of sight, so that most of the time the transmission is relatively high. However, there are two chimneys (marked with 1 and 2 in the figure 22), which blow smoke into the link under certain wind conditions, causing the transmission to drop drastically.

Figure 22: A map of the location. Alice and Bob are both located on the roof tops of university buildings.

4.3.3 Transmission Measurements Without Alignment

The first idea was to build the system with all constituent parts as passively stable as possible, in order to make the whole setup easier to maintain. Aligned once, it would have remained operational without anybody touching it afterwards. A transmission measurement was set up, using a red laser diode instead of the Alice module and a photo diode behind Bob's telescope, measuring the intensity of the transmitted light. Alice and Bob were aligned to maximal transmission and fixed at that position. The analysis of the acquired data showed that probably thermal expansion of the equipment and/or the buildings caused substantial misalignment of the telescopes on the timescale of some hours. One can easily identify a period of roughly 24 hours of the transmitted signal (figure 23) with a slightly decreasing envelope height.

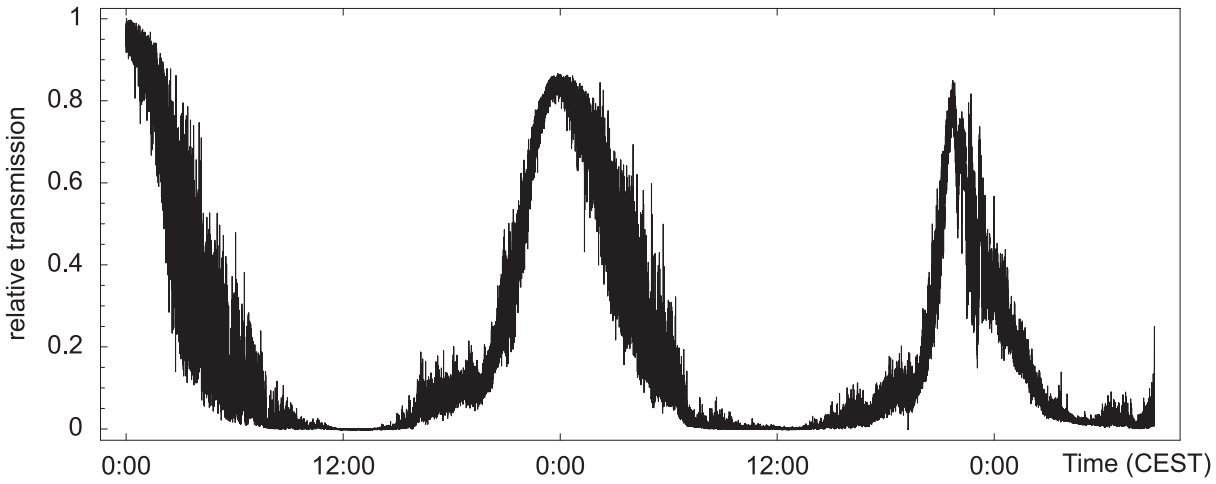


Figure 23: A transmission measurement at the test location without the alignment control mechanism. An approximately 24 hour period can be identified which leads to the conjecture, that the misalignment is caused by thermal expansion of equipment and/or buildings.

4.3.4 Automatic Alignment Control

To solve this problem, an active pointing control mechanism for both tip-tilt stages was designed, which controls the previously mentioned stepper motors.
In order to keep the hardware complexity as low as possible, the actual signal itself is used to control the alignment. The extra advantage of this is, that we do not have to align additional equipment with our telescopes, possibly leading to further problems. The disadvantage of this method is that some fraction of the signal will be lost, because it is constantly tested how countrates behave in different directions. This loss contribution will

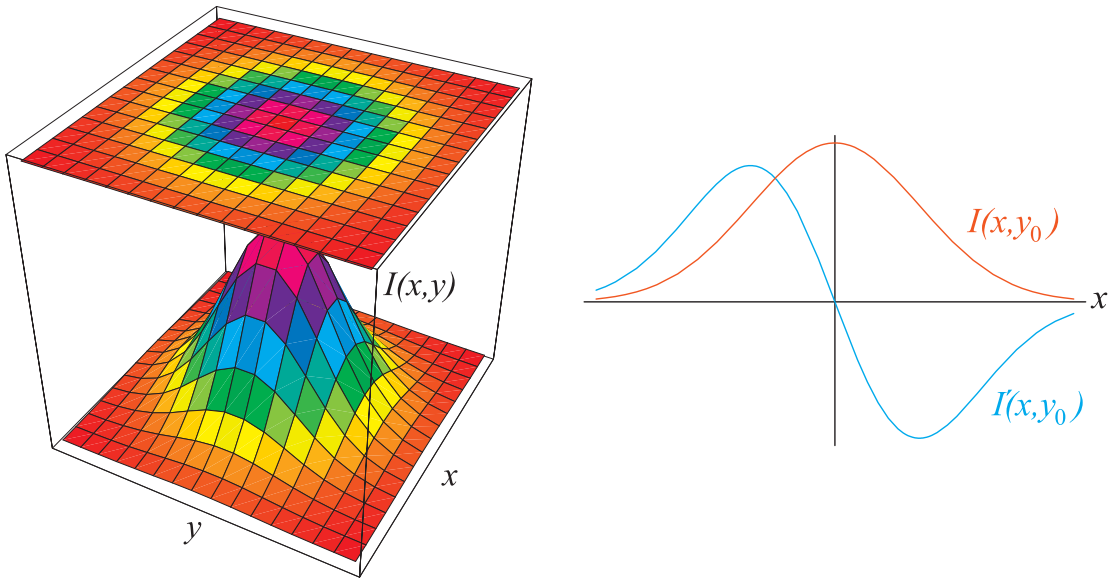


Figure 24: For a Gaussian intensity profile, the first partial derivative gives a measure, how far off the maximum is as long as one is inside the inflection points.

be on the order of a few percent, which could be compensated by increasing the repetition rate, with which Alice sends out the photons (not the mean photon number).

Principle

The idea behind the tracking algorithm is this: Suppose the sender is static and the receiver wants to find the pointing direction, where he sees the maximum intensity. When Bob scans the intensity profile in the x-y-plane (where x and y mean angular displacement in two orthogonal directions), the result shall be denoted $I(x, y)$. The peak intensity should be at $(0, 0)$ and Bob's current position is (x_0, y_0).
The Taylor expansion of $I(x, y)$ is:

$$I(x,y) = I(x_0,y_0) + \left.\frac{\partial I}{\partial x}\right|_{x_0,y_0} (x - x_0) + \left.\frac{\partial I}{\partial y}\right|_{x_0,y_0} (y - y_0) + \dots \tag{26}$$

If Bob moves around in a circle with origin (x_0, y_0) and radius r at a frequency ω_c, which means that $x = x(t) = x_0 + r\cos(\omega_c t)$ and $y = y(t) = y_0 + r\sin(\omega_c t)$, equation (26) can be expressed as[6]

$$I(x,y;t) = I(x(t),y(t)) = I(x_0,y_0) + \left.\frac{\partial I}{\partial x}\right|_{x_0,y_0} \cdot r\cos(\omega_c t) + \left.\frac{\partial I}{\partial y}\right|_{x_0,y_0} \cdot r\sin(\omega_c t) \tag{27}$$

[6]I will only use the terms up to first order. The second order does not give a contribution at that specific frequency, but the third and generally the odd orders will, but I will neglect them.

To get an indication where Bob should move to, one needs to know the first partial derivatives with respect to x and y. The direction, in which Bob should move can be concluded from this and depending on the shape of the intensity profile, it can also give a clue, how far off he is. In this special case it can be assumed to be Gaussian, so that the first partial derivative implies, how far Bob is off, as long as it is inside the inflection points (see figure 24). The important values are the coefficients of terms with frequency ω_c. This coefficient can be obtained by shifting all frequency components to the left and reading out the slowly varying part, which works like this:
If a function $f(t)$ is multiplied by an exponential function with frequency ω_0, then the whole frequency spectrum of f is shifted to the right by ω_0. This can easily be seen from the fourier transform $F(\omega)$ of $f(t)$:

$$F(\omega) = \int e^{-\imath\omega t} f(t)\,\mathrm{d}t \quad \overset{g(t)=e^{\imath\omega_0 t} f(t)}{\Longrightarrow} \quad G(\omega) = \int e^{-\imath(\omega-\omega_0)t} f(t)\,\mathrm{d}t = F(\omega-\omega_0) \tag{28}$$

In the special case of $I(x, y; t)$, only the $\cos(\omega_c t)$ and $\sin(\omega_c t)$ parts of equation (27) are important. Here, instead of multiplying with $e^{\imath\omega_c t}$, the factors $\cos(\omega_c t)$ and $\sin(\omega_c t)$ yield the desired result, keeping the calculation real:

$$\begin{aligned} I(x,y;t)\cdot\cos(\omega_c t) &= I(x_0,y_0)\cos(\omega_c t) \\ &\quad + \left.\frac{\partial I}{\partial x}\right|_{x_0,y_0} \cdot \frac{r}{2}\left(1+\cos(2\omega_c t)\right) + \left.\frac{\partial I}{\partial y}\right|_{x_0,y_0} \cdot \frac{r}{2}\sin(2\omega_c t) \end{aligned} \tag{29}$$

The constant term is proportional to the first derivative with respect to x, which predicts, where the maximum can be found. By applying a digital low pass filter, the constant part can be separated from higher frequency contributions.
Since the partial derivative in y direction is equally interesting, this has to be calculated by multiplying $I(x, y; t)$ with $\sin(\omega_c t)$:

$$\begin{aligned} I(x,y;t)\cdot\sin(\omega_c t) &= I(x_0,y_0)\sin(\omega_c t) \\ &\quad + \left.\frac{\partial I}{\partial x}\right|_{x_0,y_0} \cdot \frac{r}{2}\sin(2\omega_c t) + \left.\frac{\partial I}{\partial y}\right|_{x_0,y_0} \cdot \frac{r}{2}\left(1-\cos(2\omega_c t)\right) \end{aligned} \tag{30}$$

To summarise, what needs to be done is to change the pointing of the receiver with time so that it performs circles with frequency ω_c. The received signal has to be mixed down with $\cos(\omega_c t)$ and $\sin(\omega_c t)$ and passed through a low-pass filter to obtain correction values for x and y of Bob, as in figure 25.
The low-pass filter is implemented as an integrator like this:

$$I^{\text{new}}_{\text{filtered}} = I^{\text{previous}}_{\text{filtered}} + a^{\text{filter}} \cdot I_{\text{measured}} \tag{31}$$

The constant a^{filter} defines the gain of the loop and has to be optimised with respect to the time constant of the disturbance and the level of intensity.

