Department of Optics
Faculty of Natural Sciences
Palacký University
Olomouc, Czech Republic

Experimental Quantum Cryptography

Martin Hendrych

Doctoral Thesis
Olomouc, September 2002

Supervisor: **Prof. RNDr. Jan Peřina, DrSc.**

Acknowledgements

In the first place, I owe a great debt of gratitude to Prof. Jan Peřina, who brought me to physics and whose memorable lectures showed me into the realm of quantum optics. It has certainly been an exceptional privilege to meet and work with such a personality. I wish to acknowledge his advice, support and comments during my PhD study as well as his careful reading of the manuscript of the Thesis. I am also deeply indebted to my co-workers Miloslav Dušek, Ondřej Haderka and Robert Myška without who the quantum key distribution and quantum identification experiments could have never succeeded.

I am grateful to Prof. Malvin C. Teich for giving me the opportunity to work at the Quantum Imaging Laboratory of Boston University, co-directed by Profs. Bahaa E. A. Saleh and Alexander V. Sergienko. I would also like to express my warmest thanks to Giovanni Di Giuseppe for many fruitful and stimulating discussions. I would like to thank other members of the Quantum Imaging Laboratory as well, Ying-Tsang Liu for his help with Matlab simulations, Ayman Abouraddy for his help with the ICCD camera, Magued Nasr for his assertiveness with which he pushed some purchase orders through the bureaucratic machine of Boston University, and Jian Peng of BU Chemistry Department who lent me some components from his setup.

I would like to express appreciation to Tomáš Rosa for his consultations on classical cryptography.

I am obliged to the Czech Grant Agency, Ministry of Education of the Czech Republic, Ministry of Interior of the Czech Republic, and Research Center for Optics, whose projects I participated in. I acknowledge the NATO Science Committee that granted the Advanced Science Fellowship, which funded my 12-month stay at Boston University.

I owe a great deal of thanks to my beautiful muse Marta Saperas for all the patience while I was burning the midnight oil in the lab and in my office, and for all the encouragement while I was at home. I am greatly indebted to my mother for all her love.

Martin Hendrych
Olomouc, September 2002

Contents

1 Introduction 7

2 History 10

3 Contemporary Cryptography 12

3.1 Public-Key Cryptography 12
3.2 Secret-Key Cryptography 13

4 Quantum Approach 16

5 Quantum Key distribution 18

5.1 Vernam Cipher 18
5.2 BB84 Protocol 19
5.3 Experiment 22
5.3.1 Principle 22
5.3.2 Time-Multiplexing Interferometer 23
5.3.3 Preparation of Quantum States and Intensity Measurement 25
5.3.4 Polarization Control 27
5.3.5 Phase Encoding 28
5.3.6 Balancing the Interferometer 30
5.3.7 Detection 33
5.3.8 Visibility 35
5.3.9 Phase Drift 38
5.3.10 Quantum Alphabet 39
5.4 Test for Eavesdropping 42
5.5 Error Correction and Privacy Amplification 44
5.6 Authentication of the Public Channel 46
5.7 Eavesdropping 49
5.7.1 Intercept/Resend 49
5.7.2 Beam Splitting 49
5.7.3 Other Types of Attacks 52
5.8 QKD Session 53
5.9 Other Experimental Prototypes and Proposals 53

6 Quantum Identification System 60

6.1 Introduction 60
6.2 Identification with an Unjammable Public Channel 61
6.3 Identification with Authenticated Public Discussion 62
6.4 Necessary Condition for Secure Communication 63
6.5 Optimization 64

7 Quantum Secret Sharing 68
7.1 Introduction 68
7.2 Quantum Entanglement 69
7.3 Generation of Entangled Photons 70
7.4 Principle 71
7.5 Eavesdropping 75
7.6 Experimental Setup 78
7.7 Experimental Results 83
7.7.1 Temporal and Spatial Walk-off 83
7.7.2 Walk-off Compensation with a Quartz Crystal 84
7.7.3 CHSH Inequality 85
7.7.4 Walk-off Compensation with Two BBO Crystals 86
7.7.5 Walk-off Compensation with One BBO Crystal 87
7.7.6 Quantum Alphabet 90
8 Conclusions 92
References 95

Høffding asked: "Where can the photon be said to be?"
Bohr replied: "To be. To be. What does it mean to be?"

Chapter 1
Introduction

There is no doubt that electronic communications have become one of the main pillars of the modern society and their ongoing boom requires the development of new methods and techniques to secure data transmission and data storage. This has been the goal of cryptography. Etymologically derived from Greek *kryptós*, hidden or secret, and *graphein*, to write, cryptography may generally be defined as the art of writing (encryption) and deciphering (decryption) messages in code in order to ensure their confidentiality, authenticity, integrity and non-repudiation. Cryptography and cryptanalysis, the art of codebreaking, together constitute cryptology (*lógos*, a word).

Nowadays many paper-based communications have already been replaced by electronic means, raising the challenge to find electronic counterparts to stamps, seals and hand-written signatures. The growing variety of applications springs many tasks that must be solved. Let us name a few. The fundamental task of cryptography is to allow two users to render their communications unintelligible to any third party, while for the two legitimate users the messages remain intelligible. The goal of identification is to verify the identities of the communicating parties. Another cryptographic task is secret sharing: A secret, e.g., a password, is split into several pieces in such a way that when a certain minimal subset of the pieces is put together, the secret is recovered. Other cryptographic applications are, for example, digital signatures, authentication of messages, zero-knowledge proofs, and so on.

Nonetheless, the current cryptographic implementations only provide a conditional security that relies on limited computational and technological capabilities of the opponent. In contrast, this Thesis presents three laboratory prototypes, whose security is unconditional and is guaranteed by the fundamental laws of physics. The first experiment is an interferometric implementation of quantum key distribution (QKD), which enables two communicating parties to establish a secret cryptographic key at a distance. Information is encoded in single quantum objects, photons, which are approximated by weak coherent states. The Heisenberg uncertainty principle allows us to reveal eavesdropping which results in errors in transmissions. If eavesdropping does not exceed a certain level, all the eavesdropper's information is safely obliterated using an auxiliary procedure of privacy amplification. The generated key is then used to encrypt messages by means of the Vernam cipher.

The subsequent experiment expanded the QKD apparatus into a quantum identification system, which combines a classical three-pass identification procedure with QKD. Each identification sequence is used only once in a way similar to the Vernam cipher, and new identification sequences are refueled by means of QKD.

The third experiment implements quantum secret sharing that expediently exploits the quantum non-local correlations of entangled photon pairs, produced by nonlinear spontaneous parametric down conversion.

The first two experiments were performed at the Department of Optics of Palacký University and the Joint Laboratory of Optics of Palacký University and Institute of Physics of the Academy of Sciences of the Czech Republic in Olomouc, Czech Republic. Both quantum key distribution and quantum identification have come to fruition as a product of group work headed by Prof. Jan Peřina. Other members of the group were Miloslav Dušek, Ondřej Haderka, and Robert Myška. My main responsibility was the experimental implementation itself, including the choice and purchase of the optical components and electronics, measuring their characteristics, building the apparatus, devising solutions, and performing measurements on the whole system. I also participated in the theoretical work, conducting calculations and writing papers. Our publications [1-11] were then exploited in some Sections of the Thesis.

The experimental implementation of quantum secret sharing was my individual research project that won the NATO Advanced Science Fellowship and was conducted during my 12-month stay at the Quantum Imaging Laboratory of Boston University, directed by Profs. Malvin C. Teich, Bahaa E. A. Saleh, and Alexander V. Sergienko.

The methods and tools used to generate, manipulate and detect the quantum states for individual experiments are those of quantum optics, nonlinear optics and quantum information theory and are described in detail in their respective chapters. The Thesis is organized as follows. Chapter 2 reviews the history of cryptography up to World War II. Chapter 3 discusses the modern cryptographic techniques. Chapter 4 shows how quantum mechanics can help us reveal eavesdropping when information is encoded in individual quantum systems. The rest of the Thesis is divided into three parts, each devoted to one of the above-mentioned experiments. The first two Sections of Chapter 5 describe the Vernam cipher and the used QKD protocol. Section 5.3 depicts the experimental setup and individual hurdles that had to be overcome while building the QKD apparatus. Section 5.4 explains how the presence of an eavesdropper was tested. Sections 5.5 and 5.6 concern the auxiliary procedures of error correction, privacy amplification and authentication. Section 5.7 covers various methods of eavesdropping. Section 5.8 summarizes a typical QKD session and Section 5.9 surveys other experimental proposals and prototypes. Chapter 6 deals with the quantum identification system. After a short introduction, Section 6.2 presents an identification protocol in case the users have an unjammable public channel at their disposal. Section 6.3 illustrates how the identification procedure itself can be incorporated into the authenticated public discussion. In Section 6.4, the necessary condition for secure QKD and quantum identification has been derived. Section 6.5 describes the optimization of the system to maximize the yield of the secret cryptographic key and concludes with a short summary of a typical identification procedure. Chapter 7 covers the quantum secret sharing experiment. Sections 7.2 and 7.3 are devoted to quantum entanglement and its generation. Section 7.4 depicts the protocol. Section 7.5 deals with

eavesdropping and Sections 7.6 and 7.7 describe the experimental setup and present the experimental results. The Thesis concludes by summarizing all three experiments in Chapter 8.

Chapter 2
History

At all times people have wished to have the possibility to communicate in secrecy so as to allow nobody to overhear their messages. Archeological excavations have revealed that various types of cryptography had already been used by ancient civilizations in Mesopotamia, India, or China [12]. Four thousand years ago, ancient Egyptians used modified hieroglyphs to conceal their messages. In the Iliad, Homer depicts how Proetus, the king of Argolis, sends Bellerophon to Lycia with "a lethal message, coded symbols inscribed on a folded tablet" [13]. The coded symbols were represented by a rude type of hieroglyphics, the meaning of which was only known to Proetus and his father-in-law Iobates, the recipient of the message [14].

In the 5th century BC, the Spartans in Greece designed a Skytale cryptodevice, based on transposition of letters [15]. A stripe of parchment or leather was wound around a wooden baton, across which the message was written. When the end of line was reached, the baton was rotated. After the parchment was unwrapped, the letters looked scrambled and only the person who possessed a baton of an identical shape could recover the message.

Another favorite and easy cipher is the substitution cipher, which substitutes each letter of a message with another letter, number or a symbol. An example is the Caesar cipher [16]. To communicate between the Roman legions scattered over the Roman republic, Gaius Julius Caesar used a cipher, where each letter of a message was advanced by three letters in the alphabet; A was replaced by D, B was replaced by E, C by F, and so on. Thus *Veni, Vidi, Vici* became *Yhql, Ylgl, Ylfl*.

During the Middle Ages, most cryptosystems were based on transposition or substitution or a combination thereof [17]. The substitution cipher was also used by some writers, such as Edgar Allan Poe in his story *The Gold Bug* [18], or Arthur Conan Doyle in his Sherlock Holmes story *The Adventure of the Dancing Men* [19]. However, neither of these ciphers is secure, because it is possible to break them exploiting various characteristic properties of the language, such as the frequency of individual letters and their clusters.

The invention of the telegraph in the 1830s enormously facilitated communications between people. This ancestor of modern communications, however, had a serious drawback from the cryptographic point of view – the content of the transmitted message was known to the telegraph operator. As a consequence, various codebooks were designed by people and companies that wanted to keep their communications private. The codebooks translated significant words and phrases into short, nonsense words. The codes served two purposes: first, they reduced the size of

the message and thus decreased the costs because telegrams were charged per transmitted character; and second, if the codebook was kept secret, the codes became a cipher.

The two world wars of the 20th century accelerated the development of new cryptographic techniques. Cryptographers tried to design a system where the encryption and decryption algorithms could be publicly known, but the secrecy of the message would be guaranteed by some secret information, the cryptographic key, shared between the users. In 1917, Gilbert S. Vernam proposed an unbreakable cryptosystem, hence called the Vernam cipher or One-time Pad [20]. The One-time Pad is a special case of the substitution cipher, where each letter is advanced by a random number of positions in the alphabet. These random numbers then form the cryptographic key that must be shared between the sender and the recipient. Even though the Vernam cipher offers unconditional security against adversaries possessing unlimited computational power and technological abilities, it faces the problem of how to securely distribute the key. That is why it did not become widespread as Vernam had hoped. On the other hand, there are many military and diplomatic applications, where the security of communications outweighs the severe key management problems. The Vernam cipher was used by the infamous spies Theodore A. Hall, Klaus Fuchs, the Rosenbergs and others, who were passing atomic secrets to Moscow. Ché Guevara also encrypted his messages to Fidel Castro by means of the One-time Pad. It was employed in securing the hot line between Washington and Moscow and it is said to be used for communications between nuclear submarines and for some embassy communications. We will come back to the Vernam cipher later on, as it is this cipher that is very expedient for quantum key distribution.

In 1918, Arthur Scherbius invented an ingenious electric cipher machine, called Enigma, which was patented a year later [21]. The Enigma consisted of a set of rotating wired wheels, which performed a very sophisticated substitution cipher. After various improvements, it was adopted by the German Navy in 1926, the German Army in 1928, and the Air Force in 1935, and it was used by the Germans and Italians throughout World War II. The military Enigma had incredible 159×10^{18} possible settings (cryptographic keys). When some letter was repetitively keyed, the machine always produced a different letter and the sequence started repeating only after 16 900 keyings, when the inner mechanism returned to the initial position [22]. The immense number of potential keys led Alan Turing to construct the first electronic computer, which helped break the Enigma ciphers in the course of the War. Thus cryptography (or cryptanalysis to be more precise) was the driving force behind the development of modern computers. Today a Pentium-based computer can unscramble an Enigma-encrypted message within minutes.

Chapter 3
Contemporary Cryptography

3.1 Public-Key Cryptography

A new surge of interest in cryptography was triggered by the upswing in electronic communications in the late 70s of the 20th century. It was essential to enable secure communication between users who have never met before and share no secret cryptographic key. But the question was how to distribute the key in a secure way. The solution was found by Whitfield Diffie and Martin E. Hellman, who invented public-key cryptography in 1976 [23]. The ease of use of public-key cryptography, in turn, stimulated the boom of electronic commerce during the 1990s.

Public-key cryptography requires two keys – the public key and the private key, which form a key pair. The recipient of a message generates two keys, makes the public key public through a Trusted Authority and keeps his private key in a secret place to ensure its private possession. The algorithm is designed in such a way that anyone can encrypt a message using the public key, however, only the legitimate recipient can decrypt the message using his/her private key.

The security of public-key cryptography rests on various computational problems, which are believed to be intractable. The encryption and decryption algorithms utilize the so-called one-way functions. One-way functions are mathematical functions that are easy to compute in one direction, but their inversion is very difficult. It is, e.g., very easy to multiply two prime numbers, but to factor the product of two large primes is already a difficult task. Other public-key cryptosystems are based, e.g., on the difficulty of the discrete logarithm problem in Abelian groups on elliptic curves or other finite groups. However, it is important to point out that no "one-way function" has been proved to be one-way; they are merely believed to be. Public-key cryptography cannot provide unconditional security. We speak about computational security.

Today the most widely used public-key system is the RSA cryptosystem. RSA was invented in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman [24], whose names form the acronym. RSA exploits the difficulty of factoring large numbers. Very grossly said, the receiver picks two large primes and makes their product public. This product, called the modulus, becomes the public key. Using this key, anyone can encrypt a message. However, in order to invert the algorithm it is necessary to know the prime factors of the modulus. Although there are several ways to attack the RSA system, the most promising one still seems to be to attempt to factor the modulus.

In 1996 Richard Guy wrote [25]: "I shall be surprised if anyone regularly factors numbers of size 10^{80} without special form during the present century". The first challenge to break a 425-bit RSA key (equivalent to 129 decimal digits) was published in Scientific American in 1977 [26]. Ronald Rivest calculated that to factor a 125-digit number, the product of two 63-digit primes, would take at least 40×10^{15} years (about one million times the age of the universe) with the best factoring algorithms then known. However, 17 years later, in 1994, new factoring algorithms had been discovered and computer power had advanced to such a level that it took 1600 computers (and two fax machines!) interconnected over the Internet only 8 months. Today a single Pentium-based PC could do the same job.

While breaking 425-bit RSA required a large number of computers, in February 1999 it was only 185 machines that managed to factor a 465-bit RSA modulus in 9 weeks. At that time, 95 % of e-commerce on the Internet was protected by 512-bit keys (155-digit number). A 512-bit number was factored in August 1999 by 292 machines. That means that neither 512-bit keys provide sufficient security for anything more than very short-term security needs. All these challenges have served to estimate the amount of work and the cost of breaking a key of a certain size by public efforts. It is obviously much more difficult to estimate what can be achieved by private and governmental efforts with much larger budgets.

A network of computers is not the only way to factor large integers. In 1999 Adi Shamir proposed the TWINKLE device [27] – a massively parallel optoelectronic factoring device, which is about three orders of magnitude faster than a conventional fast PC and can facilitate the factoring of 512- and 768-bit keys. Today it is already recommended to move to longer key lengths and to use key sizes of 1024 bits for corporate use and 2048 bits for valuable keys.

Another menace to the security of public-key cryptography could originate from the construction of a quantum computer. The decryption using a quantum computer would take about the same time as the encryption, thereby making public-key cryptography worthless. Algorithms capable of doing so have already been developed [28] and first experiments with small-scale quantum computers successfully pave the way to more sophisticated devices [29].

3.2 Secret-Key Cryptography

Secret-key cryptography can provide its users with unconditional security on condition that the users share a sufficiently long secret key beforehand. The common key is then used for both encryption and decryption. Secure key distribution is the main drawback of secret-key cryptosystems. The security of communications is reduced to the security of secret-key distribution. In order to avoid the necessity of personal meetings or courier services to exchange the secret key, some users use public-key

cryptography to distribute the key, which is then used in a secret-key cryptosystem. The unconditional security of the system is thus degraded to computational security. These so-called hybrid systems have gained a widespread use, because they combine the speed of secret-key systems with the efficiency of key management of public-key systems. They have been used for electronic purchases, financial transactions, ATM transactions and PIN encryptions, identification and authentication of cellular phone conversations, electronic signatures, and many other applications, whose number is swelling.

The most spread secret-key cryptosystem is the Digital Encryption Standard (DES) and its variations. Due to its frequent use in the hybrid systems, it is the most often used cryptosystem ever. DES was developed by IBM and the U.S. government in 1975 and it was adopted as a standard two years later. It employs very simple arithmetic operations and therefore it can easily be implemented in hardware, where it can reach very high speeds of encryption.

DES has experienced a similar wave of attacks as public-key cryptosystems. The algorithm uses a 56-bit key, which is reused to encrypt the entire message. As a consequence, it is only computationally secure. In 1997, RSA Data Security, Inc. published their first challenge to decrypt a plaintext message scrambled by DES. It took 96 days to break it. The researchers applied "brute force" by searching the entire keyspace of 2^{56} possible keys on a large number of computers [30]. In January 1998, a new prize was offered. The winner of the contest used the idle time of computers connected to the Internet. More than 50,000 CPUs were linked together. The key was found after 41 days [31]. Another group of codebreakers chose a different approach. They built a single machine, which revealed the encrypted message "It's time for those 128-, 192-, and 256-bit keys" after only 56 hours, searching at a rate of 88 billion keys per second [32]. In the last challenge in January 1999, the two previous winners combined their efforts to find the key in only 22 hours and 15 minutes, testing 245 billion keys per second. In 1993, Michael Wiener designed a DES key search machine which, based on 1997's technology, would break DES in 3.5 hours [30]. The same machine based on 2000's technology would take only 100 seconds [33]. The exhaustive search is not the only possible attack on DES. During the 1990s, other successful attacks were proposed that exploit the internal structure of the cipher [34].

Cryptographers attempted to improve the security of DES. Triple DES, DESX and other modifications were developed. In October 2000, a four-year effort to replace the aging DES culminated in the announcement of a new standard, the Advanced Encryption Standard (AES) [35]. This standard was approved in December 2001 and went into effect in May 2002. How long will it last?

In summary, the security of conventional techniques relies on the assumption of limited advancement of mathematical algorithms and computational power in the foreseeable future, and also on limited financial resources available to a potential adversary. Computationally secure cryptosystems, no matter whether public- or secret-key, will always be threatened by breakthroughs, which are difficult to predict, and even steady progress of code-breaking allows the adversary to "reach back in time" and

break older, earlier captured, communications encrypted with weaker keys. This results in the necessity to periodically re-encrypt or re-sign certain documents, which are to be of a longer lifetime, such as contracts, etc., and to carefully sort information according to the used cryptosystem.

Another common problem of conventional cryptographic methods is the so-called side-channel cryptanalysis [36]. Side channels are undesirable ways through which information related to the activity of the cryptographic device can leak out. The attacks based on side-channel information do not assault the mathematical structure of cryptosystems, but their particular implementations. It is possible to gain information by measuring the amount of time needed to perform some operation, by measuring power consumption, heat radiation or electromagnetic emanation.

Chapter 4
Quantum Approach

As mentioned above, the main problem of secret-key cryptosystems is secure distribution of keys. It is here that quantum mechanics comes in handy and readily offers a solution. While the security of classical cryptographic methods can be undermined by advances in technology and mathematical algorithms, the quantum approach can provide unconditional security. The security is guaranteed by the Heisenberg uncertainty principle, which does not allow us to discriminate nonorthogonal states with certainty. Within the framework of classical physics, it is impossible to reveal possible eavesdropping, because information encoded into any property of a classical object can be acquired without affecting the state of the object. All classical signals can be monitored passively. In classical communications, one bit of information is encoded in billions of photons, electrons, atoms or other carriers. It is always possible to passively listen in by deviating part of the signal and performing a measurement on it.

Quantum cryptosystems eliminate this side channel by encoding each bit of information into an individual quantum object, such as a single photon. Single photons cannot be split, copied or amplified without introducing detectable disturbances. The linearity of quantum mechanics prohibits from cloning arbitrary unknown quantum states [37]. A device, which is to make a copy of a photon with, say, horizontal polarization $|H\rangle$, needs to perform the following operation

$$|\text{copier}_0\rangle|H\rangle \Rightarrow |\text{copier}_\text{H}\rangle|H\rangle|H\rangle, \tag{1}$$

and similarly for vertical polarization $|V\rangle$

$$|\text{copier}_0\rangle|V\rangle \Rightarrow |\text{copier}_\text{V}\rangle|V\rangle|V\rangle, \tag{2}$$

where $|\text{copier}_0\rangle$ is the initial state of the copier, and $|\text{copier}_\text{H}\rangle$ and $|\text{copier}_\text{V}\rangle$ are its final states. However, if we want to copy a linear superposition of states $|H\rangle$ and $|V\rangle$, we obtain

$$\begin{aligned} |\text{copier}_0\rangle\left(\alpha|H\rangle+\beta|V\rangle\right) &= \alpha|\text{copier}_0\rangle|H\rangle+\beta|\text{copier}_0\rangle|V\rangle \\ &\Rightarrow \alpha|\text{copier}_\text{H}\rangle|H\rangle|H\rangle+\beta|\text{copier}_\text{V}\rangle|V\rangle|V\rangle, \end{aligned} \tag{3}$$

which is different from the required state

$$\left(\alpha|H\rangle+\beta|V\rangle\right)\left(\alpha|H\rangle+\beta|V\rangle\right)=\alpha^2|H\rangle|H\rangle+\alpha\beta|H\rangle|V\rangle+\beta\alpha|V\rangle|H\rangle+\beta^2|V\rangle|V\rangle, \tag{4}$$

regardless of whether states $|\text{copier}_\text{H}\rangle$ and $|\text{copier}_\text{V}\rangle$ of Eq. (3) are identical or not. It follows from Eqs. (1) and (2) that the requirement of unitarity

$$\langle H|V\rangle\langle \text{copier}_0|\text{copier}_0\rangle = \langle H|V\rangle\langle H|V\rangle\langle \text{copier}_\text{H}|\text{copier}_\text{V}\rangle \tag{5}$$

can be satisfied only when the states to be copied are identical or orthogonal, i.e., $\langle H|V\rangle = 1$ or $\langle H|V\rangle = 0$, resp.

If the information is encoded into nonorthogonal states $|0\rangle$ and $|1\rangle$, $\langle 0|1\rangle \neq 0$, an eavesdropper, usually called Eve, cannot make a faithful copy. If she decides not to copy the information carriers, but would rather attempt to find out their state directly by quantum measurements, she faces trouble again. In order to leave the original states intact, she needs to perform unitary operations

$$\begin{aligned} |0\rangle|E\rangle &\Rightarrow |0\rangle|E_0\rangle \quad \text{and} \\ |1\rangle|E\rangle &\Rightarrow |1\rangle|E_1\rangle, \end{aligned} \tag{6}$$

where $|E\rangle$ is the initial state of her measuring apparatus, and $|E_0\rangle$ and $|E_1\rangle$ are its final states. However, the conservation of the inner product

$$\langle 0|1\rangle\langle E|E\rangle = \langle 0|1\rangle\langle E_0|E_1\rangle \tag{7}$$

holds if and only if $\langle E_0|E_1\rangle = 1$, i.e., when the final states of Eve's apparatus are identical, no matter whether she measured state $|0\rangle$ or $|1\rangle$. Eve thus gained no information. It is apparent from Eq. (7) that for Eve to discriminate between two nonorthogonal states, i.e. $\langle E_0|E_1\rangle \neq 1$, she must disturb the state of the measured objects, and thereby inevitably cause errors in transmissions. With a suitably designed protocol, these errors can later be discovered by the legitimate users of the channel, as will be seen in Section 5.2.

It should be noted that quantum mechanics does not prevent from eavesdropping; it only enables us to detect the presence of an eavesdropper. Since only the cryptographic key is transmitted, no information leak can take place when someone attempts to listen in. When discrepancies are found, the key is simply discarded and the users repeat the procedure to generate a new key.

Chapter 5
Quantum Key Distribution

5.1 Vernam Cipher

Classical cryptography can provide an unbreakable cipher, which resists adversaries with unlimited computational and technological power – the Vernam cipher. The Vernam cipher was invented in 1917 by an AT&T engineer Gilbert S. Vernam [20], who thought it would become widely used for automatic encryption and decryption of telegraph messages.

The Vernam cipher belongs to the symmetric secret-key ciphers, i.e., the same key is used for both, encryption and decryption. The principle of the cipher is that if a random key is added to a message, the bits of the resulting string are also random and carry no information about the message. If we use the binary logic, unlike Vernam who worked with a 26-letter alphabet, the encryption algorithm E can be written as

$$E_K(M) = (M_1 + K_1, M_2 + K_2, \ldots, M_n + K_n) \mod 2, \tag{8}$$

where $M = (M_1, M_2, \ldots, M_n)$ is the message to be encrypted, and $K = (K_1, K_2, \ldots, K_n)$ is the key consisting of random bits. The message and the key are added bitwise modulo 2, or exclusive OR without carries. The decryption D of ciphertext $C = E_K(M)$ is identical to encryption, because double modulo-2 addition is identity, therefore

$$M = D_K(C) = (C_1 + K_1, C_2 + K_2, \ldots, C_n + K_n) \mod 2. \tag{9}$$

For this system to be unconditionally secure, three requirements are imposed on the key: (1) The key must be as long as the message; (2) it must be purely random; (3) it may be used once and only once. This was shown by Claude E. Shannon [38], who laid the foundations of communication theory from the cryptographic point of view and compared various cryptosystems with respect to their secrecy. Until 1949 when his paper was published, the Vernam cipher was considered unbreakable, but it was not mathematically proved. If any of these requirements is not fulfilled, the security of the system is jeopardized. A good example is the revelation of the WWII atomic spies because of repetitive use of the key incorrectly prepared by the KGB [39].

The main drawback of the Vernam cipher is the necessity to distribute a secret key as long as the message, which prevented it from wider use. The cipher has so far found applications mostly in the military and diplomatic services. As will be shown in the next Section, the difficulty of secure key distribution can be removed by virtue of quantum key distribution. The Vernam cipher then turns invaluable because of its capability to provide unconditional security and ease of use.

5.2 BB84 Protocol

Quantum key distribution (QKD) was born in 1984 when Charles H. Bennett and Gilles Brassard came up with an idea of how to securely distribute a random cryptographic key with the help of quantum mechanics [40]. Hence, the protocol is called BB84. Drawing upon Stephen Wiesner's ideas about unforgeable quantum money [41], Bennett and Brassard presented a protocol that allows users to establish an identical and purely random sequence of bits at two different locations, while allowing to reveal any eavesdropping with a very high probability.

Since light propagates faster and with smaller decoherence at a distance than matter, it is natural to turn our attention to photons as information carriers. Various properties of photons can be employed to encode information for QKD, such as polarization, phase, quantum correlations of Einstein-Podolsky-Rosen pairs, wavelength or quadrature components of squeezed states of light. The only requirement on the quantum states is that they belong to mutually nonorthogonal bases of their Hilbert space, where each vector of one basis has equal-length projections onto all vectors of the other basis. That is, if a measurement on a system prepared in one basis is performed in the other basis, its outcome is entirely random and the system "loses all the memory" of its previous state.

Let us consider polarization encoding. One basis can be spanned, e.g., by horizontally and vertically polarized photons, $|H\rangle$ and $|V\rangle$, resp.; let us call this basis *rectilinear*. The other basis, *diagonal*, would be spanned by photons polarized at 45°, $|A\rangle$, and 135°, $|D\rangle$. Since

$$\begin{aligned} |A\rangle &= \frac{\sqrt{2}}{2}\left(|H\rangle + |V\rangle\right) \quad \text{and} \\ |\mathrm{D}\rangle &= \frac{\sqrt{2}}{2}\left(|H\rangle - |V\rangle\right), \end{aligned} \tag{10}$$

these four states satisfy the following relations

$$\begin{aligned} \langle H|V\rangle = \langle A|D\rangle &= 0, \\ \langle H|H\rangle = \langle V|V\rangle = \langle A|A\rangle = \langle D|D\rangle &= 1, \\ |\langle H|A\rangle|^2 = |\langle H|D\rangle|^2 = |\langle V|A\rangle|^2 = |\langle V|D\rangle|^2 &= 1/2. \end{aligned} \tag{11}$$

Any measurements in the diagonal (rectilinear) basis on photons prepared in the rectilinear (diagonal) basis will yield random outcomes with equal probabilities. On the other hand, measurements performed in the basis identical to the basis of preparation of states will produce deterministic results. Since the two-dimensional polarization Hilbert space allows complex coefficients, we could generate a third basis of right- and left-polarized photons that exhibits the same properties and its states satisfy relations

analogous to Eqs. (11). As will be shown, any two of these three bases suffice for secure quantum key distribution, so let us choose the rectilinear and diagonal ones.

At the beginning, the two parties that wish to communicate, traditionally called Alice a Bob, agree that, e.g., $|H\rangle$ and $|A\rangle$ stand for the bit value "0", and $|V\rangle$ and $|D\rangle$ stand for a binary "1". Now Alice, the sender, generates a sequence of random bits that she wants to transmit, and randomly and independently for each bit she chooses her encoding basis, rectilinear or diagonal. Physically it means that she transmits photons in the four polarization states $|H\rangle$, $|V\rangle$, $|A\rangle$, and $|D\rangle$ with equally distributed frequencies. Bob, the receiver, randomly and independently of Alice, chooses his measurement bases, either rectilinear or diagonal. Statistically, their bases coincide in 50 % of cases, when Bob's measurements provide deterministic outcomes and perfectly agree with Alice's bits. In order to know when the outcomes were deterministic, Alice and Bob need an auxiliary public channel to tell each other what basis they had used for each transmitted and detected photon. This classical channel can be tapped, because it is only information about the used bases that Alice and Bob exchange, not the particular outcomes of the measurements. Whenever their bases coincide, Alice and Bob keep the bit whereupon it becomes part of the cryptographic key. The bit is discarded when they chose different bases, or Bob's detector failed to register a photon due to imperfect efficiency of detectors or the photon was lost somewhere on the way. Any potential eavesdropper, traditionally called Eve, who listens in to this conversation can only learn whether they both set the rectilinear or diagonal basis, but not whether Alice had sent a "0" or "1". The protocol is depicted in Table I.

