Department für Physik

Free-Space Quantum Cryptography

Ivan Ordavo

Diplomarbeit unter der Anleitung von
Prof. Dr. Harald Weinfurter

Erstgutachter: Prof. Dr. Harald Weinfurter
Zweitgutachter: Prof. Dr. Eberhard Riedle

München, 16. Juni 2006

LMU

LUDWIG-
MAXIMILIANS-
UNIVERSITÄT
MÜNCHEN

Contents

1 Introduction

Cryptography is the art of obscuring the content of a message to unauthorized people, but to make it accessible to trusted parties. This practice has ancient origins and, in the course of the centuries, it could meet more and more demanding requirements determined by the parallel ability of codebreakers to gain knowledge about those secrets. Nevertheless, particularly in the information age in which we live, concerns about security questions have become an everyday topic. If, on the one hand, the internet is now the ultimate place to accelerate the flow of relevant information, on the other hand, companies, government facilities, or even private people must be sure that confidential data flows cannot be accessible to someone else but the authorized party the message is addressed to. In order to ensure such a security level over publicly available networks, some nowadays standardized procedures come into play.

For practical reasons, the most frequently used protocols rely on so called asymmetric key algorithms (public-key cryptography), where the encryption key is published, which allows any sender to perform encryption and to safely send his message, while a private key is kept secret by the receiver, which enables only him to perform decryption. Although widely used, e.g. in online-banking transactions or e-commerce, the security of such cryptographic routines is taken for granted only under some reasonable (but not necessarily true) assumptions, such, e.g., limited computational power at one's disposal or low efficiency of factorizing algorithms.

The only encryption procedure which has been shown to be unbreakable[1] is the *one-time pad*, a symmetric key algorithm. Unfortunately, some major drawbacks, key distribution above all, make this process hard to implement in the framework of classical information theory. Nevertheless, though this deficiency, it turns out that quantum information theory is able to provide a

[1] The precise expression is *unconditional secure*, that is no restriction is made about computational power or scientific progress available. The proof for the one-time pad is due to Claude Shannon, who published it in the *Bell Labs Technical Journal* in 1949.

way-out to this problem. Unlike classical cryptography, which uses mathematical techniques to restrict the amount of eavesdropped information, quantum cryptography exploits the quantum character of nature to ensure secure communication between two trusted parties. This new issue, known under the name of *Quantum Key Distribution (QKD)*[2], provides the two parties, Alice and Bob, with a setup to generate a secret key, which can be used afterwards in the encryption/decryption process of the secret message (e.g. with one-time pad). Within this scheme, single key bits are encoded in states of a quantum mechanical system (e.g. polarization states of a photon), and then distributed between two or more parties. If an eavesdropper would ever attempt to intercept key bits, he has to carry out a measurement on a quantum mechanical system, unavoidably changing its status, hence introducing errors. This revolutionary principle of *eavesdropping can be detected*, is used in analysis protocols which can assert whether the key exchange was secure, or someone tried to eavesdrop, in which case the key has to be dismissed.

In this work we present an experimental implementation of such a scheme, in which raw key bits are encoded in four different polarization states of photons. Using the first proposed quantum encoding protocol, the BB84, and weak coherent pulses from a laser source, we could realize a stable link between transmitter and receiver units over a free-space distance of 500 m. Software-based procedures for key extraction and privacy amplification lead to the final shared secure key. This thesis-work is articulated in four main sections: In the first (Chap. 2), we provide the reader with a wide overview of classical cryptographic methods, how they work and their security issues. The second (Chap. 3) illustrates the main concepts of QKD and the underlying physics involved in them. The third section (Chap. 4) deals with the description of our test-setup located in downtown Munich, with particular attention paid to transmitter/receiver units and source spectral selection. The last part describes the applied procedures for thermal management, which aims to stabilize the spectral characteristics of the source.

[2] Sometimes the expression Quantum Key Growing is used, emphasizing the fact that an initial shared secret key is needed for the process to work.

2 Classical Cryptography

2.1 General Remarks

Before computer age, the term *cryptography* (from the Greek *κρυπτός* "hidden" and *γραφή* "to write"), referred solely to the process of changing the content of a message in order to make it unreadable without special knowledge. Since then, the meaning assumed a wider dimension, and nowadays can be summarized with the words of a famous cryptologist, Ron Rivest, who stated: *"Cryptography is about communication in the presence of adversaries"* [Riv90]. Moreover, the art of gaining unauthorized information, is called *cryptanalysis* (loosely speaking *codebreaking*), and together with cryptography constitutes the field of studies of *cryptology.*
In the technical literature, a fundamental distinction between "classical" and "modern" cryptography is made. The former refers to the age where cryptographic procedures were still accomplished with paper and pen; the latter refers to almost the same tasks but carried out with the help of computers. Nevertheless, throughout this work, the meaning of the adjective "classical" is extended to include also the modern cryptography as a subset, to better outline the difference relative to cryptographic tasks accomplished with the help of quantum based devices.

2.2 Glossary

For the general discussion we need some fundamental definitions beforehand.

Plaintext: The message, cleartext or bit string, one wishes to obscure.

Cipher: The algorithm by which the plaintext is made unintelligible to unauthorized parties.

Ciphertext: The output of an encrypting algorithm.

Key: Additional piece of information which is needed for performing encryption and decryption.

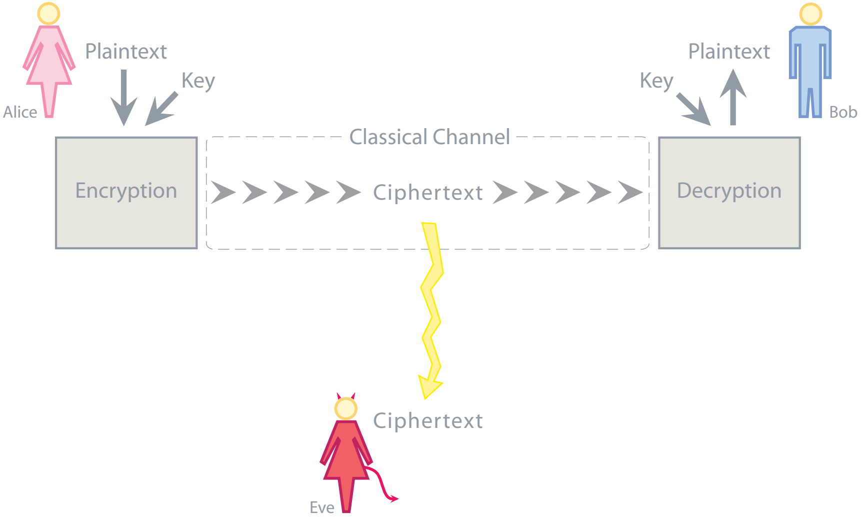


Figure 2.1: Alice wishes to send a message to Bob without revealing its content either to accidental or bad intentioned eavesdroppers. To do this, she first encrypts the message, then sends it out to Bob over a possibly unsafe communication channel; after Bob has received it, he applies the deciphering algorithm to finally get the original information again.

Encryption: The process of obscuring the information contained in the plaintext through application of a cipher.

Decryption: The process of recovering the original message from the ciphertext. It is the inverse of encryption.

Stream Cipher: Encrypting algorithm that acts on the smallest unit of the message (e.g. a letter in traditional "analog" cryptography, or a bit in computer based applications).

Block Cipher: Unlike a stream cipher, the algorithm manipulates block of characters or bits of the plaintext.

The general scheme we have in mind is depicted in Fig. 2.1.

2.3 Kerckhoffs' Principle and Encryption Keys

Historically, in the field of cryptography, we can distinguish between two different approaches. The first is condensed in the principle *"security by obscurity"*, that is the difficulty for an eavesdropper to gain information relies on his ignorance about the *cipher* which generated the ciphertext. This principle is widely used in computer related applications, where secrecy (of design, implementation, etc.) is used to gain security.

The problem of the "security by obscurity" approach is the actual difficulty to ensure secrecy of all sensible parts of the encrypting system for arbitrary long time. Moreover, as soon as the details of a cryptographic implementation are disclosed, all past, present and future pieces of encrypted informations become accessible at once. These major objections are more precisely referred to as **Kerckhoffs' law**, stated by the Flemish linguist and cryptographer Auguste Kerckhoffs in 1883 [Ker83]. After this principle, a good cryptographic system should remain secure even if it falls in adversary's hands, or, in Shannon's other formulation: *"the enemy knows the system"*. Within this second interpretation, the aim is making the output of the cipher as strongly as possible dependent from another piece of information, the **key**, which must be kept secret.

In every cryptographic design relying to the latter method, decrypting the ciphertext with the wrong key will produce a useless random sequence.

2.4 Symmetric and Asymmetric Ciphers

Following [Sch96], we can further divide key-based algorithms into two subsets: **symmetric** and **asymmetric** ones. Ciphers belonging to the first class use trivially related keys for the encryption/decryption process. Though in most algorithms of this kind the encryption and decryption key are simply identical, this doesn't need to be true in general; the important point is that the encryption key can be easily calculated from the decryption key and vice versa. The successful implementation of symmetric-key algorithms (also called secret-key algorithms), requires that sender and receiver agree on a key before the communication takes place. Moreover, since the security of the process rests in the key, this has to be safely distributed between the two parties. Actually, this last requirement constitutes a serious deficiency in the security of classical symmetric-key procedures.

Ciphers belonging to the second class use a key-pair: one for encryption and one for decryption. The encryption key is mathematically related to the decryption key by a so called **one-way function**: given the decryption key, it is easy to deduct the corresponding encryption key, while it results computationally difficult to go the other way around.

The advantage of the latter scheme is exploited in public-key algorithms, such as RSA (see Section 2.8.2), where the encryption key doesn't need to be secret, so that everyone can encrypt his message, while it can be read only by those who possess the corresponding private decryption key.

2.5 Transposition Ciphers

Because of their character based nature, this type of ciphers are among the oldest ones. The algorithm is fairly straightforward: given a plaintext, it shuffles its characters assigning to every letter a new position on an imaginary indexed table. Mathematically, the encrypting process can be seen as a bijective discrete function which maps a character position into a new one (permutation); decryption takes place with the inverse mapping.
A quite smart device to practically implement such an operation was invented in ancient Greece and widely used for military communications by the Spartans. It is called *Scytale* (Greek $\sigma\kappa\upsilon\tau\acute{\alpha}\lambda\eta$ "stick") and consists of a wooden cylinder, around which is wound a strip of paper. On the wrapped paper is now possible to write the message in the usual way, but, after unwinding, a random sequence of characters appears instead. To decrypt the message one needs to have a stick of the same diameter, which clearly plays the role of the (symmetric) key.

2.6 Substitution Ciphers

This class of algorithms replaces a unit of plaintext with another unit of text following a defined pattern; the substitution unit can be thereby a single character or an entire block of them. They are generally divided into four subclasses:

Monoalphabetic Substitution

Each character in the plaintext is replaced by another one in the ciphertext. Here are two examples.

Caesar Cipher: This is the simplest monoalphabetic substitution cipher, in which every character is substituted by the character three places on its right in the alphabet. So, for example, an "a" is replaced by "d", a "b" by "e" and so on. It is named after Julius Caesar who applied it to secretely communicate with his generals. The key is simply the integer by which the alphabet is shifted. A modern application can be found in the ROT13[1] ("Rotate by 13 places") system. This particular cipher is its own inverse, also called an *involution*, i.e.

[1] ROT13 originated in the `net.joke` newsgroup in the early 1980's to temporarily obscure the content of jokes which might be considered offensive, or the solution to simple puzzles. On UNIX-like machines the shell command `''tr A-Za-z N-ZA-Mn-za-m''` implements a ROT13 encryption/decryption.

applying it twice gives the original message back. Substitution ciphers can be regarded as weak encryption: since a given plaintext character is always substituted by the corresponding cipher character, the statistical distribution of the letters in the ciphertext is unchanged and a frequency analysis[2] would successfully yield the plaintext. An example of the Caesar cipher (key=3) is given in Fig. 2.2.

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	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
plaintext message	help we are under attack
ciphertext	khos zh duh xqghu dwwdfn

Figure 2.2: Example of Caesar cipher, where the cipher alphabet is shifted by three places with respect to the plaintext alphabet.

Mixed Alphabet Cipher: It relies on a more complicated way to create the cipher alphabet. Usually one writes down a keyword, omitting letters that appear twice, followed by the remaining characters and maps one alphabet into the other. Refer to Fig. 2.3 to see how it works with the keyword **"breakfast"**.

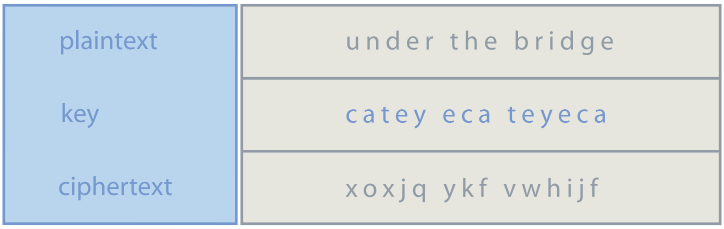
plaintext alphabet	a b c d e f g h i j k l m n o p q r s t u v w x y z
cipher alphabet	b r e a k f s t c d g h i j l m n o p q u v w x y z
plaintext message	help we are under attack
ciphertext	tkhm wk bok ujako aqqbeg

Figure 2.3: Mixed alphabet cipher at work. Notice how repeated letters in the keyword are discarded.

[2] In cryptanalysis, the study of the statistical distribution of characters or groups of characters in the ciphertext.

Polyalphabetic Substitution

This is in principle the same as the monoalphabetic case, only that two or more cipher alphabets are available for encryption. This kind of cipher has a rich history: first described by Leon Battista Alberti in 1463 in the form of discs, it became then usual practice to write it in a tableau to facilitate encryption/decryption. In particular, the so called Vigenère cipher deserves a closer look. First published in 1585 by the French diplomat Blaise de Vigenère, it was considered unbreakable until 1863, so that it earned the name of *"le chiffre indéchiffrable"*. Referring to figure 2.5, the first row of the Vigenère's table (or square) is filled with the normal alphabet, the second row, called **"cipher alphabet a"**, with the alphabet self shifted by one place, and so on until the tableau is complete. A keyword defines the mapping between two alphabets in the following way: every character in the key specifies with which particular alphabet a letter in the plaintext must be encrypted. If the key is shorter than the message, it has to be repeated. Referring to the table, with "cateye" as key, encryption works like this:



plaintext	under the bridge
key	catey eca teyeca
ciphertext	xoxjq ykf vwhijf

Figure 2.4: Example of Vigenère cipher. Encryption is performed with the help of a special look-up table, the Vigenère square.

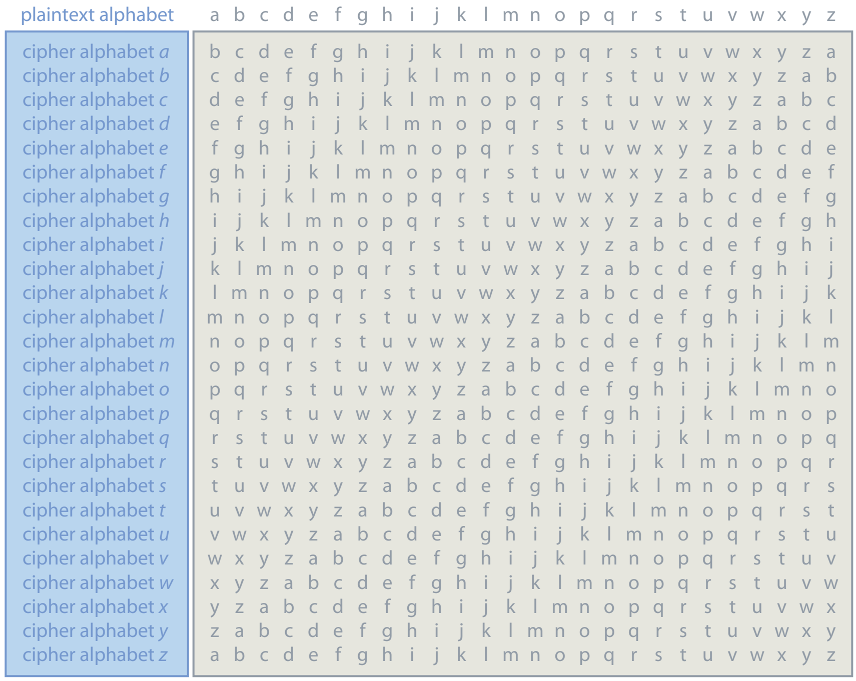
Homophonic Substitution

In this kind of substitution a single plaintext character maps to more than one symbol in the cipher alphabet. We can imagine a simple numerical substitution scheme where the letter "a" is mapped either to the numbers "24", "7" or "83", while more artistical variants can use fancy sets of symbols for encryption.

A suggestive version is the *nomenclator*[3], a hybrid mixture between a codebook[4] and large homophonic substitution tables. At the beginning only names

[3] A king's subordinate whose task was to announce the visiting dignitaries.

[4] A set of coded words (*codewords*) and their usual meanings, like a dictionary.



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

Figure 2.5: The so called Vigenère table to enable faster encryption/decryption. Every character in the key specifies with which particular alphabet a letter in the plaintext must be encrypted.

of prominent people were encoded, hence the cipher name, then the size extended to cover common words and places. Historically, this kind of cipher was employed in the Babington Plot in 1586, that aimed at murdering Queen Elisabeth I of England, and replacing her on the throne with the Catholic Mary Queen of Scotland. Encrypted correspondence between Mary and Lord Babbington was regularly intercepted and analyzed by Elisabeth I's Secretary of State Sir Francis Walsingham, who broke the code within a few months, with the help of his cipher school in London. All conspirators, including Queen Mary, were tried and sentenced to death.

Polygraphic Substitution

In such ciphers, blocks of letters (typically two, giving rise to *digraphic ciphers*) are substituted as a whole, instead of single characters. A famous digraphic method is the Playfair cipher, invented in 1854 by Charles Wheatstone and widely used by British forces during the Second Boer War and World War I and by Australians in WWII. His strength is based on the robustness against frequency analysis.

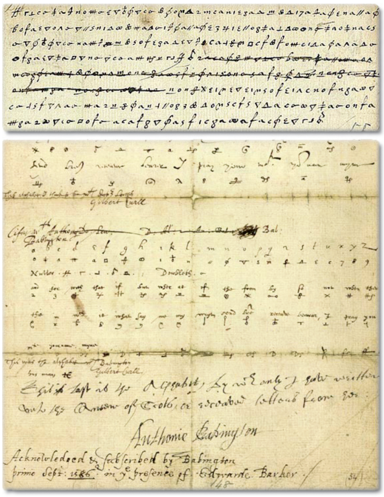


Figure 2.6: Walsingham's postscript to Mary's letter to Babington, encrypted using the nomenclator cipher. It asks Babington to reveal her the names of the conspirators using the (already broken) cipher.

Rotor Machines

In the early 1920's many electro-mechanical devices were invented to perform cryptographic tasks, thereby increasing cipher efficiency and its complexity. The basic mechanism all based on, was the **rotor**, a wired wheel with 26 different positions, each of them representing one specific alphabet permutation. The number of rotors varied from three to five on more complicated machines, while output pins of one rotor are wired to the input pins of the next, thus implementing a multiple Vigenère cipher. A famous example is the ingenious German encrypting machine called ENIGMA, invented by Arthur Scherbius and Arvid Gerhard Damm, later patented by Scherbius in the United States ("Ciphering Machine" U.S. Patent 1,657,411, 24 Jan 1928).
Commercially available from the early 20's, it was then adopted by the German Navy in 1926, by the Army in 1928 and used throughout all World War II among German forces. Though some cryptographic weaknesses, Allied could break the cipher and gain precious intelligence (codenamed ULTRA), only thanks to some accidental factors, like errors by operators, procedural flaws or captured machines and codebooks.

Figure 2.7: A picture of the Enigma encrypting/decrypting machine. This particular military model worked with three rotors.

2.7 One-time Pad

To understand how this special stream cipher works, suppose Alice wishes to send the message “under the bridge” to Bob. To do this, she first maps the alphabet to integer numbers from 0 to 25, as illustrated below.

$$\begin{array}{ccc} a & \longmapsto & 0 \\ b & \longmapsto & 1 \\ c & \longmapsto & 2 \\ & \vdots & \\ z & \longmapsto & 25 \end{array}$$

In this symmetric cipher, Alice and Bob must already share a random key, which has to be *as long as the message*. Every letter of the ciphertext is the result of a modular addition with a letter of the key. In our case the sum is carried out $mod\,26$, meaning that the remainder of the division by 26 is taken.

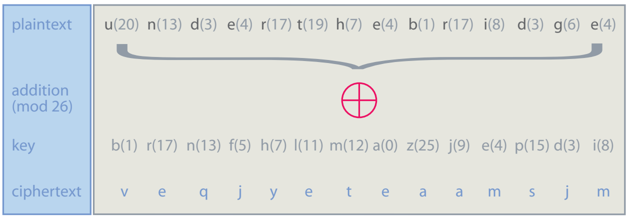

plaintext
u(20) n(13) d(3) e(4) r(17) t(19) h(7) e(4) b(1) r(17) i(8) d(3) g(6) e(4)
addition (mod 26)
key
b(1) r(17) n(13) f(5) h(7) l(11) m(12) a(0) z(25) j(9) e(4) p(15) d(3) i(8)
ciphertext
v e q j y e t e a a m s j m

Figure 2.8: One time pad encryption procedure. The algorithm works with modular addition *mod* 26. Moreover, the encryption key must be chosen randomly, as long as the message and used only once.

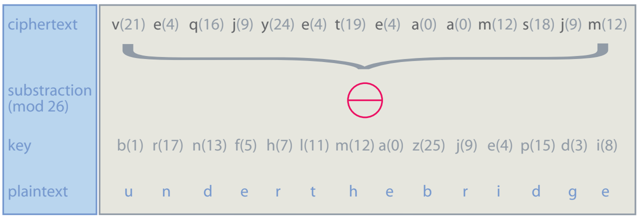

ciphertext
v(21) e(4) q(16) j(9) y(24) e(4) t(19) e(4) a(0) a(0) m(12) s(18) j(9) m(12)
substraction (mod 26)
key
b(1) r(17) n(13) f(5) h(7) l(11) m(12) a(0) z(25) j(9) e(4) p(15) d(3) i(8)
plaintext
u n d e r t h e b r i d g e

Figure 2.9: One time pad decryption procedure. The algorithm works with modular subtraction *mod* 26.

The encryption procedure is illustrated in Fig. 2.8. To decrypt the message Bob has now to carry out a modular subtraction with the same key. As expected, he gets the original message back (see Fig. 2.9).

The first algorithm of this type was realized in 1917 by Gilbert Vernam (of AT&T), and is called after him **Vernam Cipher**, later patented (U.S. Patent 1,310,719).
In this first implementation each character of the message was electrically combined with a character on a long punched strip of paper. Shortly thereafter, Captain Joseph Mauborgne recognized that, if the characters on the paper tape key were random, it should be much more difficult to break the cipher.
In fact, the Vernam-Mauborgne cipher, commonly known as the **one-time pad**, takes up a special place in the field of cryptography since the late 40's, when Claude Shannon published a paper [Sha48], in which he proved its *perfect secrecy* (his terminology). In his formulation this property is equivalent to say that the information about the plaintext contained in the ciphertext is zero, thus meaning that **all plaintexts are equally probable**. This can be understood with the help of an example. Assume one has to encrypt the message APPLEPIE with the random key JTHSZCRE; the ciphertext is the sequence JIWDDRZI. Decrypting with the right key leads of course to the original message, but if we try to decrypt with the key IXCZZTVQ, this gives us the plaintext BLUEEYES. Analogously, with the key EOLSRDLV we get the plaintext FULLMOON. Since the key has been chosen randomly, all keys

are equally probable, which in turns means that all possible plaintexts are same likely. Hence the cryptanalyst has no chance to get the right plaintext out of the ciphertext, no matter how much computational power he has.
Despite this unique feature, the requirements for the one-time pad are very hard to achieve in practice. These requirements all regard the **key**:

1. It has to be **random**.
2. It must be of the **same length as the message**.
3. It can be **used only once** (hence "one-time").
4. It has to be **safely conveyed** from one party to the other and kept secret by both.

Problems with One-time Pad

Some major drawbacks make a real-world implementation of the one-time pad difficult.
If one wishes to send a very large amount of data, he/she should also have a random key of the same length at his/her disposal. The second problem is that computer built-in random number generators (RNG) are not able to produce "real" random numbers, so a computer based algorithm that claims to implement a one-time pad encryption, actually provides "only" a Vernam cipher.[5] Moreover, and this turns out to be the hardest problem, being a symmetric cipher, there must be some secure way to transport the key from Alice to Bob and to safely store it. Unfortunately, it can be shown that in the "classical" world such means does not exist, i.e. **classical key distribution is not secure.** We will see in the next section that quantum cryptography provides a new approach to solve the problem.

2.8 Modern Cryptography

For this section, we mainly refer to the excellent book on classical cryptography by B. Schneier [Sch96]. Until now, we were dealing with character-based cryptography, while computer-based algorithms can only manipulate streams of binary information. It is simple to guess how these two concepts meet: think for example of the ASCII code, which maps 95 printable characters into the binary numbers between 32 and 126; so from now on, we can think of a bit pattern as being equivalent to letters or numbers.

[5] Nevertheless, true RNG based on quantum mechanics exist.

In the early 70's the research in the field of cryptography was mostly confined in some top secret military projects promoted by governments involved in the Cold War; as a consequence, almost no research papers about this topic were published. Small companies were developing cryptographic products and selling them, mostly to overseas governments, but nobody could independently certify whether those systems were really secure, not to mention compatibility matters.
In 1974 the National Bureau of Standards (NBS), now National Institute for Standards and Technology (NIST), issued a public call for proposals regarding the introduction of a standard cryptographic algorithm. A promising candidate was identified in a follow-up version of an algorithm developed at IBM some years earlier, called Lucifer. It was the first step towards a standardization of computer-based cryptography, that ended up in 1977 with the publication of the Data Encryption Standard (DES), the undisputed symmetric encryption algorithm over twenty years.

2.8.1 Symmetric Key Algorithms: DES and AES

DES is a symmetric block cipher, manipulating data in 64-bit long pieces. It has a 56-bit long key, usually expressed as a 64-bit number, thereby ignoring the least significant bit of every byte, used as parity check. The plaintext is first subdivided into 64-bit long blocks. Every block undergoes an initial permutation (IP), then is broken into a left (L_0) and a right (R_0) half, each 32-bit long. At this point the first iteration of the function F[6], in which the key is involved, is applied to R_0. The output of the F function is now XORed with L_0 and the result becomes the new right half, while R_0 becomes the new left half. The application of F, the XORing operation and the final swapping constitute a so called **round**. DES algorithm performs a total of 16 rounds. If B_i is the output of the i-th round, L_i and R_i its left and right half respectively, then a round looks like:

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus F(R_{i-1}, K_i) \, , \end{aligned}$$

where K_i is a piece of information obtained by compressing and permuting the original key. At the end the two blocks are brought together and the inverse of the initial permutation (IP^{-1}) completes the algorithm. A schematic diagram of how DES works is depicted in Fig. 2.10.