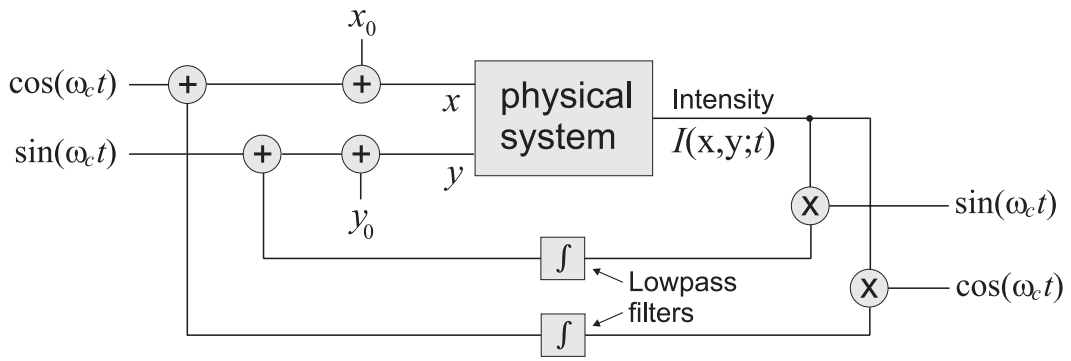


Figure 25: Pointing alignment scheme for one party. The signal is a result of the modulation with ω_c, gets mixed down with ω_c and is passed through a low pass filter (integrator). The outcome is added to the offset and should ideally compensate it completely after some time.

Since not only the receiver might lose its track, the sender needs to be realigned, too. Thus the same has to be done with Alice's telescope, using a different frequency. As long as the frequencies are kept separated during the mixing and filtering processes, the two loops do not disturb each other. Both frequencies should be chosen to be not too close to each other and one should not be an integer multiple of the other, since in that case, higher order contributions can not be neglected anymore.
The principle is very similar to the lock-in amplification technique, where a small signal that would be indistinguishable from noise, is modulated with a certain frequency to enable filtering of only this frequency component afterwards. This modulation has to be applied at the source of the signal and not after the detection. For example, this technique is used in laser spectroscopy, when an exciting laser beam is chopped to modulate the fluorescence of atoms or ions.

Algorithm

The tracking mechanism is controlled by the computer on the receiver side and works as follows:

1. Start values like radii of the circles, their frequencies and filter constants are set.

2. According to the current position, radii and frequencies, the next step on the circle is calculated for Alice and Bob, respectively.

3. Both parties adjust the pointing direction of their telescopes to the calculated values.

4. Bob measures the intensity I_{measured} at the current position.

5. Bob multiplies this measured intensity with cosine and sine terms of their respective frequencies and puts these into the four filters (one for each direction at Alice's and Bob's side).

6. In case a circle (on Alice's or Bob's side) is completed, a new centre of this circle is calculated by adding the corresponding filter outputs to the previous values (see figure 25). If the circle is not completed, this step is skipped.

7. Go to step 2.

A further refinement has been added to minimise the loss due to the tracking routine resulting from the following situation: When both parties have found the correct pointing direction, both telescopes will perform circles around the maximum. If the radii are big, this will lead to considerable loss. On the other hand, as long as the maximum position has not been reached, bigger radii accelerate the procedure.
Hence, a routine has been implemented, which adjusts the radius according to a comparison of the current intensity and the average intensity over a fixed number of previous steps. If the difference is small, so will be the radii of the circles and vice versa. A threshold has also been implemented so that the radii are not decreased when the current intensity as well as the average intensity are very low. Additionally, a lower limit prevents the circles from becoming smaller than the resolution of the stepper motors allows.

Simulation

To rule out general mistakes and to test some parameter settings, simulations of the implementation of the tracking algorithm have been carried out. The input intensity was modelled by the product of two Gaussian functions at the specific positions, meaning that if Alice's current position is (x_A, y_A) and Bob's is (x_B, y_B), the intensity will be calculated as

$$I(x_A, y_A, x_B, y_B) = e^{-\frac{(x_A - x_{A0})^2 + (y_A - y_{A0})^2}{2w_A^2}} \cdot e^{-\frac{(x_B + x_{B0})^2 + (y_B + y_{B0})^2}{2w_B^2}} \quad . \tag{32}$$

At the start of the simulation, $(x_A, y_A) = (x_B, y_B) = 0$, but the position of the maximum is (x_{A0}, y_{A0}) and (x_{B0}, y_{B0}), respectively. The task of the procedure is to set $(x_A, y_A) = (-x_{A0}, -y_{A0})$ and $(x_B, y_B) = (-x_{B0}, -y_{B0})$ to maximise the intensity.
The simulation (figure 26) shows a case without noise, but with a quantisation of the positions, i.e. a motor can only be driven in integer steps. At first, the radii of Alice's and Bob's circles are kept maximal until the moving average filters, which are responsible for the radius adjustment, are both filled. As soon as this happens, the intensity increases.

Transmission measurements

The algorithm seemed to work as desired, so that it could be tested under genuine conditions. To simplify matters, the transmission was not measured on the single photon level

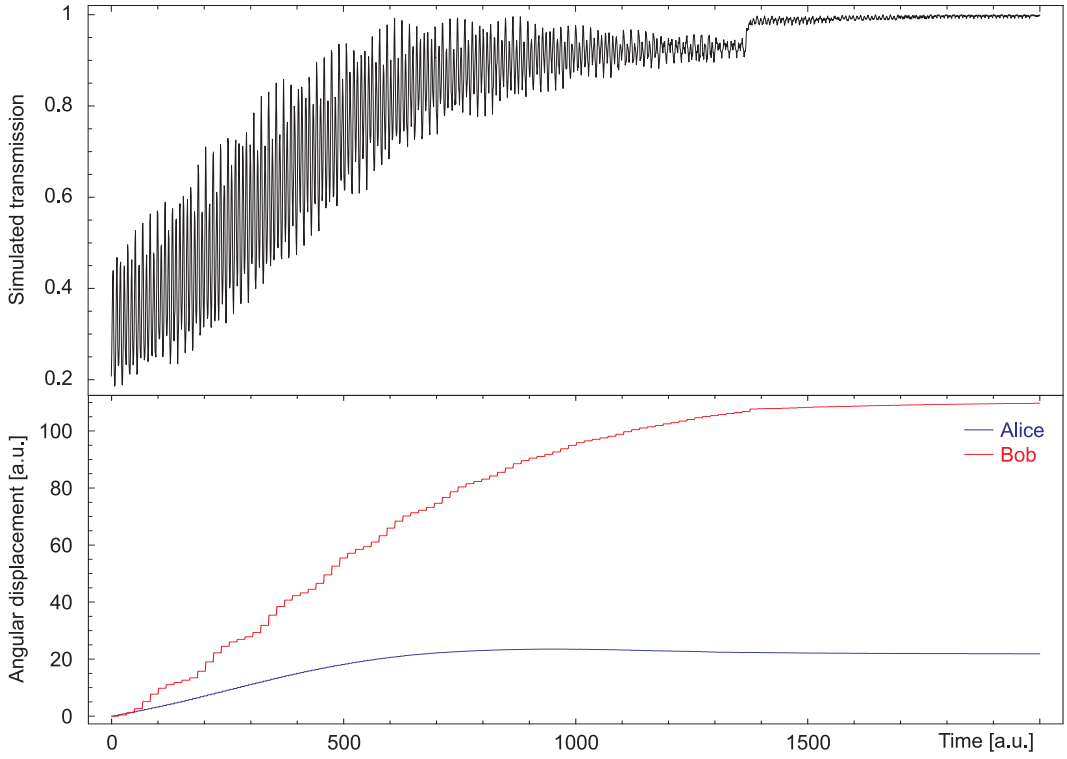


Figure 26: Simulation of the tracking procedure. Relative intensity (black) and angular adjustment versus sampling events. To prevent the radii from being decreased too soon, they are kept maximal until enough samples have been taken.

but with a 660 nm cw laser diode (coupled into the telescopes coming from an optical fibre for spatial mode cleaning) to mimic the sender and an ordinary photo diode attached to the receiver telescope (see figure 29). Since the performance of the self-aligning link should not depend on the absolute rate of photons, such a test yields a significant evaluation.

Figure 27 shows a result of one of those measurements. The black curve represents the relative transmission from Alice to Bob normalised to the maximum of the occurring values. First, the alignment was optimised by the automatic control mechanism, which can be seen by the increase in the transmission and in the angular displacement (lower part). The latter is the absolute value of the pointing direction with respect to the position at which the program was started.

When a maximal transmission was reached, the control mechanism was turned off, so that the pointing direction stayed constant. It kept being turned off for roughly one day and again a periodicity of approximately 24 hours can be identified. Before the signal was completely lost, the automatic alignment control was switched on again. After that, the transmission didn't drop nearly as much as before, but nevertheless it was far from being constant. The reasons for that are not easy to track, because outside of the lab, it

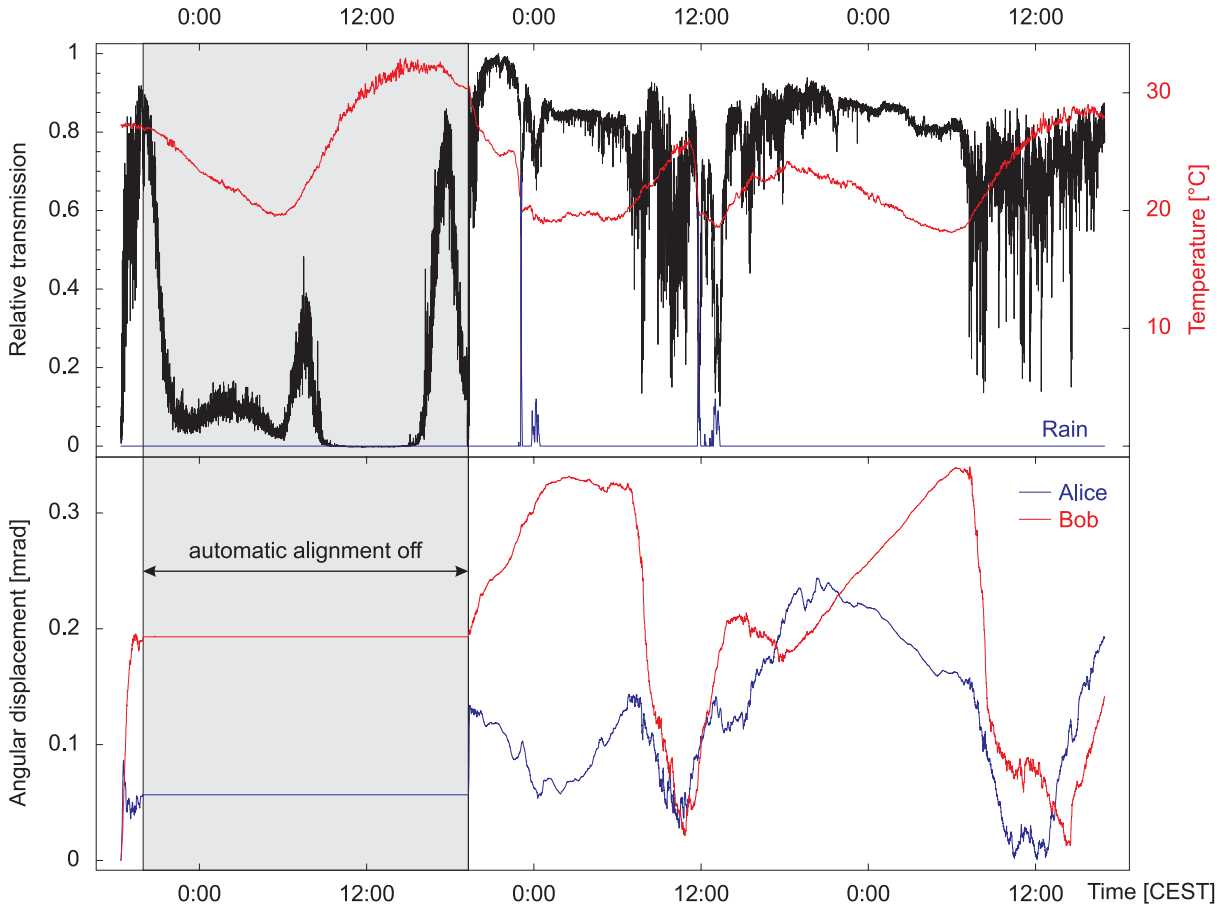


Figure 27: Relative transmission measurement with and without automatic alignment control.

is difficult to isolate the different possible causes. It can only be assumed why there are phases with lots of noise and less transmission and these assumptions can be tested by the analysis of additional data. Some possible reasons will be discussed in the following paragraphs.