0	**1**	**1**	**0**	**0**	**1**	**0**	**1**
×	×	+	+	+	×	+	×
$\|A\rangle$	$\|D\rangle$	$\|V\rangle$	$\|H\rangle$	$\|H\rangle$	$\|D\rangle$	$\|H\rangle$	$\|D\rangle$
×	+	+	×	×	+	+	×
$\|A\rangle$	R	$\|V\rangle$	R	R	R	lost	$\|D\rangle$
×	+	+	×	×	+	−	×
OK	–	OK	–	–	–	–	OK
0	–	**1**	–	–	–	–	**1**

Table I BB84 Protocol. 1st line – Alice's random bits. 2nd line – Alice's random polarization bases; "+" and "×" stand for the rectilinear and diagonal bases, resp. 3rd line – actual polarization of transmitted photons. 4th line – Bob's random detection bases. 5th line - polarization of detected photons; 'R' stands for a random outcome. 6th line – Bob publicly announces his measurement bases. 7th line – Alice publicly replies when Bob set the correct measurement basis. 8th line – the cryptographic key.

If there is Eve who wants to eavesdrop on the channel, she cannot passively monitor the transmissions, as shown in Chapter 4. What she can do is to intercept the photons sent by Alice, perform measurements on them and resend them. However, as Alice alternates her encoding bases at random, Eve does not know the basis to make a measurement in. She must choose her measurement bases at random as well. Half the time she guesses right and she resends correctly polarized photons. In 50 % of cases, though, she measures in the wrong basis, which produces errors. For example, let us suppose that Alice sends a "1" in the rectilinear basis, i.e., state $|V\rangle$, Eve measures in the diagonal basis, and Bob measures in the rectilinear basis (otherwise the bit would be discarded). Now, no matter whether Eve detects and resends $|A\rangle$ or $|D\rangle$, Bob has a 50 % chance to get $|H\rangle$, i.e., a binary "0", instead of $|V\rangle$. Thus, Bob finds errors in 25 % of bits successfully detected by him. If Alice and Bob agree to disclose part of their strings in order to compare them, they can discover these errors. When they set identical bases, their bitstrings should be in perfect agreement. When discrepancies are found, Eve is suspected of tampering with the photons, and the cryptographic key is thrown away. Thus, no information leak occurs even in the case of eavesdropping. If their strings are identical, the key is deemed secure and secret, and can be used for the above-mentioned Vernam cipher to encrypt communications. Since the bits used to test for eavesdropping are communicated over the open public channel, they must always be discarded and only the remaining bits constitute the key. A more detailed discussion of eavesdropping strategies will be provided in Section 5.7.

It should be mentioned that no physical apparatus is perfect and noiseless. Alice and Bob will always find discrepancies, even in the absence of Eve. As they cannot tell errors stemming from eavesdropping from the noise of the apparatus, they conservatively attribute all the errors in transmissions to Eve. From the number of errors, the amount of information that has potentially leaked to Eve can be estimated. Afterwards Alice and Bob reconcile their bitstrings using some error correction technique to arrive at an identical sequence of bits. This sequence is not completely secret. Eve might have partial knowledge about it. To eliminate this knowledge, they run a procedure called privacy amplification [42,43]. Privacy amplification is a method, which enables them to distill a secret bitstring from their data in such a way that Eve would know at most a single bit of the distilled string with an arbitrarily small probability. Both these procedures, error correction and privacy amplification, will be described in detail in Section 5.5.

5.3 Experiment

5.3.1 Principle

For secure QKD, information may be encoded in various degrees of freedom of quantum systems as long as the overlaps of signal states satisfy Eqs. (11) and Bob detects the same set of states as Alice sends. For instance, another approach different from polarization encoding is to encode bits in the phase difference in a Mach-Zehnder interferometer. Alice and Bob each have a phase shifter in one of the arms of the interferometer (see Fig. 1) and by applying suitable combinations of phase shifts, interference can be varied from constructive to destructive or no interference at all. The probability that a photon entering the interferometer of Fig. 1 emerges at detector D_1 or D_2, resp., is proportional to

$$\frac{1}{2}\left[1 \pm \cos(\phi_A - \phi_B)\right], \tag{12}$$

where the plus sign corresponds to D_1 and the minus to D_2, and ϕ_A and ϕ_B are Alice's and Bob's phase shifts, resp. Alice randomly sets one of the four phase shifts $(0, \pi, \pi/2, -\pi/2)$ and Bob also randomly chooses his measurement basis by setting 0 or $\pi/2$. When the difference of their phase shifts $(\phi_A - \phi_B) = 0, \pi$, they obtain deterministic outcomes and keep them. "0" is assigned to a detection at D_1 and "1" is assigned to a detection at D_2. When the phase difference is $(\phi_A - \phi_B) = \pm\pi/2$, the outcomes are random and they discard them in accordance with the protocol of Table I.

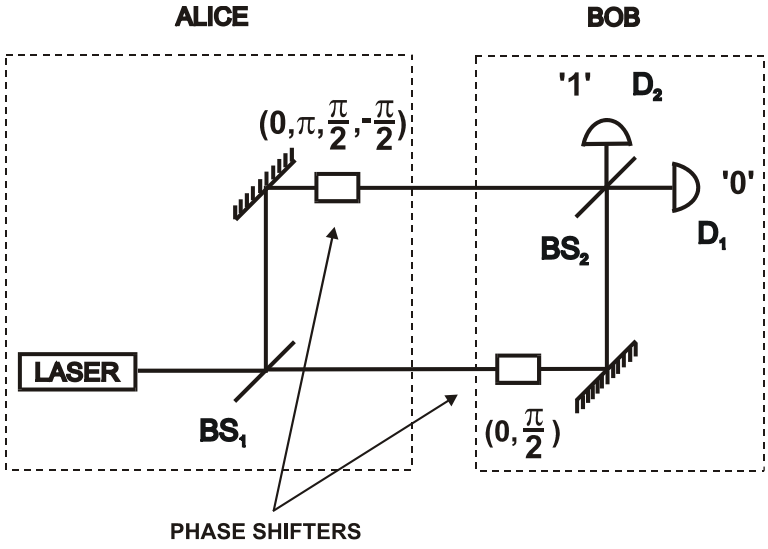

Fig. 1 The BB84 protocol can be realized by encoding information into the phase difference in a Mach-Zehnder interferometer. For $(\phi_A - \phi_B) = 0, \pi$, the outcomes of Bob's measurements are deterministic and become the cryptographic key. For $(\phi_A - \phi_B) = \pm\pi/2$, the outcomes are random and are discarded.

5.3.2 Time-Multiplexing Interferometer

If Alice and Bob were to be spatially separated, such an interferometer would, however, exhibit poor performance owing to environmental perturbations. For the interference not to be washed out, the difference of the optical lengths of the interferometer's arms must be kept constant to within a fraction of the wavelength of the used light. Connecting Alice and Bob by two optical fibers does not remove the problem either. Temperature fluctuations in the neighborhood of two adjoining optical fibers result in different changes in their refractive indices and smear out interference as well. For this reason, both paths of the interferometer were launched onto a single optical fiber, as shown in Fig. 2. Initially, a single-mode fiber of 15-m length was used.

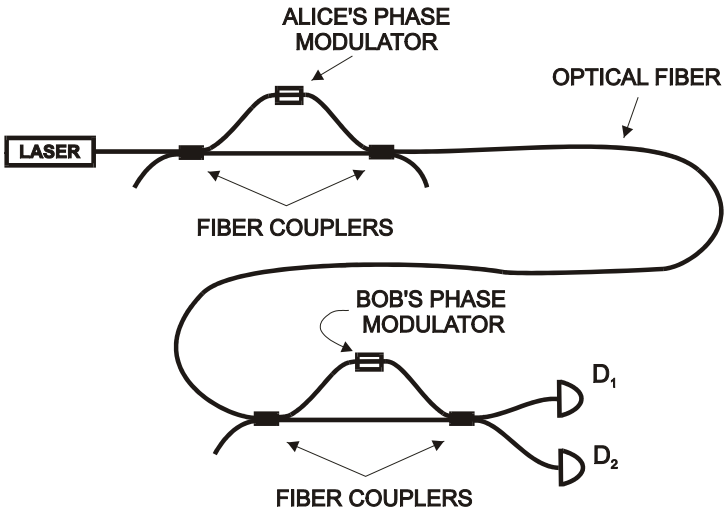

Fig. 2 Time-multiplexing interferometer that eliminates environmental fluctuations. Alice's and Bob's interferometers are identical unbalanced interferometers, whose path length differences is 2 m.

The interferometer comprised two identical unbalanced interferometers, whose path lengths difference was much greater than the coherence length of the laser. Thus no interference occurred in the small interferometers, but interference could be observed within the whole system. Fiber couplers performed random 50:50 splitting, so photons could go any of the four possible combinations of Alice's and Bob's paths: 25 % took Alice's short path and Bob's short path, 25 % took Alice's long path and Bob's short path, 25 % took Alice's short path and Bob's long path, and 25 % took both long paths. In our case, the length difference between the short and long arms of Alice's interferometer was approximately 2 meters of fiber. The same applied to Bob's interferometer. Photons then arrived at Bob's detectors in three time windows separated by 10 ns, as can be seen in Fig. 3. There is no interference in the first and third time

windows, but the middle window represents photons traveling along two undistinguishable, thereby interfering, paths – short-long and long-short, which constitute an interferometer analogous to the one of Fig. 1. At the expense of half the photons taking the "wrong" path, we are thus able to eliminate environmental fluctuations, because both paths of the interferometer are now affected the same. We only have to stabilize the small unbalanced interferometers, where the paths are spatially separate. This was secured by placing the small unbalanced interferometers in Styrofoam boxes.

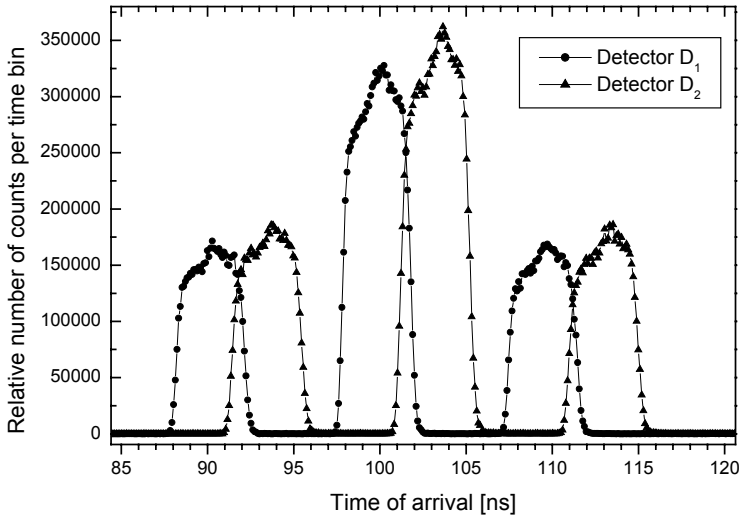

Fig. 3 Time of arrival in a 15-m time-multiplexing interferometer. Circles indicate detector D_1, triangles detector D_2. The delay between detectors arises from different lengths of coaxial cables connecting the detectors to the processing electronics. Photons arrived in 3 time windows separated by 10 ns, which correspond to 2 m of fiber. The leftmost peak corresponds to photons taking short-short paths. The rightmost peak corresponds to photons taking long-long paths. The middle peak corresponds to photons taking short-long and long-short paths. Interference only occurs in the middle time window.

The width of individual peaks of Fig. 3 is given by the width of laser pulses, 4 ns, jitter of detectors, 500 ps, and jitter of processing electronics, 300 ps. For comparison, Fig. 4 shows the three time windows in an interferometer, where the 15-m fiber, connecting Alice and Bob, was replaced with a 0.5-km piece. The spread of the peaks compared to Fig. 3 arises from lower time resolution due to scaling up the time range of the measuring electronics. Chromatic dispersion in fiber was negligible of the order of 100 ps. Modal and nonlinear dispersion did not occur; the former because single mode fibers were used, the latter because low intensity of light was used.

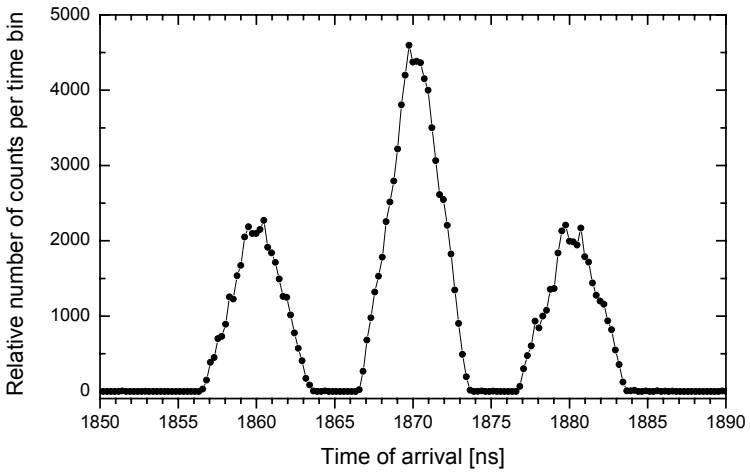

Fig. 4 Time of arrival at detector D_1 in a 0.5-km time-multiplexing interferometer. The spread of peaks in contrast to Fig. 3 is due to a greater measuring range of electronics. The values of the arrival time do not correspond to absolute time, as the timing reference pulses were electronically delayed.

5.3.3 Preparation of Quantum States and Intensity Measurement

At present, there is no source of single-photon states, which would allow us to encode bits in single quantum systems. Instead, we employed a single-mode semiconductor laser (SHARP LT015 MD), whose light was strongly attenuated. Since the spectral width of laser pulses was much smaller than their mean frequency, the light could well be approximated by a monochromatic coherent state. The photon-number distribution of the coherent state is governed by the Poisson distribution

$$p(n) = \frac{\mu^n e^{-\mu}}{n!}, \qquad n = 0,1,2, \ldots , \tag{13}$$

where μ is the mean number of photons per pulse. When the light is attenuated to, e.g., $\mu = 0.1$, 90.48 % of pulses contain no photon, 9.05 % of pulses contain one photon, 0.45 % of pulses contain two photons, 0.02 % of pulses contain three photons, etc. At the expense of more than 90 % of pulses being empty, we thus generate one-photon pulses with a total fraction of multi-photon pulses smaller than 0.5 %. The multi-photon pulses can cause problems, though. Eve could always split off one photon and perform a measurement on it without introducing an error. This potentially leaked information must be taken into account and eliminated by means of privacy amplification. A thorough analysis of the amount of information that can leak through this so-called beam-splitting attack can be found in [2] and will be summarized in Section 5.7.2.

For some measurements, it was necessary to measure the intensity of light pulses. The used detectors (see Section 5.3.7), however, could only provide yes/no

answers to the presence or absence of the optical field. Therefore, the intensity was measured indirectly in the following way.

If a coherent state with photon-number distribution $p(n)$ of Eq. (13) falls on a detector of detection efficiency η, the probability that m photoelectrons will be emitted is given by the Bernoulli transformation

$$p(m) = \sum_{n=m}^{\infty} \binom{n}{m} \eta^m (1-\eta)^{n-m} p(n). \tag{14}$$

Since the detectors cannot distinguish the number of impinging photons, the probability that the detector produces a pulse is given by the sum

$$P = \sum_{m=1}^{\infty} p(m). \tag{15}$$

Using Eqs. (13) and (14), we obtain

$$P = 1 - e^{-\eta\mu}. \tag{16}$$

If the laser is triggered N times to generate N pulses, the mean number of detected pulses is

$$\langle N_{\mathrm{Det}} \rangle = N\left(1 - e^{-\eta\mu}\right). \tag{17}$$

Now, measuring the number of detected pulses, we can readily calculate the effective intensity at the detector

$$I = \eta\mu = -\ln\left(1 - \frac{\langle N_{\mathrm{Det}} \rangle}{N}\right). \tag{18}$$

A more detailed scheme of the experimental setup is shown in Fig. 5. A pulsed semiconductor laser diode was driven by a high speed pulse generator (Avtech AVO-9A-C), and its 4 ns long laser pulses at a wavelength of 827 nm were fed at a repetition rate of 100 kHz into a computer-controlled variable attenuator (JDS Fitel HA9Z08-050). The attenuator dimmed the 2-mW pulses so that the mean intensity at the output of Alice's unbalanced interferometer was below one photon per pulse on average. The optimum level of mean intensity is a trade-off between the transmission rate and security, and it depends on various factors, such as transmission losses, detectors' efficiency, etc. It will be addressed in more detail in Section 6.5. The accuracy of the intensity setting was monitored by Alice's detector D_3.

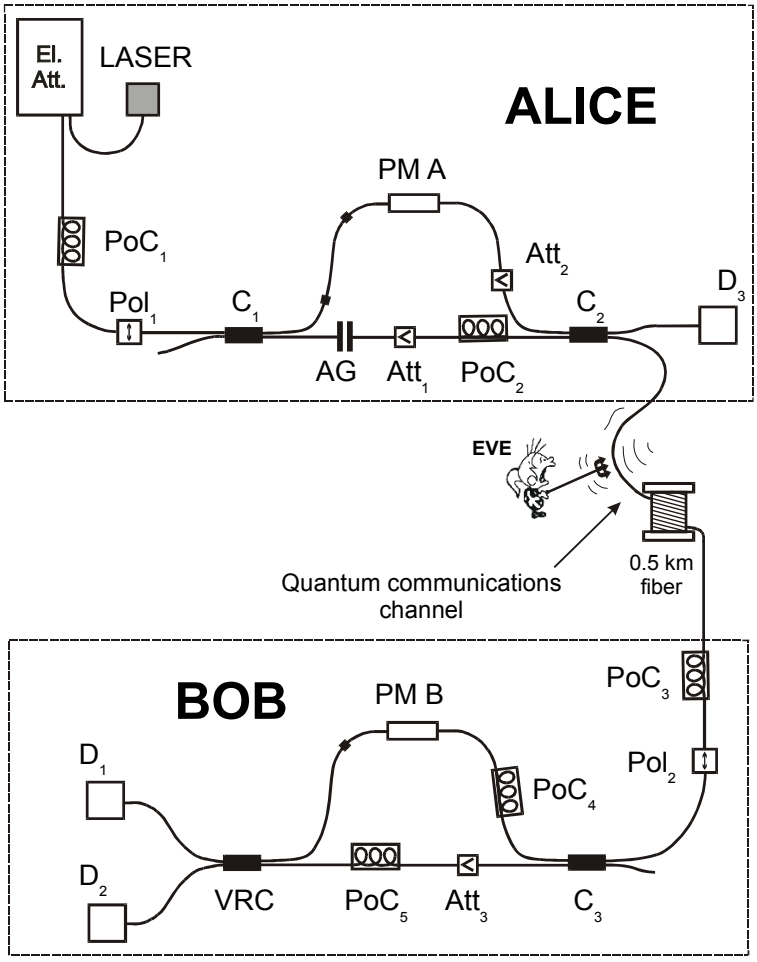

Fig. 5 Scheme of the optical part of the laboratory setup. El. Att. – computer-driven attenuator; PoC – polarization controllers; Pol – polarizers; C – 50:50 fiber couplers; PM – phase modulators; AG – air gap; Att – attenuators; VRC – single-mode variable ratio coupler; D – detectors. See details in text.

5.3.4 Polarization Control

To enhance the degree of polarization, polarizer Pol_1 was placed at the input of the interferometer, preceded by polarization controller PoC_1. Polarization controllers were used in the interferometer to adjust the polarization state in fibers. Bends and twists of the fiber induce birefringence, which gives rise to different velocities of the orthogonal polarization components. This in turn leads to deformation of the polarization state. Since the degree of polarization degrades slowly in fibers, the same stress-induced birefringence can, on the other hand, be used to compensate for this deformation. A fiber spool of a suitable diameter can act a fractional wave plate. The amount of birefringence induced by a fiber spool is a function of the fiber-cladding diameter, the spool diameter, the number of fiber loops per spool, and the wavelength of the light. If we calculate the diameter of the spool such that one loop introduces a

quarter-wave delay between the fast and slow axes of the fiber, we obtain a quarter-wave plate. Two loops of the same diameter will produce a half-wave plate. If we now coil fiber into three independent paddles, three independent wave retarders are created (Fig. 6). By rotating the paddles, we can independently adjust the angle between the fast axis of the fiber, which lies in plane of the spool, and the transmitted polarization state. When the first and third paddles contain one loop of fiber, and the middle paddle contains two loops, we have a set of two quarter-wave plates and one half-wave plate, which allow us to describe the whole Poincaré sphere.

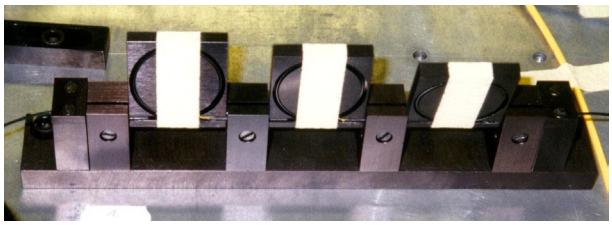

Fig. 6 Polarization controller. The left and right paddles contain one loop of fiber, acting as quarter-wave plates. The middle paddle contains two loops to act as a half-wave plate. Independent rotation of the three paddles allows describing the whole Poincaré sphere.

Polarization controllers PoC_1 and PoC_3 were employed to increase the throughput through polarizers Pol_1 and Pol_2. PoC_2 adjusted the polarization of Alice's short arm to match up with her long arm. PoC_4 minimized the losses of Bob's polarization-dependent phase modulator PM B, and polarization controller PoC_5 was used to reconcile the polarization of the interfering short-long and long-short paths of the interferometer.

5.3.5 Phase Encoding

The phase encoding was performed by means of planar electro-optic phase modulators PM (UTP APE PM-0.8-0.5, now JDS Uniphase). As their integrated-optical structure supports only one polarization mode with an extinction ratio greater than 10^5, it was necessary to minimize their losses by proper polarization adjustment using polarization controllers. The phase modulators were basically optical waveguides made of lithium niobate across which voltage was applied to produce the electro-optic effect. The manufacturer specified the modulators' half-wave voltage to be 1.1 V. The half-wave voltage is such a voltage that when applied to the modulator, the transmitted wave is delayed by π. In a Mach-Zehnder interferometer, it should thus turn constructive

interference into destructive. However, it did not correspond to observations and it was essential to measure its actual value.

The measurement of the half-wave voltage exploited the fact that an application of voltage corresponding to a 2π shift should not change the intensity at the output of the interferometer. Let us sequentially apply voltages $+U$ and $-U$, and measure corresponding intensities I_{+U} and I_{-U} at one of the detectors. If U is the true half-wave voltage, then

$$I_{+U} - I_{-U} = 0 . \tag{19}$$

For other voltages, the difference (19) will be nonzero. In practice, it will get a bit more complicated for several reasons: (1) We are not able to measure the intensity precisely; (2) the phase difference in the interferometer, and thereby the output intensity, drifts with time (see Section 5.3.9); and (3) the half-wave voltage is generated by a digital-to-analog converter (D/A converter) of finite resolution. Consequently, instead of zero, only a minimum should be observed. Since the difference $I_{+U} - I_{-U}$ can attain both positive and negative values owing to the thermal drift of the phase difference, its absolute values $|I_{+U} - I_{-U}|$ were taken. Because of the fluctuations, the intensity difference was measured 5000 times for each voltage and its average evaluated. The result for Bob's modulator is plotted in Fig. 7. The measured half-wave voltage $U_{\pi}^{(\mathrm{Bob})}$ was (0.975 ± 0.003) V. An analogous measurement of Alice's modulator yielded a half-wave voltage of (0.967 ± 0.003) V.

Now Alice could encode her bit values in the two bases by applying voltages 0, $U_{\pi}^{(\mathrm{Alice})}$, $+1/2\,U_{\pi}^{(\mathrm{Alice})}$, $-1/2\,U_{\pi}^{(\mathrm{Alice})}$, and Bob was choosing his measurement bases by applying $U_{\pi}^{(\mathrm{Bob})}$ or $+1/2\,U_{\pi}^{(\mathrm{Bob})}$.

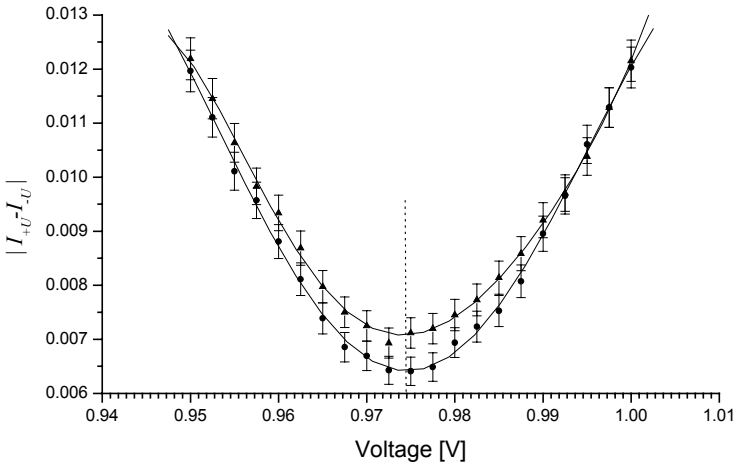

Fig. 7 Measurement of the half-wave voltage of Bob's modulator. The average of 5000 measurements of intensity difference $|I_{+U} - I_{-U}|$ is plotted as a function of voltage. 1000 laser pulses were generated for each intensity measurement. Either curve belongs to one detector. The minimum yields an actual half-wave voltage of (0.975 ± 0.003) V.

5.3.6 Balancing the Interferometer

Since it was impossible to cut and connectorize the optical fibers with a precision better than ones of centimeters, air gap AG (Fig. 8) was inserted in Alice's short arm to balance the arm lengths of the interferometer. The air gap consisted of two collimators (OZ Optics HUCO-13-830-S-2-GRD) to couple light in and out of the fiber. One of the collimators was attached to a linear computer-driven translation stage with a resolution of 100 nm (Oriel Encoder Mike 18236). Moving the stage was changing the distance between the collimators, thereby changing the optical length of the short-long arm of the interferometer.

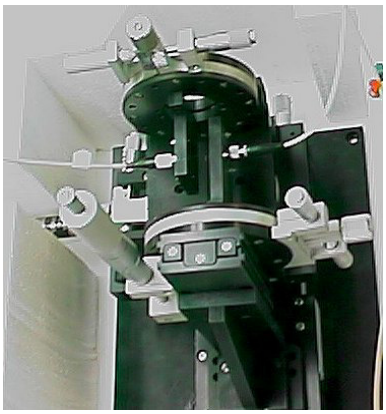

Fig. 8 A top view of the air gap, which served to balance the optical lengths of the arms of the interferometer.

The balance of losses and beam-splitting ratios is also important. Beam-splitter imperfections and unequal losses in the arms of a Mach-Zehnder interferometer adversely affect visibility. It was shown in [6] that the visibility at detector D_1 of the interferometer of Fig. 1 can be expressed as

$$V_1 = 2\left(\frac{|r_1|}{|t_1|}\frac{|t_2|}{|r_2|}\frac{|t_A|}{|t_B|} + \frac{|t_1|}{|r_1|}\frac{|r_2|}{|t_2|}\frac{|t_B|}{|t_A|}\right)^{-1}, \tag{20}$$

and similarly at detector D_2

$$V_2 = 2\left(\frac{|r_1|}{|t_1|}\frac{|r_2|}{|t_2|}\frac{|t_A|}{|t_B|} + \frac{|t_1|}{|r_1|}\frac{|t_2|}{|r_2|}\frac{|t_B|}{|t_A|}\right)^{-1}, \tag{21}$$

where r_1, r_2, and t_1, t_2 are the amplitude reflectances and transmittances of beam-splitters BS_1 and BS_2, resp., and t_A and t_B are the transmittances of Alice's and Bob's arms of the interferometer, resp. Visibilities V_1 and V_2 attain their maxima

$$V_1 = 1 \qquad \text{if} \qquad \frac{|r_1|}{|t_1|}\frac{|t_2|}{|r_2|}\frac{|t_A|}{|t_B|} = 1\,, \tag{22}$$

and

$$V_2 = 1 \qquad \text{if} \qquad \frac{|r_1|}{|t_1|}\frac{|r_2|}{|t_2|}\frac{|t_A|}{|t_B|} = 1\,. \tag{23}$$

Fig. 9 shows the degradation of V_1 and V_2 when the splitting ratios of BS_1 and BS_2 differ from 50:50 provided that losses in Alice's and Bob's arms are equal, i.e., $|t_A| = |t_B|$.

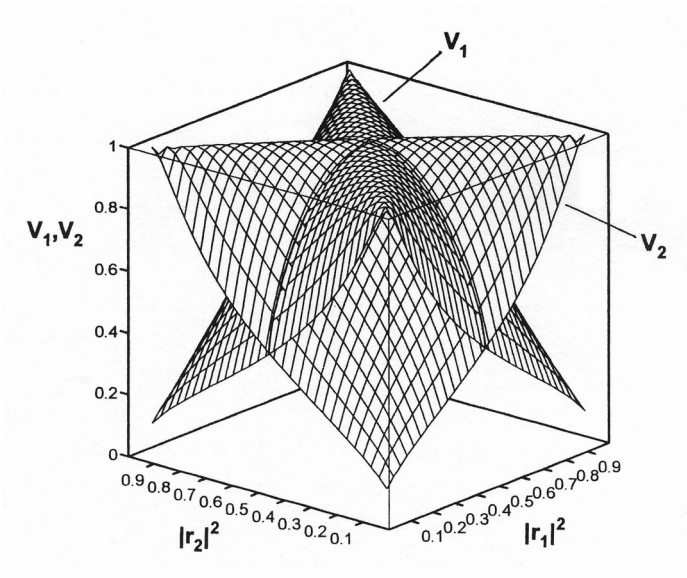

Fig. 9 A plot of V_1 and V_2 as a function of power reflectances $|r_1|^2$ and $|r_2|^2$ if $|t_A| = |t_B|$.

Visibilities V_1 and V_2 simultaneously reach unity for $|r_1|^2 = |r_2|^2 = 0.5$, as expected. If $|r_1|^2 = |r_2|^2 \neq 0.5$, V_1 remains unity while V_2 decreases to

$$V_2 = 2\left(\frac{|r_1|^2}{|t_1|^2} + \frac{|t_1|^2}{|r_1|^2}\right)^{-1}. \tag{24}$$

If $|r_1|^2 = |t_2|^2$, V_1 and V_2 exchange one another. A top view of V_1 is shown in Fig. 10(*a*).