[6] From Horst Feistel, one of the developers of Lucifer

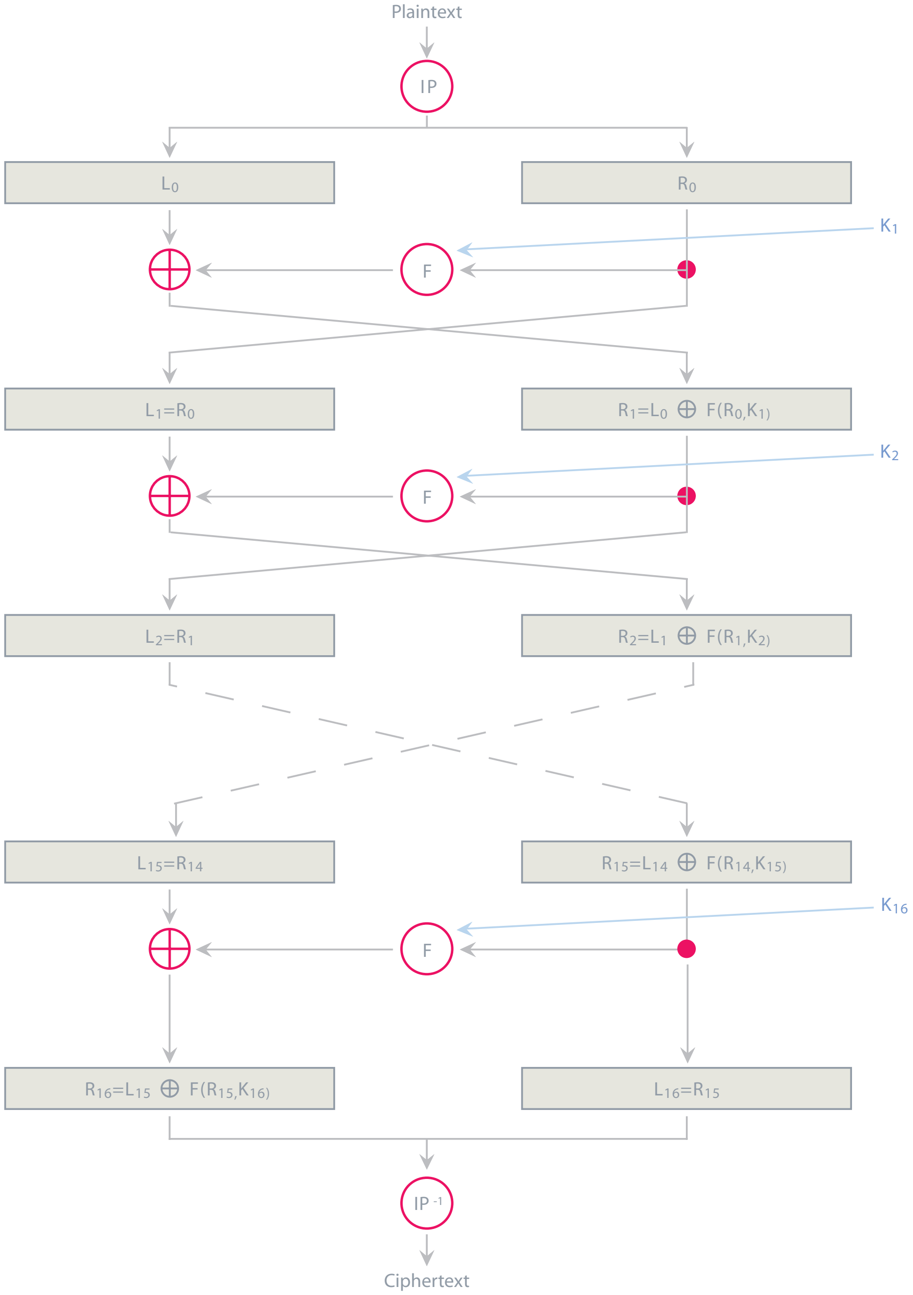


Figure 2.10: Schematical diagram of the DES encrypting algorithm. It performs a total of 16 round, every round consisting of the application of the function F, the XOR operation and the swapping procedure.

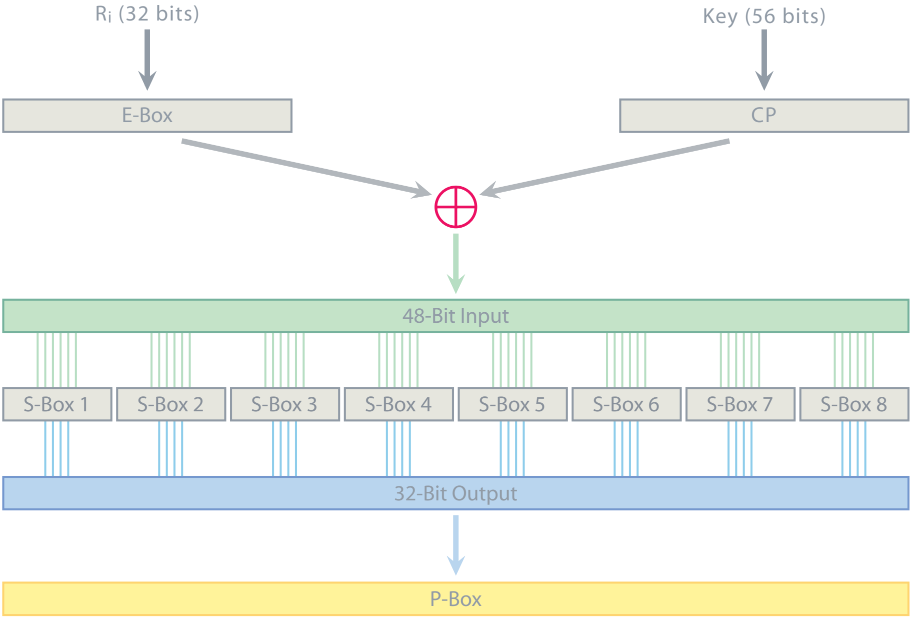


Figure 2.11: The F function of the encrypting DES algorithm. Refer to the text for implementation details.

The Feistel Function

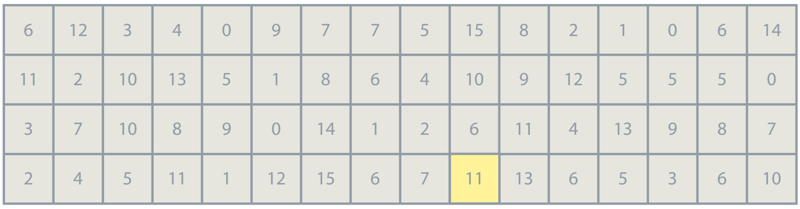
The core of DES resides in the implementation of the F function. Referring to figure 2.11, it works like this:

Step 1: The Compression Permutation
For each of the 16 rounds, a different 48-bit subkey has to be generated. First, the key is split up into two 28-bit halves, which then undergo a circular permutation by either one or two bits, depending on the round number. At this point 48 out of 56 bits are randomly selected, building up the subkey K_i for the i-th round.

Step 2: The E-box Permutation
This process expands the right side R_i to 48-bit length by cloning some of the bits. Now, the expanded right hand side $(E(R_i))$ is as long as the subkey.

Step 3: $\mathbf{E(R_i) \oplus K_i}$
In this step the modified right half is XORed with the i-th subkey.

Step 4: The S-box Substitution
The 48-bit long result from the previous step gets divided into 8 subblocks each 6-bit long. Each sub-block passes through a corresponding S-box, and



6	12	3	4	0	9	7	7	5	15	8	2	1	0	6	14
11	2	10	13	5	1	8	6	4	10	9	12	5	5	5	0
3	7	10	8	9	0	14	1	2	6	11	4	13	9	8	7
2	4	5	11	1	12	15	6	7	11	13	6	5	3	6	10

Figure 2.12: Look-up table for S-box substitution. There are 8 S-boxes like this for every round of DES encryption. Notice that raws and columns are indexed beginning from 0.

gets substituted with a 4-bit number, so that the overall output is shrank to 32-bit again. To illustrate how a S-box works consider the following example: assume the entry of the sixth S-box is the 6-bit sequence `110011`. The first and last bit form the number 3 (`11` in binary), the middle 9 (`1001` in binary); according to the lookup table in Fig. 2.12, the number at place (3,9) provides the output for the 6-th sub-block, which is `1011` (11 in decimal notation).

Step 5: The P-box Permutation
The 32-bit output from the S-box step undergoes a permutation, according to a P-box, which maps every bit position into a new one.

DES decryption process works reversing the whole procedure, i.e. it begins from the bottom of Fig. 2.10 and moves upwards. All encryption mappings are replaced by their inverses.

On December 30, 1993 DES was confirmed by the National Security Agency (NSA) as government encryption standard for unclassified information in the United States for the third time. Seven years later, DES was publicly broken in a little bit more than 22 hours (see section 2.8). Nevertheless, DES was reconfirmed in October 1999 for the fourth time, recommending the use of Triple-DES, made up of three successive DES encryptions with three different keys (total key length 168 bits), where the output of a simple DES run is used as input for the next one. Still, security could not be ensured any further, so that on November, 26 2001, after a five year selection process, the *Advanced Encryption Standard* (AES) was published. AES, also known as Rijndael[7] algorithm, is a block cipher as well, working on 128-bit long data chunks, with a key size of 128, 192 or even 256 bits. In June 2003 NSA announced that AES could be used for encrypting classified information with the following recommendation: 128, 192 or 256 bit key-length for "secret" information, 192 or 256 bit for "top secret" information.

[7] Portmanteau from the names of its inventors, the Belgian Joan Daemen and Vincent Rijmen.

2.8.2 Asymmetric Algorithms

In 1975[8], Whitfield Diffie and Martin Hellman, and independently Robert Merkle [Mer78][9] have been playing a leading role in a revolution in the field of cryptography [DH76]. They presented the idea of *public-key cryptography* in which two different keys, one for encryption and one for decryption, are involved. The encryption key is made public, so that anyone can encrypt his message, while the decryption (private) key has to be kept secret. The scheme is based on a **trapdoor one-way function**. This is a special one-way function, $f(x)$, which can be easily inverted as soon as one knows a secret (trap-door) y. Assume now that Alice wishes to share a secret with Bob; what they have to do is:

1. They agree on a public-key cryptosystem.
2. Bob sends Alice his public key.
3. Alice encrypts her message using Bob's public key.
4. Bob decrypts Alice's message using his private key.

Notice how this scheme completely overcomes the problem of the key exchange: no prior agreement on a secret key between Alice and Bob is needed. On the other hand, the security relies on the assumption that an eavesdropper has not enough computational power to deduce the private key from the public key within a reasonable period of time.

RSA

The most widely used and well understood public-key cryptosystem is the one proposed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977 at MIT, named after the three inventors' initial letters, RSA. Patented by MIT in 1983, (U.S. Patent 4,405,829, expired in September 2000), RSA relies on the computational difficulty of factoring large integers. For an eavesdropper, recovering the plaintext from partial knowledge of ciphertext and public key, is equivalent to being able to factor the product of two prime numbers. **Producing the two keys** involves prime numbers and modular arithmetic and can be summarized in the following steps:

1. Choose two random large prime numbers p and q of approximately the same size.

[8] In 1997 it was disclosed that the basic ideas of public-key cryptography were actually invented in the late 60's by researchers at GCHQ, a British intelligence agency.

[9] Because of a sluggish publication process, Merkle's papers on the subject were published only two years later, when the Diffie-Hellman algorithm was already widely known.

2. Compute the product $n = pq$
3. Choose randomly an encryption key e such that e and q are relatively prime.
4. Use the **extended Euclidean algorithm** (see Appendix A) to compute the decryption key:

$$\begin{aligned} ed &\equiv 1\, mod\, (p-1)(q-1) \qquad \text{or equivalently} \\ d &= e^{-1}\, mod\, (p-1)(q-1)\ . \end{aligned}$$

The public key is the pair (e, n), while d is the private key. The original primes p and q are no longer needed.

To **encrypt** a message m, one first splits it into smaller pieces which size is not larger than n. Let m_i be such a piece; then the corresponding encrypted text c_i is obtained according to the formula:

$$c_i = {m_i}^e\, mod\, n$$

Decryption works similarly. To get back the original partial message m_i, just compute:

$$m_i = {c_i}^d\, mod\, n\ .$$

Notice that reversing the role of public/private key, i.e. performing encryption with d and decryption with e, works as well.

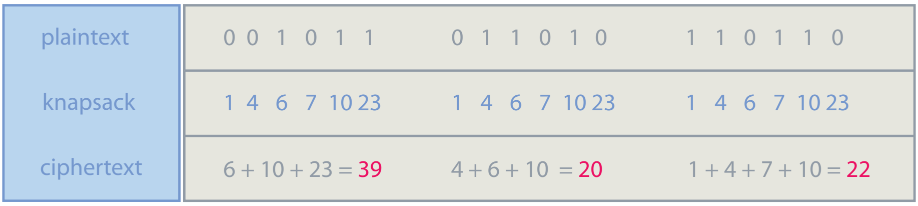
Public key cryptosystems such as RSA, find a useful additional application in so called **digital signature** processes, originally proposed also by Diffie and Hellman. Imagine Alice wants to sign a digital message and send it to Bob. The protocol is fairly simple:

1. Alice encrypts the message with her private key, *"signing"* the document.
2. She sends the signed message to Bob.
3. Bob decrypts the message with Alice's public-key.

With this procedure, what one is guaranteed of, is: the **authenticity** of the message (provided step 3 works); that the signature is **unforgeable** (the only one who is in possess of the private key is Alice, so she actually did sign); that the message has not been altered (if so, decryption would fail).

Other Public-Key Algorithms

Knapsack: This was the first algorithm for public-key encryption, developed by Ralph Merkle and Martin Hellman. It is named after the knapsack problem: given a pile of items with different weights, which items should be put into the knapsack so that the knapsack weighs a certain amount? Formally, given the values $W_1, W_2 \ldots, W_n$ and a sum S, find $b_1, b_2 \ldots, b_n$ such that $S = b_1W_1 + b_2W_2 \ldots + b_nW_n$, thereby being the values of b_i either 1 (item is in the knapsack) or 0 (item is not in the knapsack). How is this correlated to encryption? A bitwise plaintext (a sequence of 1's and 0's), corresponding to b values, combines with a knapsack to give a sum (ciphertext).



plaintext	0 0 1 0 1 1	0 1 1 0 1 0	1 1 0 1 1 0
knapsack	1 4 6 7 10 23	1 4 6 7 10 23	1 4 6 7 10 23
ciphertext	6 + 10 + 23 = 39	4 + 6 + 10 = 20	1 + 4 + 7 + 10 = 22

Figure 2.13: The knapsack encryption algorithm. The plaintext is a sequence of b values (see text), the public key is the hard knapsack. Its solution constitutes the plaintext.

Actually there are two kinds of knapsack problems, one solvable in linear time (”easy“ problem) and one which time complexity is exponentially increasing (”hard“ problem, see section 2.8.1). The easy knapsack can be readily modified to create the hard knapsack (but one cannot go the other way around), producing the private/public “key” pair: the public key is the the hard knapsack, the private key the easy problem. If one doesn't know the private key, he has to solve the hard problem.

ElGamal: This scheme can be used for both encryption and digital signatures. The basic idea is the computational difficulty of calculating discrete logarithms modulo a number. Generating a key pair works like this: choose a prime p, two random numbers g and x, with $x, g < p$, then compute $y = g^x \, mod \, p$. The public key is y, g and p, the private key is x.

Elliptic Curves: This field has been extensively studied for many years. In 1985 Neal Koblitz and V.S. Miller proposed independently to use them for public-key encryption. They produced no new algorithm, just implemented existing ones with elliptic curves over a finite field. It can be shown that they have all nice properties of finite fields but they offer more robustness with respect to cryptanalysis.

2.8.3 Hybrid Cryptosystems

In real-world implementations public-key algorithms are rarely used to encrypt and send messages, unless they are very short. This is the consequence of two facts:

- Public-key algorithms are about 1000 times slower than symmetric algorithms.
- Public-key cryptosystems are weak against chosen-plaintext attacks. If the cryptanalyst has the ciphertext C and knows that the plaintext P stems from a set with n possible plaintexts, he has to carry out at most n encryptions (he can do it, the encryption key is public), until he gets $C = E(P)$[10].

To overcome such handicaps public-key cryptography is actually used to securely distribute **session keys**, which are then used to encrypt confidential traffic. This kind of protocol is called a **hybrid cryptosystem**. Here is how it works:

1. Bob sends Alice his public key.
2. Alice encrypts a randomly generated session key K with Bob's public key $E_B(K)$ and sends it to Bob.
3. Bob recovers K using his private key, i.e. he performs $D_B(E_B(K)) = K$
4. They encrypt their messages with the same session key.

An example of such a scheme is used in the remote login UNIX utility SSH-x (Secure Shell version x). Version 2 uses RSA for client/server authentication procedure and initial key exchange, while the AES algorithm, with 128-bit key length, encrypts the data-flow.

2.9 Security

In this section, we try to answer the question how safe is the cryptography relying on classical information theory. Beforehand we need some notions of computational complexity theory, which allow us to define what the terms easy/hard mean from the algorithmic point of view.

[10] For example if P represents a sum under 1000000 €, then $n = 10^6$ and the attack would work.

2.9.1 Computational Complexity

In complexity theory, the computational complexity of an algorithm is determined by two parameters: T (for **time complexity**) and S (for **space complexity**, i.e. memory requirements). Both variables are expressed as a function of n, the size of the input. Usually, only the order of magnitude of the (time or space) complexity function is given; this corresponds to the term in the function which grows the fastest as n becomes large [11].

Algorithms classification is made according to their time or space complexity. A **constant** algorithm has a complexity function independent of n, i.e. $\mathcal{O}(1)$. An algorithm is **linear** if its complexity grows as $\mathcal{O}(n)$. If the complexity function is of order $\mathcal{O}(n^m)$, where m is a constant greater than 1, then the algorithm is classified as **polynomial** (or **P-time** problem). Algorithms which complexity is of order $\mathcal{O}(a^{f(n)})$, where a is a constant greater than 1 and $f(n)$ is a polynomial function of n, belong to the **exponential** class. A special subset of the latter are superpolynomial algorithms, whose complexity behave like $\mathcal{O}(c^{f(n)})$, where c is a constant and $f(n)$ is more than a constant but less than linear. Given these complexity classes, we can define a problem to be **tractable** (or **easy**) if the algorithm for solving it is of polynomial complexity. A problem will be intractable (or **hard**), if the solving procedure belongs to a complexity class which is more than polynomial. Obviously, a cryptographer would aim at designing his system in such a way, that the best algorithm at eavesdropper's disposal is of exponential type. Unfortunately, the best statement that can be made, in the light of state of the art complexity theory, is that all known cracking algorithms are of superpolynomial time complexity. Furthermore, there is no guarantee that no polynomial-time algorithms could ever be discovered in the future.

2.9.2 Successful Attacks

As computational power increases, tasks which seemed inconceivable only some years ago, become a mere question of a few hours calculation. So, while Ron Rivest estimated the time it would take to factor a 125-digit number in at least 40×10^{15} years (one million time the age of the universe), seventeen years later, in 1994, a network of 1600 computers accomplished this in 8 months.

And things got even worse. In February 1999, 185 machines factored a 465-bit RSA number in 9 weeks, followed by the successful task of factoring a 512-bit number, achieved by 292 machines six months later. Furthermore an optoelectronic parallel factoring device called TWINKLE, proposed by Shamir in 1999

[11] This choice ensures that the complexity estimation is system-independent, because it neglects terms of lower order which may result depending on the particular implementation.

and estimated to be three orders of magnitude faster than a conventional PC, could break 512- or 768-bit keys even more easily. Today recommended key lengths vary from 2048 to 4096 bits. Regardind symmetric algorithms, things don't look much better. In 1997 RSA Data Security Inc., issued the first challenge to test DES strength. A team (the DESCHALL project) led by Rocke Verser, Matt Curtin, and Justin Dolske, got the plaintext after **brute force attack** on the whole keyspace of 2^{56} possible keys, after 96 days. In 1998 a group called Electronic Frontier Foundation (EEF), built a 250.000$ DES-cracker in which more than 50000 CPU's were linked together, finding the key after 41 days. In the challenge in January 1999 the two previous winners joined their efforts to find the key after 22 hours and 15 minutes, with an enormous key testing rate of 245 billion keys per second. Not only brute force attacks are an efficient aid for codebreakers. So called **side-channel attacks** exploit the analysis of parameters related to the implementation of the algorithm, such as elapsed time to carry out some particular operations, machine power consumption, or even heat radiation and electromagnetic emanation, to gain enough knowledge to crack the system. As of 2006, the only successful attacks against AES were side-channel attacks based on CPU's cache-timing analysis [OST05]. Furthermore, the outstanding research field of quantum computers promises a dramatic reduction of algorithm complexity, making Gilles Brassard's words *"If a quantum computer is ever build, much of the conventional cryptography will fall apart"*, much more than a pessimistic forecast.

3 Quantum Cryptography

3.1 Introduction

As seen at the end of the previous chapter, many real-world threats no longer ensure the security of current cryptosystems against codebreakers' attacks who have at their disposal enough computational power (and enough money). The idea to exploit quantum mechanical principles for cryptographic tasks dates back to the early seventies and can be found in the works of Stephen Wiesner, later at Columbia University, Charles H. Bennett of IBM and Gilles Brassard at University of Montréal.
Their papers laid a milestone of a forthcoming revolution in the field of security-based applications, which for the first time directly involves quantum mechanics as fundamental aid.

Recall that the sticking point in the one-time pad scheme is that there is no classical way in which two parties can safely exchange the key. Quantum cryptography offers a new approach to overcome the key distribution problem. For this reason, Quantum Cryptography is more precisely referred to as **Quantum Key Distribution/Growing** (QKD/G).

Unlike computational secure cryptography, theoretical analysis of quantum cryptographic implementations sets aside the question about computational power at one's disposal or even knowledge of more efficient algorithms. This is the prerequisite for **unconditional security**. Quantum cryptography based communication makes use of the outstanding concept that **eavesdropping can be detected**. Hence a trusted party is now in the position to establish whether the information exchange occurred under safe conditions or not.

The joining of state-of-the-art optical technologies and analysis software provides with a variety of schemes for the implementation of new secure communication protocols based on quantum cryptography.

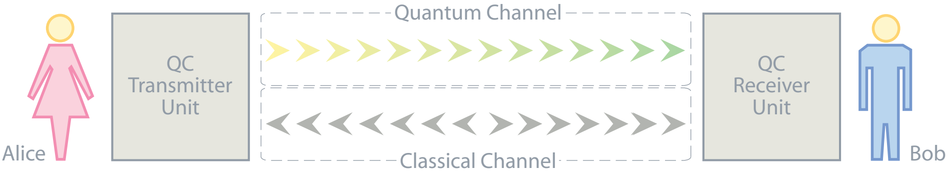


Figure 3.1: Alice can secretely communicate with Bob using an additional trusted quantum channel and a classical channel. The key-exchange procedure occurs through the quantum channel. Once the quantum transmission is over, they check whether the key is secure and, if so, they can use it to encrypt confidential data through the classical channel.

Provided Alice and Bob previously share a short secret key, which serves as initial authentication against **man in the middle attack**[1], QKG protocols yield unlimited secret-key growing. Expanding the classical key distribution scheme with a further communication channel, the typical scenario we are dealing with is depicted in Fig. 3.1.

3.2 Quantum Mechanical Background

3.2.1 Qubits

The fundamental unit, classical information theory works with, is the **bit** (binary digit); as is generally known, the bit can have two values, either 1 or 0. We can implement a bit like a switch: it can be either $on \equiv 1$ or $off \equiv 1$, each corresponding to two different physical states (e.g. voltage or current levels). In quantum information theory, the corresponding unit is the **qubit**[2] (quantum bit), an arbitrary superposition of two orthogonal basis vectors of a two dimensional complex Hilbert space.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \alpha, \beta \in \mathbb{C} \tag{3.1}$$

With the usual normalization constraint $|\alpha|^2 + |\beta|^2 = 1$, such that equation 3.1 can be turned into:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \, , \tag{3.2}$$

[1] An eavesdropping strategy in which Eve pretends to be Bob for Alice and vice versa.

[2] In the case of a three dimensional Hilbert space, the pure state is called *qutrit*, in the d-dimensional case, *qudit*.

where overall phase shifts have been neglected. An useful representation of such a **pure** qubit state makes use of the so called **Bloch sphere** (Fig. 3.2). This is a unit sphere; the qubit vector is represented by the cartesian coordinates $(\cos\phi\sin\theta, \sin\phi\sin\theta, \cos\theta)$, which build the **Bloch vector**.
Summarizing, we can state that the crucial property of a pure qubit is that, unlike a classical bit, its state can be any superposition of $|0\rangle$ and $|1\rangle$.