Since the above-mentioned measurement is one of the rare ones showing quite heavy rain (upper blue line), it can be mentioned that rain does effect the transmission. Yet, a simple correlation between the intensity of the rain and the loss in transmission was not obvious. It can be stated that rain and snow can completely inhibit the transmission, but those events seemed to appear only rarely. Because of the very dry summer, when most of the transmission measurements were carried out, more details about the effects of rain could not be obtained.

To estimate the maximal key distribution rate, relative transmission values are not sufficient. Therefore, some effort was made to get some absolute values of the transmission between Alice and Bob. Figure 28 shows the result of such a measurement run with a

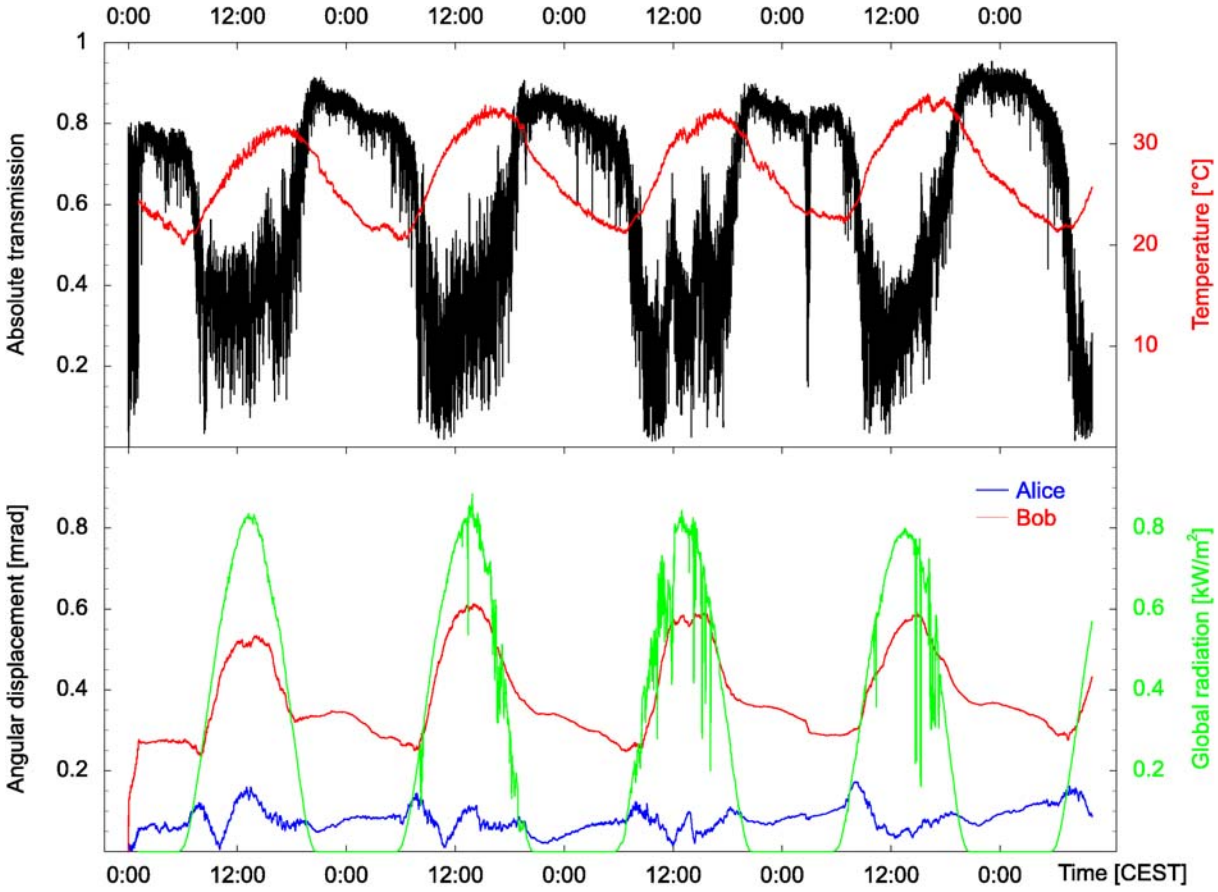


Figure 28: Absolute transmission measurement with automatic alignment control enabled. The photocurrent on the receiver side was normalised to the output at the transmitter side.

slightly extended setup: To measure the output of the receiver, a specifically coated thin glass plate (front: high reflectivity at a wavelength of 660 nm; back: broadband anti-reflex, both at an angle of 45°), was inserted between the end of the fibre and the front lens of the telescope in such a way that a fraction of 3% of the intensity at the output of the telescope was reflected onto a photodiode. The photocurrent measured there was used as the reference signal for the photocurrent at the receiver side.

The measurement shows that a peak transmission of 90% over a distance of 500 meters is possible, a value that is supported by a manual measurement which yielded 88.3% absolute transmission, including the loss of all optical kit on the receiver side. Obviously, the average transmission is considerably less and the conditions were rather good, as the weather was very dry and sunny, with absolutely no rain. An estimation of the raw key rate can be calculated if the transmission is assumed to be e.g. 40%, a mean photon number of $\mu = 0.1$ and a pulse repetition rate of 10 MHz are used: The sifted key rate

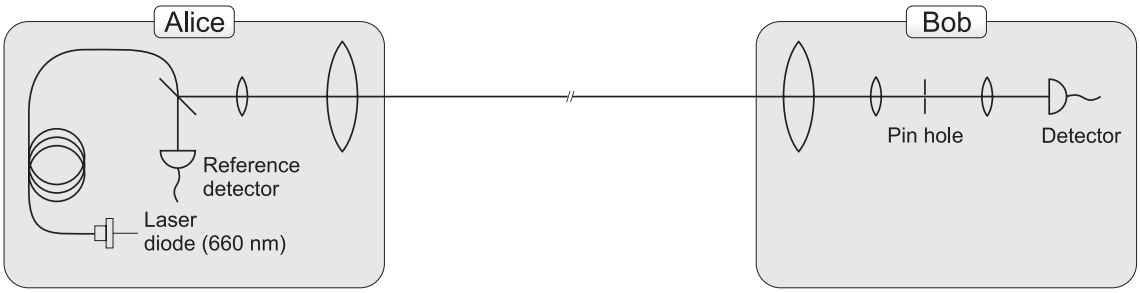


Figure 29: Setup of the absolute transmission measurement. In the case of relative transmission measurements, there was no reference detector.

would be about 190 kBit/s. The final key rate would certainly be substantially lower (depending on the bit error rate), but it could still be compared to ISDN rates.
The lower part of figure 28 shows an additional value called global radiation[7] (green curve) which was - like all other weather parameters - measured by the meteorology department of the University[8] . Comparing the transmission with global radiation and air temperature (upper red line), it appears as if the noisy, low transmission parts are connected to the radiation rather than to the air temperature. One possible explanation of this behaviour is that the beam passes closely over a black roof top (near mark 2 in figure 22) which is heated by the sun light and perturbs the air above it. During those periods of time, the beam position at the receiver telescope seemed to be rapidly fluctuating, much more so than for example during nights.
Figure 30 gives one more indication that the noise could be caused by sun radiation. During the first 24 hours, some scattered clouds blocked the sun light, which seems to have weakened the noise level, especially during the morning hours, where the roof top is most exposed to the sun. So this problem seems to be a problem of this specific location rather than a general limitation.

4.3.5 Longer Distance

Since the distance between sender and receiver should not be limited to 500 meters for applications, we tested the optical equipment over a distance of approximately 3000 meters, between Olympiaberg and a building of the LMU (see figure 31). The transmission was between 28% and 42%, measured between the end of the single mode fibre on the sender side and behind the last pinhole on the receiver side.
A linear CCD camera[9] was used to take pictures of the beam that was shining on a piece

[7] Global radiation is the sum of direct radiation from the direction of the sun and diffuse stray radiation scattered by the atmosphere on its way from earth to sun.
[8] `http://www.meteo.physik.uni-muenchen.de`
[9] Usually, the output signal of a CCD camera is not proportional to the intensity on the chip surface. This device has been chosen especially to meet that requirement.

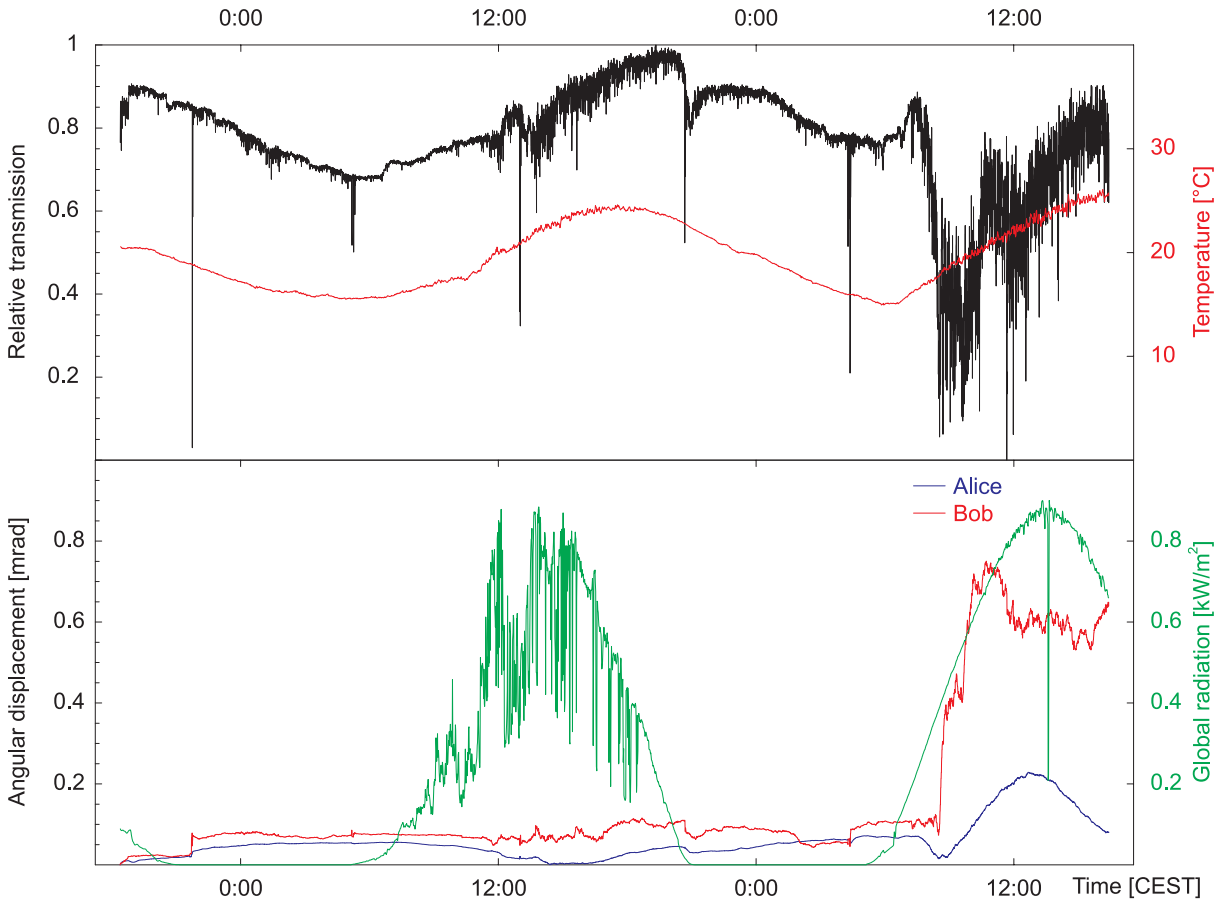


Figure 30: A relative transmission measurement with automatic alignment control and less noise.

of white paper (figure 32). The photographs show that the diameter of the bright central region of the spot is about 7.5 cm. Since this is as big as the front lens of the receiver telescope, losses are mainly due to rapid beam wandering which is also the case when the distance is less. If the distance has to be increased further, telescopes with bigger front lenses will become beneficial. For distances up to 3000 meters the optical equipment has proven to be suitable.