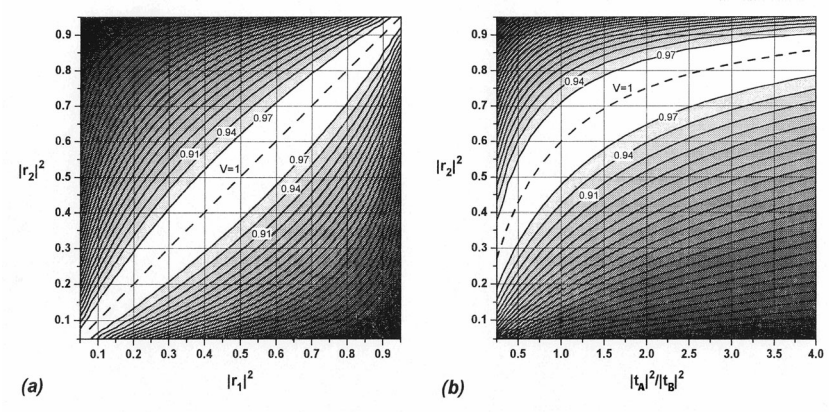

Fig. 10 A top view of V_1 (*a*) as a function of power reflectances $|r_1|^2$ and $|r_2|^2$ if $|t_A| = |t_B|$, (*b*) as a function of $|t_A|^2/|t_B|^2$ and $|r_2|^2$ when BS_1 splits 60:40. The lighter shade of grey the higher visibility. The dashed lines indicate $V_1 = 1$. Each next line indicates a visibility decrease by 3 %.

It follows from Eq. (20) that it is possible to reach unity visibility at D_1 even when $|r_1|^2 \neq |r_2|^2$. It can be achieved by introducing an appropriate amount of losses in one of the arms of the interferometer, in particular by setting the ratio $|t_A|/|t_B|$ such that the condition (22) is satisfied. V_2 consequently decreases to

$$V_2 = 2\left(\frac{|r_2|^2}{|t_2|^2} + \frac{|t_2|^2}{|r_2|^2}\right)^{-1}. \tag{25}$$

In the same way, we can improve the visibility at D_2, whereupon V_1 drops to the value given by the right-hand side of Eq. (25). Fig. 10(*b*) shows the dependence of V_1 on the ratio of Alice's and Bob's losses $|t_A|^2/|t_B|^2$ and $|r_2|^2$ with a splitting ratio of BS_1 set to 60:40.

It is important to note that the expression (25) is a function of one independent variable characterizing BS_2 only. It indicates that beam-splitter BS_2 is more significant than BS_1. If BS_2 were an ideal 50:50 beam-splitter, it would be possible to reach unity visibility at both detectors simultaneously, regardless of imperfections of BS_1. The conditions that must hold in order that $V_1 = V_2 = 1$ have the form

$$|r_2|^2 = 0.5 \qquad \text{and} \qquad \frac{|r_1|}{|t_1|}\frac{|t_A|}{|t_B|} = 1. \tag{26}$$

If $|r_2|^2 \neq 0.5$, unity visibility can only be reached at one of the detectors, D_1 or D_2. Hence, the beam-splitter whose splitting ratio is closer to 50:50 should be used as the combiner, i.e., BS_2. If only one of the equalities (26) is true, visibilities V_1 and V_2 are equal but lower than 1.

To give an illustration, an air gap of a 2-dB insertion loss placed in one of the arms of the interferometer, would cause visibility at both detectors to decrease by 2.5 %. If the splitting ratios BS_1 and BS_2 were in addition 56:44 and 53:47, V_1 would

drop to 96 % and V_2 even to 92 %. These values are not far-fetched. The coupling ratios of commercially available 3-dB (50:50) fused couplers (OZ Optics Fused-22-830-5/125-50/50) were even worse, around 62:38. These were later replaced with fiber-optic beam splitters (OZ Optics FOBS-22P-5/125-830-50/50) with splitting ratios ranging about 54:46. The fiber-optic beam splitters were regular bulk beam splitters flanked by collimators to couple light in and out of fibers. This configuration, however, exhibited up to 3 % changes of the splitting ratio, dependent on the input polarization state. Eventually, Sifam fused couplers with coupling ratios approaching 52:48 were acquired and used as C_1-C_3 of Fig. 5, and a variable-ratio coupler (Sifam SVRC) was employed as the combiner VRC.

The variable-ratio coupler consisted of two parallel single-mode fibers, stripped of their cladding, and brought into close optical contact by a thin film of oil of suitable refractive index. The cores of the fibers were in close proximity, only a few wavelengths apart from each other. Their distance determined how much power was transferred by means of evanescent waves from one fiber into the other fiber. By adjusting their distance, it was possible to set the coupling ratio very close to 50:50.

To minimize the effect of imperfect splitting ratios of fiber couplers C_1-C_3 and to balance the losses, a set of attenuators were used (OZ Optics BB-200-33-830-S). The attenuators were essentially two collimators between which a bolt was screwed to block the light. Attenuators Att_1 and Att_2 served to even the intensity in Alice's short and long arms. Attenuator Att_3 balanced the 2.5-dB insertion loss of Bob's phase modulator.

The fiber components were keyed together to minimize the losses of the communications channel and Bob's terminal. It will be shown in Section 6.4 that losses severely limit the distance over which secure QKD can be realized. The overall losses of the more than 0.5 km long interferometer did not eventually exceed 5.5 dB.

The optical fiber interconnecting Alice and Bob was subject to mechanical vibrations, temperature changes and other environmental fluctuations, which distorted the polarization state. Different polarization states then experienced different attenuation at Bob's phase modulator, which resulted in imbalance of losses, which in turn resulted in degradation of visibility. In order to remove this polarization dependence of interference, polarizer Pol_2 was inserted at the input to Bob's interferometer. Now, when the polarization state was deformed on the way to Bob, only the transmission rate was reduced, but not the visibility.

5.3.7 Detection

Single-photon counting modules D_1-D_3 were thermoelectrically cooled silicon avalanche photodiodes (EG&G SPCM-AQ 141-FC, now PerkinElmer), that were operated above the breakdown voltage in the so-called Geiger mode [44]. With a certain probability, an impinging photon is absorbed in the active volume of the detector and generates an electron-hole pair. The *p-n* junction of the photodiode is biased above the

breakdown voltage with the electric field so high that a single electron injected into the depletion layer can trigger a self-sustaining avalanche. The avalanche is amplified to a macroscopic level, discriminated, and shaped into a 9 ns long TTL pulse. Electronic circuits then quench the avalanche by lowering the bias voltage below the breakdown.

As a side effect of the quenching, some carriers can be trapped in the junction, exponentially dissipating with time. When the bias voltage is applied again to prepare the detector for another pulse, some of them can still retrigger the avalanche and produce a so-called afterpulse. The number of afterpulses is proportional to the bias voltage, thereby to photon detection efficiency, and inversely proportional to the dead time of the detector. Our detectors were adjusted to a detection efficiency about 52 % at 830 nm, which required a dead time of 30 ns. The 30-ns dead time was suitable, because the first afterpulses could not occur in the region of interest, given by the arrival of photons in the three time windows of Fig. 4.

Since interference occurred in the middle peak only, time resolution of the order of ones of nanoseconds was necessary. In order to achieve this resolution, time-to-amplitude converters were used (EG&G ORTEC TAC 566), one for each detector. The electric pulses that triggered Alice's laser served as the timing reference to start the converters. Upon receipt of a start pulse, the TAC linearly integrates voltage until it receives a stop pulse, furnished by the detector. The time interval between the start and stop pulses is thus converted to voltage, measured by a single-channel analyzer (EG&G ORTEC SCA 550A). The SCA was set so as to accept a range of voltages corresponding to the time delay of the middle peak. As the leading and trailing edges of 4-ns laser pulses exhibited poorer visibility, the time window was narrowed to 3 ns. This window size also substantially reduced the noise arising from detectors' spurious detections – the so-called dark counts. Dark counts are a function of the bias voltage and their typical values were about 60 counts per second. The probability that such a dark count will fall within a 3-ns window is less than 2^{-7}.

When the SCA received a pulse of appropriate height, it generated an output that flipped a monostable circuit, which was read by Bob's computer. Depending on which of the two monostable circuits was active, Bob recorded a logical "1" or "0". A picture of Alice's and Bob's parts of the interferometer are shown in Figs. 11 and 12.

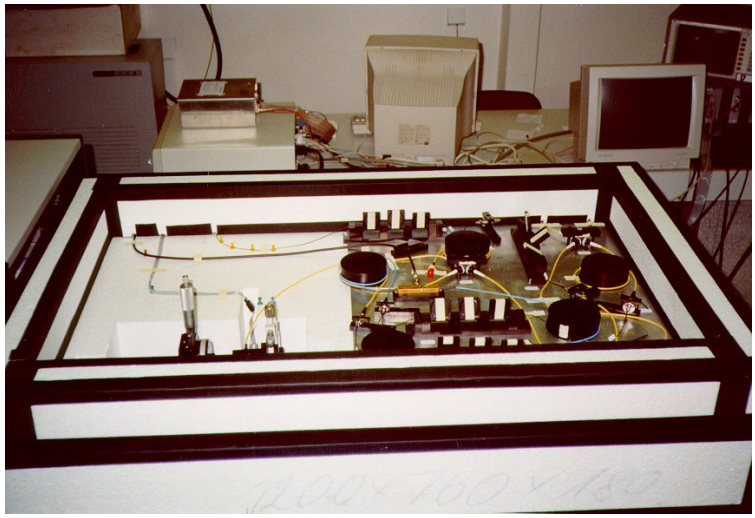

Fig. 11 Alice's part of the interferometer embedded in the Styrofoam box.

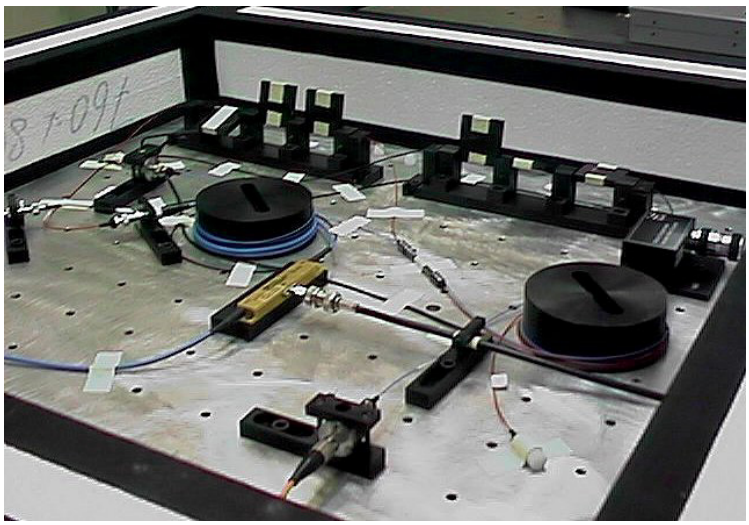

Fig. 12 Bob's part of the interferometer with his phase modulator in the center and the variable-ratio coupler in the top-right corner.

5.3.8 Visibility

With this setup, it was possible to reach visibility above 99.6 %. However, in order to achieve that, it was necessary to balance the optical lengths of the interferometer's arms with great accuracy. Fig. 13 depicts the dependence of visibility on the path lengths mismatch, which was produced by broadening the air gap in Alice's short arm of the interferometer. The visibility did not follow a Lorentzian, gradually tapering curve, as expected. Instead, a train of narrow peaks was observed, raising doubts whether the semiconductor laser was truly single-mode.

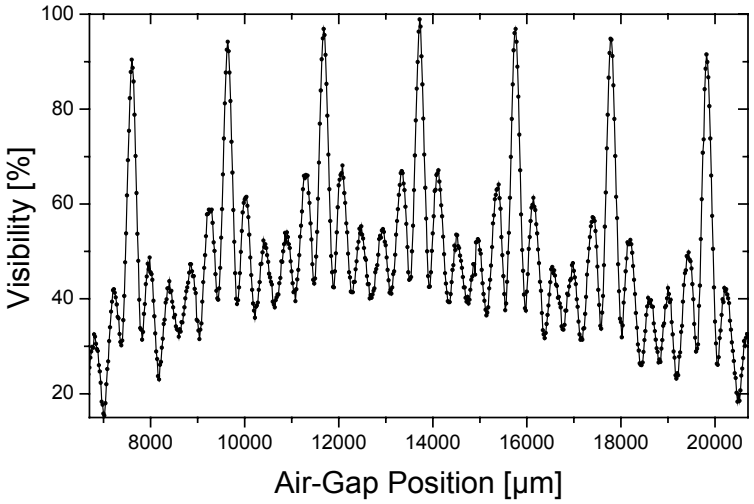

Fig. 13 Visibility as a function of the air-gap width. This pattern is a consequence of weak side modes in the spectrum of the laser. The tips of the peaks are 20 μm wide.

Since a Mach-Zehnder interferometer essentially measures the complex degree of coherence, it is interesting to calculate its Fourier transform to obtain the spectrum of the laser. The intensity at the output of a Mach-Zehnder interferometer is given by [45]

$$I = I_1 + I_2 + 2\sqrt{I_1 I_2}\ \mathrm{Re}\{\gamma(\tau)\}, \tag{27}$$

where I_1 and I_2 are the contributions from either arm when the other one is blocked. $\gamma(\tau)$ is the complex degree of temporal coherence

$$\gamma(\tau) = \frac{\Gamma(\tau)}{\sqrt{I_1 I_2}}, \tag{28}$$

$$0 \le |\gamma(\tau)| \le 1, \tag{29}$$

where $\Gamma(\tau)$ is the autocorrelation function of the interfering complex field amplitude $A(t)$

$$\Gamma(\tau) = \langle A^*(t)\, A(t+\tau) \rangle, \tag{30}$$

where $\langle \cdot \rangle$ denotes an ensemble average. For quasi-monochromatic light with central frequency $\bar{\nu}$, whose spectral width $\Delta\nu << \bar{\nu}$, the degree of coherence can be written in the form

$$\gamma(\tau) = |\gamma(\tau)|\, e^{i\varphi(\tau)}. \tag{31}$$

With the use of Eq. (31), Eq. (27) can be written as

$$I = I_1 + I_2 + 2\sqrt{I_1 I_2}\, |\gamma(\tau)| \cos\varphi(\tau). \tag{32}$$

The fringe visibility is defined as

$$V = \frac{I_{\max} - I_{\min}}{I_{\max} + I_{\min}}. \tag{33}$$

Taking the maximum and minimum of Eq. (32) and plugging them into Eq. (33), we obtain

$$V = 2\frac{\sqrt{I_1 I_2}}{I_1 + I_2}\left|\gamma(\tau)\right|. \tag{34}$$

It follows from Eq. (34) that when the losses in the interferometer are properly balanced, i.e. $I_1 = I_2$, the measured visibility is equal to the magnitude of the degree of coherence $\left|\gamma(\tau)\right|$. Its phase $\varphi(\tau)$ can then be acquired from the locations of peaks of the interference pattern. Now, using the normalized Wiener-Khinchin theorem on the spectral decomposition of the degree of coherence

$$\gamma(\tau) = \int_0^\infty g(\nu)\, e^{-i2\pi\nu\tau} d\nu, \tag{35}$$

we can calculate the normalized spectral density $g(\nu)$, which is shown in Fig. 14. The spectrum exhibits six weak side modes on either side of the central lasing wavelength. The 1st and 5th lobes reach 7 % and the remaining lobes reach about 1.5 % of the central peak's intensity. It is these "adulterants" that are to blame for the strong modulation of the visibility curve, which thus imposed strict requirements on the balance of the

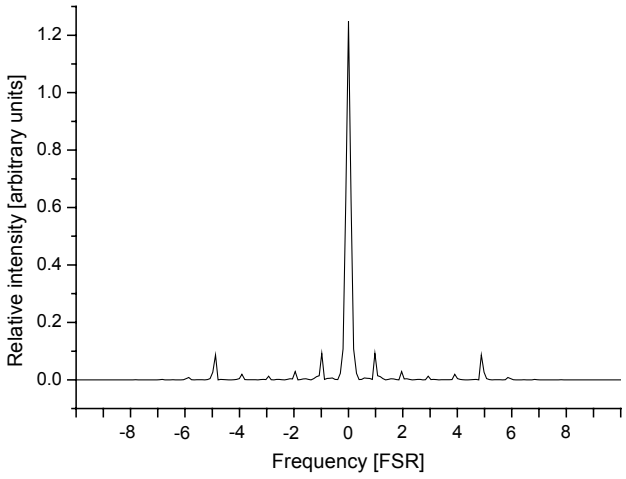

Fig. 14 Normalized spectral density $g(\nu)$ as a function of frequency. The spectrum of the supposedly single-mode laser shows six side lobes on either side of the central peak. These weak side modes result in the strong modulation of the visibility of Fig. 13.

interferometer's arms. The width, or rather the narrowness, of the plateaus at the tip of the visibility peaks was only 20 μm. An optical lengths mismatch of 150 μm would result in a plunge of the visibility down to 50 %.

5.3.9 Phase Drift

Even though the end parts of the time-multiplexing interferometer were placed in Styrofoam boxes, the phase difference still slowly drifted with time. A typical phase drift is shown in Fig. 15. We can see the phase difference cover $\pi/2$ in approximately 2000 seconds. (The seeming turning point at $\pi/2$ is accidental. The drifting phase difference sometimes changed its direction and did not span the whole range $\langle 0,2\pi \rangle$.) It was necessary to "calibrate" the interferometer, i.e., to find the voltage on Bob's phase modulator, which corresponds to the zero phase difference. When the voltage was found, it was possible to perform measurements or data transmissions for a period of about 4 s, after which the interferometer was recalibrated. The 4-s period was chosen, because during that time the phase difference drifted away by less than $\pi/1000$, on average.

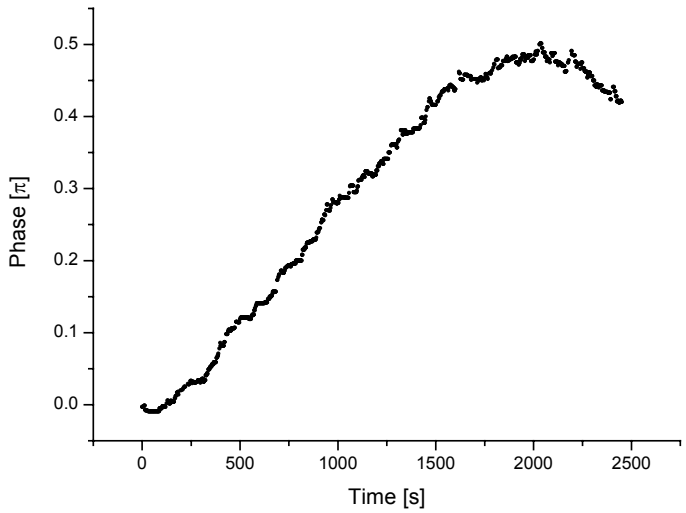

Fig. 15 Thermal drift of the phase difference in the interferometer. On average, the phase difference changed by less than $\pi/1000$ in 4 s.

In order to find his relative zero-phase voltage, Bob tells Alice to maintain her phase shift constant, say 0, and scans the whole period of an interference fringe. Applying a voltage ramp in small increments, and measuring the intensity at detectors according to Section 5.3.3, he can find an approximate position of the minimum of the fringe. Let us recall that very weak coherent states are used, thereby the intensity in the

minimum is small (but not zero due to $V < 100$ % and noise), and it would take some time to gather enough data to find its position accurately. During this time the fringe minimum could drift away. Therefore, when Bob finds his approximate minimum, he measures its intensity I_0 and calculates his relative position on the sine curve of the fringe

$$y = \frac{I_0 - I_{\min}}{I_{\max} - I_{\min}}, \tag{36}$$

where $I_{\max}$ and $I_{\min}$ are the intensities at the maximum and minimum of the fringe, resp. If

$$y < \frac{I_{\lim}}{I_{\max} - I_{\min}}, \tag{37}$$

where $I_{\lim}$ is a tolerated inaccuracy of his setting, he hit right on the minimum and the calibration is finished. If

$$y > \frac{I_{\lim}}{I_{\max} - I_{\min}}, \tag{38}$$

a quarter-wave voltage is applied and intensity $I_{\pi/2}$ measured. We can thus take advantage of the greatest slope of the sine in the neighborhood of the inflection point. When the intensity is measured there, small inaccuracies of the phase setting are more pronounced, and Bob can determine his phase offset more precisely. Once known, he then sets his new, corrected phase shift, measures the intensity I_0 again and checks whether Eq. (37) is fulfilled. If it is so, the calibration was successful and the interferometer is ready for communication. If not, the procedure is repeated. Now, if Bob calibrates every 4 seconds, he can easily keep track of his relative zero and the scan of the fringe is not needed anymore. Intensities $I_{\max}$ and $I_{\min}$ do not change either, because the visibility varied only slightly on a day-to-day basis or when an adjustment to the interferometer was made.

5.3.10 Quantum Alphabet

Now that the interferometer was properly aligned and tuned, it was finally possible to run a procedure, termed the *quantum alphabet*, to check the performance of the interferometer as a communication device. Alice and Bob set different combinations of their bases, and Alice in turn transmits sequences of 0's and 1's for each of them. The outcomes of a typical run of the quantum alphabet are summarized in Table II. Each sequence comprised 10 blocks at 32 kbits and over 500 sequences were evaluated.

Let us define the correlation between Alice's and Bob's bitstrings

$$C = \sum_{i=1}^{N} \frac{\overline{a_i \oplus b_i}}{N}, \tag{39}$$

where $\overline{a_i \oplus b_i}$ denotes the exclusive NOR between Alice's and Bob's i-th bits, and N is the number of bits in compared bitstrings. We can see that for matching bases the correlation was approaching 100 % for both, sequences of 0's and sequences of 1's; for different bases, it was close to 50 %, as expected. Fig. 16 illustrates the frequency distribution of correlations between Alice's and Bob's bits for individual sequences, when their bases were different (*a*) and when they were identical (*b*).

+	+	+	+	×	×	×	×
0	1	0	1	0	1	0	1
0	π	0	π	π/2	−π/2	π/2	−π/2
+	+	×	×	+	+	×	×
0	0	π/2	π/2	0	0	π/2	π/2
99.72±0.37	99.76±0.29	49.18±3.12	50.70±3.23	49.17±3.10	51.48±3.22	99.72±0.33	99.75±0.30

Table II Quantum alphabet. 1st line – Alice's encoding bases. 2nd line – the bit value used to generate a sequence. 3rd line – Alice's actual phase shifts. 4th line – Bob's detection bases. 5th line – Bob's actual phase shifts. 6th line – correlation C between Alice's and Bob's bitstrings [%].

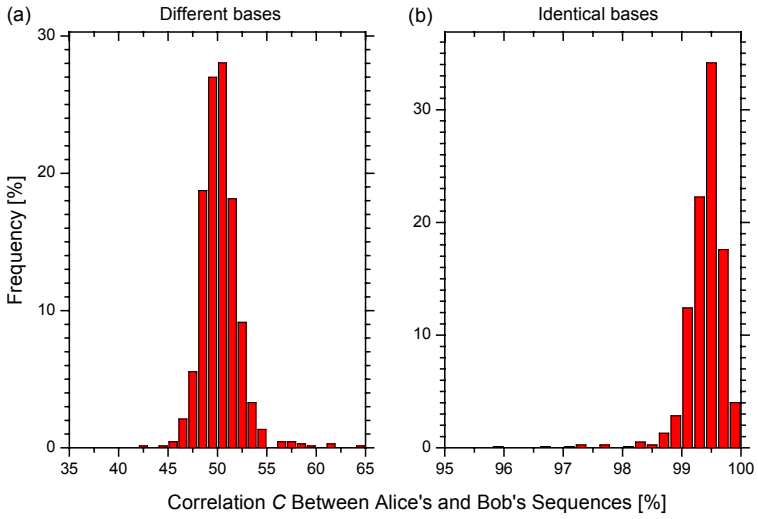

Fig. 16 Frequency distribution of correlations between Alice's and Bob's sequences, when their bases were (*a*) different and (*b*) identical.

A quantitative figure of merit used to assess the quality of a communications line is the so-called bit error rate (*BER*). The bit error rate is defined as the ratio of the number of wrongly detected bits to the total number of the detected bits. Its measurement proceeded as follows. Alice's pseudo-random number generator generated random bits and random encoding bases. Based on the measurements of the half-wave voltage, described in Section 5.3.5, her D/A converter applied corresponding voltages to her phase modulator. Similarly, Bob's independent generator produced random bits, which set his random detection bases by means of his D/A converter. Data was transmitted in 32-kbit sequences. The visibility was 99.7 % and the interferometer was recalibrated every 4 seconds. After transmitting 500 sequences, Alice and Bob announced their bases over the public channel (the local computer network), and dropped the cases when the bases differed. In the remaining cases, they compared their data and calculated the *BER* in individual sequences. The distribution of *BER*s is shown in Fig. 17. The average *BER* achieved was 0.32 %. For illustration, Fig. 18 plots an actual *BER* as a function of the sequence number. The dashed line depicts the moving average of the *BER*.

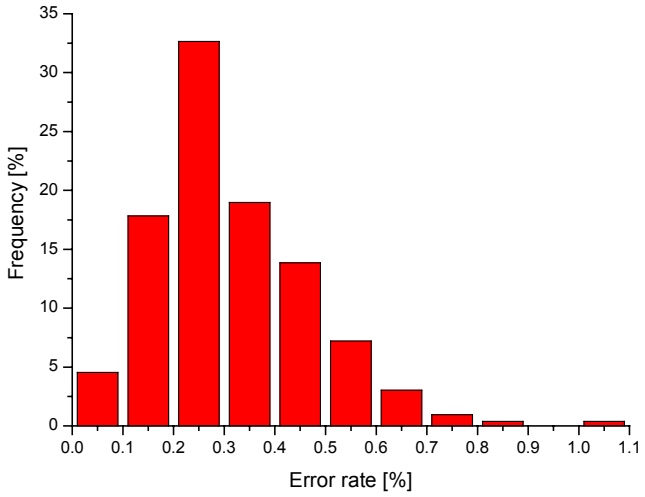

Fig. 17 Frequency distribution of *BER*s of individual sequences. The average *BER* was 0.32 %.

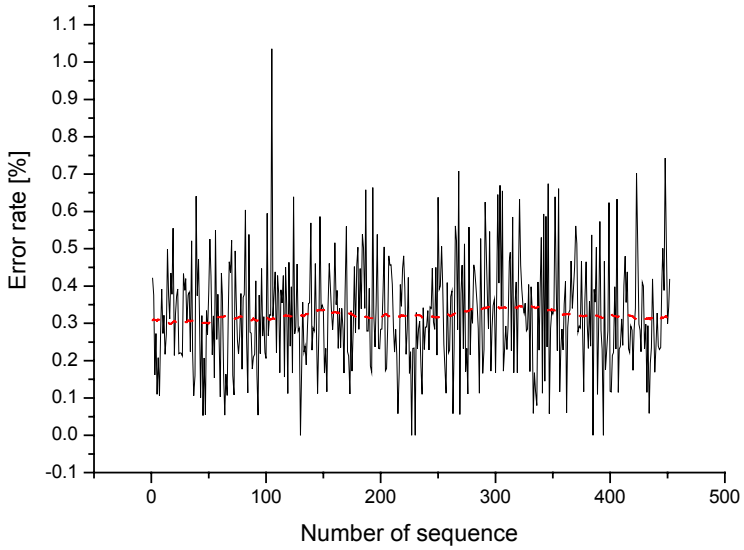

Fig. 18 A plot of the *BER* as a function of the sequence number. The dashed line shows the moving average calculated from 100 points.

5.4 Test for Eavesdropping

The *BER* is a measure of how much information might have leaked to Eve during the quantum transmission. Even though Alice and Bob know that their system produces a certain error rate owing to imperfections and noise, they must assume it all arises from eavesdropping. Eve is allowed to possess any technology permitted by quantum mechanics. She could find out the causes of these imperfections, attempt to fix them, and subsequently take advantage of the reduced *BER*.

It was shown in [46] that if Eve follows an optimal eavesdropping strategy allowed by quantum mechanics, there is an upper bound to the information she can gain, while introducing a given error rate (under the assumption that Eve performs the so-called individual attacks; see Section 5.7). In addition, when the mutual information I_{AB} between Alice and Bob after eavesdropping

$$I_{AB} > \max\{I_{AE}, I_{EB}\}, \tag{40}$$

where I_{AE} and I_{EB} are the mutual information between Alice and Eve and between Eve and Bob, resp., it is possible to obliterate Eve's information with the help of privacy amplification (see next Section) in such a way that Eve would know at most one bit of the secret key with an arbitrarily small probability. If Eve has acquired more information than I_{AB}, she must have introduced an error rate greater than $BER_{safe} \cong 14.6\,\%$. When Alice and Bob find their error rate $BER \geq 14.6\,\%$, the channel is not safe and all the data must be discarded.

During quantum key distribution, however, Alice and Bob cannot measure the actual *BER* by publicly comparing all their bases and bit values, as was described in the previous Section. The public channel is subject to eavesdropping and Eve could easily learn the entire cryptographic key. Therefore, the users only choose a random subset of their bitstrings to estimate the *BER*. Since the bit values in the subset are disclosed, they must always be discarded and never become part of the key.

In the experiment, Alice generated 320-kbit sequences of laser pulses. After each sequence, the interferometer was recalibrated. Once 20 sequences had been transmitted, Alice and Bob generated a random, and identical, subset of their *raw key* and compared the bit values to estimate the error rate. An important issue is to find a suitable length of the subset so that the error rate can be estimated faithfully. Alice and Bob also have to agree on some limiting error-rate estimate $\varepsilon_{\lim}$ they will accept as safe. When their error-rate estimate is lower than $\varepsilon_{\lim}$, they want to conclude that the probability that the actual error rate is higher than BER_{safe}, is lower than some "safety parameter" δ (see [1]).

Let us suppose that Bob selects a subset of length $2s$, out of which s bits remain on average after he compares his bases with Alice. Provided that the actual error rate is ε, the probability that he finds k errors in the subset of length s is given by

$$p\left(\varepsilon_{\text{est}}|\varepsilon\right)=\binom{s}{k}\varepsilon^{k}\left(1-\varepsilon\right)^{s-k}, \tag{41}$$

where $\varepsilon_{\text{est}}=k/s$ is the error-rate estimate. Applying Bayes' theorem, the probability that the actual error rate is ε, when the estimate is ε_{est}, is given by

$$p\left(\varepsilon|\varepsilon_{\text{est}}\right)=\frac{\left[\varepsilon^{\varepsilon_{\text{est}}}\left(1-\varepsilon\right)^{1-\varepsilon_{\text{est}}}\right]^{s}}{\int_{0}^{1}\left[\varepsilon^{\varepsilon_{\text{est}}}\left(1-\varepsilon\right)^{1-\varepsilon_{\text{est}}}\right]^{s}d\varepsilon} \tag{42}$$

under the assumption of uniform distribution of ε. We are now interested in finding a limiting value $\varepsilon_{\lim}$ such that for all $\varepsilon_{\text{est}}\leq\varepsilon_{\lim}$ the probability that the actual error rate ε is greater than some maximum tolerable error rate $\varepsilon_{\max}$, is

$$P\left(\varepsilon>\varepsilon_{\max}\right)=\int_{\varepsilon_{\max}}^{1}p\left(\varepsilon|\varepsilon_{\text{est}}\right)d\varepsilon\leq\delta, \tag{43}$$

where a small positive number δ denotes a security parameter, i.e., the probability of Eve's escape. Fig. 19 plots the solution of the equation

$$\frac{\int_{\varepsilon_{\max}}^{1}\left[\varepsilon^{\varepsilon_{\lim}}\left(1-\varepsilon\right)^{1-\varepsilon_{\lim}}\right]^{s}d\varepsilon}{\int_{0}^{1}\left[\varepsilon^{\varepsilon_{\lim}}\left(1-\varepsilon\right)^{1-\varepsilon_{\lim}}\right]^{s}d\varepsilon}=\delta \tag{44}$$

with respect to $\varepsilon_{\lim}$ for several values of δ. A maximum acceptable error rate $\varepsilon_{\max}=7\,\%$ was chosen, which is well bellow the security limit BER_{safe}. The graph in Fig. 19 should be understood as follows: Once we choose suitable values of the subset length s and the security parameter δ, the corresponding curve suggests a limiting value

for the estimated error rate, above which the transmitted sequence should be rejected as it cannot be guaranteed to have the actual error rate $\varepsilon \le \varepsilon_{\max}$ with the required probability $1 - \delta$. If we choose, e.g., $s = 1000$ and $\delta = 10^{-10}$, we find $\varepsilon_{\lim} \approx 2.4\ \%$.