Practical Realization of Qubit States

Generally speaking, any two-level quantum mechanical system can be considered as a qubit. This allows us to treat all these systems equivalently, so the same formalism applies for an electron in a two-level atom as well as for the spin of a particle, or the polarization of a photon. Measurements in a two-level system can be represented by the three Pauli matrices, σ_x, σ_y, σ_z. Their corresponding eigenvectors build three different bases represented on the Bloch sphere (Fig. 3.2). If $|\uparrow\rangle$ and $|\downarrow\rangle$ are the two eigenstates of the σ_z operator, corresponding to the eigenvalues ±1, then the mapping

$$\begin{array}{ccc} |\uparrow\rangle & \longmapsto & |0\rangle \\ |\downarrow\rangle & \longmapsto & |1\rangle \end{array}$$

points up the equivalency between any two level system and a qubit state. In the relevant case that the qubit is represented by a **polarized photon**, the eigenstates of σ_z with eigenvalues ±1 are denoted with $|H\rangle$ (for horizontal polarization) and $|V\rangle$ (for vertical polarization), respectively. Further, eigenvectors of σ_y are denoted $|+\rangle$ (rotated by +45° with respect to $|H\rangle$) and $|-\rangle$ (rotated by −45° with respect to $|H\rangle$). Finally, those of σ_x, are denoted $|R\rangle$ (rightwise circularly polarized) and $|L\rangle$ (leftwise circularly polarized). The transformation rules from one basis to the other are listed below:

$$\bigoplus \begin{cases} |H\rangle = (|+\rangle - |-\rangle)/\sqrt{2} \\ |V\rangle = (|+\rangle + |-\rangle)/\sqrt{2} \end{cases}$$

$$\bigotimes \begin{cases} |+\rangle = (|V\rangle + |H\rangle)/\sqrt{2} \\ |-\rangle = (|V\rangle - |H\rangle)/\sqrt{2} \end{cases}$$

$$\{|R\rangle, |L\rangle\} \begin{cases} |R\rangle = (|V\rangle + i|H\rangle)/\sqrt{2} \\ |L\rangle = (|V\rangle - i|H\rangle)/\sqrt{2} \end{cases}$$

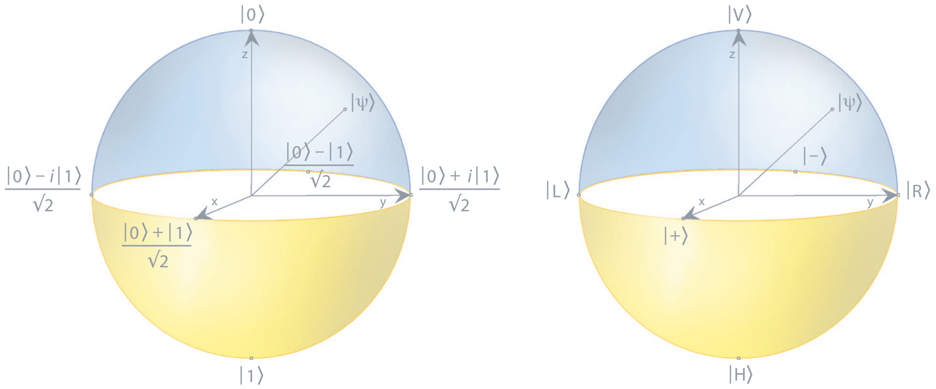


Figure 3.2: Bloch (left) and Poincaré (right) sphere. Any general pure qubit state can be represented by a point on the surface of the Bloch sphere. If the qubit is the polarization state of a photon, then the Poincaré sphere is used. On both spheres, the two equatorial conjugated bases and the polar computational basis can be identified.

The pair $\{|H\rangle, |V\rangle\}$ is called **computational basis**, while $\{|+\rangle, |-\rangle\}$ and $\{|R\rangle, |L\rangle\}$ are the two **conjugated bases**[3]. In the special case of the polarized photon, the sphere to represent the qubit is essentially the same as the Bloch sphere and is called the **Poincaré sphere** (Figure 3.2)

3.2.2 No-go Theorems

This is a series of no-knowledge principles which directly descend from the probabilistic nature of quantum mechanics. This unavoidable intrinsic ignorance builds the basis for eavesdropping detection schemes implemented in every quantum cryptographic protocol.

Non-Distinguishability of Non-Orthogonal States

Two quantum mechanical states, $|\psi\rangle$ and $|\phi\rangle$, are said to be non-orthogonal if their inner product is not zero; in Dirac's notation:

$$\langle\psi|\phi\rangle \neq 0\,. \tag{3.3}$$

[3] In a N dimensional Hilbert Space two bases are said to be conjugated if the projection of every basis vector of one basis onto the other equals $\frac{1}{\sqrt{N}}$.

Moreover, in quantum mechanics any measurement can be represented by a Hermitian operator, the possible outcomes of the measurement corresponding to its eigenvalues. The special feature of non-orthogonal states can be expressed by the following

Theorem 1. *There exists no measurement which can deterministically distinguish between two non-orthogonal states.*

Proof. The proof is indirect: assume $|\psi\rangle$ and $|\phi\rangle$ are non-orthogonal and let M be any measurement (Hermitian operator) such that:

$$\begin{aligned} M|\psi\rangle &= m_\psi|\psi\rangle && (3.4) \\ M|\phi\rangle &= m_\phi|\phi\rangle && (3.5) \end{aligned}$$

with $m_\psi \neq m_\phi$, i.e. the states $|\psi\rangle$ and $|\phi\rangle$ can be unambiguously distinguished through the measurement M. At this point let's compute the following:

$$\begin{aligned} \langle\phi|M|\psi\rangle = \langle\phi|\left(M|\psi\rangle\right) = m_\psi\langle\phi|\psi\rangle && (i) \\ \langle\phi|M|\psi\rangle = \left(\langle\phi|M\right)|\psi\rangle = m_\phi\langle\phi|\psi\rangle && (ii) \end{aligned}$$

where, in the second equality of Eq. (ii), we used the fact that $M^\dagger = M$ and that all eigenvalues are real. Let's calculate:

$$(i) - (ii): \quad 0 = (m_\psi - m_\phi)\langle\psi|\phi\rangle\ .$$

But this result in a contradiction, since, having assumed $m_\psi - m_\phi \neq 0$, we must have

$$\langle\psi|\phi\rangle = 0\ .$$

↯

If we look at the strucure of our basis vectors in the polarization space, we can immediately argue that there is no measurement which can deterministically distinct a photon in the state $|H\rangle$ from one in the state $|+\rangle$ or $|-\rangle$.

No-Cloning Theorem

To overcome the previous limitation, a possible ploy one could think of, could be to make a perfect copy of the system under measurement. This would give the possibility of performing a measurement in **both** polarization bases, thus leading to a deterministic outcome in almost one case. (Un)fortunately, again a fundamental theorem limits the amount of information which can be gained about non-orthogonal quantum states. It was stated in 1982 by Wootters, Zurek [WZ82] and Dieks [Die82] and, despite its simplicity, it builds the pillar for quantum cryptography to work, as it prevents any eavesdropper from getting a duplicate of potential key bits. It reads as follows:

Theorem 2. *It is not possible to create a perfect copy of an unknown quantum mechanical state.*

Proof. Suppose there exists a quantum copying machine consisting of two parts: a *data* slot and a *target* slot. The data slot contains the unknown but pure quantum state to be copied, $|\psi\rangle$, while the target slot is initially in some pure state $|s\rangle$. Thus, the machine initial state is:

$$|\psi\rangle \otimes |s\rangle \; . \tag{3.9}$$

To get a copy of $|\psi\rangle$ in the target slot, we let a unitary operator act on the initial state, i.e.:

$$|\psi\rangle \otimes |s\rangle \xrightarrow{U} U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \; . \tag{3.10}$$

Suppose this procedure works for two **non-orthogonal** states $|\psi\rangle$ and $|\phi\rangle$, i.e.:

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{3.11}$$

$$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle \tag{3.12}$$

Computing the inner product of the two expressions yields:

$$\begin{aligned} \langle\psi|\langle s|\underbrace{U^\dagger U}_{\mathbb{1}}|\phi\rangle &= \langle\psi|\langle\psi|\phi\rangle|\phi\rangle \\ \Rightarrow\langle\psi|\phi\rangle &= (\langle\psi|\phi\rangle)^2 \; . \end{aligned}$$

So either $|\psi\rangle = |\phi\rangle$ or $\langle\psi|\phi\rangle = 0$. ↯

Thus, a quantum cloning machine can only copy states which are orthogonal to each other, hence there is no general cloning device for quantum states. This holds in particular for the polarisation states defined in the previous section: since $\langle H|\pm\rangle = 1/2 \neq 0$ any attempt to clone any of the states $|\pm\rangle$, $|H\rangle$, $|V\rangle$ won't work perfectly.

Though the impossibility of getting a perfect copy of the system, some special devices, called quantum cloning machines (QCM), have been investigated, particularly in [GM97], [BEM97] and in the excellent review article [SIAG05]. This kind of setups can perform an **approximate** cloning procedure, both for finite and infinite dimensional Hilbert spaces. As universal cloning process, Gisin and Massar consider a state-independent QCM, in which the input state is an unknown pure qubit on the Poincaré sphere $|\psi\rangle = \cos\frac{\theta}{2}|\uparrow\rangle + e^{i\phi}\sin\frac{\theta}{2}|\downarrow\rangle$.

The figure of merit, or fidelity, for the process is the overlap between any of the copies and the input state, and can be expressed as:

$$\mathcal{F} = \int \langle\psi|\rho_{out}|\psi\rangle \, \mathrm{d}\,\Omega \,. \tag{3.13}$$

where $\rho_{out}(\theta, \phi)$ is the reduced density matrix of one of the copies and $\int \mathrm{d}\Omega =$ $= \int_0^{2\pi} \mathrm{d}\phi \int_0^{\pi} \mathrm{d}\theta \sin\theta/4\pi$. In the case that N identical qubit states are taken as input, and we wish to get $M > N$ identical copies as output states, they found a closed form for $\mathcal{F}$:

$$\mathcal{F}_{N,M} = \frac{M(N+1)+N}{M(N+2)} \,. \tag{3.14}$$

This gives an upper bound to how "good" our cloning trial can be. For the relevant case of an eavesdropping attack, where Eve is attempting to create two copies ($M = 2$), from one unknown qubit state ($N = 1$), the fidelity assumes the value of 5/6.

3.3 Quantum Entanglement and Bell's Theorem

Entanglement is perhaps the most astonishing feature arising in the quantum world. A wide class of QKD protocols exploits entanglement of quantum mechanical systems to achieve secure communication [BBM92], [Eke91]. Formally, two or more quantum states are said to be **entangled**, if the global state cannot be expressed as a tensor product or a statistical mixture of tensor products of any quantum states of the individual systems.

This definition is responsible for one of the most exciting discussions on the foundations of quantum mechanics, initiated in 1935 by a famous research paper by Einstein, Podolsky and Rosen [EPR35]. In that article, they formulated a Gedanken Experiment, known as the EPR paradox, which was later adapted by Bohm [Boh51] to better fit into an experimental setup. In that modified version (referred to as EPRB paradox), two entangled particles (e.g. electrons), e_A and e_B, are emitted from a source[4]. The particles e_A and e_B are then sent to Alice and Bob respectively, who perform a spin measurement along the z axis[5] on their particle.

[4] After that, a source that produces entangled particles is called an EPR source.

[5] The choice of the measurement direction is arbitrary. Any other choice doesn't affect results.

Before any measurement is performed, the global wave function for the system $e_A + e_B$ is described by the following superposition state:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}} \left(|\uparrow\rangle_A \, |\downarrow\rangle_B - |\downarrow\rangle_A \, |\uparrow\rangle_B \right) , \tag{3.15}$$

where subscript A and B refer to the particle measured by Alice and Bob respectively and $|\uparrow\rangle$, $|\downarrow\rangle$ are eigenstates of the Pauli matrix σ_z. According to quantum mechanics, after Alice has performed her spin measurement, the wave function collapsed either on $|\uparrow\rangle_A \, |\downarrow\rangle_B$ or on $|\downarrow\rangle_A \, |\uparrow\rangle_B$ state. Hence, in the case she obtained the measurement result spin up, Bob will measure spin down particle with 100% probability, while if she measured spin down, Bob's result will be spin up.

This conclusion is quite amazing: it seems that a measurement on one side could instantaneously[6] determine the result of a measurement far away in space.
These implications and the Copenhagen interpretation of these results were unacceptable for Einstein, Podolsky and Rosen. To express his position, Einstein liked to say that the moon is "out there" even if no one is observing it. In order to preserve the local realistic description of the physical world[7], Einstein Podolsky and Rosen concluded that quantum mechanics cannot be a complete theory. In other words, there must be some more general theory for the description of objects in the real world, to which quantum mechanics acts only as a statistical approximation. Hence, the complete theory must contain some **local hidden parameters**, corresponding to the elements of physical reality. Such a theory is called a **local hidden variable (LHV) theory**.

In 1964 John S. Bell [Bel64] showed that *no local realistic hidden variable theory can reproduce all predictions of quantum mechanics.* Therefore he derived a mathematical formulation in the form of inequalities (known as *Bell's inequalities*), which must be satisfied by any local realistic theory, but are violated by quantum mechanics under certain conditions.
To illustrate Bell's idea, consider the two measurement outcomes $A(\mathbf{n}_1)$ and $B(\mathbf{n}_2)$ of Alice and Bob, which according to quantum mechanics can take the values $+1$ (spin up) and -1 (spin down) for the state in Eq. 3.15.
The unit vectors $\mathbf{n}_1$ and $\mathbf{n}_2$ denote the direction of the spin measurement for the variable A and B respectively. Moreover, according to locality, the value of A depends only on $\mathbf{n}_1$ and that of B only on $\mathbf{n}_2$ and not on the orientation

[6] Though, measurement on an entangled state does not violate the causality principle, because Alice' information about her result can still not be conveyed faster than light. Moreover the result of a single particle measurement is always with equal probability up or down.

[7] Einstein could not accept the idea that God plays dice with the world

of the other observer's detector. In a LHV theory randomness of outcome A and B is due to the statistical distribution of the unknown set of parameters λ (prerequisite for reality), which can be common for both particles. Bell's inequality, in the form derived by Clauser, Horne, Shimony and Holt [CHSH69], also referred to as CHSH inequality, reads as follows:

$$|C(\mathbf{n}_1,\mathbf{n}_2)+C(\mathbf{n}_1{}',\mathbf{n}_2)+C(\mathbf{n}_1,\mathbf{n}_2{}')-C(\mathbf{n}_1{}',\mathbf{n}_2{}')|\leq 2\,, \tag{3.16}$$

where $C(\mathbf{n}_1,\mathbf{n}_2)$ is the correlation function defined by:

$$C(\mathbf{n}_1,\mathbf{n}_2)=\langle A(\mathbf{n}_1)B(\mathbf{n}_2)\rangle\,, \tag{3.17}$$

The CHSH inequality has to be fullfilled by any theory based on LHV. For LHV theories, the RHS of Eq. 3.17 is given by:

$$\langle A(\mathbf{n}_1)B(\mathbf{n}_2)\rangle=\int A(\mathbf{n}_1,\lambda)B(\mathbf{n}_2,\lambda)\mathrm{d}\rho_\lambda\,, \tag{LHV}$$

while, for quantum mechanics:

$$C(\mathbf{n_1},\mathbf{n_2})=\langle\psi|(\mathbf{n}_1\cdot\boldsymbol{\sigma})(\mathbf{n}_2\cdot\boldsymbol{\sigma})|\psi\rangle\,, \tag{QM}$$

where $\boldsymbol{\sigma}=(\sigma_x,\sigma_y,\sigma_z)$, is the vector of Pauli matrices. If we assume we analyze the state $|\Psi^-\rangle$ given by Eq. 3.15 and if we adjust the setup in such a way that the angle between $\mathbf{n}_1$ and $\mathbf{n}_2$, $\mathbf{n}_1$ and $\mathbf{n}_2{}'$, $\mathbf{n}_1$ and $\mathbf{n}_2$ is 45° and that between $\mathbf{n}_1{}'$ and $\mathbf{n}_2{}'$ is 135°, we finally get the quantum mechanical prediction:

$$|C(\mathbf{n}_1,\mathbf{n}_2)+C(\mathbf{n}_1{}',\mathbf{n}_2)+C(\mathbf{n}_1,\mathbf{n}_2{}')-C(\mathbf{n}_1{}',\mathbf{n}_2{}')|=2\sqrt{2}>2\,. \tag{3.18}$$

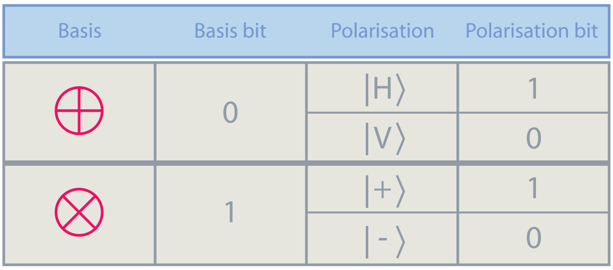
Thus, quantum mechanics contradicts the postulates of LHV theory.

3.4 Quantum Protocols

3.4.1 Four-State Protocol: BB84

The BB84 was the first key distribution protocol based on quantum cryptography. It is called after the two inventors Charles Bennett and Gilles Brassard, who proposed it at an IEEE conference in 1984 [BB84].

Its easy comprehension and simple practical realization, make the BB84 up to now the most attractive quantum cryptographic protocol for experimental purposes. The protocol implementation uses polarization states of single photons to encode information. In particular, polarization from the previously analyzed non orthogonal states, $\{|H\rangle,|V\rangle\}$ and $\{|+\rangle,|-\rangle\}$, are chosen. The table on the next page illustrates the bit encoding scheme. A classical two-bit pattern defines the mapping to the polarization. The first bit represents



Basis	Basis bit	Polarisation	Polarisation bit
⊕	0	|H⟩	1
		|V⟩	0
⊗	1	|+⟩	1
		| - ⟩	0

Figure 3.3: BB84 polarization-encoding scheme. Classical two-bit patterns define basis and polarisation of the outcoming photons.

the basis, the second bit the polarization in the corresponding basis; so, for instance, to the bit pattern `01` will correspond a $|H\rangle$ polarized photon. The key distribution between Alice and Bob consists of the following steps:

Step 1: Alice and Bob agree on an encoding scheme such as the one described in Table 3.3.

Step 2: Alice generates two random independent strings of classical bits with the same length. Each bit of the first string is used for the basis mapping, while the corresponding bit of the second string is used for the polarization choice. According to the resulting bit pattern, Alice prepares the corresponding photon and sends it out to Bob through the **quantum channel**. For instance, assume the m-th bit from the basis string is `1`, the m-th from the polarization string is `0`, then Alice has to send out a $|+\rangle$ polarized photon, (resulting pattern = `10`). The procedure is repeated for every bit-string pair.

Step 3: Everytime Bob expects to receive a photon, he selects a measurement basis randomly and independent of Alice' choice, either $\{|H\rangle, |V\rangle\}$ or $\{|+\rangle, |-\rangle\}$. Bob measures the polarization of the received photon in the chosen basis.

Step 4: Due to a lossy channel and imperfect detectors, Bob won't be able to receive every photon Alice sent out. Thus, he has to communicate her which ones he has detected. Alice discards all entries corresponding to the missing detection events.

Step 5: Alice and Bob communicate each other through the **classical channel**, which basis they used for sending and receiving. Whenever they used the same basis, Bob's measurement was **deterministic**, and they must share the same bit. In the case where the bases did not coincide, the result of the polarization measurement is completely randomized and they have to discard the corresponding entry. This step is called the **sifting procedure**.

Step 6: Ideally, after the sifting procedure, Alice and Bob share a common sequence of randomly generated bits, which constitutes their symmetric en-

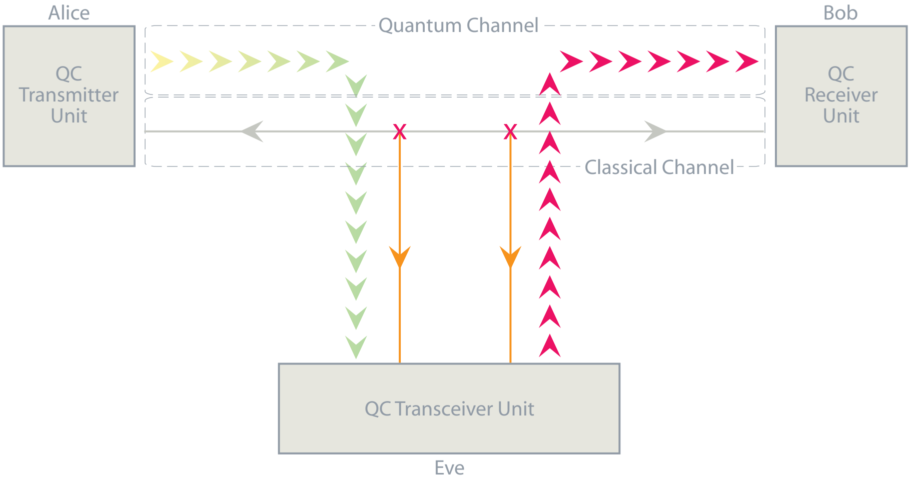


Figure 3.4: The picture illustrates the schematical setup for an intercept-resend attack.

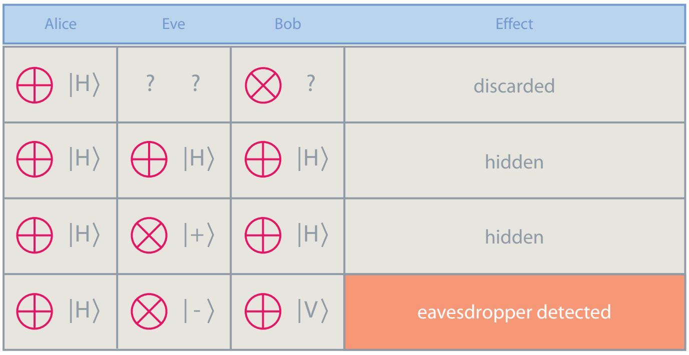
cryption key. At this point they have to check whether an eavesdropper was present. To do this, they randomly select a piece of sifted key and calculate the fraction of different bits, yielding the **quantum bit error rate (QBER)** for this transmission.

Step 7: If the calculated QBER is higher than a given limit (more precise numerical values will be given later), they have to discard the key and repeat the transmission. If the QBER is below that limit, they estimate the maximum amount of possibly eavesdropped information and proceed with the error correction and privacy amplification routines (see Section 3.5), to end up with a common secure key string K_s.

Security: Intercept-Resend and Cloning Attack

The strength of any quantum protocol is actually based on the possibility of detecting whether someone tried to listen in the quantum channel. For this purpose, the QBER plays a fundamental role. To illustrate how the eavesdropping detection works, imagine Eve is in possess of a quantum transceiver device, which can perform a polarization measurement and successively send a photon *in the measured state* further to Bob, as Alice does.
Such a scheme is known as **intercept-resend attack**, for obvious reasons. As previously stated, Eve as well as Bob, cannot deterministically distinguish between non-orthogonal states, hence the only strategy Eve can apply is to

measure every incoming photon choosing the basis randomly. But, according to the postulate that measuring disturbs the state, we can argue that there must be some detectable consequence for what Eve is doing. Indeed, this results in an increasing of the QBER parameter. To understand more quantitatively how the QBER is affected by this attack, assume Alice sends out a polarized photon, which is intercepted and measured by Eve, who forwards it to Bob.



Alice	Eve	Bob	Effect
⊕ |H⟩	? ?	⊗ ?	discarded
⊕ |H⟩	⊕ |H⟩	⊕ |H⟩	hidden
⊕ |H⟩	⊗ |+⟩	⊕ |H⟩	hidden
⊕ |H⟩	⊗ |-⟩	⊕ |V⟩	eavesdropper detected

Figure 3.5: The effect of a intercept-resend eavesdropping attack.

With the help of table 3.5 let us analyse the possible scenarios which can arise. In the first row a $|H\rangle$ polarized photon is sent out, first measured by Eve, then resent and finally measured by Bob in the "wrong" basis. So, independently of what Eve measures (denoted by "?"), the photon will be discarded anyway in the sifting procedure, so no contribution to the QBER is produced. More interesting cases occur if Bob measures in the same basis as Alice sends. In the second row, Eve chooses the "right" basis too, so she gets a deterministic result. After sending out the same state, Bob's and Alice' results will coincide, hence the QBER is still not affected and Eve can gain full information. In the third and fourth case, Eve's and Alice' choice don't coincide: Eve's measurement swaps the polarization to either $|+\rangle$ or $|-\rangle$, hence completely randomizing Bob's result. The QBER can be estimated if we consider that with 50% probability Eve chooses the wrong basis, and in those cases, Bob's result won't match with 50% probability as well. This analysis leads to the conclusion that **an intercept-resend attack causes a QBER of 25%** in the sifted key. If we consider that in a typical experimental environment the QBER is about a few percent, we conclude that this attack would be easily detected.

Another class of eavesdropping strategies exploits the cloning procedure and is thereafter called a **quantum cloning attack**. Though, as discussed before, quantum cloning cannot be performed with arbitrary precision, an optimal cloning machine is able to reach a fidelity of about 83.3%.

The scheme works as follows: Eve is in possess of an universal quantum cloning machine (UQCM), which attempts to make two identical copies of every photon coming from Alice. She then stores one copy in a quantum memory (a rather ideal device used to store qubits) and forwards the other to Bob. When the bases are publicly announced, she retrieves the stored qubits and performs the measurement in the correct basis. The error rate introduced by this procedure will be **QBER**$= (1 - \mathcal{F}) * 100 \approx \mathbf{16,7\%}$. Though much lower than in the previous case, the introduced error is still easily detectable.

3.4.2 Two-State Protocol: B92

This protocol, proposed by Bennett in 1992 [Ben92], can be considered as a simplified version of the BB84. Unlike the latter, it makes use of only two non-orthogonal states, which are already sufficient to implement secure QKD. Following [NC02], suppose Alice has a random string of classical bits, and let b_A be the m-th bit. Depending on its value she sends one of the following states to Bob:

$$|\psi\rangle_m = \begin{cases} |H\rangle\,, & \text{if}\, b_A = \mathtt{1} \\ \\ |+\rangle = \dfrac{|H\rangle + |V\rangle}{\sqrt{2}}\,, & \text{if}\, b_A = \mathtt{0} \end{cases} \tag{3.19}$$

According to a random classical bit b_B, Bob performs a measurement either in the $\oplus$ basis (if $b_B = \mathtt{0}$), or in the $\otimes$ basis (if $b_B = \mathtt{1}$). Whenever he detects a $|V\rangle$ polarized photon, he knows Alice has sent a bit value $\mathtt{0}$ (if not so, he would have no chance to detect $|V\rangle$, since the two states are orthogonal).
Analogously if he detects a $|-\rangle$ he can safely conclude that he measured a bit value $\mathtt{1}$. In the two remaining cases, called *erasures*, he cannot assert with certainty which bit value he received, so he discards those measurements. In the sifting procedure, Bob announces the position of photons he could identify with certainty, and the bit value he obtained (but not the basis he measured with). After that, Alice and Bob conduct a public discussion, keeping only those pairs b_A, b_B, for which Bob obtained the bit $\mathtt{1}$ (note that when $b_A = b_B$, then Bob gets always $\mathtt{0}$). Only in those cases where $b_B = 1 - b_A$ will Bob get a bit value $\mathtt{1}$, and that occurs with 50% probability. Finally, the key is b_A for Alice and $1 - b_B$ for Bob. Analogously to the BB84 protocol, eavesdropping detection occurs with the analysis of the QBER in a randomly chosen fraction of the sifted key.