Figure 31: Transmission measurement between Olympiaberg and LMU Munich. The picture was taken by Thorsten Naeser.

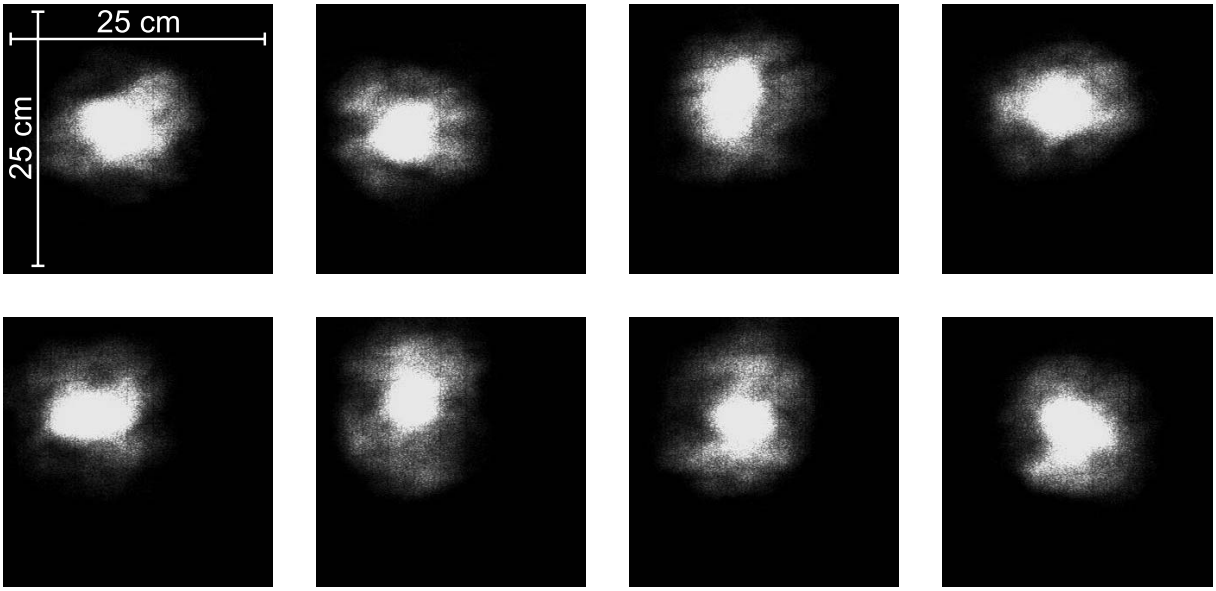
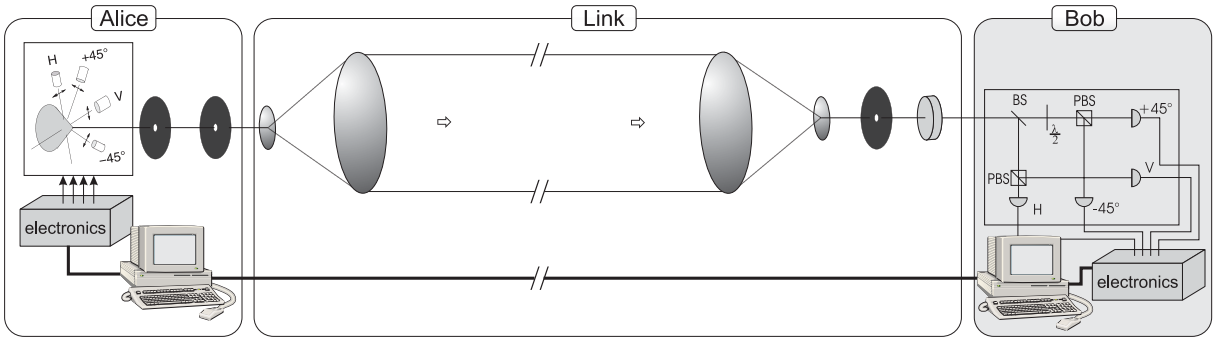


Figure 32: A sequence of pictures taken by a linear camera of the beam after approximately 3000 meters.

4.4 Receiver: Bob



The third part of the setup is the receiver unit. It has to detect single photons, analyse their polarisation and record their time of arrival. The main constituents of the receiver unit are

- the "Bob module", consisting of polarisation optics and single photon detectors (electronics included),
- the timestamp card, which assigns a time to every click of a detector and
- the software in Bob's computer, which is responsible for finding out the number of the received photon, so that Alice and Bob talk about the same photons.

4.4.1 Bob Module

At the heart of the receiver unit resides the Bob module, directly connected to the end of the receiver telescope. The first vital part of it is an interference filter with a FWHM of 3 nm on red colour glass filter. This is tremendously important to allow for daylight operation, because the background count-rate due to stray light would outperform the signal by several orders of magnitude on a bright day, even with a narrow field of view.
The remaining optical components (figure 33) form a device that detects incoming photons and analyses their polarisation randomly in one of two bases, H/V and +/−. It is based on an idea by John Rarity and Paul Tapster [42] and works like this: An incident photon first sees the 50/50 beam splitter (BS). If it is reflected it will next see the polarising beam splitter PBS 2, which in combination with the two Silicon APDs 2 and 4 analyses the polarisation of the photon in the H/V basis. A click of detector 2 means the photon was reflected by PBS 2, hence its polarisation is said to be vertical. On the other hand, when detector 4 registers the photon, it was transmitted by the PBS, so it is assigned horizontal polarisation.
Any photon transmitted by the non-polarising beam splitter passes through a half-wave plate, set at an angle of 22.5°, so that it rotates linear polarisation by 45° mapping

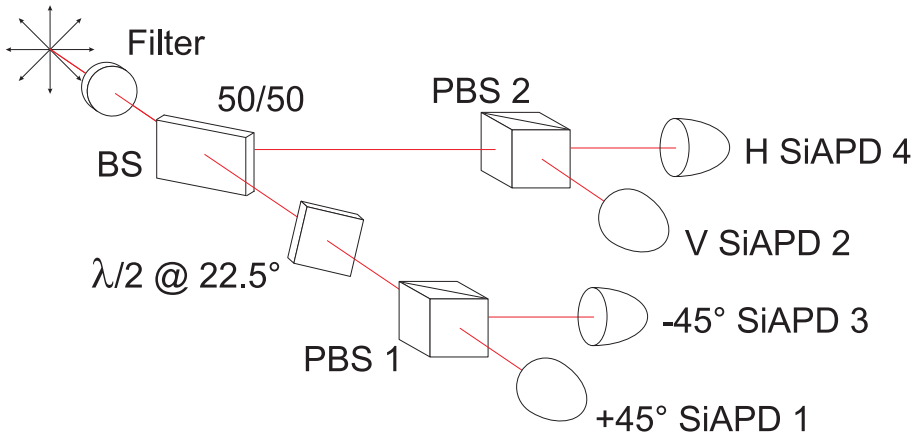


Figure 33: The basic setup of the Bob module. If an incoming photon gets transmitted at the beam splitter (BS), its polarisation will be analysed in the +/− basis. Whenever a photon gets reflected at the BS, its polarisation is analysed in the H/V basis.

$|+\rangle \mapsto |H\rangle$ and $|-\rangle \mapsto |V\rangle$. Whenever a +45° polarised photon hits the half-wave plate, its polarisation will be horizontal afterwards, so that it will be transmitted at PBS 1 and trigger detector 1. A −45° polarised photon will be detected by APD 3. Whenever a photon gets analysed in the "wrong" basis, the measurement outcome is completely random. For example, if a horizontally polarised photon gets transmitted on the first beam splitter, its polarisation will be -45° after the half-wave plate, so that it is equally likely to be detected by APD 1 or APD 3.
The idea of using two channels for the analysis in two bases and the use of a 50/50 beam splitter as a passive random choice device has simplified the receiver a lot, because neither active switching of the analysis basis is needed nor additional random numbers to decide which basis is used. Hence, a Bob module can be build as small as 130 mm × 80 mm × 55 mm, including all fast detection electronics. (figure 34).
The APDs have to be cooled in order to reduce dark counts. Depending on the tolerable dark count rate, they can be used at temperatures between −25° C and −10° C. To reach these temperatures, the photo diodes are put into an aluminium block which is cooled by a peltier element glued to it from below.
The set of electronics directly attached to the Bob module (on the right-hand side of figure 34) is composed of three layers. The lower layer is responsible for the temperature control of the aluminium blocks housing the APDs to keep them at −23° C. This temperature has been chosen, because it leads to low dark count rates between 400 and 500 per second and detector. A test on the roof top during a hot summer day has shown that such a low temperature cannot be sustained if the environment gets too warm, because the peltier elements can achieve a maximal temperature difference between the two layers of about 50° C. For those periods −10° C appears to be the most reasonable value.