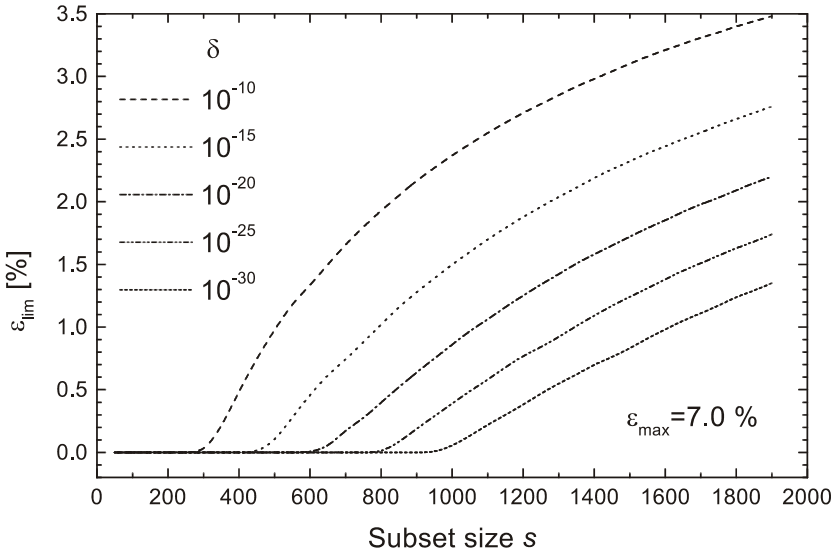

Fig. 19 The dependence of limiting value $\varepsilon_{\lim}$ on subset size s for different values of the security parameter δ, when a maximum error rate of $\varepsilon_{\max} = 7\ \%$ is tolerated. A subset of length $2s$ is randomly selected from the raw quantum data, which yields s bits with coincident bases on average. Quantum transmission is considered insecure (i.e., the probability of the actual error rate ε being higher than $\varepsilon_{\max}$ is not lower than δ), if the error-rate estimate ε_{est} obtained from the subset check exceeds the value $\varepsilon_{\lim}$.

5.5 Error Correction and Privacy Amplification

When Alice and Bob estimate the error rate and find that the actual BER is greater than $\varepsilon_{\max}$ only with probability smaller than δ, they can proceed to generate the cryptographic key. They compare the remaining encoding bases (but not the bit values) and establish the so-called *sifted key* from the bits when their bases coincided. Now they possess two data strings, which are not completely identical owing to the error rate, and which are not even secret, because Eve can have partial knowledge of them. They first have to remove the errors to reconcile their data and then to blot out Eve's information.

Various error-correcting schemes may be used for the reconciliation of the strings [42]. We only have to bear in mind that the public channel can be monitored; therefore care must be taken not to disclose any additional information to Eve. For the laboratory prototype, a slight modification of the error correction proposed in [43] was employed.

For error correction to be efficient, Alice and Bob perform a random, but identical, permutation of bits in their sifted keys to randomize the distribution of errors. Eve does not have to eavesdrop continuously, but only at certain times, which would result in fluctuations of the *BER*. Also, the permutation must be different for each QKD, otherwise Eve could exploit its knowledge to produce such patterns of errors that the error-correcting procedure would perform less well than average. After the permutation, Alice and Bob divide their sifted keys into blocks of such length that the probability of an error occurrence is 1/2 per block. Then they calculate and compare the block parities. If the parities match, the block is for the moment considered errorless. If the parities are different, a bisective search is carried out – the block is split in half and parities of the subblocks are compared. This continues until the error is found. The parity bits increase Eve's information on the key. To keep Eve's information constant, Alice and Bob agree to discard the last bit of each block, whose parity was disclosed. Since some blocks could contain an even number of errors, the resulting strings are again randomized by permutation, and a second round of block parity comparison is performed. The block size in the second round is already larger, because some errors were removed in the first round. Permutations and parity comparisons with increasing block sizes are repeated until Alice and Bob estimate that only a few errors are left. Then block parity comparison becomes inefficient. With a small number of errors, it is more efficient to compare parities of random subsets of half the length of the whole string. When the parities disagree, a bisective search is executed as before. Again, the last bit of each subset is thrown away not to increase Eve's information. A new random subset is generated for each round. Rounds are again repeated until the parities agree. To make sure that no errors were "overlooked", Alice and Bob regarded their data strings as identical after 20 consecutive rounds had yielded matching parities.

Now Alice and Bob had at their disposal a *corrected key* that was errorless with very high probability, but about which Eve could have partial information. It was shown in [42] that provided Eve knows at most l bits of an N-bit string common to Alice and Bob, they can publicly distill a shorter string of length $N-l-t$, where t is an arbitrary security parameter, on which Eve has less than $2^{-t}/\ln 2$ bits of information on average. For example, a secret key can easily be obtained by calculating the parities of random subsets of the corrected key. In contrast to error correction, these parities will now be kept secret and will constitute the final *distilled key*. If Alice and Bob generate $N-l-t$ different, random subsets of length $n > l$, Eve cannot compute the parity bits correctly and her knowledge of the key will be reduced to $2^{-t}/\ln 2$ bits. In our case, $t = 30$ was chosen and random subsets of length $n = N/2$ were generated. Eve could then know at most a singe bit of the distilled key with a probability smaller than 10^{-10}. With this t and typical error rates around 0.3-0.4 %, the error correction and privacy amplification procedures reduced the size of the sifted key to 1/3. More concrete figures will be given in Section 6.5.

It should also be mentioned that if error correction omitted an error and did not remove it, privacy amplification would generate two completely different and

uncorrelated strings, and key distillation would not be successful. Alice and Bob would each end up with a different key. Besides its very small probability, that does not jeopardize the security. A comparison of small parts of the distilled keys can verify their identity. If they are different, Alice and Bob can simply run error correction and privacy amplification again at the expense of more discarded bits. If not enough bits were left, they would have to repeat QKD from the beginning.

5.6 Authentication of the Public Channel

Throughout this work, it has been assumed that the public channel has no privacy. Eve can eavesdrop all the classical communications unnoticed. On the other hand, she is not allowed to anyhow modify, suppress or fabricate the messages. If she could do so, she could easily interrupt both the quantum and public channels, and exchange separate keys with Alice and Bob in order to impersonate Alice to Bob and Bob to Alice. To thwart this threat, the public channel must be authenticated, i.e., the messages must be certified that they are from whom they say they are from and that they have not been altered in transit. Channels with a good level of authentication are, for example, newspapers or the radio. Since Eve is granted unlimited technology allowed by quantum mechanics, we must presume she has technology to manipulate any classical transmissions, however sophisticated.

The most common way to authenticate communications today is to use seals, stamps and hand-written signatures. That, however, does not work for electronic communications. To authenticate an electronic message, the sender uses some secret key (different for each message) to compute a message-dependent tag that can only be reproduced by the intended receiver. The authentication tag is then sent along with the message. The receiver calculates his/her authentication tag from the received message, using his/her key, and checks whether the tags agree. The probability that Eve could extract the key from the sent message-tag pair and generate another valid message-tag pair, can be set to an arbitrarily low level. Authentication thus requires that the sender and receiver share a common secret key initially. On the other hand, part of the key generated by QKD can be used for authentication of future communications. In the strict sense, once we do not have a public channel with perfect authenticity at our disposal, we had better speak about quantum key expansion rather than quantum key distribution. As we will see, the amount of key required to authenticate QKD is fortunately small and there is enough key material left for other cryptographic purposes.

A universal class of hash functions that can generate provably secure authentication tags was presented in [47,48]. The particular authentication method used with the QKD apparatus described in the previous Sections was based on the so-called orthogonal arrays [49]. Orthogonal arrays are combinatorial structures equivalent to mutually orthogonal Latin squares. An orthogonal array OA(n, m, λ), n, m, λ, being

positive integers, is a $\lambda n^2 \times m$ array of n symbols, such that in any two columns of the array every one of the possible n^2 pairs of symbols occurs in exactly λ rows. If such an array generates an authentication code, where n is now the number of all possible authentication tags, m is the number of all possible messages the authentication code can accommodate while maintaining unconditional security, and $\kappa = \lambda n^2$ is the number of all possible keys, it can be proved with the help of the orthogonal arrays theory that

$$\kappa \geq m(n-1)+1 . \tag{45}$$

It follows from Eq. (45) that

$$\kappa > m, \quad \text{if } n \geq 2 . \tag{46}$$

That means that the space of all possible authentication keys must be greater than the space of all messages to be authenticated. However, the length of messages (in bits) communicated over the public channel is always greater than the length of the transmitted raw key. For each qubit, at least one bit of information about the basis chosen by Alice and one bit about the basis chosen by Bob must be interchanged. In addition, only about one half of all successfully received qubits can be used as a key, as follows from the requirement of coincidence of bases. Part of the key also has to be compared and sacrificed by Alice and Bob in order to detect potential eavesdropping. There does not seem to be enough key material to replace the used bits for the next authentication even in the case one does not intend to use the transmitted key (or its part) for any other purpose.

The way out of this impasse is to realize that it is not necessary to authenticate all parts of the public discussion. The most important and characteristic feature of quantum key distribution is that it enables us to detect an eavesdropper. An attempt at eavesdropping inevitably increases the number of errors in the transmitted key. Thus it is necessary to prevent Eve from modifying in any way the part of public discussion connected with the error-rate estimation. All messages containing the sacrificed part of the raw key (including corresponding bases, positions of sacrificed bits, and the total number of detected bits) have to be authenticated. Any modification of the rest of public communication could impair QKD, but would not undermine the security of the system. It should be noted that Eve can disrupt the communication in many other ways: She can cut the optical fiber, she can perform measurements on the quantum states to increase the error rate above the limit, she can jam the classical communication, etc. The value of QKD lies in the fact that if she does not do it, the legitimate users are sure to possess a key about which Eve knows at most a single bit with a very small probability. The legitimate users cannot be deceived into thinking that their key is shared and secret, when actually it is not.

The authentication code was generated in the following way [1,7]. If p is a prime and $d \geq 2$ is an integer, an authentication code can be created for $(p^d - 1)/(p-1)$ messages with p^d keys and p authentication tags. Since every authentication tag is equally likely, the deception probability that Eve would generate a valid tag is $1/p$. For a

given message and a given authentication key, an authentication tag can be calculated as follows: (1) Convert the given authentication key to the number system of base p (its maximum length in this system is d) and denote the i-th "digit" by r_i. (2) Construct and order all nonzero "numbers" in the number system of base p of the maximum length d that have the first nonzero "digit" from the left equal to 1 [there are $\left(p^d - 1\right)/\left(p - 1\right)$ such numbers]. A one-to-one mapping exists between all possible messages and all "numbers" (or sequences) from this set. Assign the corresponding "number" to the message to be authenticated (the ordering of the "numbers" is assumed to be fixed). (3) Denote the i-th "digit" of that particular "number" by c_i. The authentication tag is then given by the formula

$$A\left(r,c\right) = \sum_{i=1}^{d} r_i c_i \mod p\,. \tag{47}$$

In particular, the prime $p = 2^{61} - 1$ and $d = 739$ were chosen. The deception probability was then 5×10^{-19}, the authentication key length was 45 079 bits, the length of messages could be up to 45 017, and the authentication tags consisted of 61 bits. In the case of p in the above form, it was not necessary to carry out the conversion of item (1), and only groups of 61 random bits were generated. In the case that a group of 61 ones was generated, it was discarded, but the probability of its occurrence was extremely small.

An elegant way to reduce the amount of authentication key was proposed by Charles H. Bennett [50]. The idea is to "one-time pad" encrypt the authentication tags themselves. Then we do not need to renew those 45 079 authentication bits for each message, but only a small sequence of the length of the authentication tag itself, i.e., 61 bits in our case.

It should be stressed that the authenticated check on error rate should be performed as the first step of the public discussion, even before the establishment of the sifted key by comparison of bases. Otherwise a malicious Eve could manipulate the non-authenticated public communication for her benefit. She could, e.g., exchange separate sifted keys with Alice and Bob and then choose only those bits, where the choice of bases coincides for all three of them, thus obtaining full knowledge of the key without increasing the error rate. That would, of course, decrease the transmission rate. However, the transmission rate fluctuates owing to natural causes as well, e.g., when the polarization state is deformed on the way to Bob due to a temperature change of the fiber. For this reason, the number of actually detected bits must be authenticated as well.

5.7 Eavesdropping

For the security of QKD, it is crucial to determine as precisely as possible the amount of information that might have leaked to Eve. Its knowledge allows Alice and Bob to choose such security parameter t that privacy amplification will safely obliterate Eve's information on the distilled key. Let us first take a closer look at two simple attacks that Eve could mount, intercept/resend and beam splitting.

5.7.1 Intercept/Resend

As was shown in Section 5.2, when Eve attempts to intercept, measure and resend photons on their way to Bob, she inevitably introduces errors in the transmissions. When she intercepts and resends photons in the rectilinear and diagonal bases, the number of errors amounts to 25 % of bits successfully detected by Bob. If Alice and Bob estimate the error rate $\varepsilon_{\text{est}} \leq \varepsilon_{\text{lim}}$, they know that the actual error rate could be higher than ε_{max} only with a very small probability δ (in our case 10^{-10}). They conclude that Eve could have intercepted/resent at most $4\varepsilon_{\text{max}} N_S$ pulses of the sifted key, where N_S is the number of bits in the sifted key. However, only for approximately half these pulses, Eve set the correct measurement bases. Thus, the maximum number of bits Eve can know is $2\varepsilon_{\text{max}} N_S$. The other half of Eve's bits is completely random and she knows nothing about them.

Eve does not have to eavesdrop in the rectilinear and diagonal bases. It was shown in [43] that if she eavesdrops in the basis halfway between the rectilinear and diagonal bases, she can even learn each bit with a probability 85 %, regardless of the bases used by Alice and Bob. On the other hand, her information is probabilistic, i.e., she knows each bit of the key with an 85 % probability, but she does not know which ones are the correct ones. In contrast to the previous case, her deterministic information in the Shannon sense is even smaller and is safely eradicated by privacy amplification.

Eavesdropping in other bases yields less information and can result in error rates greater than 25 %. Choosing an intercept basis different from the resending basis also increases higher error rates above 25 % without gaining any useful information.

5.7.2 Beam Splitting

As it is very difficult to prepare a good approximation of one-photon states, our QKD apparatus used highly attenuated laser pulses with an average photon number below one photon. If the spectral width of pulses is much smaller than their mean frequency, they can be represented by coherent states. Since coherent states exhibit Poissonian statistics of the photon-number distribution, more than one photon per pulse may appear. Consequently, an eavesdropper can attempt to split the signal state, deviate

part of it and gain some information on the key without disturbing the transmissions in a substantial way. Not disturbing the transmissions in a substantial way means that Eve does not introduce errors (and thus can escape detection), but reduces the mean intensity of pulses.

Let us assume that Eve's detectors have 100 % efficiency, she possesses a "quantum memory" to store the split parts of pulses until the announcement of bases, she can non-destructively measure the numbers of photons in pulses, and she can extract exactly one photon from multi-photon pulses. Let N denote the total number of laser pulses generated by Alice. If we further suppose that Alice transmits coherent states with mean photon number μ, then an average number of bits that an eavesdropper can gain through beam splitting is equal to at most one half of all the pulses containing more than one photon

$$N_E^{(\max)} = \frac{N}{2}\left[1 - e^{-\mu}(1+\mu)\right], \tag{48}$$

where we used Eq. (13) and the factor of 1/2 results from Eve's wrong guessing of her measurement bases. Owing to the losses of the quantum channel and the losses of Bob's part of the interferometer, not all these bits are to become part of the key. Since Eve is capable of learning deterministic information about these bits, her optimum strategy is to maximize Bob's chances of detecting them. In order to do so, she can replace the lossy transmission line connecting Alice and Bob by a lossless one (it is allowed by quantum mechanics) and split off at most one photon from each multi-photon pulse. Eve does not want to split off more than one photon, because she needs to minimize the reduction of the mean intensity at Bob's detectors. When she measures the photon number of a pulse and finds only 1 photon, she cannot beam split, so she performs the above-mentioned intercept/resend attack, or some other type of attack. She can also pass the photon down to Bob or simply block it. If she finds 2 or more photons, she splits off one, stores it and waits for the public announcement of bases. After the announcement, she performs a measurement in the correct basis. In this way, an eavesdropper can obtain deterministic information on those bits of the key, which originated from multi-photon pulses and were later successfully detected by Bob in the correct basis. To split off only one photon, she can, e.g., direct the beam to a beam splitter with a very small reflectance and measure the photon number at its reflecting port. If she finds "zero", she lets it pass again, measuring the photon number after each pass. After some time she extracts, with high probability, just one photon.

Let us now assume that Bob receives states $|n\rangle$ with distribution $\pi(n)$. The photocounting statistics are then given by the Bernoulli transformation

$$p(m) = \sum_{n=m}^{\infty} \binom{n}{m} \eta_{\mathrm{Bob}}^m (1-\eta_{\mathrm{Bob}})^{n-m} \pi(n), \tag{49}$$

where η_{Bob} is the intensity transmittance of Bob's part of the interferometer, including detection efficiency of his detectors. Since Bob's detectors cannot count the number of

impinging photons, and they only distinguish between the presence and absence of the field, the detection probability is given by the sum

$$P = \sum_{m=1}^{\infty} p(m). \tag{50}$$

For the beam-splitting attack, only pulses with an original number of photons $l \geq 2$ are of interest. After Eve has split off one photon, Bob receives states $|l-1\rangle$, and $\pi(n)$ in turn becomes

$$\pi(n) = \begin{cases} 0 & \text{for } n = 0, 1, \\ p_{\text{Poisson}}(n+1) = \dfrac{\mu^{n+1}}{(n+1)!} e^{-\mu} & \text{for } n \geq 2. \end{cases} \tag{51}$$

Now using

$$\sum_{m=1}^{n} \binom{n}{m} \eta_{\text{Bob}}^{m} (1-\eta_{\text{Bob}})^{n-m} = \sum_{m=0}^{n} \binom{n}{m} \eta_{\text{Bob}}^{m} (1-\eta_{\text{Bob}})^{n-m} - (1-\eta_{\text{Bob}})^{n} = 1 - (1-\eta_{\text{Bob}})^{n} \tag{52}$$

and

$$\sum_{n=1}^{\infty} \frac{x^{n+1}}{(n+1)!} = \sum_{k=0}^{\infty} \frac{x^{k}}{k!} - 1 - x = e^{x} - 1 - x\,, \tag{53}$$

we obtain Bob's detection probability [2]

$$\begin{aligned} P &= e^{-\mu} \sum_{m=1}^{\infty} \sum_{n=m}^{\infty} \binom{n}{m} \eta_{\text{Bob}}^{m} (1-\eta_{\text{Bob}})^{n-m} \frac{\mu^{n+1}}{(n+1)!} = \\ &= e^{-\mu} \sum_{n=1}^{\infty} \frac{\mu^{n+1}}{(n+1)!} \sum_{m=1}^{n} \binom{n}{m} \eta_{\text{Bob}}^{m} (1-\eta_{\text{Bob}})^{n-m} = \\ &= 1 - \frac{e^{-\eta_{\text{Bob}}\mu}}{1-\eta_{\text{Bob}}} - e^{-\mu} \left(1 - \frac{1}{1-\eta_{\text{Bob}}} \right). \end{aligned} \tag{54}$$

From this it follows that an average number of key bits Eve can learn through beam splitting is

$$N_E^{(\text{BS})} = \frac{N}{2} P = \frac{N}{2} \left[1 - \frac{e^{-\eta_{\text{Bob}}\mu}}{1-\eta_{\text{Bob}}} - e^{-\mu} \left(1 - \frac{1}{1-\eta_{\text{Bob}}} \right) \right]. \tag{55}$$

The number of bits Eve can learn through individual attacks then must be taken into account to properly set the compression parameter of privacy amplification. Let us recall that the distilled key is generated as $N - l - t$ parity bits of the corrected key, where

$$l = 2\varepsilon_{\max} N_S + N_E^{(\text{BS})} + N_E^{(\text{other})}. \tag{56}$$

The first term is the number of bits Eve can obtain by means of intercept/resend, the second term is the number of bits gained by means of beam splitting, and the third term includes other attacks.

5.7.3 Other Types of Attacks

In addition to general attacks, there are, of course, attacks that are implementation-specific. For instance, it is reasonable to assume that detection efficiency and losses of Bob's part of the interferometer are out of Eve's direct control. However, detection efficiency depends on the wavelength of the used light. An eavesdropper could shift the wavelength of the resent signal in order to increase the number of Bob's detections of the successfully split pulses, while suppressing those she did not manage to split. Therefore, narrow-band filters should be inserted before Bob's detectors.

It is possible to design other attacks along these lines. Each particular setup of a cryptographic apparatus should thus be carefully examined. A detailed analysis of all possible attacks is beyond the scope of this Thesis, as it could produce another feature-length study. To demonstrate the security of QKD under ideal conditions is not difficult, however, to prove the unconditional security of QKD over a noisy and lossy channel with imperfect source states has already been a challenging task. In brief: The case when Eve is not restricted to von Neumann measurements, but she performs POVM measurements before the announcement of bases was investigated by N. Lütkenhaus [51]. The work was later extended to provide the maximum information that can leak to Eve in realistic QKD systems [52]. C. Fuchs *et al*. [46] derived the upper bound on information Eve can gain through measurements after the announcement of bases if she follows an optimal eavesdropping strategy to maximize her information, while minimizing disturbance of the transmissions. All the above papers deal with the so-called *individual attacks*, when the eavesdropper is only allowed to perform separate measurements on individual signals.

Another class of attacks are the so-called *collective attacks* when Eve entangles each signal qubit with an independent probe (ancilla), unentangled to the other probes, and performs a joint (collective) measurement on all the ancillas in a quantum computer after the measurement bases have been announced. Bounds on Eve's information acquired by means of collective attacks were presented in [53]. When all the qubits are entangled to one ancilla or a set of entangled (coherent) ancillas, which are measured in a quantum computer after the announcement of bases, the attack is called *coherent*. A proof of security against any type of attack was provided by D. Mayers [54] under the assumption that single-photon states are used. In [55] H.-K. Lo and H. F. Chau proved the unconditional security of QKD provided that Alice and Bob possess quantum gates to implement quantum error-correcting codes. And eventually, in 2001 H. Inamori, N. Lütkenhaus and D. Mayers extended the former Mayer's proof [54] to incorporate non-perfect sources of quantum states, whereby they provided the ultimate proof of unconditional security of realistic QKD against an adversary with unlimited classical or quantum computational power [56].

5.8 QKD Session

Drawing upon the previous Sections, let us now summarize how a typical QKD session proceeded. Bob typed a message he wanted to send to Alice. Then he let her know through the public channel (the local computer network) that he would like to start quantum key distribution and calibrate the interferometer. Alice's electronic attenuator increased the mean intensity of laser pulses to about 1.6 photons per pulse to minimize the error of intensity measurements and set her phase shifter to zero. Bob scanned the interference fringe, found $I_{\min}$ and $I_{\max}$ (Section 5.3.9) and calculated visibility. If the measured visibility exceeded 97 %, a calibration was performed. Since then the interferometer was recalibrated every 4 seconds to keep track of the relative zero phase difference. Alice decreased the mean intensity below one photon per pulse and started the raw quantum transmission according to the BB84 protocol of Table I. The particular choice of the mean intensity will be further elaborated in Section 6.5. After the transmission, Bob selected a random, 2000 bits long subset of the raw key to test for eavesdropping. Exchanging authenticated messages over the computer network (Section 5.6), Alice and Bob estimated the actual error rate ε. If $\varepsilon_{\text{est}} < \varepsilon_{\text{lim}} = 2.4\ \%$, they concluded that the actual error rate ε could be greater than the maximum tolerable error rate $\varepsilon_{\max} = 7\ \%$ with a probability smaller than $\delta = 10^{-10}$ (Section 5.4). The bases of the remaining raw data were compared to obtain the sifted key, which was subsequently error corrected (Section 5.5). The values $\varepsilon_{\max}$ and the used mean intensity μ were used to estimate the maximum amount of possibly leaked information. Accordingly, the compression parameter l of privacy amplification was set to generate a distilled key of length $N - l - t$ about which Eve could know at most one bit with a probability smaller than $2^{-30}/\ln 2 = 10^{-10}$. The message Bob wanted to communicate to Alice was then Vernam encrypted using the formula (8) and sent to Alice's computer via the public channel. Eventually, Alice recovered the message using the decryption algorithm (9) and confirmed successful decryption. The surplus cryptographic key was saved for authentication of future communications.

5.9 Other Experimental Prototypes and Proposals

The idea to utilize the uncertainty principle for quantum coding comes from S. Wiesner, who wanted to make money that cannot be counterfeited (41). Since it is not easy to keep quantum states free from decoherence for extended periods of time (even for very short times at present), this concept is not very practical. In the same paper, Wiesner proposed a quantum multiplexing channel, which allows to transmit two messages, either but not both of which may be read by the receiver. The principle was later coined oblivious transfer by M.O. Rabin [57] and can be used for various cryptographic applications, such as coin tossing. Coin tossing would allow two,

mutually distrustful users to flip a coin at a distance with a guarantee that neither user can bias the probability of obtaining heads or tails. Classical oblivious transfer and coin tossing again rely on computational security. Quantum coin tossing based on quantum bit commitment was proposed by C.H. Bennett and G. Brassard in their BB84 paper [40]. Quantum bit commitment allows Alice to give some information to Bob, who cannot read it unless she gives him the key. However, once Alice commits herself to some information, she can in no way change her mind and fabricate such a key that would later allow her to modify the information and thereby deceive Bob. A proposal of a quantum bit commitment protocol over noisy channels was published in [58]. Wiesner's quantum oblivious transfer was also combined with public-key cryptography to provide unforgeable subway tokens [59]. Unfortunately, both quantum oblivious transfer and quantum coin tossing can be foiled if one of the users has a source of EPR-entangled photons at their disposal. In 1996, [60-63] proved that unconditionally secure quantum bit commitment and oblivious transfer are impossible in principle. Quantum key distribution remained the only unconditionally secure application of quantum cryptography at that time.

The first QKD experiment took place in 1989 [64,43]. A LED generated light pulses that were subsequently attenuated by an interference filter and polarized by a polarizer (see Fig. 20). The qubits were encoded in the polarization of photons by means of Pockels cells. The quantum channel was 32 cm of free air. Bob analyzed the polarization states using a Wollaston prism, which was preceded by another Pockels cell to choose his polarization basis. The output ports of the prism were monitored by photomultipliers.

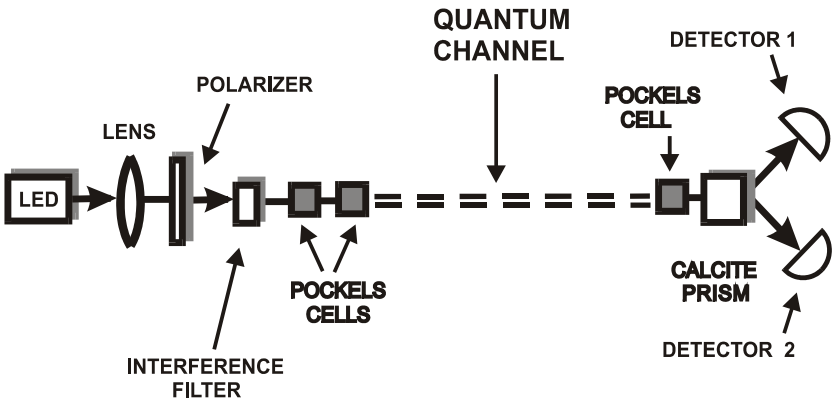

Fig. 20 First QKD experiment. Protocol BB84 and polarization encoding were used.

Four years later, N. Gisin's group of the University of Geneva replaced the free-air optical path by a 1-km optical fiber [65,66]. A semiconductor laser at 800 nm was used to generate light pulses that were detected by silicon avalanche photodiodes. To

compensate for temporal changes of polarization in the fiber, a manually adjustable polarization controller was employed. To this end, J.D. Franson built a QKD device with polarization-maintaining fibers [67]. In the same paper, an active polarization-alignment feedback loop was proposed to eliminate the need for PM fibers and such a system was demonstrated to work over a distance of 1 km [68]. The first experiment when Alice and Bob were placed in different laboratories (in this case even different towns of Geneva and Nyon) was performed by the Geneva group [69,70]. Error rates of only 3-4 % were achieved between two stations, connected by a 23-km fiber deployed under Lake Geneva. In order to reduce fiber losses, a laser at 1.3 μm was used and the photons were detected by liquid-nitrogen-cooled germanium avalanche photodiodes.

Because of the problems with polarization, some researchers turned to phase encoding in interferometers. In 1993, P.D. Townsend, J.G. Rarity and P.R. Tapster realized quantum key exchange at 1.3 μm over 10 km of fiber in a time-multiplexing Mach-Zehnder interferometer [71]. Visibility of 91 % was achieved with this setup. Then, polarization multiplexing was added [72-74]. Alice rotated the polarization of light pulses in her long arm by 90 degrees and Bob replaced his first fiber coupler (C_3 in Fig. 5) with a polarizing beam splitter. The polarizing beam splitter was oriented so as to direct the photons taking Alices's short arm into his long arm and vice versa, thereby removing the side peaks of Fig. 4. This configuration released the stringent requirements on detection time resolution and in addition to doubling the data rate, it enhanced visibility to 98 %. In the following experiments, the public channel was wavelength-multiplexed onto the quantum channel [75] and a 30-km coil of fiber was inserted between Alice and Bob [76]. A similar experiment was recently built at the Norwegian University of Science and Technology [77].

Even though information is encoded in phase differences, it is still necessary to actively adjust polarization due to its temporal changes arising from various thermal and mechanical causes. A beautiful idea of how to avoid the need for polarization alignment was presented in [78,79]. Bob generates bright light pulses, which take either of two possible paths of his unbalanced interferometer with mutually orthogonal polarizations, whereupon they are launched into a fiber leading to Alice. Once the pulses reach Alice, she attenuates them to a quantum level, reflects them using a Faraday mirror, applies her phase shift and sends them back to Bob, who in turn applies his phase shift. Since the Faraday mirror transforms the input polarization into its orthogonal state, each pulse travels one way with one polarization and the other way with an orthogonal polarization, only in different order depending on which 'path' the pulse took. Provided the polarization deformation induced by the fiber does not change within the time the pulse needs to go back and forth, the pulse polarization is automatically aligned upon reaching Bob's interferometer. As the interferometer does not require active stabilization, it is referred to as a 'plug-and-play' setup. This system has also its drawbacks. Since the pulses must go back and forth, Bob transmits pulses of classical intensity to avoid excessive reduction of the transmission rate. This does not undermine the security because the first encoding is done by Alice who attenuates the pulses to a

safe level before reflecting them back to Bob. Pulses contain no information on the way to Alice yet. On the other hand, the classical intensity of light pulses gives rise to Rayleigh scattering in the fiber, which is detected by single-photon detectors as noise. The problems were overcome in an improved setup with the help of a photon "storage line" that "stores" the light pulses until the scattering dissipates [80,81]. However, the storage line, which is an optical fiber as long as half the distance between Alice and Bob, introduces additional losses and thereby reduces the secure communication distance. Nevertheless, the achieved raw-key transmission rate over a distance of 23 km was 486 bits per second with an error rate of 5.4 %. Similar experiments were later performed at the Royal Institute of Technology in Stockholm at 1.55 μm [82,83] and at the IBM Almaden Research Center in San Jose [84]. The plug-and-play configuration is also more subject to the so-called Trojan horse attacks. Eve can try to find out Alice's phase-shift setting by sending a probing classical pulse into her interferometer, where it is reflected by the Faraday mirror. For this reason, Alice must monitor the intensity of incoming pulses.