Security: Unambiguous State Discrimination Attack

This is a special case of an intercept-resend attack, and applies whenever the signal states sent by Alice are linear independent. Eve can perform an **unambiguous state discrimination (USD)** measurement on the signal states, thereby distinguishing between cases where she got a deterministic result or a random one.
She can then apply the following strategy: in those cases where she knows the state with certainty, she forwards it to Bob, while, in all other cases, she sends no signal at all, mimicking a lossy channel.

The previously discussed B92, is an example for a protocol which can be affected from such an attack. Under a given threshold, which depends on the state non-orthogonality, no secure key transmission is possible. This threshold is defined as the transmissivity where the probability of success of an USD measurement equals Bob's detection probability on the lossy channel. For the threshold of the transmissivity we find the expression ([TKI03]):

$$\eta_{th} = 1 - |\langle\phi_0|\phi_1\rangle| \tag{3.20}$$

where, $|\phi_0\rangle$ and $|\phi_1\rangle$ are the two non-orthogonal states. In our example, plugging in the states defined in 3.13, we get $\eta_{th} = 1 - 1/\sqrt{2} \approx 0.293$, or a channel attenuation of about 5 dB.

3.4.3 QKD with Weak Coherent Pulses

Although the unconditional security of many QKD protocols, (including BB84), has been proven in various papers (see e.g. [May96], [SP00]), this is not a guarantee for QKD in practice, due to imperfect real-world implementations. All protocols considered up to now, postulate the existence of an ideal device which can produce single photons on demand. Unfortunately, in the real world such a device still doesn't exist, so that experimenters strive to approximate such a behavior. A widespread practical solution, is the use of weak coherent pulses from a laser source. The outcoming radiation is described by a single mode coherent state with Poissonian photon number distribution:

$$p(n) = \frac{\mu^n}{n!} e^{-\mu} \, , \tag{3.21}$$

where μ is the mean photon number. In Fig. 3.6 we plotted the Poisson distribution for $\mu = 0.1$, a typical value used in experiments (see section 4.1 for the origin of that value).
The probability of zero photons in a pulse is $p(0) \approx 0.905$, the one photon probability $p(1) \approx 0.090$, and the multi-photon probability $p_{multi} \approx 0.005$, so that with a high probability most pulses carry no signal state. The reason for

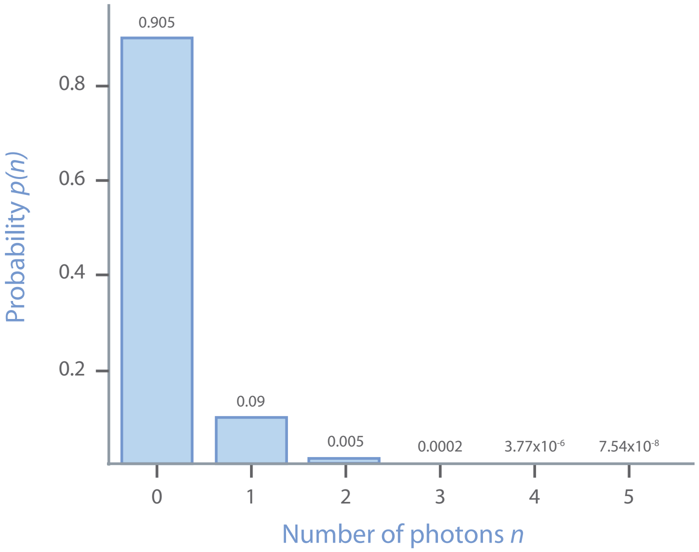


Figure 3.6: The photon number probability distribution for a source with μ=0.1 photons/pulse.

such a low mean photon number resides in the corresponding low probability for multiphoton pulses p_{multi} compared to $p(1)$. A too high fraction $\frac{p_{multi}}{p(1)}$ represents a potential source for an eavesdropping attack described in the following section.

Photon Number Splitting Attack

A very strong class of eavesdropping strategies is known as **photon number splitting (PNS) attack**, first described by Dušek [DHH99], Lütkenhaus [Lüt00], and Brassard [BLMS00]. It is not based on a security flaw in the protocol self, but rather on its physical implementation. Imagine Eve is listening in the quantum channel and waiting for signal states. She could apply the following strategy (see Fig. 3.7):

- For every incoming signal she performs a quantum non demolition (QND)[8] measurement on the number of photons contained in the signal.

[8] The name comes from the fact that Eve actually performs a measurement in the photon number Hilbert space, hence no disturbance of polarization state is made.

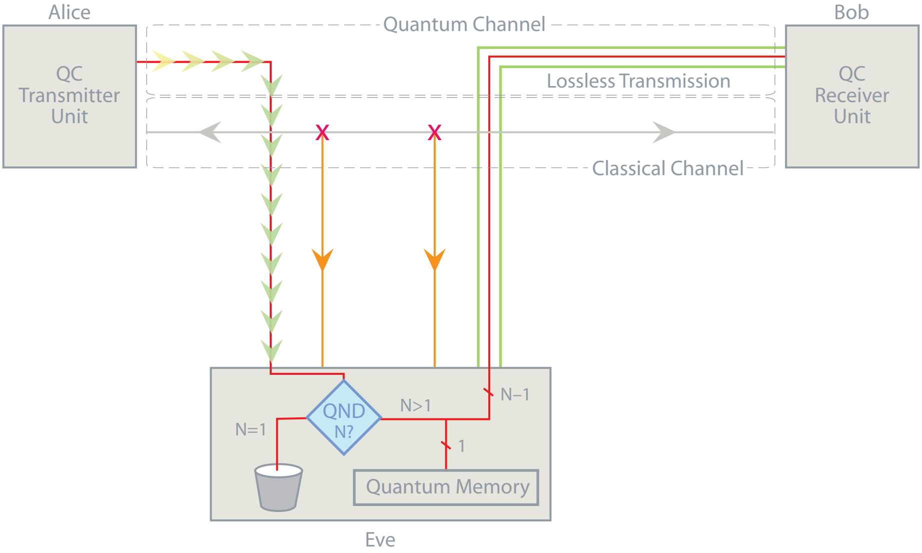


Figure 3.7: The picture illustrates the powerful strategy behind a PNS attack. For every intercepted pulse, Eve performs a QND measurement in the photon number Hilbert space. Depending on the outcome N of her measurement, either she blocks the pulse , or (if $N > 1$) she stores a photon in a quantum memory (if $N = 1$) and forwards the rest to Bob. Then she waits until the bases are announced and retrieves the stored photons to measure them deterministically.

- Depending on the result of the QND measurement she does the following:
  - if the photon number is $n = 0$ she doesn't perform any action
  - if the photon number is $n = 1$ she blocks the photon
  - if the photon number is $n > 1$ she stores one of the photons in a quantum memory and forwards the remaining one(s) to Bob
- She waits until the bases are publicly announced, then retrieves the stored photons and she measures them in the correct basis.

Actually, such an attack results in a very powerful mean, since Eve can ideally share the whole information with Alice and Bob, without being detected. Indeed, a PNS attack will cause an overall attenuation of the quantum channel transmission rate, but no increasing in the QBER. Therefore, to prevent such an eavesdropping risk, particular attention must be paid to the quantum channel transmissivity and to the mean photon number[9].

[9] In [BLMS00] an upper bound for the transmissivity, which could allow Eve to gain full information over the key, is given by: $\eta < \left(1 - e^{\mu} - \mu e^{-\mu}\right)/\mu$.

Decoy State Protocol

A way to efficiently counteract a PNS attack has been proposed in recent years by Hwang, [Hwa03], Wang, [Wan04a] and [Wan04b], Lo, [LMC05], and Ma [Ma04] and is called **decoy state protocol**. In this section we focus our attention on the main results of Hwang's proposal [Hwa03].
The basic idea is to use three different mean photon sources or classes: one, denoted S_μ for signal states with mean photon number μ, one, denoted $S_{\mu'}$ for the so called decoy state with mean photon number $\mu' > \mu$ and one as vacuum state source S_0, with $\mu_0 = 0$. Signal and decoy source differ from each other only in their μ parameters, i.e. they have the same characteristics, such as wavelength, timing information, etc.. According to a randomly generated pattern of classical bits, Alice sends out photons alternating from all three sources to Bob. The three states $|\mu\rangle, |\mu'\rangle$ and $|\mu_0\rangle$ are non-orthogonal, since, e.g.:

$$\langle\mu|\mu'\rangle^2 = \exp(-|\mu - \mu'|^2) \neq 0 \quad \text{if} \quad \mu \neq \mu' \,. \tag{3.22}$$

Hence Eve is not able to deterministic distinguish between these states. Whenever a PNS attack takes place, this unavoidably influences the photon statistics (she cannot establish to which mean photon number class the photon stems from). In the public discussion Alice announces for every transmitted photon the basis she used and its mean photon number class. If the quantum channel transmission and detector efficiencies are known, it is easy for Bob to calculate the expected values for μ, μ' and μ_0. If the three mean photon numbers show different attenuations, then we can conclude that Alice and Bob have been victim of a PNS attack and should discard the key. To make some more quantitative assertions, define the gain Q_n for a state containing n photons as the quantity:

$$Q_n = Y_n \frac{\mu^n}{n!} e^{-\mu} = Y_n P_n(\mu) \tag{3.23}$$

where $P_n(\mu)$ is the Poissonian distribution with mean photon number μ, and Y_n is the yield of an n-photon signal (conditional probability that Bob detects an event, provided Alice sent out a n-photon signal). The total gain of the source is the sum over all possible photon numbers n:

$$Q_\mu = \sum_n Q_\mu = \sum_n Y_n P_n(\mu) \,. \tag{3.24}$$

For the two signal sources S_μ and $S_{\mu'}$, we get:

$$\begin{aligned}
Q_\mu &= Y_0 e^{-\mu} + Y_1 \mu e^{-\mu} + \sum_{n=2}^{\infty} Y_n P_n(\mu) && (3.25)\\
&= Y_0 e^{-\mu} + Y_1 \mu e^{-\mu} + cY_m && (3.26)\\
Q_{\mu'} &= Y_0 e^{-\mu'} + Y_1 \mu' e^{-\mu'} + \sum_{n=2}^{\infty} Y_n P_n(\mu') && (3.27)\\
&= Y_0 e^{-\mu'} + Y_1 \mu' e^{-\mu'} - \frac{\mu'^2 e^{-\mu'}}{\mu^2 e^{-\mu}} cY_m + dY_d && (3.28)
\end{aligned}$$

where Y_0, in the absence of eavesdropping, is simply given by the measured background detection event rate of the system. Q_μ, and $Q_{\mu'}$ are directly measured, and c and d are given by:

$$\begin{aligned}
\mu e^{-\mu} Q_{\mu'} c &= 1 - e^{-\mu} - \mu e^{\mu} > 0 && (3.29)\\
d &= 1 - e^{-\mu} - \frac{\mu'^2 e^{-\mu'}}{\mu^2 e^{-\mu}} c \geq 0\,. && (3.30)
\end{aligned}$$

Our task is now to find a parameter for security check which can be easily estimated by Alice and Bob. This quantity, denoted Δ, is the fraction of multiphoton events originating from the source S_μ to the total counts Q_μ, i.e.:

$$\Delta = \frac{cY_m}{Q_m}\,. \tag{3.31}$$

Hence the task is reduced to formulating Y_m as a function of parameters $\{Y_0, Q_\mu, Q_{\mu'}\}$. Note that in equation 3.28 Y_1 and Y_d are unknown, but never negative, so we can write down a first estimation for cY_m:

$$cY_m \leq \frac{\mu^2 e^{-\mu}}{\mu'^2 e^{-\mu'}} \left(Q_{\mu'} - e^{-\mu'} Y_0 - \mu' e^{-\mu'} Y_1 \right)\,. \tag{3.32}$$

From this, it is now easy to get Hwang's main result presented in [Hwa03]:

$$cY_m \leq \frac{\mu^2 e^{-\mu}}{\mu'^2 e^{-\mu'}} \left(Q_{\mu'} - e^{-\mu'} Y_0 \right) \leq \frac{\mu^2 e^{-\mu}}{\mu'^2 e^{-\mu'}} Q_{\mu'}\,. \tag{3.33}$$

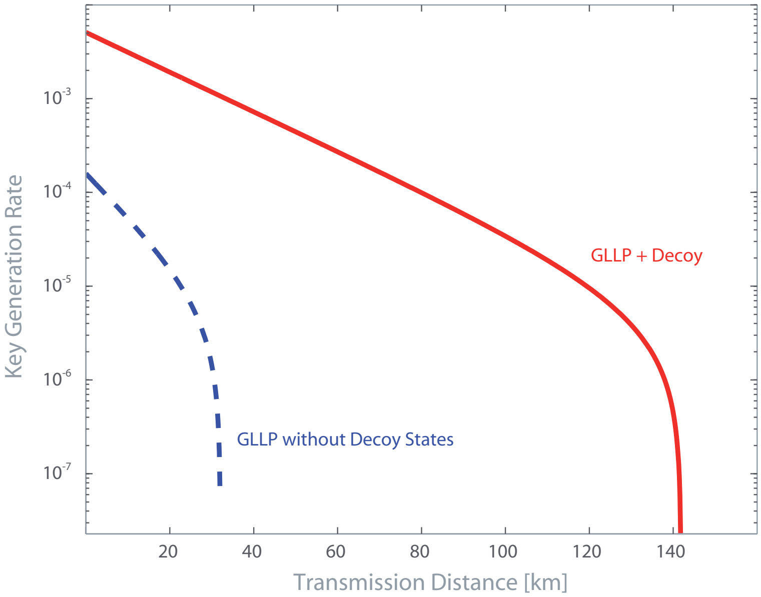


Figure 3.8: Diagram from [LMC05]. Simulation of kgr vs. distance with and without decoy state protocol, plotted using real parameters from GYS experiment [GYS04]. With decoy the maximal distance is extended to over 140 km, while with prior art method the achievable distance was about 30 km.

Combining 3.24 with 3.22, we get:

$$\Delta \leq \frac{\mu^2 e^{-\mu} Q_{\mu'}}{\mu'^2 e^{-\mu'} Q_\mu} \tag{3.34}$$

which can also be found in Hwang's paper. In the case there is no Eve's attack Alice and Bob will asymptotically find:

$$\frac{Q'_\mu}{Q_\mu} = \frac{1 - e^{-\eta\mu'}}{1 - e^{-\eta\mu}} = \frac{\mu'}{\mu} \tag{3.35}$$

where η is the channel transmission. Therefore they are able to verify $\Delta \leq$ $\leq \frac{\mu e^{-\mu}}{\mu' e^{-\mu'}}$. This gives the needed parameter for security check against PNS attacks. We try now to illustrate one of the main advantages in using a decoy state protocol. As reported in [GLLP02], later addressed as GLLP, as long as the channel transmission η is not dramatically low, the extraction of a secure shared key between Alice and Bob is still possible.

GLLP scheme assumes that Fred is collaborating with Eve, "tagging" some photons at Alice' side to facilitate Eve's measurement in the right basis. If $\Delta = p_M / p_D$ is the fraction of tagged to detected photons, then we can derive an expression for the key generation rate, which is defined as the length of the secure key[10] to the total number of signals sent by Alice :

$$kgr \approx \frac{1}{2}\nu p_D \approx \frac{1}{2}\nu\eta\mu \approx \nu\eta^2\Delta \tag{3.36}$$

where ν is the source repetition rate, and the $\frac{1}{2}$ factor comes from the random choice of the basis in the BB84 protocol. The interesting thing to note is the $\mathcal{O}(\eta^2)$ dependence of the kgr, that is for very lossy channel or large distances, a secure key exchange becomes impossible (see figure 3.8).
Nevertheless a decoy state protocol can restore the unconditional security over larger distances. The fact that security check bases on multiphoton pulses, allows the choice of higher values for μ and μ', typically varying from 0.1 to 0.3. Moreover, both sources can be used simultaneously as signal and decoy state. The enhancement of the range where a kgr is still achievable is clear from the diagram shown in Fig. 3.8.

3.4.4 Entanglement-Based QKD: Original and Simplified Ekert Protocols

In 1991 A. Ekert proposed a QKD protocol based on quantum entanglement[11][Eke91]. A way to produce polarization entangled photons, which find applications in such protocols, is based on the non-linear properties of some crystals like e.g. β-BaB$_2$O$_4$ (β-barium-borate or BBO), KNbO$_3$, LiNbO$_3$, etc.. In this process, called spontaneous parametric down conversion (SPDC), some photons of a pump beam are down-converted into two photons under conservation of energy and momentum. The two photons emerge along two orthogonally polarized emission cones (see Fig. 3.9). Collecting only photons from the two intersection regions provides a maximally entangled polarization state:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|V\rangle_S|H\rangle_I - |H\rangle_S|V\rangle_I\right) . \tag{3.37}$$

Alice and Bob each receive a particle from this entangled pair. Afterward, they measure their particle in one out of three different bases. Suppose, for

[10] The secure key is the result of a distillation procedure, applied to the sifted key, to enhance security (see section 3.5). The higher the μ, the more the sifted key has to be shrunk down, because of multi-photon contributions.

[11] The particular nature of the entangled particles is not relevant for the general discussion, so it doesn't matter whether they share two spin 1/2 particles or two polarization entangled photons. However, in all practical QKD realizations, photons are used, because they are easy to transport over large distances.

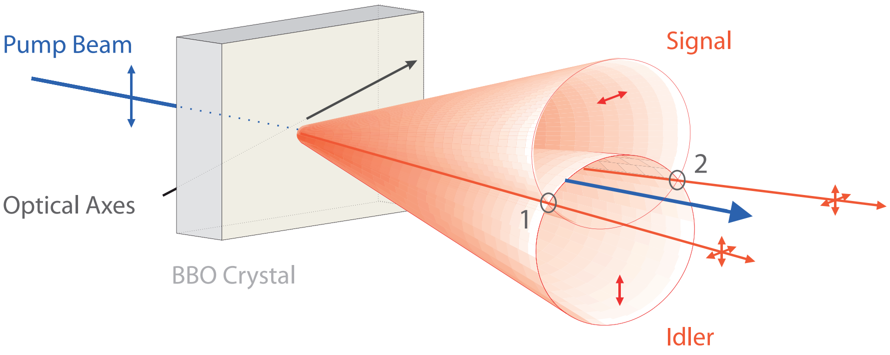


Figure 3.9: Spontaneous parametric down conversion (SPDC) exploits the non-linear properties of some crystals to produce polarization-entangled photon pairs.

instance, they choose the measurement directions lying on the plane perpendicular to the particle trajectory, at angles with respect to the vertical of 0° 45° and 90° at Alice' side and 45° 90° and 135° at Bob's side (see Fig. 3.10). They perform measurements on their entangled particles using random and independent basis settings.

At the end of the transmission they conduct a public discussion telling each other which base settings were used for each pair. Whenever they used the same basis, their results are perfectly correlated and these cases constitute the shared key, while, in all other cases the outcomes are random . It is easily verified that their measurement settings will coincide with probability 2/9. The

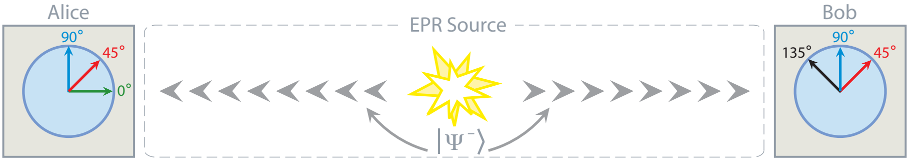


Figure 3.10: Schematical setup for an entangled state protocol. The source produces entangled particles which are analyzed by Alice and Bob randomly choosing one out of three possible measurement directions.

protocol provides of course also a security check. This is performed using the outcomes of the uncorrelated pairs. An eavesdropper attempting to correlate his probe with one of the EPR particles, will unavoidably corrupt the quality of entanglement, resulting in a lower violation of the CHSH inequality.

A year later, Bennett, Brassard and Mermin [BBM92] proposed a simplified version, without making direct use of Bell's theorem. Alice and Bob have to choose randomly only from two possible orientations, which build a conjugated basis pair. Unlike in BB84, Alice doesn't need to prepare particles in a given polarization or spin orientation state, but she only limits herself to measuring her half of the EPR pair. Eavesdropping check is carried out calculating the QBER in the sifted key as well.

3.5 Error Correction and Privacy Amplification

Every QKD protocol which deserves this name, must provide a procedure to identify and successively correct accidental errors in the shared key. After the sifted key is extracted, Alice and Bob should ideally share the same sequence of bits. This won't be the case in real world implementations, where noisy quantum links or detectors, or even an eavesdropper, will generate a fraction of wrong bits in the sifted key.
Moreover, if we assume that the QBER is due **exclusively** to the presence of an eavesdropper, we should consider some procedures to reduce the leaked information towards zero, otherwise no secure key distribution can be established.

3.5.1 Error Correction

According to a theorem stated by Shannon [Sha48], it is not possible to perform error correction without disclosing some information. The ratio between the minimum number of bits N_{corr}^{Shan} needed to correct a sifted key of length η_{sif} in the limit $\eta_{sif} \to \infty$ is given by:

$$\frac{N_{corr}^{Shan}}{\eta_{sif}} = -e \log_2 e - (1-e) \log_2 (1-e) \,, \tag{3.38}$$

where e is the observed error rate in the sifted key. Unfortunately, the limit in 3.38 is only a theoretical lower bound to the amount of key information needed to perform error correction. How large this leakage is, actually depends on the adopted particular procedure. The error correction algorithm proposed by Brassard and Salvail, called `CASCADE` [BS93], is very close to this limit. We briefly outline how it works. The starting point is a sifted key bit-string of given length at both Alice' and Bob's side, with an expected fraction of wrong bits (≈ QBER). The error correction is now performed in a few cycles, where each round runs as follows:

Step 1: Alice and Bob partition their respective string into blocks of fixed length.

Step 2: They compute the parity bit of each block, and publicly compare the results. Two cases can arise:

- if the parities of the block coincide, they go on with the next block.
- if the parities differ, Bob knows there must be an **odd** number of errors in that block. To find one of these errors he applies the routine `BINARY` to this block. It performs a recursive binary search, first dividing the block into two equal sub-blocks, then comparing their parities with the same sub-blocks of Alice to determine in which of the two the error lies. The search proceeds now with this sub-block, and so on until the wrong bit is isolated and corrected by Bob.

  Notice that if the flipped bit was present in a block of the previous round (which had an even number of errors), then Bob knows there must be one more error in that block. Again `BINARY` makes sure that this error is located and corrected.

Step 3: Alice and Bob apply a permutation to their bit string and start the next round with an increased block length, usually twice that of the previous step.

Within a few cycles, Alice and Bob share the same key. Notice that the parity bits which are sent through the public classical channel constitute leaked information. This can be eavesdropped as well and must be taken into account when performing privacy amplification.

3.5.2 Privacy Amplification

After the error correction, Alice and Bob share the same bit string, and Eve is supposed to have gained all leaked information. The goal of privacy amplification is to reduce Eve's knowledge to a negligible quantity by creating a shorter, truly secret key. Following Lütkenhaus [Lüt00], we assume that the final key length η_f is given by the formula:

$$\eta_f = 1 - \eta_{sif}(1 - \tau_1) - \eta_S \,, \tag{3.39}$$

where η_{sif} is the sifted key length τ_1 is the shrinking factor, and η_S is a security parameter. The latter becomes negligible for long enough keys, so it is dropped from the discussion. The requirement that Eve's knowledge about the key is arbitrary small, can be made rigorous by two assumptions:

1. all keys of length η_f should have equal probability p. If x is any given key, this means: $p(x) = 2^{-\eta_f}$.
2. the difference between *a priori* and *a posteriori* probability for any key x should vanish.

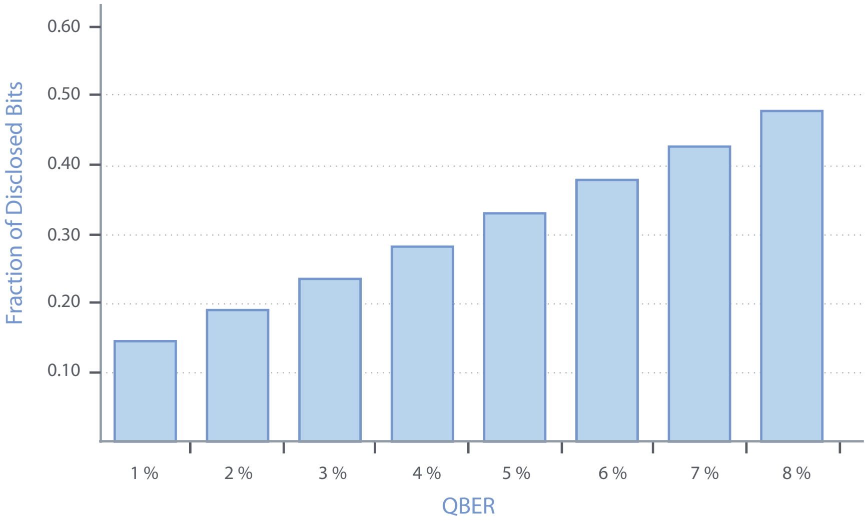


Figure 3.11: Plot of the fraction of disclosed bits vs. QBER, as resulting from the implementation of the `CASCADE` algorithm. Picture adapted from [BS93].

This results in an upper bound for the shrinking factor:

$$\tau_1 \leq \begin{cases} \log_2(1+4e-4e^2) & \text{for } e \leq 1/2 \\ 1 & \text{for } e \geq 1/2 \end{cases} \tag{3.40}$$

where e is the previously measured QBER. Once τ_1 has been estimated, Alice and Bob can actually proceed with the privacy amplification. Suppose the final key must be m bit long to be considered secure. According to [BBCM95] they choose one from a set of public **universal**[12] **hash functions**[13], which is then exchanged over the public channel. They then apply this function to the sifted key, which is thus shrunk down to the required length m. At this point, Alice and Bob end up with a **secret** symmetric key which can be now safely used for encrypting confidential information. How the whole procedure is implemented in practice can be made clear by means of an example. Assume

[12] A class G of functions $A \mapsto B$ is universal if for any distinct x_1 and x_2 in A, the probability that $g(x_1) = g(x_2)$ is at most $1/|B|$ when g is randomly chosen from G according to a uniform distribution.

[13] A one-way hash function is a shrinking algorithm which “mixes” and “chops” input bits to give a random looking output called the *hash value* or *message digest* (MD). An ideal hash function is collision-free, meaning that for any two different inputs their hash values are never the same.

the sifted key has the length n. First, this is converted into a column vector $\mathbf{v}_{sif}$ which is then multiplied by a $m \times n$ Toeplitz[14] matrix and added to a constant random vector of length m. The result is a secure key $\mathbf{K}_s$ of length m:

$$\mathbf{K}_s = M_{Toe} \cdot \mathbf{v}_{sif} + \mathbf{y}_{rand}$$

[14] A Toeplitz matrix is a matrix which entries are of the form $a_{ij} = a_{i-j}$, i.e. all entries along negative sloping diagonals are equal. It can be shown that the inversion of a Toeplitz matrix takes only $\mathcal{O}(n^2)$ operations, where n is the size of the matrix.