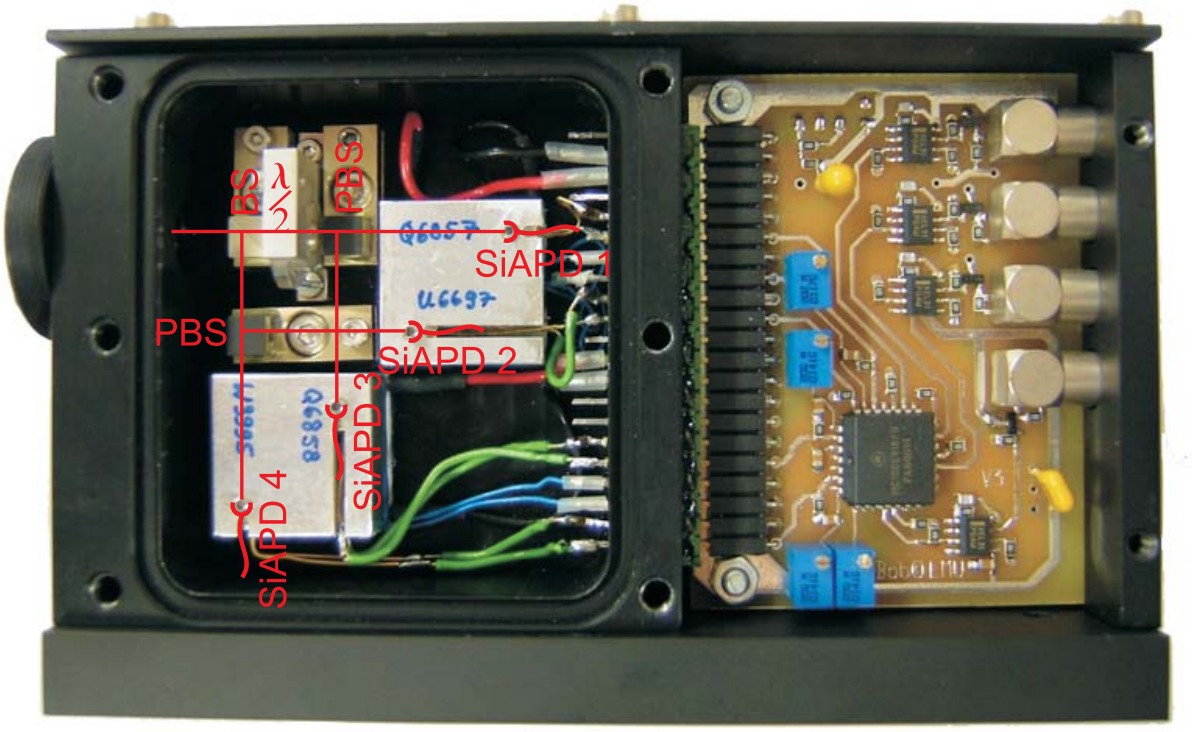


Figure 34: A photograph of the open Bob module. Nonpolarising (BS) and polarising (PBS) beam splitters, the half-wave plate and the avalanche photodetectors (SiAPD) are marked. The signalling electronics is visible on the right-hand side.

The next layer provides the high bias voltage for the APDs which they need to work in the so-called Geiger mode, where a single incident photon triggers a detectable avalanche of electrons. The bias voltage can be adjusted individually for each of the four diodes and is set to approximately 15 V over breakdown, i.e. 15 V above the threshold where an avalanche signal can be distinguished from background for the first time. The APDs are passively quenched by a resistor which limits the current flow and regulates the pulse width in connection with the capacitance of the diode itself.
The upper part of the electronics (directly visible in figure 34, the full circuit is shown in figure **??** in the appendix) is needed to form an output pulse with defined height and width, whenever an avalanche is triggered. The four potentiometers set the threshold voltages of the comparator, defining the level at which the input signal is considered to be an event. The Bob module features four outputs, one for each diode. When a detector registers a photon, a NIM pulse (logical 0 is 0 V, logical 1 is −1 V) is produced in the corresponding channel.
Whenever there is a logical 1 at either of the four outputs, it is treated as a detection of a photon with corresponding polarisation, APD 1 and 3 imply +45° and -45, whereas APD

2 and 4 refer to vertical and horizontal polarisation, respectively.

4.4.2 Synchronisation

Up to now it has been described how Alice sends polarised photons to Bob, who detects the photons and analyses them in a randomly chosen basis as required by the BB84 protocol. The next vital task is to assign numbers to the photons so that Alice and Bob can be sure that they later talk about the same events. The process of assigning the correct number to each photon is called **synchronisation**. Furthermore, precise synchronisation to about 2 ns enables the receiver to set the detection time window to a corresponding value, thereby reducing stray light effects significantly.
The first step is to attach a timestamp to every registered click, a task which is accomplished by an electronic device, the timestamp card. This card is connected to Bob's computer via a second Nudaq PCI 7200 digital I/O card. A first software unit translates the digital input into timestamps represented as 64 bit integers, the first 49 bit of which are used for time information in units of 1/8 of a nanosecond, while the last 4 bits indicate which detector has fired. The remaining bits are yet unused and read as 0.
If the local clocks at Alice and Bob were sufficiently synchronous, they would only have to define a mutual start time. This would require extremely stable local oscillators, but it can also be done without extra hardware by adding some software. The rest of this section will deal with our design and implementation of this software.

Basic Idea

It is known that Alice sends out photons at a repetition frequency of $\omega_{\text{sender}} = 2\pi \cdot 10$ MHz. As soon as this raster has been identified, good events can be discriminated from bad ones, so that a large fraction of dark and background counts can be filtered out. Since the local oscillators are not necessarily as stable as required, the calculated frequency and phase of the good events has to be adjusted all the time. Then, known patterns in the photon stream which have been inserted by Alice can be used to find out the number of each detected photon. Using this technique, Alice and Bob do not even have to communicate classically during the synchronisation, since Alice doesn't need to know when Bob wants to synchronise himself to Alice. The advantage of this fact is that a temporarily unavailable or slow classical channel will not hinder the synchronisation routine and the sifting produce can be performed later, when classical communication is available.

Stage I: Finding the 10 MHz Beat

Bob knows the repetition frequency ω_{sender}, with which Alice sends out photons. Unfortunately, Bob's clock is not necessarily synchronous with Alice's clock, so that he might see a slightly different frequency because of a difference in the clock speeds and also a phase, because he has probably started his clock at a different time than Alice.

The frequency can be calculated using a Fast Fourier Transform (FFT) (see e.g. [43]). As it is already known, that the frequency is roughly 10 MHz, not the whole frequency range has to be taken into account, it is sufficient to consider an interval around ω_{sender}. This can be done by mixing the input signal with ω_{loc}, represented by multiplying the incoming signal with $e^{-\imath\omega_{\text{loc}}}$ (see section 4.3.4).
This process has to be translated into the world of discrete time and frequency. The timestamps of the detected photons are denoted as t_i, integers in units of 0.125 ns and they form a discrete signal

$$h(t_j) = \sum_i \delta_{t_i,t_j} \quad . \tag{33}$$

At times t_j, where a click has been recorded, this function has a value of 1, otherwise it remains 0. This function has to be mixed with ω_{loc} and resampled by adding up k values of the mixed signal:

$$g(t_n) = \sum_{j=n\cdot k}^{(n+1)\cdot k-1} h(t_j)\cdot e^{\imath\omega_{\text{lock}}t_j} = \sum_{j=n\cdot k}^{(n+1)\cdot k-1}\sum_i \delta_{t_i,t_j} e^{\imath\omega_{\text{loc}}t_j} = \sum_{i=nk}^{(n+1)k-1} e^{\imath\omega_{\text{loc}}t_i} \tag{34}$$

Here, $n \in \{0..(N-1)\}$ and k is the sampling interval in timestamp units ($1\,\texttt{tu} = 0.125$ ns). N is the number of available samples, which is directly connected to the total sampling time $T_{\text{sampling}} = k \cdot N$. In a next step, the discrete FFT of $f(t_n)$ can be calculated:

$$G(\omega_m) = \sum_{n=0}^{N-1} e^{\imath\omega_m t_n}\cdot g(t_n) \qquad\qquad m \in \{0..(N-1)\} \tag{35}$$

The maximal frequency considered in the FFT is

$$\omega_N = \frac{\pi}{k} \quad , \tag{36}$$

the so-called Nyquist frequency. The reason is that the associated period is $T_P = \frac{1}{f_N} = \frac{2\pi}{\omega_N} = 2k$, which means that a whole oscillation happens in only two steps of n, the signal is alternating between 0 and 1. Therefore the number of samples N after the mixing procedure and the integration time per sample k have to be chosen to match the requirements. We have opted for $N = 2^{14}$ and $k = 2^{16}\,\texttt{tu} = 2^{13}$ ns, resulting in a total sampling time of $T_{\text{sampling}} = 2^{30}\,\texttt{tu} = 2^{27}$ ns $= 0.1342$ s. This value is important, because frequency drifts during this period of time might lead to problems.
The first task of the program (essential parts of it are shown in section **??**) is to calculate the function $g(t_n)$, which is appreciable, because this function has to evaluate only those cases, where a click was found. To do this more efficiently, all floating point operations are substituted by integer arithmetic. Furthermore, the required trigonometric functions are calculated in advance and stored in a look-up table, since there are only 1024 possible

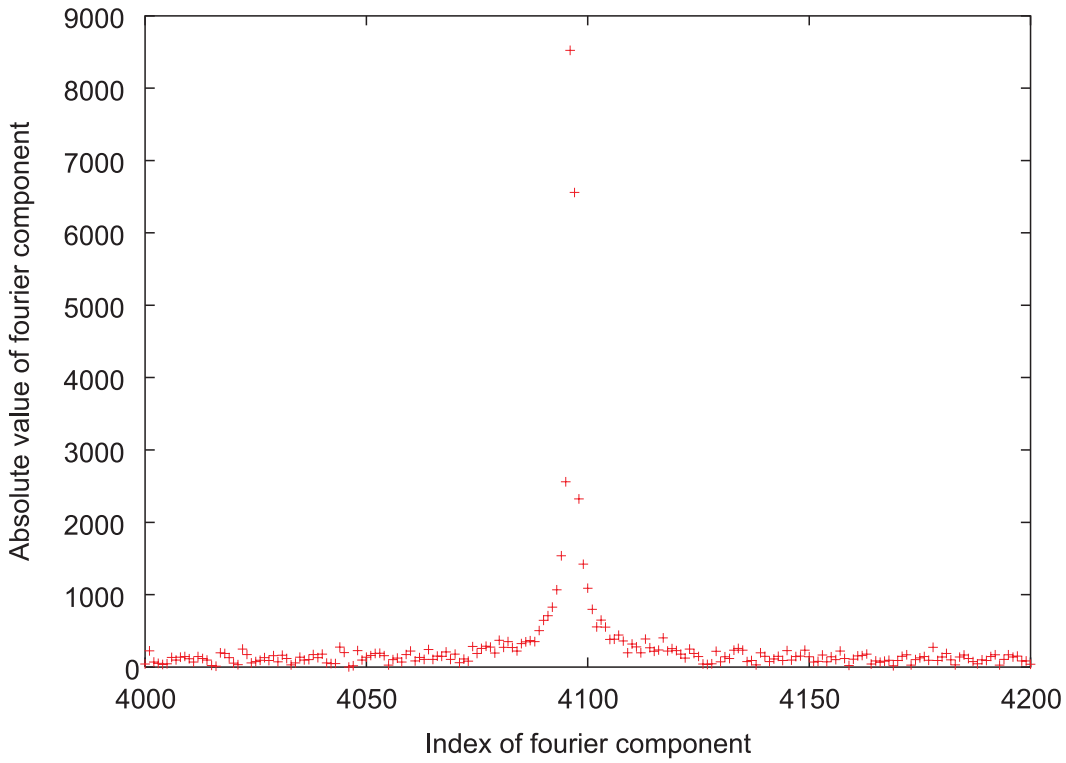


Figure 35: The important section of the result of the fast Fourier transform. The horizontal axis shows the index of the frequency component while the vertical axis shows the absolute value of the Fourier transform.

arguments. Only the cosine is used, because the sine can be calculated by $\sin\varphi = \cos(\varphi - \pi/2)$

After $g(t_n)$ has been computed, the fast Fourier transform can be performed. When the corresponding function `fourier()`, taken from [43], has been applied (the result of a simulated example is shown in figure 35), the maximally contributing frequency component is identified and translated into standard units by the procedure `get_frequency()`. The frequency `f_measured` has been calculated with a resolution given by the frequency range and the number of frequency components $\delta\omega = \frac{\omega_N}{N/2} = \frac{2\pi}{2^{14}\,\mathrm{ns}} \cdot \frac{1}{2 \cdot 2^{13}} \approx 2\pi \cdot 7.451\,\mathrm{Hz}$.