Despite their drawbacks, the self-compensating systems with phase encoding seem to be most promising for any practical use of QKD in the near future. On the other hand, using optical fiber is not the only way to implement QKD at a distance. Another approach is to try to communicate directly through free space. Unlike fibers, the atmosphere is non-birefringent, thereby polarization encoding comes into play again. The feasibility of free-space QKD was shown by B.C. Jacobs and J.D. Franson [85], who managed to communicate over 150 m in a fluorescent-tube-illuminated corridor and over 75 m outdoors in daylight. It was the first free-space implementation of QKD after the celebrated 1989 Bennett and Brassard experiment and there were more to come. The Los Alamos group first exchanged keys at 1 km by night bouncing the photons between mirrors [86,87], then point-to-point communication over 0.5 km in daylight was performed [88] and eventually over 1.6 km in daylight [89]. 1.9 km at night were covered by P.M. Gorman, P.R. Tapster, and J.G. Rarity [90]. Free-space QKD over the largest distance so far was performed by the Munchen group of H. Weinfurter [91]. Unlike the other groups, they moved to the high altitudes of the Alps to take advantage of thinner air and less air turbulence. Alice was located on the summit of Zugspitze (2950m) and Bob was on a 23.4 km distant Karwendelspitze (2244m). These achievements clearly illustrate that ground-to-satellite and satellite-to-satellite QKD need not be in too distant a future.

In 1992, C.H. Bennett showed that two nonorthogonal states are already sufficient to implement secure QKD [92]. Let Alice choose two nonorthogonal states and send them to Bob in random order. When Bob performs random projections onto subspaces orthogonal to the signal states, he sometimes learns Alice's bit with certainty and sometimes he obtains an inconclusive outcome. After the transmission, Bob tells Alice when he detected a bit. In this case, he does not announce the used basis, because a basis in which he detected a photon, uniquely identifies the bit Alice had sent. However, such a scheme is secure only in lossless systems. With a lossy system, an

eavesdropper could sit in the middle and make measurements on the quantum states. If she has obtained an inconclusive result, she blocks the signal, while if she has detected a photon, she resends a correct copy to Bob, because she knows its state with certainty. To compensate for the blocked photons, she sends a pulse of higher intensity so that Bob would not observe any decrease in the expected transmission rate. One of possibilities of how to counter this attack is to encode bits into a phase difference between the quantum state and a classical reference pulse. When Eve gets an inconclusive result, she cannot suppress the classical pulse, because Bob must receive all of them. However, when she fabricates one, it does not interfere properly and results in a detectable error. Even though this so-called B92 protocol can be unconditionally secure if properly implemented, Fuchs *et al*. showed [46] that Eve can acquire more information on the key for a given disturbance compared to BB84.

Encoding qubits into the phase difference in a fiber-based Mach-Zehnder interferometer, R.J. Hughes *et al*. implemented B92 over a short distance [93], which was extended to 14 km [94,95] and in 1996 even up to 48 km [96]. Alice and Bob were still placed in the same room, while the connecting fiber was going out in the field and back. However, their setup omitted the classical reference pulse and therefore was not secure. Furthermore, too high intensities of laser pulses were used for given attenuation of their fibers.

In 1991, A.K. Ekert proposed a different QKD protocol based on EPR correlations and Bell's inequality [97]. A source generates pairs of spin-½ particles in the state

$$\phi^{+} = \frac{\sqrt{2}}{2}\left(\left|\uparrow\right\rangle_A\left|\uparrow\right\rangle_B + \left|\downarrow\right\rangle_A\left|\downarrow\right\rangle_B\right), \tag{57}$$

where Alice and Bob each obtain one particle from the pair (see Fig. 21). Here $\left|\uparrow\right\rangle$ and $\left|\downarrow\right\rangle$ denote a spin-up and spin-down particle, resp. Regardless of whether the qubits are encoded in polarization-, phase- or spin-entanglement, Alice and Bob perform measurements on their respective particles in three bases defined by three directions on the Poincaré sphere: Alice's bases make angles with respect to the vertical $0, \pi/4, \pi/2$, and Bob's bases are in the same plane making $\pi/4, \pi/2, -\pi/4$. There are nine possible combinations. After the quantum transmission, when Alice and Bob randomly and independently set their measurement bases, the settings are publicly announced. When identical bases were used, the outcomes of their measurements are correlated and become the cryptographic key. The probability that Alice and Bob use the same basis is 2/9. The outcomes of measurements in the other bases are used to verify the violation of the CHSH inequality (how the violation of the CHSH inequality can be measured is described in the quantum secret sharing part of the Thesis, Section 7.7). An eavesdropper attempting to correlate his probe with the other two particles would disturb the purity of the singlet state, which would result in a smaller violation of the inequality or no violation at all. The first QKD experiment of this type was performed by Ekert *et al*. a year later [98], when one of the beams propagated down a 170-m

multimode fiber. However, the achieved visibility was low, about 15 %. Using a single-mode fiber increased visibility to 93 % [99]. Shortly afterwards, Alice and Bob were separated by a 4.3-km fiber [100]. The down-conversion source generated nondegenerate photon pairs at 820 nm and 1300 nm; the former were detected locally by high-efficiency silicon detectors, the latter were coupled into the fiber and detected by germanium detectors. A theoretical analysis of the interferometric implementation of an entanglement-based cryptosystem is given in [101]. In 2000, Ekert's protocol was realized with polarization-entangled photons by a group in Los Alamos [102]. A modified experiment, also with polarization-entangled photons, was conducted in Innsbruck [103], where three measurement bases were replaced with two [104] and Wigner's inequality was used instead of CHSH. The BB84 protocol was run with the same setup as well. In contrast to the Los Alamos group, where Alice and Bob shared one optical table, the photon pairs were coupled into two 500 m long fibers bringing them to Alice and Bob, who were spatially separated by 360 m.

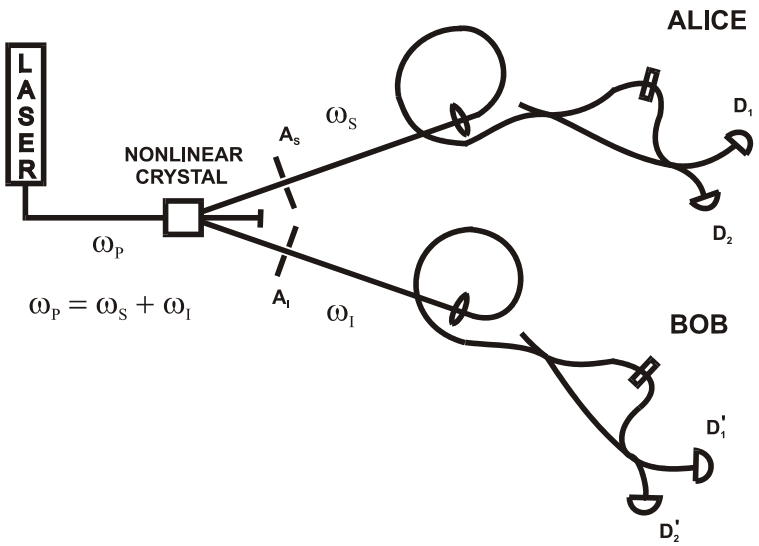

Fig. 21 Quantum key distribution with entangled photon pairs generated in a nonlinear crystal.

In 1998, the Geneva group repeated the 1992 Ekert experiment with energy-time entangled photons at a different level [105]. The down-conversion source produced photons at 1310 nm that were launched into a 9.3-km and 8.1-km fibers leading to terminals about 11 km apart. The achieved visibilities were about 85 %. Two years later, the experiment was optimized in the sense that the down-conversion source produced nondegenerate pairs at 810 nm and 1550 nm. 810-nm photons were detected by Alice at a local station by high-quantum-efficiency silicon detectors and 1550-nm photons were sent down a 8.5-km coil of fiber to Bob [106]. A visibility of 92 % was

achieved. In [107], a pulsed source of energy-time entangled photon pairs was proposed that reduces the requirements on the laser coherent length. An unbalanced Mach-Zehnder interferometer identical to Alice's and Bob's interferometers of Fig. 21 is inserted before the nonlinear crystal. It splits the pump pulse into two successive pulses with a fixed phase delay. Interference again arises from indistinguishable paths the photons can take. A QKD experiment based on this setup was demonstrated in [108]. The same configuration with energy-time Bell states was also used to implement quantum secret sharing [109,110]. By contrast, the quantum secret sharing experiment performed within this PhD Thesis employed polarization-entangled states (see Chapter 7).

In general, entanglement-based QKD systems seem to be superior to weak-coherent-pulse systems, because their security can be further enhanced using the so-called quantum privacy amplification or entanglement purification techniques provided quantum gates have been constructed [111-114]. On the other hand, quantum entanglement is subtler in comparison with weak-coherent-state schemes that are more robust to decoherence.

There are many other proposals of QKD systems and this review is far from being exhaustive. In the six-state protocol [115], three nonorthogonal bases are used to increase the error rate caused by eavesdropping. Consequently, smaller transmission rates can be achieved, because the probability that Alice's and Bob's bases differ is 2/3. L. Goldenberg and L. Vaidman [116-118] proposed a protocol using orthogonal states. A superposition of quantum states is divided into parts, which are sent separately with a time delay larger than the time distance between Alice and Bob. P.C. Sun, Y. Mazurenko and Y. Fainman built a long distance interferometer based on frequency division [119]. In [120,121], QKD systems on multi-user optical networks were presented, when Alice exchanges cryptographic keys with several Bobs. In order to overcome the limited communication distance of QKD, so-called quantum repeaters were proposed [122,114] that enable to create entangled particles over arbitrary large distances with the help of entanglement swapping and purification. A new, impetuously developing field is quantum key distribution with continuous variables [123-127]. A QKD system based on quantum correlations between amplitude and phase quadratures of squeezed light is being built by G. Leuchs' group in Erlangen.

Chapter 6
Quantum Identification System

6.1 Introduction

Identification is one of the fundamental cryptographic tasks. Its goal is to verify the identity of another person. It must be designed in such a way that Bob can securely identify himself to Alice, but an eavesdropper listening in to his identification cannot impersonate Bob to anybody else later on. Furthermore, it must also prevent Alice from being able to pose as Bob.

Today identification applications are numerous and sometimes overlap with QKD or secret sharing. Quantum identification can be used to restrict access to nuclear power stations, nuclear weapon sites, national bullion depositories, and other areas, where a high level of security is required. It can be employed for communications between government agencies, diplomatic services, military and security forces, revenue authorities, etc. Financial institutions could use it for clearing houses, interbank payments, for money withdrawal from automated-teller machines, and so on.

It is not an easy task to build an identification system that satisfies the above conditions and simultaneously offers unconditional security. The present systems are either computationally secure or they suffer from the key distribution problem by analogy to QKD systems. A quantum identification system was first proposed by C. Crépeau and L. Salvail in [128]. Their identification protocol is based on quantum oblivious transfer [129,130]. Alice and Bob mutually check their knowledge of a common secret string without disclosing it. However, quantum oblivious transfer has been proved insecure against collective attacks by D. Mayers [60,61], and H.-K. Lo and H.F. Chau [62,63].

The quantum identification system proposed here elegantly finds a solution in combining a classical three-pass identification procedure and QKD. Each identification sentence (IS) is used only once by analogy to the Vernam cipher, and new sequences are “refueled” from a shared provably secret key distributed by means of QKD. Moreover, it will be shown that the identification procedure can expediently be incorporated in the authenticated part of the QKD protocol described in Chapter 5.

6.2 Identification with an Unjammable Public Channel

Let us suppose that Alice and Bob have an unjammable public channel at their disposal. Even though Eve can monitor all the communications, she is not capable to alter, suppress, or fabricate any of the messages. Let us further suppose that Alice and Bob share some information initially. This information is divided into several identification sequences that are grouped together in triads. The protocol then goes as follows:

(1) Alice and Bob say to each other their ordinal numbers of the IS triad – a pointer to the first Alice's (Bob's) unused sequence – and choose the higher one if they differ.

(2a) Alice sends the first IS of the triad to Bob.

(2b) Bob checks whether it agrees with his copy. If not, Bob aborts communication and shifts his pointer to the next triad. Otherwise, he sends the second IS of the triad to Alice.

(2c) Alice compares whether her and Bob's second ISs agree. If not, she aborts communication and shifts her pointer. Otherwise, she sends the third IS to Bob. If Bob finds it correct, the identification has succeeded.

(3) In order to replace the used ISs, Alice and Bob refuel new ISs by means of QKD and set their pointers to their initial positions.

Three passes are necessary for the following reason: An eavesdropper can pretend to be Bob and get the first IS from Alice. Of course, Alice recognizes that Eve is not Bob, because Eve cannot send the correct second IS. Alice aborts communication, discards her triad and shifts her pointer to the next one. However, Eve can now turn to Bob, masquerading as Alice, because she knows the first IS. Bob can only recognize a dishonest Eve because she does not know the third IS.

Let us note that in this case there is no need to perform error correction and privacy amplification after QKD. The agreement between two compared ISs need not be perfect, no matter whether the errors arise from eavesdropping or noise. If the ISs are sufficiently long, Eve has a very small probability to succeed in the identification procedure. In particular, for error rates below a certain level, the deception probability that Eve successfully deceives Alice (Bob) into thinking that she is Bob (Alice) is upper bounded and can be made arbitrarily small by prolonging the ISs.

Let Alice and Bob agree to tolerate at most $k = \lceil \varepsilon N \rceil$ in an identification sequence of length N, where ε is the QKD error rate and $\lceil x \rceil$ denotes the smallest integer greater than x. Further, let p_i denote the probability that Eve correctly guesses the i-th bit of the IS. Then if Eve's measurements are independent, the deception probability can be expressed in the form

$$P(N,\varepsilon) = \sum_{l=0}^{k} \sum_{\{i_1 \ldots i_l\}} \left(\prod_{j=1}^{N} p_j \right) \left(\prod_{m=1}^{l} \frac{q_{i_m}}{p_{i_m}} \right), \tag{58}$$

where $q_i = (1 - p_i)$ and the second sum goes over all l-tuples of numbers from 1 to N (for $l = 0$ there is only $\prod_j p_j$).

Using Jensen's inequality [131], we find

$$\prod_{j=1}^{N} p_j \le \left(\overline{p}\right)^N , \tag{59}$$

where $\overline{p}$ is the average probability that Eve guesses an IS bit correctly

$$\overline{p} = \frac{1}{N}\sum_{j=1}^{N} p_j . \tag{60}$$

From Eqs. (58) and (59), we obtain an upper bound to deception probability

$$P(N,\varepsilon) \le \left(\overline{p}\right)^N 2^k \binom{N}{k}. \tag{61}$$

It can be shown [1] that there exist a limiting probability p_{lim} such that for all $\overline{p} < p_{\text{lim}}$, the deception probability approaches zero with an increasing size of the IS

$$\lim_{N\to\infty} P(N,\varepsilon) = 0 . \tag{62}$$

For example, for ISs of length $N = 50$ bits and error rate ε = 1 %, an average Eve's guess is $\overline{p} \cong 0.6$ [46] to give deception probability $P(N,\varepsilon) \le 8\times 10^{-10}$.

It should also be noted that it is not necessary to verify triads of identification sequences. It is sufficient to verify only one identification sequence, which Alice and Bob send bit by bit in an alternate manner. Communication is aborted when an admissible number of errors have been exceeded. In that case, however, the derivation of deception probability is more complicated.

6.3 Identification with Authenticated Public Discussion

In practice, there is no truly unjammable channel; it is necessary to authenticate the public discussion. On the other hand, this authenticated discussion can be expediently employed to serve as the three-pass identification described in the previous Section. In contrast with the ideal case of an unjammable public channel, error correction now must be carried out, because different authentication keys would produce different authentication tags. It is advisable to carry out privacy amplification as well to make the evaluation of Eve's deception probability transparent.

Provided Alice and Bob initially share a pool of secret information, the identification procedure proceeds as follows:

(1) Alice and Bob perform quantum distribution according to the protocol of Section 5.2.

(2) Alice and Bob say to each other their addresses in the pool of shared secret information and undertake a three-pass authenticated public discussion that serves for the estimation of the error rate and mutual identification:

(a) Bob sends Alice an authenticated message (Section 5.6) containing the positions of bits, randomly selected for the error-rate estimation.

(b) Alice checks whether her authentication tag agrees with Bob's, and aborts communication if not. Otherwise she sends back to Bob an authenticated message containing the bases and bit values of the selected qubits.

(c) Bob checks authentication and aborts communication if it fails. If passed, he compares bases of the selected subset and retains only those bits where his and Alice's bases coincide. He estimates the error rate (Section 5.4) and sends to Alice an authenticated message with the value of the estimate. Alice checks authentication and aborts communication if it fails.

(3) If the error rate estimate is lower than a maximum tolerable error ε_{lim}, Alice and Bob compare bases of the rest of their raw data and arrive at their sifted keys. If $\varepsilon_{\text{est}} > \varepsilon_{\text{lim}}$, they suspect Eve of listening in and cannot safely generate new shared secret sequences.

(4) Error correction and privacy amplification procedures are performed to establish an error-free distilled key (Section 5.5). The security of privacy amplification is based on $\varepsilon_{\max}$ and the used intensity μ.

(5) Alice and Bob refuel their shared secret information. The used authentication/identification sequences are discarded. The length of the raw transmission must be chosen such that the length of the obtained distilled key is greater than the number of bits consumed for authentication/identification purposes. It is convenient if it covers several unsuccessful identification acts. The optimization of the length of the transmission and of the mean intensity μ will be described in Section 6.5.

6.4 Necessary Condition for Secure Communication

The amount of information that can potentially leak to Eve sets limits to a practical implementation of secure quantum identification or QKD. In Section 5.7.2 we derived the average number of bits Eve can learn through beam splitting [Eq. (55)]. If an eavesdropper replaces the lossy line by a lossless one and blocks all pulses where she has found only one photon, Bob does not even have to notice any decrease of the data rate. Since actual numbers of detected pulses fluctuate, a small decrease of data rate is hardly detectable. If losses on the line exceed a certain limit, Eve could even learn all the bits of the key without introducing any errors. Communication can thus be secure only if the number of key bits Bob has received is greater than the number of key bits Eve could overhear. If we limit ourselves to individual attacks, the maximum information Eve can gain using an optimal eavesdropping strategy is $N_E^{(\text{opt})} = 2\varepsilon_{\max} N_S / \ln 2$ [46], which already includes the $2\varepsilon_{\max} N_S$ intercepted/resent bits of Section 5.7.1, where N_S is the length of the sifted key. It follows that

$$N_S > N_E^{(\text{opt})} + N_E^{(\text{BS})}. \tag{63}$$

If η_L denotes the intensity transmittance of the transmission line, Eq. (17) implies that the mean number of bits Bob expects after the comparison of bases is

$$N_S = \frac{N}{2}\left(1 - e^{-\eta_L \eta_{\mathrm{Bob}} \mu}\right). \tag{64}$$

If we substitute for $N_E^{(\mathrm{opt})}$, $N_E^{(\mathrm{BS})}$, and N_S, Eq. (63) yields

$$1 \geq \eta_L > \frac{1}{\eta_{\mathrm{Bob}} \mu} \ln\left[\frac{(1-\eta_{\mathrm{Bob}})(\ln 2 - 2\varepsilon_{\max})}{\ln 2\left(e^{-\eta_{\mathrm{Bob}}\mu} - \eta_{\mathrm{Bob}} e^{-\mu}\right) - 2\varepsilon_{\max}(1-\eta_{\mathrm{Bob}})}\right]. \tag{65}$$

Decreasing Bob's losses (increasing η_{Bob}) enables us to establish secure communication with a lossier quantum channel (lower η_L). However, η_L has a lower bound for $\eta_{\mathrm{Bob}} \to 1$

$$\begin{aligned} \eta_L^{(\min)} &= \lim_{\eta_{\mathrm{Bob}} \to 1} \left\{ \frac{1}{\eta_{\mathrm{Bob}} \mu} \ln\left[\frac{(1-\eta_{\mathrm{Bob}})(\ln 2 - 2\varepsilon_{\max})}{\ln 2\left(e^{-\eta_{\mathrm{Bob}}\mu} - \eta_{\mathrm{Bob}} e^{-\mu}\right) - 2\varepsilon_{\max}(1-\eta_{\mathrm{Bob}})}\right] \right\} \\ &= 1 + \frac{1}{\mu} \ln\left[\frac{\ln 2 - 2\varepsilon_{\max}}{\ln 2(\mu+1) - 2\varepsilon_{\max} e^{\mu}}\right]. \end{aligned} \tag{66}$$

For quantum channels with transmittance below this limit, $\eta_L < \eta_L^{(\min)}$, it is not possible to guarantee secure communication in principle. Hence, losses and imperfect detectors limit the distance over which secure communication is feasible.

In practice, transmittances η_L and η_{Bob} are given by the attenuation of the fiber connecting Alice and Bob, by the characteristics of Bob's detectors and by the particular implementation of his part of the interferometer. The condition (65) then determines the upper limit imposed on the mean number μ of photons per pulse, Alice and Bob can use to enable unconditional security of their communications. With the experimental setup described in the preceding Chapter, the transmittance of the 0.5-km fiber was $\eta_L = 0.63$, the transmittance of Bob's interferometer $\eta_{\mathrm{B}} = 0.35$ and the quantum efficiency of Bob's detectors $\eta_{\mathrm{Det}} = 0.55$. Inequality (65) was then satisfied for any $\mu < 1.65$, where $\eta_{\mathrm{Bob}} = \eta_{\mathrm{B}} \eta_{\mathrm{Det}}$.

6.5 Optimization

Since the condition (65) sets an upper limit to the mean intensity, it is natural to ask what mean photon number will maximize the yield of the distilled secret key, while using a minimum number of laser pulses.

After the quantum transmission, Alice and Bob generate a sifted key of an average length given by Eq. (64), where the total transmittance of the apparatus $\eta = \eta_L \eta_{\mathrm{B}} \eta_{\mathrm{Det}} = 0.12$. The subsequent error correction reduces the sifted key to $N_C = f(\varepsilon) N_S$ bits of the *corrected key*, where $0 \leq f(\varepsilon) \leq 1$ is some function of the error rate, dependent on the particular error-correction procedure. With the error

correction of Section 5.5, this function was empirically found to be approximately

$$f(\varepsilon) = 1 - 2.7\varepsilon^{2/3}. \tag{67}$$

Error rates around 0.3-0.4 % thus shortened the sifted key by about 6-7 %. The security parameter of privacy amplification was $t = 30$ so that Eve could know at most one bit of the distilled key with a probability smaller than 10^{-10}, which resulted in a further reduction to

$$N_D = N_C - \frac{\eta_{\mathrm{Bob}}\mu^2}{4}N - \frac{2\varepsilon_{\max}}{\ln 2}N_s - 5\sqrt{N\frac{\eta_{\mathrm{Bob}}\mu^2}{8}\left(1-\frac{\eta_{\mathrm{Bob}}\mu^2}{8}\right)+\frac{2(\ln 2+1)N_S\varepsilon_{\max}}{\ln^2 2}} + \frac{\ln(\delta \ln 2)}{\ln 2} \tag{68}$$

bits of the distilled key. Here, the second term on the right-hand side is the second-order expansion of Eq. (55), expressing the number of bits Eve can learn by beam splitting with the capability of replacement of the lossy communication line by a line of $\eta_L = 1$. The third term contains the number of bits Eve can obtain by optimal eavesdropping according to [46]. The fourth term is a five-standard-deviations safeguard for sampling errors, whose derivation is analogous to that in [43]. The left term under the square root is the variance in the number of split pulses at fixed μ; the right term is the variance in the number of bits Eve can get by virtue of a probe interaction attack on individual photons. The last term is a privacy amplification compression that decreases Eve's information to δ bits.

Now that Alice and Bob share a secret distilled key, they have to allocate its part for new authentication/identification sequences. Since $2s$ = 2000 bits are used to estimate the error rate, they need (i) $2s\lceil \log_2 N \rceil + a$ bits to convey and authenticate positions of selected bits, (ii) $4s + a$ bits to convey authenticated bases and bit values of the selected bits, and (iii) say, $32 + a$ bits to convey the final message whether everything is OK or not. Here $[x]$ denotes the smallest integer greater than x, and $a \geq \lceil \log_2(1/\delta) \rceil$ is the length of the authentication tag. In particular, $a = 61$ was used (see Section 5.6). Altogether it means that

$$b_{\min} = 2s(\lceil \log_2 N \rceil + 2) + 32 + 3a \tag{69}$$

bits must be allocated for the next identification session. Obviously, they have to share the same number of bits initially before the first identification, e.g., stored in a smart card.

From the above it follows that there is a lower bound to the number of pulses N required to distill a key sufficiently long so as to cover all auxiliary procedures and refill new secret information. Once the ratio

$$r = N_D / b_{\min} > 1, \tag{70}$$

the apparatus can serve as an "expander" of secret information with unconditional security. If Eq. (70) is now optimized with respect to μ to maximize gain N_D / N, we find an optimum average intensity $\mu \approx 0.6$ photons per pulse (see Fig. 22). This value

represents a trade-off between the number of pulses successfully detected by Bob and the reduction of key length by privacy amplification. The minimum number of laser pulses N sensitively depends on the overall losses, so graphs for three values of the communications line attenuation are plotted. On the other hand, the ratio N_D / N depends on δ only weakly so that it is easy to achieve an arbitrary security level. For our system, $r = 1$ for approximately $N = 4.3 \times 10^6$ laser pulses.

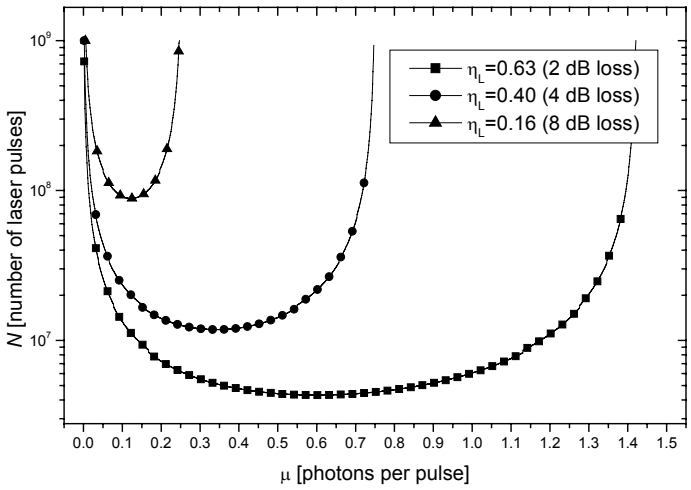

Fig. 22 The dependence of the number of laser pulses N required to generate as much distilled key [Eq. (68)] as it is consumed for authentication during identification [Eq. (69)] on intensity μ of laser pulses at the output of Alice's interferometer for three different values of transmittance of the communications line η_L. The higher the losses of the transmission line (or its length), the lower must be the intensity of Alice's pulses and the greater is the number of laser pulses needed to generate enough distilled key. We can see that in our case ($\eta_L = 0.63$) the optimum mean intensity is about 0.6 photons per pulse.

A typical identification procedure proceeded as follows. Alice's laser generated sequences of 320 000 laser pulses at a repetition rate of 100 kHz. After each sequence, the interferometer was calibrated. During the calibration, the electronic attenuator increased the mean intensity to about 1.6 photons per pulse to minimize the error of intensity measurement. An average raw-key data rate was about 4.3 kbits per second, including the calibration. Once Bob detected approximately 700×10^3 photons, three-pass authenticated public discussion was carried out over the local computer network. If all three authentications were found correct, Alice and Bob have mutually identified themselves. If $\varepsilon_{\text{est}} < \varepsilon_{\text{lim}}$, they could safely refuel new secret material. They compared the bases of the remaining raw-key data, arriving at ~ 350 kbits of sifted key, which was further shortened by error correction and privacy amplification to about 114 kbits of

distilled key. This well covered approximately 52 kbits of previously shared secret key consumed during the authenticated discussion (thus $r \approx 2$). The whole identification procedure took about 3 minutes, including the auxiliary processes, resulting in a net average rate of distilled-key generation ~ 650 bits per second. It would still be possible to speed up the generation rate, however, the bottleneck was Alice's and Bob's computers (single chips would do better than PCs) and the bandwidth of the processing electronics.

Chapter 7
Quantum Secret Sharing

7.1 Introduction

The third experiment performed during my PhD study was quantum secret sharing [4]. A secret is split into pieces, called *shares,* in such a way that certain subsets of shares can recover the secret when put together. Secret sharing schemes, also called threshold schemes, were proposed independently by G.R. Blakley [132] and A. Shamir [133]. In the (*m,n*)-threshold scheme (read '*m*-out-of-*n*' threshold scheme), a cryptographic key conveying secret information is divided into *n* shares which are distributed to *n* participants; each participant obtains one. Then if and only if a certain minimal number of shares *m* ($1 \le m \le n$) are pieced together, the original secret key can be recovered. If any subset of the participants $s \le m-1$ pool together their shares, they are not able to reveal the key.

Secret sharing can be used, e.g., to condition access to a bank vault. If (2,3)-threshold scheme is used, it will require at least two out of the three bank vice presidents to act in concert in order to be able to open the vault. No single vice president will be able to do so. The same principle can be applied to access restriction in similar areas as quantum identification. Secret sharing can also be employed to protect industrial secrets. It is useful when an only cryptographic key providing access to sensitive information is lost, because, e.g., the person who possesses the key becomes unavailable or the computer storing the key is damaged. Except these classical applications of secret sharing, quantum secret sharing can prove very helpful to implementations of quantum error-correcting codes and to the construction of quantum computers. It can be used to render quantum storage and quantum computation more resistant to failure of a component or a group of components due to defects and decoherence, or due to sabotage by malicious parties. And of course, quantum secret sharing can be employed for military and diplomatic purposes.

A theoretical proposal of how to implement secret sharing in a quantum way was set forth by Mark Hillery and his co-workers in 1999 [134,135]. Their quantum (2,3)-threshold scheme utilizes three-particle entanglement of Greenberger-Horne-Zeilinger states (GHZ states) [136-139]. Each of the three participants obtains one particle from the GHZ state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) \tag{71}$$

and, by analogy with quantum key distribution, makes a measurement in one of two mutually nonorthogonal bases. Details of the protocol can be found in the above-cited papers. GHZ states have not, however, been neatly produced in the laboratory yet.

Anders Karlsson and his collaborators proposed a modification of Hillery *et al.*'s scheme, which is based on two-particle quantum entanglement [140]. Two-particle entanglement is already within the reach of today's technologies.