4 The Munich Experiment

So far, the theoretical background for potentially unconditional secure QKD schemes with their respective protocols has been illustrated. In this chapter, we' ll be basically dealing with the practical realization of such a cryptographic system. Since the first experimental realization of a QKD scheme, by Bennett *et al.* in 1989 [BB89] and [BBB$^+$92], more and more groups worldwide dedicated their attention to this challenging topic. In some cases the research effort culminated in the production of commercially available cryptographic devices based on quantum optics (see e.g. `http://www.idquantique.com` or `http://www.magiqtech.com`).
In the very first QKD experiment of 1989, Bennett and Brassard could successfully test their protocol. They used the light coming from a pulsed green LED (light emitting diode), which was subsequently attenuated by an interference filter and its polarization adjusted by a polarizer. The bit encoding took place by the polarization rotation using Pockels cells placed in the beam. The free-space quantum channel amounted to 32 cm; at receiver's side a further Pockels cell performed the choice of the basis, and after that, the two outputs of a Wollaston prism were monitored by a pair of photomultipliers. Since then, larger transmission distances were achieved and, by the time of this work, an experiment involving H. Weinfurter's and A. Zeilinger's groups is aiming at performing a free-space QKD over the largest distance of about 140 km.

Our test setup is located in downtown Munich and performs a point-to-point QKD over a line-of-sight distance of about 0.5 km. Transmitter and receiver units are located on rooftops of two university buildings, a public internet connection serves as the classical communication channel, while the quantum channel is free-space. We implement the four states BB84 protocol with faint laser pulses from four laser diodes, randomly switching among polarization states with a repetition rate of 10 MHz. At the receiver's side, after a passive random basis choice (see Sec. 4.3), polarization analysis of single photons occurs by means of a half-wave plate, two polarizing beam splitters and four silicon-based avalanche photo diodes (APD).
A software based synchronization procedure labels the photons at both sides to allow the successive sifting procedure. Embedded error correction and privacy

amplification algorithms complete the setup. In the following the various parts of the apparatus and their interaction will be described in detail.

4.1 Sender Unit: Alice

This unit is responsible for the generation of photons in four different polarization states. To achieve this, four laser diodes with a maximal optical output power of 5 mW are aligned on a circular mounting head, each rotated by an angle of 45° with respect to each other. Because of their fabrication characteristics, this kind of semiconductor devices emits highly linearly polarized light (better than 1:1000) parallel to the edge which delimits the p- and n-doped surfaces. In this way, without resorting to any polarization optics, the above arrangement ensures that diodes enclosing an angle of 90° (e.g. $\{|H\rangle$ and $|V\rangle$ in Fig. 4.1), can define the $\{|H\rangle, |V\rangle\}$ basis, while the other diode pair builds the conjugated $\{|+\rangle, |-\rangle\}$ basis.

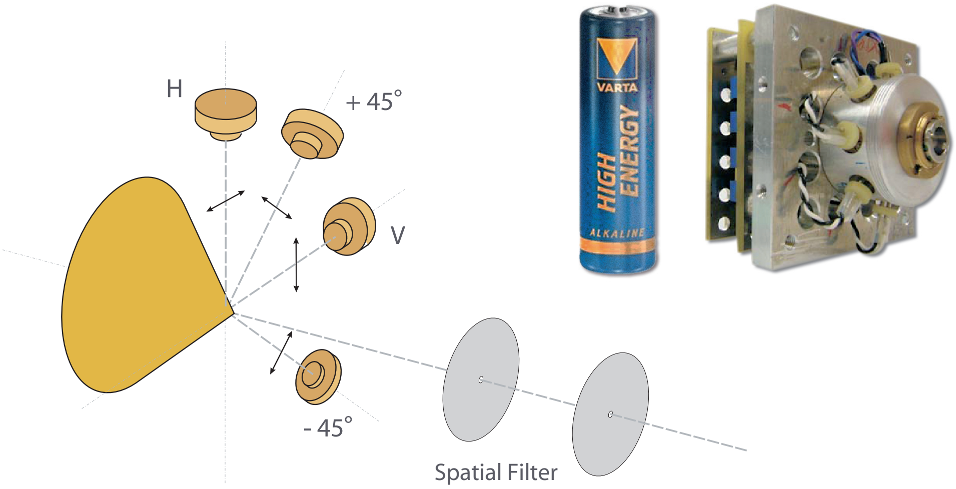


Figure 4.1: Left: schematical picture of the laser diode circular arrangement. Right: picture of the sender unit with driving electronics placed behind.

The four diodes shine from the side to a **conical mirror** screwed inside the head, on which a gold layer has been evaporated to enhance reflectivity. The outgoing beam is now parallel to the optical axis. In order to collect as many photons as possible, a small lens with focal length f=2.75 mm is placed in front of the mirror. The next stage is the **spatial filter**, a pair of pinholes with 100 μm diameter at a distance of 9.2 mm from each other. Its main purpose is to prevent an eavesdropper from gathering information by observing the spatial dependence of the outgoing photons. Since the four output beams from the conical mirror have small spatial overlap, measuring the $\vec{k}$ vector of

a photon would immediately determine from which diode it has been emitted, thus disclosing its polarization. At the output of the second pinhole the spatial modes of the four laser diodes completely overlap, so that indistinguishability is ensured.
The relative distances of mirror, lens and spatial filter are adjusted in such a way, that the waists of the four diodes lie in the middle of the two pinholes. It can be shown that this is a requirement for maximum transmission.

The critical point in this setup is the mean photon number μ, which has to be the same for all four polarizations. The choice of a suitable value for μ results from taking into account several aspects. If, on the one hand, transmission losses and detector noise would suggest to push up the mean photon number, on the other hand the probability of multi-photon pulses must be kept as low as possible, because of the security threat (see Sec. 3.4.3). Following [Lüt00], an upper bound for μ can be derived from the constraint that the key shrinking does not become too restrictive. This happens for $\mu \gtrsim \eta_T$, where η_T is the channel transmittance. The optimal value is that which maximizes the secure key generation rate for given conditions. In the case of real attenuated sources, this optimum is given from the following expression:

$$\mu_{opt} \approx \eta_B \eta_T \ , \tag{4.1}$$

where η_B is the detector efficiency, and the estimation holds under the assumption $\eta_B \eta_T \ll 1$, which is indeed the case for any realistic setup. In our experiment the mean photon number is chosen to be $\mu = 0.1$ photons/puls. To achieve this, the count rate of every diode is independently adjusted with the help of a calibrated silicon APD module to adjust the desired μ. With a measured detector efficiency at 850 nm of $\eta_B = 0.4$, and a pulse rate of 10 MHz, we expect about 400×10^3 counts/s from each polarization direction. To refine the adjustment, the spatial filter is mounted on a small x-y translation stage, which allows parallel displacement with respect to the diodes mounting head.

Driving Electronics

Recalling the BB84 protocol, we need two random strings as input for Alice. The first one determines the basis she uses, and the second the polarization she is sending out. After creating the strings[1], a software translates them

[1] For experimental tasks, computer generated pseudo-random strings are enough, but keep in mind that, in order not to compromise the high level of security which can be reached with quantum cryptography, truly random number generators should be used.

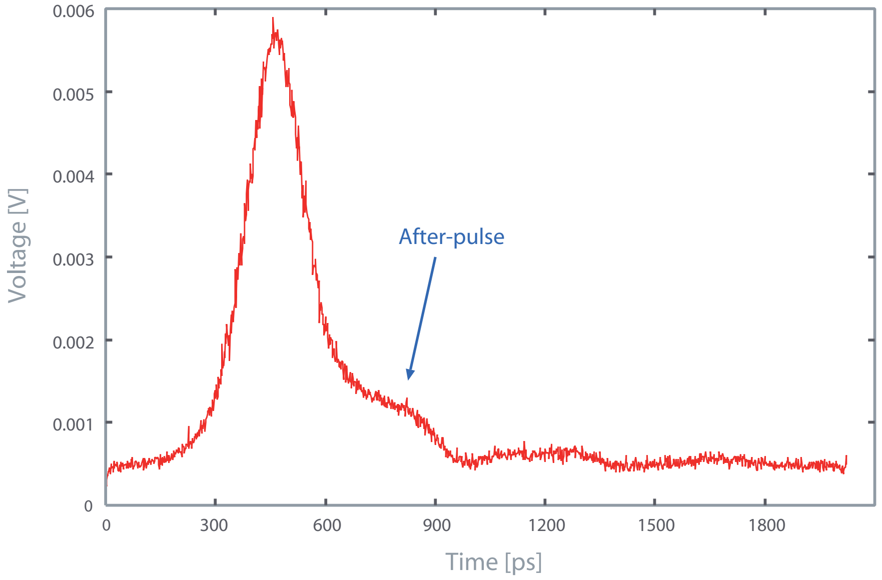


Figure 4.2: The optical pulse captured with a 7 GHz broadband photodiode. The small after-pulse, due to reflections in the driving electronics, accounts for a total pulse width of 375 ± 25 ps.

into a readable format for an input/output card on Alice' computer, which successively transfers them to a FIFO (first in first out) buffer memory. The FIFO constitutes the input for the last driving stage, located behind the diodes mounting head. This last stage takes five inputs: one clock signal at 10 MHz frequency and four TTL signals, each corresponding to one of the four laser diodes. Each TTL signal is combined with the clock signal by means of a AND gate (to ensure that diodes actually fire with fixed repetition rate). Thus a TTL *high* together with a clock pulse raises the voltage of the corresponding diode by a fixed amount (0.5 V) above the offset voltage. The offset voltage has been adjusted so that it lies under the laser diodes threshold voltage, which is about 1.5 V at 25 °C. The duration of the electrical pulse can also be varied with an adjustable capacitor at the input of the AND gate. For a detailed description of the circuit, refer to Weier [Wei03].
The graph 4.2 shows the time resolved optical pulse of the free laser diode (without spatial filter) measured with the help of a 7 GHz broadband photodiode. From the data and the sensitivity curve of the photodiode, the total amount of emitted photons per pulse can be inferred. Comparing it with the desired rate of 0.1 photons/pulse, leads to an overall attenuation of roughly 65 dB at the output of the spatial filter. Due to reflections inside the driving electronics, we can recognize a small after-pulse, which affects the total pulse

length and shape[2]. The optical pulse width (FWHM) is approximately 375 ps ± 20 ps, taking into account the weak after-pulse.

4.1.1 Laser Diode Electrical Characterization

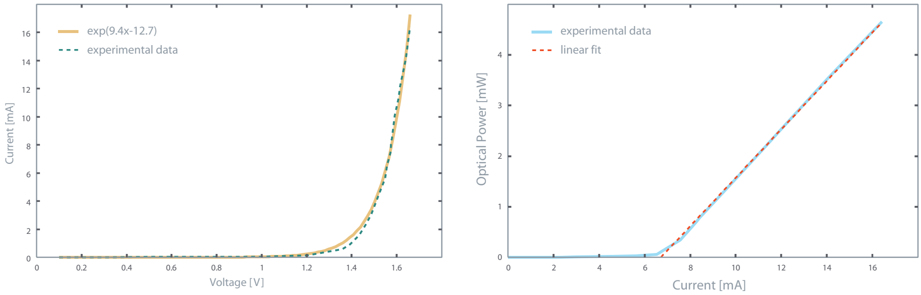


Figure 4.3: The current-voltage (left) and optical power-current (right) characteristic curves of a source sample diode taken at room temperature. the threshold current has been estimated in $I_{thr} = 6.48$ mA, corresponding to a threshold voltage of $V_{thr} = 1.55$ V.

The dependence of the laser diode current on the voltage and the dependence of the optical power on the current have been measured at room temperature (25 °C), using the setup described in [Reg05]. The resulting curves are shown in Fig. 4.3. From the fit, the threshold current can be inferred, resulting in $I_{thr} = 6.48$ mA; the corresponding threshold voltage is: $V_{thr} = 1.55$ V. The investigation of the dynamical behavior of the diodes plays a fundamental role for the dimensioning of the driving electronics. The dynamical resistance is defined by:

$$\rho_D = \frac{\mathrm{d}U}{\mathrm{d}I} \ . \tag{4.2}$$

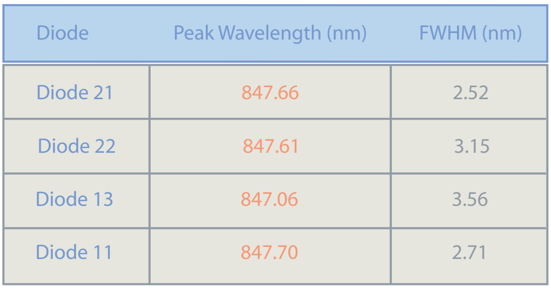
Fixing the operating point, gives an estimation for the impedance. For instance, $\rho_D = 10.2\ \Omega$ is found at a voltage of 1.60 V, which is the correct operation point for obtaining the desired 0.1 photons/pulse. This becomes an

[2] Though, this fact doesn't constitute a security threat due to the large attenuation of the pulses.

important issue when considering the problem of impedance matching. Ideally, the output impedance of one stage at a given frequency, should match the input impedance of the following one at the same frequency. If this is not the case, electromagnetic waves running through the circuit path can undergo reflections. The general problem is quite complicated, even in theory, involving circuit design optimization, component characterization, etc. and its full description would be beyond the scope of this work, so I refer to technical literature about this topic. Another relevant question is the behavior of the laser source under different conditions of the environment. For instance, we expect that the electrical characteristic of the laser diodes strongly depends on the temperature at which they are operated. This has been measured and documented [Reg05] and we can here summarize some results: for lower temperatures, the threshold current reduces, while the current-voltage characteristic becomes steeper for higher temperatures. This behavior can be explained if we consider the dependence of density of free charge carriers (electrons and holes) with the temperature. While the total carrier number increases with increasing temperature, the probability for radiative electron-hole recombination contributing to laser power decreases.

4.1.2 Laser Diode Spectral Characterization

The investigation of optical characteristics of the four laser diodes is very important in order to prevent side-channel attacks relying on slightly different spectral properties. The strategy could be to measure the wavelength of the intercepted photons, and attempt to assign different polarizations to different wavelengths. Hence, particular care must be taken of the spectral distribution of the diodes. Ideally undistinguishability of the sources is guaranteed if all four spectra perfectly overlap, in pulsed mode. With real devices, this can only be achieved with some approximation. Figure 4.4 shows the spectral distribution of the four laser diodes in the Alice module in pulsed operation. Fitting a Lorentz function to these data sets (see Fig. 4.5), leads to the characteristics summarized in the table below:



Diode	Peak Wavelength (nm)	FWHM (nm)
Diode 21	847.66	2.52
Diode 22	847.61	3.15
Diode 13	847.06	3.56
Diode 11	847.70	2.71

Table 4.1: The spectral characteristics of the four laser diodes used in the experiment.

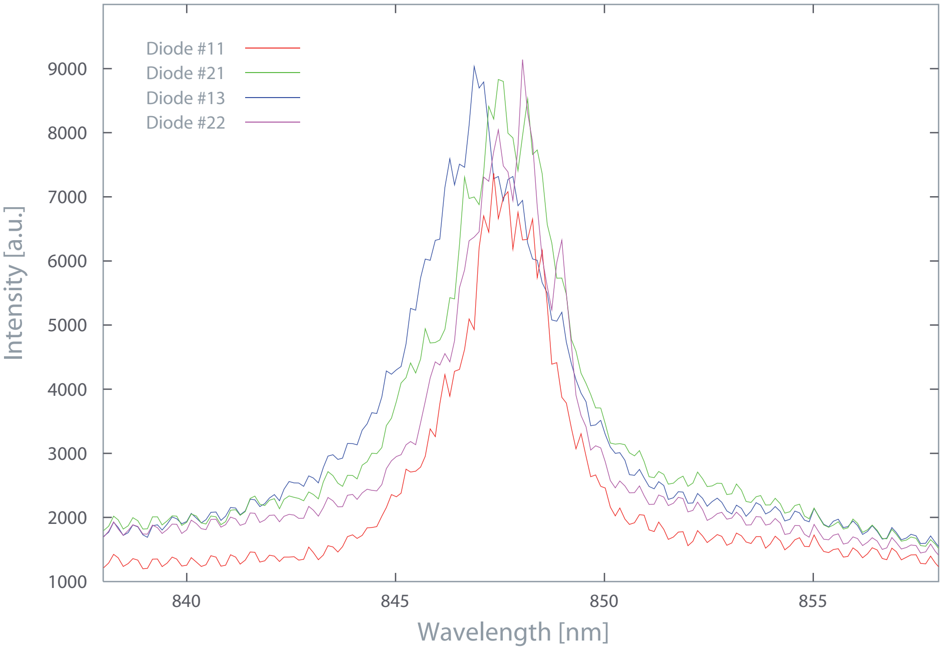


Figure 4.4: Spectral distribution of the four laser diodes operated in pulsed mode measured with a grating spectrometer.

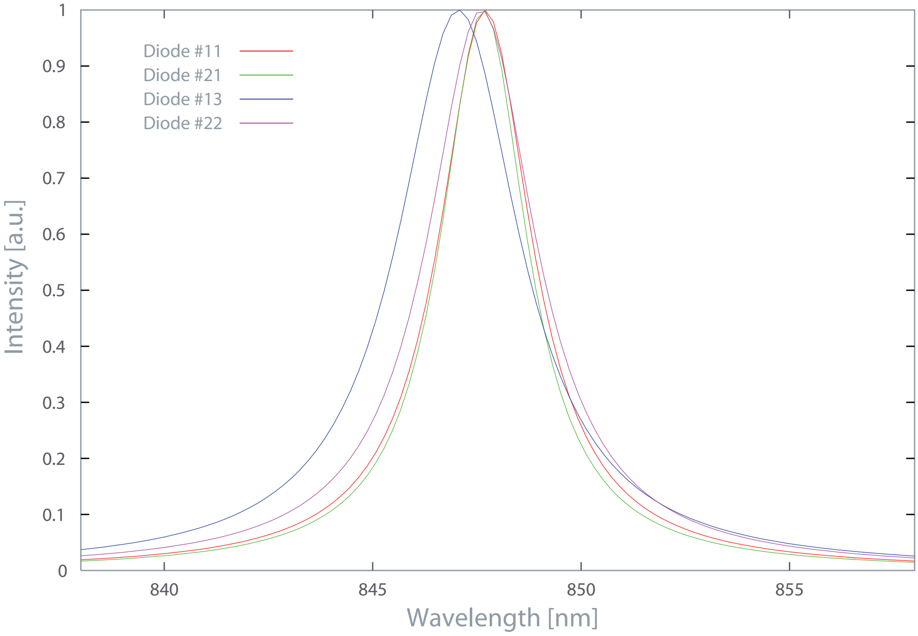


Figure 4.5: The spectral distributions of the figure above have been fitted with four normalized Lorentz curves.

All wavelengths lie within 0.6 nm apart from each other, while we suppose that the measured widths are mainly due to mode hopping.

4.1.3 Information Gain from Spectral Measurements

In the following, we try to estimate the amount of information which can be gained by measuring the wavelength of an intercepted photon. What we are given is the spectral distribution of the i-th source, $s_i(\lambda)$. This has to be normalized, i.e.:

$$\int_{-\infty}^{+\infty} s_i(\lambda)\mathrm{d}\lambda = 1 \, . \tag{4.3}$$

The Lorentz curve which fulfills Eq. 4.3 is given by:

$$s_i(\lambda) = \frac{1}{\pi}\frac{\Gamma_i/2}{(\lambda-\lambda_i)^2 + (\Gamma_i/2)^2} \, , \tag{4.4}$$

where λ_i and Γ_i are the peak wavelength and the width of the i-th source spectrum, respectively. Furthermore let $p^{pr}(i)$ be the a priori probability that the detected photon has been emitted by source i (this should be simply the constant factor $1/4$). Armed with this, we can calculate the probability that the wavelength λ is observed. This is given by:

$$p(\lambda) = \sum_{i=1}^{4} p(\lambda|i)\cdot p^{pr}(i) = \sum_{i=1}^{4} s_i(\lambda)\cdot p^{pr}(i) \, , \tag{4.5}$$

where $p(\lambda|i)$ is the probability of measuring λ, provided that the i-th source sent out a photon. Furthermore, by Bayes' theorem we must have:

$$\begin{aligned} p(i|\lambda) &= \frac{p(\lambda|i)\cdot p(i)}{p(\lambda)} \quad \text{or} & (4.6)\\ p(i|\lambda)\cdot p(\lambda) &= p(\lambda|i)\cdot p(i) \, , & (4.7)\end{aligned}$$

so that we can write $p(i|\lambda)$ as:

$$p(i|\lambda) = \frac{p(\lambda|i)\cdot p^{pr}(i)}{\sum_{j=1}^{4} s_j(\lambda)\cdot p^{pr}(j)} = \frac{s_i(\lambda)\cdot p^{pr}(i)}{\sum_j s_j(\lambda)\cdot p^{pr}(j)} \, , \tag{4.8}$$

where we used Eq. 4.6 and 4.7 to derive the RHS of the second equality. We can now estimate the amount of information contained in a measurement of the wavelength λ. According to information theory, this is given by the Shannon's entropy function calculated at the value λ, i.e.:

$$H_\lambda = -\sum_{i=1}^{4} p(i|\lambda)\cdot \log_2\left[p(i|\lambda)\right] \, . \tag{4.9}$$

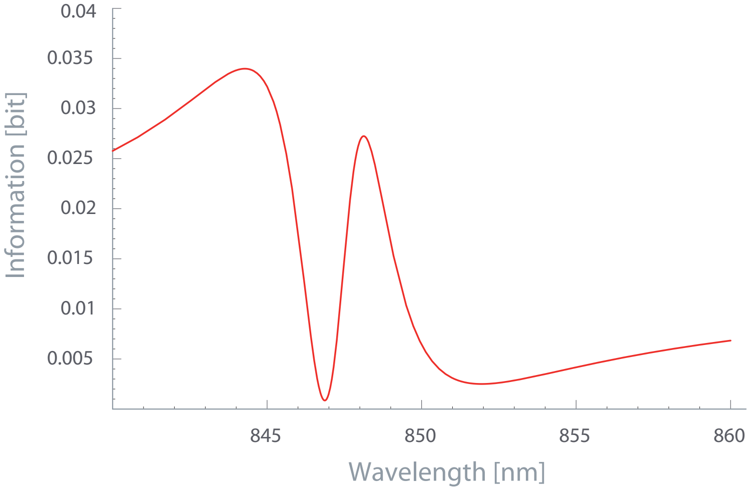


Figure 4.6: Graph which illustrates the information gain of a spectral measurement. Plotted after Eq. 4.10

Ideally, in the case of perfect overlapping spectra, $H_\lambda = 2$ bit. The information gain, provided the wavelength λ has been measured, is then given by:

$$I(\lambda) = 2 - H_\lambda\,. \tag{4.10}$$

The resulting function for our realistic source is plotted in Fig. 4.6. To know the *total information gain*, we have to average Eq. 4.10 over all possible wavelengths. Assuming an a priori probability $p^{pr}(i) = 1/4$ for $i = 1 \ldots 4$, this is given by:

$$\begin{aligned} I_{totgain} &= 2 - \sum_{i=1}^{4} \int_\lambda H_\lambda \cdot p(\lambda|i) \cdot p^{pr}(i) \mathrm{d}\lambda & (4.11) \\ &= 2 - \frac{1}{4} \sum_{i=1}^{4} \int_\lambda H_\lambda \cdot s_i(\lambda) \mathrm{d}\lambda = 0.0152\,. & (4.12) \end{aligned}$$

The result presented in 4.6 can be better understood by means of an example. Assume we want to transmit the bit sequence resulting from tossing a coin one million times (`1` for head and `0` for tail). If the coin is fair (head and tail occur with the same probability), we will need exactly one million bits to send the whole sequence. In this case the coin toss is said to have 1 bit information. Imagine now the coin is biased in such a way that head occurs with 1/100 probability and tail with 99/100 probability, then it can be shown that there exists an optimal coding which allows to send the entire sequence with only 23273 bits. So it seems that in the biased case the coin has a lower amount of information, namely 23273/1000000=0.0233 bit. The same concept apply to

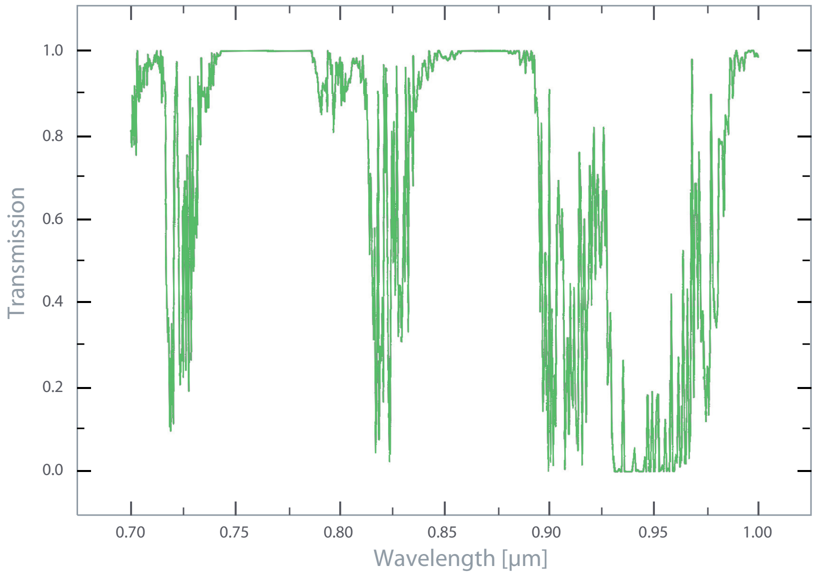


Figure 4.7: Diagram of atmospheric transmission from the earth surface in space after the LOWTRAN-Code (Los Alamos National Laboratory, USA). Picture adapted from [GRTZ02]

our source. The less biased is the system, the more information is needed to transmit the sequence, hence the more information is carried by every single photon.

4.2 Quantum Channel

The quantum channel of our QKD experiment is free-space, i.e. photons propagate through air. This is made possible because of the very low absorption coefficient of the atmosphere in the near infrared window between 740 and 820 nm and between 830 and 860 nm (see Fig. 4.7). Fortunately, there exist also efficient detectors for this wavelength region. Moreover, atmospheric birefringence and dispersion are negligible at these wavelengths. The only requirement is a free line-of-sight between transmitter and receiver unit.
One major drawback in free-space setups resides in the undesirable dependance of the transmission on weather conditions. While, with clear air, the attenuation for 860 nm can be lower than 0.2 dB/km, this rises to 2-10 dB/km in case of moderate rain, until 20 dB/km under heavy rain up to 100 dB/km in clouds.