The next task is to calculate the phase ϕ_0 resulting from a constant timing difference between the local oscillators of sender and receiver. In principle, this could be computed by multiplying every timestamp by the frequency `f_measured` modulo 2π. Unfortunately, the spacing between two adjacent frequencies $\delta\omega$ is too big to give a suitable result, because if the calculated frequency is maximally wrong, the deviation of $\delta\omega/2$ will result in a phase difference after the total sampling time T_{sampling} of

$$|\delta\varphi| = \left|\frac{\delta\omega}{2} \cdot T_{\mathrm{sampling}}\right| = \pi \qquad . \tag{37}$$

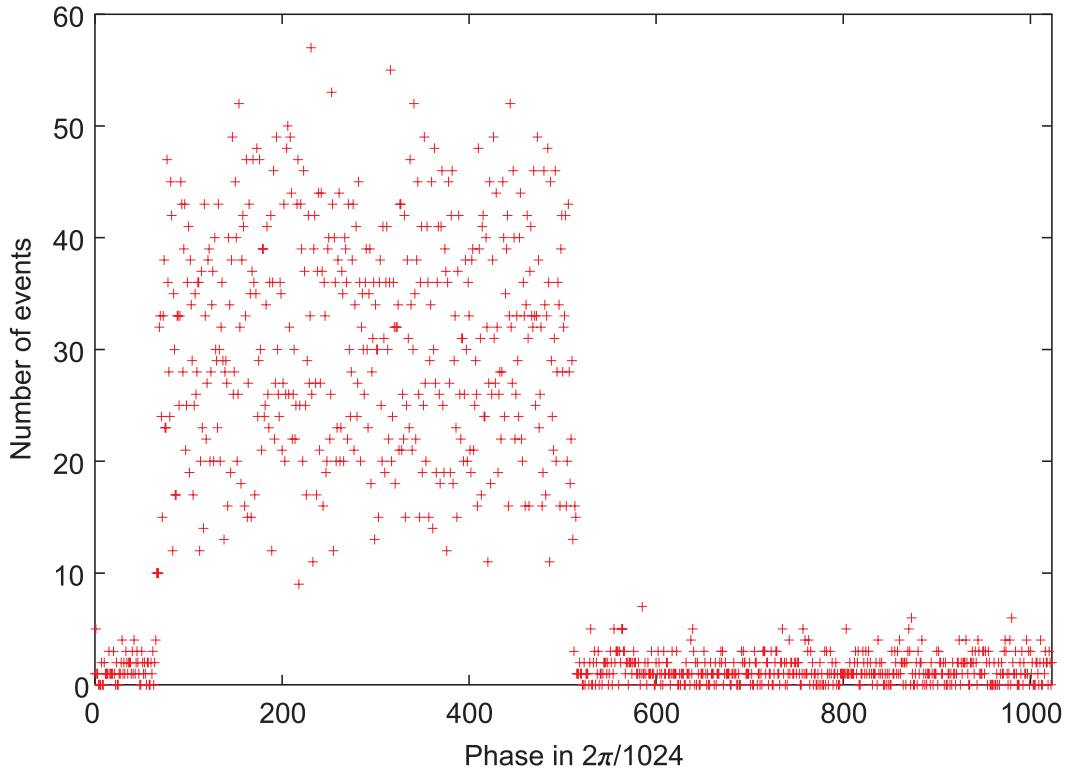


Figure 36: A histogram of the phase calculation for the same set of simulated data as in figure 35. The horizontal axis shows the phase in 10 bit, while the vertical axis shows how often the value appeared. Since the frequency was not calculated precisely enough, the phase is not static.

This is illustrated in figure 36, where the calculation was performed with the same data set that was used in figure 35. To overcome this problem, the frequency has to be calculated with a significantly higher precision. The FFT is unable to do that because an increased frequency resolution would increase the total sampling time by the same amount, so that the phase problem is not solved.
But, nevertheless it can be overcome by exploiting the fact that the phase develops linearly with time (see figure 37). A linear regression can find the value where the fitted line intersects the vertical axis to yield the starting phase and the slope can be used to correct the frequency with high precision. The only problem is to obtain a good fit despite the noise (which has been included in the simulation, see figure 37). This noise (possibly resulting from ambient light and dark counts) is assumed to be uniformly distributed. The linear regression procedure can be adapted to be insensitive to this kind of noise (see section A). This algorithm depends strongly on the statistics, so that it is not suitable for low count-rates as it has been implemented. But it could be improved by iterating this method on a subset of the data, cutting off more and more noise.
The result of the currently implemented algorithm applied to the simulated data is vi-

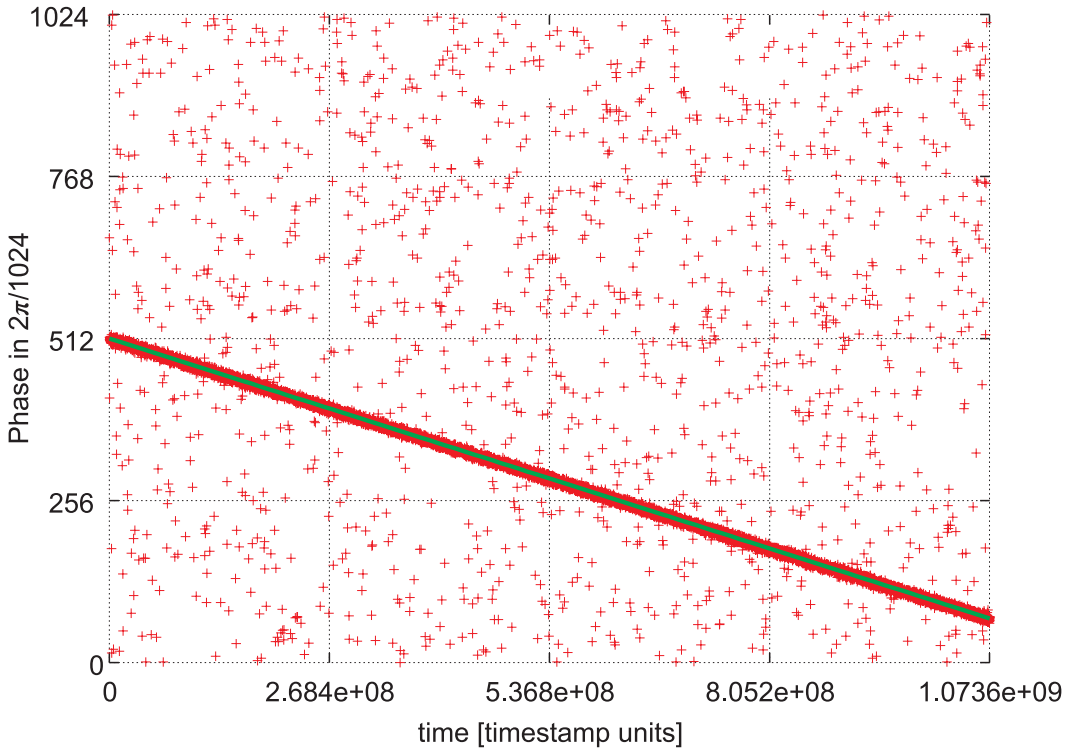


Figure 37: Linear regression fit (green line) with compensation for uniformly distributed noise. The data set is the same as in figures 35 and 36.

sualised by the green line in figure 37. It is plotted according to the parameters yielded by the linear regression. The important part of the C/C++ source code can be found in section ?? in function `linear_regression_with_background()`. The input data set was calculated using the following parameters: The frequency was 10.0000003 MHz, 10000 randomly distributed and 100000 regular events per second in the total sampling time of 1 second were simulated. The timestamps of the regular counts were also uniformly distributed in an interval of ±3 timestamp units around the correct value to simulate a jitter of the timing electronics. The offset of these timestamps, relative to a full period was set to 0.5, corresponding to a phase of 511 in figure 37, because there a period corresponds to 1024 steps, starting from 0.

Stage II: Keeping the 10 MHz Beat

The high precision frequency and the initial phase allow for a discrimination between "good" and "bad" events. Good events are those which happen in a narrow time window around an anticipated click according to the sender frequency. A second piece of software is responsible for the elimination of bad events using what I call the "Cinderella principle": *The good into the pot, the bad into the crop* [44]. Furthermore, it accounts for adjusting

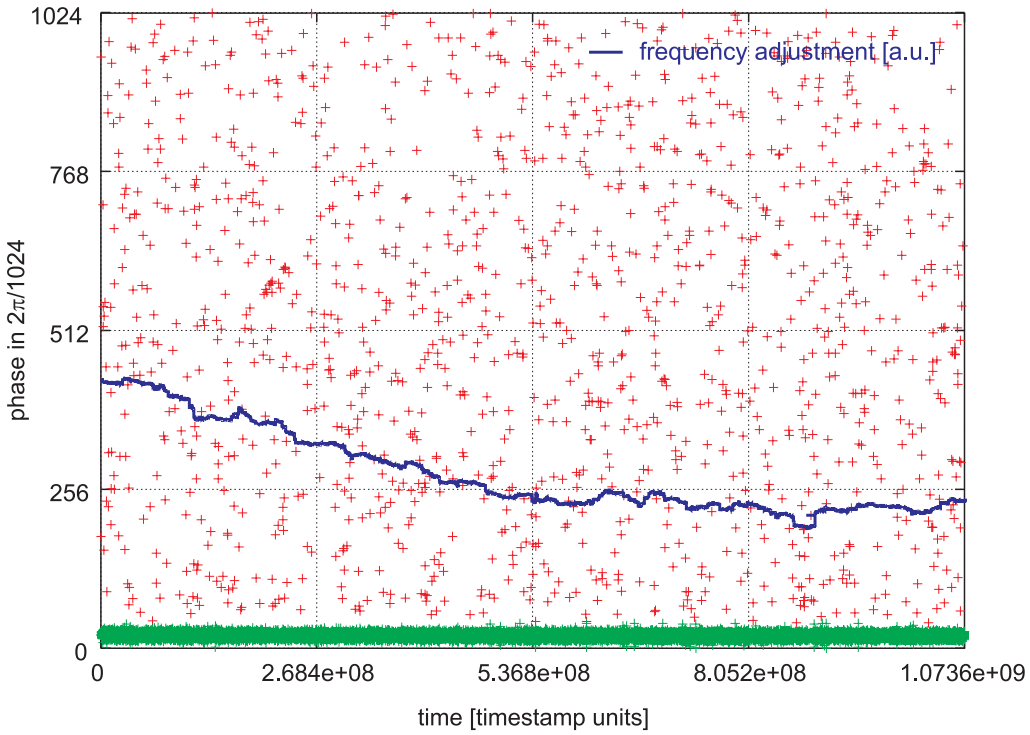


Figure 38: A result of the feedback algorithm. Good events are green, bad ones red. The time window was 40/1024 of the calculated period (about 4 ns full width). The blue line depicts the adjustment of the frequency in arbitrary units. The starting value of the frequency was manually detuned in order to see the compensation.

the high precision frequency and its phase with every good event. A part of the source code of this program can be found in section **??**.