The first implementation of quantum secret sharing was done by Wolfgang Tittel *et al.* [109,110]. Their experiment uses "pseudo-GHZ states" based on energy-time entanglement of photons, as described in Section 5.9; the "pseudo" arising from the fact that the three photons do not exist at the same time. In contrast, my implementation of quantum secret sharing was based on polarization-entangled photon pairs generated by spontaneous nonlinear type-II down conversion.

7.2 Quantum Entanglement

Let us consider two systems, which mutually interacted in the past. Some time after the interaction they are spatially separated and there is no interaction between them any longer. Suppose their states before the interaction are known. In their EPR paper [141], Albert Einstein, Boris Podolsky and Nathan Rosen show that "… by measuring either A [the momentum of the first particle] or B [the coordinate of the first particle] we are in a position to predict with certainty, and without in any way disturbing the second system, either the value of the quantity P [the momentum of the second particle] or the value of the quantity Q [the coordinate of the second particle]". This conclusion can be drawn only on the assumption of locality that "… the process of measurement carried out on the first system … does not disturb the second system in any way". Surprisingly, in reality a measurement on one system can affect the outcome of a measurement on the other system with which it has interacted in the past. "This onslaught came down upon us as a bolt from the blue [142]." Einstein with his co-workers published this so-called EPR paradox to prove that quantum mechanics is not a complete theory, implying that additional variables should be introduced to restore causality and locality of quantum mechanics. Einstein ruled out any "spooky actions at a distance". "No reasonable definition of reality could be expected to permit this." The EPR paradox was further elaborated by David Bohm, who reformulated the hypothetical EPR experiment in terms of spin-½ particles [143]. In 1964 John Bell derived an inequality which sets an upper limit to correlations of distant systems, provided Einstein's requirement of locality is valid [144]. The Gordian knot was cut when it was demonstrated experimentally that quantum-entangled particles can indeed violate this inequality. They exhibit correlations which are stronger than the correlations predicted by any local, realistic theory, i.e., such a theory where "the real factual situation of the system S_2 is independent of what is done with the system S_1, which is

spatially separated from the former [145]". Those states that violate Bell's inequality maximally are called the *Bell states*.

7.3 Generation of Entangled Photons

There are various quantum systems that can be entangled: atoms, ions, photons, electrons, etc. Material particles are more convenient to use for storage and information processing, whereas for communications it is more advantageous to use field particles. Hence our attention will focus on photons.

Various properties of photons can be entangled, e.g., their energies, momenta, and polarizations. Polarization-entangled γ-photons were first generated by the process of positron annihilation [146]. γ-photons are, however, not easy to handle. A better source of entangled photons was proposed and built, which utilized an atomic cascade in calcium [147-150]. An atom of Ca^{40}, excited by two-photon absorption, decays while emitting two polarization-entangled photons. Their entanglement arises from spin conservation between the excited and ground states of the calcium atoms. Stuart Freedman and John Clauser paved the way and Alain Aspect *et al.* already showed an impressive violation of Bell's inequalities at the time, even though their experiments suffered from low brightness and visibility due to the recoil of the atoms. Other experiments were also performed, using either mercury cascades [151,152] or proton-proton scattering [153].

A more efficient way to produce entangled photons is spontaneous parametric down conversion. When an optical medium is exposed to an optical field of sufficiently large amplitude, the response of the polarization of atoms of the medium becomes nonlinear. This effect can under certain conditions lead to the generation of new optical fields of different frequencies. Spontaneous parametric down conversion occurs when some of the photons of the pump beam split into pairs of photons. During the process, the energy and momentum of the photons must be conserved; the sum of the frequencies of the down-converted photons adds up to the frequency of the pump photon and the same applies to their momenta,

$$\omega_3 = \omega_1 + \omega_2 , \tag{72}$$

$$\mathbf{k}_3 = \mathbf{k}_1 + \mathbf{k}_2 . \tag{73}$$

These requirements result in correlations of the down-converted photons in various degrees of freedom, such as the time of creation, their wavelengths, the directions in which they are emitted and polarization. Two types of down conversion can be distinguished: type-I and type-II. With type-I down conversion, the emitted photons have identical polarization; with type-II their polarizations are mutually orthogonal.

In principle, all types of entanglement are equal, but in practice each of them has its pros and cons. As mentioned before, polarization states propagating down an optical

fiber are deformed due to bend-induced birefringence and polarization dispersion in fiber. Devices used to control polarization are also rather slow (~ 10 kHz). On the other hand, a particular polarization state can be set with a high precision (typical extinction ratios are of the order of 10^{-5}) and optical materials are quite insensitive to thermally induced birefringence. By comparison, phase modulators, used to encode information in the schemes based on time-energy entanglement, are fast (~ 10 GHz), but ambient temperature fluctuations that cause changes in the refractive index can easily wipe out any interference effects.

This quantum secret sharing experiment used polarization encoding. Polarization entanglement of photons can be created by both types of down conversion, type-I and type-II. Type-I, however, produces a product state, out of which the polarization-entangled state must be extracted by post-selection. In 1995, a type-II down-conversion source was proposed and constructed [154], which can directly produce the maximally entangled Bell state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_1|V\rangle_2 + |V\rangle_1|H\rangle_2\right), \tag{74}$$

where $|V\rangle_i$ and $|H\rangle_i$ are two orthogonal polarizations of the respective particle 1 and 2. The next Section will show us how this state can be used to implement quantum secret sharing.

7.4 Principle

The implementation of quantum secret sharing involved three parties, called Alice, Bob and Charlie (see Fig. 23). Alice's goal is to manipulate her messages in such a way that Bob and Charlie can reconstruct them only if they collaborate. Alice is connected with Bob and Charlie by means of optical fibers, which form the quantum channels. In addition to the quantum channels, all participants are connected by classical means, such as a computer network, telephone, etc. This public channel is open and can be tapped by anyone, but all the communications transmitted through it are authenticated to prevent an eavesdropper from altering them (Section 5.6).

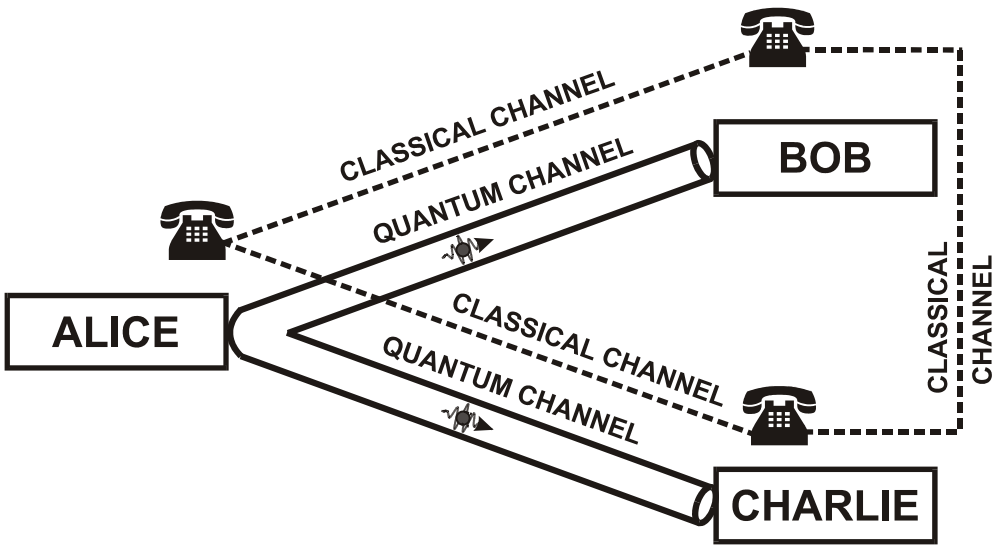

Fig. 23 Scheme of quantum secret sharing.

By analogy to quantum key distribution, two nonorthogonal bases of quantum states, mutually rotated by 90 degrees on the Poincaré sphere, are used. For example, let us generate Basis I by the Bell states $\left|\psi^+\right\rangle$ and $\left|\phi^-\right\rangle$

$$\left|\psi^+\right\rangle = \frac{\sqrt{2}}{2}\left(\left|H\right\rangle_B\left|V\right\rangle_C + \left|V\right\rangle_B\left|H\right\rangle_C\right), \tag{75}$$

$$\left|\phi^-\right\rangle = \frac{\sqrt{2}}{2}\left(\left|H\right\rangle_B\left|H\right\rangle_C - \left|V\right\rangle_B\left|V\right\rangle_C\right), \tag{76}$$

where $\left|H\right\rangle_i$ and $\left|V\right\rangle_i$ form the rectilinear polarization basis of horizontally and vertically polarized photons at Bob's and Charlie's terminals. Basis II is spanned by the Bell states $\left|\Psi^+\right\rangle$ and $\left|\Phi^-\right\rangle$, which are defined as linear superpositions of $\left|\psi^+\right\rangle$ and $\left|\phi^-\right\rangle$

$$\left|\Psi^+\right\rangle = \frac{\sqrt{2}}{2}\left(\left|\phi^-\right\rangle + \left|\psi^+\right\rangle\right), \tag{77}$$

$$\left|\Phi^-\right\rangle = \frac{\sqrt{2}}{2}\left(\left|\phi^-\right\rangle - \left|\psi^+\right\rangle\right). \tag{78}$$

These four Bell states satisfy relations analogous to relations (11)

$$\begin{aligned} \langle \psi^+ | \phi^- \rangle &= \langle \Psi^+ | \Phi^- \rangle = 0, \\ |\langle \psi^+ | \Psi^+ \rangle|^2 &= |\langle \psi^+ | \Phi^- \rangle|^2 = \frac{1}{2}, \\ |\langle \phi^- | \Psi^+ \rangle|^2 &= |\langle \phi^- | \Phi^- \rangle|^2 = \frac{1}{2}. \end{aligned} \tag{79}$$

The Bell states within one Basis are mutually orthogonal, but any two Bell states from different Bases are nonorthogonal. Using the definitions (10), we can rewrite the above Bell states in the following form

$$|\psi^+\rangle = \frac{\sqrt{2}}{2}\left(|H\rangle_B|V\rangle_C + |V\rangle_B|H\rangle_C\right) = \frac{\sqrt{2}}{2}\left(|A\rangle_B|A\rangle_C - |D\rangle_B|D\rangle_C\right), \tag{80}$$

$$|\phi^-\rangle = \frac{\sqrt{2}}{2}\left(|H\rangle_B|H\rangle_C - |V\rangle_B|V\rangle_C\right) = \frac{\sqrt{2}}{2}\left(|A\rangle_B|D\rangle_C + |D\rangle_B|A\rangle_C\right), \tag{81}$$

$$|\Psi^+\rangle = \frac{\sqrt{2}}{2}\left(|H\rangle_B|A\rangle_C + |V\rangle_B|D\rangle_C\right) = \frac{\sqrt{2}}{2}\left(|A\rangle_B|H\rangle_C + |D\rangle_B|V\rangle_C\right), \tag{82}$$

$$|\Phi^-\rangle = \frac{\sqrt{2}}{2}\left(|H\rangle_B|D\rangle_C + |V\rangle_B|A\rangle_C\right) = \frac{\sqrt{2}}{2}\left(|D\rangle_B|H\rangle_C + |A\rangle_B|V\rangle_C\right). \tag{83}$$

Relations (80-83) show us how the individual Bell states behave when we perform local measurements on them in the rectilinear and diagonal polarization bases. For example, if Bob and Charlie each have one photon from state $|\psi^+\rangle$ and they both make a measurement on their particle in the rectilinear basis, their outcomes will be anticorrelated. If they both make a measurement in the diagonal basis, their outcomes will be correlated. Plugging Eqs. (10) into Eq. (75), we can express $|\psi^+\rangle$ as follows

$$\begin{aligned} |\psi^+\rangle &= \frac{1}{2}\left(|H\rangle_B|A\rangle_C - |H\rangle_B|D\rangle_C + |V\rangle_B|A\rangle_C + |V\rangle_B|D\rangle_C\right) \\ &= \frac{1}{2}\left(|A\rangle_B|H\rangle_C - |D\rangle_B|H\rangle_C + |A\rangle_B|V\rangle_C + |D\rangle_B|V\rangle_C\right). \end{aligned} \tag{84}$$

If Bob and Charlie measure $|\psi^+\rangle$ in different polarization bases, their outcomes will be utterly random. A similar analysis can be done for the other states. The measurements when Bob and Charlie obtain deterministic outcomes are summarized in Table III.

In the deterministic cases, Bob and Charlie can find out what Bell state they measured, if they tell each other their outcomes. For example, if they both measured $|\psi^+\rangle$ in the diagonal basis, they would always detect the same polarizations of their photons. If they measured $|\phi^-\rangle$ in the diagonal basis, their polarizations would always be opposite. On the other hand, with these settings, $|\Psi^+\rangle$ and $|\Phi^-\rangle$ will give them random outcomes. $|\Psi^+\rangle$ and $|\Phi^-\rangle$ behave in a deterministic way when Bob and Charlie each measure in a different polarization basis, whereupon the states from Basis I give random outcomes.

Bob \ Charlie		Rectilinear Basis		Diagonal Basis	
		$\|H\rangle_C$	$\|V\rangle_C$	$\|A\rangle_C$	$\|D\rangle_C$
Rectilinear Basis	$\|H\rangle_B$	$\|\phi^-\rangle$	$\|\psi^+\rangle$	$\|\Psi^+\rangle$	$\|\Phi^-\rangle$
	$\|V\rangle_B$	$\|\psi^+\rangle$	$\|\phi^-\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$
Diagonal Basis	$\|A\rangle_B$	$\|\Psi^+\rangle$	$\|\Phi^-\rangle$	$\|\psi^+\rangle$	$\|\phi^-\rangle$
	$\|D\rangle_B$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	$\|\phi^-\rangle$	$\|\psi^+\rangle$

Table III Bob and Charlie make local measurements in the rectilinear and diagonal polarization bases on their particle of a Bell state. The first row and column of the table show their possible combinations of outcomes in the deterministic cases when a certain Bell state is present.

Let us now proceed to the very protocol. Let $|\psi^+\rangle$ and $|\Psi^+\rangle$ stand for the bit value '1', and $|\phi^-\rangle$ and $|\Phi^-\rangle$ for the bit value '0'. Alice prepares the Bell states (80-83) and sends them in random order down the quantum channels to Bob and Charlie. Bob and Charlie, also at random, set their detection bases. Statistically, 50 % of their outcomes are deterministic. Alice, Bob and Charlie publicly compare their bases and discard the cases with random outcomes. It should be stressed that again only the bases are disclosed, not the particular outcomes Bob and Charlie detected. The retained bits become the cryptographic key, whose values Bob and Charlie do not know yet. Upon the public comparison of bases, Charlie knows that Alice sent a state in, say, Basis I, Bob measured in the rectilinear basis and he himself detected a horizontal photon. All this information is still insufficient for him to determine what state Alice had sent. Only if Bob tells him what he detected, Charlie can look up the state sent by Alice in Table III and find out the binary value of the bit. The same applies to Bob or an eavesdropper listening in on the public communication. If and only if Bob and Charlie collaborate, can they reconstruct the secret key. The protocol is depicted in Tables IV(*a*) and IV(*b*).

$\|\psi^+\rangle$	$\|\psi^+\rangle$	$\|\psi^+\rangle$	$\|\psi^+\rangle$	$\|\Psi^+\rangle$	$\|\Psi^+\rangle$	$\|\Psi^+\rangle$	$\|\Psi^+\rangle$
+ +	× ×	+ ×	× +	+ +	× ×	+ ×	× +
OK	OK	dump	dump	dump	dump	OK	OK
$\|V\rangle$	$\|A\rangle$	R	R	R	R	$\|H\rangle$	$\|D\rangle$
$\|H\rangle$	$\|A\rangle$	R	R	R	R	$\|A\rangle$	$\|V\rangle$
'1'	'1'	–	–	–	–	'1'	'1'

Table IV(*a*) Possible states and detection bases' settings when Alice sends a binary '1'. 1st line – the states Alice selects at random and sends down the quantum channels. 2nd line – Bob and Charlie reveal their randomly set detection bases over the public channel; "+" and "×" stand for the rectilinear and diagonal bases, resp. 3rd line – Alice publicly tells them when their measurements produced deterministic outcomes. 4th line – Bob's outcomes; 'R' stands for a random outcome. 5th line – Charlie's outcomes. 6th line – when Bob (Charlie) tells Charlie (Bob) his outcome, Charlie (Bob) can look up the state sent by Alice in Table III and reconstruct the key.

$\|\phi^-\rangle$	$\|\phi^-\rangle$	$\|\phi^-\rangle$	$\|\phi^-\rangle$	$\|\Phi^-\rangle$	$\|\Phi^-\rangle$	$\|\Phi^-\rangle$	$\|\Phi^-\rangle$
+ +	× ×	+ ×	× +	+ +	× ×	+ ×	× +
OK	OK	dump	dump	dump	dump	OK	OK
$\|H\rangle$	$\|A\rangle$	R	R	R	R	$\|H\rangle$	$\|D\rangle$
$\|H\rangle$	$\|D\rangle$	R	R	R	R	$\|D\rangle$	$\|H\rangle$
'0'	'0'	–	–	–	–	'0'	'0'

Table IV(*b*) Continuation of Table IV(*a*) when Alice sends a binary '0'.

7.5 Eavesdropping

Since the security of quantum secret sharing relies on the same principles as the security of quantum key distribution, the analysis of eavesdropping can be made along the same lines. When Eve sits in the middle and attempts to intercept and resend the photon pairs, she again faces trouble as to what measurement basis to choose for either photon. 50 % of Eve's choices will be correct and she will resend the correct Bell states,

but in half the cases she will make a measurement in the wrong Basis. Suppose Alice had sent state $\left|\Psi^{+}\right\rangle$ and Eve measured both particles in the diagonal basis. She would then detect either $\left|\psi^{+}\right\rangle$ or $\left|\phi^{-}\right\rangle$. When Eve sends any of these two states down to Bob and Charlie, who measure in different polarization bases (otherwise the qubit would be discarded), they have a 50 % chance to get $\left|\Phi^{-}\right\rangle$ instead of $\left|\Psi^{+}\right\rangle$ [see Eqs. (80-83)]. The intercept/resend attack results in a 25 % error rate, which can be discovered by public comparison of a random subset of the received bits. In contrast to QKD, Bob and Charlie now pick a random subset of their bitstrings together, because one of them could want to acquire the secret key for himself and thus only meddled with the photons, which will not be put to the test. The test for eavesdropping proceeds as follows.

When the subset is chosen, Bob reveals the outcome of his measurement at the first position of the subset. Charlie reveals his outcome and the basis in which he measured the corresponding photon. Then Bob reveals his polarization basis. Eventually, Alice tells them what Basis she had used and what state she had sent. They proceed in the same way for the remaining bits of the subset. When the bases were set to produce deterministic results, there must be total agreement between the states sent by Alice and the states detected by Bob and Charlie. Any discrepancies in their bitstrings attest to eavesdropping. If an eavesdropper has been discovered, all the bits are discarded and the procedure starts over. If no eavesdropping has taken place, the participants resume the protocol according to Tables IV(*a*) and IV(*b*), and compare the rest of their bases. Since the bits used to test for the presence of an eavesdropper or a dishonest participant are publicly disclosed, they must always be thrown away and cannot constitute part of the key.

The order in which the bases and outcomes are disclosed is very important. There are ten possibilities. Let us denote C_B Charlie's basis, C_O Charlie's outcome, B_B Bob's basis, and B_O Bob's outcome. Suppose Charlie reveals his basis and outcome first and then Bob reveals his basis and outcome. Using the above notation, we write $C_BC_OB_BB_O$. It can be shown that this order is not secure from a dishonest Bob. Bob could intercept and store both photons of the pair sent by Alice, and send Charlie an arbitrary dummy photon. After Charlie has announced his basis and outcome, Bob would measure one of the photons of the original Alice's state in Charlie's basis and the other photon in a random basis. If the bases were set to produce deterministic outcomes, he measured the state correctly and knows what basis and outcome to "reveal" to match Charlie's basis and outcome with the state sent by Alice. When the bases were set incorrectly, the bit is discarded according to the protocol. The same is true for the order $C_BB_BC_OB_O$.

It is more complicated for Bob to cheat when he has to reveal his outcome before Charlie, $C_BB_BB_OC_O$. Still, Bob can get around if after the interception of Alice's pair, he sends Charlie a photon from another entangled pair, which he generated. After Charlie has revealed his basis, Bob accordingly makes a measurement on his particle of

the bogus pair to produce a deterministic outcome. Now that Bob knows what Charlie must have detected, he proceeds as in the previous case.

Another possible order is $C_O B_O C_B B_B$. This order allows cheating with the states from Basis II. Bob intercepts Alice's pair and sends Charlie an arbitrary photon. Then he measures one of the intercepted particles in the rectilinear basis and the other in the diagonal basis. Charlie discloses his outcome. Depending on whether Bob detected $\left|\Psi^+\right\rangle$ or $\left|\Phi^-\right\rangle$, he announces an anticorrelated or correlated outcome with Charlie. When Charlie reveals his basis, Bob always reports the opposite basis. Again, when the bases were incorrect, the bit is discarded. This procedure, however, does not work for the states from Basis I, because these states change symmetry according to whether projected onto the rectilinear or diagonal bases [Eqs. (80-83)]. Suppose Bob intercepted Alice's photon pair and detected $\left|\psi^+\right\rangle$. First Charlie reveals his outcome. Then Bob discloses his outcome, which must be correlated if Charlie set the diagonal basis, or anticorrelated if Charlie set the rectilinear basis. But Bob does not know at the moment what basis Charlie had set. His guessing will result in 25 % of errors in total. In the case producing an error, Bob could also try to announce the basis opposite to Charlie's, but that will give rise to a detectable imbalance between the numbers of discarded states from Bases I and II due to "incorrectly" set bases.

Let us now consider the order $C_O B_O B_B C_B$ when Bob must disclose his basis before Charlie. Suppose Alice sends a state from Basis I, Bob intercepts it, measures it in Basis II and sends Charlie a dummy photon. Charlie reveals his outcome and Bob reports a correlated or anticorrelated outcome according to his measurement. Since Bob must announce his basis first, Charlie will sometimes report the same basis. Thus, unlike the previous case when Bob could always report the opposite basis, the bit will not be discarded. Since Bob measured in the wrong Basis, an error will be detected in half the cases. The order $C_O B_O B_B C_B$ is also secure from a dishonest Charlie. Since Charlie announces his outcome first, he cannot control whether Bob will report a correlated or anticorrelated outcome. Charlie could send Bob a photon from a bogus entangled pair to increase their correlations, however, half the cases would still be random as Bob keeps alternating his nonorthogonal detection bases. Charlie could also suppress the cases leading to errors by reporting such a basis that the bit would be discarded. This would, however, result in a detectable increase of discarded bits above 50 %.

Obviously, all the orders of releasing bases and outcomes analyzed above have their counterparts when Bob and Charlie are swapped. Other combinations can be converted to some of them.

It should be mentioned that the beam-splitting attack described in Section 5.7.2 can also be applied to quantum secret sharing. If the entangled states are prepared by means of spontaneous nonlinear down conversion, there is always a nonzero probability that more than one pair will be created at the same time. For a more detailed analysis of possible attacks, the reader is referred to Section 5.7 in the QKD part of the Thesis.

7.6 Experimental Setup

This Section will show us how the required Bell states were generated and how the experimental apparatus was set up to implement quantum secret sharing. As it was already mentioned in Section 7.3, a very efficient source of polarization-entangled photons is spontaneous parametric down conversion. Parametric down conversion is an example of three-wave mixing that can occur in a non-centrosymmetric medium with a second-order nonlinearity. When the conditions of conservation of energy and momentum are satisfied, there is a nonzero probability that a photon propagating through the nonlinear medium will split into a pair of photons of lower energies.

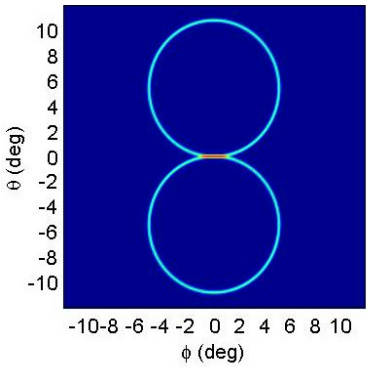

Fig. 24 Cross-section of the cones of down-converted photons emerging from the crystal in the collinear configuration. ϕ and θ determine directions in the horizontal and vertical planes. The photons in the upper ring have vertical polarization, photons in the lower ring have horizontal polarization. At the intersection of the rings, photons with both polarizations can be found. Generated in MATLAB with the help of Ying-Tsang Liu.

Materials used to produce second-order nonlinear effects are various birefringent crystals, periodically poled materials, some organic molecules and polymers. A single crystal of beta-barium borate, β-BaB_2O_4 or BBO, was used which was cut so that its optic axis made an angle $\vartheta = 41.3°$ with the normal to the entrance face, and φ was equal to $0°$ to maximize the efficiency of the process. When a vertically polarized violet laser beam at 406 nm illuminates the crystal, this cut guarantees that type-II phase-matching conditions will be satisfied. If we focus on the degenerate case, i.e., we select those down-converted photon pairs, whose photons have the same wavelength (812 nm in our case), the crystal generates two cones of down-converted photons of mutually perpendicular polarizations, which touch each other. The photons forming one cone (signal photons) have extraordinary (vertical) polarization and the photons forming the other cone (idler photons) have ordinary (horizontal) polarization. Because the intersection of the two cones is a line, this configuration is called *collinear*. The

photons that make up an entangled pair are emitted symmetrically with respect to the pump beam into the different cones. Fig. 24 shows a theoretical simulation generated in MATLAB. Fig. 25 is a picture of down conversion taken with an intensified CCD camera capable of detecting single photons (ANDOR ICCD DH5H7). In contrast to the simulation, Fig. 25 lacks the extraordinary ring as a polarizer was inserted between the crystal and the camera to remove the intense pump beam.

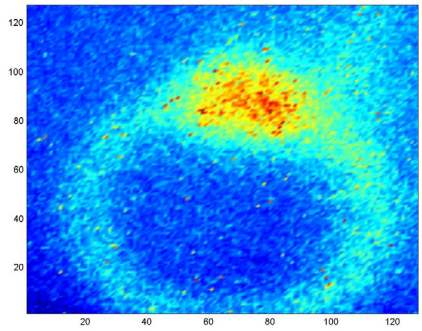

Fig. 25 A picture of collinear type-II down conversion, viewed through a narrow band-pass filter at 812 nm. The ICCD camera was placed behind the crystal. Only the ordinary ring can be seen. The extraordinary ring was removed by a polarizer inserted between the crystal and the camera to eliminate the intense pump beam. The bright spot at the top of the ring is the remaining pump photons that made it through the polarizer and the filter. The picture was taken with the help of Ayman Abouraddy and Giovanni Di Giuseppe.

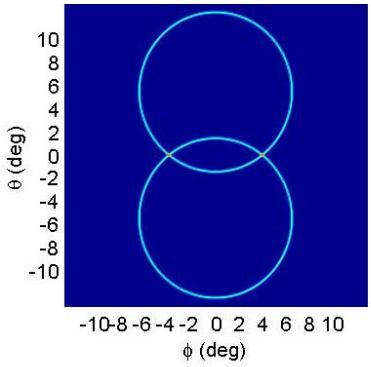

Fig. 26 Cross-section of the cones of noncollinear down conversion. ϕ and θ determine directions in the horizontal and vertical planes. The polarization-entangled state can be found at the intersections of the two rings.

The collinear configuration can provide energy-time entangled photons and momentum entangled photons, however, in order to obtain polarization-entangled photons, we have to use post-selection of the generated states. By changing the angle

between the crystal's optic axis and the direction of the pump beam, we change the extraordinary refractive index and thereby the phase-matching conditions (73). If the angle is increased, the angle between the axes of the two cones decreases. The cones start to overlap and their intersection is two *noncollinear* lines, along which photons of both polarizations propagate (see Fig. 26). If we measure the polarization of photons in either of the two directions, we observe unpolarized light. However, if we look at the correlations between the polarizations of signal and idler photons, we find the photons in the entangled state

$$|\psi\rangle = \frac{\sqrt{2}}{2}\left(|H\rangle_S|V\rangle_I + e^{i\delta}|V\rangle_S|H\rangle_I\right), \tag{85}$$

where *S* and *I* stand for the signal and idler beams, and the phase factor δ is determined by the birefringent properties of the crystal. Indeed, if we trace the density matrix of the state (85) over the states of one subsystem, say the idler, we obtain the reduced density matrix

$$\rho^{(S)} = Tr^{(I)}\left(|\psi\rangle\langle\psi|\right) = \frac{1}{2}\left(|V\rangle_{S\,S}\langle V| + |H\rangle_{S\,S}\langle H|\right), \tag{86}$$

which represents a uniform mixture of photons with vertical and horizontal polarizations.

A small catch should be noted, though. In birefringent media, the ordinary and extraordinary beams travel at different velocities, which results in their *temporal walk-off*. Also, if the extraordinary beam is neither parallel nor perpendicular to the optic axis, its energy does not flow along the direction of the wave vector **k**. The deviation between the Poynting vector and the vector wave **k** results in a *spatial walk-off*. In consequence, the nonlinear crystal turns the pure state (85) into a mixed state – a noncoherent mixture of states $|H\rangle_S|V\rangle_I$ and $|V\rangle_S|H\rangle_I$. By the order in which the signal and idler detectors fire, we can distinguish which part of the superposition we measured. Similarly, the individual terms of the superposition arrive at spatially different locations. A description of how to compensate for the temporal and spatial walk-offs will be given in the next Section.

Let me now depict the experimental setup (Fig. 27). A krypton ion laser generates a pump beam at 406 nm. The beam passes through a dispersion prism and a set of irises, which remove the fluorescence arising from the radiative transitions in the plasma of the laser. The remaining 60 mW of violet photons pump the nonlinear BBO crystal. The crystal was tilted by 2.5° to achieve noncollinear generation with an angle of 8° between the signal and idler photons. The entangled pairs pass through half-wave plates, birefringent compensating crystals, irises and interference filters, and after 90 cm of free-space propagation are coupled into optical fibers (Fig. 28) that guide them to Bob's and Charlie's terminals. If Alice slightly tilts one of the compensating crystals,

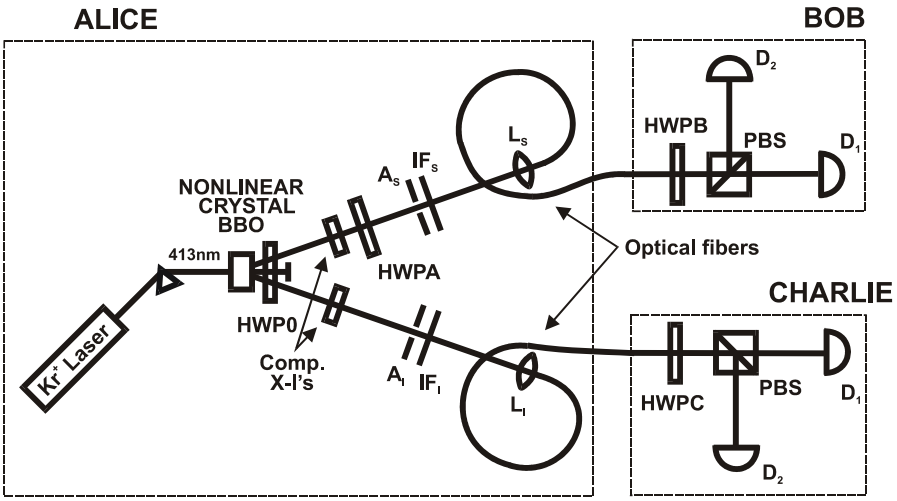

Fig. 27 Scheme of the optical part of the quantum secret-sharing apparatus. HWP0, HWPA, HWPB, HWPC – half-wave plates; Comp. X-l's – compensating crystals; A_S, A_I – apertures in signal and idler beams; IF_S, IF_I – interference filters; L_S, L_I – coupling lenses; PBS – polarizing beam splitters; D – single-photon counting modules.