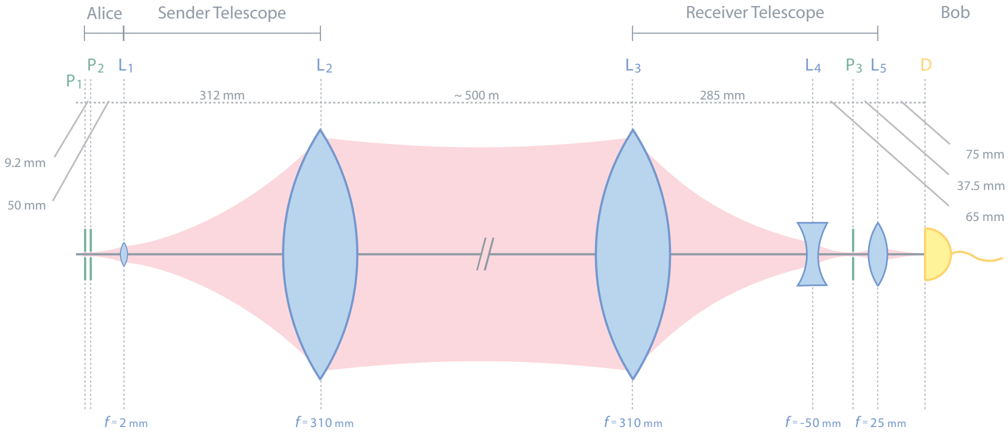


Figure 4.8: Scheme of the optical arrangement for sender and receiver unit. L_{1-5}: lenses, P_{1-3}: 100 μm Pinholes.

free-space quantum link has a length of 500 m. To enhance transmission efficiency, two telescopes at sender and receiver sides make sure to collect as many photons as possible. Furthermore, the optical arrangement shown in Figure 4.8 is necessary. The telescopes at both sides share the same front lens (L_2 and L_3) with a focal length f = 310 mm and open aperture a=75 mm, while the remaining optics is chosen to match the different requirements for sender and receiver.

On Alice' side, the spatial filter formed by the two pinholes P_1 and P_2 defines the initial beam parameters, which result in a beam waist w_0 = 50 μm located in the middle between the pinholes. The following lens (C150, f=2 mm) is used to increase the small beam divergence, adapting it to the aperture of the telescope lens L_2. After L_2, the beam propagates in free-space with a calculated new waist w_0 = 1.55 mm located in the middle between the two telescopes. On the receiver side the beam is collected by a second telescope consisting of the three lenses L_3, L_4, L_5 and a pinhole P_3 (diameter 100 μm), to reduce background light contributions. The position of the pinhole is chosen to be in the focal plane of the system formed by L_3 and L_4, hence maximizing transmission. Finally the lens L_5 images the P_3 onto Bob's detectors.

Automatic Alignment

Once the telescopes of Alice and Bob are aligned, one could think of fixing the components in that position and leaving the system untouched. Unfortunately, because of thermal expansion of the buildings and the equipment, a progressive misalignment between the two telescopes occurs until the transmission drops to very low values. Therefore, to maximize the transmission rate between Alice and Bob, an active alignment procedure has been implemented. First of all, two stepper motors driving micrometer screws control the two tilt angles of each telescope, one with respect to the horizontal plane and the other with respect to the vertical. The signal for the correct alignment is directly obtained from the single photon count rate of Bob's detectors.

The idea behind the tracking procedure is to initially keep the sender unit fixed and to move the receiver's telescope around the gaussian intensity profile $I(x, y)$ of the incoming photon mode. Assume the peak intensity is at point $(0, 0)$ and Bob's telescope current position is (x_0, y_0), then expansion of the intensity around (x_0, y_0) is given by:

$$\begin{aligned} I(x,y) &= I(x_0,y_0) + \left.\frac{\partial I}{\partial x}\right|_{x_0,y_0} (x-x_0) + \left.\frac{\partial I}{\partial y}\right|_{x_0,y_0} (y-y_0) \\ &\quad + \mathcal{O}\left((x-x_0)^2, (y-y_0)^2\right) \end{aligned} \tag{4.13}$$

To scan the intensity profile, Bob's telescope moves along a circle of radius r centered at x_0, y_0, with angular frequency ω_c, so that the position at time t is given by: $(x(t), y(t)) = (x_0 + r\cos(\omega_c t), y_0 + r\sin(\omega_c t))$. Plugging these values in Eq. 4.13, yields the following expression for the time dependent intensity profile:

$$I(x,y;t) = I(x_0,y_0) + \left.\frac{\partial I}{\partial x}\right|_{x_0,y_0} r\cos(\omega_c t) + \left.\frac{\partial I}{\partial y}\right|_{x_0,y_0} r\sin(\omega_c t) \tag{4.14}$$

In the above equation and in the following discussion, terms of order higher than one will be neglected. In order to know the direction in which the telescope should be moved, the first partial derivatives with respect to x and y need to be estimated. This cannot be done directly, but can be achieved with some mathematical manipulations. If we multiply $I(x, y; t)$ by a factor $\cos(\omega_c t)$ we get:

$$\begin{aligned} I(x,y;t) &= I(x_0,y_0)\cos(\omega_c t) \\ &\quad + \left.\frac{\partial I}{\partial x}\right|_{x_0,y_0} \frac{r}{2}\left(1+\cos(2\omega_c t)\right) + \left.\frac{\partial I}{\partial y}\right|_{x_0,y_0} \frac{r}{2}\sin(2\omega_c t) \end{aligned} \tag{4.15}$$

The constant term is proportional to the first derivative of I with respect to x. A similar consideration applies for the y direction, this time by multiplying

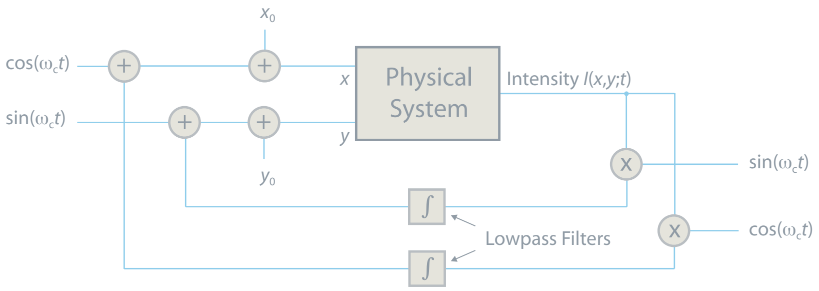


Figure 4.9: Schematical diagram of the tracking algorithm for the automatic alignment. The procedure runs without user interaction over several hours.

$I(x,y;t)$ with $\sin(\omega_c t)$. Thus, both constant terms can be isolated from the time varying contributions through a digital low pass filter (integrator) and analyzed separately. Similarly to the lock-in amplification technique, the signal modulation has to be applied at the source of the signal too. Hence, the same has to be done with Alice' telescope with another angular frequency, which has to be chosen not to be an integer multiple of ω_c, nor too close to it, otherwise it could not be filtered by the integrator in Bob's lock procedure. The tracking algorithm can be summarized in the following steps:

1. Set initial values for r and ω_c at both sides.
2. According to the actual position, the next step on the circle is calculated at both sides.
3. Alice an Bob move to the point calculated in step 2.
4. Bob measures the intensity I_{act} at this new position.
5. I_{act} is multiplied with sin and cos functions of the two frequencies, and passed through four filters (two per direction and telescope).
6. If a circle is completed, a new center is calculated adding the filter output to the old center. If not, this step is skipped.
7. Go to step 2.

A further improvement in the procedure has been added to minimize transmission losses. These arise from the following situation: when both parties have found the point of maximum intensity, the telescopes perform circles around this maximum. If the raddi are big, this would lead to high losses. On the other hand, bigger radii accelerate the seeking procedure if they are far from the maximum. Therefore, an additional routine has been implemented. It consists of the variable choice of the circle radii. The closer to the maximum, the smaller become the radii and vice versa, thus preventing from big losses if they are close to the peak, and on the other hand, accelerating the search if they are far from it.

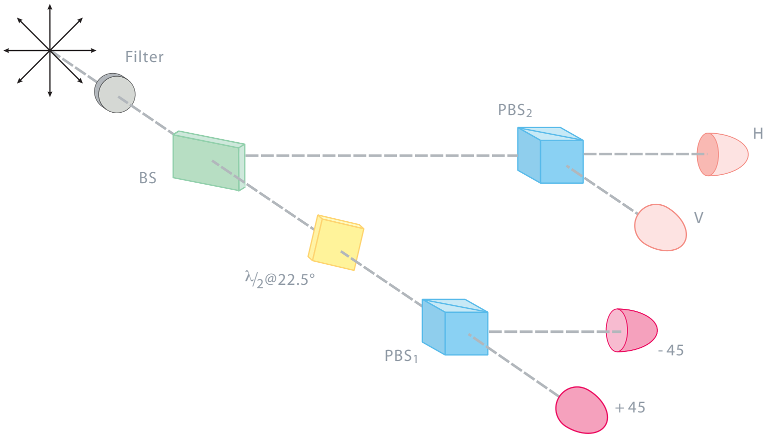


Figure 4.10: Optical setup for the polarization analysis. The initial 50/50 BS provides the passive random choice of the measurement basis.

4.3 Receiver Unit: Bob

This unit is responsible for the detection and polarization analysis of the photons sent from Alice. As single photon detectors, four passively quenched silicon APDs, one for each polarization state, are used. The setup for polarization analysis is illustrated in Fig. 4.10, and is based on an original idea by John Rarity and Paul Tapster [RT]. After passing an initial special interference filter, the incoming photon undergoes a passive random choice of the bases, using a 50/50 beam splitter (BS). The BS randomly directs the photon to a polarization analyzer either in the $\{|+\rangle, |-\rangle\}$ or $\{|H\rangle, |V\rangle\}$ basis. The polarization analysis in $\{|H\rangle, |V\rangle\}$ basis is performed by sending the photon onto a polarizing beam splitter (PBS) with an APD at each output port. The analysis in the $\{|+\rangle, |-\rangle\}$ basis is similar but the photon polarization is initially rotated by 45° using a $\lambda/2$ polarization plate for 850 nm, tilted by an angle of 22.5°. Thus, a click in one of the four photo diodes corresponds to the detection of a defined polarization state: $|H\rangle$, $|V\rangle$, $|+\rangle$ or $|-\rangle$ respectively.

Figure 4.11 illustrates the setup used to adjust the $\lambda/2$ retardation plate inside the receiver unit at the right angle. For this purpose a 5 mW (maximum optical power) laser diode operated in cw mode at a wavelength of 850 nm is placed in front of the Bob module. First, a PBS defines the initial beam polarization, then a $\lambda/2$ plate rotates the polarization by an angle which can be continuously varied by means of a micrometer stepper motor. Finally, a lens of focal length f =75 mm focuses the beam onto the four detectors. The stepper motor rotates the retardation plate in 4° steps and, at each step, the single photon count rate of all four detectors is sampled. The resulting curves

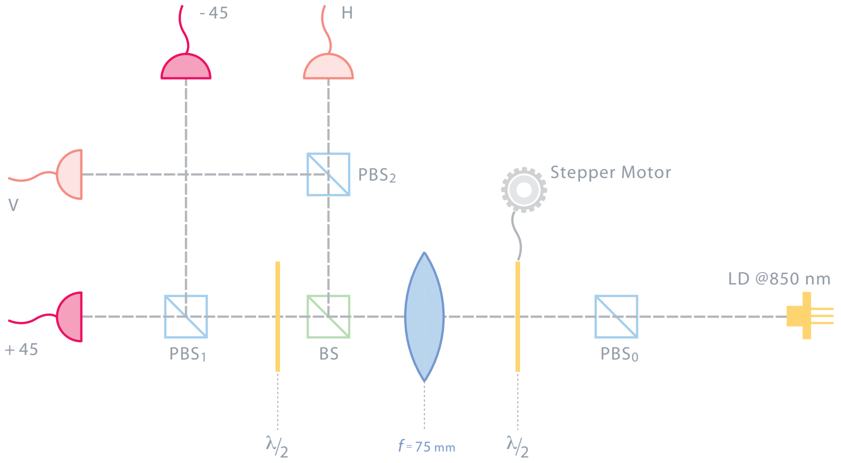


Figure 4.11: The setup used to adjust the $\lambda/2$ retardation plate at the right angle of 22.5°.

are shown in Fig. 4.12. The *visibility* of detector i is defined by:

$$V_i = \frac{(I^i_{max} - I^i_0) - (I^i_{min} - I^i_0)}{(I^i_{max} - I^i_0) + (I^i_{min} - I^i_0)} = \frac{I^i_{max} - I^i_{min}}{(I^i_{max} - I^i_0) + (I^i_{min} - I^i_0)} \quad i = 1 \dots 4 \tag{4.16}$$

where I^i_{max}, I^i_{min} and I^i_0 are the maximum, minimum and dark count rates of the i-th detector. The right orientation of Bob's $\lambda/2$ plate corresponds to the simultaneous maximum visibility for all four detectors and to a phase shift of 45° between $|H\rangle$ and $|+\rangle$ and between $|V\rangle$ and $|-\rangle$. The resulting visibilities, inferred from the data points in Fig. 4.12, are listed below:

Detector	Visibility
|H⟩	99.6 %
|V⟩	96.8 %
|+⟩	98.5 %
|-⟩	97.6 %

Table 4.2: The visibilities of the four detectors as inferred from the curves shown in 4.12.

All four detectors are mounted into two aluminum blocks, each of them cooled by a Peltier element, ensuring a constant operating temperature of -23 ° C. This is necessary to keep the dark count rate below 400 counts/s per detector. The Peltier module hot side is thermally coupled with the external aluminum

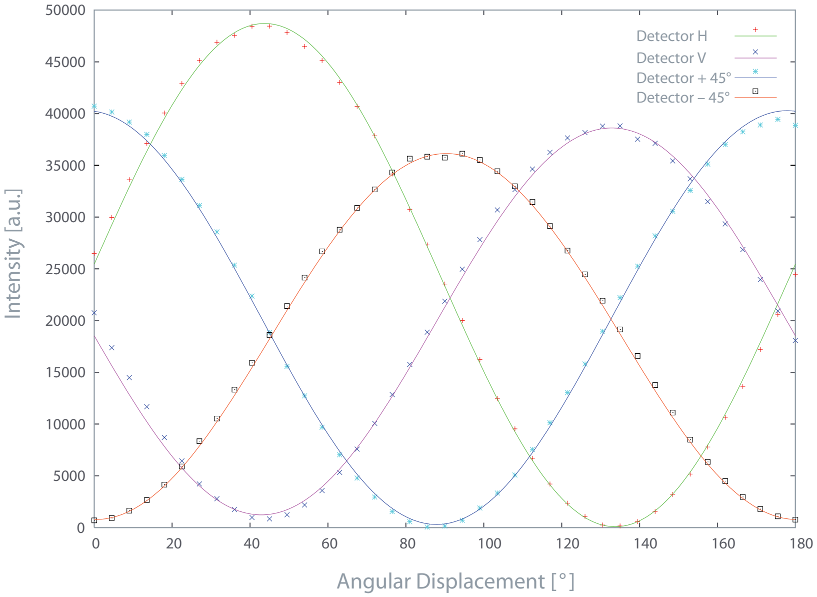


Figure 4.12: Visibility curves for the four detectors. The different peak values arise from the slightly different detector efficiencies. The experimental data points are fitted with sinusoidal curves.

case, which acts as a heat sink. The silicon-based APDs are operated in Geiger mode, therefore a large voltage is applied in the reverse direction. In the experimental setup this amounts 225 V (15 V above breakdown).
The Bob module provides four NIM (logical 0 is 0 V, logical 1 is -1 V) outputs, one for each detector. Whenever an avalanche is triggered, the consequent voltage pulse is compared with a threshold value, distinguishing between background noise and detection events. If the detection event occurred, the voltage rises above threshold and the respective channel produces a logical 1.

4.4 Synchronization

For the successful implementation of the BB84 protocol, Alice and Bob have to "speak" about the same photons. As a consequence, every event sent out by Alice, as well as any detection event at Bob's side must be somehow tagged to allow the sifting procedure to actually compare the same qubit. For this purpose, a **synchronization** routine is implemented in the protocol.
First of all, a timestamp card labels every detector click at the receiver side with their detection time, in units of 1/8 of nanosecond. Notice that a fraction of those events won't correspond to photons sent from Alice, but rather from detector dark counts or background photons. If Alice and Bob would

dispose of extremely precise oscillators, they could agree on their respective start times, and let the procedure run without any further concerns. Unfortunately, their hardware clocks are not sufficiently synchronous, leading to different clock frequencies of sender and receiver. Moreover, Alice and Bob probably started their clocks at different times, hence the receiver will suffer from a constant shift in the detected photon number. To overcome these problems, a synchronization algorithm was developed (see [Wei03] for implementation details). The basic idea exploits the approximate knowledge of the local repetition frequency $\omega_{send} = 2\pi \cdot 10$ MHz used to send out photons. As it will be shown here, we do not have to know this repetition frequency with extremely high precision. First, Bob has to identify the local frequency of the detected photons. This is done by performing a discrete FFT of the detected signal, given by[3]:

$$h(t_j) = \sum_i \delta_{t_i,t_j} , \tag{4.17}$$

where t_i denotes the timestamp of the i-th detection event (integer in unit of 0.125 ns). At the time t_j, where a click has been recorded, the function has the value 1, otherwise it is 0. Since background events and dark counts are uniformly distributed over the whole frequency spectrum, the resulting FFT will show a sharp peak corresponding to the local frequency of the detection events ω_{det}.

The next task is to calculate the time-dependent phase shift between Alice and Bob due to the frequency difference of their local oscillators/clocks . This is accomplished noting that this phase difference is a linear function of time. A linear regression algorithm applied to the line $\phi(t) = 2\pi\omega_{det}t_i + \phi_0$, yields the value for the initial phase shift ϕ_0, while the slope can be used to estimate the frequency with higher precision. Once frequency and phase shift are known, we are able to distinguish between “good” and “bad” events. Good clicks are those which fall within a narrow time window around an anticipated click according to the sender frequency, and the rest are bad events. This procedure allows Bob to assign each of the detected photons a well defined number.

However, there is still an unknown global offset relative to Alice’ number, due to different starting times. To obtain this global offset Alice divides the stream of outgoing photons into frames of fixed length. The beginning of each frame contains a header, which is known to Bob, consisting of the frame start (FSI = frame start identifier, see fig. 4.13) and of the frame number (FNI = frame number identifier). The FSI consists of a pseudo-random bit pattern, repeated

[3] Actually, since the frequency is already roughly known, it is sufficient to consider a frequency interval around $\omega_{send}/2\pi$. This is done by mixing down the spectrum of $h(t_j)$ with a frequency not too far from 10 MHz and then calculating the FFT of the resulting function.

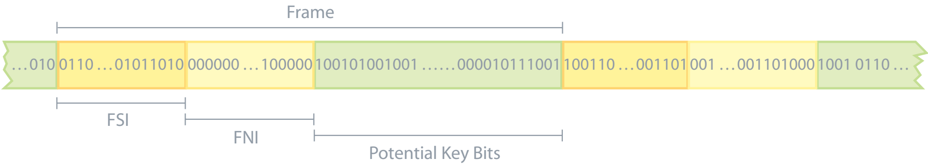


Figure 4.13: Example of the implemented frame partition. Each frame is splitted into three sub-blocks. The first contains a pseudo-random sequence which is used to identify the frame start. The second embodies the information relative to the absloute frame number and the rest is a sequence of potential key-bits.

in every frame, encoded with the presence (1) or absence of photons (0). To enhance Bob's detection probability, whenever a 1 has to be sent, all four diodes are switched on simultaneously. Once the key-bit string is divided into blocks of the frame length, it is easy to efficiently identify the FSI with the help of a FFT.
The last step is to assign an absolute number to every frame. This piece of information is embodied in the FNI pattern, again a fixed pseudo-random bit sequence which gets progressively shifted by one place for every consecutive frame. This would give the necessary redundancy which prevents from channel losses, while a FFT helps to efficiently locate the pattern in the received bit string.

4.5 Conclusion

The interaction of all parts described above provides a real QKD device between Alice and Bob. Key-exchange tests have been successfully carried out with this setup in different experimental runs (see [Reg05]), leading to several gigabytes of secure key material. All runs took place during the night, since no daylight operation could be implemented yet. The mean photon number μ was set to 0.1 photons/pulse, but, due to the missing temperature stabilization, oscillations in the value of μ could not be excluded.

As an example, we refer to the results obtained in one of these tests. Thanks to the tracking algorithm, a constant raw-bit key rate between 200 and 300 kcounts/s could be held for about 13 hours. All these detection events occurred within a time window of 10 ns around the expected photon arriving time. A maximum sifted-key rate of 66 kbit/s has been achieved, with a QBER of 2.8%. Since every detected photon has 50% probability to be analyzed in the right basis, one would expect a sifted-key rate equal to one half of the raw-key count rate. The fact that the sifted-key rate results in a lower value, is the direct consequence of how the sifting procedure works. After that the good detection events have been identified by the synchronization routine, a buffer memory is filled with the relevant information relative to those events.

In the sifting procedure Bob sends 1kB long blocks from the buffer memory out to Alice through the 10 Mbit/s public ethernet connection and **waits** until these have been processed by Alice and the result sent back to him. As a consequence of this real-time procedure, only half of the classical channel bandwith is exploited, leading to the fact that, at high count rates, the buffer is overwritten before all stored data can be transmitted.

The influence of bad weather conditions has also been tested. In the case of a heavy snow fall the transmission sank approximately to 20 kcounts/s and the sifted-key rate stabilized to the half of that value, because the buffer memory could be processed with the same speed as it was filled by the synchronization routine.

Concluding, we could provide the needed theoretical and technological background for the implementation of a potentially unconditional secure point-to-point cryptographic system based on quantum mechanical principles. After a rough initial alignment, the setup is able to keep a stable link between sender and receiver unit for several hours without user interaction. An error correction and privacy amplification routine further enhance the security level. The maximum reachable sifted-key rate is about 66 kbit/s, slightly higher than the ISDN bit rate. Different weather conditions influence the transmission; however a sifted-key rate of 10 kbit/s could be achieved in very bad weather conditions. A further improvement regards the temperature stabilization of the source, which is the topic of the next capter. This has two main advantages. The one is that it enhances the security against PNS attacks, yielding a constant mean photon number, hence a predictable multi-photon contribution which can be taken into account in the privacy amplification routine. The other is that the spectral characteristics of the laser diodes become independent of the temperature oscillations in the environment. This could allow the application of a spectral filtering for ambient light, improving the daylight operation of the apparatus.

5 Temperature Stabilization

5.1 The Main Idea

One major drawback that still limits the widespread feasibility of free space based quantum cryptography networks, is the limited performance, in terms of key-exchange rate, of such devices by daylight. This is mainly due to “ambient” photons that don’t belong to the set of qubits sent by Alice. In the previous section we mentioned two possible ways to reduce the undesired contribution from background light entering the system. One method exploits the spatial filtering of the light detected by the receiver unit by means of a pinhole placed in the optics. The other possibility is to filter by time-dependent procedures. As discussed at the end of the previous chapter, a time bin around an expected photon is used for the selection of good clicks. Unfortunately, as soon as stray light from the sun comes into play, both procedures are too ineffective. A key exchange is not possible any more, since detector count rates rise above the saturation limit.

However, to overcome this problem, another possible approach, based on the spectral filtering, is possible. For this purpose, a narrow band interference filter has been added to the optics at receiver’s side. To ensure that the transmission rate is not affected by the new component, the wavelengths of the source diodes have to be carefully selected to have their central wavelengths not too far from 850 nm. Another problem arises from the strong dependence of laser diodes spectral characteristics on their operation temperature. Since the whole apparatus operates in an open environment, it is subjected to both daily and seasonal temperature oscillations. Therefore, a temperature controller circuit, based on a thermoelectric cooling (TEC) device, has been realized and integrated into a new design for the transmitter mounting.

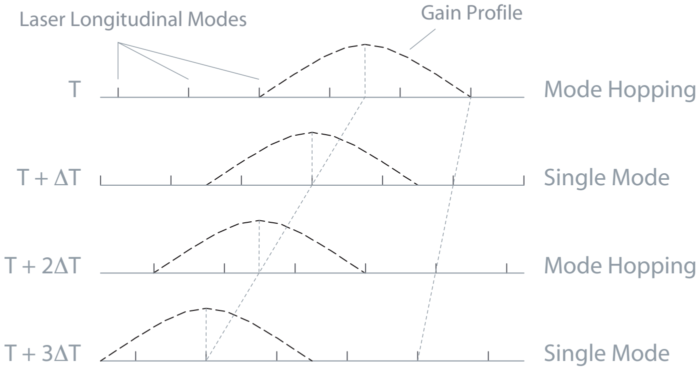


Figure 5.1: The gain profile and mode wavelengths are temperature dependent. When the gain peak is centered on the mode, the laser runs single mode. If the gain peak happens to be between two modes, the laser mode hops.

5.2 Thermal Management

5.2.1 Spectral Dependency

As stated before, the spectral and electrical characteristics of semiconductor laser diodes are very sensitive to different environmental conditions. In particular, for a given current, their lasing wavelength and power output will be affected by oscillations in the temperature[1]. As experimental fact, the mode wavelengths and the gain peak wavelength depend on the laser's temperature. The mode wavelength shift is caused by the change in the index of refraction of the material as well as thermal expansion of the cavity with the temperature. The gain peak shift is caused by the temperature dependance of the band gap. Hence, as the laser temperature increases, the gain peak goes through the modes one at the time. If the gain peak happens to be in the middle between two modes, the laser mode hops (see Fig. 5.1). This dependancy has been measured, leading to the curve in figure 5.2, where data points are fitted with a straight line. The experimental data were taken at four different case temperatures (T_c) of a 5 mW (max. optical power) laser diode. The laser operates nominally at a wavelength of 850 nm at 25 °C. T_c was stabilized with a temperature controller, keeping the output power at a constant value of 2 mW. The rate of temperature change inferred from the measurement was 0.23

[1] As an example consider that a temperature rise of 15 °C, causes a fall in optical power of typically 17%. This dependance will affect for instance the mean photon number of our source

nm/K, which means a central wavelength around 845 nm for our laser diode source.