The first task is achieved as follows: Using the values for frequency and phase obtained by the program described in the previous section, the time when good clicks are expected can be calculated by multiplying the timestamp of the incoming photon by the frequency modulo 2π. This is again a sort of phase relative to the calculated raster of events. When this phase is in a narrow time window around 0, the photon is considered to be initially send out by Alice, otherwise the entry is discarded. A positive effect of this procedure is that background and dark counts are suppressed significantly, depending on the width of the time window. This has to be adapted to the timing jitter of sender and receiver electronics, at the moment, a value of 2 ns seems to be feasible. With a period of 100 ns, this allows for a noise reduction by 1/50 due to temporal filtering.

To be able to cope with relative frequency drifts between the local oscillators and compensate for slightly wrong starting parameters, frequency and phase have to be adjusted continuously. To achieve that, the calculated relative phase of each good event is used.

If it indicates that the photon arrived earlier than expected, the calculated frequency is slightly increased and the computed phase is decreased a little. The effect of remaining false events should average out since they are assumed to be randomly distributed in time. To enhance the efficiency of this procedure, it also was implemented using integer arithmetic, calculating the relative phase of each event as a 10 bit integer, which is shown in figure 38. Furthermore, every event can be labelled with the number of periods since the start of the measurement. This represents the number, Bob assigns to each good click.

Stage III: Identifying the Frame Start

Since Alice and Bob might have started the experiment at a different time, their photon numbers can also differ. The next task for Bob is to find out that difference by finding patterns in the photon stream, Alice sends. This has not been fully implemented, hence I will only describe the basic idea.
As already mentioned, Alice divides the stream of photons she sends out into frames of a certain length. At the start of every frame, there is a frame header which is known to Bob, consisting of deterministic patterns, coded in presence and absence of photons. If a 1 should be sent out, she fires all four laser diodes, while she leaves all laser diodes turned off for sending a 0. This way, Bob has a higher probability to distinguish correctly between 0 and 1. The bits contained in the header will not be used for the key itself.
The header is again divided into two parts: The first part is a constant pseudo-random[10] bit pattern, repeated in every frame. Its only function is to identify the start of a frame, hence I call it the frame start identifier. To reduce the effect of noise from background and dark counts, it can be exploited that the frame length is known. When the bit string is divided into parts of the length of a frame, the pattern will be easier to find, because the same information has been sent repeatedly. The position of the known sequence can efficiently be found with the help of the fast fourier transform. This technique is also described in [43].

Stage IV: Calculating the Frame Number

As soon as the start of a frame has been identified, the only thing that is missing is the absolute frame that Alice has assigned to the specific frame. The second part of the frame header, the frame number identifier, has to convey this piece of information. Furthermore, it has to be coded in such a way that it is insensitive to loss and errors. One possible method is to use a similar pseudo-random pattern as above and shift this pattern one bit further in every consecutive frame. This would give redundancy to compensate for loss as well as a low chance of reading the same bit twice which doesn't yield any new information. Bob could find the position of his pattern in the known ideal string again by using a correlation function calculated with the help of FFTs.

[10] Pseudo-random numbers are needed here, because the string must not be periodic within the used length.

5 Conclusion & Outlook

Within the scope of this thesis, some progress towards a continuously working quantum cryptography system could be achieved. The main focus was kept on the development of a stable optical free space link as a main constituent of such a system. The automatically aligning link was tested extensively under different conditions and works as desired.
A second emphasis was the design and implementation of software that performs synchronisation of sender and receiver without using classical communication. Simulations with realistic parameters indicate that the most important part of the task is successfully accomplished by the program.

When all components will be connected together, the complete system should be close to the goal. One vital improvement has yet to be incorporated, namely the total remote control of the sender module. The mean photon number has to be observed and adjusted constantly. As soon as this is implemented, the system could be considered as a prototype for commercial application, which should be possible within the next year. Alongside of the described plans, a link over a larger distance should be tested. The experiments presented in this work indicate that the currently used optical equipment is sufficient for distances of at least 3 km.

As soon as the system is working reliably, all prerequisites exist to build a simple quantum cryptography network consisting of at least one sender unit and two receiver units or vice versa. Furthermore, some effort will have to be made in order to integrate quantum key distribution into existing IT infrastructure, adapting the classical protocols by adding the possibility to exchange keys for symmetric encryption algorithms via a quantum channel, providing one is available. One implementation of this idea has already been realised [45]. The trouble-free integration of quantum cryptography into the world of classical networks is one of the necessary conditions for it to become a regular member of the toolkit of IT security. In this context, it would certainly be interesting to build a heterogeneous network, connecting fibre based and free space quantum cryptography systems.

Another necessity is to bypass existing limitations regarding the link distance. Fibre based systems have been reported to work up to distances off 100 km (this limit could be pushed to about 300 km with more efficient detectors), while the free space record is 23 km. Two possible extension mechanisms have be proposed: Quantum relays [46] could divide the quantum channel into sufficiently short sections, using entangled photon pairs and Bell measurements to convey information. Free space links offer the possibility to communicate via satellites. A quantum cryptography system on a low earth orbit

satellite could exchange a key with Alice, wait until it is in reach of Bob, exchange a key with him and securely transmit Alice's key to him. Or they could exchange keys with a satellite in a geo-stationary orbit in parallel. To improve security, the satellite could carry a source of entangled photon pairs, directing one of them towards Alice and the other one towards Bob. They could employ an entanglement based quantum cryptography protocol to exchange a key with additional security, because they don't have to trust the satellite. As unbelievable as this idea may sound, the European Space Agency (ESA) examines at present, whether it is beneficial for them to support a quantum cryptography project with the ultimate goal of sending a QKD sender unit into space in only a few years time.
Entangled photon pair cryptography could furthermore solve the problem of obstacles in the direct line of sight between two parties. The source could be located on a tall building, possibly a telecommunications tower, visible by both parties. A different solution would be to use a single particle scheme as in the non-stationary satellite case, again under the assumption that the third party can be trusted. One more approach implies the use of a mirror to connect two parties without direct inter-visibility. This method would not even introduce a security risk.

The next few years will probably be crucial for the further evolution of quantum cryptography. Commercial investors have started to show a little interest, but they seem to wait for a market to develop. Small companies may use the chance of testing the market situation and it is difficult to anticipate the result. If there is a substantial need for realistic quantum cryptography systems, these devices could be the first ones widely used in real-world applications that rely directly on quantum physics. More fundamental research areas of quantum information would benefit from such a development, because the activity in the whole field would probably be increased. It will certainly be very interesting to watch and perhaps participate in this process.

A Linear Regression with Uniform Background

Linear regression is the most basic fit method [43] (often, a and b is used in the reverse order). If a straight line $y = ax + b'$ has to be fitted to some set of data $\{(x_i, y_i)\}$ by linear regression, the least squares method is used. I.e. the task is to minimise the error function

$$\chi^2(a,b,\ldots) \overset{\text{generally}}{=} \sum_{i=1}^{N} \left(\frac{y_i - y(x_i;a,b,\ldots)}{\sigma_i} \right)^2 \overset{\text{here}}{=} \sum_{i=1}^{N} \left(y_i - (ax_i + b) \right)^2 \quad (38)$$

$$\begin{aligned} \chi^2(a,b) &= \sum_i \left(y_i - (ax_i + b) \right)^2 && (39a) \\ &= \sum_i \left(y_i^2 - 2(ax_i + b)y_i + (ax_i + b)^2 \right) && (39b) \\ &= \sum_i \left(y_i^2 - 2ax_iy_i - 2by_i + a^2x_i^2 + 2abx_i + b^2 \right) && (39c) \end{aligned}$$

To find the minimum of χ^2, one can calculate vanishing derivatives with respect to a and b:

$$\begin{aligned} \frac{\partial \chi^2(a,b)}{\partial a} &= \sum_i \left(-2x_iy_i + 2ax_i^2 + 2bx_i \right) && (40a) \\ &= -2 \underbrace{\sum_i x_iy_i}_{S_{xy}} + 2a \underbrace{\sum_i x_i^2}_{S_{xx}} + 2b \underbrace{\sum_i x_i}_{S_x} && (40b) \end{aligned}$$

$$\begin{aligned} \frac{\partial \chi^2(a,b)}{\partial b} &= \sum_i \left(-2y_i + 2ax_i + 2b \right) && (41a) \\ &= -2 \underbrace{\sum_i y_i}_{S_y} + 2a \underbrace{\sum_i x_i}_{S_x} + 2b \underbrace{\sum_i 1}_{N} && (41b) \end{aligned}$$

A linear system of equations with parameters a and b has to be solved.

$$S_{xx}a + S_x b = S_{xy} \tag{42a}$$
$$S_x a + Nb = S_y \tag{42b}$$

The solution is

$$a = \frac{NS_{xy} - S_x S_y}{NS_{xx} - (S_x)^2} \tag{43a}$$
$$b = \frac{S_{xx}S_y - S_x S_{xy}}{NS_{xx} - (S_x)^2} \quad . \tag{43b}$$

To distinguish between signal and background, the set of events $\{(x_i, y_i)\}$ can be divided into signal events $\{(x_k, y_k)\}$ and noise events $\{(x_l, y_l)\}$. Of course, they are complementary $\{(x_i, y_i)\} = \{(x_k, y_k)\} \cup \{(x_l, y_l)\}$. So the sums can be expressed as:

$$N = N_{\text{signal}} + N_{\text{noise}} \tag{44a}$$
$$S_x = \sum_i x_i = \sum_k x_k + \sum_l x_l \tag{44b}$$
$$S_y = \sum_i y_i = \sum_k y_k + \sum_l y_l \tag{44c}$$
$$S_{xx} = \sum_i x_i^2 = \sum_k x_k^2 + \sum_l x_l^2 \tag{44d}$$
$$S_{xy} = \sum_i x_i y_i = \sum_k x_k y_k + \sum_l x_l y_l \tag{44e}$$

If the total number of background counts N_{noise} is known and it is assumed that these events are evenly distributed over the whole area, the contribution to those factors can be calculated. Hence it is possible to extract this effect and end up with the values for the system without noise.