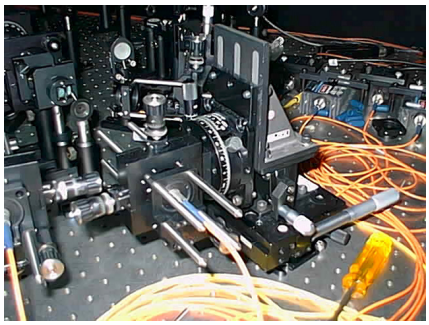

Fig. 28 Bob's fiber-coupling stage.

she can set the phase factor δ in Eq. (85) to 0 or π. If she further rotates her half-wave plate HWPA, she can prepare any of the four Bell states (80-83). Each detection terminal consists of a Glan-Thompson polarizing beam splitter and two single-photon counting modules, one at each output port. Single-photon counting modules were thermoelectrically cooled silicon avalanche photodiodes operated in the Geiger mode above the breakdown voltage (PerkinElmer SPCM-AQ). Bob and Charlie set their detection bases using a half-wave plate, placed before their respective beam splitter. A picture of the layout on the optical table is in Fig. 29.

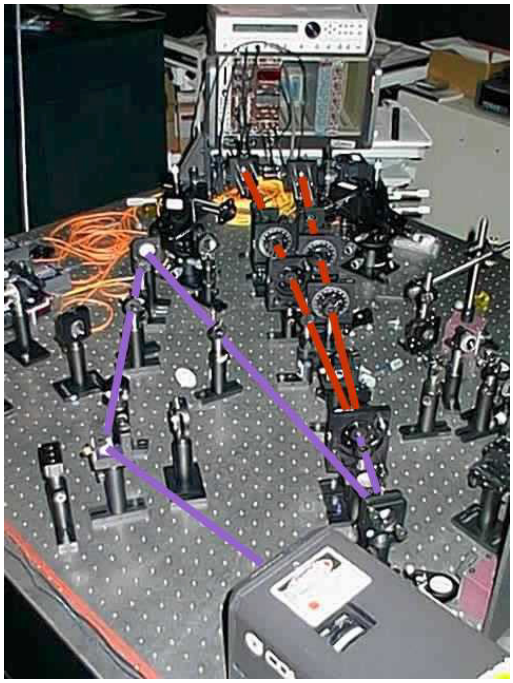

Fig. 29 A picture of the layout on the optical table.

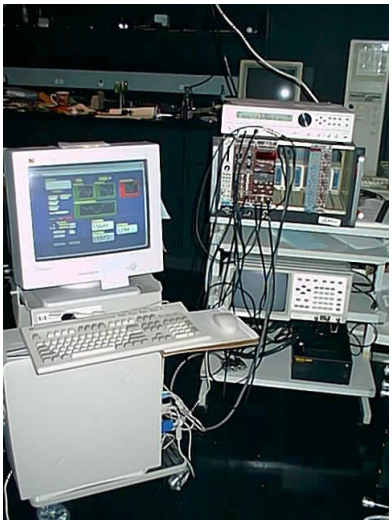

Fig. 30 A picture of the electronic equipment used to take data.

The detectors produced TTL pulses that were fed into a counter (Stanford Research Systems SR400), which counted all "single" events, i.e., those events when at least one of the photons of a pair was detected. The coaxial cables between the detectors and the counter were of different lengths; thus simultaneous detection of an entangled pair was transformed into TTL pulses with a predetermined time delay. The pulses started and stopped a time-to-amplitude converter (EG&G ORTEC TAC/SCA 567),

which converted their time delay into voltage. A single-channel analyzer selected the voltage that corresponds to "coincidence" events, and another counter (EG&G ORTEC Quad Counter/Timer 974) counted its outputs. This configuration enabled simultaneous counting of single events and coincidences (Fig. 30). The devices were driven by a PC through a GPIB interface. The program taking and analyzing the data was written in LabVIEW (Fig. 31).

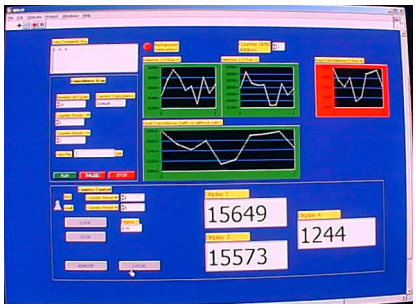

Fig. 31 The interface of the LabVIEW data-processing program.

7.7 Experimental Results

7.7.1 Temporal and Spatial Walk-off

As mentioned in the previous Section, a nonlinear crystal itself does not produce a pure polarization-entangled state. In consequence of the temporal and spatial walk-offs, the terms in (85) can be distinguished.

In a uniaxial crystal, the dependence of the refractive index of the extraordinary beam on its direction is described by an ellipsoid of revolution. The energy of the extraordinary beam flows in the direction of the normal to the surface of the ellipsoid at the point of intersection with the wave vector **k**. If we calculate the angle between the Poynting vector and the vector wave **k** in the plane given by the optic axis and the pump beam, we obtain the walk-off angle ρ

$$\rho = \arctan\left[\left(\frac{n_o}{n_e}\right)^2 \tan\theta\right] - \theta\,, \tag{87}$$

where θ is the angle between the optic axis and the direction of the extraordinary beam, and n_o and n_e are the ordinary and extraordinary refractive indices, respectively. The maximum spatial walk-off Δx at the output face of the crystal of length L is

$$\Delta x = L \tan\rho\,. \tag{88}$$

A 1.5 mm BBO crystal with the above cut ϑ and tilt gives rise to $\rho = 4°$ and $\Delta x = 0.1\,\text{mm}$. In our case, Δx is small compared to the pump beam diameter (2 mm), thereby the overlap of the ordinary and extraordinary beams is large and a suitably placed iris can eliminate the spatial walk-off.

In a negative crystal, the ordinary wave packet acquires a time delay $\Delta\tau$ with respect to the extraordinary wave packet

$$\Delta\tau = L\left(\frac{1}{v_g^o} - \frac{1}{v_g^e}\right), \tag{89}$$

where the term in parentheses is the mismatch of the inverse group velocities. If a birefringent element, which produces the same time delay but of the opposite sign, is inserted in one of the down-conversion legs, the temporal walk-off can be compensated. Such an element causes $|H\rangle|V\rangle$ pairs created at a distance x before the center of the crystal, $L/2 - x$, to arrive with the same time delay as $|V\rangle|H\rangle$ pairs created at $L/2 + x$, and likewise when $|H\rangle$ and $|V\rangle$ are swapped.

7.7.2 Walk-off Compensation with a Quartz Crystal

A 1.5 mm BBO crystal with the above orientation produces a temporal walk-off of 294 fs, which slightly exceeds the entanglement time of down-converted photons determined by the 10 nm interference filters and irises. A 10.8 mm thick crystal of positive birefringent quartz produces a "negative" temporal walk-off of equal size.

Fig. 32 shows state $|\phi^-\rangle$ compensated by a 10 mm piece of quartz. Alice prepared $|\phi^-\rangle$, Charlie set his half-wave plate HWPC so as to measure in the rectilinear basis (squares) or in the diagonal basis (triangles), and Bob was rotating his measurement basis by angle β. Coincidences between Bob's and Charlie's transmitted beams at their respective beam splitters are plotted as a function of the rotation of Bob's basis. We can see correlations in the rectilinear basis and anticorrelations in the diagonal basis, as expected. Each basis exhibited a different visibility, though, arising from improper compensation. The difference in visibilities attests to the fact that in addition to the maximally entangled state $|\phi^-\rangle$, a noncoherent mixture of $|H\rangle|V\rangle$ and $|V\rangle|H\rangle$ states was present. The diagonal basis displays the true quantum non-local behavior, however, the curve in the rectilinear basis can be mimicked by a classical system. When the Clauser-Horne-Shimony-Holt (CHSH) inequality [155] was consequently measured, this imbalance in visibilities lead to its violation by 18 standard deviations, even though the visibility required for its violation, $\sqrt{2}/2$, was not reached in this setup.

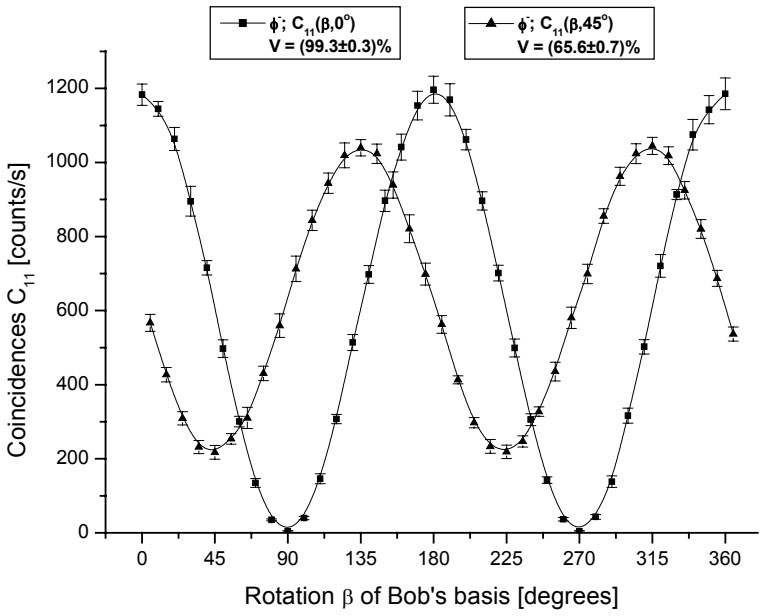

Fig. 32 Alice prepared state $\left|\phi^{-}\right\rangle$. Coincidences between Bob's Detector 1 and Charlie's Detector 1 $C_{11}(\beta,0°)$ and $C_{11}(\beta,45°)$ are plotted as a function of rotation β of Bob's measurement basis when Charlie set his basis to 0° (squares) or 45° (triangles). The temporal walk-off of a 1.5 mm BBO crystal was compensated by a 10 mm crystal of quartz. Visibility in the rectilinear basis was (99.3 ± 0.3) %. Visibility in the diagonal basis was (65.6 ± 0.7) %. A maximum visibility of (85.0 ± 4.4) % could be reached (see text). The data with lower visibility is shown to enable comparison based on the same coincidence rate.

7.7.3 CHSH Inequality

The CHSH inequality is a generalization of Bell's inequality. Let Bob and Charlie measure in bases rotated by angle β and γ, respectively, with respect to the rectilinear basis. Their polarizing beam splitters can either transmit a photon (outcome takes value +1), or reflect it (outcome takes value –1). If we denote $C_{ij}(\beta,\gamma)$ the number of coincidences between Bob's detector i and Charlie's detector j, where $i, j \in \{1,2\}$, the correlation coefficient of Bob's and Charlie's measurements can be expressed as

$$E(\beta,\gamma)=\frac{C_{11}(\beta,\gamma)+C_{22}(\beta,\gamma)-C_{12}(\beta,\gamma)-C_{21}(\beta,\gamma)}{C_{11}(\beta,\gamma)+C_{22}(\beta,\gamma)+C_{12}(\beta,\gamma)+C_{21}(\beta,\gamma)}. \tag{90}$$

The normalization to the total number coincidences can be made under the assumption that the detected events represent a faithful sample of all pairs generated by the crystal.

If we now construct

$$S(\beta,\beta',\gamma,\gamma') = E(\beta,\gamma) - E(\beta,\gamma') + E(\beta',\gamma) + E(\beta',\gamma'), \tag{91}$$

it can be shown [155] that any local hidden-variable theory predicts

$$-2 \le S \le 2. \tag{92}$$

Quantum mechanics, however, predicts that $E(\beta,\gamma) = \cos 2(\beta - \gamma)$. It is then possible to find such settings of angles that the inequality (92) is violated. Its violation shows that quantum-entangled states exhibit correlations stronger than classical systems. The maximum violation is attained when $\beta = 0°, \beta' = 45°, \gamma = 22.5°$, and $\gamma' = 67.5°$. The first, third and fourth term in Eq. (91) are then equal to $\sqrt{2}/2$ and the second one is $-\sqrt{2}/2$, which altogether adds up to $S = 2\sqrt{2} \cong 2.83$.

With a visibility of 65.6 %, S should diminish to $S = 2\sqrt{2}V = 1.85$, whereas $S = 2.36 \pm 0.02$ was measured. The visibility should, however, be independent of the measurement basis. The measured value of parameter *S* arises from the fact that the first two terms in Eq. (91) were artificially boosted by deeper modulation of the interference pattern in the rectilinear basis. When the visibility in the rectilinear basis was degraded to 65.6 %, while maintaining the visibility in the diagonal basis at the same value, *S* indeed decreased to 1.81, which already corresponds to the expected value.

Irises of a smaller diameter (1 mm) could push visibility up to (85.0 ± 4.4) % at the expense of the number of coincidences, whereupon the number of coincidences went down by an order of magnitude (the drop in the number of coincidences resulted in the increased standard deviation). Higher visibility could not be achieved due to the improper thickness of the quartz. The quartz could also be tilted to increase its effective length, but this would have decreased the group velocity mismatch and increased the transversal walk-off. Eventually the data with lower visibility was chosen for Fig. 32 to enable comparison of different compensation approaches, based on the same coincidence rate.

7.7.4 Walk-off Compensation with Two BBO Crystals

To use a single crystal of quartz is not the only way to compensate for the temporal walk-off. Sliding two quartz wedges against each other, we can introduce a variable time delay and achieve a better match.

Two BBO crystals, one in each down-conversion leg, of the same cut ϑ as the generating crystal but half its thickness, can do the same job as well. If the two crystals are rotated by 90° about the axis given by the down-converted beams, the ordinary and extraordinary polarizations exchange their roles, and indistinguishability of the terms in (85) is restored. As it was tricky to rotate the compensating crystals while maintaining their tilt (necessary because of the tilt of the generating crystal), a half-wave plate HWP0 was inserted after the generating crystal to swap the polarizations (see Fig. 27). Coincidences between Bob's D_2 and Charlie's D_1 are plotted in Fig. 33 when Alice was

sending states $|\psi^+\rangle$. With the same coincidence rate as in the previous setup, the visibility in the diagonal basis rose to (88.0 ± 1.0) %. S was again inflated by the "interference" in the rectilinear basis up to 2.62 ± 0.03 in contrast with the expected value of 2.49. Smaller irises could increase visibility to (92.2 ± 3.8) % at the expense of the number of coincidences. With this configuration I expected to obtain best results, however, visibility was degraded due to lower optical quality of the BBO crystal.

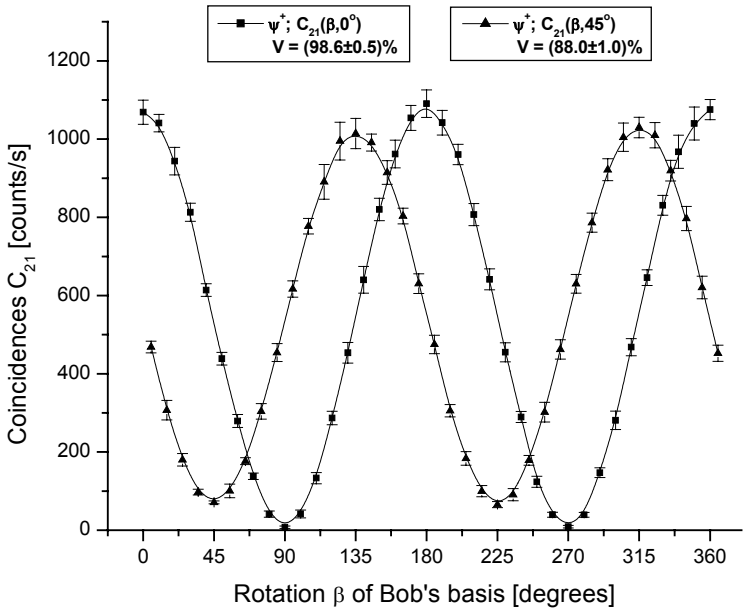

Fig. 33 Alice prepared state $|\psi^+\rangle$. Coincidences $C_{21}(\beta,0°)$ and $C_{21}(\beta,45°)$ between Bob's D_2 and Charlie's D_1 are shown as a function of rotation β of Bob's basis, when Charlie set his basis to 0° (squares) or 45° (triangles). The temporal walk-off of a 3 mm BBO crystal was compensated by two 1.5 mm BBO crystals, one in each arm, preceded by a half-wave plate. Visibility in the rectilinear basis was (98.6 ± 0.5) %. Visibility in the diagonal basis was (88.0 ± 1.0) %.

7.7.5 Walk-off Compensation with One BBO Crystal

Better results were achieved in an asymmetrical configuration when only one compensating crystal of the same thickness and cut as the generating crystal was inserted in one of the arms. Fig. 34 shows coincidences $C_{11}(\beta,0°)$ when Alice was preparing states $|\psi^+\rangle$ and $|\phi^-\rangle$; the achieved visibilities were (97.3 ± 0.8) % and (97.2 ± 0.6) %, respectively. The diagonal basis exhibited slightly lower visibilities of (94.8 ± 0.6) % and (95.1 ± 0.9) %, resp. (Fig. 35).

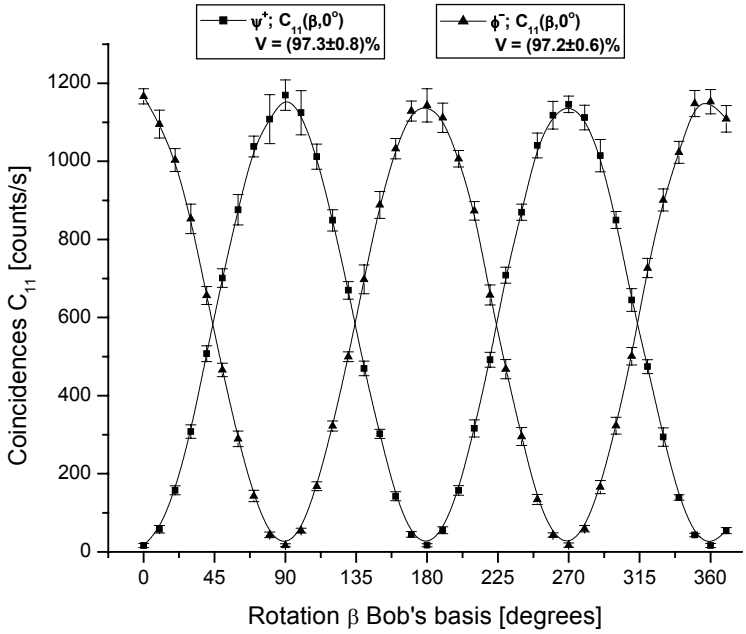

Fig. 34 States $\left|\psi^{+}\right\rangle$ (squares) and $\left|\phi^{-}\right\rangle$ (triangles) in the rectilinear basis. Coincidences $C_{11}(\beta,0°)$ are plotted as a function of rotation β of Bob's measurement basis, when Charlie set his basis to 0°. The temporal walk-off of a 1.5 mm BBO crystal was compensated by one 1.5 mm BBO crystal in Charlie's arm, preceded by a half-wave plate. Visibility of $\left|\psi^{+}\right\rangle$ was (97.3 ± 0.8) %. Visibility of $\left|\phi^{-}\right\rangle$ was (97.2 ± 0.6) %.

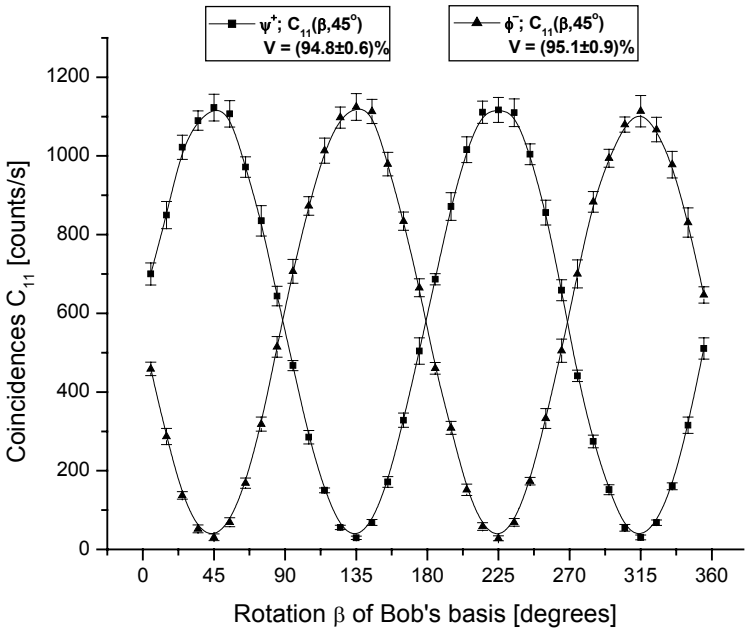

Fig. 35 States $\left|\psi^{+}\right\rangle$ (squares) and $\left|\phi^{-}\right\rangle$ (triangles) in the diagonal basis. Coincidences $C_{11}(\beta,45°)$ are plotted as a function of Bob's measurement basis β, when Charlie set his basis to 45°. The compensation of the temporal walk-off was identical as in the previous Figure. Visibility of $\left|\psi^{+}\right\rangle$ was (94.8 ± 0.6) %. Visibility of $\left|\phi^{-}\right\rangle$ was (95.1 ± 0.9) %.

Fig. 36 displays the behavior of state $\left|\Phi^{-}\right\rangle$ in Basis II. One curve (squares) was obtained when Charlie measured in the rectilinear basis, while Bob was rotating his half-wave plate. At $\beta = 45°$, we can see correlations (anticorrelations in C_{12}), as expected [Eq. (83)]. Basically Bob only undoes the local unitary transformation that Alice performed on his particle. It corresponds to measuring $\left|\psi^{+}\right\rangle$ or $\left|\phi^{-}\right\rangle$ in the rectilinear basis and therefore this curve exhibits higher visibility (97.1 ± 0.6) %. The other curve (triangles) was obtained when Bob measured in the rectilinear basis and Charlie was rotating his basis. This measurement already reveals the true quantum non-local interference with visibility attaining (95.4 ± 0.6) %. The CHSH inequality was violated by $S = 2.72 \pm 0.03$.

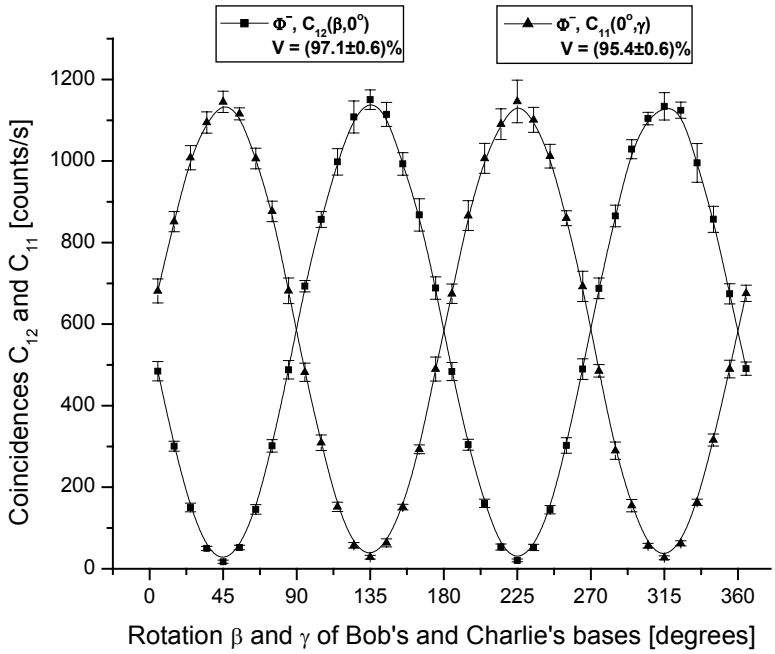

Fig. 36 State $\left|\Phi^{-}\right\rangle$ in Basis II. Coincidences $C_{12}(\beta,0°)$ are plotted as a function of rotation β of Bob's measurement basis, when Charlie set his basis to 0° (squares). Coincidences $C_{11}(0°,\gamma)$ are plotted as a function of rotation γ of Charlie's basis, when Bob set his basis to 0° (triangles). The compensation of the temporal walk-off was identical as in Fig. 34. Curve $C_{12}(\beta,0°)$ describes classical behavior with visibility (97.1 ± 0.6) %. Curve $C_{11}(0°,\gamma)$ shows quantum interference with visibility (95.4 ± 0.6) %.

Fig. 37 illustrates the adverse effect of the transversal walk-off. When irises A_S and A_I of Fig. 27 were broadened to a diameter of 3 mm, the visibility of state $\left|\phi^{-}\right\rangle$ in the rectilinear basis degraded to (96.6 ± 0.1) % and the visibility in the diagonal basis fell to (87.7 ± 0.6) %. A detailed analysis of the influence of the shape and size of

apertures on the quality of the entangled state produced in the collinear configuration was made by Mete Atatüre *et al*. [156].

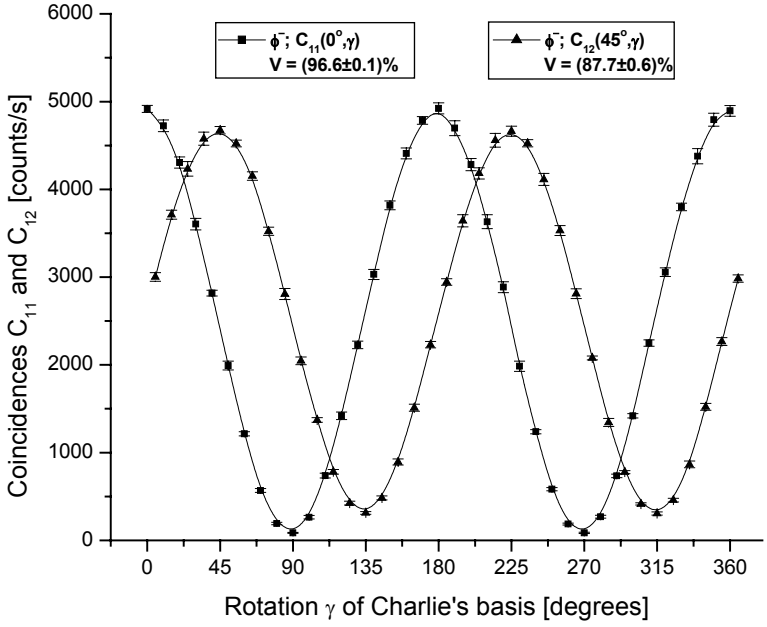

Fig. 37 The effect of the transversal walk-off on state $\left|\phi^{-}\right\rangle$, when irises A_S and A_I were broadened to a diameter of 3 mm. Coincidences $C_{11}(0°,\gamma)$ (squares) and $C_{12}(45°,\gamma)$ (triangles) are shown as a function of Charlie's basis γ. Visibility in the rectilinear basis dropped to (96.6 ± 0.1) % and visibility in the diagonal basis fell to (87.7 ± 0.6) %.

7.7.6 Quantum Alphabet

In the end, the quantum alphabet was run to test the communication performance of the experimental setup. Alice in turn generated the four Bell states $\left|\psi^{+}\right\rangle$, $\left|\phi^{-}\right\rangle$, $\left|\Psi^{+}\right\rangle$, and $\left|\Phi^{-}\right\rangle$, and Bob and Charlie set the 4 possible combinations of their measurement bases, ++, ××, +×, ×+, for each of the Bell states. Typical data is shown in Tables V(*a*) and V(*b*). $C_{ij}, i, j \in \{1,2\}$, are the numbers of coincidences per second that Bob and Charlie detected between their detectors *i* and *j*, when individual Bell states were sent and different combinations of their measurement bases were set. We can see all correlations, anticorrelations and random outcomes in accordance with relations (80-83). The measured *BER* was 1.9 %.

	$\|\psi^+\rangle$	$\|\psi^+\rangle$	$\|\psi^+\rangle$	$\|\psi^+\rangle$	$\|\Psi^+\rangle$	$\|\Psi^+\rangle$	$\|\Psi^+\rangle$	$\|\Psi^+\rangle$
	+ +	× ×	+ ×	× +	+ +	× ×	+ ×	× +
C_{11}	17±4	1057±32	544±18	549±17	551±22	552±26	16±4	21±3
C_{22}	15±4	1067±29	558±33	557±28	556±20	557±32	12±3	26±5
C_{12}	1096±31	29±5	561±21	525±15	518±12	535±17	1086±27	1078±38
C_{21}	1078±44	21±4	541±23	558±23	548±19	554±20	1100±50	1080±30

Table V(*a*) Quantum alphabet. Alice sends the four Bell states (first line), and Bob and Charlie set different combinations of their measurement bases for each state (second line); "+" and "×" stand for the rectilinear and diagonal bases, resp. $C_{ij}, i, j \in \{1,2\}$, are the numbers of coincidences per second Bob and Charlie detected between their detectors *i* and *j*. This data yields $BER = 1.9\ \%$.

	$\|\phi^-\rangle$	$\|\phi^-\rangle$	$\|\phi^-\rangle$	$\|\phi^-\rangle$	$\|\Phi^-\rangle$	$\|\Phi^-\rangle$	$\|\Phi^-\rangle$	$\|\Phi^-\rangle$
	+ +	× ×	+ ×	× +	+ +	× ×	+ ×	× +
C_{11}	1087±31	27±2	557±24	518±22	539±23	535±28	1087±32	1077±43
C_{22}	1090±37	22±5	556±24	558±27	548±20	564±16	1070±28	1072±35
C_{12}	19±4	1070±27	552±19	547±11	575±18	539±25	20±6	27±4
C_{21}	16±4	1094±29	555±23	544±14	564±28	583±26	19±4	31±6

Table V(*b*) Quantum alphabet. Continuation of Table V(*a*).

The next step of the experiment would be to replace the CW laser with a pulsed source to enable full synchronization of Alice's, Bob's and Charlie's terminals. Furthermore, if half-wave plates were replaced with Pockels cells, it would be possible to make the settings of Bell states and Bob's and Charlie's measurement bases fully automated in a way similar to the experimental implementations of quantum key distribution and quantum identification, as described in Chapters 5 and 6. Eventually, Alice, Bob and Charlie should be placed in different rooms or buildings.

Chapter 8
Conclusions

The goal of this PhD Thesis was to experimentally investigate phenomena of quantum interference and quantum nonlocal correlations using the methods of quantum optics. The Thesis has presented three laboratory experiments in the field of quantum cryptography: Quantum key distribution, quantum identification and quantum secret sharing. In contrast to classical cryptographic schemes, whose security is vulnerable to advancement of computer power and mathematical algorithms, the security of quantum cryptographic schemes is guaranteed by the fundamental laws of Nature. It was shown that exploiting the Heisenberg uncertainty principle, unconditionally secure quantum communications schemes can be designed. Their security stems from the impossibility to distinguish nonorthogonal quantum states with certainty. A potential eavesdropper introduces errors in the transmissions, which can later be discovered by the legitimate participants of the communication. The legitimate users sacrifice part of the key by public comparison in order to find out discrepancies in their bitstrings and to estimate the amount of information that might have leaked to an eavesdropper. Since only a cryptographic key consisting of random bits is transmitted, no security breach occurs in the case of eavesdropping; the key is simply discarded and a new one is generated.