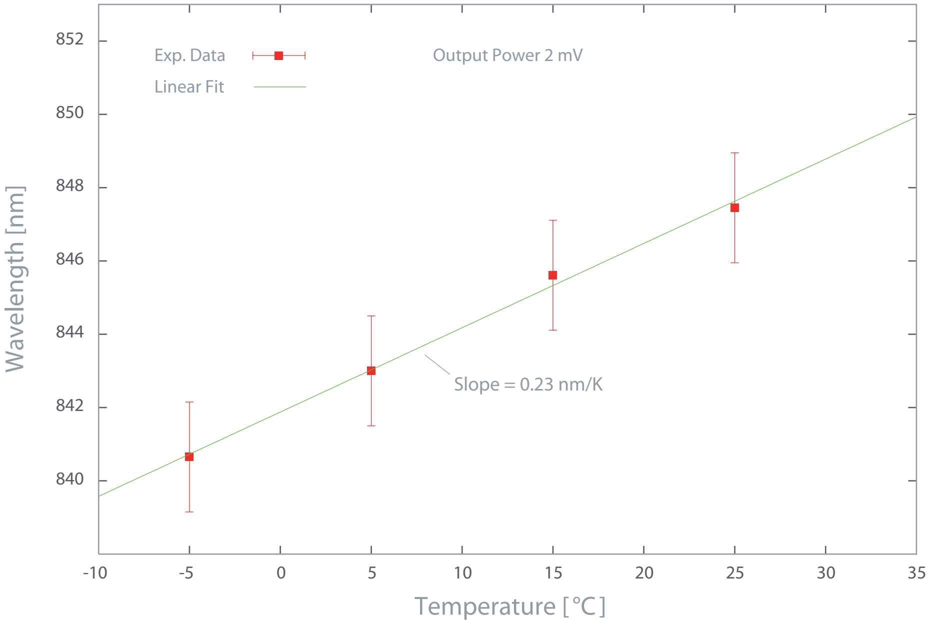


Figure 5.2: The wavelength characteristics of a semiconductor laser diode plotted against its case temperature. The temperature-dependent resonator length causes the laser to jump to the next longitudinal resonating mode as the case temperature increases.

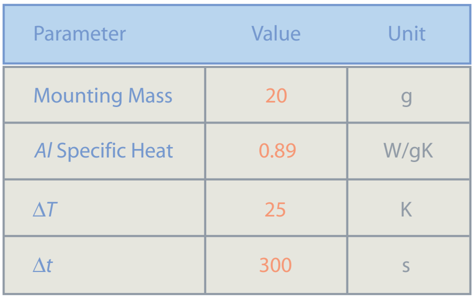
5.2.2 Preliminary Analysis

The four laser diodes are mounted in a cylindrical aluminum housing. The metallic cases of the diodes are thermally contacted by means of a heat-conducting silicon paste, to facilitate the heat flow through the surrounding housing. The starting point of our analysis consists of fixing the operating temperature we want the source to work at. Since the aim is to let the apparatus run without user interaction during the whole day, in hot as well as cold months, our choice should be a good trade-off between cooling and heating power at our disposal. Temperatures of the environment in summer can be as high as $+40$ °C, in winter as low as -15 °C.

A reasonable choice seemed to be around $+15$ °C, thereby considering a positive contribution from the laser diodes in a cold environment (they help heating) and a negative one in a hot environment (additional heat has to be removed). The first task is a rough estimation of the maximum cooling power W_{max} needed to cool down the mounting. This can be done using the formula:

$$\langle W \rangle = m \cdot c_{Al} \cdot \frac{\Delta T}{\Delta t_{steady}} \ , \tag{5.1}$$

where $\langle W \rangle$ is the mean cooling power (in Watt) needed to change the temperature of the housing from the initial to the final value, $\Delta T = T_i - T_f$ (in K), in the time Δt_{steady} (in seconds). Other parameters are m, the mass of the housing (in grams, including the conical mirror and front lens mounting) and c_{Al}, aluminum specific heat (in W/gK). Values from the experiment are listed below:



Parameter	Value	Unit
Mounting Mass	20	g
Al Specific Heat	0.89	W/gK
ΔT	25	K
Δt	300	s

Table 5.1: The relevant parameters needed for the temperature stabilization of our source.

Thereby, a maximal environment temperature of T_i =+40 °C, an operating temperature of T_f =+15 °C and a relaxation time of 300 seconds have been chosen. Plugging these values in Eq. 5.1 we get $\langle W \rangle \approx 1.5$ W. This gives a lower bound for the cooling system we should make use of. A more realistic approach consists of using the heat equation, which states that the rate of heat loss in a body is proportional to the difference in temperatures between the body and its environment. The latter has to be defined yet. Our purpose is to cool down the aluminum case, at the beginning in thermal equilibrium with the ambient, by thermal contact with the cold side of a Peltier element at temperature T_f. Hence our colder environment is the Peltier's cold side and the temperature of the body is that of the environment. With these boundary conditions the heat equation reads:

$$\frac{\mathrm{d}T}{\mathrm{d}t} = -\frac{1}{\tau}\left(T_i - T_f\right) \ . \tag{5.2}$$

The solution to 5.2 is an exponential decay of T with time constant τ:

$$T(t) = (T_i - T_f)e^{-t/\tau} + T_f \ . \tag{5.3}$$

It will result useful to calculate the derivative of Eq. 5.3, or alternatively, to substitute $T(t)$ in Eq. 5.2. We get:

$$T'(t) = \frac{(T_f - T_i)}{\tau} e^{-t/\tau} \; . \tag{5.4}$$

After the time τ, the body has reached a temperature $T(\tau) = (T_i - T_f)/e + T_f \approx$ ≈ 24.2 °C, while after 4 time constants, $T(4\tau)$ differs from T_f only by 3%. This can be made clear if we write the instantaneous form of Eq. 5.1:

$$W(t) = Q'(t) = m \cdot c \cdot T'(t) \; . \tag{5.5}$$

For t large enough, $T'(t) \to 0 \Leftrightarrow Q'(t) \to 0$ which means that in the steady state, the heat removed equals the heat absorbed from ambient in the unit time, thus no change in the temperature occurs. If we assume that this happens approximately after a time $t = 4\tau$, we can get an estimate for τ. To achieve this, we just set $4\tau_{est} = \Delta t_{steady}$, and get $\tau_{est} = 75$ s. With this knowledge is easy to deduce an useful value for W_{max}. From Eq. 5.5, we only need to maximize the function $T'(t)$. To do this, notice that the derivative of Eq. 5.4 is also a monotone decreasing function, meaning that $T'(t)$ has its maximum at $t = 0$, leading finally to:

$$W_{max} = m \cdot c_{Al} \cdot T'_{max}(t) = m \cdot c_{Al} \cdot \frac{(T_f - T_i)}{\tau_{est}} \approx 6 \,\mathrm{W} \; . \tag{5.6}$$

So far, we neglected possible heating from the operation of the laser diodes. Since these are low-power devices, we will show that their contribution can actually be considered very low. The current they draw is in the 10-20 mA range, while the voltage across them doesn't exceed a few volts. Hence, assuming that the whole electric power is dissipated in warming up the case, the total amount of transferred heat per unit time is below 0.2 W.

5.2.3 TEC Device

Once the cooling power has been estimated, we proceed now with a detailed description of the components which are needed for the temperature stabilization. Due to the moderate amount of the previously estimated heat flow, we can design our cooling system in such a way to keep the setup as compact as possible. For the cooling of small metallic parts, as in the case of our 20 g aluminum mounting head, the best solution is often represented by a thermoelectric cooler (TEC) element, a quite handy device which exploits electric energy to work as a heat pump in cooling mode (heating mode is also pos-

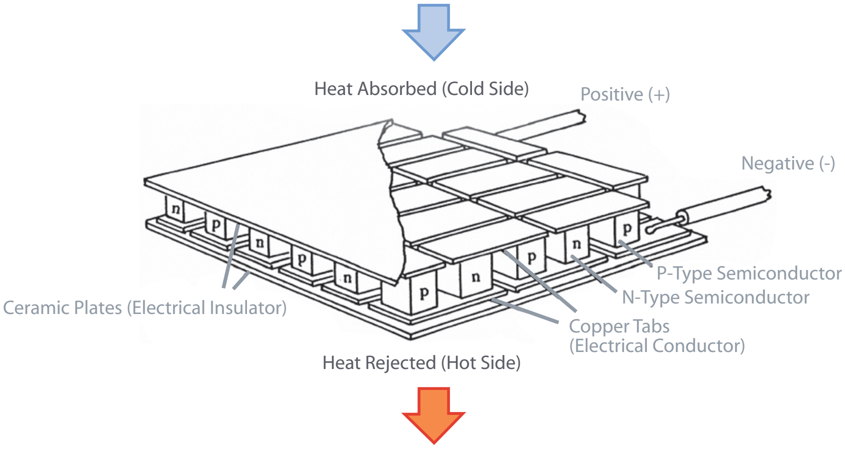


Figure 5.3: The picture illustrates the operating principle of thermoelectric cooling. An applied voltage causes electrons in the p-doped material to move from a lower to a higher potential, filling the energy gap with heat absorption from the upper side. When moving from the n- to the p-doped material they release energy instead, hence heating the lower side.

sible). The working principle of these devices is based on the Peltier effect[2]. Whenever an electric current is flowing between the terminals connecting two different matallic materials, a temperature difference arises.
Referring to Fig. 5.3, a solid state Peltier element is an ordered array alternating two types (n- and p-doped) semiconductor material (often Bismuth Tellurid), electrically connected in series by a metallic junction. On the top and bottom side, two ceramic plates provide electric insulation and heat transfer at the same time. The origin of the thermal activity resides in the different energy levels occupied by electrons while flowing from the negative to the positive terminal. In the heavily p-doped material, electrons are forced to move to a higher energy level (n-doped zone), thereby extracting the necessary energy from the top Peltier's side in the form of heat. The inverse happens at the bottom of the n-doped element, where heat is set free from electrons flowing to a lower energy level, hence heating the lower side. The alternating structure of such p-n couples enhances the overall cooling/heating effect. Inverting the polarity causes the Peltier to work in heating mode, i.e. the top side becomes hot, the bottom cold. For particularly demanding applications, more thermo-

[2] Actually, this is the inverse of the Seebeck effect, where different metals connected at two different locations, will develop a voltage difference if the junctions are hold at different temperatures. Application of this principle is the thermocouple thermometer, used for industrial temperature measurements.

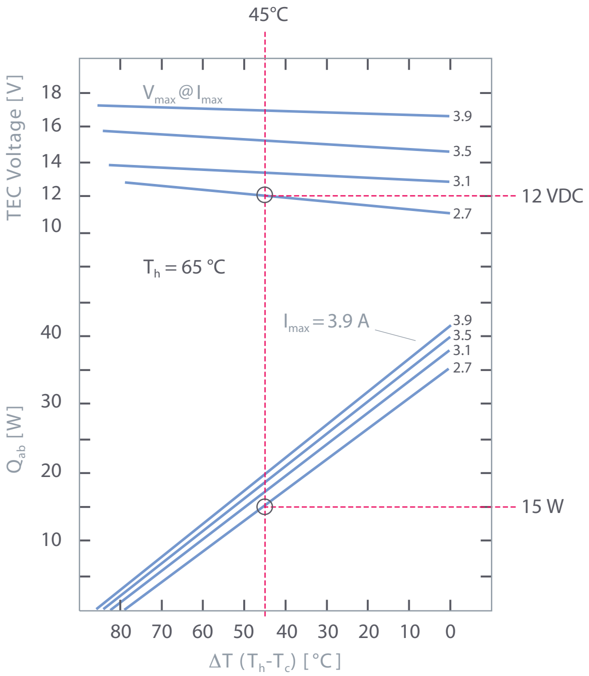


Figure 5.4: Performance curves for a typical one-stage Peltier element. Red lines serve to fix the operating point: given the desired amount of heat to be removed, 15 W in the example, ΔT is found to be $\Delta T = T_h - T_c = 45$ K at a current of 2.7 A, corresponding to 12 V across the Peltier (Source: Tellurex Corp., `http://www.tellurex.com/cthermo.html`).

electric stages are stacked on each other giving rise to cascaded devices, but this is obviously not our case.

The characterization of such a device happens through the specification of various parameters: T_c (T_h), Peltier's cold (hot) side temperature, ΔT_{max}, the maximum achievable temperature difference between Peltier's cold and hot side, Q_{max} (in Watt), the maximum heat rate that can be removed, I_{max}, the input current at ΔT_{max}, and V_{max}, the applied DC voltage at I_{max}. Manufacturers provide performance curves showing $\Delta T = T_h - T_c$ as a function of Q_{ab}, the absorbed heat rate at cold side, operating voltages and currents, such as the one in figure 5.4. Unfortunately, such curves depend on so many parameters, such e.g. Peltier's current and voltage, ambient temperature, heat sink characteristics, etc., that they provide only a rough approximation of Peltier's behavior under different conditions. Notice that the maximum heat that can be removed, Q_{max}, is defined for $\Delta T = 0$, which is of course just an idealization of real cases. To work properly, a TEC needs a heat sink for dissipating the large amount of heat accumulated at the hot side. If I_p is the total current flowing through the Peltier and R_p its resistance, the total heat rate at the hot side is given by:

$$Q_d = Q_{ab} + I_p^2 R_p \ , \tag{5.7}$$

where $I_p^2 R_p$ is the contribution from Joule heating[3]. Peltier elements come in a huge variety of size, shape and performance specifications. Our choice has been primarily guided by design considerations. In order to modify as little as possible the already existing setup, we opted for a special-designed, but commercially available, one-stage Peltier element with a central drill (see next section for the assembling details). The module is quite compact, being 22.5 mm large, 17.5 mm wide and 3.2 mm thick with a drill diameter of 9.5 mm. The specified Q_{max} is 19 W, $\Delta T_{max} = 69$ K, $I_{max} = 5.8$ A at a voltage $V_{max} = 5.3$ V. Its performance curve is a straight line given by: $\Delta T = -3.63Q + 69$. A CPU cooling block and an attached fan provide the necessary heat sink. Performance tests have been carried out both in simulated cold and hot environments, leading to the curve shown in fig. 5.5, in the case of ambient temperature of about 40 °C. To simulate the heating from the laser diodes, two of them, already damaged, were mounted in the housing and driven in constant current mode at 0.1 A. The absorbed heat at cold side, inferred from the exponential fit, was $Q_{ab} = 6.23$ W in good accordance with our previous estimation. The current drawn by the Peltier was 1 A and, with R_p=0.91 Ω, lead to $Q_d \approx 7.1$ W. This means a Peltier's hot side temperature of $7.1 \cdot 0.5 = 3.55$ K above ambient or about 43.5 °C, assuming a heat sink thermal resistance of 0.5 K/W.

5.2.4 TEC Controller Unit

There are generally two ways to drive a TEC: the open loop and the closed loop method. The former is basically a passive procedure, in which an operator adjusts the amount of current or voltage until the desired temperature is reached. The latter is an active procedure, in which the temperature is electronically adjusted by a controller unit. The closed loop continuously compares a set value with the actual temperature, monitored by means of a sensor placed inside the mounting, until their difference is regulated to zero. The sensor device is realized by a temperature dependent resistor, or thermistor[4]. The precise dependency of thermistor resistance, R_{th}, on the temperature is given by an exponential law:

$$R_{th} = R_0 \cdot e^{B(1/T_0 - 1/T)} \quad \text{or,} \quad 1/T = 1/T_0 + B \cdot \ln(R_{th}/R_0) \ , \tag{5.8}$$

[3] Due to the small cross-sectional and surface area of the mounting, both radiative and convective heat transfer contributions can be neglected.

[4] More precisely, the used sensor is a negative temperature coefficient (NTC) thermistor, meaning that the resistance value decreases with increasing temperature

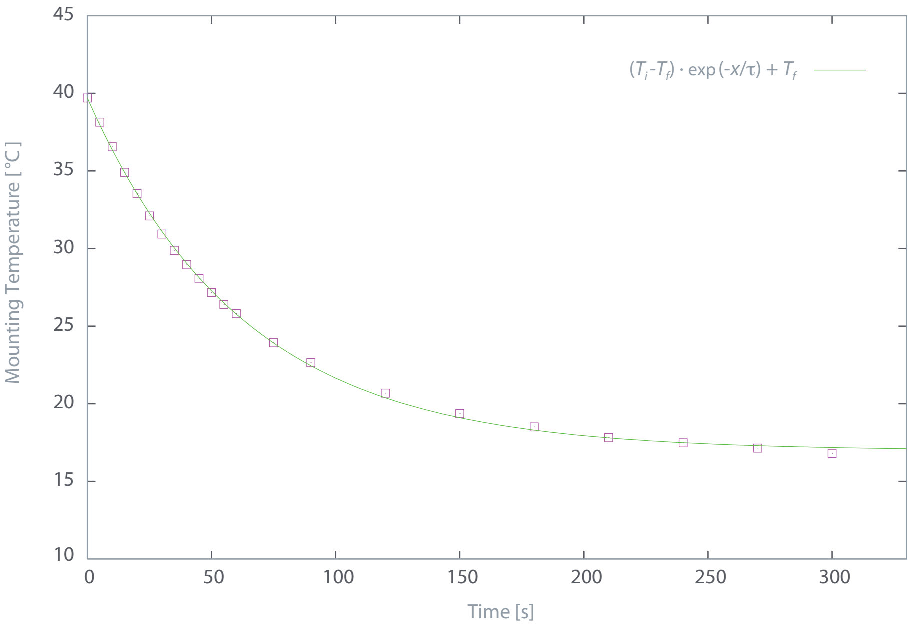


Figure 5.5: The temperature-time dependence fitted according to Eq. 5.3. The lower side of the mounting was held at a constant temperature of about 16.5 °C, while ambient temperature was slightly below 40 °C.

where R_0 in Ω is the resistance at a reference value T_0 in K, B is a characteristic thermistor parameter and T is the temperature in K. According to manufacturer's specifications these values are:
$R_0 = 10$ KΩ at $T_0 = 298.15$ K and $B = 3988$ Ω. Referring to Fig. 5.6, we proceed to the description of the block diagram single stages.

The input stage has two input signals V_{act} and V_{set}, both outputs of a voltage divider, given by:

$$V_{act} = V_Z \cdot \frac{R_{th}}{R_{act} + R_a} \tag{5.9}$$

$$V_{set} = V_Z \cdot \frac{R_{set}}{R_{set} + R_a} , \tag{5.10}$$

where $V_Z = 10$ V is the voltage from a Zener-diode stabilized voltage source, R_a=16 KΩ and R_{set} is the temperature set value in KΩ.
Both voltages feed successively the inputs of a differential operational amplifier (Diff OP) with a gain factor $K_{diff} = 3.5$, which ensures a differential output of about ±10 V in correspondence of a maximum voltage (temperature) difference at the input of $|V_{act} - V_{set}|_{max} = 2.9$ V. The output of the input stage is the amplified error, $e(t) = setpoint - measurement$, which will be a function

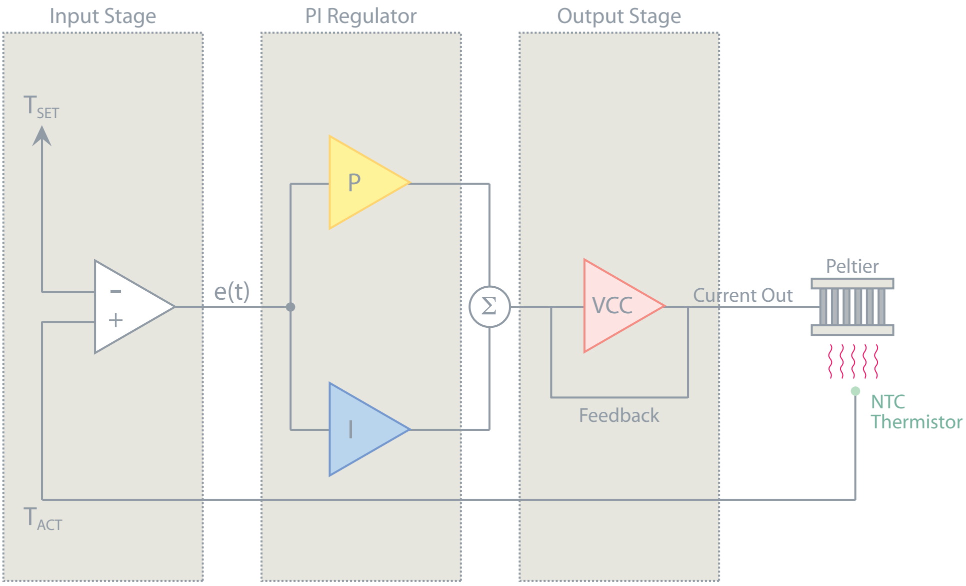


Figure 5.6: Block diagram of the closed-loop temperature controller used to drive the TEC. T_{set} is the setvalue, T_{act} is the measured value; their difference is amplified and constitutes the input stage for the proportional and integral amplifiers. The voltage-to-current converter adjusts the output current according to the signal at its input through a feedback loop.

of time. The next stage is a parallel PI (proportional-integral) regulator. The control law for this stage is given by:

$$m(t) = K_d \cdot e(t) + \frac{1}{\tau_I} \int_0^t e(\tau) \mathrm{d}\tau \ , \tag{5.11}$$

where K_d is the adjustable linear gain of the proportional component and τ_I is the integral time constant which can be varied through a potentiometer in the range $0.01 \ldots 1$ s. The integrator prevents from an offset in the output, the latter being unavoidable when implementing a proportional only controller. The output stage is a high power OP voltage-to-current converter which can supply up to 5 A to the TEC. The circuit feedback loop is designed in such a way that the amplifier will attempt to adjust its output current according to the error signal at its input. For this reason, the controller unit can be used to actively drive a TEC in cold as well as warm environments. For both cases various tests have been performed, leading to the curve in Fig. 5.7 for the cooling mode, while in a performance test in heating mode the system could achieve a set value of +18 °C in a environment at −20 °C. Finally, a good trade-off between overshooting and relaxation time of the system has been achieved with tuning methods.

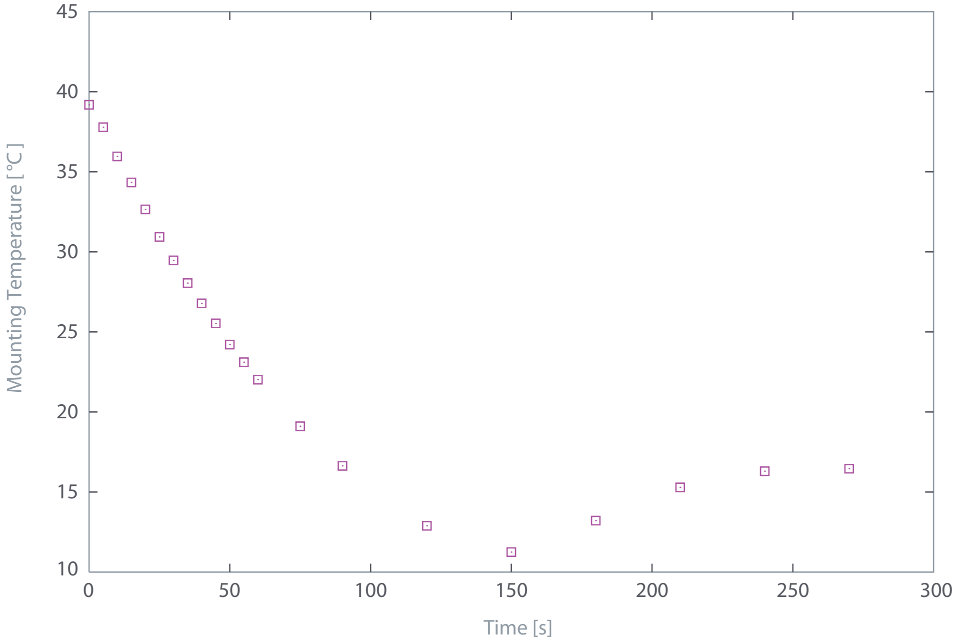


Figure 5.7: The mounting temperature variation with the time. The curve represents an overdamped oscillation, as expected from the controller adjusting procedure. The overshoot was about 4 °C below the final temperature.

5.3 New Design

The integration of the new cooling system required a slight modification of the existing setup. To keep things simple, a collinear design with respect to the optical axis has been conceived and beforehand simulated with the help of the CAD 3-D software Autodesk Inventor® (see Fig. 5.9). First, a tapped hole for a M6 screw has been bored in the conical mirror, in order to hold the head of a PVC screw. Once tightened, this will support the Peltier element and the aluminum heat sink and ensure sufficient pressure between the parts to favor the heat flow. Because conical mirror and heat sink operate at very different temperatures, when the TEC unit is on, it is important that the screw is made of a thermal insulating material like PVC or similar, to prevent from the detriment of the cooling/heating process. Successively, a new holder for the driving electronics has been directly mounted on the heat sink, leading to the final working prototype shown in Fig. 5.10.

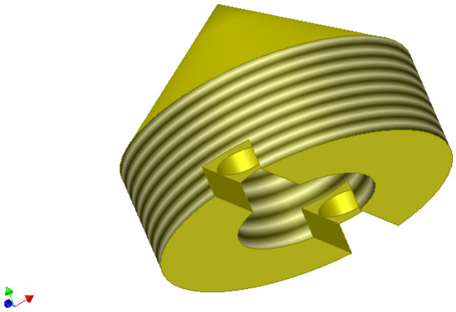


Figure 5.8: The modified conical mirror with the new M6 borehole in the middle for the PVC screw.

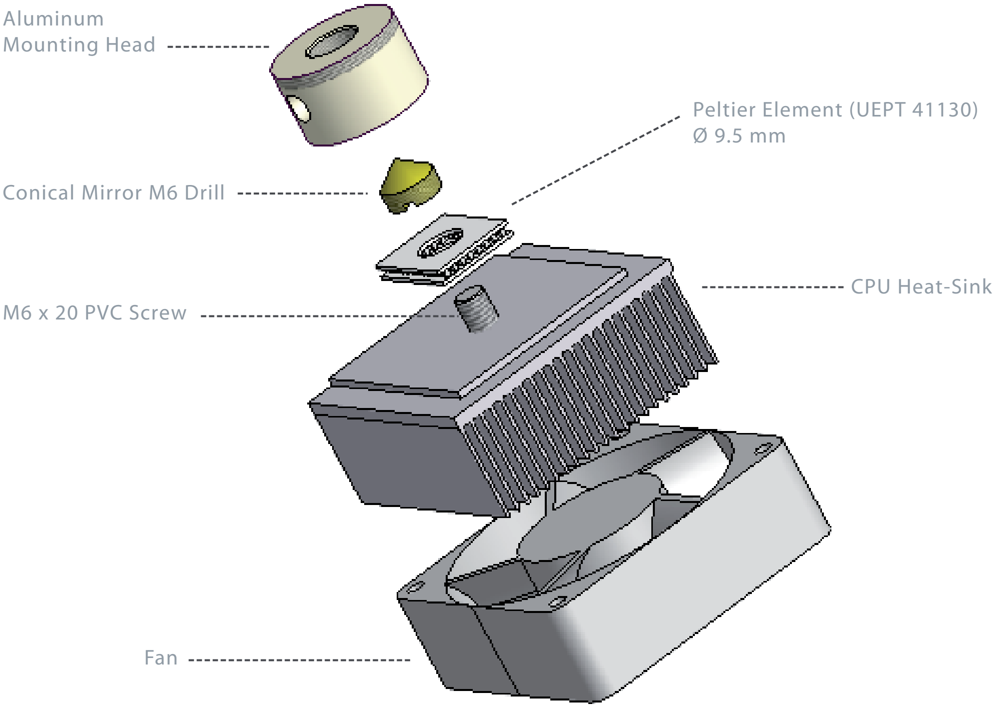


Figure 5.9: The new design of the source with Peltier cooling module and heat sink, as simulated with a 3-D CAD software. Driving electronics is not shown.