$$\sum_l x_l = \sum_l \left(l \cdot \frac{x_{\max}}{N_{\text{noise}}} \right) = \frac{x_{\max}}{N_{\text{noise}}} \sum_{l=1}^{N_{\text{noise}}} l \approx \frac{x_{\max} \cdot N_{\text{noise}}}{2} \tag{45}$$

$$\sum_l x_l^2 = \sum_{l=1}^{N_{\text{noise}}} \left(l \cdot \frac{x_{\max}}{N_{\text{noise}}} \right)^2 \tag{46a}$$
$$= \frac{x_{\max}^2}{N_{\text{noise}}^2} \sum_{l=1}^{N_{\text{noise}}} l^2 \tag{46b}$$
$$= \frac{x_{\max}^2}{N_{\text{noise}}^2} \cdot \frac{N_{\text{noise}}(N_{\text{noise}}+1)(2N_{\text{noise}}+1)}{6} \tag{46c}$$
$$= \frac{x_{\max}^2}{N_{\text{noise}}} \cdot \frac{(N_{\text{noise}}+1)(2N_{\text{noise}}+1)}{6} \tag{46d}$$
$$\approx \frac{x_{\max}^2 \cdot N_{\text{noise}}}{3} \tag{46e}$$

$$\sum_l x_l y_l = \sum_{l=1}^{N_{\text{noise}}} \left(l \cdot \frac{x_{\max}}{N_{\text{noise}}} \right) \cdot \langle y_l \rangle \tag{47a}$$

$$= \sum_{l=1}^{N_{\text{noise}}} \left(l \cdot \frac{x_{\max}}{N_{\text{noise}}} \right) \cdot \frac{y_{\max}}{2} \tag{47b}$$

$$= \frac{x_{\max} \cdot (N_{\text{noise}} + 1)}{2} \cdot \frac{y_{\max}}{2} \tag{47c}$$

$$\approx \frac{x_{\max} \cdot y_{\max} \cdot N_{\text{noise}}}{4} \tag{47d}$$

In order to get the correct a and b without noise, the following values have to be calculated:

$$N_{\text{signal}} = N - N_{\text{noise}} \tag{48a}$$

$$S_x^{\text{signal}} = \sum_i x_i - \frac{x_{\max} \cdot N_{\text{noise}}}{2} \tag{48b}$$

$$S_y^{\text{signal}} = \sum_i y_i - \frac{y_{\max} \cdot N_{\text{noise}}}{2} \tag{48c}$$

$$S_{xx}^{\text{signal}} = \sum_i x_i^2 - \frac{x_{\max}^2 \cdot N_{\text{noise}}}{3} \tag{48d}$$

$$S_{xy}^{\text{signal}} = \sum_i x_i y_i - \frac{x_{\max} \cdot y_{\max} \cdot N_{\text{noise}}}{4} \tag{48e}$$

When N_{Noise} is known, equations (48b) to (48e) can be evaluated and afterwards the values for a_{signal} and b_{signal} can directly be obtained:

$$a_{\text{signal}} = \frac{N_{\text{signal}} S_{xy}^{\text{signal}} - S_x^{\text{signal}} S_y^{\text{signal}}}{N_{\text{signal}} S_{xx}^{\text{signal}} - \left(S_x^{\text{signal}} \right)^2} \tag{49a}$$

$$b_{\text{signal}} = \frac{S_{xx} S_y^{\text{signal}} - S_x^{\text{signal}} S_{xy}^{\text{signal}}}{N_{\text{signal}} S_{xx}^{\text{signal}} - \left(S_x^{\text{signal}} \right)^2} \quad . \tag{49b}$$

Bibliography

[1] R. P. Gwinn, P. B. Norton and R. McHenry.
The new Encyclopædia Britannica.
Volume 16. Macropædia, Chicago, (1992).

[2] S. Singh.
The Code Book.
Fourth Estate, (1999).

[3] B. Schneier.
Applied Cryptography.
John Wiley & Sons, Inc., New York, (1996).

[4] U. D. of Commerce/ National Institute of Standards and Technology.
Data Encryption Standard (DES), Federal Information Processing Standards Publication 46-3.
Reaffirmed 1999, October 25;
`http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf`.

[5] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone.
Handbook of Applied Cryptography.
CRC Press.
`www.cacr.math.uwaterloo.ca/hac/`.

[6] M. A. Nielsen and I. L. Chuang.
Quantum Computation and Quantum Information.
Cambridge University Press, (2001).

[7] D. Bouwmeester, A. Ekert and A. Zeilinger (Eds.).
The Physics of Quantum Information.
Springer, (2000).

[8] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden.
Quantum cryptography.
Rev. Mod. Phys., **74**:145–195, (2002).

[9] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin.
Experimental Quantum Cryptography.
Journal of Cryptology, **5**, 1, (1992).

[10] H.-K. Lo, S. Popescu and T. Spiller (Eds.).
Introduction to Quantum Computation and Information.
World Scientific, Singapore, (1999).

[11] N. Gisin and S. Massar.
Optimal Quantum Cloning Machines.
Phys. Rev. Lett., **79**, 11:2153–2156, (1997).

[12] V. Bužek and M. Hillery.
Quantum copying: Beyond the no-cloning theorem.
Phys. Rev. A, **54**, 3:1844–1852, (1996).

[13] C. H. Bennett and G. Brassard.
Quantum Cryptography: Public Key Distribution and Coin Tossing.
Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, (1984).

[14] H.-K. Lo and H. F. Chau.
Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances.
Science, **283**:2050–2056, (1999).

[15] N. Lütkenhaus.
Security against eavesdropping in quantum cryptography.
Phys. Rev. A, **54**, 1:97–111, (1996).

[16] N. Gisin and B. Huttner.
Quantum cloning, eavesdropping and Bell's inequality.
Phys. Lett. A, **228**:13–21, (1997).

[17] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu and A. Peres.
Qptimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy.
Phys. Rev. A, **56**, 2:1163–1172, (1997).

[18] R. B. Griffiths and C.-S. Niu.
Optimal eavesdropping in quantum cryptography. II. A quantum circuit.
Phys. Rev. A, **56**, 2:1173–1176, (1997).

[19] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat and P. Grangier.
Single Photon Quantum Cryptography.
Phys. Rev. Lett., **89**, 187901, (2002).

[20] E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon and Y. Yamamoto.
Quantum cryptography with a photon turnstile.
Nature, **420**:762, (2002).

[21] A. Yariv.
Quantum Electronics.
John Wiley & Sons, (1989).

[22] N. Lütkenhaus.
Security against individual attacks for realistic quantum key distribution.
Phys. Rev. A, **61**, 052304, (2000).

[23] H. Inamori, N. Lütkenhaus and D. Mayers.
Unconditional Security of Practical Quantum Key Distribution.
quant-ph/0107017, (2001).

[24] G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders.
Limitations on Practical Quantum Cryptography.
Phys. Rev. Lett., **85**, 6:1330–1333, (2000).

[25] M. Curty and N. Lütkenhaus.
Practical quantum key distribution: On the security evaluation with inefficient single-photon detectors.
quant-ph/0311066, (2003).

[26] N. Lütkenhaus and M. Jahma.
Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack.
New Journal of Physics, **4**, 44:1–9, (2002).

[27] A. Einstein, B. Podolsky and N. Rosen.
Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?
Phys. Rev., **47**:777–780, (1935).

[28] A. K. Ekert.
Quantum Cryptography Based on Bell's Theorem.
Phys. Rev. Lett., **67**, 6:661–663, (1991).

[29] J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt.
Proposed experiment to test local hidden-variable theories.
Phys. Rev. Lett., **23**, 15:880–884, (1969).

[30] J. S. Bell.
On the Einstein-Podolsky-Rosen paradox.
Physics, **1**, 195, (1964).
Reprinted in *Speakable and unspeakable in quantum mechanics*, Cambridge University Press, pp. 14-21 (1987).

[31] C. H. Bennett, G. Brassard and N. D. Mermin.
Quantum Cryptography without Bell's Theorem.
Phys. Rev. Lett., **68**, 5:557–559, (1992).

[32] D. Gottesman and J. Preskill.
Secure quantum key distribution using squeezed states.
Phys. Rev. A, **63**, 022309, (2001).

[33] G. Brassard and L. Salvail.
Secret-Key Reconciliation by Public Discussion.
Advances in Cryptology - Proceedings of Eurocrypt'93, (1993).

[34] P. Møller Nielsen, C. Schori, J. L. Sørensen, L. Salvail, I. Damgard and E. Polzik.
Experimental quantum key distribution with proven security against realistic attacks.
J. Mod. Opt., **48**, 13:1921–1942, (2001).
`http://www.cki.au.dk/experiment/qcrypto/doc/`.

[35] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden and N. Gisin.
"Plug and play" systems for quantum cryptography.
Appl. Phys. Lett., **70**, 7:793–795, (1997).

[36] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden.
Quantum key distribution over 67 km with a plug & play system.
New Journal of Physics, **4**, 41:1–8, (2002).

[37] H. Kosaka, A. Tomita, Y. Nambu, T. Kimura and K. Nakamura.
Single-photon interference experiment over 100 km for quantum cryptography system using a balanced gated-mode photon detector.
quant-ph/0306066, (2003).

[38] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter and A. Zeilinger.
A fast and compact quantum random number generator.
Review of Scientific Instruments, **71**, 4:1675–1680, (2000).

[39] **id Quantique**.
`http://www.idquantique.com`.

[40] R. J. Hughes, J. E. Nordholt, D. Derkacs and C. G. Peterson.
Practical free-space quantum key distribution over 10 km in daylight and at night.
New Journal of Physics, **4**, 43:1–14, (2002).

[41] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster and J. G. Rarity.
A step towards global key distribution.
Nature, **419**:450, (2002).

[42] J. G. Rarity and P. R. Tapster (Inventors).
Cryptographic receiver.
European patent specification EP 0 722 640 B1, (1994).

[43] W. H. Press, S. A. Teukolsky, W. T. Vetterling and B. P. Flannery.
Numerical Recipes in C, The Art of Scientific Computing.
Volume 2. Cambridge University Press, (1992).

[44] R. Riemann (Eds.).
Kinder und Hausmärchen, gesammelt durch die Brüder Grimm, Jubiläumsausgabe.
Turm Verlag, Leipzig, (1907).

[45] C. Elliot, D. Pearson and G. Troxel.
Quantum Cryptography in Practice.
quant-ph/0307049, (2003).

[46] D. Collins, N. Gisin and H. de Riedmatten.
Quantum Relays for Long Distance Quantum Cryptography.
quant-ph/0311101, (2003).

Index

Acknowledgements

First of all I would like to thank Professor Alfred Laubereau, because all I contributed to was making the pile of work on his desk a little higher.
The next person I want to express my gratitude to is Professor Harald Weinfurter, who gave me the opportunity to work in his group and participate in all sorts of events. I know that this is special and I really appreciate it.
I wish to thank Professor Christian Kurtsiefer for the inspiring teamwork and the patient explanations of so many things I should have learned a lot earlier. I hope I will get an opportunity to join your team again.

Furthermore, I want to thank Tobias Schmitt-Manderbach for collaborating with me in the lab (and on the roofs) and for being responsible for so many funny moments, even if it might not always have been in your favour.
Special thanks go to Carsten "I'm from Hamburg, but I can shovel snow like mad" Schuck for a lot of jokes and illuminating discussions. Remember, you still have your trunk here in the lab and your bike in the courtyard, so you'll have to come back some time.
I'd like to thank Jürgen Volz and Oliver Schulz for many interesting and joyful discussions and for their help with many things.
I thank Dr Mohamed Bourennane for a lot of pleasant and funny conversations. Good luck for the future! (I know you would rather read something else, but this is much more important.)
A big "Zers" to Patrick Zarda for a nice time on Westliche Karwendelspitze and afterwards in Munich. It's really a shame you had to leave when it had just got very funny. Anyway, we still have a can of "Vinzenzmurr Ungarische Gulaschsuppe" here, so jump onto Santa's sledge and visit us.
Of course I want to thank all the other members of the group for contributing to the good atmosphere: Gerhard Huber, Christian Schmid, Pavel Trojek, Chunlang Wang, Johann B. Schachaneder, Johannes Vrana, Markus Weber, Julia Lau, Nikolai Kiesel, Sascha Gaertner, Manfred Eibl and Daniel Schlenk.

Last but not least I wish to thank my family for the unlimited support that they have given to me.

Erklärung

Mit der Abgabe der Diplomarbeit versichere ich, dass ich die Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

München, 12.12.2003

Henning Weier