The quantum key distribution experiment was based on interference of weak coherent states in a time-multiplexing interferometer. An extended, 0.5 km long, optical-fiber-based interferometer was built with visibility reaching 99.6 %. The quantum states were prepared by attenuating light pulses generated by a semiconductor laser; silicon avalanche photodiodes were used for their detection. It was described in detail how the interferometer was balanced and stabilized, including the problems arising from the multi-mode structure of the spectrum of the semiconductor laser, polarization deformation in fibers, thermal phase drift, unbalanced losses, beam-splitter imperfections, etc. This setup allowed Alice and Bob to establish a common secret key with bit error rates 0.3-0.4 %. A choice of a 2000-bit subset of the raw key to test for eavesdropping was justified. When error-rate estimate $\varepsilon_{\mathrm{est}}$ determined from this subset was smaller then a limiting value $\varepsilon_{\mathrm{lim}}$, the users could conclude that the actual error rate might have exceeded a maximum tolerable error rate $\varepsilon_{\mathrm{max}}$ only with a probability smaller than 10^{-10}. The beam-splitting attack was analyzed in detail and the maximum number of bits an eavesdropper can learn was derived. $\varepsilon_{\mathrm{max}}$ and the maximum number of beam-split pulses was then used to determine the upper limit to the amount of information that could have leaked to an eavesdropper. Based on this information, the raw key was error corrected and privacy amplified to reduce eavesdropper's information so that she could know at most one bit of the distilled key with a probability

smaller than 10^{-10}. In the end, the distilled key was used to encrypt messages by means of the Vernam cipher. The phase encoding, interferometer calibration and all the auxiliary communications were fully automated, driven by computers communicating over the local computer network.

The quantum identification experiment combined a classical three-pass identification procedure and QKD. Each identification sequence was used only once and QKD served to supply new secret identification sequences. Two identification protocols were presented. First, an identification protocol was set forth that can be used provided the users have an unjammable public channel at their disposal. The upper bound to eavesdropper's deception probability was derived. In case the users do not have an unjammable channel at their disposal, it was shown how the identification procedure can be incorporated in the authenticated QKD public discussion. Since losses limit the distance over which secure quantum communication can be performed, a necessary condition was derived that sets an upper bound to the attenuation of the quantum channel. The same condition also restricts the mean intensity of laser pulses if weak coherent states are used instead of single photons. Eventually, given the losses of the actual experimental apparatus, the mean intensity of laser pulses was optimized to maximize the yield of the new cryptographic key. After the optimization, the system generated ~ 650 bits per second of a distilled cryptographic key with an expansion ratio $r = 2$. The whole identification took about 3 minutes, including all the auxiliary processes. The performance of the system could have been improved yet if Alice's and Bob's personal computers were aided by single-chip computers and faster electronics.

The third experiment was an implementation of quantum secret sharing. The constructed apparatus was based on the peculiar correlations of entangled states. In particular, polarization entanglement of photon pairs was employed. Polarization-entangled photon pairs were generated in a nonlinear crystal by spontaneous parametric down conversion. It was demonstrated that the four Bell states $|\psi^+\rangle$, $|\phi^-\rangle$, $|\Psi^+\rangle$, and $|\Phi^-\rangle$ in two nonorthogonal bases can easily be prepared. After free-space propagation, the entangled states were coupled into optical fibers. Different setups with different levels of purity of entangled states were built. A violation of the CHSH inequality was tested with each setup. It was demonstrated how improper preparation of entangled states can bias the measured value of parameter *S*. The visibility depended on the used compensation of the temporal walk-off arising from the birefringence of the generating BBO crystal. With the last setup, when the walk-off was compensated by one BBO crystal identical to the generating crystal, rotated by 90 degrees, a visibility of quantum interference exceeding 95 % was achieved. The CHSH inequality was violated by $S = 2.72 \pm 0.03$. When the quantum alphabet was tested, a bit error rate of 1.9 % was measured.

Let me conclude that three experiments in the flourishing fields of quantum information technologies and quantum communications were implemented. Together with other successful experiments of the past decade, they represent another small achievement that ushers in a new and very promising era of quantum technologies, and

it draws nearer the time when quantum technologies will expediently complement the classical ones even in everyday life. It should be pointed out, though, that quantum cryptography should not intend to replace conventional cryptography. In the same way as public-key cryptography has not eliminated private-key cryptography, it will always be beneficial to use a combination of different cryptographic approaches.

References

[1] M. Dušek, O. Haderka, M. Hendrych, and R. Myška, *Quantum Identification System*, Phys. Rev. A **60**, pp. 149-156 (1999).

[2] M. Dušek, O. Haderka, and M. Hendrych, *Generalized Beam-Splitting Attack in Quantum Cryptography with Dim Coherent States*, Opt. Comms. **169**, pp. 103-108 (1999).

[3] M. Dušek, O. Haderka, and M. Hendrych, *Practical Aspects of Quantum Cryptography*, in *Proc. of Fourth International Conference on Quantum Communication, Measurement, and Computing*, eds. Kumar et al., Northwestern University, Evanston, Illinois, USA, August 1998, Kluwer/Plenum, New York, p. 393 (2000).

[4] M. Hendrych, *Quantum Secret Sharing*, Technical Report, NATO Advanced Science Fellowship Programme, February 2002.

[5] M. Hendrych is a co-author of Secs. IV and VIII in the book J. Peřina *et al*., *Nonlinear Phenomena in Quantum Optics*, in *Modern Nonlinear Optics*, Part I, ed. M. Evans, Advances in Chemical Physics, vol. **119**, J. Wiley & Sons, Inc. New York (2001).

[6] M. Hendrych, M. Dušek, and O. Haderka, *The Effect of Beam-Splitter Imperfections and Losses on Fringe Visibility in a Mach-Zehnder Interferometer*, Acta Phys. Slov. **46**, pp. 393-398 (1996).

[7] M. Dušek, O. Haderka, and M. Hendrych, *Application of Quantum Key Distribution for Mutual Identification – Experimental Realization*, Acta Phys. Slov. **48**, pp. 169-176 (1998).

[8] O. Haderka, M. Hendrych, and M. Dušek, *Experimental Implementation of Quantum Cryptography*, in Proc. of SPIE, Vol. **3820**, 11th Slovak-Czech-Polish Optical Conference on Wave and Quantum Aspects of Contemporary Optics, Stara Lesna, High Tatra Mountains, Slovakia, pp. 88-93 (1999).

[9] M. Dušek, O. Haderka, and M. Hendrych, *Physical Aspects of Optical Implementation of Quantum Cryptography*, in *Proc. 1st Intl. Conf. on Theory and Applications of Cryptology*, Pragocrypt '96, Prague, CTU Publ. House, Prague, pp. 234-241 (1996).

[10] M. Dušek, O. Haderka, and M. Hendrych, *Quantum Cryptography*, Vesmír **77**, in Czech, pp. 633-637 (1998).

[11] O. Haderka, M. Hendrych, and M. Dušek, *Quantum Cryptography (Communications with the Help of Single Photons – the End of Eavesdropping?),* Optics Communications O.K.'99, Prague, Tech-Market, Prague, in Czech, pp. 52-62 (1999).

[12] D. Kahn, *The Codebreakers: The Story of Secret Writing*, Macmillan, New York (1967).
[13] Homer, *Iliad* 6.213, transl. Ian Johnston (in English), Malaspina University-College, Nanaimo, BC, Canada (2000).
[14] Charles Anthon, *The first six books of Homer's Iliad with English notes, critical & explanatory, a metrical index, & Homeric glossary*, Harper & Brothers, New York, p. 396 (1875).
[15] Old Spartan Facts at http://www.geocities.com/Athens/Aegean/7849/spfacts.html.
[16] D.R. Stinson, *Cryptography, Theory and Practice*, CRC Press, Inc., Boca Raton, p. 4 (1995).
[17] T.P. Leary, *Cryptology in the 15th and 16th Century*, Cryptologia **20**, No. 3, pp. 223-242 (July 1996).
[18] E.A. Poe, *The Gold Bug*, in *Tales of Mystery and Imagination*, Wordsworth Editions Ltd., Ware, pp. 1-46 (1993).
[19] A.C. Doyle, *The Adventure of the Dancing Men*, in *The Annotated Sherlock Holmes*, Vol. 2, ed. W.S. Baring-Gould, Wings Books, New Jersey, pp. 527-545 (1992).
[20] G.S. Vernam, *Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications*, J. AIEE **45**, pp. 109-115 (1926).
[21] C.A. Deavours and L. Kruh, *Machine Cryptography and Modern Cryptanalysis,* Artech House, Dedham MA (1985).
[22] *Codebreakers: The Inside Story of Bletchley Park,* eds. F.H. Hinsley and A. Stripp, Oxford University Press, Oxford (1997).
[23] W. Diffie and M.E. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory **22**, pp. 644-654 (1976).
[24] R.L. Rivest, A. Shamir, and L.M. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, Vol. **21**, No. 2, pp. 120-126 (1978).
[25] R.K. Guy, *Proc. Fifth Manitoba Conf. Numer. Math*., Congressus Numerantium **16**, p. 49 (1976).
[26] M. Gardner, *Mathematical Games*, *A New Kind of Cipher That Would Take Millions of Years to Break*, Sci. Am. **237**, pp. 120-124 (1977).
[27] A. Shamir, *Factoring Large Numbers with the TWINKLE Device*, in *Advances in Cryptology – Eurocrypt '99*, International Conference on the Theory and Application of Cryptographic Techniques, Prague, May 1999.
[28] P.W. Shor, *Algorithms for Quantum Computation: Factoring and Discrete Logarithms*, in *Proc. 35th Annual Symposium on Foundations of Comp. Science*, ed. by S. Goldwasser, IEEE Press, Bellingham, pp. 124-134 (1994).
[29] L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, and I.L. Chuang, *Experimental Realization of Shor's Quantum Factoring Algorithm Using Nuclear Magnetic Resonance*, Nature **414**, pp. 883-887 (2001).

[30] Michael Wiener, *Efficient DES Key Search – An Update*, RSA Laboratories' Cryptobytes Vol. **3**, No. 2, pp. 6-8 (1997).
[31] http://www.distributed.net/index.html.en.
[32] http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker.
[33] R.D. Silverman, *A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths*, RSA Laboratories' Bulletin, No. 13, April 2000.
[34] E. Biham and L.R. Knudsen, *DES, Triple-DES and AES*, RSA Laboratories' Cryptobytes Vol. **4**, No. 1, pp. 18-23 (1998).
[35] http://www.nist.gov/aes.
[36] T. Rosa, *Future Cryptography: Standards Are Not Enough*, in *Proc. of Security and Protection of Information*, NATO – IDET, Military Academy in Brno, Brno, pp. 237-245 (2001).
[37] W.K. Wooters and W.H. Zurek, *A Single Quantum Cannot Be Cloned*, Nature **299**, pp. 802-803 (1982).
[38] C.E. Shannon, *Communication Theory of Secrecy Systems*, Bell Syst. Tech. J. **28**, pp. 656-715 (1949).
[39] http://www.nsa.gov/docs/venona/.
[40] C.H. Bennett, G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, IEEE, New York, pp. 175-179 (1984).
[41] S. Wiesner, *Conjugate Coding*, original manuscript written circa 1969, published in Sigact News, Vol. **15**, No. 1, pp. 78-88 (1983).
[42] C.H. Bennett, G. Brassard, and J.-M. Robert, *Privacy Amplification by Public Discussion*, SIAM J. Comput. **17**, No. 2, pp. 210-229 (1988).
[43] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *Experimental Quantum Cryptography*, J. Cryptology **5**, pp. 3-28 (1992).
[44] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, *Avalanche Photodiodes and Quenching Circuits for Single-photon Detection*, Appl. Opt. **35**, pp. 1956-1976 (1996).
[45] J. Peřina, *Quantum Statistics of Linear and Nonlinear Optical Phenomena*, Kluwer Academic Publishers, Dordrecht, Netherlands, Chapter 3 (1991).
[46] C. Fuchs, N. Gisin, R.B. Griffits, C.-S. Niu, and A. Peres, *Optimal Eavesdropping in Quantum Cryptography, I. Information Bound and Optimal Strategy*, Phys. Rev. A **56**, pp. 1163-1172 (1997).
[47] J.L. Carter and M.N. Wegman, *Universal Classes of Hash Functions*, J. Comp. Sys. Sci. **18**, pp. 143-154 (1979).
[48] M.N. Wegman and J.L. Carter, *New Hash Functions and Their Use in Authentication and Set Equality*, J. Comp. Sys. Sci. **22**, pp. 265-279 (1981).
[49] D.R. Stinson, *Cryptography, Theory and Practice*, CRC Press, Inc., Boca Raton, Chap. 10 (1995).
[50] C.H. Bennett, private communication.

[51] N. Lütkenhaus, *Security against Eavesdropping in Quantum Cryptography*, Phys. Rev. A **54**, pp. 97-111 (1996).

[52] N. Lütkenhaus, *Security against Individual Attacks for Realistic Quantum Key Distribution*, Phys. Rev. A **61**, 052304 (2000).

[53] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, *Security of Quantum Key Distribution Against All Collective Attacks*, Los Alamos Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9801022.

[54] D. Mayers, *Unconditional Security in Quantum Cryptography*, Los Alamos Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9802025.

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

[56] H. Inamori, N. Lütkenhaus and D. Mayers, *Unconditional Security of Practical Quantum Key Distribution*, Los Alamos Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/0107017.

[57] M.O. Rabin, *How to Exchange Secrets by Oblivious Transfer*, Technical Report TR-81, Aiken Computation Laboratory, Harvard University (1981).

[58] G. Brassard, C. Crépeau, R. Josza, and D. Langlois, *A Quantum Bit Commitment Scheme Provably Unbreakable by Both Parties*, in *Proc. 34th Annual IEEE Symp. Found. of Comp. Sci*., pp. 362-371, Palo Alto (1993).

[59] C.H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, *Quantum Cryptography, or Unforgeable Subway Tokens*, in *Advances in Cryptology: Proc. of Crypto '82*, pp. 267-275, Plenum, New York (1982).

[60] D. Mayers, *Unconditionally Secure Quantum Bit Commitment Is Impossible*, Los Alamos Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9605044.

[61] D. Mayers, *The Trouble with Quantum Bit Commitment*, Los Alamos Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9603015.

[62] H.-K. Lo and H.F. Chau, *Why Quantum Bit Commitment and Ideal Quantum Coin Tossing Are Impossible*, Los Alamos Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9711065.

[63] H.F. Chau and H.-K. Lo, *Making an Empty Promise with a Quantum Computer*, Los Alamos Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9709053.

[64] C.H. Bennett and G. Brassard, *The Dawn of a New Era for Quantum Cryptography: The Experimental Prototype Is Working!* Sigact News **20**, No. 4, pp. 78-82 (1989).

[65] A. Muller, J. Bréguet, and N. Gisin, *Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over More than 1 km*, Europhys. Lett. **23**, pp. 383-388 (1993).

[66] J. Bréguet, A. Muller, and N. Gisin, *Quantum Cryptography with Polarized Photons in Optical Fibers: Experimental and Practical Limits*, J. Mod. Opt. **41**, pp. 2405-2412 (1994).

[67] J.D. Franson and H. Ilves, *Quantum Cryptography Using Polarization Feedback*, J. Mod. Opt. **41**, pp. 2391-2396 (1994).

[68] J.D. Franson and B.C. Jacobs, *Operational System for Quantum Cryptography*, Electron. Lett. **31**, pp. 232-234 (1995).

[69] A. Muller, H. Zbinden, and N. Gisin, *Underwater Quantum Coding*, Nature **378**, p. 449 (1995).

[70] A. Muller, H. Zbinden, and N. Gisin, *Quantum Cryptography over 23 km in Installed Under-Lake Telecom Fibre*, Europhys. Lett. **33**, pp. 335-339 (1996).

[71] P.D. Townsend, J.G. Rarity, and P.R. Tapster, *Single Photon Interference in 10 km Long Optical Fibre Interferometer,* Electron. Lett. **29**, pp. 634-635 (1993).

[72] P.D. Townsend, J.G. Rarity, and P.R. Tapster, *Enhanced Single Photon Fringe Visibility in a 10 km-Long Prototype Quantum Cryptography Channel*, Electron. Lett. **29**, pp. 1291-1293 (1993).

[73] P.D. Townsend and I. Thompson, *A Quantum Key Distribution Channel Based on Optical Fibre*, J. Mod. Opt. **41**, pp. 2425-2433 (1994).

[74] P.D. Townsend, *Secure Key Distribution System Based on Quantum Cryptography*, Electron. Lett. **30**, pp. 809-810 (1994).

[75] P.D. Townsend, *Simultaneous Quantum Cryptographic Key Distribution and Conventional Data Transmission over Installed Fibre Using WDM*, Electron. Lett. **33**, pp. 188-190 (1997).

[76] C. Marand and P.D. Townsend, *Quantum Key Distribution over Distances As Long As 30 km*, Opt. Lett. **20**, pp. 1695-1697 (1995).

[77] http://www.fysel.ntnu.no/research/index_e.html.

[78] A. Muller, T. Herzog, B. Huttner, W.Tittel, H. Zbinden, and N. Gisin, *'Plug and Play' Systems for Quantum Cryptography*, Appl. Phys. Lett. **70**, pp. 793-795 (1997).

[79] H. Zbinden, J.-D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, *Interferometry with Faraday Mirrors for Quantum Cryptography*, Electron. Lett. **33**, pp. 586-588 (1997).

[80] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, *Automated "Plug & Play" Quantum Key Distribution*, Electron. Lett. **34**, pp. 2116-2117 (1998).

[81] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, *Fast and User-Friendly Quantum Key Distribution*, J. Mod. Opt. **47**, pp. 517-531 (2000).

[82] M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren, and E. Sundberg, *Experiments on Long Wavelength (1550 nm) 'Plug and Play' Quantum Cryptography System*, Opt. Express **4**, pp. 383–387 (1999).

[83] M. Bourennane, D. Ljunggren, A. Karlsson, P. Jonsson, A. Hening, and J. P. Ciscar, *Experimental Long Wavelength Quantum Cryptography: From Single Photon Transmission to Key Extraction Protocols*, J. Mod. Opt. **47**, pp. 563–579 (2000).

[84] D. Bethune and W. Risk, *An Autocompensating Fiberoptic Quantum Cryptography System Based on Polarization Splitting of Light*, IEEE J. Quantum Electron. **36**, pp. 340–347 (2000).

[85] B.C. Jacobs and J.D. Franson, *Quantum Cryptography in Free Space*, Opt. Lett. **21**, pp. 1854–1856 (1996).

[86] W.T. Buttler, R.J. Hughes, P.G. Kwiat, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, and C.M. Simmons, *Free-Space Quantum-Key Distribution*, Physical Review A **57**, pp. 2379-2382 (1998).

[87] W.T. Buttler, R.J. Hughes, P.G. Kwiat, S.K. Lamoreaux, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, and C. Simmons, *Practical Free-Space Quantum Key Distribution over 1 km*, Phys. Rev. Lett. **81**, pp. 3283–3286 (1998).

[88] R.J. Hughes, W.T. Buttler, P.G. Kwiat, S.K. Lamoreaux, G.L. Morgan, J.E. Nordhold, and C.G. Peterson, *Free-Space Quantum Key Distribution in Daylight*, J. Mod. Opt. **47**, pp. 549–562 (2000).

[89] W.T. Buttler, R.J. Hughes, S.K. Lamoreaux, G.L. Morgan, J.E. Nordholt, and C.G. Peterson, *Daylight Quantum Key Distribution over 1.6 km*, Phys. Rev. Lett. **84**, pp. 5652–5655 (2000).

[90] P.M. Gorman, P.R. Tapster, and J.G. Rarity, *Secure Free-Space Key Exchange to 1.9 km and Beyond*, J. Mod. Opt. **48**, pp. 1887–1901 (2001).

[91] http://scotty.quantum.physik.uni-muenchen.de/exp/qc/poster_qc.pdf.

[92] C.H. Bennett, *Quantum Cryptography Using Any Two Nonorthogonal States*, Phys. Rev. Lett. **68**, pp. 3121-3124 (1992).

[93] R.J. Hughes, D.M. Alde, P. Dyer, G.G. Luther, G.L. Morgan, and M. Schauer, *Quantum Cryptography*, Contemporary Physics **36**, p. 149 (1995).

[94] R.J. Hughes, G.G. Luther, G.L. Morgan, C.G. Peterson, and C. Simmons, *Quantum Cryptography over Underground Optical Fibers*, in *Advances in Cryptology – Proc. Crypto 96'*, Springer, Berlin (1996).

[95] R.J. Hughes, G.G. Luther, G.L. Morgan, C.G. Peterson, and C. Simmons, in *Lecture Notes Comput. Sci*. **1109**, Ed. by N. Koblinz, Springer, New York, pp. 329-342 (1996).

[96] R.J. Hughes, G.L. Morgan, and C.G. Peterson, *Quantum Key Distribution over a 48-km Optical Fiber Network*, J. Mod. Opt. **47**, pp. 533-547 (2000).

[97] A.K. Ekert, *Quantum Cryptography Based on Bell's Theorem*, Phys. Rev. Lett. **67**, pp. 661-663 (1991).

[98] A.K. Ekert, J.G. Rarity, P. Tapster, and G.M. Palma, *Practical Quantum Cryptography Based on Two-Photon Interferometry*, Phys. Rev. Lett. **69**, pp. 1293-1295 (1992).

[99] J.G. Rarity, J. Burnett, P.R. Tapster, and R. Paschotta, *High-Visibility 2-Photon Interference in a Single-Mode-Fiber Interferometer*, Europhys. Lett. **22**, pp. 95-100 (1993).

[100] J.G. Rarity, P.C.M. Owens, and P.R. Tapster, *Quantum Random-Number Generation and Key Sharing*, J. Mod. Opt. **41**, pp. 2435-2444 (1994).

[101] A.K. Ekert and G.M. Palma, *Quantum Cryptography with Interferometric Quantum Entanglement*, J. Mod. Opt. **41**, pp. 2413-2423 (1994).

[102] D.S. Naik, C.G. Peterson, A.G. White, A.J. Berglund, and P.G. Kwiat, *Entangled State Quantum Cryptography: Eavesdropping on the Ekert Protocol*, Phys. Rev. Lett. **84**, pp. 4733-4736 (2000).

[103] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, *Quantum Cryptography with Entangled Photons*, Phys. Rev. Lett. **84**, pp. 4729-4732 (2000).

[104] C.H. Bennett, G. Brassard, and N.D. Mermin, *Quantum Cryptography Without Bell's Theorem*, Phys. Rev. Lett. **68**, pp. 557-559 (1992).

[105] W. Tittel, J. Brendel, N. Gisin, and H. Zbinden, *Long-Distance Bell-Type Tests Using Energy-Time Entangled Photons*, Phys. Rev. A **59**, pp. 4150-4163 (1999).

[106] G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin and H. Zbinden, *Long-Distance Entanglement-Based Quantum Key Distribution*, Phys. Rev. A **63**, 012309 (2001).

[107] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, *Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication*, Phys. Rev. A **82**, pp. 2594-2597 (1999).

[108] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, *Quantum Cryptography Using Entangled Photons in Energy-Time Bell States*, Phys. Rev. Lett. **84**, pp. 4737-4740 (2000).

[109] W. Tittel, H. Zbinden, and N. Gisin, *Experimental Demonstration of Quantum Secret Sharing*, Phys. Rev. A **63**, 042301 (2001).

[110] W. Tittel, H. Zbinden, and N. Gisin, *Quantum Secret Sharing Using Pseudo-GHZ States*, Los Alamos Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9912035.

[111] D. Deutch, A.K. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, *Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels*, Phys. Rev. Lett. **77**, pp. 2818-2821 (1996).

[112] C. Macchiavello and A. Sanpera, *An Unconditionally Secure Protocol for Quantum Cryptography*, Acta Phys. Slov. **46**, pp. 439-444 (1996).

[113] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W. Wootters, *Mixed-State Entanglement and Quantum Error Correction*, Phys. Rev. A **54**, pp. 3824-3851 (1996).

[114] W. Dür, H.-J. Briegel, J.I. Cirac, and P. Zoller, *Quantum Repeaters Based on Entanglement Purification*, Phys. Rev. A **59**, pp. 169-181 (1999).

[115] D. Bruss, *Optimal Eavesdropping in Quantum Cryptography with Six States*, Phys. Rev. Lett. **81**, pp. 3018-3021 (1998).

[116] L. Goldenberg and L. Vaidman, *Quantum Cryptography Based on Orthogonal States*, Phys. Rev. Lett. **75**, pp. 1239-1243 (1995).

[117] A. Peres, *Quantum Cryptography with Orthogonal States?* Phys. Rev. Lett. **77**, p. 3264 (1996).

[118] L. Goldenberg and L. Vaidman, *A Reply to the Comment* by Asher Peres, Phys. Rev. Lett. **77**, p. 3265 (1996).

[119] P.C. Sun, Y. Mazurenko, and Y. Fainman, *Long-Distance Frequency-Division Interferometer for Communication and Quantum Cryptography*, Opt. Lett. **20**, pp. 1062-1064 (1995).

[120] P.D. Townsend, S.J.D. Phoenix, K.J. Blow, and S.M. Barnett, *Design of Quantum Cryptography Systems for Passive Optical Networks*, Electron. Lett. **30**, pp. 1875-1876 (1994).

[121] S.J.D. Phoenix, S.M. Barnett, P.D. Townsend, and K.J. Blow, *Multi-User Quantum Cryptography on Optical Networks*, J. Mod. Opt. **42**, pp. 1155-1163 (1995).

[122] H.-J. Briegel, W. Dür, J.I. Cirac, and P. Zoller, *Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication*, Phys. Rev. Lett. **81**, pp. 5932-5935 (1998).

[123] H.P. Yuen, *High-Rate Strong-Signal Quantum Cryptography*, in *Proc. 1995 Conf. on Squeezed States and Uncertainty Relations*, NASA Conference publication 3322, pp. 363-368 (1996).

[124] T.C. Ralph, *Continuous Variable Quantum Cryptography*, Phys. Rev. A **61**, 010303 (2000).

[125] M. Hillery, *Quantum Cryptography with Squeezed States*, Phys. Rev. A **61**, 022309 (2000).

[126] C. Silberhorn, N. Korolkova, and G. Leuchs, *Quantum Key Distribution with Bright Entangled Beams*, Phys. Rev. Lett. **88**, 167902 (2002).

[127] C. Silberhorn, T.C. Ralph, N. Lütkenhaus, and G. Leuchs, *Continuous Variable Quantum Cryptography – Beating the 3 dB Loss Limit*, Los Alamos Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/0204064.

[128] C. Crépeau and L. Salvail, *Quantum Oblivious Mutual Identification*, in *Advances in Cryptology: Proc. of Eurocrypt '95*, Springer-Verlag, Berlin, pp. 133-146 (1995).

[129] C.H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, *Practical Quantum Oblivious Transfer*, in *Advances in Cryptology: Proc. of Crypto '91*, Lecture Notes in Comp. Sci., Vol. **576**, Springer-Verlag, Berlin, pp. 351-366 (1992).

[130] C. Crépeau, *Quantum Oblivious Transfer*, J. Mod. Opt. **41**, pp. 2445-2454 (1994).

[131] D.S. Mitrinović, *Analytic Inequalities*, Springer-Verlag, Berlin (1970).

[132] G.R. Blakley, *Safeguarding Cryptographic Keys*, in *AFIPS Conference Proceedings* **48**, pp. 313-317 (1979).

[133] A. Shamir, *How To Share a Secret*, Communications of the ACM **22,** pp. 612-613 (1979).

[134] M. Hillery, V. Bužek, and A. Berthiaume, *Quantum Secret Sharing*, Phys. Rev. A **59**, pp. 1829-1834 (1999).

[135] M. Hillery, V. Bužek, *Secret Sharing via Quantum Entanglement*, Acta Phys. Slov. **49**, pp. 533-539 (1999).

[136] D.M. Greenberger, M.A. Horne, A. Zeilinger, *Going Beyond Bell's Theorem*, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, ed. M. Kafatos, Kluwer, Dordrecht, pp. 73-76 (1989).

[137] D.M. Greenberger, M.A. Horne, A. Shimony, and A. Zeilinger, *Bell's Theorem Without Inequalities*, Am. J. Phys. **58**, pp. 1131-1143 (1990).

[138] N.D. Mermin, *What's Wrong with These Elements of Reality?* Physics Today **43**, pp. 9-11 (1990).

[139] N.D. Mermin, Am. J. Phys. **58**, *Quantum Mysteries Revisited*, pp. 731-734 (1990).

[140] A. Karlsson, M. Koashi, N. Imoto, *Quantum Entanglement for Secret Sharing and Secret Splitting*, Phys. Rev. A **59**, pp. 162-168 (1999).

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

[142] Commentary of Rosenfeld on the EPR paper in 1967, in *Quantum Theory and Measurement*, Eds. J.A. Wheeler and W.H. Zurek, Princeton University Press, Princeton, New Jersey, p. 137 (1983).

[143] D. Bohm, *Quantum Theory*, Prentice-Hall, Englewood Cliffs, Chap. 22, Sec. 16, p. 614 (1951).

[144] J. Bell, *On the Einstein Podolsky Rosen Paradox*, Physics **1**, pp. 195-200 (1964).

[145] A. Einstein in *Albert Einstein, Philosopher Scientist*, Ed. P.A. Schilp, Library of Living Philosophers, Evanston, Illinois, p. 85 (1949).

[146] C.S. Wu and I. Shaknov, *The Angular Correlation of Scattered Annihilation Radiation*, Phys. Rev. **77**, p. 136 (1950).

[147] S.J. Freedman and J.S. Clauser, *Experimental Test of Local Hidden-Variable Theories*, Phys. Rev. Lett. **28**, pp. 938-941 (1972).

[148] A. Aspect, P. Grangier and G. Roger, *Experimental Tests of Realistic Local Theories via Bell's Theorem*, Phys. Rev. Lett. **47**, pp. 460-463 (1981).

[149] A. Aspect, P. Grangier and G. Roger, *Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities*, Phys. Rev. Lett. **49**, pp. 91-94 (1982).

[150] A. Aspect, J. Dalibard and G. Roger, *Experimental Tests of Bell's Inequalities Using Time-Varying Analyzers*, Phys. Rev. Lett. **49**, pp. 1804-1807 (1982).

[151] J.F. Clauser, *Experimental Investigation of Polarisation Anomaly*, Phys. Rev. Lett. **36**, pp. 1223-1226 (1976).

[152] E.S. Fry and R.C. Thompson, *Experimental Test of Local Hidden-variable Theories*, Phys. Rev. Lett. **37**, pp. 465-468 (1976).

[153] M. Lamehi-Rachti and W. Mitting, *Quantum Mechanics and Hidden Variables: A Test of Bell's Inequality by the Measurement of the Spin Correlation in Low-Energy Proton-Proton Scattering*, Phys. Rev. D **14**, pp. 2543-2555 (1976).

[154] P.G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A.V. Sergienko, and Y. Shih, *New High-Intensity Source of Polarization-Entangled Photon Pairs*, Phys. Rev. Lett. **75**, pp. 4337-4341 (1995).

[155] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt, *Proposed Experiment to Test Local Hidden-Variable Theories*, Phys. Rev. Lett. **23**, pp. 880-884 (1969).

[156] M. Atatüre, G. Di Giuseppe, M. Shaw, A.V. Sergienko, B.E.A. Saleh, and M.C. Teich, *Multiparameter Entanglement in Quantum Interferometry*, Los Alamos Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/0111024.