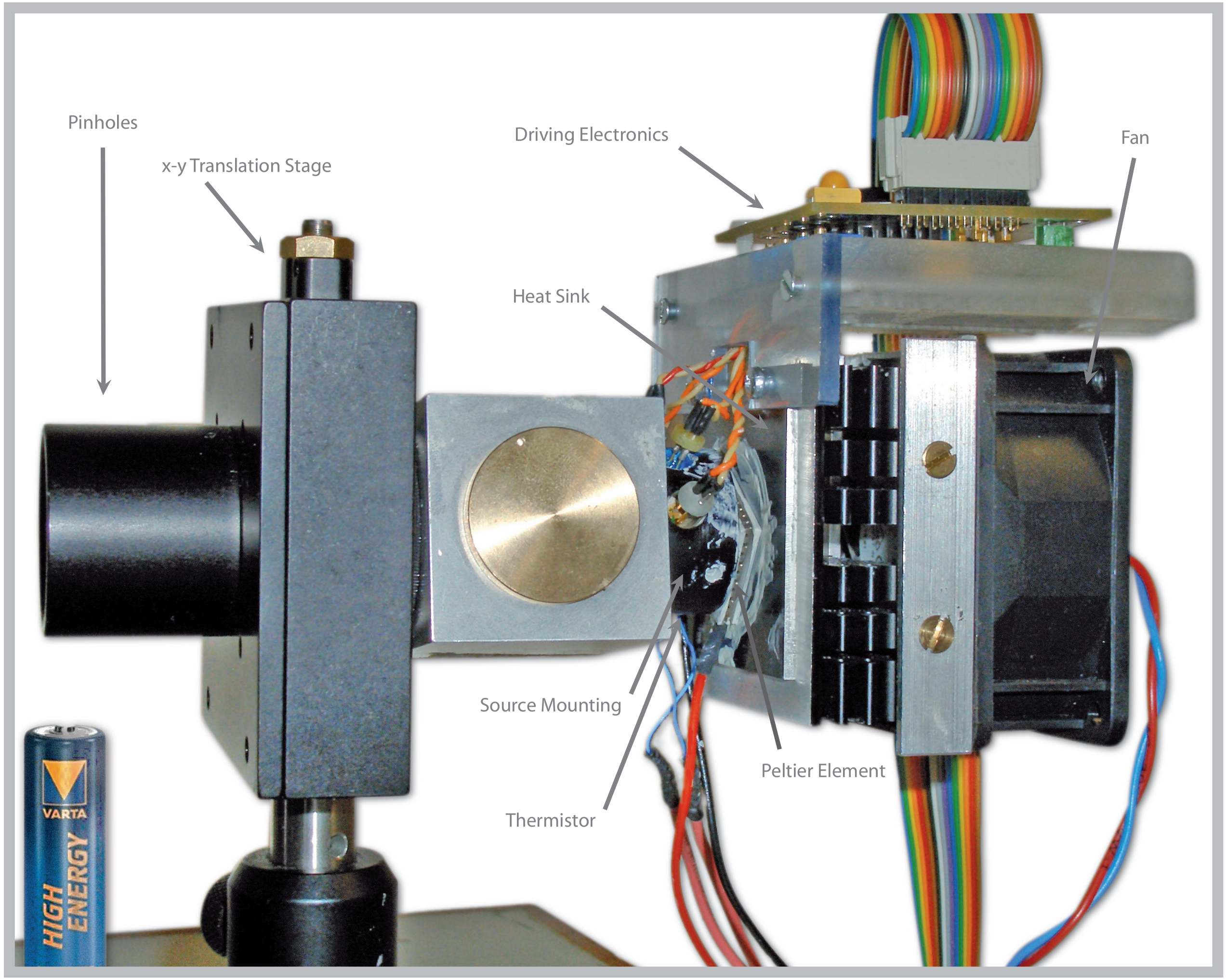


Figure 5.10: A picture of the final prototype projected to include the source temperature stabilization with the help of a TEC device.

6 Summary & Outlook

In this work, we presented the main ideas and underlying physical concepts for the realization of a potentially unconditional secure point-to-point cryptographic scheme realized with quantum optical devices. Our setup is designed to implement the BB84 four-state protocol over a free-space link of about 500 m, using weak coherent pulses for transmitting and four silicon-based avalanche photo diodes detectors for receiving. Information is encoded in the polarization states of single photons. An automatic alignment algorithm is able to keep a stable optical link between sender and receiver over several hours without user interaction. Software-based error correction and privacy amplification procedures complete the setup.

The QKD system could achieve transmission rates which are comparable with ISDN bit rates. Even in a bad weather environment, the raw-bit rate could be stabilized around 20 kbit/s. We also discussed possible security loopholes which could arise from multi-photon pulses and source spectral distinguishability, and how to minimize those risks. The so called decoy state protocol represents the solution for the first problem. The protocol is a powerful means to prevent from side-channel attacks relying on photon number splitting strategies. Concerning the second question, the information leakage due to slightly different spectral distributions of the sources has been estimated. Once this amount is known, it can be fed into the privacy amplification routine leading to a secure shared key.

One major limitation of free-space based cryptography is represented by its unability to operate by daylight, due to the high rate of detected background photons. To improve the compatibility with daylight, the idea of spectral filtering has been implemented. For this purpose, temperature stabilisation of the source is needed, and this has been achieved with the help of a thermoelectric device driven by a closed-loop PI controller. Performance tests with different environment temperatures and TEC devices have been carried out. The next step in this direction will be a key-exchange test carried out by daylight.

Should the daylight tests produce reasonable key rates, there would be all prerequisites for building a quantum-cryptography based network consisting of one sender and at least two receivers. Thinking forward in this direction, the next step could be the integration on large scale of quantum cryptographic devices into existing IT infrastructures[1]. A hybrid classical-quantum based protocol could manage the exchange of encryption keys over the quantum channel and succesively allow symmetric encryption algorithms to use those secure keys for exchanging sensible information.

Nevertheless, the main challenge QKD has to bear for becoming an usual tool in IT security, is the improvement of its operation range. As fo today, fiber based systems can afford a maximum link distance of about 100 km, while the free space record could be hopefully pushed up to 140 km within the next months. An idea how to extent this limit is based on so called quantum relays, a sort of amplification stages for quantum information, placed at regular distances between a longer quantum channel (see e.g. [CGdR03]). Furthermore, free-space systems offer the possibility to communicate via satellites. Within this scheme, a geo-stationary orbiting satellite could exchange keys in parallel with Alice and Bob. Security could be further improved if the satellite would carry a source of entangled particles, directing one particle to Bob and one to Alice. They can then apply an entangled based protocol to extract the key. In this case, the satellite wouldn't even need to be trusted. QKD with entangled pairs could also solve the free-space problem of the free line of sight between Alice and Bob: it would be sufficient to ensure that both parties have a direct link with the source (e.g. placing it on a tall building).

As visionary as these scenarios may appear, the european project named SECOQC [sec] (Secure Communication through Quantum Cryptography) is aiming at the realization of a global network architecture based on the new issue of quantum-cryptography. Should future technological developments seriously menace the security of classical cryptography, quantum-based cryptography is indeed the perfect candidate to guarantee an all-time high security dimension. The way for QKD schemes for becoming an everyday technology is still a long one, but all prerequisites show in the right direction.

[1] A first implementation of this idea has been realized in 2004 by the team of Chip Elliott at BBN Technologies in Cambridge, Massachusetts [EPT03]. The QC based network consists of six servers interconnected by ordinary telecommunication fibers. The actual key distribution occurs with polarized photons produced by weak coherent sources.

A The Extended Euclidean Algorithm

The Euclidean algorithm is a P-time procedure to calculate the greatest common divisor between two non-negative integers a and b, denoted $GCD(a, b)$. Suppose w.l.o.g. that $a > b$; then we can write $a = q_1 \cdot b + r_1$, where q_1 and $r_1 < b$ are the quotient and remainder of the integer division of a by b, respectively. Since $r_1 = a - q_1 b$, any common divisor of a and b also divides r_1, and similarly any common divisor of b and r_1 will also divide a. Therefore, denoting with $[x]$ the integral part of a real number x, we can write the following iteration:

$$\begin{array}{rcll}
q_1 = \left[\dfrac{a}{b}\right] & & a = q_1 \cdot b + r_1 & r_1 = a - q_1 \cdot b \\
q_2 = \left[\dfrac{b}{r_1}\right] & & b = q_2 \cdot r_1 + r_2 & r_2 = b - r_1 \cdot q_2 \\
\vdots & & \vdots & \vdots \\
q_n = \left[\dfrac{r_{n-2}}{r_{n-1}}\right] & & r_{n-2} = q_n \cdot r_{n-1} + r_n & r_n = r_{n-2} - r_{n-1} \cdot q_n \\
q_{n+1} = \left[\dfrac{r_{n-1}}{r_n}\right] & & r_{n-1} = q_{n+1} \cdot r_n + 0 & r_n = r_{n-1}/q_{n+1}
\end{array}$$

the algorithm terminates when q_{n+1} divides r_{n-1} exactly and r_n is the $GCD(a, b)$. A simple C/C++ implementation of the algorithm looks like:

```
int gcd(int a, int b) {
  int t;
  while (b != 0) {
    t = b;
    b = a % b;
    a = t;
  }
  return a;
}
```

The extended Euclidean algorithm is essentially the same as the Euclidean algorithm, only that it keeps track of quotients during the computation, in order to find x and y, such that:

$$a \cdot x + b \cdot y = GCD(a, b)\,. \tag{A.1}$$

Eq. A.1 (known as *Bezout's identity*) is very useful if the two integers a and b are **coprime** (i.e. $GCD(a, b) = 1$). In this case x is the **multiplicative inverse** of a modulo b (see Sec. 2.7.2 for an application in the RSA algorithm). The multiplicative inverse modulo a number does not exist for all couples (a, b), but if a and b are coprime, then it can be shown that there exists a unique inverse of $a\ mod\ b$. This is an implementation of the extended Euclidean algorithm in C++ (source code taken from [Sch96]):

```
#define isEven(x)     ((x & 0x01) == 0)
#define isOdd(x)     (x & 0x01)
#define swap(x,y) (x^=y, y^=x, x^=y)

void ExtBinEuclid(int *u, int *v, int *u1, int *u2, int *u3){

  int k, t1, t2,t3;

  if( *u < *v) swap(*u,*v);
  for (k=0; isEven(*u) && isEven(*v): k++) {
          *u >>= 1; *v >>= 1;
  }

  *u1 = 1; *u2 = 0; *u3 = *u ; t1 = *v; t2 = *u-1; t3 = *v;
  do {
      do{
         if (isEven(*u3)) {
             if(isOdd(*u1)) || isOdd(*u2) {
                *u1 += *v; *u2 += *u;
             }
             *u1 >>= 1; *u2 >>= 1; *u3 >>= 1;
                        }
             if (isEven(t3) || *u3 < t3) {
                 swap(*u1,t1); swap(*u2,t2); swap(*u3,t3);
             }
         } while (isEven(*u3));
             while (*u1 < t1 || *u2 < t2) {
                               *u1 += *v; *u2 += *u;
             }
              *u1 -= t1; *u2 -= t2; *u3 -= t3;
  } while (t3 > 0);
  while (*u1 >= *v && *u2 >= *u) {
          *u1 -= *v; *u2 -= *u;
  }

  *u1 <<= k; *u2 <<= k; *u3 <= k;
}

main(int argc, char **argv) {
  int a, b, gcd;
  if (argc < 3 ) {
      cerr << "Usage␣exteuclid␣u␣v" << endl;
      return -1;
  }
  int u = atoi(argv[1]);
  int v = atoi(argv[2]);
  if ( u <= 0 || v <= 0) {
      cerr << "Please␣provide␣two␣positive␣integers" << endl;
                return -2
  }
  ExtBinEuclid(&u, &v, &a, &b, &gcd);
  cout << a << "*" << u << "+(-" << b << ")*" << v
       << "=" << gcd << endl;
  if (gcd == 1)
      cout << "the␣multiplicative␣inverse␣of␣" << v << "mod"
           << u << "␣is:␣" << u-b << endl;
        return 0;
  }
```

B Beam Parameters

In this section we estimate the initial beam parameters as defined by the optical arrangement shown in Fig. B.1. If we assume that a Gaussian beam passes through a pinhole with Diameter D, placed at the point z, then the fraction of transmitted light is given by (see [Sieg]):

$$T = 1 - e^{-D^2/2\omega^2(z)} \tag{B.1}$$

where $\omega(z)$ is the beam waist at the point z given by the formula:

$$\omega(z) = \omega_0 \sqrt{1 + \left(\frac{z}{z_R}\right)^2} \tag{B.2}$$

where we have chosen the origin of the z axes at the point of minimal waist ω_0 and $z_R = \frac{\pi\omega_0^2}{\lambda}$ is the Rayleigh range. The transmission through **two** pinholes separated by a distance d, under the assumption that the beam minimal waist is in the middle of the pinholes, is then given by:

$$T_{tot} = \left(1 - e^{-D^2/2\omega^2(z)}\right)^2 \tag{B.3}$$

The two constraints for a maximum in the transmission for our setup are:

- The beam minimal waist is in the middle betweeen the two pinholes (this leads to Eq. B.3).
- For given D and pinholes distance d, $\omega(z)$ must have its minimum at the point $d/2$.

The latter condition yields the optimum value for the Rayleigh range z_R:

$$\frac{\partial\omega^2}{\partial z_R} = \frac{z_R\lambda}{\pi}\left(1 - \frac{z^2}{z_R^2}\right) = 0\,, \tag{B.4}$$

which is fullfilled for $z_R = z = d/2$.

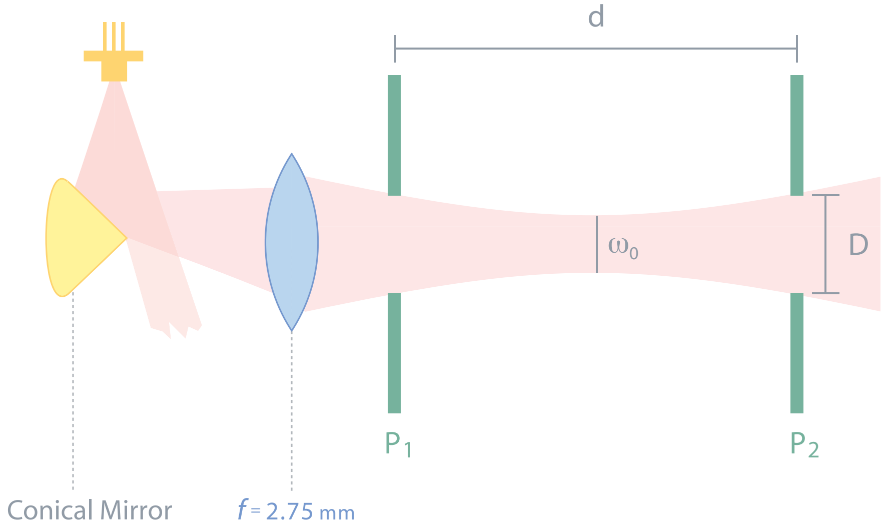


Figure B.1: The setup which defines the initial beam parameters.

Finally, for $\lambda = 850$ nm, $D = 100$ μm, the above relation and the definition of the Raleygh range give a beam minimal waist between the pinholes of $\omega_0 = 50$ μm. With the help of Eq. B.3, the overall transmission evaluates to:

$$T_{tot} = \left(1 - e^{-\frac{D^2 \pi}{2\lambda d}}\right) = \left(1 - e^{-2}\right)^2 \approx 74.8\% \tag{B.5}$$

Bibliography

[BB84] C. H. Bennett and G. Brassard. “Quantum cryptography: Public key distribution and coin tossing”. In *Proceedings of IEEE Conference on Computers, Systems and Signal Processing, Bangalore, India*, 1984.

[BB89] C. H. Bennett and G. Brassard. “The dawn of a new era for quantum cryptography: The experimental prototype is working!” *Sigact News*, 20(4):78–82, 1989.

[BBB$^+$92] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. “Experimental quantum cryptography”. *Journal of Cryptology*, 5(3):3–28, 1992.

[BBCM95] C. H. Bennet, G. Brassard, C. Crépeau, and M. U. Maurer. “Generalized privacy amplification”. *IEEE Transactions on Information Theory*, 41(6):1915–1923, November 1995.

[BBM92] C. H. Bennett, G. Brassard, and N. D. Mermin. “Quantum cryptography without Bell’s theorem”. *Phys. Rev. Lett.*, 68(557), 1992.

[Bel64] J. S. Bell. “On the Einstein-Poldolsky-Rosen paradox”. *Physics 1*, 195, 1964.

[BEM97] E. Bruß, A. K. Ekert, and C. Macchiavello. “Optimal universal quantum cloning and state estimation”. *Los Alamos e-print archive:* `http://arxiv.org/abs/quant-ph/9712019`, 1997.

[Ben92] C. H. Bennett. “Quantum criptography using any two orthogonal states”. *Phys. Rev. Lett.*, 68, 1992.

[BLMS00] G. Brassard, N. Lütkenhaus, T. Mor, and C. Sanders. “Limitations on practical quantum cryptography”. *Phys. Rev. Lett.*, 85, 2000.

[Boh51] D. Bohm. “The paradox of Einstein, Rosen, and Podolsky”. *Quantum Th*, pages 611–623, 1951.

[BS93] G. Brassard and L. Salvail. “Secret-key reconciliation by public discussion”. In *Advances in Cryptology - Proceedings of Eurocrypt ’93*, 1993.

[CGdR03] D. Collins, N. Gisin, and H. de Riedmatten. “Quantum relays for long distance quantum cryptography”. *Los Alamos e-print archive:* `http://arxiv.org/abs/quant-ph/0311101`, 2003.

[CHSH69] J. F. Clauser, M.A Horne, A. Shimony, and R. A. Holt. “Proposed experiment to test local hidden-variable theories”. *Phys. Rev. Lett.*, 23:880–884, 1969.

[DH76] W. Diffie and M. Hellmann. “New directions in cryptography”. In *IEEE Transactions on Information Theory*, pages 644–654, 1976.

[DHH99] M. Dušek, M. O. Haderka, and M. Hendrych. “Generalized beam-splitting attack in quantum cryptography with dim coherent states”. *Opt. Commun*, 169(103), 1999.

[Die82] D. Dieks. “Communication by EPR devices”. *Phys. Rev. Lett. A*, 92, 1982.

[Eke91] A. K. Ekert. “Quantum cryptography based on Bell’s theorem”. *Phys. Rev. Lett.*, 67(661), 1991.

[EPR35] A. Einstein, B. Podolsky, and B. Rosen. “Can quantum-mechanical description of physical reality be considered complete?” *Phys. Rev.*, 47:777–780, 1935.

[EPT03] Chip Elliott, D. Pearson, and G. Troxel. “Quantum cryptography in practice”. *Los Alamos e-print archive:* `http://arxiv.org/abs/quant-ph/0307049`, 2003.

[GLLP02] D. Gottesmann, H.-K. Lo, N. Lütkenhaus, and J. Preskill. “Security of quantum key distribution with imperfect devices”. *Los Alamos e-print archive:* `http://arxiv.org/abs/quant-ph/0212066`, 2002.

[GM97] N. Gisin and S. Massar. “Optimal quantum cloning machines”. *Phys. Rev. Lett.*, 11(79), 1997.

[GRTZ02] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. “Quantum cryptography”. *Reviews of Modern Physics*, 74:145–195, 2002.

[GYS04] C. Gobby, Z. L. Yuan, and A. J. Shields. “Quantum key distribution over 122 km of standard telecom fiber”. *Appl. Phys. Lett.*, 84(19), 2004.

[Hep] C. J. Hepburn. `http://britneyspears.ac/lasers.htm`. Britney Spears guide to semiconductor physics.

[Hwa03] W.-Y. Hwang. “Quantum key distribution with high loss: Toward global secure communication”. *Phys. Rev. Lett.*, 91, 2003.

[Ker83] A. Kerckhoffs. *La criptographie militaire*, volume 5 of *Journal des Sciences Militaires.* 1883.

[Kur] C. Kurtsiefer. Private communications. 2006

[LMC05] H.-K. Lo, X. Ma, and K. Chen. “Decoy state quantum key distribution”. *Phys. Rev. Lett.*, 94, 2005.

[Lüt00] N. Lütkenhaus. “Security against individual attacks for realistic quantum key distribution”. *Phys. Rev. Lett. A*, 61, 2000.

[Ma04] X. Ma. “Security of quantum key distribution with realistic devices”. *Los Alamos e-print archive:* `http://arxiv.org/abs/quant-ph/0503057`, 2004.

[May96] D. Mayer. *Advances in Cryptology-Proc. Crypto ’96*, volume 1109 of *Lecture Notes in Computer Science*, pages 343,357. Springer-Verlag New York, 1996.

[MdRT$^+$04] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, Legré M., and N. Gisin. “Distribution of time-bin qubits over 50 km of optical fiber”. *Los Alamos e-print archive:* `http://arxiv.org/abs/quant-ph/0404124`, 2004.

[mel] Thermoelectric handbook. Technical report, Melcor Corp.

[Mer78] R. Merkle. “Secure communications over insecure channels”. *Communications of the Association for Computing Machinery (CACM)*, pages 294–299, 1978. Submitted in 1975.

[NC02] M. A. Nielsen, I. L. Chuang. *Quantum computation and quantum information* Cambridge University Press, 2002

[OST05] D.A. Osvik, A. Shamir, and E. Tromer. “Cache attacks and countermeasures: the case of AES”. *Cryptology ePrint Archive:* `http://eprint.iacr.org/2005/271`, 271, 2005.

[Reg05] N. Regner. “Experimentelle Freiraum-Quantenkryptographie”. Master’s thesis, Technische Universität München, 2005.

[Riv90] R. Rivest. *Handbook of Theoretical Computer Science.* Elsevier Science Publishers B.V., 1990.

[Roith] Roithner Laser Technik. Laser diodes data sheets. `http://www.roithner-laser.com/All_Datasheets /Laserdiodes/RLT8505MG.pdf`

[RT] J. G. Rarity and P. Tapster. “Cryptographic receiver”. European patent EP 0 722 640 B1.

[Sch96] B. Schneier. *Applied Cryptography. Protocols, Algorithms and Source Code in C.* John Wiley & Sons, Inc., 1996.

[sec] Homepage of the SECOQC project: `http://www.secoqc.net`.

[Sha48] C. E. Shannon. “A mathematical theory of communication”. *Bell System Technical Journal*, 27:379–423 and 623–656, July and October 1948.

[SIAG05] V. Scarani, S. Iblisdir, A. Acín, and N. Gisin. “Quantum cloning”. *Reviews of Modern Physics*, 77, October 2005.

[Sieg] A. E. Siegman *Lasers.* University Science Books, 1986. Chapter 6

[son05] Laser diode application guide. Technical report, Sony Corporation. Available at: `http://www.sony.net/Products/SC-HP/laserdiodewld/application`, 2005.

[SP00] P. W. Shor and J. Preskill. “Simple proof of security of the BB84 quantum key distribution protocol”. *Phys. Rev. Lett.*, 85(441), 2000.

[TKI03] K. Tamaki, M. Koashi, and N. Imoto. “Security of the B92 quantum key distribution protocol against individual attacks over a realistic channel”. *Phys. Rev. Lett. A*, 67(32310), 2003.

[Wan04a] X.-B. Wang. “Beating the PNS attack in practical quantum qryptography”. *Los Alamos e-print archive:* `http://arxiv.org/abs/quant-ph/0410075`, 2004.

[Wan04b] X.-B. Wang. “A decoy-state protocol for quantum cryptography with 4 intensities of coherent light”. *Los Alamos e-print archive:* `http://arxiv.org/abs/quant-ph/0411047`, 2004.

[Wei03] H. Weier. “Experimental quantum cryptography”. Master’s thesis, Technische Universität München, 2003.

[wik] Wikipedia the free encyclopedia. `http://www.wikipedia.org`.

[WZ82] W.K. Wooters and W. H. Zurek. “A single quantum cannot be cloned”. *Nature*, 289, 1982.

Index

Acknowledgements

At this point I would like to address my acknowledgements to all the people who assisted me with the realization of this work. In particular, I wish to thank Prof. Dr. Harald Weinfurter for giving me the chance to participate in this outstanding research project, for the uncomplicated affiliation in his staff and the helpful guidance. The next person my gratitude is addressed to is Prof. Dr. Eberhard Riedle, for the interest shown for the topic of this work and the time he dedicated to me.

A special thank goes to Tobias Schmitt-Manderbach, Henning Weier and Martin Fürst for their valuable advice and assistance in all scientific and technical questions. I'm looking forward to hear from your new free-space record as soon as possible. Sincere thanks are given to Dr. Jürgen Volz, Dr. Markus Weber, Daniel Schlenk and Chunlang Wang for their support, the stimulating discussions and the corrections to this work. I want to thank Florian Henkel for the funny atmosphere in the lab and in the office; Toni Scheich for the technical support in electronics-matter, Ms. Nicole Schmidt and Ms. Gabi Gschwendtner for their assistance in all administrative questions. Thank to Wenjamin Rosenfeld, Stefan Berner, Asli Ugur and Nadja Regner.

Furthermore, I'd like to express my gratitude to
- my family and in particular to my mother, who always stand behind me with her unlimited love and sympathy and, after all, who made this education possible
- my better half for her unconditional support, the endless patience and the affectionate presence by my side and
- schoendruck.de for the kind assistance and expertise in printing this work.

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, 16.06.2006

Ivan Ordavo